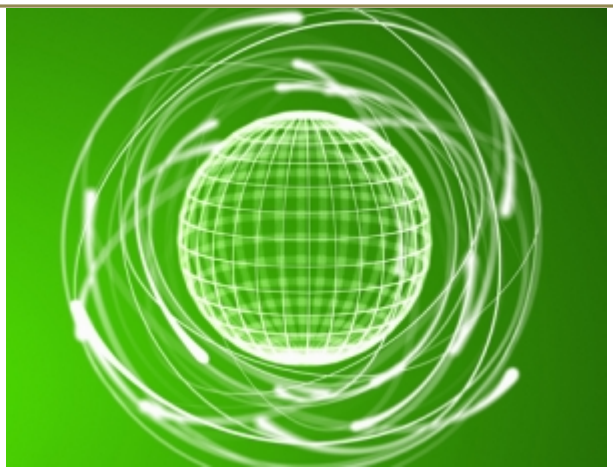
Universitat Oberta de Catalunya



Grado de Tecnologías de Telecomunicación

REDES WIRELESS INDUSTIRALES

TFG

Joaquin Sala Fayos - Semestre 2014-2

UOC Universitat Oberta de Catalunya

Título:

REDES WIRELESS INDUSTRIALES

Grado de Tecnologías de Telecomunicación

Semestre 2014-2

Joaquin Sala Fayos

Profesor responsable de la asignatura:

Xavi Vilajosana Guillen

Consultor:

Jose Lopez Vicario

Aplicaciones y servicios multimedia

Estudios de Informática, Multimedia y Telecomunicación

JUNIO 2014

Resumen

Este proyecto realiza un recorrido a través de las redes industriales Wireless, empezando por un análisis de las problemáticas a las que se ven expuestas, para comprender las problemáticas que deben superar e para llegar a cubrir los requerimientos que se exigen en las redes industriales. Posteriormente se mostraran los conceptos básicos de enlaces radioeléctricos que aplican directamente a las redes Wireless Industriales que se deben conocer todo ingeniero que pretenda diseñar redes Wireless. Se tendrá la oportunidad de ver como difieren las redes Wireless industriales a las comerciales, profundizando en los requerimientos que deben cumplir las redes Wireless Industriales para llegar a poder ser parte fundamental de cualquier red industrial y poder llegar a los niveles de implantación como los alcanzados en redes comerciales donde el Wireless está presente de forma masiva. En el proyecto nos contrataremos en uno de los aspectos que más le está afectando hoy en día a las redes Wireless Industriales y que hace que no alcance los niveles de implementación como lo han realizado las redes comerciales, la Confiabilidad por parte del usuario final e ingenieros involucrados en el diseño de redes industriales y de instrumentación y control que suelen tener la responsabilidad del diseño de las mismas en el sector de la Industria de la Automatización y Control (IACS). Veremos los aspectos que influyen directamente a la confiabilidad como la fiabilidad, mantenibilidad, testabilidad, seguridad, confidencialidad, resiliencia, etc. Una vez llegado a este punto, veremos cuáles son los principales componentes en una red industriales como los PLC's (Programmable Logic Controllers), SCADA (Supervisory Control and Data Acquisition) y el DCS (Distributed Control System), donde uno de los principales objetivos de las redes Industriales es la comunicación con y entre estos sistemas. Todo seguido, se verá cuáles son los principales estándares inalámbricos que son candidatos a la implantación en entornos industriales, centrándonos en los dos grandes ganadores a día de hoy que son WirelessHART e ISA100.11a, debido principalmente que han sido diseñados específicamente para la IACS. Se verá en detalle ambas tecnologías en base al modelo OSI, analizándolas desde la capa física hasta la capa de aplicación. Del mismo modo se muestra una comparativa entre ambas donde se aprecian las similitudes y diferencias, y se podrá conocer que tecnología cuenta con mayor presencia y aceptación en el mercado y por qué. Finalmente, se realizara una implantación paso a paso de una red WirelessHART en una planta de procesado de Hidrogeno del cliente Pemex en México, desde la definición de la dimensión de la red, realizando el diseño de la red aplicando adecuadamente todas las reglas y directrices adecuadamente, definiendo y aplicando la seguridad adecuada y finalmente viendo la integración de la red Wireless de campo con el sistema de control central.

Tabla de Contenido

Capítulo 1 . Introducción

1.1 Justificación del tópico y su relevancia

Actualmente somos testigos de cómo las redes Wireless han crecido rápidamente en el sector residencial y comercial, debido principalmente a la reducción tan significativa en los costos del diseño, instalación de cableado y mantenimiento, sin embargo, no ha ocurrido lo mismo en el sector industrial. A pesar de que esta ventaja pudiese parecer clave para el crecimiento de las redes Wireless en el sector industrial, las exigencias en el sector van mucho más allá que las requeridas en el sector residencial o comercial. Estos requerimientos son concernientes a la fiabilidad y rendimiento, así como a la seguridad, la disponibilidad y la privacidad, que junto al desconocimiento de la tecnología de una gran parte de técnicos, no permiten que el despliegue y la aceptación sean una tarea fácil, sobre todo en plantas industriales, es por esta razón, por lo que todavía no ha tenido un gran crecimiento.

Actualmente las tecnologías inalámbricas en el área industrial están en constante mejora y hay un gran interés por parte de grandes integradores en promocionarlas. Entre las tecnologías inalámbricas de mayor proyección en la Industria de la Automatización y Control de Sistemas (IACS), podemos encontrar: ISA100 Wireless (ISA100.11a), WirelessHART, WIA- PA, así como los protocolos Wi-Fi (IEEE 802.11n y 802.11ac)

Es por esta razón que este proyecto pretende analizar la tecnología Wireless, mostrando qué requisitos debe cubrir la tecnología para ser robusta y fiable, haciendo un estudio a modo comparativo de las tecnologías con mayor proyección disponibles en el mercado como son ISA100 Wireless (ISA100.11a) y WirelessHART. Del mismo modo, se analiza de qué forma estas llegan a cubrir los requisitos en cuestión de seguridad, disponibilidad y privacidad en la IACS.

1.2 Análisis de las problemáticas y beneficios

Parece un hecho que las redes Wireless sean la mejor alternativa en cuestión económica a las ya consolidadas redes cableadas. No obstante, estas aún cuentan con algunas limitaciones que hay que considerar a la hora de realizar un diseño Wireless e implementar la misma en la IACS, que hacen que se complemente al cableado. Hay que tener en cuenta que el Wireless y el cableado no son dos componentes IT separados, estos deben ser parte integral para satisfacer todos los requisitos de cualquier proyecto en la IACS (International Society of Automation, 2011). Aun así, se está realizando un gran esfuerzo día a día, en buscar soluciones que hagan más eficiente la tecnología Wireless y que llegue a niveles de fiabilidad, robustez y rendimiento incluso en algunos casos más altos que el cableado.

A continuación se muestran algunas de las limitaciones a las que se debe enfrentar la tecnología Wireless hoy en día según el entorno donde se aplican, para ganarse la confianza en la IACS.

Para que las redes Wireless no pierdan la gran ventaja que ofrecen de la movilidad, obliga a la industria a buscar alternativas a la alimentación energética externa, como cableado o mediante PoE (Power

over Ethernet), estándar que suministra la corriente eléctrica mediante el cableado de red, el cual fue creado para evitar la dependencia de fuentes de alimentación externas. Por lo que, la alternativa actual de alimentación de los dispositivos Wireless es médiate baterías internas limitadas en el tiempo. Hoy en día ofrecen una durabilidad de incluso hasta 10 años.

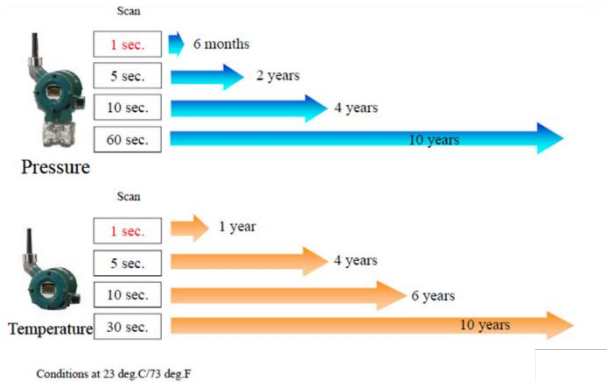


Figure 1: Consumo batería según tiempo refresco. Padilla J.J. (n.d.)

Otros de los inconvenientes que se pueden sufrir con las instalaciones inalámbricas son las pérdidas de señal (Fading). Muchas veces se puede experimentar como la cobertura Wireless o la señal del móvil desaparece y de repente vuelve aparecer sin ningún motivo aparente, a veces sin dejarte tiempo a poder ver cuál es la causa que ha motivado este desvanecimiento.

La señal Wireless en las frecuencias usadas en la IACS, puede sufrir interferencias por consecuencia de otras señales de radio que puedan haber presentes: señales microondas, teléfonos inalámbricos a 2.4 GHz, etc.

La propagación de las ondas de radio son lineales y muy parecidas a las ondas de la luz, del mismo modo, estas pueden pasar a través de los cristales u objetos transparentes sin ser muy afectadas por la atenuación, pero, en materiales densos como por ejemplo muros, la atenuación será proporcional a la densidad del objeto cruzado. También hay materiales, que suele absorber o atenuar la mayoría de señales y están muy presentes en plantas industriales, como son los metales, especialmente el acero inoxidable, el cual crea puntos muertos de sombra. Las ondas de radio, a menor frecuencia, mejor pasan a través de los materiales, pero no pasa lo mismo con las superficies metálicas, independientemente de la longitud de onda, la onda siempre es reflejada (PEPPERL+FUCHS, 2012).

Otro elemento que influye a las ondas de radio es el sol, el cual aporta su parte de ruido, ya que al emitir un amplio espectro de ondas electromagnéticas en todas las frecuencias, estas interfieren en transmisiones de radio, llegando incluso a la posibilidad de interferir en comunicaciones cableadas.

Otra de las problemáticas del Wireless que hoy en día ya empieza a dejar de serlo, porque está siendo usada de forma beneficiosa, es el Multipath Distortion. Este fenómeno puede distorsionar la señal a lo largo de una transmisión hasta el punto de anularla, debido a la reflexión de la señal en objetos sólidos como puedan ser metales, muros, personas, etc. del mismo modo como hemos comentado anteriormente lo hace la luz en los cristales. Este puede llegar incluso a darse en zonas abiertas (Open path). Por otro lado, puede ocasionar el efecto contrario, cuando las señales afectadas por el Multipath

son recibidas con la misma fase, esto ocasiona un aumento en la señal, del mismo modo que lo harían varias antenas transmitiendo al mismo tiempo. Es por este hecho que se esté usando de forma beneficiosa en el estándar IEEE 802.11n, usando una tecnología de múltiples antenas de forma conjunta para transmisión y emisión, llamada MIMO (Multiple Input, Multiple Output).

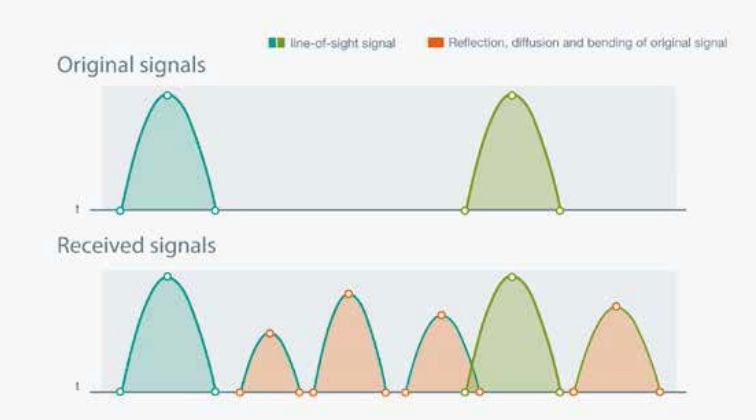


Figura 1: La recepción de la señal original y sus reflexiones, flexiones, y difusiones (Fuente: PEPPERL+FUCHS, 2012)

Otras de las problemáticas a las cuales está expuesto el Wireless es que el espectro de radio está limitado. Como podemos ver en el artículo "*Will we ever... face a wireless 'spectrum crunch'?*" escrito el 15 Octubre del 2013 por Frank Swain para la BBC. Donde habla de cómo el problema es que cada vez son más los dispositivos presentes en la sociedad que usan el espectro de radio para enviar y recibir datos, sobre todo en las bandas libres como la banda de los 2,4 GHz. Al principio cuando los gobiernos dividieron este lo hicieron según sus usos sin reparar en cuán rápido podían crecer unos u otros, como la radio, la televisión, la navegación, la astronomía, la marítima, la aeronáutica, la militar y las telecomunicaciones. A consecuencia de esto, se ha generado una situación en la que mientras parte del espectro reservado para los militares siguen sin usarse, otros se están saturando, como el de las telecomunicaciones. Simon Saunders director de tecnología de Real Wireless, una consultora independiente basada en Pulborough, Reino Unido, comento: "Hay un alto riesgo a que el espectro se colapse hacia el 2020"…" Si el problema no es solucionado pronto, en áreas locales con una alta demanda hay riesgo de que todo se ralentice". En mi opinión esto es totalmente posible, ya que los sistemas Wireless crecen a un ritmo incontrolado, alrededor de nosotros hay miles de señales Wireless desde uso doméstico hasta industrial, y pasando por servicios para telefonía móvil hasta la televisión, lo que se traduce en un sinfín de emisiones de radio. Una posible solución podría ser unificar estas en un mismo servicio y de esta forma optimizar la distribución de acuerdo a la demanda, para llegar a reducir de forma significativa el consumo de espectro. Este es un problema que ya se debe tratar de forma global y deberían dedicar esfuerzos en la búsqueda de la unificación de servicios y de este modo liberar parte del espectro. Cabe mencionar, que los gobiernos ya son conscientes del problema y están viendo formas de poder solucionarlo antes de que todo el sistema empiece a fallar, por ahora la principal estrategia que se han definido, es la de buscar más espectro, lo cual no es tarea fácil. El principal organismo de la regulación del espectro, es "The International Telecommunication Union", que ha planificado una conferencia en el 2015 en el World Radio Conference en Ginebra para discutir sobre este problema (Swain, 2013).

Otro de los grandes retos a los que se enfrenta hoy en día y en los cuales se invierten muchos esfuerzos es la seguridad. Una vez se transmiten datos a través de medios inalámbricos quedan expuestos a posible pérdida de privacidad, ya que todo el mundo con un sistema adecuado puede recibirlo. Algo que no parece posible con las redes cableadas, pareciendo que estas solo quedan expuestas si se realiza una conexión física a la misma red o si tienen acceso a internet sin sistemas de protección adecuados.

Con Wireless se queda expuesto desde el primer momento a posibles interferencias inalámbricas (Jamming). También son vulnerables al Hacking, donde un hacker puede acceder a la red Wireless, con la posibilidad de llegar a robar datos o infectar a los nodos con software malicioso. Sin embargo, existen métodos que permiten que una conexión Wireless pueda llegar a ser más segura que una cableada.

Una combinación de encriptación, espectro ensanchado en todas sus formas es la base para un alto grado de seguridad Wireless. La técnica de modulación del espectro ensanchado permite aplicar métodos para mejorar la seguridad en la información comunicada, como la difusión y el entrelazado. Estos métodos pueden hacer que las transmisiones de radio sean imposibles de interceptar si no se tienen conocimiento de ellas. Una de sus principales ventajas es que resiste todo tipo de interferencias, tanto las no intencionadas como las malintencionadas (más conocidas con el nombre de jamming)[1]. Como protección adicional contra la explotación de la señal, hay disponibles niveles de cifrado para aumentar la seguridad de la red inalámbrica (International Society of Automation, 2011).

Existen cinco técnicas de espectro ensanchado: Sistemas de secuencia directa, Sistemas de salto de frecuencia, Sistemas de salto temporal, Sistemas de frecuencia modulada pulsada (o Chirping) y Sistemas híbridos. Este último que aún no está disponible comercialmente, es una combinación del sistema de secuencia directa y el sistema de salto de frecuencia, operando por debajo del nivel del ruido a excepción de cuando se sincronizan periódicamente los relojes, y es prácticamente indetectable sino se cuenta con sofisticados medios. Resiste todo tipo de interferencias, tanto las no intencionadas como las malintencionadas (más conocidas con el nombre de Jamming), siendo más efectivo con las de banda estrecha.

Por último, también podríamos ver como una problemática, la dificultad a la hora de desarrollar la estimación de un proyecto mediante tecnología Wireless, esta puede llegar a ser más complicada de lo que sería mediante cableado. Ya que mediante cableado a la hora de estimar se tienen en cuenta el total de los costes de los materiales a granel, como pueden ser: cableado de red, cableado de alimentación, armarios, cajas de empalmes, así como la instalación de los mismos. En Wireless se deben considerar tanto cableado hasta cada uno de los puntos de acceso, los equipos Wireless y las pruebas de cobertura que puedan requerir los mismos.

[1] http://en.wikipedia.org/wiki/Spread_spectrum

Una vez vistas las posibles problemáticas, se muestran algunos de los principales beneficios clave de la tecnología Wireless:

- Menores costes y tiempo en instalación, mantenimiento y puesta en marcha, algo muy significativo en grandes proyectos. Reduce el número de cableado, racks, bandejas, cajas de distribución.
- Facilita el despliegue de dispositivos móviles y rotacionales, incluso en áreas hostiles y remotas.
- Amplia en ámbito de monitorización a aplicaciones que antes no se consideraban por los costes de la implementación mediante cableado.
- Mantiene la eficiencia de la transmisión de datos respecto del desgaste de equipos.
- Facilita la introducción de sistemas de Micro-electromecánicos (MEMS, Micro-Electromechanical Systems), cuyas ventajas incluyen un aumento de la eficiencia de los costes, bajo consumo de energía, alto rendimiento e integración (Flammini et al, 2008).
- Un grado bastante aceptable de eficiencia en las comunicaciones sin altos costes de conexión (Forgue, 2010).
- Una vez implementada e instalada, ofrece una alta escalabilidad mediante la conexión directa de sensores a instrumentos existentes, minimizando los tiempos inactivos e interrupciones sin la necesidad del coste que supondría una nueva implementación.
- Ofrece mayor movilidad sobre la planta, lo que se traduce en una mayor seguridad de los operarios (como por ejemplo en el mantenimiento).

1.3 Objetivos principales

La principal motivación por la que seleccione este tema es debido a que me encuentro trabajando dentro de una empresa de ingeniería en el área de estimación de proyectos, en el cual puedo comprobar la importancia en el ahorro de costes, así como es conocer cuáles son las principales características de un proyecto, por lo que podre vincular mis conocimientos profesionales al desarrollo este trabajo. De igual forma este proyecto será de gran utilidad, y aprendizaje para alcanzar un mayor crecimiento profesional, ya que mi objetivo es especializarme en el diseño de redes de telecomunicaciones en el sector industrial, y para lograrlo necesito ampliar mis conocimiento de las diferentes tecnologías inalámbricas para poder sacar el máximo rendimiento a las mismas y de esta forma poder diseñar redes industriales inalámbricas bajo los requerimientos específicos de cada sector.

Dadas las condiciones económicas en el que la eficiencia ha pasado a ser un factor decisivo en la viabilidad y rendimiento de numerosas actividades empresariales e industriales, la implementación de

redes inalámbricas supone el paso obligado para la automatización y control de procesos. Que conllevaría una reducción bastante importante del peso de los costes en las cuentas de explotación, y que según el área de actividad se considera que puede alcanzar un porcentaje significativo. Justificando plenamente la inversión.

1.4 Estructura del documento

Este documento está dividido fundamentalmente en tres capítulos, los cuales se subdividen en subtemas con la intención de facilitar su lectura y entendimiento.

En el capítulo 1: Introducción, proporciona una justificación del tópico, la importancia y el análisis del estudio, así como, algunas ventajas y beneficios, sin embargo, para alcanzar un correcto análisis de la situación en el punto 1.2, se encuentran descritas las problemáticas y las dificultades. Una vez conociendo los puntos anteriores, se plantean los objetivos principales, a donde se prende llegar con esta investigación y para quienes se dirige.
Por último pero no menos importante son los Resultados potenciales que se pretenden alcanzar. Así como, la estructura del documento para darle un orden y explicación al mismo.

En el capítulo 2: Aspectos Básicos, Es la parte explicativa del documento que pretende dar una clara explicación de los aspectos técnicos básicos que son recomendables conocer antes de poder entrar en detalle a conocer los estándares Wireless en el sector industrial.

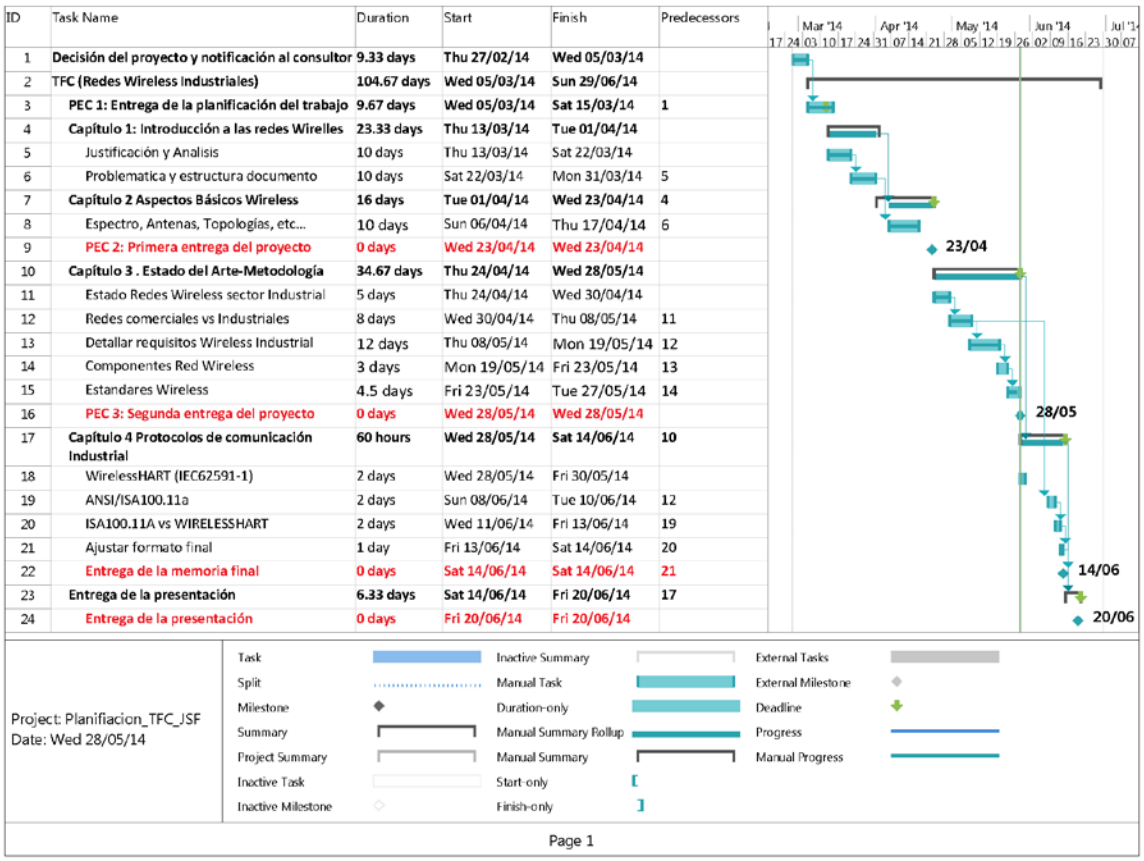
En el capítulo 3: El estado del Arte, que también se conoce como *Literature Review* es la parte más teórica y explicativa del documento que pretende dar una clara explicación de las aplicaciones técnicas, recursos, así como, un análisis del estudio, de las teorías y los resultados que se pueden aplicar al proyecto.

En el capítulo 4: Protocolos de comunicación Industrial, en este capítulo se abordará en detalle los protocolos con mayor implantación ahora mismo en la Industria de la Automatización y Control de Sistemas en el sector del Petróleo y el Gas para posteriormente finalizar el proyecto con una comparativa entre ambos.

En el capítulo 5: Diseño red WirelessHART , se abordará paso a paso el diseño de una red industrial Wireless siguiendo todas las guías de recomendación, así como los requerimientos que el cliente pueda tener al respecto, incluyendo la integración con el sistema central de control.

Finalmente las Conclusiones, se realiza un resumen de los aspectos más importantes a considerar.

1.5 Planificación



ID	Task Name	Duration	Start	Finish	Predecessors
1	**Decisión del proyecto y notificación al consultor**	**9.33 days**	**Thu 27/02/14**	**Wed 05/03/14**	
2	**TFC (Redes Wireless Industriales)**	**104.67 days**	**Wed 05/03/14**	**Sun 29/06/14**	
3	**PEC 1: Entrega de la planificación del trabajo**	**9.67 days**	**Wed 05/03/14**	**Sat 15/03/14**	**1**
4	**Capítulo 1: Introducción a las redes Wirelles**	**23.33 days**	**Thu 13/03/14**	**Tue 01/04/14**	
5	Justificación y Analisis	10 days	Thu 13/03/14	Sat 22/03/14	
6	Problematica y estructura documento	10 days	Sat 22/03/14	Mon 31/03/14	5
7	**Capítulo 2 Aspectos Básicos Wireless**	**16 days**	**Tue 01/04/14**	**Wed 23/04/14**	**4**
8	Espectro, Antenas, Topologías, etc...	10 days	Sun 06/04/14	Thu 17/04/14	6
9	PEC 2: Primera entrega del proyecto	0 days	Wed 23/04/14	Wed 23/04/14	
10	**Capítulo 3 . Estado del Arte-Metodología**	**34.67 days**	**Thu 24/04/14**	**Wed 28/05/14**	
11	Estado Redes Wireless sector Industrial	5 days	Thu 24/04/14	Wed 30/04/14	
12	Redes comerciales vs Industriales	8 days	Wed 30/04/14	Thu 08/05/14	11
13	Detallar requisitos Wireless Industrial	12 days	Thu 08/05/14	Mon 19/05/14	12
14	Componentes Red Wireless	3 days	Mon 19/05/14	Fri 23/05/14	13
15	Estandares Wireless	4.5 days	Fri 23/05/14	Tue 27/05/14	14
16	PEC 3: Segunda entrega del proyecto	0 days	Wed 28/05/14	Wed 28/05/14	
17	**Capítulo 4 Protocolos de comunicación Industrial**	**60 hours**	**Wed 28/05/14**	**Sat 14/06/14**	**10**
18	WirelessHART (IEC62591-1)	2 days	Wed 28/05/14	Fri 30/05/14	
19	ANSI/ISA100.11a	2 days	Sun 08/06/14	Tue 10/06/14	12
20	ISA100.11A vs WIRELESSHART	2 days	Wed 11/06/14	Fri 13/06/14	19
21	Ajustar formato final	1 day	Fri 13/06/14	Sat 14/06/14	20
22	Entrega de la memoria final	0 days	Sat 14/06/14	Sat 14/06/14	21
23	**Entrega de la presentación**	**6.33 days**	**Sat 14/06/14**	**Fri 20/06/14**	**17**
24	Entrega de la presentación	0 days	Fri 20/06/14	Fri 20/06/14	

Capítulo 2 Aspectos Básicos comunicaciones inalámbricas

2.1 Espectro Electromagnético

El Espectro Electromagnético es el rango en el cual se engloba la distribución energética del conjunto de las ondas electromagnéticas. El cual cubre las radiaciones desde menor longitud de onda hasta las ondas electromagnéticas de mayor longitud de onda, donde se ubican las ondas de radio.

Las ondas electromagnéticas con una longitud de onda corta son de alta frecuencia y disponen de mucha energía mientras que las ondas con grandes longitudes de onda son de baja frecuencia y disponen de poca energía.

A medida que varía la longitud de onda de las radiaciones electromagnéticas también lo hace su comportamiento. Del mismo modo, estas se suelen clasificar según su longitud de la onda:

- Ondas de radio
- Microondas
- Infrarrojos
- Ultravioleta (que percibimos como luz visible)
- Rayos X
- Rayos gamma.

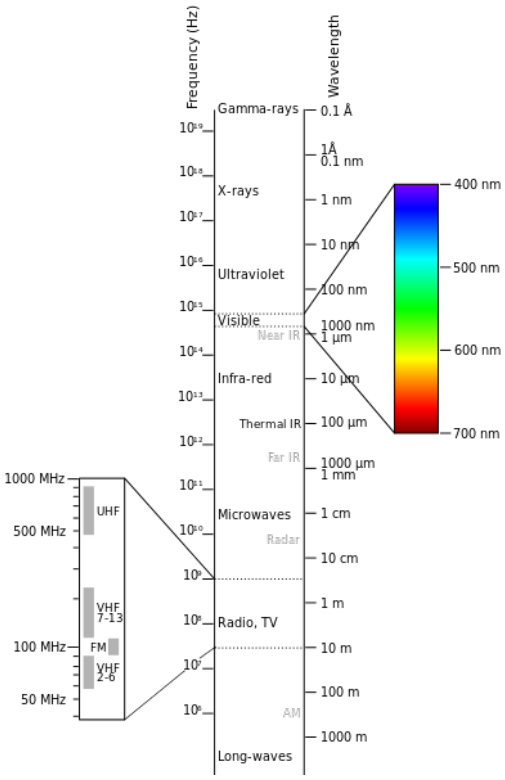


Figure 2: Espectro Electromagnético (Wikipedia, 2012)

Las ondas de radio tienen frecuencias que van desde los 300GHz hasta un mínimo de 3KHz, y las longitudes de ondas van desde 1 milímetro a 100 kilómetros[2].

La generación y uso de las ondas de radio está protegido por ley y regulado por la ITU (International Telecommunications Union), para prevenir que este se use de forma incontrolada o de forma que pueda generar interferencias entre los diferentes usuarios. Por este motivo, el radio espectro está dividido en bandas de radio como mostramos a continuación[3]:

Banda	*Abrev.*	*Banda ITU*	*Medio de propagación*	*Medios de transmisión*	*Frecuencia y longitud de onda (aire)*	*Ejemplos de uso*
Frecuencia tremendamente baja	TLF				< 3 Hz > 100,000 km	Frecuencia en la que trabaja la actividad neuronal
Frecuencia extremadamente baja	ELF	1			3–30 Hz 100,000 km – 10,000 km	Actividad neuronal, Comunicación con submarinos
Súper baja frecuencia	SLF	2			30–300 Hz 10,000 km – 1000 km	Comunicación con submarinos

[2] http://en.wikipedia.org/wiki/Radio_wave
[3] http://en.wikipedia.org/wiki/Radio_spectrum

Ultra baja frecuencia	ULF	3	Radio de onda larga	Pares de alambres	300–3000 Hz 1000 km – 100 km	Comunicación con submarinos, Comunicaciones en minas a través de la tierra
Muy baja frecuencia	VLF	4	Radio de onda larga	Pares de alambres	3–30 kHz 100 km – 10 km	Radioayuda, señales de tiempo, comunicación submarina, pulsómetros inalámbricos, Geofísica
Baja frecuencia	LF	5	Radio de onda larga	Pares de alambres	30–300 kHz 10 km – 1 km	Radioayuda, señales de tiempo, radiodifusión en AM (onda larga) (Europa y partes de Ásia), RFID, Radioafición
Frecuencia media	MF	6	Radio de onda larga	Cable coaxial	300–3000 kHz 1 km – 100 m	Radiodifusión en AM (onda media), Radioafición, Balizamiento de Aludes
Alta frecuencia	HF	7	Radio de onda corta	Cable coaxial	3–30 MHz 100 m – 10 m	Radidifusión en Onda corta, RFID, Radar, Telefonía móvil y marina, etc.
Muy alta frecuencia	VHF	8	Radio de onda corta	Cable coaxial	30–300 MHz 10 m – 1 m	FM, Televisión, Telefonía móvil marítima y terrestre, Radioaficionados, etc.
Ultra alta frecuencia	UHF	9	Rayo Microondas	Cable coaxial	300–3000 MHz 1 m – 100 mm	Televisión, Hornos microondas, Comunicaciones por microondas, Radioastronomía, Telefonía móvil, Redes inalámbricas, Bluetooth, ZigBee, GPS, Comunicaciones uno a uno como FRS y GMRS, Radioafición
Súper alta frecuencia	SHF	10	Rayo Microondas	Guías de onda	3–30 GHz 100 mm – 10 mm	Radioastronomía, Comunicaciones por microondas, Redes inalámbricas, radares modernos, Comunicaciones por satélite, Televisión por satélite, DBS, Radioafición
Frecuencia extremadamente alta	EHF	11	Rayo Microondas	Guías de onda	30–300 GHz 10 mm – 1 mm	Radioastronomía, Transmisión por microondas de alta frecuencia, Teledetección, Radioafición, etc.
Terahercios o Frecuencia tremendamente alta	THz or THF	12	Rayo Laser	Fibras ópticas	300–3,000 GHz 1 mm – 100 nm	Radiografía de terahercios Comunicaciones/computación mediante terahercios, etc.

Tabla 1: División bandas de radio, Adaptada de Wikipedia y (Gómez B. E.)

2.2 Propagación

Las ondas de radio se propagan de forma esférica y equitativa cuando son emitidas o propagadas por el emisor, del mismo modo que lo hace la luz. Como cuando se enciende una bombilla, esta no solo proyecta en una sola dirección, sino en todas. Del mismo modo estas son afectadas por fenómenos como son la reflexión, difracción, absorción, polarización y dispersión[4].

Con la propagación de forma esférica, la densidad de la radiación decrece con el incremento al cuadrado de la distancia desde la fuente de emisión como se muestra en la siguiente imagen:

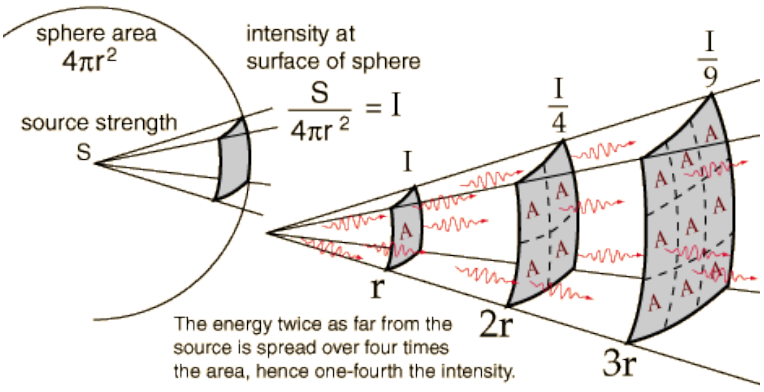


Figura 2: Inverse Square Law, Light (HyperPhysics)

[4] http://en.wikipedia.org/wiki/Radio_propagation

La unidad de medida que se usa para la atenuación de la señal suelen ser los decibelios (dB). El cual mide la relación entre dos magnitudes de forma logarítmica de una cantidad física como suelen ser la potencia y la intensidad. Este gracias a las propiedades de los logaritmos facilita ciertas operaciones, convirtiendo los productos y las divisiones en simples sumas y restas respectivamente, además presenta valores pequeños para magnitudes altas.

Si lo vemos desde un ejemplo, imaginemos que un emisor transmite con 15 dBm (decibelios relativos a un milivatio) con una antena que tiene una ganancia de 5 dB y el camino tiene unas pérdidas de 85 dB, el receptor recibe -65 dB ($Pr[dB] = 20 - 85$). Por lo tanto, una pérdida de 20dBm significa que la potencia de salida es 1/100 parte de la potencia original de entrada y una pérdida de 30 dBm es 1/1000 de la potencia original de entrada. Alternativamente, una ganancia de 20dBm es 100 veces la potencia de entrada original y 20dBm es 1000 veces. (PEPPERL+FUCHS, 2012)

dB	Factor
40	10 000
30	1 000
20	100
10	10
6	2
0	1
-6	0.5
-10	0.1
-20	0.01
-30	0.001
-40	0.0001

Las unidades de potencia que se usan son los dBm, dBW (decibelios relativos a un vatio), dB/.1V (decibelios relativos a un voltio) y dBmV (decibelios relativos a un milivoltio), las cuales se pueden utilizar para expresar potencias o tensiones absolutas en un mismo punto. Es por este motivo que se utilizan como referencia, potencias o niveles determinados y a pesar de no tener dimensiones, si miden la potencia en este punto.

El dBµV (decibelios relativos a un microvoltio) y el dBmV también son expresiones de potencia pero referidas a una impedancia común. Tanto las unidades de potencias dBm, dBW como dBµV y el dBmV se usan para medir la potencia a la salida de los dispositivos y se pueden relacionar siempre que se conozca sobre que impedancia se mide. (Gómez B. E. (n.d.).

2.3 Propagación en espacio libre

Como hemos comentado anteriormente las ondas de radio se propagan de forma esférica y equitativa hacia todas las direcciones, y cuando lo hacen de forma libre sin obstáculos se llama propagación de espacio libre (free space propagation). A continuación podemos ver una gráfica en la que se muestra las perdidas en relación a la distancia del emisor:

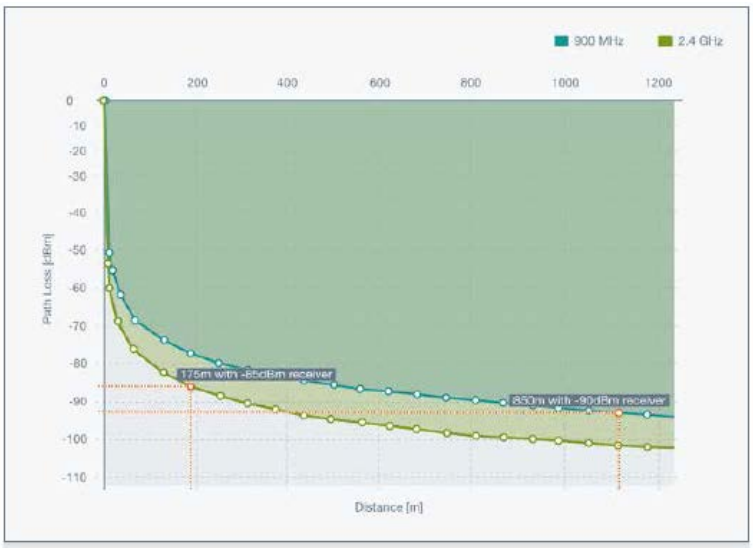


Figura 3: Propagación teórica en espacio libre (PEPPERL+FUCHS, 2012)

Este método, se considera optimista, todo y que tiene en cuenta las condiciones atmosféricas como la lluvia, nieve, niebla, polvo y la polución. Para redes locales estos efectos atmosféricos no influyen de forma relevante, aunque cabe indicar que no es el caso de las comunicaciones satélite o de teléfonos móviles, las cuales no se van a tratar en este documento. Por ejemplo, señales de 2.4 GHz serían atenuadas hasta un 0.0 dB/km por lluvias torrenciales (100 mm/hr o 100 l/m2 por hora o 4 pulgadas/hr). Otro ejemplo, es que una niebla fina produce una atenuación de hasta 0.02 dB/km, lo que tampoco afecta a redes locales y puede descartarse. (PEPPERL+FUCHS, 2012).

2.4 Zona Fresnel

Cuando se diseña un enlace radio y se quiere obtener una conexión fiable y estable se debe considerar la zona de Fresnel, que son áreas de figuras elipses como se muestra en la imagen entre la línea de vista del emisor y el receptor.

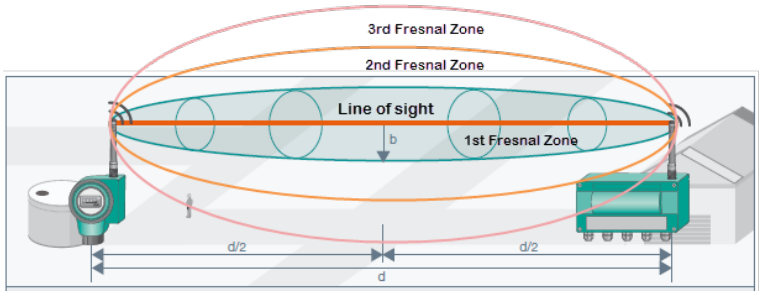


Figura 4: Zona Fresnel (Imagen adaptada de PEPPERL+FUCHS, 2012)

La mayor parte de la energía es transferida en la primera zona de Fresnel, por lo que preferiblemente esta debe estar totalmente libre de obstáculos, aunque, con al menos un 60% libre de cualquier obstáculo se puede considerar visibilidad directa, y de esta forma garantizar un alto rendimiento de la

conexión[5]. Cuando el grado de interferencias en la zona Fresnel alcanza niveles aproximados al 50%, se pueden producir caídas de hasta 6dB.

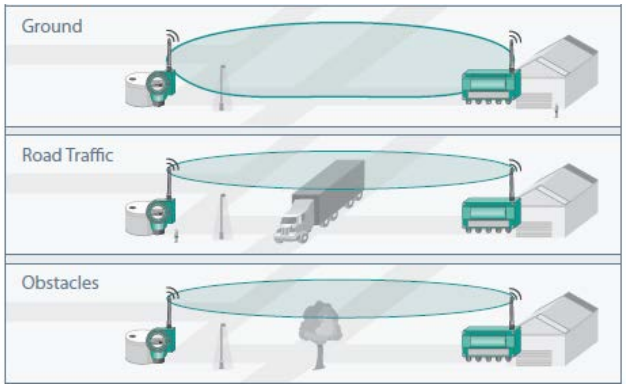


Figura 5: Posibles obstáculos (Imagen de PEPPERL+FUCHS, 2012)

d [m]	n[m] 900 MHz	b[m] 2.4 GHz
10	0.913	0.559
25	1.443	0.884
50	2.041	1.25
100	2.887	1.768
150	3.536	2.165
200	4.082	2.5
250	4.564	2.795

Tabla 2: Radio 1ra Zona Fresnel

En la tabla podemos ver el radio de la zona de Fresnel hasta los 250 m, para las frecuencias de 900 MHz y 2.4 GHz. Es especialmente importante siempre considerar la zona de Fresnel cuando se implantan redes industriales de campo, verificando que la línea de visión entre dispositivos este lo suficientemente despejada.

2.5 Propagación en diferentes entornos

A continuación mostramos una tabla de valores de pérdidas de trayecto para diferentes entornos, donde podemos apreciar que cuando más estructuras y materiales presentes entre el emisor y el receptor mayor atenuación sufrirá la señal.

Entorno	Exponente Pérdida trayecto
Espacio libre	2
Entorno urbano	2.7 to 3.5
Entorno urbano denso	3 to 5
Interior de edificios sin línea de visión	4 to 6
Interior de las fábricas sin línea de visión	2 to 3

Tabla 3: Exponente de pérdida de trayectoria para diferentes entornos (PEPPERL+FUCHS, 2012)

[5] http://www.zytrax.com/tech/wireless/fresnel.htm

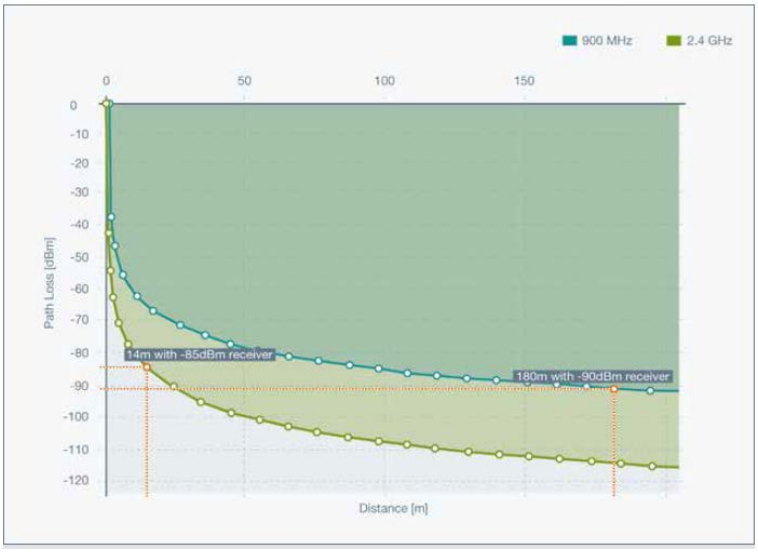


Figura 6: Propagación real en un ambiente urbano sombreado (exponente de pérdida de 3.7) (PEPPERL+FUCHS, 2012)

Las figuras anteriores muestran la diferencia entre la propagación en espacio libre y la propagación en un entorno urbano denso con un exponente de pérdida de 3.7. Comparando la propagación teórica en espacio libre y en un entorno urbano denso a una frecuencia de 2.45 GHz, se puede observar que la distancia teórica de 175 metros con un receptor con una sensibilidad de -85 dBm se reduce justo a los 14 metros. Comparando ambas curvas a 900 mHz la distancia teórica de 850 metros con un receptor con una sensibilidad de -90 dBm decrece a los 180 metros. (PEPPERL+FUCHS, 2012).

2.6 Antenas

Es uno de los elementos pasivos clave para la comunicación entre el emisor y receptor. El rendimiento de la conexión depende directamente de la ganancia de las mismas.

Son construidas con un conductor eléctrico fino que convierte energía eléctrica en ondas electromagnéticas irradia energía electromagnética (EM) (Kaufman D. R., 2010) del mismo modo que capturan ondas electromagnéticas y las convierten en electricidad es capturada de manera eficiente, a este fenómeno se le llama reciprocidad (antenna reciprocity). Se diseñan para frecuencias o bandas específicas, por lo que es muy importante tener en cuenta la frecuencia a la que se va a emitir para elegir la misma. Su tamaño es la inversa con la longitud de onda de la señal a transmitir, y vienen dada por la fórmula: $wavelength(m) = {}^{299{,}792{,}458}/_{frequency(Hz)}$

Por lo que para las frecuencias habitualmente usadas en redes de campo (fieldbus), 2.4GHz, la longitud total de la antena es de unos 12.49 cm aproximadamente, por lo que permite que sean integradas en los instrumentos o computadoras (Caro R. H., 2008):

Las características más importantes a considerar en una antena son (Mishr U., York R.,2001):

- Patrón de radiación y Directividad

En la teoría, una antena ideal sería la que radiase de forma uniforme en todas las direcciones, concepto llamado radiador isotrópico. Los patrones de radiación son usualmente representados con vista de elevación (perfil) y azimut (planta) (WNI México. n.d.). A continuación podemos ver un ejemplo tridimensional, resultado de la combinación de los patrones de elevación y perfil:

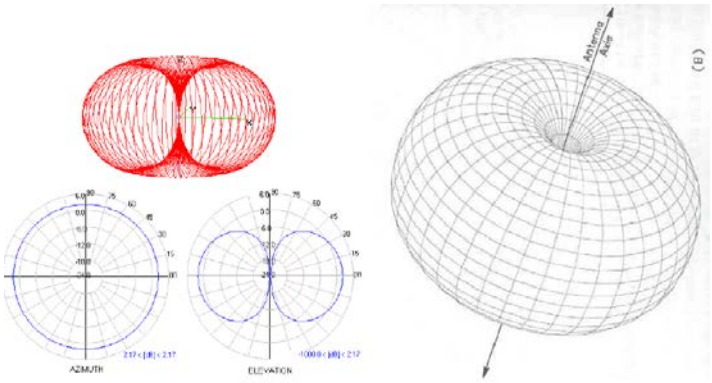


Figure 3: Radiación de una antena (Londoño J. 2009)

Los patrones son un buen método visual de comparación de antenas. Cuando disponemos de dos antenas con la misma potencia de radiación, la comparación más significativa que se puede hacer entre ambas es la de la magnitud de densidad de potencia en varias direcciones.

Los patrones de radiación también ofrecen información sobre las propiedades de direccionalidad de una antena, que es una relación de intensidad de radiación en una dirección particular en comparación a la intensidad promedio isotrópica. (WNI México. n.d.).

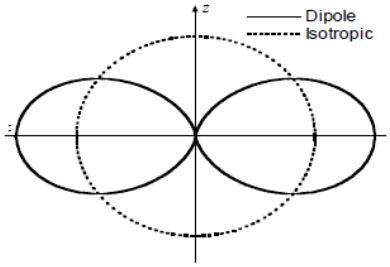


Figure 4: Comparación patrón de potencia isotrópico contra dipolo (Mishr U., York R. 2001)

Por ejemplo si vemos la figura anterior vemos como la intensidad de radiación en la zona de campo lejano es mayor usando una fuente dipolo en comparación a una isotrópica (patrón de radiación esférico perfecto), aunque en algunas direcciones la fuente dipolo es más pequeña. A este incremento o decremento de potencia en una dirección en comparación a una fuente isotrópica es lo que se llama “ganancia directiva” o “directividad” de la antena.

- Ganancia:
  La ganancia de la antena es la diferencia entre la potencia radiación efectiva y la potencia de transmisión, la cual viene dada por la fórmula: $G(dBi) = log_{10}\left(\frac{P_{ERP}}{P_{TX}}\right)$

Donde tenemos que los términos P_{ERP} hacen referencia a la medida de la potencia de radiación en direcciones específicas y P_{TX} es la potencia de transmisión. (Kaufman D. R., 2010)
Una de las precauciones que debemos tomar a la hora de elegir una antena es ver como vienen expresada la ganancia, esta puede venir de varias formas:
dBi: es la más habitual, y se usa cuando la ganancia es comparada a la potencia de transmisión como hemos visto anteriormente, o ganancia comparada a una antena isotrópica.
dBd: cuando se compara a un dipolo.
La diferencia entre ambos es la ganancia intrínseca de un dipolo, 2.14 dB, (que suele redondearse a 2 dB), por lo que tendríamos que: $DBd = dBi - 2$

- Polarización
  Esta característica indica la orientación de las antenas y es muy importante que esta sea igual en la antena emisora como en la receptora para obtener el máximo rendimiento de la conexión. Existen dos tipos de polarización aplicados a las antenas: Lineal (incluye vertical, horizontal y oblicua) y circular (que incluye circular derecha, circular izquierda, elíptica derecha, y elíptica izquierda) (WNI México. n.d.).

  Mediante una transmisión con una antena vertical se obtiene una polarización vertical, mientras que con una transmisión horizontal se obtendrá polarización horizontal.

Tipos de tecnologías en antenas:

Los diferentes tipos de tecnologías que podemos encontrar en antenas en Wireless son (Caro R. H., 2008):

- Omnidireccionales

  Las antenas omnidireccionales son de las más usadas en redes de campo, estas transmiten de forma equitativa en todas las direcciones del plano horizontal. Estas se consideran que tienen ganancia 0 medidas en dB y son habitualmente polarizadas de forma vertical por conveniencia.
  Como se vio anteriormente, debido a que radian de forma equitativa proporcional hacia todas las direcciones, se ve afectada por ley del inverso de la distancia al cuadrado, así como la atenuación proporcional a la densidad de los elemento que cruza y especialmente en los elementos metálicos donde es totalmente derivada a un punto de tierra si existe. La antena receptora recibe de forma indiscriminada las ondas electromagnéticas de todos los transmisores que estén en el alcance e incluso las ondas reflejadas por obstáculos.

- Direccionales de alta ganancia
  Se usan para realizar conexiones con la antena receptora de forma directa, evitando así perdidas como las de las antenas omnidireccionales. Este tipo de antes concentran la radiación en un haz muy estrecho y con alcance largo. Debido a esto no siempre es fácil enlazar el

transmisor y el receptor, por lo que muchas veces se tienen que recurrir a herramientas software que ayudan a conseguir la orientación de forma rápida.

Estas antenas también tienden a mejorar la recepción, optimizando la relación señal-ruido, eliminando ruido, señales estacionarias en la misma frecuencia y reflexiones.

Las antenas direccionales más comunes son las YAGI, Parabólicas y Panel.

Figura 7: Prototipo antena quasi-Yagi

- Antenas Planar

  Estas antenas se diseñaron para dispositivos móviles y estás han evolucionado a diferentes tipos ya que cuentan con la ventaja que pueden ser fabricadas a un costo mucho más bajo que la tecnología de antenas basadas en guía ondas y son mucho más compactas y ligeras. Estas están disponibles de forma comercial y disponen de un amplio abanico de posibilidades.

- Antenas de fase

  Los primeros en usar estos tipos de antenas fueron los militares. Están organizadas en 2 dimensiones. Debido a su alto coste no hace atractivo su uso en aplicaciones comerciales e industriales. El principal atractivo de estas antenas es que puede alcanzar ganancias similares a las antenas direccionales, además de ser direccionadas sin tener que mover la base de la antena, ofreciendo una gran ventaja a la hora de conectar dispositivos móviles que se mueven más allá de la gama de antenas omnidireccionales.

2.7 Topologías redes Wireless

La topología de las redes Wireless viene caracterizada por el diseño, o por la disposición de los nodos y los componentes de la red. Hoy en día, las topologías más extendidas en redes industriales sobre todo debido a sus ventajas son las topologías en estrella, malla en estrella y malla. A continuación se muestran las más habituales en redes industriales:

2.7.1 Estrella.

Esta topología es la más habitual en redes Wireless donde el punto de acceso es el centro de la red, y todos los nodos se comunican en un solo salto con el gateway directamente el cual se encarga de gestionar todas las conexiones. El punto de acceso puede estar conectado de forma inalámbrica o cableada a otros puntos de acceso o Switchs.

Las topologías de red en estrella son las que mayor velocidad ofrecen en recopilación de datos y el que menor consumo ofrece entre todas las topologías de red Wireless, pero se ve limitado por la distancia a la cual el transmisor puede enviar datos, que es de un rango de entre 30 y 100 metros aproximados (PEPPERL+FUCHS, 2012).

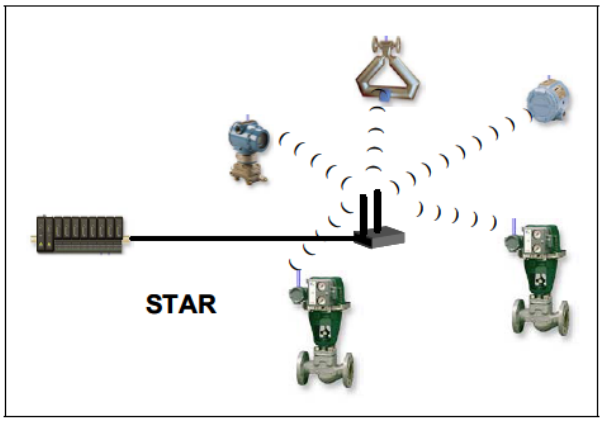


Figura 8: Topología de red Wireless en estrella (Caro R. H., 2008).

2.7.2 Árbol

La topología en Árbol no es de las más habituales pero, al igual que en redes cableadas las redes Wireless pueden estructurarse con esta topología como se muestra en la figura:

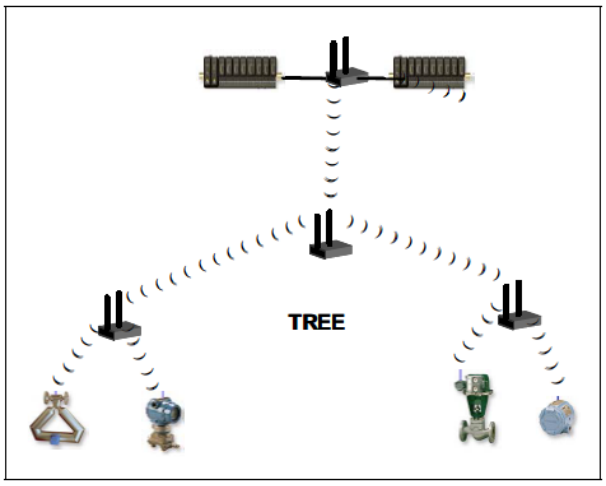


Figura 9: Topología de red Wireless en Árbol (Caro R. H., 2008).

2.7.3 Malla

Todo y que la topología en Malla en redes cableadas no es una novedad ya que es la que se usa en internet, en el ámbito de las redes Wireless si lo es, y además revolucionaria. Esta topología es un sistema de saltos múltiples, donde todos los nodos actúan como Routers y se encargan de redirigir la información recibida ya sea de otros nodos o del gateway que no va dirigida a ellos mismos o a los demás nodos dentro de su alcance.

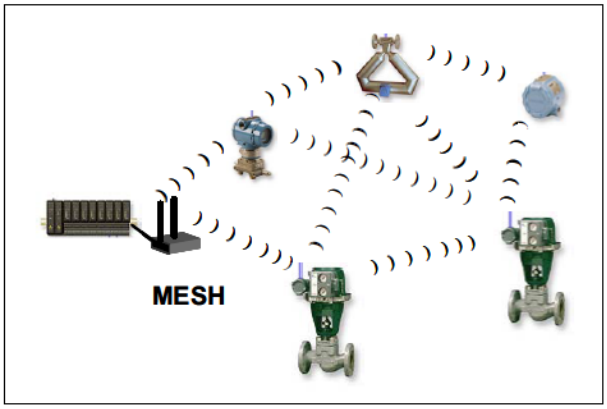


Figura 10: Topología de red Wireless en Malla (Caro R. H., 2008).

Estas redes cumplen con los requerimientos exigidos en las redes de automatización industriales, ya que se recuperan automáticamente y además son redundantes, lo que las convierte en altamente tolerantes a fallos y además son capaces de auto configurarse y determinar el camino más óptimo y rápido entre los mismos nodos y el gateway. De este modo si detectan que hay algún problema en el enlace a otro nodo, inmediatamente buscan la alternativa más rápida.

La topología en Malla con la técnica de saltos múltiples soporta un rango mucho mayor que la topología en estrella pero consume mucha más energía debido a que la relación de trabajo de la red es mayor. Ya que los nodos están constantemente a la espera de mensajes o cambios a través de los enlaces (PEPPERL+FUCHS, 2012).

Algunos de los problemas presentes en redes Wireless malla son: la latencia puede a llegar a ser alta según el número de nodos y su distancia. Y la duplicidad de mensajes o ruteo múltiple debido a que no hay forma de prevenir que el mensaje transmitido por un nodo no sea recibido por otros nodos ocasionando que los mensajes sean duplicados. Existe una técnica que puede llegar a detectar mensajes duplicados y descartarlos, la cual es mediante la identificación del mensaje de campo de la trama IP (Caro R. H., 2008).

Esta topología es recomendable cuando la redundancia es un requisito primordial, pero en cambio no lo es la potencia y la alimentación mediante baterías (PEPPERL+FUCHS, 2012).

2.7.4 Malla en Estrella

Como su nombre indica, es una combinación las dos topologías vistas anteriormente, para obtener las ventajas de cada una. La velocidad, el bajo consumo y simplicidad de la topología en estrella y la auto-recuperación, redundancia y el ancho rango de la topología en malla (PEPPERL+FUCHS, 2012).

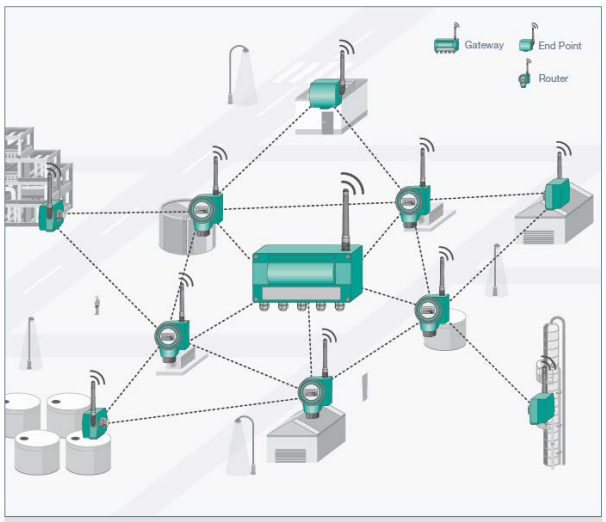


Figura 11: Topología de red de Malla en Estrella (PEPPERL+FUCHS, 2012).

2.8 Conclusión

En conclusión, entre las topologías y antenas que mayor implantación tienen en el sector industrial son la topología en malla y las antenas omnidireccionales. La topología en malla como se ha comentado cumple con los requerimientos exigidos en las redes Wireless industriales que se mostraran a continuación, ya que como se ha comentado cuenta con la gran ventaja de que son redundantes y altamente tolerante a fallos y son capaces de auto configurarse. Por último, las antenas omnidireccionales son las más adecuadas para una topología en malla, ya que en la topología en malla los dispositivos esta distribuidos de forma des-uniforme, por lo que con la transmisión de forma equitativa en todas las direcciones del plano horizontal de la antena omnidireccional se consigue fácilmente la conectividad entre los dispositivos.

Capítulo 3 . Estado del Arte-Metodología

3.1 Estado redes Wireless industriales

Todo y que aún el mercado de las redes Wireless Industriales es aun pequeño, este está en continuo crecimiento y desarrollo y cuenta con gran interés por parte de grandes integradores que ven en él un mundo de oportunidades. Hay un gran número de tecnologías compitiendo y apostando por la estandarización como se muestra a continuación:

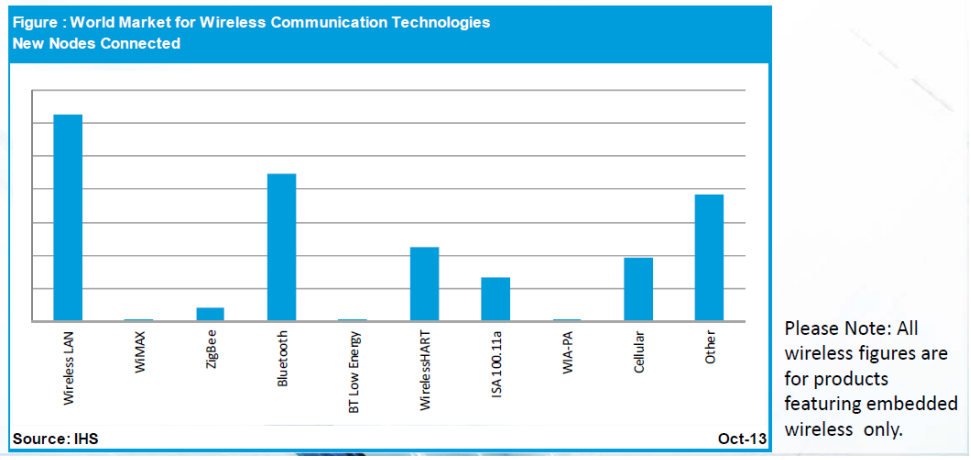
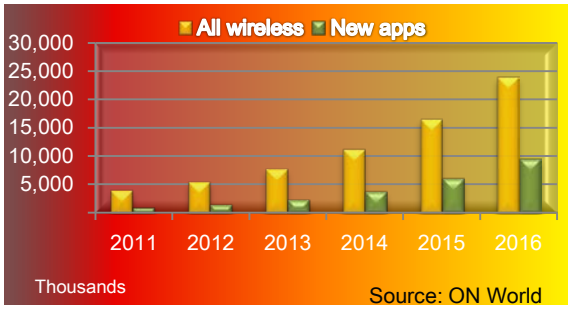


Figura 12: Mercado Global para comunicaciones industriales (Nuevos nodos conectados)

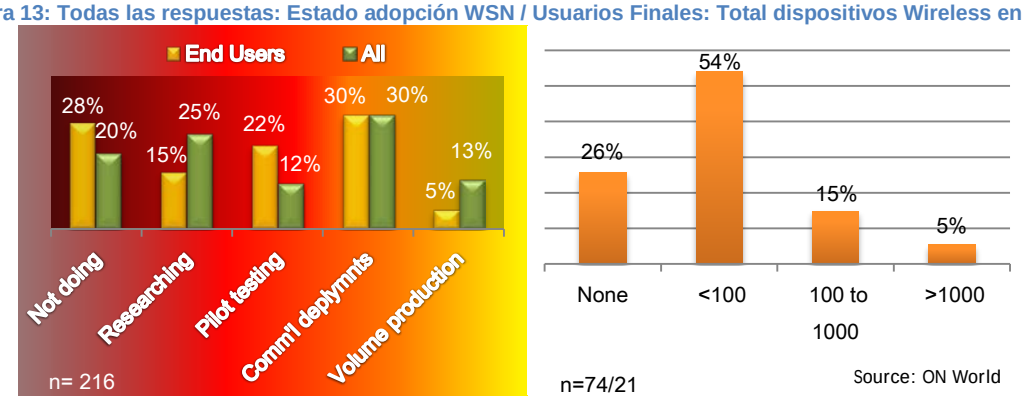
El futuro de la WIFI en la industria es prometedor a pesar de la situación económica en la que estamos ahora mismo. En 2012, según un estudio de ON Worlds's indicaba que esta se había doblado durante los dos últimos anos, dejando ver con esto como la industria está creciendo y es una fuente de nuevas oportunidades.

Esta organización lleva 12 años en la investigación en la industrial de los sensores Wireless. Entonces era muy raro hacer despliegues de más de 20 nodos Wireless cuando ahora algunos sitios llegan a tener desplegados más de 3000 nodos Wireless. Hecho que según nos indica la encuesta, es consecuencia del aumento del conocimiento en estos sistemas, la fiabilidad que estos ofrecen hoy en día, la convicción que las redes malla ofrecen hoy en día y la rapidez en la migración a estándares industriales, como WirelessHART o un hibrido entre WirelessHART e ISA100.11a. Los cuales, son los preferidos por la mayoría de los usuarios finales en el sector industrial y están recibiendo un gran apoyo por parte de grandes integradores de la industria.



Entre las principales conclusiones de este estudio, predice que durante los próximos 5 años, el número de dispositivos de campo Wireless industriales se incrementara en un 553%, cuando habrá cerca de 24 millones de sensores Wireless activos y actuadores, o puntos de detección desplegados. Al mismo tiempo, predice que para el 2016, el 39% de los nodos desplegados para nuevas aplicaciones solo estarán habilitados con tecnología WSN.

Figura 13: Todas las respuestas: Estado adopción WSN / Usuarios Finales: Total dispositivos Wireless en campo



Las tendencias del uso del Wireless varían en gran medida según el área geográfica.

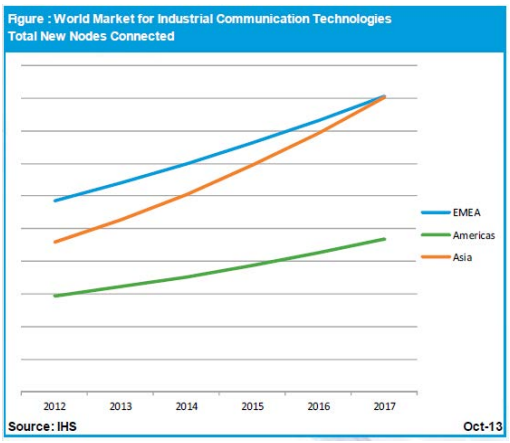


Figura 14: Mercado Global para comunicaciones industriales (Total nuevos nodos conectados)

En América, el mercado es más pequeño pero muestra un crecimiento estable. Por otra parte, en Europa, Oriente Medio y África (EMEA), hubo un fuerte impulso de suministros Wireless 2012, aunque sufre un crecimiento lento motivado por la falta de confianza en el Wireless y el crecimiento económico lento. Por último Asia cuenta con un crecimiento sólido debido al crecimiento acelerado de su industria y es un mercado el cual es fuertemente perceptible a la adaptación de nuevas tecnologías debido principalmente a que es un mercado virgen. (IHS)

Los sectores industriales que mayormente están adoptando soluciones Wireless y dan mayor apoyo a la misma son el sector de Gas y Petróleo y del Automóvil. El sector industrial de Gas y Petróleo lo utiliza principalmente en el Control de Sistemas, con sensores y monitorización ya que como hemos visto antes, ofrece ventajas como la reducción de infraestructura, lo que supone ahorro en mantenimiento y posibilita un gran de ahorro de energía. En el sector del Automóvil lo están desplegando principalmente en los robots modulares y líneas de ensamble, con la ventaja de que reduce los cambios en las radios (frayed) y el daño en el cableado. (IHS)

3.2 Redes Comerciales contra Redes Industriales (Requerimientos)

Durante los últimos años las redes comerciales han evolucionado de forma rápida, incluso llegando a influir en el comportamiento y hábitos de los ciudadanos. Lo mismo ha pasado en el sector industrial,

donde que en un principio todo el control de la fabricación y los procesos en las plantas se realizaban de forma mecánica. A posteriori, poco a poco, a medida que la electrónica discreta ganaba popularidad, los sistemas de control mecánicos fueron reemplazados por lazos de control electrónicos, mediante transductores, relés y circuitos de control cableado. Estos sistemas consumían mucho espacio y habitualmente se requería una gran cantidad de cableado para su interconexión, los conteos llegaban a ser de muchos kilómetros de cable. Posteriormente llegaron los circuitos integrados y los microprocesadores, donde la funcionalidad de múltiples lazos analógicos podían ser replicados con un solo controlador digital. Estos empezaron a reemplazar el control analógico, sin embargo las comunicaciones de campo continuaban usando señales analógicas.

Todo este cambio está dirigido hacia los sistemas digitales, lo que ha llevado a tener que inventar nuevos protocolos de comunicación tanto para la comunicación entre controladores así como para las de campo. Estos son conocidos como protocolos Fieldbus. Recientemente, ya empieza a verse la interoperabilidad de redes corporativas con redes industriales a nivel de campo, llegando a niveles de gestión y control integral muy altos, del mismo modo los sistemas digitales de control empiezan a incorporar Networking a todos los niveles de control industrial por medio del uso de estándares Ethernet. Con estos últimos avances, las redes industriales cada vez llegan a ser más parecidas a redes convencionales a nivel físico, pero siguen teniendo requisitos muy diferentes (Galloway B. y Hanke G. P., 2012). A modo de ejemplo, unas de los principales requisitos de los que hacemos referencia, es el nivel de QoS (Quality Of Service) requerido entre las redes industriales y las redes convencionales, ya que los requisitos de transferencia de datos en tiempo real y fiabilidad de la misma es muy diferente. A continuación mostramos una tabla donde se reflejan las diferencias en requerimientos entre ambos tipos de redes:

Requerimientos	Industriales	Convencionales
Función Primaria	Control de equipamiento físico	Proceso y transferencia de información
Sectores Aplicables	Fabricación, transformación y distribución de servicios públicos	Ambientes corporativos y domésticos
Jerarquía	Profunda, jerarquías funcionalmente separados con muchos protocolos y estándares físicos	Poco profunda, Jerarquías integradas con protocolos uniformes
Escalabilidad	Requerida	No requerida
Severidad Fallos	Alto	Bajo
Fiabilidad	Alto	Moderada
Seguridad	Requerida	No requerida
Round-Trip Time (RTT)	250 µs - 10 ms	50+ ms
Determinismo	Alto	Bajo
Composición Datos	Paquetes pequeños de trafico periódico y aperiódico	Grande, paquetes aperiódicos
Consistencia Temporal	Requerida	No requerida
Ambiente Operación (Robustez)	Condiciones hostiles, habitualmente expuestas a altos niveles de humedad, polvo, corrosión, calor y vibración	Ambientes limpios, habitualmente habilitados para equipamiento sensible

Tabla 4: Diferencias entre redes industriales y redes convencionales (Tabla adaptada del artículo, (Galloway B. y Hanke G. P., 2012)

Como se puede ver en la tabla, las redes industriales son utilizadas principalmente para el control y monitorización de procesos en un amplio abanico de sectores, como pueden ser producción y distribución eléctrica, industria alimentaria, logística, redes de distribución de agua, gestión de residuos y efluentes y en refinerías químicas de petróleo y gas. El control de procesos involucra sistemas dinámicos e interconectados, los cuales requieren una interconexión a bajo nivel y la disponibilidad de todo el equipamiento de la planta para que funcione correctamente. Por otro lado las redes convencionales solo procesan y envían información (Galloway B. y Hanke G. P., 2012).

3.2.1 Arquitectura

Respecto a las diferencias en la arquitectura de ambas redes, mientras que las arquitecturas en redes comerciales en las compañías habitualmente consisten en Redes de Área Local (LAN) conectadas a Redes de Área Amplia (WAN), las redes industriales generalmente cuentan con arquitecturas más profundas, tendiendo a tener hasta 3 o cuatro niveles.

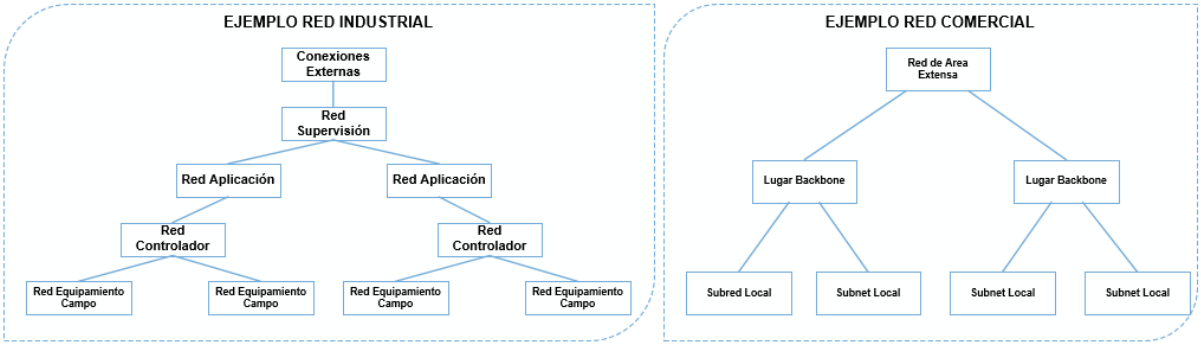


Figura 15: Arquitecturas redes industriales y comerciales, fuente: (Galloway B. y Hanke G. P., 2012).

Como se observa en la anterior gráfica, en las redes industriales podemos tener por un lado la conexión de los controladores a los instrumentos en un nivel, en el siguiente las interconexiones de los controladores a las aplicaciones. Por encima de este nos encontramos con el nivel HMI (Human Machine Interface) y finalmente el último nivel a las conexiones externas. Para las comunicaciones entre los diferentes niveles se usan gateways, que suelen requerir diferentes protocolos. (Galloway B. y Hanke G. P., 2012).

3.2.2 Estructura Jerárquica

Así mismo, en la industria de los sistemas de automatización de procesos se puede encontrar una estructura jerárquica que está basada en la arquitectura funcional ISA-95 (Purdue Network Model) que es conocida como la pirámide de la automatización.

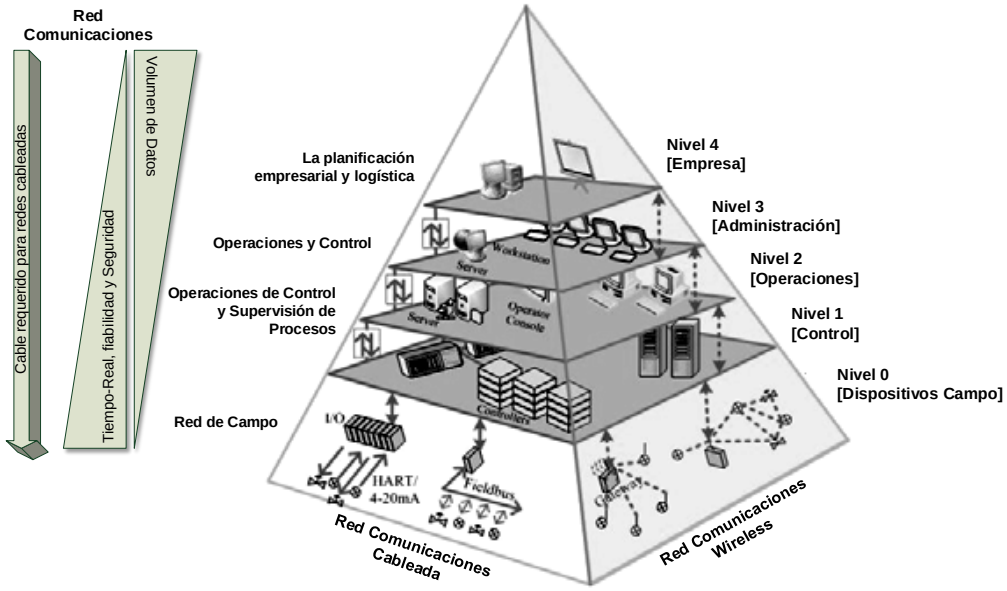


Figura 16: Pirámide de la automatización basada en la jerarquía funcional ISA-95. (Ikram W., Thornhill N. F., 2010).

La pirámide presenta dos caras con las mismas funcionalidades. La cara derecha muestra la arquitectura de los componentes en tecnología cableada y la izquierda con tecnología Wireless. Donde los niveles jerárquicos definen los estados en los cuales se toman decisiones. La base empieza en el proceso de producción, y va todo el camino hacia arriba hasta el nivel empresarial de administración a través de las diferentes capas intermedias (Ikram W., Thornhill N. F., 2010). Del mismo modo ofrece información sobre los requerimientos de red entre los diferentes niveles, que como se dijo anteriormente requieren de diferentes tecnologías de comunicación. Estos requerimientos son principalmente en términos de volumen de información, rapidez en la disponibilidad de la información desde que pasa un evento, la fiabilidad y robustez (Sikora, 2007).

En el nivel 0 las condiciones de operación también suelen ser más duras que en niveles superiores, ya que en el nivel de campo se requiere incluir instrumentos neumáticos, sistemas 4-20mA, digitales así como soluciones Wireless, las cuales su uso no está limitado a nivel de red de campo sino que también pueden ser aplicadas a nivel de red de la planta. (Ikram W., Thornhill N. F., 2010)

3.2.3 Escalabilidad

Debido a que las redes industriales pueden albergar cientos de nodos o pueden sufrir cambios habitualmente en los procesos de producción, es un requisito que estas estén optimizadas para que la escalabilidad no sea un inconveniente.

3.2.4 Severidad fallos

Por lo que respecta al requisito en la severidad en los fallos, se puede ver en la tabla como en las redes industriales es mayor, debido principalmente a que en las redes industriales todos los equipos e instrumentos están conectados físicamente y un fallo en la red podría ocasionar graves efectos, como parar toda la producción de la planta y en consecuencia dañar seriamente equipos mecánicos, reducir la producción, incluso según la gravedad se podría llegar a pérdida de vidas.

3.2.5 Round trip times y Fiabilidad

El anterior requisito da una visión de lo critico que puede llegar a ocasionar un fallo, por este motivo el Round trip times (RTT) y la fiabilidad "Reliability" es muy importante. La transmisión de los datos es crítica cuando se está controlando o monitorizando un proceso por lo que él envió, el proceso y la recepción de la misma debe ser lo más rápido que sea posible. En redes industriales se pueden tener requerimientos de respuesta que van desde 250µs a 1ms en aplicaciones de control de movimiento, pero por otro lado en procesos menos estrictos se pueden llegar a requerir desde 1ms a 10ms. En cambio, en las redes comerciales no suele haber requerimientos en tiempos de respuesta (Galloway B. y Hanke G. P., 2012).

3.2.6 Seguridad

Otro requisito a considerar es la seguridad, en ambientes industriales, donde con condiciones altamente inflamables, puede verse en riesgo la seguridad de la misma con una alta concentración de transmisión de ondas electromagnéticas, debido a que estas pueden causar ignición (Schultz, S., 2007). Por lo tanto en condiciones altamente inflamables se debe mantener un nivel bajo de concentración de ondas electromagnéticas (Estándar BS6656, 2002).

3.2.7 Determinismo

Por lo que respecta al determinismo, como vemos en la tabla es un requisito alto. Para que una red sea determinística, tiene que ser posible predecir cuando la respuesta a una transmisión será recibida. Para esto, la latencia de la señal tiene que ser limitada y tener una varianza muy baja (Galloway B. y Hanke G. P., 2012).

3.2.8 Composición Datos

En cuanto al tamaño de los paquetes de datos transmitidos en redes industriales, estos suelen ser generalmente pequeños, del tamaño de unos pocos bytes, sobre todo en los niveles bajos de la arquitectura donde solo se requiere la transmisión de una simple mesura o valor digital. Mientras que en las redes comerciales se llegan a transmitir habitualmente paquetes aperiódicos con un mínimo de 64 bytes, es por esto, lo que hace que se requieran protocolos significantemente diferentes. El tráfico de la información puede ser periódico o aperiódico, dependiendo si se transmite información de cualquier variación en los instrumentos según los requerimientos del control o si se transmite información que ocurre en cualquier momento de forma esporádico como por ejemplo el debido al salto de una alarma (Galloway B. y Hanke G. P., 2012).

3.2.9 Consistencia Temporal

En las redes industriales es muy importante guardar un orden en los eventos ocurridos así como un control exhaustivo del momento del mismo, sobre todo en transmisiones aperiódicas. Esto se lleva a cabo mediante los timestamps y relojes sincronizados, habilidad que no está disponible en el protocolo TCP/IP (Transmission Control Protocol/Internet Protocol) (Galloway B. y Hanke G. P., 2012).

3.2.10 Robustez

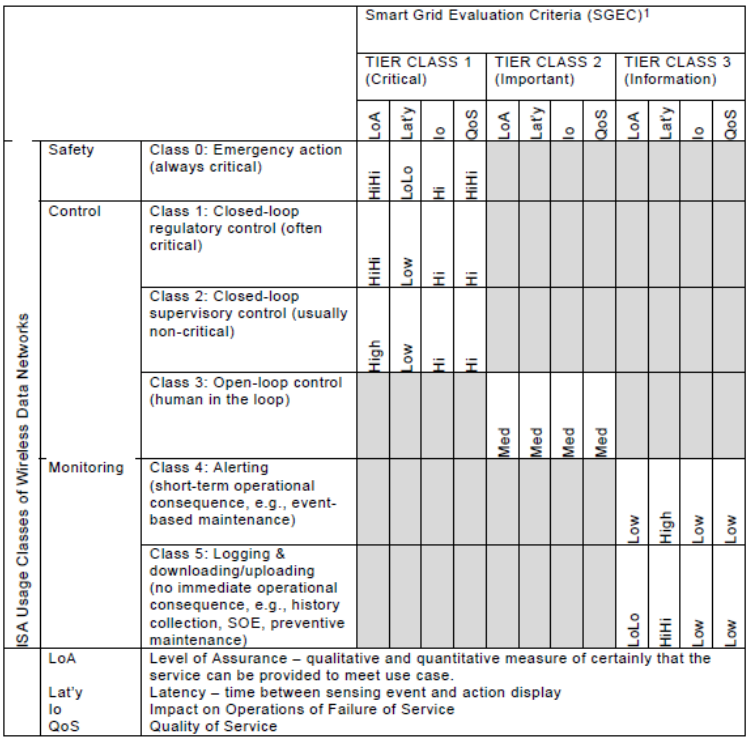
Y por último, tenemos la Robustez, debido a que habitualmente las redes industriales son implementadas en una gran variedad de lugares con condiciones adversas, quedando expuestas a humedad, polvo, corrosión, calor, vibración, y condiciones meteorológicas. Por lo tanto, todo el equipamiento tiene que estar protegido contra cualquier daño que este pueda ocasionar. En cambio, las redes comerciales siempre están bajo condiciones totalmente limpias, y entornos especialmente habilitados con las mejores condiciones para su óptimo funcionamiento.

3.3 Confianza Wireless en redes industriales

Como hemos visto anteriormente los requerimientos en las redes industriales son mucho más estrictos que las redes convencionales, estos cambian según el nivel jerárquico en la pirámide de automatización. Esta sección se centra en mostrar que requisitos debe cumplir una red Wireless en el área de la automatización y los sistemas de control para que esta demuestre ser fiable. Hoy en día el Wireless ha sustituido casi por completo las comunicaciones en nuestras vidas personales, algo que no está pasando en el sector industrial, probablemente debido a la falta de conocimiento que muchos tienen sobre la misma, generando falta de confianza para utilizar esta en cualquier ambiente industrial.

En el área industrial se han identificado por parte de ISA (The International Society of Automation), 6 clases de aplicaciones que dependiendo en la aplicación, la seguridad y la fiabilidad como tiempo de latencia de la transmisión difieren desde no muy importante hasta absolutamente necesario (PEPPERL+FUCHS, 2012). A continuación podemos ver una tabla que muestra una referencia cruzada entre las actividades fiables del ISA100 (industrial) y el desempeño de los sistemas de automatización para los Criterios de Evaluación de Redes Inteligente (SGEC)[6] (International Society of Automation, 2011):

[6] IEEE P2030-10-0050-00-0012 - http://grouper.ieee.org/groups/scc21/2030/email3/pdfr6V0WGSSKT.pdf



			Smart Grid Evaluation Criteria (SGEC)[1]											
			TIER CLASS 1 (Critical)				TIER CLASS 2 (Important)				TIER CLASS 3 (Information)			
			LoA	Lat'y	Io	QoS	LoA	Lat'y	Io	QoS	LoA	Lat'y	Io	QoS
ISA Usage Classes of Wireless Data Networks	Safety	Class 0: Emergency action (always critical)	HiHi	LoLo	Hi	HiHi								
	Control	Class 1: Closed-loop regulatory control (often critical)	HiHi	Low	Hi	Hi								
		Class 2: Closed-loop supervisory control (usually non-critical)	High	Low	Hi	Hi								
		Class 3: Open-loop control (human in the loop)					Med	Med	Med	Med				
	Monitoring	Class 4: Alerting (short-term operational consequence, e.g., event-based maintenance)									Low	High	Low	Low
		Class 5: Logging & downloading/uploading (no immediate operational consequence, e.g., history collection, SOE, preventive maintenance)									LoLo	HiHi	Low	Low
	LoA Lat'y Io QoS	Level of Assurance – qualitative and quantitative measure of certainly that the service can be provided to meet use case. Latency – time between sensing event and action display Impact on Operations of Failure of Service Quality of Service												

Figura 17: Actividades fiables del ISA100

La utilización del Wireless industrial hoy en día se centra principalmente desde las clases 3 a la 5, las cuales no son críticas, donde hay el suficiente tiempo para repetir él envió de un mensaje o redirigirlo a través de una red en malla. Para las siguientes clases del 0 al 2, se debe tener mayor cuidado, y requiere de medidas especiales. De seguro, la tecnología Wireless a medida que se gane experiencia con la misma en el sector industrial y esta mejore tecnológicamente, podrá ser implementada en aplicaciones más críticas.

El hecho que ahora mismo solo se esté aplicando en las clases 3 a la 5, se debe principalmente a que como hemos visto, uno de los principales requisitos en las redes Industriales es que la información se envié en un tiempo definido de tiempo y sin errores. A continuación mostramos una tabla que muestra la Tasa de Error de Bit, "bit error rate", de forma estadística según las diferentes tecnologías de comunicación, el VBER es uno de los parámetros que miden el desempeño de un sistema de comunicaciones digital (PEPPERL+FUCHS., 2012).

Medio	Bit Error Rate [BER]
Enlace de radio	10^{-3}
Cable teléfono no apantallado	10^{-4}
Cable teléfono trenzado apantallado	10^{-5}
Cable coaxial en aplicaciones locales	10^{-9}
Fibra Óptica	10^{-12}

Tabla 5: Tasa de Error de Bit, "bit error rate"

En esta tabla podemos ver como un link de radio (10^{-3}) es 10 veces peor a una conexión mediante cable de teléfono no apantallado (10^{-4}), lo que significaría que para cada paquete que se envía se debería repetir él envió. Un BER de 10^{-4} es inaceptable para comunicaciones en sistemas industriales de automatización y sistemas de control, ya que significa que por cada 10.000 bits transmitidos hay un

error, los cuales no son solicitados de nuevo por el receptor, lo que genera carga adicional al bus de comunicación (PEPPERL+FUCHS., 2012).

3.3.1 Confiabilidad

Para que un sistema Wireless sea fiable en la automatización industrial y los sistemas de control (IACS), este debe contar con los siguientes principales atributos (International Society of Automation, 2011):

- Fiabilidad - resistente a la interrupción de las amenazas no intencionadas.
- Seguridad - resistente a la interrupción de las amenazas maliciosas
- Resiliencia- capaz de restaurar los servicios después de cualquier interrupción
- "Designable" - pueden seleccionarse y utilizarse con nivel aceptable de consecuencias imprevistas.

La confiabilidad en la tecnología Wireless es clave desde mi punto de vista en el camino hacia el éxito en la implementación por parte de usuarios finales e ingenierías en el sector industrial, especialmente en la IACS. Esta sección de confiabilidad se da una posible respuesta a muchas dudas a las cuales los ingenieros se cruzamos a la hora de tener que confiar en la tecnología Wireless, incluso se puede llegar a romper con ideas preconcebidas. Soy de la opinión que mediante pasos seguros, sin querer que un sistema abarque más de lo que técnicamente es capaz, se puede llegar a la confiabilidad necesaria para que cada vez su implementación sea de mayor grado, incluso puede que en un futuro próximo veamos la tecnología Wireless presente en el control de procesos y sistemas de seguridad de Clase 0 a Clase 2 en las actividades fiables del ISA100.

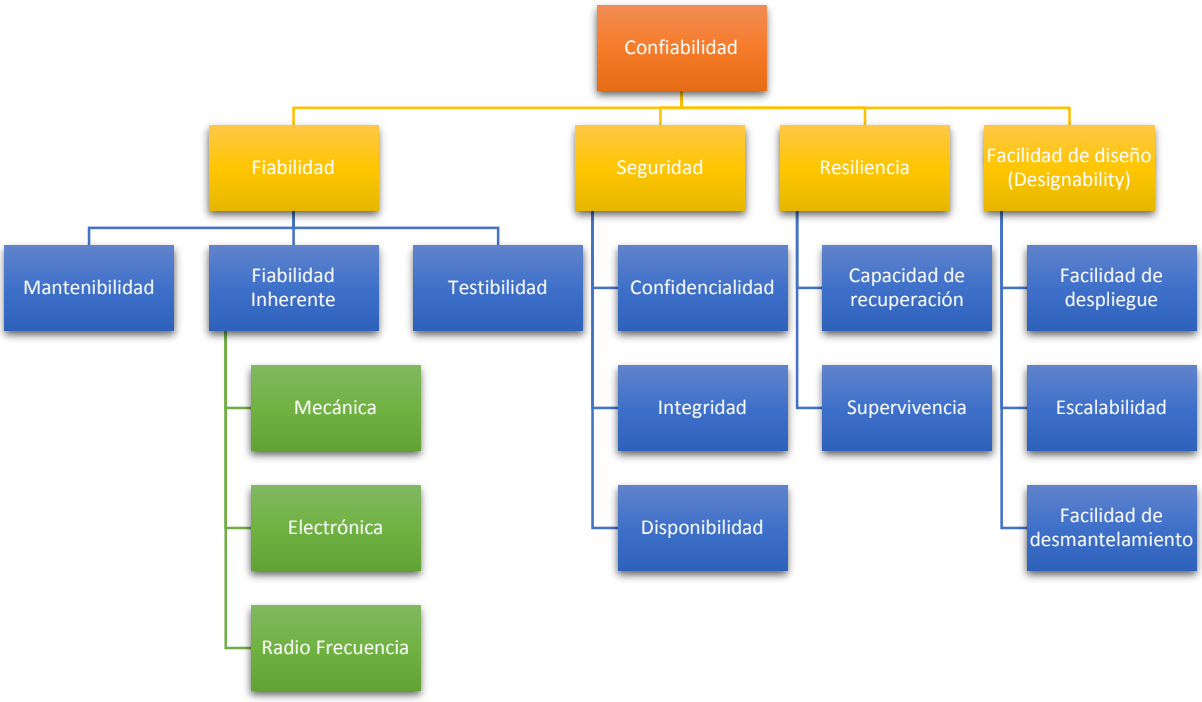


Figure 5: Confiabilidad tecnología Wireless (Requisitos). (International Society of Automation, 2011)

3.3.2 Fiabilidad

En la IACS, la fiabilidad se asociada habitualmente a la evitación de fallos derivados de una causa física casi siempre de naturaleza no intencionada, como fallos en diseño, errores de mantenimiento, errores de software, etc. Fiabilidad típicamente se mide como el tiempo entre fallos o el ratio de fallos, que es el inverso del tiempo entre fallos (International Society of Automation, 2011).

La fiabilidad no tiene límite, lo que conlleva a que el coste tampoco lo tenga. Por lo que siempre hay un diseño intermedio entre fiabilidad y coste que tiene que ser ajustado para la aplicación (International Society of Automation, 2011).

3.3.3 Fiabilidad inherente

Cuando se habla de fiabilidad inherente, es cuando el diseño fiable se basa en el entorno de operación para el que va a ser destinado. En entornos Wireless en IACS, estos deben ser diseñados con componentes que se ajusten al entorno al cual van a estar expuestos, en IACS son habituales los ambientes con altas temperaturas, vibraciones, corrosiones, humedades.

Del mismo modo, el software también debe ser considerado. Los comercializadores (distribuidores) deben utilizar procesos de calidad de software y rigurosas prácticas de control de configuración con el objetivo de producir Wireless fiable.

Otro de las principales fuentes de amenazas inesperadas que afecta a la fiabilidad es el entorno dinámico de radio frecuencia (RF). Como hemos comentado anteriormente en los entornos de la AICS, hay otras fuentes de radiación intencionadas que pueden generar interferencias, como pueden ser otras redes Wireless. Así mismo la compleja estructura inherente a las planas industriales con materiales que causan reflexión y absorción de las señales de radiofrecuencia, hace que sea un ambiente difícil para comunicaciones de RF. Además el ambiente físico puede sufrir cambios en el tiempo, se pueden construir nuevos muros, añadir nuevas plataformas metálicas como pipe racks, puede haber objetos metálicos grandes que cambien su ubicación a lo largo del tiempo como contenedores de reciclaje. Otras fuentes de interferencia pueden ser radiadores incidentales como hornos microondas, soldadores de arco y motores industriales eléctricos. Por lo que el sistema para ser fiable debe ser correctamente diseñado para este ambiente y debe ser robusto al mismo.

Por último, mencionar que la complejidad es el enemigo de fiabilidad. Cuando más simple se conserve el diseño mejor será este, aportando mayor fiabilidad inherente y menor probabilidad de fallos resultantes de uso normal o problemas inesperados.

3.3.4 Mantenibilidad

Cuando se habla de mantenibilidad, es la habilidad de mantener un producto en una condición favorable para su funcionamiento normal. En el contexto que estamos tratando viene a hacer referencia a la frecuencia y la dificultada de las tareas que son requeridas para que los equipos se mantengan en un desempeño aceptable. Aunque mantenibilidad también tiene relación con el atributo de la

resistencia a través de su relación con el tiempo de reparación, donde habitualmente MTTR (Mean Time to Restore) es usado como una unidad de medida de mantenibilidad. Una tarea particular de gran interés en las redes Wireless IACS es reemplazar la batería a los equipos inalámbricos.

3.3.5 Testabilidad

Es imprescindible saber el estado de operación de la red Wireless IACS para que esta sea fiable. Si no se conoce el estado mediante la testabilidad, este sistema puede ser una fuente inesperada de problemas y errores sin que el usuario final sea consciente. La testibilidad puede darse tanto en la implementación como en el mantenimiento. Hay que tener la precauciona, que el testeo siempre se ajuste a la función del sistema que se está diagnosticando, para no someter a un sistema a una rutina de prueba que consuma más batería que la que consume normalmente con la función a la que está destinado.

3.3.6 Seguridad

La Seguridad es otro requisito muy importante, que genera mucha desconfianza sobre las redes Wireless y en la cual se está dedicando muchos recursos por mejorarla. El sistema debe ser seguro contra espionaje, manipulación e interferencia intencional. Si no se tienen en cuenta debidamente las consideraciones de seguridad, como la confidencialidad, la integridad y la disponibilidad durante el ciclo de vida del sistema, estaremos ante un sistema mal desplegado (International Society of Automation, 2011). Hoy en día existen técnicas muy avanzadas de encriptación y protección de las conexiones contra posibles ataques

Los sistemas, como hemos visto anteriormente en la pirámide de la automatización, dependen normalmente de estrechas integraciones con la infraestructura TI corporativas para el intercambio de activos físicos de red, suministro de información a los sistemas empresariales, etc. El departamento de TI (Tecnologías de la Información) tiene la responsabilidad de proteger la infraestructura empresarial, mientras que los grupos de procesos tienen la responsabilidad de maximizar el rendimiento y minimizar el coste. Para que no se desencadene un conflicto entre ambos, ISA sugiere algo de lo que estoy totalmente de acuerdo y es vital para llevar a buen cabo un proyecto Wireless Industrial evitando retrasos, es involucrar significantemente al departamento de TI desde el principio en el diseño, para que puedan asegurar que se toman las consideraciones oportunas en medida de seguridad desde el principio (International Society of Automation, 2011).

3.3.7 Confidencialidad

Desde mi punto de vista está directamente vinculada a al anterior requerimiento. No obstante es importante verlo de forma independiente porque una de las principales consideraciones a tener en cuenta en las redes Wireless es la protección contra accesos no autorizados. Es importante añadir en este apartado, que unas de las principales causas que generan desconfianza en el Wireless y que genera el efecto inverso en el cableado, es la idea que el cableado es inmune a los accesos no autorizados, debido a que suele estar en zonas perimetrales controladas y si no se conecta físicamente

a él no es posible acceder a la información, generando sensación de que la confidencialidad está asegurada. Pero, hoy en día no es así, hay técnicas que permiten interceptar la información del cable usando señales electromagnéticas emitidas por los mismos (International Society of Automation, 2011).

En Wireless debido a que controlar el acceso físico a la señal es más difícil, la información se codifica de una cierta forma, como por ejemplo usando un conjunto de chips DSSS, los cuales hacen que la comprensión sea mucha más difícil, incluso sin estar encriptada. En Wireless se tiene que invertir un gran esfuerzo en evitar la radiación de señales fuera del área que queremos cubrir, evitando intrusos que puedan generar problemas en la red, para ello se pueden usar blindaje y/o direccionalidad de señales para mantenerlas dentro del área a cubrir, al mismo tiempo que se usan otros métodos para mantener la confidencialidad (International Society of Automation, 2011).

Hay que ser conscientes que a mayor nivel de cifrado mayor consumo de batería, y por consiguiente se traduce en un alto coste con el cambio de estas. Por lo tanto, se debe evaluar si el nivel de riesgo en cada caso de posibilidad de acceso no autorizado. Por ejemplo, si la red Wireless se encuentran en lugares remotos donde poca o ninguna persona suele llegar o cuando la distancia es corta y la potencia emitida es muy baja, se puede mantener un nivel de cifrado bajo para mantener un consumo óptimo de batería. Con esto lo que se intenta mostrar, es que mediante las soluciones fiables existentes en medidas de seguridad, el nivel debe adaptarse al grado de vulnerabilidad, pero desde mi punto de vista, en ningún caso se debería dejar una red sin cifrado.

3.3.8 Integridad

En las redes Wireless la integridad es un aspecto fundamental de la fiabilidad, y puede ser comprometida de forma inadvertida o intencionadamente. Un ataque típico que puede suponer un peligro intencionado es el “man-in-the-middle”, que mediante técnicas de “spoofing” una entidad no autorizada se introduce en la red y reemplaza paquetes correctos de información por incorrectos o engañosos. Por otra parte, peligros inadvertidos suelen incluir interferencias en las señales Wireless o cableadas.

La autenticación y el no-repudio de entidades en la red son críticas para la protección de la información en redes Wireless. Para que un nodo se una a la red Wireless y no se vea vulnerada la información de la misma se deben emplear métodos de autenticación rigurosos, por lo que el nodo que pretenda unirse a la red inalámbrica debe disponer de las credenciales adecuadas.

Los métodos de autenticación se clasifican típicamente en tres categorías. Dependiendo de la sensibilidad de la información, se puede aplicar uno, dos o a hasta los tres en conjunto (International Society of Automation, 2011):

1. Mediante una única identificación asignada permanentemente EUID (Enterprise UserID).
2. Mediante una clave única.

3. Mediante una característica física, como por ejemplo la capa de Control de acceso al medio (MAC).

Por otra parte, con el no-repudio se asegura que el remitente que está enviando datos, no pueda a posteriori negar que han sido enviados por él. Si una entidad que está autorizada en la red Wireless envía algún dato, estos no pueden ser enviados de vuelta. La entidad receptora, debe ser capaz de realizar la comprobación pertinente de que el remitente de los datos es realmente quien dice ser. Algunas formas para lograr los niveles deseados de no-repudio conocidas hoy en día son las firmas digitales que operan en un entorno de cifrado de clave pública (International Society of Automation, 2011).

3.3.9 Disponibilidad

Disponibilidad desde el punto de vista de seguridad se puede definir como el acceso fiable a la información y al uso de la misma en el momento oportuno. Por lo que se trata de que la información esté disponible en el momento exacto que se requiera, para ello los departamentos de IT deberán considerar implicaciones de seguridad (como ataques) y conectividad (fallos hardware) que puedan comprometer la disponibilidad de la información. Según ISA, todas las amenazas para el acceso oportuno y fiable a la información deben ser adecuadamente defendidos en las redes Wireless en la IACS (International Society of Automation, 2011).

3.3.10 Resiliencia

Resiliencia, debe ser uno de los atributos más importantes en una buena red industrial Wireless y se refiere a la capacidad de la red en recuperarse a un estado de operación después de una interrupción. Es evidente que siempre puede haber fallos impredecibles y aleatorios en el sistema que hacen que una rede no sea 100% fiable, pero la clave está en minimizar estos eventos al máximo (Supervivencia) y ser capaz de recuperarse fácilmente de estos eventos cuando ocurran (Recoverability) (International Society of Automation, 2011).

3.3.11 Capacidad de recuperación

La capacidad de recuperación o (Recoverability) es el ratio de tiempo entre fallos (fiabilidad) y el tiempo en restaurar las operaciones en caso de fallo (Mantenibilidad).

En el diseño de redes Wireless y los procesos en IACS para alcanzar la fiabilidad requerida se pude compensar mediante la redundancia. Una red que puede recuperase fiablemente y rápidamente de cualquier interrupción permite cierta libertad en el diseño y en la selección del equipamiento. Anteriormente hemos visto como una red en malla puede ofrecer una solución a este tipo de capacidad de recuperación a través de la redundancia, ya que un sistema con muchos elementos redundantes pero no fiables será mucho más fiable comparado con un sistema compuesto con un número pequeño de dispositivos. (International Society of Automation, 2011).

3.3.12 Supervivencia

La superveniencia también puede ser definida como tenacidad, y se refiere e la capacidad de seguir operando sin interrumpir el sistema aun con problemas que puedan ocasionar danos. Esta propiedad es muy importante en el hardware de comunicaciones expuesto en ambientes extremos con altas temperaturas, áreas peligrosas y entornos físicos con alta humedad.

3.3.13 Facilidad de diseño (Designability)

“Designability” es un concepto propuesto por ISA, para definir a la familia de atributos que tienen por objeto proporcionar la superación de consecuencias no previstas cuando se considera la adopción de una nueva tecnología, y de la cual todavía no se tienen muchas referencias. “Designability” se centra en las etapas iniciales y finales del ciclo de vida del sistema, teniendo en cuenta todas las consecuencias no previstas que pueden tener lugar. Si el sistema debe dar respuesta a la típica pregunta: "Si funciona: ¿por qué cambiarlo?” y motivar su instalación, si no, no habrá ninguna posibilidad de que se implemente. Esto dirige el diseño hacia una dirección en la que la implementación sea fácil, escalable y pueda desmantelarse al final de su vida útil. La tecnología debe mostrar que si se lleva a cabo la implementación, no va a ser un camino en una única dirección (sin retorno) donde el proyecto pueda llegar a un punto muerto y sin alternativas. Muchas de las consideraciones a tener en cuenta son las mismas que con una solución cableada, aunque con diferencias. Algunas positivas (no hay que remover cables) y otras negativas (eliminación de baterías peligrosas) (International Society of Automation, 2011).

3.3.14 Facilidad de despliegue

Ya se ha visto que la facilidad en el despliegue es uno de las mayores ventajas que ofrece la tecnología Wireless frente a la tecnología cableada. Pero para que este beneficio no se vea frustrado, se deben tener en consideración que las características del sistema Wireless faciliten esta tarea, entre las que se pueden comentar como obvias, que los sistemas no sean demasiado pesados o que requiera de una solución a medida con muchos accesorios que no estén estandarizados.

Durante la fase de instalación, la configuración y la solución de problemas son críticos. Si no se tiene cuidado durante la fase de instalación, se pueden llegar a perder sensores si estos no se configuran adecuadamente a medida que la implementación avanza, ya que puede que se vea el nodo en la red pero sin posibilidades de localizarlo físicamente. Para evitar este problema es necesario que la red inalámbrica disponga de un medio simple de captura de la ubicación física del sensor y asociar los tags en el sistema de adquisición de datos, como pudiera ser la MAC del nodo. (International Society of Automation, 2011).

Por la misma razón, la solución de problemas puede ser todo un reto durante el despliegue de la red Wireless. Si se pretende realizar un despliegue extensivo de un gran número de nodos inalámbricos, sin ninguna comprobación a medida que se avanza, postergando las conexiones y puesta en marcha para una última etapa, es casi misión imposible. Por lo que es obligatorio que el proveedor de red proporciona un sistema con instalación fácil de usar y un proceso de solución de problemas que incluya la posibilidad de verificar la instalación a medida que se avanza. ISA propone que un enfoque que ha

demostrado ser adecuado es desplegar la red en anillos concéntricos alrededor del nodo central, de esta forma se puede ver inmediatamente si los nodos han sido correctamente asociados a la red a medida que se avanza (International Society of Automation, 2011).

3.3.15 Escalabilidad

La facilidad de implementación puede llevar a problemas de escalado cuando el número de sensores y actuadores que se pueden implementar en la red están limitados por esta, especialmente en las redes en malla. Las consideraciones de escalado para aplicaciones Wireless difieren según donde se utilice cable o fibra (International Society of Automation, 2011).

Como se vio inicialmente, el espacio radioeléctrico es finito, hay limitaciones inherentes en la capacidad del canal en un determinado momento. Además, aun siendo los ciclos de trabajo ("Duty Cycle") relativamente bajos por nodo, si todos los nodos trabajan como Routers, como es el caso en una topología de red en malla, los ciclos de trabajo se incrementan cuando se acumula el tráfico de radio, y esto genera el efecto de la carga acumulativa de datos, como el progreso de la información a través de múltiples saltos desde los nodos hasta el nodo gateway (puerta de enlace). Esto plantea algunos límites prácticos para una red dada, pero no debe considerarse como una limitación real. Las redes modernas deben ser capaces de superponer el uno sobre otro, de forma que se pueda tener múltiples redes operando en el mismo espacio físico e informar a diferentes puertas de enlace. Además, los avances en los protocolos de codificación de datos y la reducción del tiempo en las redes seguirá ampliando el ancho de banda disponible (International Society of Automation, 2011).

3.3.16 Facilidad de desmantelamiento

Cuando se llega al momento en una planta en la que se debe realizar un mantenimiento de alto nivel o cuando la vida útil del sistema ya llego a su final, es necesario retirar el sistema y restaurar potencialmente la planta a su configuración original. En estos casos, el sistema inalámbrico resulta más práctico y fácil de desmantelar que un sistema cableado de igual magnitud, por lo que no debe ser una preocupación de que pueda haber grandes problemas inesperados. Con el sistema inalámbrico el desmantelamiento se facilita debido a que no hay cables que eliminar, incluso reduce drásticamente el coste que supondría la restauración al no tener que reparar las tiradas de cables. Aunque tiene el inconveniente de que puede que se tenga que manejar materiales peligrosos como las baterías. En el desmantelamiento también se debe considerar, el realizar una contabilidad cuidadosa de los medios de almacenamiento de datos, el firmware utilizado en dispositivos, incluso el almacenamiento temporal de datos o instrucciones que se mantienen en cachés de memoria (International Society of Automation, 2011).

3.4 Componentes redes Industriales

El principal objetivo de las redes industriales es la de ofrecer la comunicación con y entre los componentes y sistemas especializados encargados del control y la adquisición de los datos como los PLC's (Programmable Logic Controllers), el sistema SCADA (Supervisory Control and Data

Acquisition) y el DCS (Distributed Control System) (Introduction to Industrial Control Networks, Brendan Galloway).

1. PLC: Los PLC's han progresado significativamente desde la primera vez que fueron usados en 1968, reemplazando a los sistemas cableados de relés por la división de transmisión automática de General Motors, y los hay disponible con un amplio abanico de características y coste. Estos fueron diseñados con el objetivo de que cumpliesen requerimientos como fácil programación y reprogramación, fácil mantenimiento y reparación y con tamaños cada vez más pequeños y económicos, con la capacidad de operar en la planta y comunicarse con los sistemas de adquisición de datos. Hoy en día son capaces de procesar entradas y salidas tanto digitales como analógicas, e implementar lazos de control tanto proporcionales, integrales como derivados o incluso PID (controlador proporcional-integral-derivado) que puede ser usado por ejemplo para el control de temperatura de un proceso. Históricamente el uso de PLC's se limitaba a un pequeño grupo de lazos, cuando en una planta se requerían cientos o miles de lazos, se usaba un DCS[7]. Aunque a medida que los PLC's han evolucionado y son más potentes la diferencia entre las aplicaciones de PLC's o DCS's se ha reducido. Hoy en día el PLC de seguridad, diferentes a los convencionales PLC's se han vuelto muy popular los cuales son usados, debido a que están específicamente diseñados para ser usados en aplicaciones críticas como pueda ser en un sistema ESD (Emergency Shutdown System), un sistema de apagado de emergencia de una línea de producción.
2. SCADA: Es un sistema que en si no realiza ningún control, solo tienen la función de supervisar. Centrado principalmente en la adquisición de datos y presentación de la misma en una interfaz Hombre-Máquina (HMI), aunque incluso permite él envió de comandos de alto nivel a hardware de control, como por ejemplo el encendido de un motor. SCADA es especialmente apto para industrias donde la distribución geográfica muy grande (cientos de km) con gran diversidad de hardware. Los dispositivos de control que se comunican con SCADA son llamados RTU (Remote Terminal Unit) y son un tipo especial de PLC. Los RTU's se comunican con el MTU (Master Terminal Unit). Debido a la larga distancia a la que pueden estar los RTU's, hace que el sistema SCADA tenga restricciones, siendo esto el aspecto más importante sobre el que el sistema SCADA está diseñado. Estás largas distancias obliga la utilización de comunicaciones poco fiables o con anchos de banda limitados, lo que hace que SCADA este orientado a el control de eventos en vez de al control continuo del estado de los procesos, centrándose solo en el reporte de cambios en el estado de la monitorización. Esto hace que los requisitos de ancho de banda de SCADA sean relativamente bajos.
3. DCS: Con funcionamiento similar a SCADA, presenta la información en un HMI de los dispositivos de control, pero con la diferencia que está orientado a control de proceso. Esto significa que se centra en la presentación de una información constante del estado del proceso. En general, los dispositivos de control consisten en PLC's tradicionales, habitualmente con procesadores potentes implementando múltiples lazos de control cerrados. Lo que no lo hace

[7] http://en.wikipedia.org/wiki/Programmable_logic_controller

tan indicado para sistemas geográficamente distribuidos, pero si para la interconexión de plantas locales en refinerías, estaciones de energía y otros ámbitos de procesos. El alto nivel de interconexión entre el software DCS y el hardware de control permite que una sola herramienta de ingeniería pueda ser usada tanto para programar controladores como configurar la capa software. En el mercado, el sistema DCS se suele encontrar como un paquete completo de software y hardware ofrecido por el mismo vendedor, incluyendo la instalación y configuración del mismo. Esto desde mi punto de vista, es una gran ventaja que posibilita a los clientes finales obtener un gran ahorro tanto en tiempo de implantación y configuración como en coste, sobre todo porque no es fácil encontrar personal capacitado en la instalación, configuración, testeo y puesta en marcha de un sistema DCS. El DCS también puede ser implementado usando computadoras que se comunican con equipamiento de la planta directamente o a través de un bus de comunicaciones, donde aplicaciones de servidor coordinan las aplicaciones cliente que muestran la información.

3.5 Redes Wireless de Planta (WPN) y Red Wireless de Campo (WFN)

En la pirámide de la automatización se pueden diferenciar dos topologías de redes. Por un lado tenemos la WFN, que se ubica en el nivel 0, donde se encarga de la interconexión de todos los elementos finales de control para medición y control de las variables de proceso, así como sensores. Por otro lado, la WPN se acomoda en cualquiera de los otros niveles de la pirámide, mediante la virtualización debidamente aislada de cada uno de los niveles con los mismos dispositivos de red (Salgado J. R., 2014):

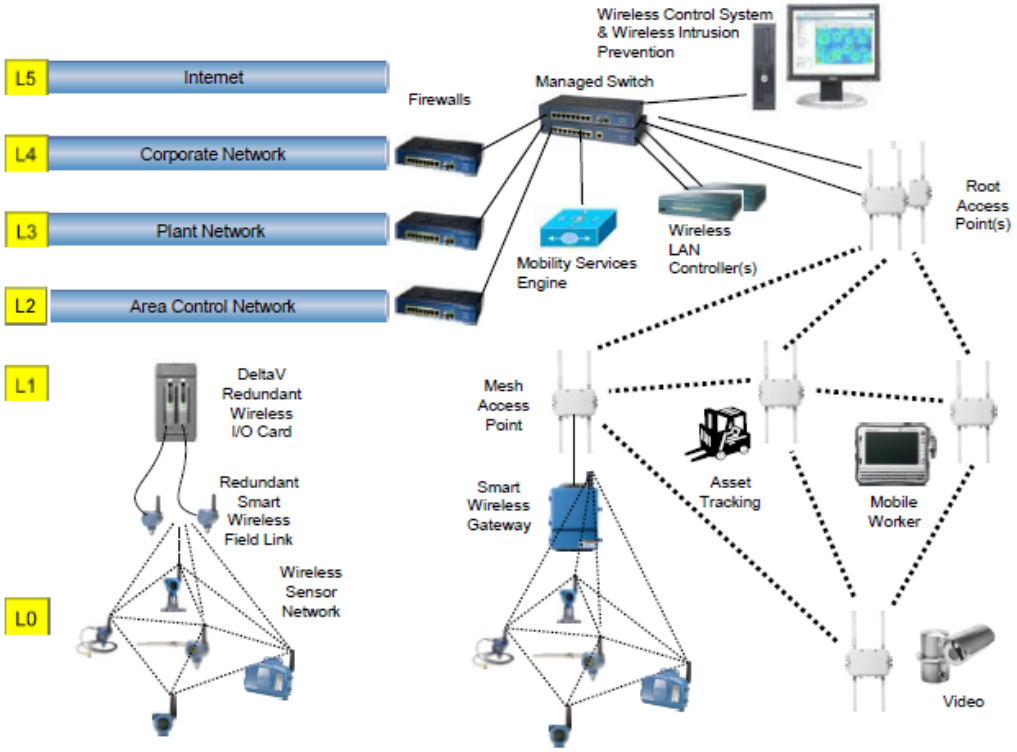


Figura 18: Redes WFN y WPN (Emerson Process Management, 2011).

Cada uno de los dispositivos de red, como las PDA's, ordenadores, RFID tags o los instrumentación de campo inalámbricos, tienen todo el tráfico se transmite a través de uno de los puntos de acceso en malla de la red de planta (Mesh Access Point). Desde los puntos de acceso, la comunicación pasa a través de la red en malla hasta que alcanza el punto de acceso principal (Root Access Point) y de ahí, la comunicación pasa a través del Switch gestionado (Managed Switch) donde todas las LAN's virtuales son separadas en diferentes LAN's físicas. Finalmente, la comunicación se encamina a través de los diferentes firewalls de cada nivel al dispositivo final de la red (Emerson Process Management, 2011). En las redes WFN suelen estar formadas por una gama de dispositivos Wireless para control y monitorización de presión, caudal, nivel, temperatura, analizadores, interruptores, así como están saliendo nuevos desarrollos en posición de válvulas manuales, detectores fugas de vapor, detectores de hidrocarburos, detectores de gas, detectores de corrosión, señales discretas (E/S), vibración de máquinas, así como adaptadores Wireless, como el adaptador WirelessHart de Emerson (Salgado J. R., 2014).

Figura 19: Adaptador WirelessHART (Emerson)

Las redes WFN puede tanto estar directamente conectada a los diferentes sistemas de control y gestión de planta, a través de la puerta de enlace, como son el Sistema de Control, Sistema ESD/F&G, Sistema de gestión de activos, mantenimiento, o integrase en la red WPN mediante un enlace a uno de los Gateways existentes. Por lo que respecta la integración de ambas redes, se puede llevar a cabo mediante 3 formas diferentes (Salgado J. R., 2014):

- Mediante una conexión cableada del Gateway a la red de control, lo que está totalmente aislada de la red de planta.

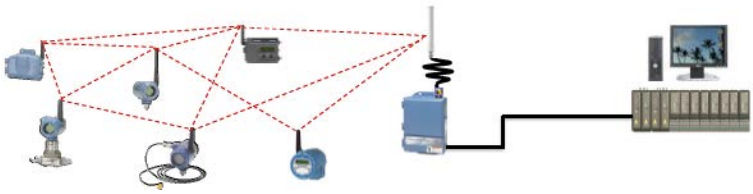


Figura 20: Conexión cableada del Gateway a la red de control

- Mediante un enlace cableado del Gateway a la red de planta y a través de esta la WFN se conecta a los sistemas de control.

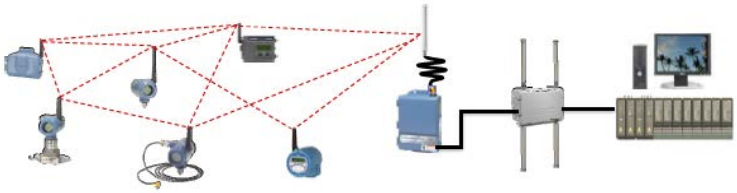


Figura 21: Conexión del Gateway a la WPN y de esta a los sistemas de control

- Y por último, mediante una conexión directa inalámbrica de la red WFN a un Gateway de la WPN, quedando totalmente integradas.

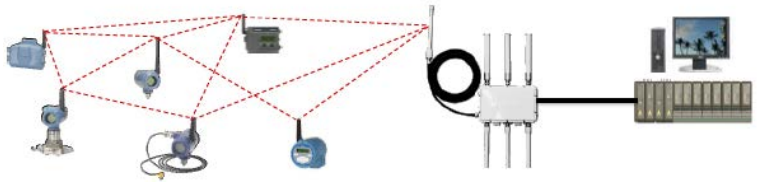


Figura 22: Conexión directa inalámbrica de la red WFN a un Gateway de la WPN

3.6 Estándares Wireless

En las redes industriales la cobertura no es un requisito muy importante, ya que habitualmente en las redes en campo con topología en malla no suelen haber grandes distancias entre instrumentos, en caso de haberlas, se suelen reforzar con repetidores. El requerimiento dependerá de la aplicación, Pero, debido a que muchas veces se usa la cobertura para categorizar las tecnologías Wireless vamos a mostrar a continuación una comparativa de las diferentes tecnologías inalámbricas disponibles en el mercado. Esta incluye el rango, la potencia de transmisión y la velocidad de transmisión.

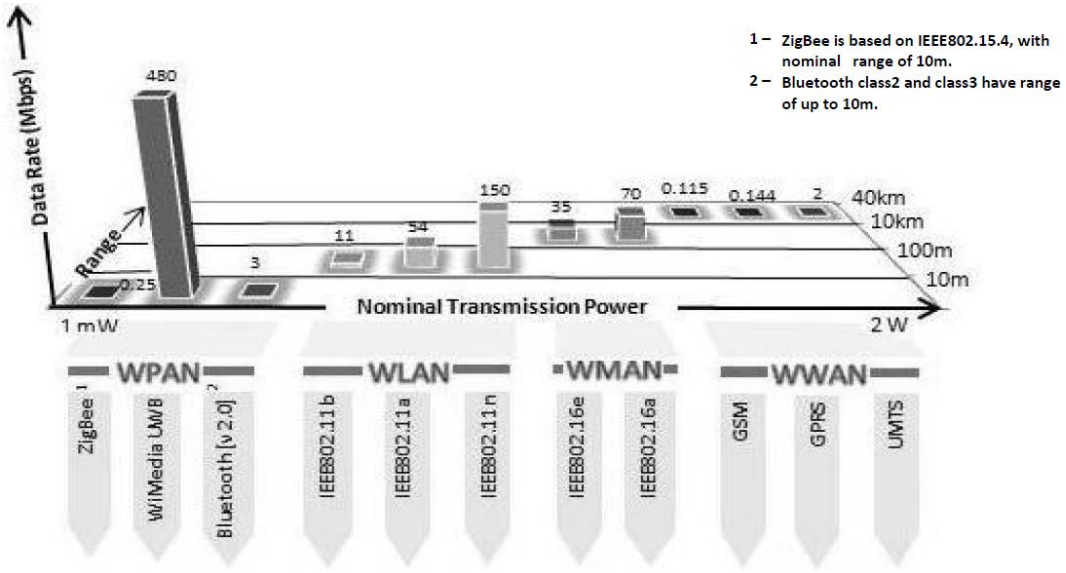


Figura 23: Fuente: Comparativa tecnologías Wireless (Ikram W., Thornhill N. F., 2010)

Los estándares cubiertos por las redes WPAN y WLAN son las que mayor interés despiertan en las redes Wireless de la IACS, sobre todo en los niveles bajos de la pirámide de la automatización. Las demás pueden usarse, pero en niveles corporativos o en la red de planta. Vamos a ver a continuación cada una de ellas.

3.6.1 IEEE 802.15.4 (Low Rat e WPAN/ZigBee)

ZigBee es un estándar relativamente nuevo que fue diseñado específicamente para sensores con baterías y está basado en el estándar IEEE 802.15.4 (Ikram W., Thornhill N. F., 2010). Es altamente atractivo para aplicaciones simples con baja velocidad de transferencia, baja potencia y que se requiera de un coste bajo. Sobre las bandas 868MHz (Europa) ofrece un canal, 10 sobre la banda Estadounidense 902-928MHz y 6 en la banda mundial ISM 2.4GHz. Una característica importante es

que permite Dispone de una garantía muy baja de Quality-of-Service, no soporta de determinismo y no emplea saltos de frecuencia haciendo susceptible a interferencias.

3.6.2 IEEE 802.15.3a (WPAN/UWB)

Ultra-Wideband es una tecnología diseñada para aplicaciones que requieren de un bajo consumo y un alto ancho de banda, además ofrece una alta productividad. Gracias al ancho de banda que ofrece mayor de 500 MHz o del 25% de la frecuencia central permite abordar asuntos de trayectoria múltiple y la interferencia. Puede usar frecuencias que no pueden hacer uso otras tecnologías, y que recientemente han sido aprobadas, estas van desde 3.1 GHz hasta 10.6 GHz: más de 7 GHz de anchura. Dispone de una anchura de más de 500 MHz por cada canal de radio, dependiendo de su frecuencia central[8].

3.6.3 IEEE 802.15.1 (WPAN/Bluetooth)

Bluetooth opera en la banda ISM de los 2.4GHz y usa FHSS para evitar interferencias por medio de saltos de frecuencia a 1600 veces por segundo. Es una red ad-hoc generada por un maestro con la posibilidad de hasta siete nodos esclavos activos (Bluetooth, 2009), esto es un problema de escalabilidad que junto con la complejidad de sus protocolos y la falta de flexibilidad en la topología de red, lo hacen muy poco atractivo en redes industriales (Ikram W., Thornhill N. F., 2010).

3.6.4 IEEE802.11a/b/g/n (WLAN)

Todos estamos más acostumbrados al estándar IEEE802.11, ya que es el que habitualmente se usa las redes locales convencionales y se conoce como Wi-fi (diminutivo de Wireless fidelity). El IEEE 802.11 es la especificación que describe las características de una red Wireless LAN (Local Area Network) en las bandas 2.4, 3.6, 5 y 60 GHz. El estándar 802.11 define 14 canales en la banda de los 2.4GHz, con una amplitud de 22MHz y están separados por un espacio de 5MHz, sobreponiéndose unos canales con otros. El estándar hace uso de métodos de señalización DSSS y OFDM para controlar las interferencias que pueden causar hornos microondas, teléfonos inalámbricos, así como de dispositivos Bluetooth, en dispositivos Ethernet Wireless que usen las bandas 802.11b y g[9]. A pesar de que este estándar ha prestado poca atención aspectos tan importantes en redes industriales como la energía, transferencia en tiempo real, QoS, fiabilidad y escalabilidad que hemos visto anteriormente, ha sido usada extensivamente en redes industriales por su altos ratios de transferencia sobre distancias cortas (Ikram W., Thornhill N. F., 2010).

3.6.5 IEEE 802.16 WiMax (WMAN)

Wimax (Worldwide Interoperability for Microwave Access) es un estándar relativamente reciente para servicios fijos de ancho de banda con ratios de 30 a 40 megabits por segundo, llegando a 1 Gbit/s en estaciones fijas. Opera en las bandas 2.3, 2.5 y 3.5 GHz. Generalmente se suministra a través de las

[8] http://en.wikipedia.org/wiki/Ultra-wideband
[9] http://en.wikipedia.org/wiki/IEEE_802.11

redes de proveedores comerciales, aunque también se prevén redes privadas (Industrial Wireless Technology and Planning).

3.6.6 Red Celular (WWAN)

GSM (GPRS, EDGE, UMTS/HSDPA), CDPD, CDMA, LTE y IMT-Advanced son diferentes sistemas para comunicaciones móviles que se utilizan en la transmisión de datos. A pesar de que se utilizan en entornos industriales para la gestión de inventario, no son habitualmente usados para aplicaciones de planta en la IACS (Industrial Wireless Technology and Planning).

Finalmente, a lo largo de esta sección se ha podido ver las diferentes antenas que pueden ser implementadas en redes Wireless industriales, de las cuales las Omnidireccionales son las más implementadas sobre todo en redes Wireless con topología en malla, por la flexibilidad que ofrecen, y que tienen una cobertura de 360 grados, además no requiere de un estudio detallado de la ubicación de los dispositivos. Además de las antenas omnidireccionales ya se empiezan a ver dispositivos con antenas integradas Planar, permitiendo así tamaños más compactos. Por lo que respecta a los estándares Wireless, soy de la opinión de Ikram W., Thornhill N. F. (2010), donde según Backer (2005) desde el punto de vista industrial, ZigBee tiene mayor ámbito de aplicación en aplicaciones industriales que Bluetooth, principalmente debido a su posibilidad de topología en malla, al alcance y que la vida útil de la batería es mayor. No obstante, ZigBee es más vulnerable a interferencias y jamming debido a que utiliza un canal estático para las comunicaciones en la red. Por motivo de que las interferencias desde otras fuentes pueden provocar retardo en la entrega de paquetes, e incluso la perdida de datos, hace poco recomendable la utilización de ZigBee para el control de aplicaciones industriales (Lennvall et al., 2008). Por otro lado, Wi-Fi tampoco llega a ser una solución apropiada debido a que comparado con otras tecnologías, su consumo energético es alto, con el 802.11A/b/g la seguridad de la red es menor y además presenta problemas al operar en ambientes con un alto nivel de ruido eléctrico (Caro, 2009).

Capítulo 4 Protocolos de comunicación Industrial

Entre los principales protocolos de comunicación que han surgido para cumplir con los requisitos demandados en las redes industriales podemos encontrar: el estándar ISA100.11a, y el estándar WirelessHART. Ambos se basan en el uso del estándar IEEE 802.15.4 para redes de área personal de baja velocidad, operando en la banda de los 2.4GHz. Para asegurar la máxima utilización de la banda, la configuración de los puntos de acceso en redes Wireless industriales se suelen hacer con canales que no se solapan, como el 1, el 6 y el 11. La tecnología de radio usa una combinación de saltos de canal y secuencias directas, espectro ensanchado (DSSS) para permitir la coexistencia con otros usuarios del mismo espectro, de este modo las redes pueden ocupar el mismo espectro y espacio físico sin interferirse uno con otro (Nixon M., 2012). Además tienen la característica de bajo consumo energético, permitiendo así prolongar la vida útil de las baterías.

ANSI/ISA100.11a: Este estándar fue desarrollado por ISA y fue anunciado en el año 2009. Fue diseñado para aplicaciones no críticas relacionadas con el control de procesos, aunque en su primera emisión soporta el control de lazos de control con tiempos de ciclos de más de 1 segundo y latencias mayores de 100ms. Se espera que en futuras revisiones mejorar la capacidad de controlar aplicaciones críticas con el control de lazos con tiempos de ciclos por debajo de 1 segundo y latencias de menos de 100ms (Caro R. H., 2008).

WirelessHART (IEC62591-1): Protocolo desarrollado por HART (Highway Addressable Remote Transducer Protocol), el cual salió a la luz en el año 2007. Está basado en el protocolo de comunicación HART, actualmente en la versión 7, que se lleva usando desde finales de los años 80, el cual proporciona una conexión cableada con los instrumentos de campo de dos sentidos mediante una señal analógica de 4-20mA. WirelessHART ha heredado de su análogo características como amplias funciones de seguridad, transferencias de datos no solicitados, notificaciones de eventos, las transferencias en modo bloque y diagnósticos avanzados (Nixon M., 2012). Fue especialmente diseñado para cubrir las necesidades en las redes de campo en el control de procesos y permite la interoperabilidad con diferentes estándares.

ZigBee PRO: Es una extensión de ZigBee que salió a la luz en 2007, fue diseñado para cubrir requerimientos de bajo consumo energético y baja velocidad de transmisión, además ofrece características de seguridad mejoradas.

A día de hoy tanto el estándar WirelessHART como ISA100.11a son las soluciones más usadas y las que mejor se ajustan al sector industrial de la Automatización y Control de Sistemas. Por esta razón el resto del documento mostraran como aun siendo muy similares, tienen sus diferencias.

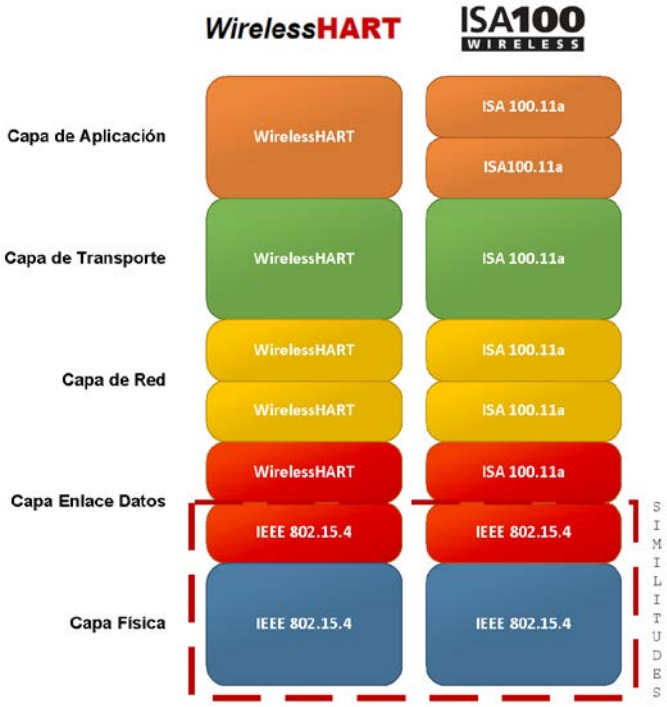


Figura 24: Esquema modelo OSI estándares Wireless (Creación propia basada en Radmand P., et al. 2010).

4.1 WirelessHART (IEC62591-1)

4.1.1 Arquitectura

Las redes WirelessHART habitualmente están compuestas por diferentes tipos de elementos, como[10]:

- Dispositivos de campo con capacidades de enrutamiento de paquetes (Routers) en la red en malla.
- Adaptadores para unir dispositivos HART cableados a la red Wireless en malla.
- Puntos de acceso, responsabilizados de la comunicación entre las aplicaciones host y los dispositivos de campo conectan la red en malla WFN al Gateway.
- Gateway o pasarela, actúa como interfaz entre la WPN y la WFN.
- Administrador de red que puede estar incluida en el Gateway o estar implementados de forma independiente. Encargado de controlar toda la red, debe identificar las mejores rutas y gestionar la distribución de tiempos de acceso, así como de la programación de la comunicación de cada dispositivo en la red.
- De uno a varios administradores de seguridad que puede estar incluidos en el Gateway o estar implementados de forma independiente. Encargados de gestionar el acceso a la red de dispositivos autorizados y las claves de cifrado.
- Repetidores encargados de dirigir los mensajes WirelessHART sin ningún tipo de acceso a los procesos, con el objetivo de ampliar el alcance de la red o evitar obstáculos.
- Dispositivos de móviles de mano, como por ejemplo los que puedan llevar los operarios o ingenieros de planta para mantenimiento o diagnóstico.

Un ejemplo típico de la arquitectura estándar WirelessHART se muestra a continuación:

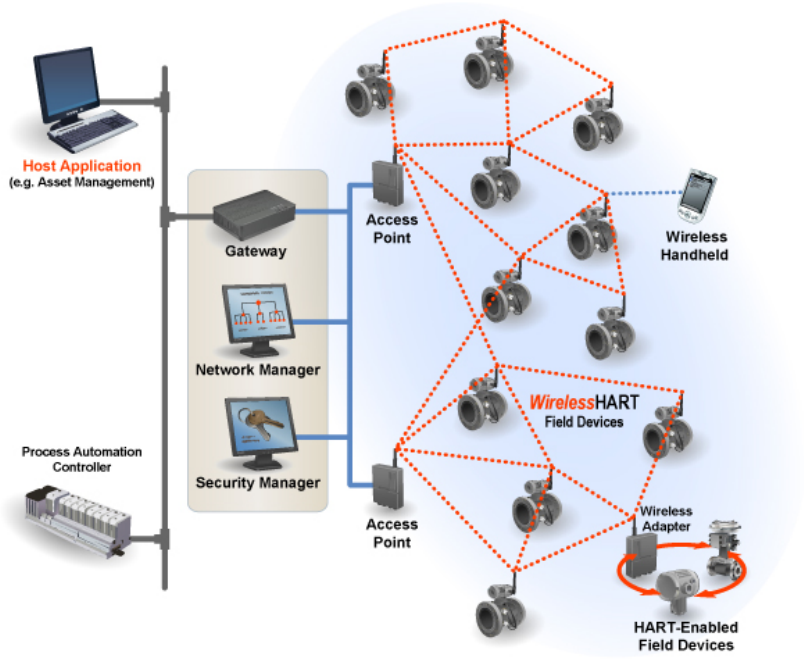


Figura 25: Arquitectura estándar WirelessHART (Fuente: hartcomm.org)

[10] http://sp.hartcomm.org/protocol/wihart/wireless_how_it_works.html

Las radios utilizadas en las redes WirelessHART operan en la banda de los 2.4GHz. Las comunicaciones son sincronizadas mediante Acceso múltiple por división de tiempo (TDMA) el cual tiene la ventaja que cada dispositivo tiene su turno sin ninguna interrupción, reduciendo los problemas de latencia y aumentando la utilización del ancho de banda (Alexfeng, 2013). La comunicación se realiza de forma programada a través de las diferentes rutas redundantes definidas previamente por parte del administrador de red, basándose en la latencia, eficiencia y fiabilidad. Para evitar que las rutas no se cierren y se saturen, los mensajes se alternan continuamente entre las diferentes rutas. La programación se basa en la información general de ruteo de la red en combinación con los requerimientos de comunicación requeridos por los dispositivos y las aplicaciones. La programación se lleva a cabo por un administrador de red utilizando la información general de encaminamiento de red en combinación con los requisitos de comunicación que los dispositivos y aplicaciones han proporcionado. La programación se traduce en la transmisión y recepción de ranuras de tiempo (Time Slots) y se transfiere desde el administrador de red a cada dispositivo, donde WirelessHART divide cada segundo en ranuras de 10 milisegundos. El administrador de red adapta las rutas y la programación constantemente adaptándose a los requerimientos de la red.

El administrador de red control los recursos (Chen D., Nixon M., Mok A., 2010).

- Los 15 canales RF permitidos en un sistema WirelessHART
- Tiempo de ranuras, los 10mseg de cada ranura subdividen súper tramas de tamaños configurables.
- Links, conexiones a dispositivos vecinos especificando un canal y tiempo de ranura en una súper trama usada para la transmisión y recepción.
- Enrutamiento gráfico (Graph): es el camino a través de una red en malla de dispositivos WirelessHART desde un dispositivo origen a un dispositivo destino;

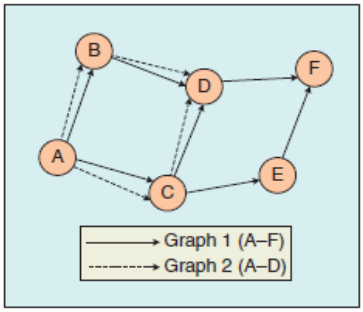


Figura 26: Ejemplo Enrutamiento gráfico

Varias arquitecturas son posibles para escalar WirelessHART de forma que pueda albergar un gran número de dispositivos y permita velocidades de transmisión altas. Una de más habituales que ha sido implementada en diferentes tipos de plantas donde hay Centros de Control Distribuidos (DCS) existentes, es usando múltiples Gateways conectados a HART sobre red troncal IP.

Otra forma de escalar la red WirelessHART es mediante el uso de múltiples puntos de acceso como se muestra en la imagen siguiente:

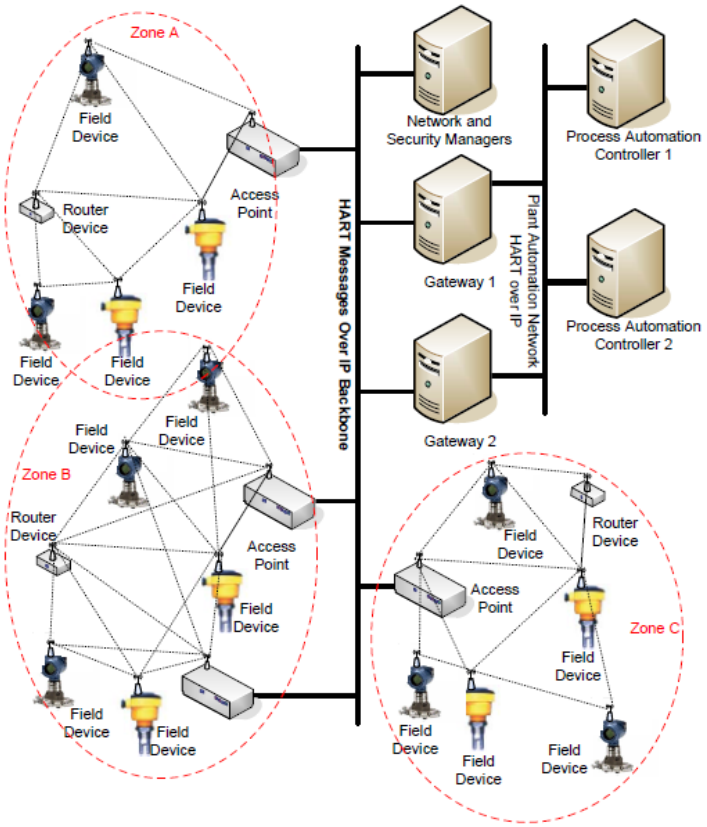


Figura 27: Múltiples puntos de acceso mediante una red troncal (Chen D., Nixon M., Mok A., 2010).

La cual ofrece algunas ventajas como (Chen D., Nixon M., Mok A., 2010).

- Coordina los recursos Wireless para prevenir islas que se solapan en el espacio RF.
- Reutiliza recursos Wireless en islas no solapadas para escalar la red a un gran número de dispositivos y un mayor rendimiento del sistema.
- Proveer múltiples puntos de acceso troncales para un mayor rendimiento hacia la red troncal (donde cada punto de acceso tiene un rendimiento de 100 paquetes por segundo).
- Proveer puntos de acceso para conectar a la red troncal que va a plantas con estructuras diferentes y plantas alejadas.

La arquitectura de la pila de protocolos de WirelessHART está basada las capas OSI 7, que incluye las capas: capa física, capa de enlace de datos, capa de red, capa de transporte y capa aplicación, las cuales se describen a continuación.

Figura 28: Pila protocolos HART (Creación propia basada en Costa M. S. y Amaral J., 2012).

4.1.2 Capa física

La capa física es responsable del método de modulación, potencia de señal y la sensibilidad del dispositivo (WANG G., 2011). La capa física WirelessHART está basada en el estándar IEEE 802.15.4-2006 en la banda de 2.4Ghz, que emplea el espectro ensanchado por secuencia directa (DSSS) y modulación Offset Desplazamiento de fase en cuadratura Shift Keying (O-QPSK), junto con sus requerimientos adicionales y excepciones. O-QPSK es una variante de cambio de fase de modulación de claves usando 4 valores diferentes de la fase a transmitir. A medida que evoluciona la tecnología radio, puede fácilmente añadir capas físicas adicionales (Chen D., Nixon M., Mok A., 2010).

4.1.3 Capa de enlace de datos

La capa de enlace de datos tradicionalmente provee acceso a los canales de radio y es responsable de la sincronización de radio. Está encargada de la transmisión segura, fiabilidad y libre de errores de paquetes entre dispositivos en una red en malla basada en la capa física del estándar IEEE802.15.4.para entornos industriales con condiciones extremas (WANG G., 2011).

Opera en las bandas ISM desde la 2400 hasta la 2483.5 MHz, usando los canales del 11 al 26, con una separación de 5MHz y con velocidades de transferencia de hasta 250kbits/s. La capa de enlace de datos extiende la funcionalidad de la capa MAC definiendo tiempos de ranuras fijos de 10ms, saltos de frecuencia sincronizados y división de tiempo múltiple para permitir comunicaciones libres de colisiones y deterministas. Para la gestión de los tiempos de ranuras, se incorpora el concepto de súper trama que incorpora un grupo consecutivo de tiempos de ranuras. Una súper trama es periódica, con el total de la longitud de las ranuras miembro como periodo. Todas las súper tramas en las redes WirelessHART empiezan desde la ASN 0 (número de ranura absolución), el tiempo cuando la red es creada inicialmente. Cada súper trama se repite a lo largo del tiempo basado en su periodo. Una

transacción en un tiempo de ranura es descrito mediante un vector: {frame id, index, type, src addr, dst addr, channel offset}, donde tenemos que, el frame id identifica la supertrama, el índex es el índice de la ranura en la supertrama, type indica el tipo de ranura (transmit/receive/idle), src addr y dst addr son las direcciones de los dispositivos de origen y destino respectivamente, mientras que channel offset contienen el canal lógico a ser usado en la transacción. WirelessHART introduce el concepto de la lista negra de canales (blacklisting), con el objetivo de definir correctamente el canal a usar. Esta lista contiene la lista de canales que son afectados por interferencias, de este modo, el administrador de la red puede desactivar completamente el uso de estos canales. Esta tabla debe contener menos de 16 entradas, lo que limita de este modo a la tabla de canales activa que mantiene cada dispositivo para soportar el salto de canales. Para un desplazamiento de canal y ranura dada, el canal actual se determina por medio de la siguiente formula (Chen D., Nixon M., Mok A., 2010):

$$\text{ActualChannel} = (\text{ChannelOffset} + \text{ASN}) \,\%\, \text{NumChannels}$$

4.1.3.1 Formato de la Unidad de datos de protocolo (DPDU)

En la Capa 2 del modelo OSI, la unidad de datos de protocolo es la trama la cual en WirelessHART tiene la siguiente forma (WANG G., 2011):

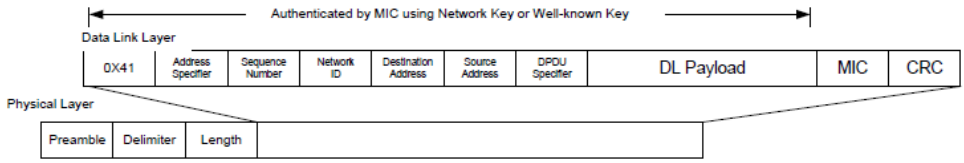


Figura 29: Formato trama WirelessHART

- La Address Specificier, es usada para especificar qué tipo de dirección es contenida en el campo origen y destino de la DPDU, ya sea un nikname de 16 bits que es asignado por el administrador de red o la dirección EUI (Identificador único extendió) de 64 bits.
- Los bits en el campo DPDU Specifier indica la prioridad de la DPDU, si la DPDU se valida mediante clave de red y el tipo de DPDU como Data, Avertise, Keep-Alive, etc.
- Los 32 bits de MIC es un código de integridad de mensaje para la autenticación de la Capa de enlace de datos usando clave de red. Durante el proceso de unión, el MIC del DPDU es generado usando una clave conocida (Well-Known).
- Los 16 bits CRC son usados para verificar errores aleatorios, y que el formato de cabecera de la capa física es acorde al estándar IEEE 802.15.4.

4.1.4 Capa de red

La capa de red se encarga de diferentes funciones, pero entre las principales están de la proveer la seguridad y fiabilidad en las conexiones extremo a extremo, las tablas de ruteo que son usadas para encaminar los mensajes a través de las rutas gráficas y las tablas de tiempo que son usadas para contener la información de ancho de banda para servicios específicos dentro de la red en malla.

4.1.4.1 Especificación Cabecera

A continuación se muestra el único tipo de cabecera en WirelessHART, con direccionamiento y enrutamiento básico. Los campos especificaciones y parámetros de implementación de seguridad están contenidas en subcabecera NL Playload.

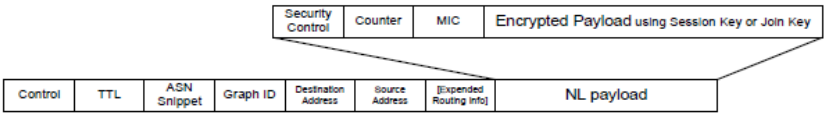


Figura 30: Estructura NPDU WirelessHART

4.1.5 Capa de transporte

La capa de transporte con la cooperación de la capa de red, garantiza la conexión en la red malla y le ofrece a la capa de aplicación la posibilidad de transporte en modo sin conexión. Soporta transacciones conocidas y desconocidas, donde las conocidas es para garantizar la entrega del mensaje y las transacciones desconocidas son para comunicaciones específicas como la publicación de datos.

4.1.3.1 Formato de la Unidad de datos de protocolo (TPDU)

En WirelessHART la TPDU esta especificada de forma simple (WANG G., 2011):

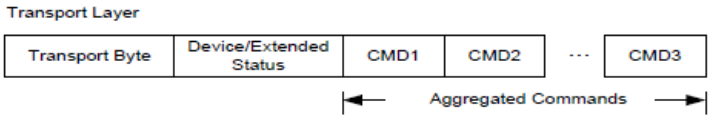


Figura 31: TPDU en WirelessHART

- Transport Byte: especifica el tipo de transacción (conocida o desconocida), el tipo de mensaje (petición o respuesta), la identificación del propietario de la difusión y el número de secuencia utilizado para gestionar el tráfico de paquetes.
- Device/Extended status.
- Aggregated Commands: WirelessHART permite transportar múltiples comandos en una simple transacción.

4.1.6 Capa aplicación

La capa de aplicación proporciona servicios de procesos de aplicación definidos por el usuario y define los servicios necesarios de comunicación para habilitar la comunicación de objeto a objeto entre aplicaciones distribuidas.

En WirelessHART la capa de aplicación está orientada a comandos, y es heredada de la capa de aplicación del estándar HART para el cableado, la cual define los comandos, respuestas, tipos de datos y los reportes de estado soportados (Petersen S. y Carlsen S., 2011). Toda la comunicación entre dispositivos al nivel de la capa de aplicación es a través de los siguientes grupos de comandos definidos: Comandos Universales, de prácticas comunes, de familia de dispositivos y específicos de dispositivo.

4.1.6.1 Formatos cabeceras Capa de Aplicación

La APDU en WirelessHART puede verse como simple o comandos agregados, donde cada uno incluye un numero de comando de 16 bits, longitud y campo de datos.

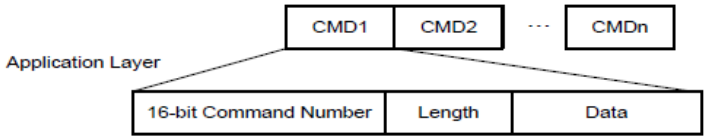


Figure 6: Formato APDU WirelessHART ((WANG G., 2011).

4.2 ANSI/ISA100.11a

4.2.1 Arquitectura

ISA100.11a está destinado a ser parte de un grupo de estándares diseñados especialmente bajo criterios como: flexibilidad, soporte múltiples protocolos, uso estándares abiertos, soporte múltiples aplicaciones, fiabilidad (detección de errores, salto de canal), determinismo (TDMA, soporte QoS) y seguridad. Con el objetivo de soportar un amplio rango de necesidades de plantas industriales Wireless, incluyendo automatización de procesos, automatización de fabricación y RFID. De los cuales solo ISA100.11a ha sido hasta ahora aprobado (Nixon M., 2012).

Las redes ANSI/ISA100.11a habitualmente están compuestas por diferentes tipos de elementos, como (Hatler M., 2012):

- Dispositivos de campo sin capacidad de enrutamiento, como dispositivos de Entrada/Salida (sensores y actuadores).
- Dispositivos de campo con capacidad de enrutamiento que además pueden actuar como dispositivos E/S.
- Routers troncales (backbone), capaces de encaminar información desde/hacia la red troncal.
- Administrador de sistema.
- Administrador de seguridad.
- Gateway.
- Dispositivo con capacidad de mantener la fuente de tiempo master para el sistema.

Un ejemplo típico de la arquitectura estándar ISA100.11a se muestra a continuación:

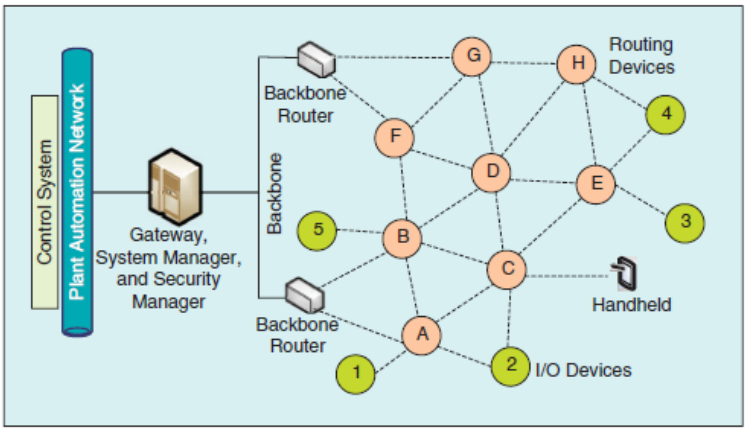


Figura 32: Arquitectura estándar ISA100.11a (Petersen S. y Carlsen S., 2011).

En la arquitectura se puede apreciar como el Gateway y el sistema de administración y de seguridad, deben implementarse con la función de Router troncal para tener acceso a la red troncal. ISA100.11a basa sus capas de red y transporte en 6LoWPAN, IPv6 y estándares UDP. La capa de enlace de datos es única para ISA100.11a y usa una forma de la capa MAC IEEE802.15.4 que no se ajustaban a las especificaciones. La capa de enlace de datos implementa enrutamiento gráfico, salto de frecuencia y ventajas la multiplexación por división de tiempo. En las redes Wireless, es en la capa de enlace de datos se realiza toda la redirección de mensajes, la cual permite flexibilidad a la hora de especificarla, mediante la configuración de opciones como el tamaño del slot de tiempo y saltos de frecuencia lentos, así como duo-ACKs. (Nixon M., 2012).

La arquitectura de la pila de protocolos de ISA100.11a está basada las capas OSI 7, que incluye las capas: capa física, capa de enlace de datos, capa de red, capa de transporte, las cuales se describen a continuación.

Figura 33: Pila protocolos HART: Creación propia, adaptada de (Costa M. S. y Amaral J., 2012).

4.2.2 Capa física

La capa física en ISA100.11a al igual que con WirelessHART está basada en el estándar IEEE 802.15.4-2006 en la banda de 2.4GHz, que emplea el espectro ensanchado por secuencia directa (DSSS) y modulación Offset Desplazamiento de fase en cuadratura Shift Keying (O-QPSK). Con la pequeña diferencia de que el canal 26 lo incluye como opcional, de los definidos en el estándar IEEE 802.15.4, el cual no está incluido en WirelessHART ya que no es legal en algunos países. Estos canales son del 11 al 25, tienen un ancho de banda de 2 MHz y están espaciados en 5-MHz. A continuación se muestra una imagen de la distribución de los canales para ambos estándares, donde para garantizar la máxima utilización de las bandas suele ser habitual en despliegues industriales la utilización de canales no superpuestos (Petersen S. y Carlsen S., 2011):

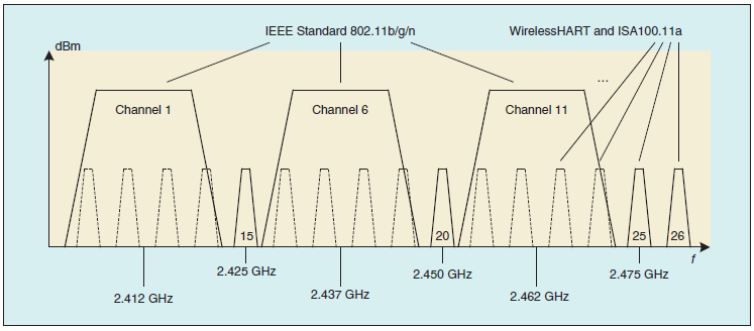


Figura 34: Distribución canales IEEE 802.11 y 802.15.4 en la banda 2.4 GHz

4.2.3 Capa de enlace de datos

En ISA100.11a la capa de enlace de datos se divide en subcapas MAC, una extensión MAC y una capa superior de encale de datos. La subcapa MAC es un subconjunto de la MAC del estándar 802.15.4, con la responsabilidad principal de enviar y recibir tramas de datos individuales. La extensión MAC incorporar mejoras adicionales que no son soportadas por el MAC del estándar IEEE 802.15.4, que tienen que ver sobre todo con mecanismos del protocolo Carrier Sense Multiple Access With Collission Avoidance (CSMA-CA), usado en el control de redes para evitar colisiones entre paquetes especialmente en redes Wireless, incluyéndole espacio adicional, frecuencia y diversidad te tiempo. Por otra parte, a diferenciad e WirlessHART y de la definición de la capa de enlace de datos definida por el modelo OSI, la capa superior de enlace de datos soportas aspectos de enlaces y malla por encima del nivel MAC, y es responsable del enrutamiento dentro de la subred de enlace de datos. Por lo que la responsabilidad del enrutamiento de la red en malla es de la capa de enlace de datos y esta capa está comprendida por uno más grupos de dispositivos de campo con un sistema compartido de administración y una red troncal. La subred de la capa de enlace de datos termina en el router troncal, pero el enrutamiento de la red se debe extender a lo largo de la red troncal y la red de planta. El enrutamiento dentro de la red troncal es responsabilidad de la capa de red.

Cada dispositivo que participa en la subred de la capa de enlace de datos se le asigna una dirección de subred corta de 16-b para una identificación local por el administrador del sistema. Para sostener el enrutamiento en malla, el protocolo soporta tanto algoritmos de enrutamiento gráfico como de origen. Donde una ruta origen, no es más que una ruta directa entre nodo de origen y destino, que define el camino especifico que debe tomar un paquete en la comunicación. Si esta ruta falla el paquete se pierde, mientras que mediante el enrutamiento gráfico, hay múltiples caminos por lo que por lo que podrá ser enviado el paquete.

Al igual que con WirelessHART el TDMA combinando con salto de frecuencia es usado para el acceso al canal, donde la comunicación es dividida en una matriz de dos dimensiones. Esta consiste en ranuras de tiempo y los 16 canales en el caso de ISA100.11a contando con el canal opcional 26 (15 en el caso de WirelessHART). Un grupo de ranuras de tiempo forma una supertrama, las cuales se repiten en tiempo a lo largo de toda la red. El termino trama se usa para separar en tiempo instancias consecutivas una supertrama. Las supertramas siempre deben estar activas y es posible que tengan longitud variable. Estas son gestionadas por el administrador de red y seguridad y pueden ser añadidas

o eliminadas por estos mientras la red este operacional. ISA100.11a permite configurar el valor de la ranura de tiempo por medio del administrador de red cuando un dispositivo se une a esta.

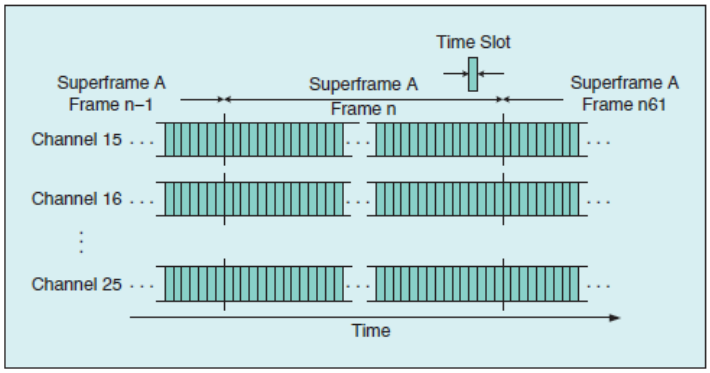


Figura 35: Estructura canales TDMA, ranuras de tiempo y supertramas

El administrador de red asigna dos dispositivos a un link, como transmisor y receptor, a excepción de los mensajes broadcast donde todos los recibidores son asignados a la misma ranura de tiempo. El enlace es especificado por una supertarma, el desplazamiento de la ranura de tiempo y el desplazamiento del canal. Donde en consecutivas supertramas un enlace siempre tendrá el mismo desplazamiento de ranura de tiempo, mientras el canal de comunicación cambiara según el patrón seudoaleatorio de saltos.

4.2.3.1 Formato de la Unidad de datos de protocolo (DPDU)

La trama en ISA100.11a es mucho más complicada que la de WirelessHART, además tiene un formato distinto. (WANG G., 2011):

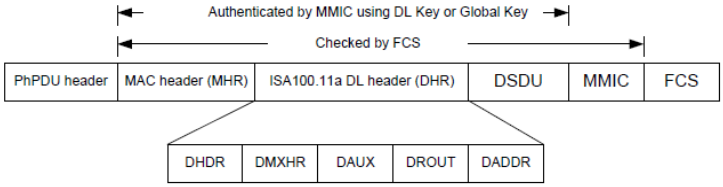


Figura 36: Formato trama ISA100.11a

- La cabecera PhPDU, la cabecera MAC y el campo Frame Check Sequence (FCS) son específicos como en el estándar IEEE 802.15.4. La capa de enlace de datos del ISA 100.11a adopta un subconjunto de MAC IEEE 802.15.4 como su MAC y extiende su Capa MAC con otras funcionalidades lógicas MAC que no están incluidas en la MAC IEEE 802.15.4.
- El DHR consiste en una serie de subcabeceras que resume funciones de la capa de enlace de datos, como por ejemplo, links, malla, aspectos de seguridad, etc.
- La campo DHDR (Data Link Layer header sub-header) contiene el número de versión de la Capa de enlace de datos y genera una selección de capas de acceso de datos como si el recibidor requiere de ACK o no.
- La campo DMXHR (Data Link Layer Media Access Control (MAC) Extension sub-header) contiene campos como control de seguridad e identificador clave que indica la opción de seguridad adoptada por la subcapa seguridad. El campo MMIC de 32, 64 o 128 bits según el

nivel de seguridad, como se muestra en la tabla, que es generado por la clave de la capa de enlace durante el proceso de validación para la autenticación de datos (integridad) debe ser lógicamente parte de DMXHR. El DMXHR también implementa campos adicionales que están incluidos en el estándar IEEE 802.15.4.

- La subcabecera DHR Auxiliary (DAUX) está solamente presente en anuncios dedicados o solicitación de mensajes.
- La subcabecera Routing (DROUT) ofrece información de enrutamiento a nivel de subred en términos de ID de Enrutamiento gráfico o ruta de origen, prioridad DPDU, etc.
- La subcabecera Address (DADDR) contiene el origen de la capa de red y direcciones de destino así como control explícito de congestión (ECN), Último Salto (LH), Descarte Elegible (DE) que son suministrador por una capa superior.

4.2.4 Capa de red

ISA100.11a utiliza 6LoWPAN (Ipv6 over Low Power Wireless Area Networks). El cual se encarga de la definición de la encapsulación y de los mecanismos de compresión para transportar paquetes Ipv6 a través redes Wireless IEEE 802.15.4 manteniéndolos conforme a los estándares existentes (WANG G., 2011). En una red ISA100.11a se pueden generar paquetes Ipv6 por parte de parejas cliente/servidor que son posteriormente reenviados a través de un Router perimétrico 6LoWPAN el cual adapta el formato de Ipv6 a 6LoWPAN, a dispositivos activos 6LoWPAN ISA100.11a. Bajo redes en malla, la cabecera de la capa de enlace contiene la información de enrutamiento de los paquetes basados en IP. En la capa de adaptación 6LoWPAN se lleva a cabo la fragmentación y re-ensamblado de los paquetes Ipv6 (Nixon M., 2012),

4.2.4.1 Formatos cabeceras Capa de Red

ISA100.11ª soporta hasta tres formatos diferentes de cabeceras NPDU, basadas en las consideraciones de ISA100.11ª define respecto al enrutamiento a nivel de subred en malla y red troncal, lo que requiere que los diferentes parámetros y requerimientos se adapten a los diferentes escenarios de enrutamiento, así como desde un punto de vista de eficiencia energética, donde el despliegue de una dirección de 16 bits en enrutamiento de subred consume mucha menos energía y ancho de banda que una dirección global de 128 bits (WANG G., 2011).

4.2.5 Capa de transporte

La capa de transporte en ISA100.11a a diferenciad de WirelessHART permite servicios en modo no conexión con seguridad opcional. Estos se basan en el protocolo User Datagram Protocol (UDP) con procesado opcional de seguridad usando clave de sesión. Cuando una sesión tiene que proveer encriptación y autenticación extremo a extremo entre dos dispositivos, esta se define al nivel de la capa de transporte en ISA100.11a, mientras que en WirelessHART se define a nivel de la capa de red (WANG G., 2011).

4.2.5.1 Formato de la Unidad de datos de protocolo (TPDU)

La TPDU tiene la siguiente forma en ISA100.11a (WANG G., 2011):

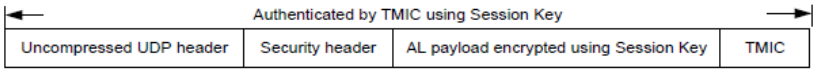


Figura 37: Formato TDPU en ISA100.11a

- Uncompressed UDP header: además de que debe ser descomprimida, requiere de un checksum UDP obligatorio por IPv6.
- Security header: contiene parámetros de control a nivel de seguridad.
- TMIC: se genera usando la clave de sesión para la autenticación de datos.

4.2.6 Capa aplicación

En ISA100.11a la capa de aplicación es orientada a objetos. La arquitectura está dividida en 2 subcapas:

- La capa de aplicación superior (UAL) que contiene aplicaciones de proceso para el dispositivo y puede ser usada para controlar hardware de entrada o salida, soporta tunneling o la realización de funciones calculo computacional.
- La subcapa de aplicación (ASL), la cual proporciona los servicios necesarios para que la UAL lleve a cabo sus funciones, como comunicación orientada a objetos y enrutamiento de objetos dentro de un proceso de aplicación de usuario (UAP) a través de la red (Petersen S. y Carlsen S., 2011).

Los dispositivos poden reportar estado y valores, incluso se garantiza la calidad de servicio requerido por la aplicación mediante la creación de contratos entre el sistema de administración y el dispositivo (Costa M. S. y Amaral J., 2012).

4.2.6.1 Formatos cabeceras Capa de Aplicación

El formato APDU en ISA100.11a se muestra a continuación:

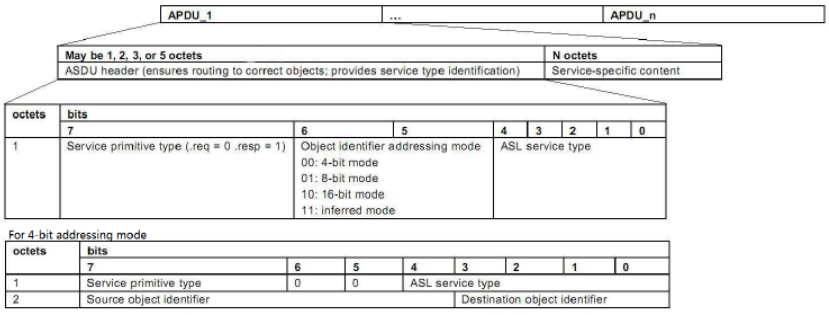


Figura 38: Formato ADPU en ISA100.11a

Como se puede observar, contiene información de identificador de objeto para el direccionamiento del mismo, el tipo de identificación de servicio específico que está ofreciendo la APDU.

4.2.7 Security WirelessHART e ISA100.11a

Se debe recordar que las redes Wireless son potencialmente susceptibles a ciberataques, esto es especialmente importante a tener en cuenta en la IACS. Por lo que las redes deben garantizar la confidencialidad de la información, la integridad y la autenticidad mediante la implantación adecuada de algoritmos y mecanismos de seguridad.

Tanto WirelessHART como ISA100.11a aplican protección de seguridad a través de encriptación de carga útil (payload) y autenticación de mensajes para mensajes de salto simple (hop-by-hop) y mensajes de extremo a extremo (end-to-end). En los dos, la protección de salto simple toma lugar en la capa de enlace de datos, mientras que la protección de mensajes extremo a extremo es llevada a cabo por la capa de red en WirelessHART y la capa de transporte en ISA100.11a. Mientras que la seguridad en la capa de red y transporte protege de posibles ataques en las rutas de la red entre el transmisor y receptor, la seguridad en la capa de enlace de datos defiende de posibles ataques desde fuera del sistema.

Ambos estándares soportan contadores con modos de operación para proveer seguridad a la información, confidencialidad y autenticidad como el cipher block chaining message authentication code (CCM)[11] en conjunto con el Estándar de Encriptación Avanzada (AES) 128 (Estándar con un bloque de tamaño de 128 bits) cifra bloques usando claves simétricas para la encriptación y autenticación de mensajes (Petersen S. y Carlsen S., 2011).

4.2.8 Modelos Clavisaje

En ambos estándares se definen un grupo de claves de seguridad. Los dispositivos nuevos que se quieren unir a la red deben conocer la clave de acceso a la red antes de unirse a esta. En ISA100.11a el uso de la calve de acceso es opcional, donde una clave global conocida puede también ser usada para el proceso de asociación a la red para dispositivos que no soportan claves simétricas.
Por otra parte WirelessHART, adicionalmente a la clave de acceso define sesiones y calves de red. La clave de sesión es usada por la capa de red para la autenticación de comunicaciones extremo a extremo entre dos dispositivos y es diferente por cada par de comunicaciones. La clave de red es usada por la capa de enlace de datos para autentificar mensajes en base a un salto (one-hop). La generación y administración de la clave es responsabilidad del administrador de seguridad y distribuida a los dispositivos de campo por el administrador de red.

En ISA100.11a, una vez se han unido a la red los dispositivos, se les suministra una clave maestra, un clave de capa de enlace de datos y una clave de sesión, si son soportadas por el dispositivo. Mediante la conexión del dispositivo y el administrador de seguridad se usa la calve master. La clave de la capa enlace es usada por la capa enlace de datos para procesar el message integrity code (MIC), y la clave de sesión es una clave opcional usada para encriptar y/o autenticar mensajes de la capa de transporte. Estas claves expiran en el tiempo y deben ser actualizadas periódicamente. Además de estas claves

[11] http://en.wikipedia.org/wiki/CCM_mode

simétricas, ISA100.11a también soporta claves opcionales asimétricas, donde las claves para encriptar y desencriptar el mensaje son diferentes. Cada dispositivo dispone de un par de claves, la pública y la privada. Mientras que la clave privada se mantiene en secreto la pública es publicada libremente. Los mensajes encriptados con la clave pública solo pueden ser desencriptados con la clave privada. Por lo tanto, cuando un dispositivo ISA100.11a se une a la red, debe usar o claves simétricas, claves públicas o no seguridad, donde en esta última se usa la calve global y el MIC será equivalente a una comprobación de redundancia cíclica (CRC) sin garantías de seguridad, por lo que para estos dispositivos la seguridad extremo a extremo no está permitida (Petersen S. y Carlsen S., 2011).

4.3 ISA100.11A vs WirelessHART

Entre las mayores diferencias que se pueden encontrar entre ambos estándares están directamente relacionadas con los objetivos de cada una. Mientras que WirelessHART está especialmente pensado para cubrir requerimientos que se han visto anteriormente en el sector industrial, como fiabilidad, seguridad, interoperabilidad, soporte para aplicaciones Clase 1 hasta Clase 5, etc. lo que lo hace Por otra parte, ISA100.11A, está diseñado para ofrecer flexibilidad, mediante la posibilidad poder personalizar el sistema operativo por parte de los fabricantes, una gran variedad de extensión de red disponibles y la compatibilidad con una amplia variedad de estándares de red (Nixon M., 2012).
A continuación mostramos una tabla comparativa centrada en el modelo de interconexión de sistemas abiertos (OSI) y la otra con las diferencias técnicas entre ambos.

Capas	WirelessHART	ISA 100.11a
Arquitectura	Puntos de Acceso. Dispositivos de campo (routers y E/S, routers).	Router troncal Dispositivos de campo (E/S, routers, y routers y E/S) Múltiples subredes QoS para comunicación dispositivos
Capa física	IEEE 802.15.4 2.4GHz DSSS radio.	IEEE 802.15.4 2.4GHz DSSS radio
Capa de enlace de datos	IEEE 802.15.4 con TDMA, Salto de canal (Channel hopping) y topología en malla. Tiempo ranura fijo. Propagación reloj. Seguridad: Integridad de datos hop-by-hop.	IEEE 802.15.4 con TDMA, Salto de canal (Channel hopping) y topología en malla. Tiempo ranura configurable Propagación reloj Seguridad: Integridad de datos hop-by-hop y encriptación Enrutamiento gráfico y origen Saltos lentos e híbridos (saltos lentos y rápidos) Asociación a la red (joining) con métodos simétricos y asimétricos
Capa MAC	Cumple con MAC 802.15.4-2006 MAC y los servicios MAC Enrutamiento gráfico y origen	Basada en una versión modificada que no cumple con MAC del estándar IEEE 802.15.4-2006

	Asociación a la red (joining) con métodos simétricos	
Capa de red	Basada en direccionamiento HART 16 y 64bits Enrutamiento gráfico y origen Seguridad: encriptación extremo a extreme e integridad de datos	Basada en direccionamiento IPv6 Compatible 6LoWPAN (IETF RFC4944) Direccionamiento de 16, 64 y 128 bits Fragmentación y re-ensamblado en el router troncal. 3 especificaciones de encabezado
Capa de transporte	Auto-segmented transfer of large data sets, reliable stream transport Solo una especificación de encabezado	Servicio UDP no orientado a conexión (IETF RFC768) Compatibilidad con 6LoWPAN Seguridad: encriptación extremo a extreme e integridad de datos
Capa de aplicación	Orientado a comando, tipos de datos predefinidos y soporta protocolo HART	Orientado a objeto, soporte protocolos (tunneling) heredados. 3 modelos de comunicación interactiva
Control Proceso	HART 7	No dispone
Administración	Diagnósticos Configuración centralizada de supertramas, enlaces y routers Asociación a la red	Diagnostico Configuración centralizada de supertramas, enlaces y routers Asociación a la red
Seguridad	Administración de clave Protección interferencia (blacklist, salto de canal) Claves de acceso son suministrada mediante dispositivo de mano Soporta claves simétricas AES-128 Las claves tienen tiempo de expiración	Administración de calve Protección interferencia (blacklist, salto de canal) Claves de acceso son suministradas usando over the air provisioning (OTAP). Soporta claves simétricas AES-128 Las claves tienen tiempo de expiración
Subcapa Aplicación	Estructura de comando y respuesta Codificación de datos Seguridad: Encriptación e integridad de datos	Estructura de servicios de objetos y métodos Codificación de datos

Tabla 6: Comparativa centrada en el modelo de interconexión de sistemas abiertos (OSI)

Como se ha comentado anteriormente aunque WirelessHART e ISA100.11a son muy simialres, entre las diferencias mas significativas que se pueden extrar de la anterior tabla son:

1. Sus arquitecturas tienen pequeñas diferencias, mientras que ISA100.11a utiliza routers troncales, WirelessHART usa puntos de acceso. ISA100.11a introduce el concepto de roles y permite a estos ser aplicados en diferentes combinaciones, mientras que WirelessHART extiende el protocolo HART con la introducción de nuevos dispositivos. En mi opinión, esto da

a WirelessHART una amplia ventaja sobre el ISA100.11a ya que HART ha sido el protocolo con más implantaciones hasta el momento en redes de campo y hace que las implantaciones desde el primer momento estén completamente integradas con la arquitectura. Además en el mercado se pueden encontrar sistemas que amplían la capacidad a los dispositivos de campo HART a WirelessHART con un simple adaptador inalámbrico evitando así el coste adquisición de nuevos dispositivos y conservando las mismas herramientas de administración y configuración a las existentes en los dispositivos cableados. Por otro lado, por ahora con ISA100.11a la integración no es completa, lo que reduce la funcionalidad de la red, en cuanto a la utilización de diagnósticos y configuración.

Otras de las diferencias que podemos encontrar a nivel de arquitectura es la limitación en cuanto a la asignación de direcciones existente en WirelessHART, limitada a 30K en una sola red, mientras que en ISA100.11a funciona muy bien en grandes redes ya que se basa en IPv6 lo que no tiene prácticamente limitaciones y le da la posibilidad de crear mediante routers troncales grandes extensiones de redes Wireless. ISA100.11a define como subnet a toda una red de campo, lo que hace significativa la escalabilidad del estándar pudiendo tener múltiples subnets con un total de 2^{16} dispositivos. No obstante en WirelessHART se pueden usar puntos de acceso en paralelo para unir subredes en un amplio espacio de direcciones.

Creo que es importante comentar que todo y que desde el punto de vista técnico ISA100.11a no tiene casi limites, según el artículo WirelessHART versus ISA100.11a escrito por STIG Petersen y Simon Carlsen en el año 2011, comenta que el número de dispositivos que se pueden sostener en una red es el mismo en ambos estándares, típicamente es de 50 a 100 dispositivos. Esto es debido principalmente a los problemas que conlleva en si la generación de tráfico, el cual es proporcional al ratio de actualización de la información de los dispositivos y el número de los mismos. Todo este tráfico pasa por los dispositivos más cercanos a los puntos de acceso o routers troncales, lo que en grandes redes esto puede ocasionar un alto grado de procesado en estos dispositivos disparando el consumo de las baterías. Por lo que en mi opinión, siempre se debe evaluar la forma de ajustar el ratio de actualización de los dispositivos a los requerimientos del proceso teniendo en cuenta que no desemboque en un problema, con el aumento del tráfico de red y en consecuencia en consumo de baterías.

2. Otras de las diferencias que se observan en la capa de enlace de datos, es que mientras en ISA100.11a se definen 3 variantes y patrones de salto de canal pre-definidos, aumentando así la fiabilidad evitando canales ocupados, WirelessHART incluye el definido por el estándar.
3. La capacidad de enrutamiento en los dispositivos, que en mi opinión incide directamente en la complejidad de diseño y despliegue de la red así como en el coste de la misma. Mientras que en WirelessHART se especifica que todos los dispositivos deben tener la capacidad de enrutamiento aunque luego se puede elegir si hacer uso de la mismo o no, en ISA100.11a el soporte de enrutamiento es opcional, dando a lugar a un mayor coste en el diseño, implementación y mantenimiento. Esto es debido a que si se va a disponer de una red con dispositivos sin enrutamiento, se debe realizar un diseño de la topología y un estudio de cobertura determinando donde irán ubicados los dispositivos con capacidad de enrutamiento

para garantizar que se cubren con suficiente señal todas las áreas que lo requieran. Esto obliga a llevar a cabo un control de compras y stock de recambios en la adquisición de dispositivos con enrutamiento y sin. Además, los dispositivos que no estén en modo enrutamiento no se adaptan a los cambios en los requerimientos de la red lo que compromete a un mantenimiento dedicado a estos en caso de cambios.

4. En seguridad, WirelessHART define que todas las comunicaciones deben ir encriptadas, mientras que ISA100.11a permite que las comunicaciones no sean encriptadas. Esto en mi opinión le da cierta ventaja a WirelessHART, en la IACS es muy importante la seguridad y para ello debe ser algo inherente en toda red industrial. Con la opción de que se puede aumentar o disminuir el grado de seguridad de la misma según requerimientos de la red o proceso, pero en ningún caso debería ser una opción, ya que la red podría verse gravemente comprometida por descuidos o errores en la configuración, falta de mantenimiento o problemas en la adquisición de dispositivos que no soportan comunicaciones seguras.
5. Las ranuras de tiempo (time slots) en WirelessHART son de 10ms, mientras que para ISA100.11a es configurable.
6. Mientras que ISA100.11a define diferentes formatos de cabeceras de capa de red que soportan IPv6 y formatos de cabeceras comprimidas, WirelessHART define solo una cabecera de red. Por lo que cuando se implanta cualquiera de ambos estándares se debe verificar que todos los dispositivos existentes en la red son compatibles, pero esto es más complejo cuando se trata de ISA100.11a ya que se debe verificar la compatibilidad con los diferentes formatos. Desde mi punto de vista, la implantación de cabeceras IP pueden tener la desventaja de que nuestras redes pasarían a ser vulnerables a muchos de los ataques basados en IP que a diario se dan, es uno de los motivos por los que muchos usuarios en el sector les preocupa el uso de cabeceras IP.
7. La fragmentación y reensamblado de mensajes se lleva a cabo en diferentes capas según el estándar, para el caso de WirelessHART este se desarrolla a nivel de la capa de aplicación y se lleva a cabo en cada dispositivo, mientras que en ISA100.11a se realiza a nivel de la capa de red y debe coordinarse entre en los routers troncales. La función de coordinación entre estos es algo que aún no está definido, y para que se pueda hacer uso de esta funcionalidad obliga a trabajar bajo los mismos tipos de routers troncales en la red. Desde mi punto de vista, hasta que esta funcionalidad no esté debidamente definida es una desventaja sobre WirelessHART, porque te obliga a estar ligado a un solo suministrador. En la IACS en cada proyecto o dependiendo del cliente se suele definir los suministradores homologados para cada área que estarán encargados de todo el suministro de dispositivos iniciales, soporte a la configuración y puesta en marcha. Por lo que muchos ingenieros podrían pensar que como es habitual el tener un solo suministrador, no debería ser una desventaja. Desde mi punto de vista en Wireless lo es, ya que depender de un solo suministrador, puede reducir el posible acceso y adaptación a nuestras tecnologías Wireless que puedan ser ofrecidas por otros suministradores que podrían aportar grandes beneficios a la red.

8. Otra diferencia entre ambos, es que mientras WirelessHART usa HART en su capa de aplicación, ISA100.11a no especifica una capa de aplicación como se ha visto anteriormente.
9. Comparando desde el punto de vista de la seguridad, se ha visto como ISA100.11a usa tanto claves simétricas como asimétricas, definiendo parcialmente Over the Air Provisioning (OTAP) que es un método de distribución a dispositivos de claves de encriptación, actualizaciones de software, configuración, etc. Esto en mi opinión, hace que el estándar ISA100.11a sea muy bueno para redes muy grandes, ya que facilita la administración de la misma. Por otro lado, WirelessHART soporta la función de bloque transferencia, lo que se deben hacer a través de dispositivos de mano, pero no especifica un método de transferencia sobe el aire (over-the-air).

   Otras de las ventajas que desde mi punto de vista hace que ISA100.11a vaya muy bien para redes muy grandes es la posibilidad de realizar el proceso de asociación a la red de los dispositivos mediante clave asimétrica, permitiendo al dispositivo integrarse por sí mismo en la red Wireless con únicamente la supervisión del sistema de seguridad, mientras que WirelessHART actualmente no soporta criptografía asimétrica.

Por último se va a mostrar una tabla con las caracterisiticas especificas que cubren las requerimientos que hemos comentado al principio del proyecto como fiablidada, determinismo, etc.

Característica	WirelessHART	ISA 100.11a
Topología	Malla, Estrella, Combinación Malla y Estrella	Malla, Estrella, Combinación Malla y Estrella
Seguridad - Encriptación	AES 128	AES 128
Supertrama	10ms	Configurable (10-12ms)
Acceso al canal	TDMA	TDMA/CSMA
Escalabilidad	Si	Si
Determinismo	Si	Si
Implementación	Desafiante	Desafiante
Severidad Fallos	Buena	Buena
Fiabilidad	Alta	Alta
Determinismo	Si	Si
Ambiente Operación (Robustez)	Buena	Buena
Cambio Canal RF	Si	Si
Lista negra canales	Si	Si
Calves	Simétricas	Simétricas y Asimétricas
Tiempo de vida bacteria	Buena	Buena
Interoperabilidad con otros sistemas	Si	Si

Tabla 7: Comparativa WirelessHART e ISA100.11a

Una vez vistas las principales diferencias entre WirelessHART e ISA100.11a, así como una tabla de características, finalizaremos el documento mediante una pequeña guía de diseño e implementación de una red WirelessHART. La elección de WirelessHART se debe principalmente a que WirelessHART gracias a HART, el cual ha sido líder en implantación en la IACS, disfruta de una cuota de mercado mucho mayor que ISA100.11a, con una amplia variedad de productos en el mercado. Algunos fabricantes que ofrecen Gateways WirelessHART ofrecen la posibilidad de ampliar la funcionabilidad de dispositivos existentes HART a WirelessHART, garantizando la máxima interoperabilidad a la red.

Por lo que respecta a ISA100.11a, aun siendo un estándar más flexible y pensado para un mayor abanico de aplicaciones, incluye cierta complejidad a la que en mi opinión los usuarios hoy en día tienen tendencia a huir y requiere de mayor atención a la hora de implementarlo. Además cuanta con un punto negativo desde mi punto de vista, que es que aun siendo interoperable con HART, los clientes e ingenieros suelen minimizar al máximo el número de estándares y suministradores en las plantas, y sobre todo siempre existe el miedo a la falta de apoyo por parte de los suministradores en cualquier momento a seguir trabajando en la interoperabilidad con otros sistemas.

Otro aspecto que hace que la balanza caiga sobre WirelessHART es como se ha comentado anteriormente, todos los dispositivos incluyen la opción de ruteo haciendo así que el diseño e implementación resulte más sencillo que con ISA100.11a.

Capítulo 5 Guía de implementación WirelessHART

A continuación se muestra cómo se cubre el diseño de una red WirelessHART en una planta de Hidrogeno en México, propiedad de PEMEX. Al cliente se le recomienda la implementación de WirelessHART por su compatibilidad con dispositivos existentes cableados HART, con el objetivo de reducir costes y ampliar la monitorización de aplicaciones no consideradas anteriormente por la inviabilidad del uso de cableado.

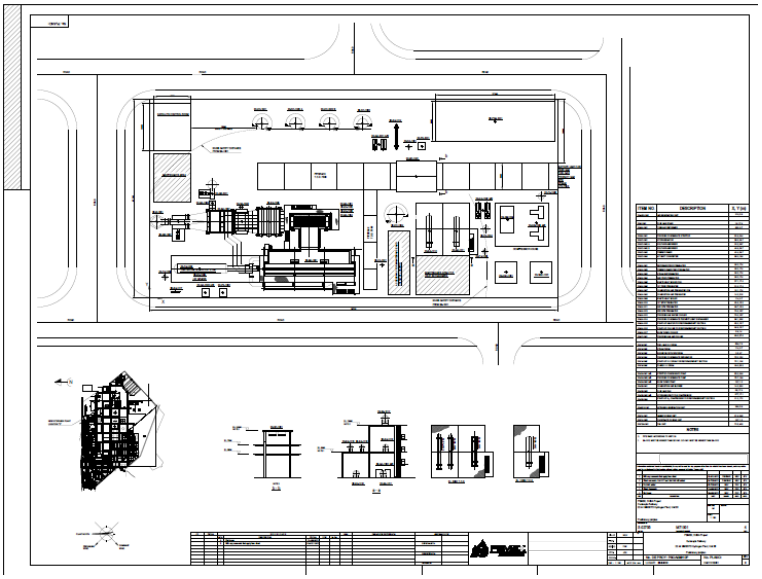


Figura 39: Plot Plan planta Hidrogeno

5.1 Antecedentes del proyecto Wireless

En todo proyecto Wireless, el primer paso es realizar un estudio de la aplicabilidad de tecnologías WirelessHART junto a otros protocolos como puede ser HART, Fundation Fieldbus y Profibus para cada uno de los procesos específicos del proyecto. Después, se define el alcance de implantación de WirelessHART, si se implementara en el control, principalmente en lazos abiertos donde haya intervención humana y la monitorización, junto con la definición de los tiempos de actualización, En este aspecto se debe considerar que a mayor ratio de actualización, menor vida de la batería. Una recomendación por mi parte es que para que los costes de mantenimiento de la planta se mantengan dentro de unos niveles aceptables, siempre que el dispositivo dependa de una batería, debemos considerar un ratio de actualización que permita que la duración de la batería sea lo máximo posible, preferiblemente años. Obviamente, este punto pierde su relevancia cuando los dispositivos son alimentados con fuente externa.

En un proyecto de mayor envergadura con dispositivos ya definidos, se establecerían los puntos que serán implementados mediante Wireless en base a criterios como: Económicos, aplicaciones que sean potenciales para el uso de Wireless, donde aporten ahorros operacionales, donde añadir mediciones no consideradas anteriormente que ofrezcan beneficios económicos o prácticos, como por ejemplo las duchas de seguridad y donde aporte beneficios en la ejecución del proyecto, como por ejemplo que

facilita el incluir o mover puntos de control o monitorización durante la construcción para manejar efectivamente el coste de cambios in-situ.

Por lo que respecta a la integración de la red WFN con la WPN es mediante conexión cableada del Gateway a Puntos de Acceso de la red de planta, la cual está última queda fuera del alcance de este proyecto.

5.2 Diseño Red Wireless de Campo

El proyecto habitualmente se aborda mediante tres fases, independiente del tipo al de industria al que vaya orientado o del suministrador que elija en cada proyecto en concreto, aunque puede que haya pequeñas variaciones según el tipo de estructura física que pueda interferir en las señales:

1. Definir la dimensión de las redes de campo por unidad de proceso o por subsección de proceso.
2. Una vez definido adecuadamente el alcance, se inicia el diseño de la red aplicando adecuadamente todas las reglas para garantizar una conectividad optima, así como cualquier directriz que puede haber por parte del cliente o para el proyecto en concreto.
3. Ya por último y muy importante, definir la seguridad adecuada para evitar cualquier vulnerabilidad.

5.2.1 Definiendo la dimensión:

Para poder definir la división de las redes, es muy importante fijarse en la estructura de la planta de procesado en la que se va implementar Wireless. Según la organización de la planta podemos diseñar la estructura de las diferentes redes de campo WirelessHART, para que se adapten a la estructura de la planta de proceso. Como se observa en el Plot Plan mostrado anteriormente, se aprecia que es una planta totalmente exterior, todo agrupado en una sola planta a nivel de suelo. Hay que tener en cuenta que si existen niveles, además del suelo, las redes Wireless se podrían estructurar por pisos. Como la planta está delimitada por carreteras, estas se toman como los límites para nuestras redes de campo Wireless, 92.74 x 45.28 metros.

Otro punto que también permite segmentar las redes Wireless por unidad de proceso, es el contar con un índice de Instrumentos del proceso, información que normalmente se encuentra disponible, no es el caso del presente proyecto. Con este, podemos determinar cuántos puntos de E/S pueden ser conectados vía Wireless. Vamos a suponer que tenemos contabilizados un total de 300 puntos E/S en el índice de instrumentos, y asumimos que del total de estos nuestra unidad de proceso va a tener 58 puntos Wireless, lo que se traduce en 58 dispositivos WirelessHART (distribuidos homogéneamente a lo largo de toda la unidad de proceso), sin considerar que algunos dispositivos WirelessHART puedan soportar más de un punto Wireless, como puede ser el caso de un Transmisor WirelessHART que puede tener input de 2 o más elementos de temperatura.

A continuación se define para cada uno de los dispositivos los ratios de actualización que van a requerir para cumplir con los requerimientos del proceso y de la duración de vida de la batería. Los ratios de actualización en los dispositivos WirelessHART van desde 1 segundo hasta los 60 minutos. Esto hace que WirelessHART no cumpla con los requisitos para el control de procesos donde se requieran tiempos de actualización por debajo de un segundo, como es el caso en las aplicaciones de seguridad y en control, principalmente en control con lazos cerrados, no obstante puede llegar a implementarse en ciertos casos. Se considera que el ratio de actualización debe ser de 3 a 4 veces más rápido que la constante de tiempo del proceso para monitorización y control con lazos abiertos, y de 4 a 10 veces más rápido para control regulado con lazo cerrado y en algún tipo de control de supervisión. A modo de ejemplo práctico, para la medición de cambios de temperatura un ratio de actualización típico son 16 segundos o mayor, debido a que es tres veces más rápido que la constante de tiempo que tarda en penetrar la temperatura el Termopozo (elemento protector del sensor), hasta el Termopar (sensor) (System Engineering Guide, Revision 3.0, May 2012). También es importante tener en cuenta que a mayor ratio de actualización, menor es la vida de la batería, un aspecto muy importante que hay que considerar. Si vemos la figura 1, con los 4 segundos tendrías en temperatura una duración aproximada de 4 años, contra los 2 años en presión. A modo de referencias, Emerson ofrece una aplicación web "**Emerson Power Module Life Estimator**"[12] donde se puede estimar la vida de la batería según el tipo de sensor Wireless, ratio de actualización y variable de entorno.

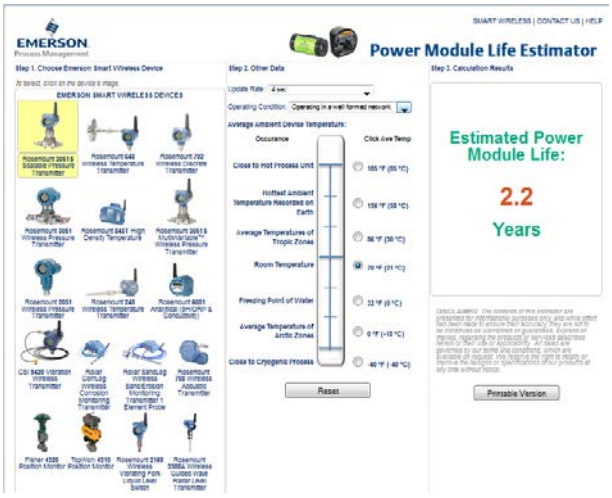


Figura 40: Aplicación web estimación baterías Emerson

Del mismo modo, ratios de actualización por debajo de 4 segundos pueden impactar en el número total de dispositivos que puede soportar un Gateway. Por lo que en este proyecto se define que los ratios de actualización van a ser de 4 a 60 segundos, y en el caso de que contase con un Índice de Instrumentos, indicaríamos en el los ratios de actualización para cada uno.

Una vez se conocen el número de dispositivos disponibles en la unidad de procesos y los ratios de actualización de cada uno, se determina la capacidad de los gateways mediante la situación más pesimista, que sería la de todos los dispositivos transmitiendo al mismo tiempo con un ratio de

[12] http://www3.emersonprocess.com/rosemount/PowerModuleLifeCalculator/Default.aspx

actualización de 4 segundos. Como nota, hoy en día hay en el mercado softwares como: AMS Wireless SNAP-ON, WiNCSim, WirelessHART Simulator que permiten simular las redes mediante diferentes ratios de actualización. Otro criterio importante a la hora de seleccionar los Gateways es el fabricante o suministrador. Es habitual en la industria del Petróleo y el Gas homogenizar los proveedores por ventajas en costes, suministro y soporte, por lo que puede ocurrir que el suministrador del Gateway coincida con el suministrador de los dispositivos Wireless. En este caso se supone que el cliente ha elegido por razones que no se van a detallar aquí, a Emerson, una de las empresas que está apostando muy fuerte en la tecnología Wireless. Emerson dispone de un Gateway con las siguientes características, tanto en antena incorporada como externa[13]:

- Update rate: User selectable 1, 2, 4, 8, 16, 32 second or 1 to 60 minutes
- Maximum Network Size
  - 100 wireless devices @ 8 sec or higher.
  - 50 wireless devices @ 4 sec.
  - 25 wireless devices @ 2 sec.
  - 12 wireless devices @ 1 sec.
- Output: Ethernet, EtherNet/IP™, Modbus TCP/IP, OPC, Serial, HART-IP
- Approvals: FM, ATEX, IECEx
- Radio Frequency Power Output from Antenna
  - Maximum of 10 mW (10 dBm) EIRP
  - Maximum of 40 mW (16 dBm) EIRP for WN2 High Gain option

En este caso elegimos el Gateway con antena externa, los cuales en mi opinión son mucho más versátiles y permiten adaptar el tipo y la potencia de la antena según requerimiento y necesidades. Por ejemplo, podríamos usar antenas direccionales o sectoriales para cubrir ciertas áreas específicas de la unidad de proceso, o usar antenas omnidireccionales de mayor potencia para ampliar el rango de cobertura.

Una vez elegido el Gateway se determina, teniendo en cuenta cualquier requerimiento por parte del cliente o de la misma empresa encargada del diseño, la reserva de capacidad, que servirá para calcular el número de Gateways que vamos a necesitar. Supondremos que el cliente exige una reserva de capacidad del 38%. Cuando ya se dispone de este dato, se procede a calcular el número de Gateway que serán necesarios para cubrir toda la unidad de proceso.

$$N^{o}Gateways = \left(\frac{Total\ dispositivos\ WirelessHART\ en\ la\ unidad\ de\ proceso}{Capacidad\ Gateway\ *(1-requerimientos\ reserva\ capacidad}\right) = \left(\frac{58}{50\ *(1-0.38)}\right) = 1.87$$

Redondeando se tiene que se deben instalar un total de 2 Gateways. Pero, en este proyecto se va a suponer que nuestro cliente exige que todos los Gateways sean redundantes, lo que se implementarán un total de 4 Gateways, estos se deben instalar de forma conjunta para que en caso de fallo de uno,

[13] http://www2.emersonprocess.com/siteadmincenter/PM%20Rosemount%20Documents/00813-0200-4420.pdf

el otro garantice la continuidad de la red dando cobertura a la misma área. Por lo tanto en cada ubicación que se defina, irán dos Gateways.

Llegado aquí, se define la ubicación de los Gateways en la unidad de proceso, definiendo secciones de la unidad de proceso lo más homogénea posible y centrando los Gateways lo máximo posible en la sección que van a cubrir. Esta distribución también se realiza considerando las limitaciones en número de dispositivos que pueden soportar los Gateways. Según las características del Gateway que hemos seleccionado para este proyecto, para ratios de actualización de 4 segundos soporta hasta un total de 50 dispositivos. Por lo tanto, con esta distribución, considerando que los dispositivos están distribuidos de forma uniforme, el Gateway no cubre más de $^{58}/_{2} = 29$ dispositivos. Se puede tener Gateways con mayor carga que otros, lo importante es no pasar los límites de cada uno. Para este proyecto la unidad de proceso se divide en 2 zonas de forma homogénea en vertical para minimizar la distancia a cubrir, 45.28 metros en vertical y $^{92.74}/_{2} = 46.37$ metros en horizontal. A continuación se estudiara mediante la cobertura efectiva de los dispositivos si esta distancia puede suponer un problema.

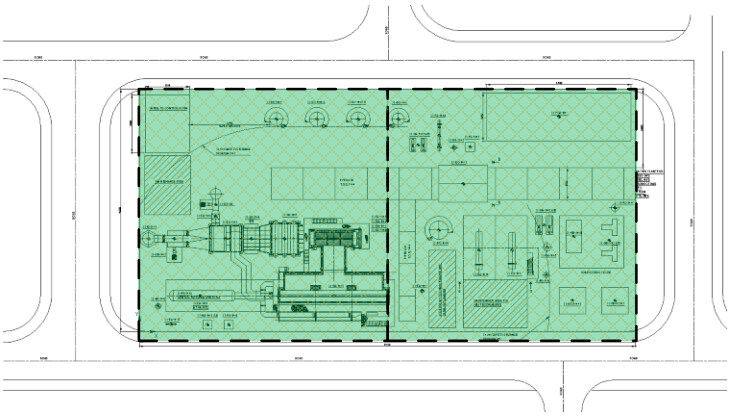


Figura 41: Plot Plan con el dimensionado de la planta

Es importante saber que el dimensionado es la regla más importante de diseño, esta se debe usar para garantizar la capacidad de la red Wireless, la escalabilidad a largo plazo, su fiabilidad y el alineamiento de los dispositivos WirelessHART con otros procesos en la planta, la organización o procedimientos.

5.2.2 Diseño:

A continuación se muestra la distancia de cobertura efectiva de los dispositivos de campo en base a datos reales y muy conservadores de otros proyectos de implementación WirelessHART en redes de campo, el alcance efectivo de los dispositivos. Este suele ser habitualmente lineal entre los dispositivos WirelessHART, cuando están implementados en infraestructuras de procesos. Típicamente, tienen una línea de visión clara sin obstrucciones entre ellos, y se suelen montar a una distancia de al menos 2 metros por encima del suelo, siempre por encima de cualquier instalación presente, como tuberías. La distancia de cobertura efectiva aproximada para una potencia de 10mW/10dBi es de 228 metros aunque las obstrucciones pueden reducir este alcance (System Engineering Guide Revision 3.0 May 2012). Como se he comentado a lo largo del trabajo, en la industria del petróleo y gas, la mayoría de los entornos de las unidades de proceso tienen una alta concentración de metales que reflectan la

señal de radio frecuencia de una forma impredecible, haciendo rebotar esta contra otros metales alrededor. A continuación se muestra una clasificación de la distancia de cobertura efectiva en función de los ambientes de procesos:

Obstrucción	Ambiente	Cobertura efectiva (metros)
Fuerte	Plantas con áreas muy densas	30
Media	Plantas con áreas ligeras con espacio entre equipos e infraestructura	76
Ligera	Plantas con áreas muy ligeras como campos de tanques con grandes espacios	152
Nula (Línea Visión Clara)	Antena por encima de obstrucciones y el ángulo del terreno cambia por debajo de los 5 grados	228

Es importante saber que si los dispositivos se instalan cerca del suelo la señal no se va a propagar. Como se observa en el Plot Plan, se puede considerar que en la planta de hidrogeno se dispone de un nivel de obstrucción medio, con espacios entre los equipos y la infraestructura, por lo que se obtendrán distancias efectivas de cobertura de hasta 76 metros. Así que con el tamaño de las dos secciones a cubrir de 45.28 x 46.37 metros, no se tendrá mayor problema en la distribución.

Figura 42: Plot Plan con ubicación Gateways con huellas

Para obtener una mayor garantía en la red en malla respecto a la cobertura efectiva, siempre se deben considerar las siguientes 3 reglas:

1. La regla de 5 mínimo: Cada red Wireless de campo debe tener al menos 5 dispositivos WirelessHART dentro de la distancia de cobertura efectiva del Gateway, para que funcione adecuadamente y de este modo aproveche la ventaja de la redundancia intrínseca de la auto-organización de una red en malla. Para cumplir esta regla, podemos hacer uso de repetidores.
2. Cada dispositivo debe tener un mínimo de 3 dispositivos dentro de su distancia de cobertura efectiva. En el caso de que en algún momento no se cumpla la regla, debemos re-analizar para añadir más dispositivos de medida WirelessHART.

3. En una red con más de 5 dispositivos, aunque se ha comprobado que puede trabajar con el Gateway teniendo dentro de su cobertura efectiva el 10% de los dispositivos WirelessHART, se recomienda que debe tener dentro de su rango de cobertura efectiva como mínimo el 25% de los dispositivos para optimizar el ancho de banda y eliminar los puntos muertos o sombras. Del mismo modo, si disponemos de dispositivos WirelessHART con ratios de actualización por debajo de los 2 segundos, este porcentaje se aumenta al 50%, para maximizar el tiempo de respuesta en aplicaciones que requieran velocidades altas de respuesta.

Si se observa la red, se puede ver en rojo como se está vulnerando la regla 2 de un mínimo de 3 dispositivos dentro de la cobertura efectiva de cada dispositivo, al mismo tiempo se ve en naranja otra que puede causar algún problema, y en verde donde se cumple adecuadamente.

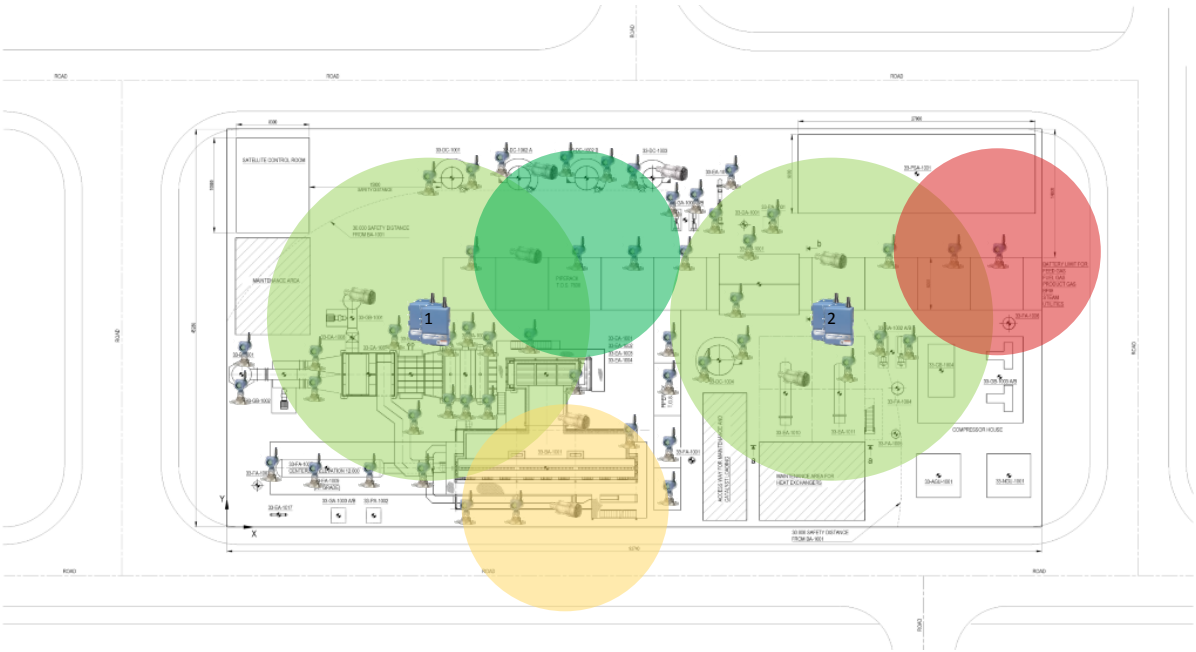


Figura 43: Plot Plan con estudio de cobertura efectiva

Para solucionar este problema, se deben incluir más dispositivos WirelessHART o repetidores al proceso, de este modo ampliar la cobertura efectiva y evitar obstáculos. En este caso en concreto se van a usar repetidores para solucionar el problema en la huella roja y en la huella naranja, ya que si se realiza una prueba de estrés en la huella naranja reduciendo la cobertura efectiva un 15% se rompe la regla. Por ejemplo, considerando que el proyecto está basado en una obstrucción media con una cobertura efectiva de 76m, con un estrés de del 15% se realiza el mismo estudio mediante una cobertura efectiva con 11 metros menos, lo que equivale a una huella de 65 metros, por lo tanto, en este dispositivo se rompe la regla número 3, en consecuencia se incluyen dos repetidores en cada uno de las áreas para garantizar la conectividad. Estas pruebas son totalmente recomendables y se deben poner en práctica en cada proyecto, ya que son realmente efectivas para identificar debilidades potenciales en el diseño de la red. Por lo tanto, el diseño quedaría así:

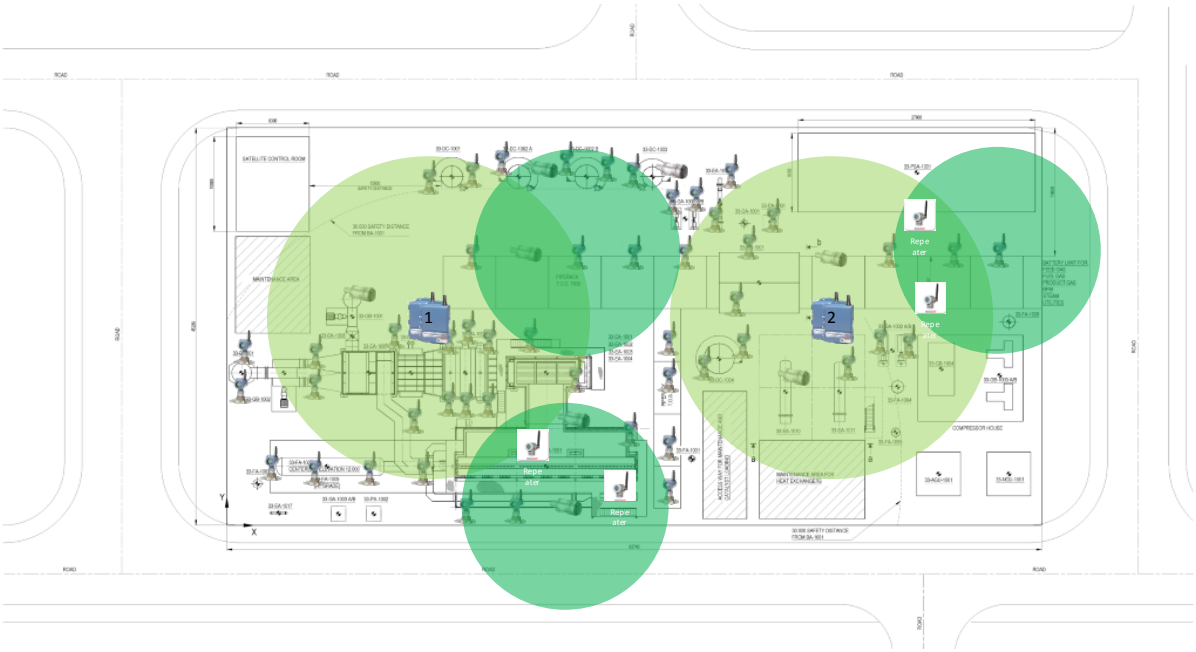


Figura 44: Plot Plan con repetidores

Hay que tener en cuenta que a mayor tamaño del proyecto, más irrelevantes son las reglas 1 y 2 por la gran cantidad de dispositivos que dispondrá la unidad de proceso, en este caso, como todos los instrumentos están concentrados, también se vuelven casi irrelevantes. En cambio la regla del porcentaje se vuelve de gran transcendencia. En este proyecto, el Gateway 1 está soportando 17 dispositivos WirelessHART dentro de su cobertura efectiva, de un total aproximado de 29 dispositivos WirelessHART, hay que tener en cuenta que hablamos de un valor aproximado porque no tenemos los datos procedentes del Índice de instrumentos, por lo tanto significa un 59 %, porcentaje muy por encima del 25% que pide la regla del porcentaje, y del mismo modo estamos cumpliendo la regla 1 de los 5 dispositivos. Por otro lado el Gateway 2, está soportando 13 dispositivos aproximadamente, lo que significa un 45%, respetando debidamente la regla 3 del porcentaje y la regla 1 de los 5 dispositivos.

5.2.3 Seguridad

Cada Gateway dispone de una identificación HART (HART Tag) como la pueda tener otro dispositivo HART, y este gestiona su propia red de campo que llevara un único identificador (Network ID) el cual es usado por los dispositivos para conectarse a la de red de campo correcta y evitar conexiones a otras redes colindantes. A parte de este identificador, se debe definir si se implementará una clave de acceso conjunta para todos los dispositivos de una red de campo específica o una clave única para cada dispositivo de campo. Estos dos parámetros componen la identificación y autenticación completa del dispositivo de campo. En mi opinión, aunque puede que haya quien recomienda una clave única para cada dispositivo dado el alto nivel que aporta. Para tamaños pequeños de redes de campo esto puede que no acarree mayor problema en la implementación, gestión y mantenimiento de la seguridad, pero para medianas y grandes redes, puede que el remedio sea peor que la enfermedad y convertirse en un problema de mayor nivel del que podría suponer un menor grado de seguridad. Esto conllevaría tener que gestionar un gran número de claves, obligando a tener que almacenarlas en una base de

datos, algo que sería una fuente de vulnerabilidades de seguridad si no se toman las medidas de seguridad adecuadas en el almacenamiento de la información. Del mismo modo, aporta una complejidad muy alta a la implementación de la red, aumenta la posibilidad de problemas de asociación a la red y puede disparar los costes de mantenimiento.

Por lo que respecta al proyecto, se ha elegido una clave compartida que cumpla con unos requerimientos mínimos, como los que se pueden exigir en las contraseñas para servidores o sistemas críticos como el DCS, aportando el mismo nivel de efectividad.

Parámetros	Opciones parámetros	Ejemplos	Detalles Técnicos
Gateway HART TAG	Campo	UNIT_H_G1	32 caracteres - ISO Latin-1 (ISO 8859-1).
ID de red	Entero	01459	Entero entre 0 y 36863
Clave de acceso	AES-128	X48FaCSpnWiEQiSEV0qYzg	claves simétricas AES-128

Tabla 8: Ejemplos parámetros configuración red campo WirelessHART

Por lo que, como recomendación sería conveniente siempre adaptar el nivel de seguridad de forma que esta no se convierta en un problema.

5.2.4 Sistema central (Host System)

Por último, puede que toda la información que se genera en la red de campo WirelessHART no tiene que ser enviada al sistema de control o a los sistemas PLC's. Puede que tengamos aplicaciones Wireless que no sean de control o monitorización y generen información que se quiera almacenar en un sistema centralizado como por ejemplo almacenar un historial de vibración de equipos con motor rotativo en un sistema Bently Nevada14, así como la temperatura de los mismos. O puede ser que se quiera almacenar toda la información generada en las redes de campo en un sistema captura, procesado, analizado y almacenamiento de datos. Para permitir esta interoperabilidad en este proyecto, se diseña la siguiente arquitectura:

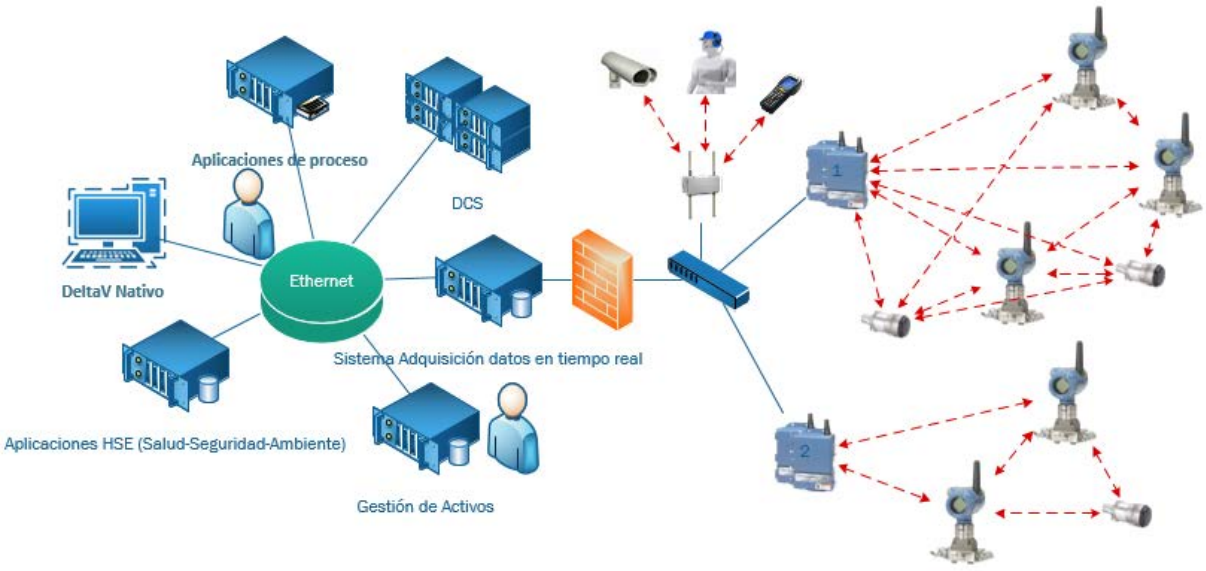


Figura 45: Arquitectura centralizada red WirelessHART Planta Hidrogeno

[14] http://www.ge-mcs.com/en/bently-nevada.html

Esta arquitectura centralizada integra la WFN WirelessHART con el sistema central y con la WPN. Esta arquitectura ofrece un alto nivel de escalabilidad a largo plazo. Permite agregar tantas redes de campo como sean necesarias e integrarlas inmediatamente a los sistemas conectados a la misma red mediante Ethernet. Con esta arquitectura se envía la información al sistema de captura, procesado, analizado y almacenamiento de datos en tiempo real (por ejemplo, OSIsoft PI[15]), y este está conectado a cada uno de los sistemas de los usuarios finales que hacen uso de la información que requieran. La integración de la información originada en la red de campo por los dispositivos Wireless al sistema central de control se realiza mediante el uso de estándares abiertos como Modbus u OPC.

Conclusión

En conclusión, una vez hemos finalizado el proyecto hemos podido analizar como las redes Wireless se enfrentan a problemáticas tanto inherentes a sus propiedades, incluso como puede verse afectadas en un futuro por una mala gestión por parte de políticos y organismos encargados de la distribución del espectro. A esto, hemos comprobado como sufre por parte de muchos usuarios finales e ingenieros la falta de confiabilidad motivada principalmente por desconocimiento de la tecnología, lo que está frenando que estas se consolide plenamente en el sector industrial, especialmente en la IACS y lleguen a niveles de implementación como los de la tecnología Wireless en el sector comercial. La falta de confiabilidad también viene motivado por las características actuales de la misma que no permiten que a día de hoy pueda ser implementada como hemos visto en el proyecto en todo tipo de aplicaciones en el sector de la IACS, orientándose principalmente al control con lazos abiertos y la monitorización, lo que reduce bastante su ámbito de aplicación. No obstante, cabe destacar que también está aportando grandes ventajas como el ahorro de costes, mediante la reducción de ingeniería y de mano de obra, ya que reduce elementos como cableados, racks, bandejas de cables y cabinas, elementos que suponen un coste significativo en proyecto de procesos industriales, adicionalmente el factor más importante y que debe tomarse en cuenta es la reducción en el tiempo de ejecución del proyecto. Así como no menos importante, ha abierto el ámbito de oportunidades de aplicación de la monitorización a aplicaciones que ni siquiera antes se consideraban por la complejidad o coste, que suponía implantar estos sistemas mediante cableado. Estas problemáticas seguro que a medida que la tecnología Wireless mejore tecnológicamente y siempre que se diseñen las redes definiendo correctamente la dimensión y alcance de la red Wireless, se podrá comprobar adecuadamente que el diseño supera todas pruebas pertinentes de estrés para prevenir cualquier situación, las cuales pueden vulnerar la comunicación y en consecuencia el buen funcionamiento de la planta. Con todo lo explicado anteriormente se garantizara el éxito de implementación y no se añadirá más desconfianza. De esta forma se irá cubriendo holgadamente los requisitos de las redes Wireless industriales y llegara a la confiabilidad requerida para ser el modelo de comunicaciones preferente en redes industriales en la IACS.

A través de este estudio hemos podido comprobar cómo dentro de los estándares Wireless, los que

[15] http://www.osisoft.com/

mejor se ajustan a los requerimientos en las redes industriales son el WirelessHART e ISA100.11a, desarrollados específicamente para estos entornos, debido a la falta de estándares que cumpliesen con la mayoría de los requisitos exigidos en la industria. Hemos visto como ISA100.11a, ofreciendo una mayor flexibilidad con un gran abanico de soluciones para la automatización de procesos, como el ratio de actualización ajustable, la minimización de la latencia de la red malla mediante la red troncal, QoS, la estructura mediante subnets que le ofrecen una gran escalabilidad, las claves asíncronas que permiten la asociación automática a la red, compatibilidad IPv6, etc. WirelessHART está siendo líder del Mercado. Al estar basado en HART, tiene la versatilidad de poder aprovechar los más de 28 millones[16] de dispositivos HART en el mundo adaptándolos a WirelessHART, evitando así mayores cambios en las estructuras existentes. Hemos visto como ambos estándares siendo similares en algunas características como la capa física, la longitud de la ranura de tiempo, tienen sus diferencias como se mostraba en la tabla. Cabe mencionar que parece ser posible la integración de ambos equipando al dispositivo una pila de doble protocolo sobre la capa de control de acceso al medio, de esta forma el dispositivo entendería ambos estándares, lo que en ese caso desde mi punto de vista podría darle ventaja a ISA100.11a por sus características comentadas anteriormente que lo hacen más flexible e indicado para redes de mediano y gran tamaño (WANG G., 2011). Por último, hemos visto como diseñar una red WirelessHART con guías y reglas que son aplicables para cualquier tipo de red industrial. En esta hemos podido ver las ventajas que ofrece la red en malla como la fiabilidad, la redundancia, etc. Es muy importante recordar que hay que definir adecuadamente el alcance de las redes de campo para que podamos llegar un buen diseño siguiendo todas las directrices por parte de los clientes y reglas para garantizar que la red va a disponer de una conectividad optima, en el sector industrial sobre todo en el sector del Petróleo y del Gas es muy importante la redundancia para garantizar la continuidad de la red y por último analizar adecuadamente la seguridad que se va a aplicar para evitar vulnerabilidades y sobre todo ajustarla a un nivel razonable, para que sea totalmente gestionable y se convierta en un problema por sí misma. En un proyecto Wireless industriales es muy importante realizar todas las pruebas necesarias para verificar posibles causas que pueden afectar al funcionamiento de la red.

Por último, comentar que este trabajo se eligió basarlo en redes Wireless industriales con la idea de poder cubrir todas las fases de los proyectos, pero en dos fases, esta sería la primera de en la que se ha intentado conseguir el objetivo de plasmar desde aspectos básicos hasta el diseño de la red, quedando para un futuro trabajo el profundizar en aspectos como la más relacionado con la implementación, configuración y puesta en marcha. Profundizando en temas como la integración e interoperabilidad con los sistemas centrales, la configuración, las pruebas FAT (Factory Acceptance Testing), alertas y mantenimiento, documentación, etc.
Por otro lado es importante comentar, que se ha podido comprobar el potencial que aportan las comunicaciones Wireless al sector industrial en especial a la IACS, le garantiza un futuro prometedor.

[16] http://de.hartcomm.org/protocol/about/faq.html

Referencias:

Alexfeng (2013), *Advantage of TDMA in WirelessHART over CSMA,* WirelessHART Blog, obtenida el 30 de Mayo de 2014, http://www.awiatech.com/advantage-of-tdma-in-wirelesshart-over-csma/.

Boyes, Walt (2010). *Instrumentation Reference Book (4th Edition).* Elsevier. [Versión electrónica]. *obtenida el 30 de Mayo de 2014,* Disponible en Knovel.com http://app.knovel.com/hotlink/toc/id:kpIRBE0016/instrumentation-reference

Caro R. H., (2008). *Wireless Networks for Industrial Automation 3rd Edition,* [versión electrónica] CMC Associates, EE.UU.

Chen D., Nixon M., Mok A., (2010). *WirelessHART Real-Time Network for Industrial Automation*, Editorial Springer New York Dordrecht Heidelberg London.

Costa M. S. y Amaral J. (2012), *Web Exclusive: Analysis of wireless industrial automation standards: ISA-100.11a and WirelessHART,* InTech magazine, November/December 2012, Copyright © 2012 ISA.

Deal W., Qian, T., Radisc V. (1999), *Planar Integrated Antenna Technology*., obtenida el 19 de Mayo de 2014, Microwave Jornal, http://www.microwavejournal.com/articles/2677-planar-integrated-antenna-technology)

Emerson Process Management (2011), *Wireless Security Wireless HART® and Wi-Fi Security*, [versión electrónica, Texas EE.UU. obtenida el 5 de Junio de 2014 http://www2.emersonprocess.com/siteadmincenter/PM%20Central%20Web%20Documents/Emerson%20Wireless%20Security.pdf

Flammini, A et al 2008, *"Wired and wireless sensor networks for industrial applications",* Elsevier, Microelectronics Journal , Volume 40, Issue 9, Sep 2009, Pages 1322-1336.

Forgue, B. (2010), *Next-Gen Wireless in Control Systems, Going Wireless: Why and How?,* 23rd February [Presentation]: IET London: Savoy Place, UK.

Galloway B. y Hanke G. P. (2012), *Introduction to Industrial Control Networks*, [versión electrónica] University of Pretoria, Sud África, *obtenida el 30 de Mayo de 2014*.

Gómez B. E. (n.d.), *Conceptes bàsics Xarxes de distribució i radiodifusió,* Universitat Oberta de Catalunya UOC, Barcelona.

Hatler M. (2012) *Industrial Wireless Sensor Networks: Trends and developments*, InTech magazine, September/October 2012. Copyright © 2012 ISA.

HyperPhysics (n.d.), *Inverse Square Law, Light*, EE.UU. http://hyperphysics.phy-astr.gsu.edu/hbase/vision/isql.html)

International Society of Automation (2011), *ISA-TR100.14.01-2011 Trustworthiness in Wireless Industrial Automation: Part I – Information for End Users and Regulators*, Copyright International Society of Automation Provided by IHS under license with ISA Licensee=Fluor Corp no FPPPV per administrator /2110503106.

Ikram W., Thornhill N. F. (2010), *Wireless Communication in Process Automation: A Survey of Opportunities*, Requirements, Concerns and Challenges, Imperial College London, UK.

Kaufman D. R., (2010). *Industrial Wireless Technology and Planning,* capitulo 20, [versión electrónica]. *obtenida el 30 de Mayo de 2014,* Disponible en Knovel.com

Londoño J. (2009), *Diagrama de radiación (Patrón de radiación),* obtenida el 10 de Mayo de 2014, http://jhonatanlondon.blogspot.com.es/

Mishr U., York R. (2001), *Fundamental Properties of Antennas* , obtenida el 10 de Mayo de 2014, University of California in Santa Barbara, *obtenida el 10 de Mayo de 2014,* http://my.ece.ucsb.edu/York/Bobsclass/201C/Handouts/Chap3.pdf

Nannegari M., Brans T. Wireless (2006)*, Transmitters in Refinery: A Case Study & Promises to Keep,* [presentación electronica]. Fluor Enterprises, Inc. and Emerson Global Users Exchange.

Nixon M. (2012), *A Comparison of WirelessHART™ and ISA100.11a*,[versión electrónica] Texas, EE.UU.

Padilla J.J. (n.d.), ISA SP 100 y Wireless HART, [presentación electrónica] PHD.

PEPPERL+FUCHS (2012). *Wireless Technology - an Overview* [versión electrónica].Ottawa: National Library of Canada.

Petersen S. y Carlsen S. (2011), *Wirelesshart Versus ISA100.11a*, IEEE Industrial Electronics Magazine, Digital Object Identifier 10.1109/MIE.2011.943023, Noruega.

Radmand P., Talevski A., Petersen S. y Carlsen S. (2010), *Comparison of Industrial WSN Standards*, DEBII, Curtin University of Technology, Perth, Australia.

Salgado J. R. (2014), *Presentación Redes Wireless de Campo*, [presentación electrónica].FLUOR, Emerson Process Management.

Schultz, S. (2007), *"Wireless Goes Process Automation – Challenges in Hazardous Areas"* [versión electrónica], obtenida el 30 de Mayo de 2014, Germany.

Sikora, A., *Wireless for Industrial and Process Automation-Trends, Challenges, and Protocol*, obtenida el 13 de mayo del 2014, http://www.baloerrach.de

Swain F. (2013). *Will we ever... face a wireless 'spectrum crunch'?,* obtenida el 15 de Mayo de 2014, http://www.bbc.com/future/story/20131014-are-we-headed-for-wireless-chaos.

United States Department of Commerce (2011) *United States radio spectrum frequency allocations chart as of 2011*, obtenida el 20 de Mayo de 2014, EE.UU. http://www.ntia.doc.gov/files/ntia/publications/spectrum_wall_chart_aug2011.pdf

Universidad Nacional de Colombia (n.d), *ANTENA YAGI-UDA*. Obtenida el 19 de Mayo de 2014, http://www.virtual.unal.edu.co/cursos/sedes/manizales/4040050/Descargas/capseis/yagiuda.pdf

WANG G. (2011), *Comparison and Evaluation of Industrial Wireless Sensor Network Standards* ISA100.11a and WirelessHART, Chalmers University of Technology, Gothenburg, Sweden.

Wikipedia, the free encyclopedia (2014), *Spread spectrum,* obtenida el 15 de Marzo de 2014, http://en.wikipedia.org/wiki/Spread_spectrum.

Wikipedia, the free encyclopedia (2012), *File:Electromagnetic spectrum-es.svg,* obtenida el 20 de Febrero de 2014, http://commons.wikimedia.org/wiki/File:Electromagnetic_spectrum-es.svg

Wikipedia, the free encyclopedia (2014), Radio wave, obtenida el 17 de Marzo de 2014, http://en.wikipedia.org/wiki/Radio_wave

Wikipedia, the free encyclopedia (2014), *Radio spectrum,* obtenida el 10 de Febrero del 2014, http://en.wikipedia.org/wiki/Radio_spectrum

Wikipedia, the free encyclopedia (2014), *Radio propagation,* obtenida el 15 de Mayo de 2014, http://en.wikipedia.org/wiki/Radio_propagation

WNI México S.A. de C.V.(n.d.), *Tipos de Antenas y Funcionamiento*, obtenida el 10 de Mayo de *2014,* http://www.wni.mx/index.php?option=com_content&view=article&id=62:antenassoporte&catid=31:general&Itemid=79

Lista de Tablas

Lista de Gráficos