DISEÑO Y PLANEACIÓN DE LA ARQUITECTURA DE RED RADIO/WIRELESS INDUSTRIAL PARA LA AUTOMATIZACIÓN DE DOS PLANTAS REMOTAS

ANEXOS

RUBEN DARIO ESCOBAR LEDEZMA
CESAR AUGUSTO GOMEZ SANDOVAL

UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
PROGRAMA DE INGENIERIA EN AUTOMÁTICA INDUSTRIAL
Departamento de Instrumentación y Control
Popayán
2010

ANEXO A. TEORÍA DE RF

1. TRANSMISIÓN Y GENERACIÓN DE RF

1.1 Transmisión de RF

La generación de una señal RF es labor del trasmisor, el cual está constituido por un conjunto de elementos cada uno de los cuales cumple una función específica, sus componentes principales se muestran en la Figura 1 (1).

Transmisores con frecuencias de 2,4 GHz (utilizada por la norma IEEE 802.11) pueden oscilar normalmente entre 30 m, o 100 m aproximadamente (en interiores o exteriores) con antenas omnidireccionales.

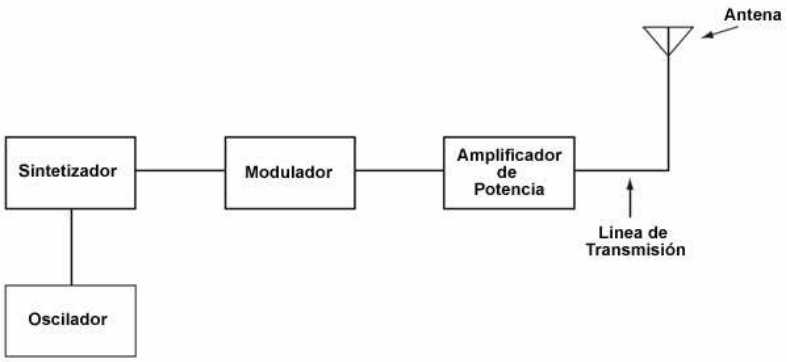

Figura 1. Diagrama en bloques de un transmisor

Oscilador: Lo primero que se debe realizar para generar una señal RF es producir la señal base a la frecuencia de operación deseada, esta es la labor del oscilador, o en los radios modernos, el sintetizador de frecuencia. El oscilador funciona bajo los conceptos de amplificación, realimentación y resonancia, básicamente es un amplificador en el cual parte de la señal de salida realimenta la entrada del sistema, esto es conocido como realimentación positiva. Si el acoplamiento de la entrada con la salida es continuo, el amplificador se estabilizará a la frecuencia de resonancia de los componentes que conforman el amplificador y el lazo de realimentación.

Amplificador de potencia: El objetivo de este módulo es producir una imagen de alta potencia de la señal presente en su entrada. El amplificador toma la señal de baja potencia producida por el oscilador, y aumenta su potencia a un nivel que permita la transmisión de la energía RF a lo largo del trayecto entre el transmisor y el receptor.

Las características principales de un amplificador son la potencia de salida, linealidad y la eficiencia. La potencia de salida se mide en *watts*; la linealidad, se define como los parámetros operativos del dispositivo que dan como resultado una relación lineal de ganancia entre la señal de entrada y la de salida; la eficiencia, es la relación entre la potencia de salida y la potencia total de entrada, este valor es por lo general expresado como un porcentaje.

Antenas y líneas de Transmisión: La antena normalmente se conecta al transmisor o receptor mediante un cable coaxial, conocido como línea de transmisión, el cual dentro del argot utilizado en las instalaciones de sistemas como WiFi, se denomina *pigtail.* Este medio, es mucho más que un simple pedazo de cable, está constituido por cuatro elementos, cada uno de los cuales tiene un efecto en las características de impedancia y pérdidas de la línea. Estos cuatro elementos son el centro conductor, el dieléctrico, el conductor externo y la cubierta.

Cuando se trabaja con dispositivos de radio, los cables coaxiales más utilizados son los de 50 o 75 ohm de impedancia. Tener en cuenta este valor es muy importante pues la selección del cable con la impedancia adecuada es vital para lograr una correcta adaptación entre la antena y el radio. Esto se debe a que la energía fluye con la menor atenuación cuando la impedancia de los elementos que atraviesa son iguales, una incongruencia en este factor provocaría que la energía se reflejara desde la carga hacia su fuente, siendo disipada en forma de calor, pero dado que el calor no es energía RF, cada porción de energía reflejada seria desperdiciada.

La radiación de las antenas puede ser no direccional o direccional. En general, las antenas direccionales alcanzar mayores rangos de transmisión, sin embargo, este no es el efecto de una mayor potencia de transmisión, pero si el resultado de la forma del campo de la radio.

- **Antenas Omnidireccionales**

Las antenas omnidireccionales o no direccionales, siempre tienen la forma de una varilla o un alambre recto. El término es engañoso en la medida en que la intensidad de la radiación no es igual en todas las direcciones. El campo de radio llega a la intensidad máxima en un plano a un ángulo recto con el eje de la antena como se ve en la Figura 2 (2). La intensidad del campo disminuye rápidamente por encima y por debajo del ángulo de apertura vertical de este plano y tampoco se puede esperar la señal verticalmente por encima y por debajo de la antena.

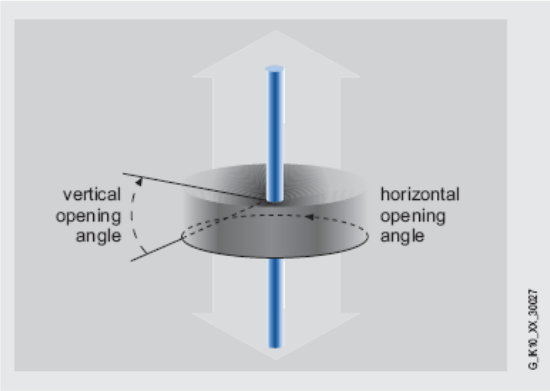

Figura 2. Patrón de radiación de una antena omnidireccional

El campo emitido es radialmente simétrico, lo que significa que la intensidad del campo es igual en todas las direcciones cuando se ven desde arriba a lo largo del eje de la antena. En este caso, el ángulo de apertura horizontal es de 360 ° grados.

- **Antenas direccionales**

Las antenas direccionales, normalmente tienen la forma de una caja plana, generan un campo de radio en la forma de un cono en ángulo recto a la caja. El cono se define por un ángulo de apertura horizontal y vertical, fuera de este punto la intensidad disminuye rápidamente, en la Figura 3 (2) se puede apreciar lo antes dicho.

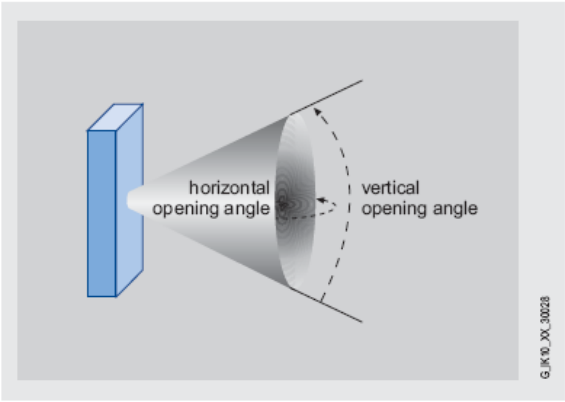

Figura 3. Patrón de radiación de una antena direccional

En la dirección de mayor intensidad el rango de transmisión de una antena direccional es típicamente diez veces más grande que el rango de una antena omnidireccional.

1.2 Recepción de RF

De igual forma que el transmisor, el sistema encargado de la recepción de la señal cumple funciones especificas para lo cual debe estar equipado con los componentes

adecuados para realizar dicha función, en la Figura 4 (1) se muestra su diagrama de bloques general.

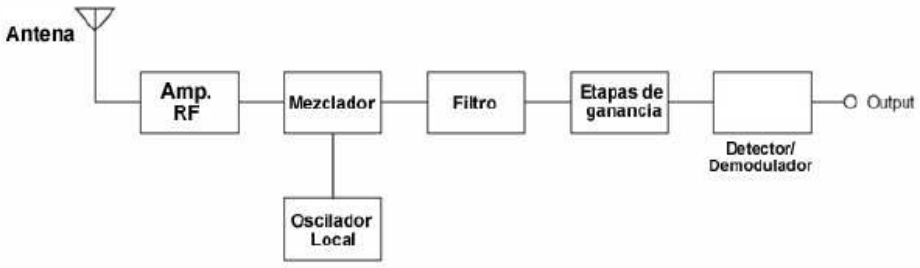

Figura 4. Diagrama en bloques del receptor

Cuando la señal llega a la antena receptora, su nivel de potencia no es el mismo con el cual fue emitida desde el transmisor, pues ha sufrido múltiples atenuaciones debido a su desplazamiento a través del espacio, al contacto con objetos ubicados en su trayectoria, y a posibles interferencias de otras señales RF presentes en el espacio, el primer paso que se realiza en la recepción es amplificar la señal para luego limpiarla mediante un *filtro* pasa banda.

Este filtro permite remover cualquier señal fuera de la banda de trabajo, de tal forma que al amplificador solo lleguen las señales que son de utilidad. El amplificador RF está diseñado para tratar con señales de muy baja potencia, en algunos casos del orden de *picowatts*, por lo cual su tarea principal es incrementar el voltaje de la señal por un amplio factor, hasta un punto donde pueda ser procesada por el mezclador o *mixer*.

El mezclador obtiene una entrada del amplificador RF y otra del oscilador local (LO), su misión es combinar las dos señales para producir cuatro frecuencias en su salida, la frecuencia de recepción, la frecuencia del oscilador local, su suma y su resta. La señal que más tiene valor es la producida por la resta de las frecuencias de recepción y del oscilador, es la más fácil de amplificar y procesar. De esta forma, la mezcla de señales pasa a través de un filtro que resuena solo a la frecuencia equivalente a la resta de las señales, permitiendo que solo esta pase a través de él. Luego, la señal pasa por una serie de amplificadores de frecuencia intermedia (IF) y después que ha sido lo suficientemente amplificada como para ser procesada, se envía a un detector/demodulador. El demodulador a su vez se utiliza para extraer la información útil de la señal y devolverla a su forma original.

2. MODULACIÓN DE SEÑALES RF

El trabajo del modulador es imprimir la información que se quiere transmitir en la onda portadora, esto es posible mediante la modulación de cualquier propiedad de la portadora,

el tiempo, frecuencia, amplitud o fase. Un fenómeno interesante que ocurre cuando se modula una portadora, es la generación de energía adicional que ocupa parte del espectro en las bandas de la onda, esto se conoce como bandas laterales. La energía en estas bandas define la forma de la onda transmitida, y es la razón por la cual los canales de comunicación se asignan con una determinada cantidad de ancho de banda.

Las normas y regulaciones que determinan la asignación y uso del espectro, tienen en cuenta los tipos de modulación que pueden utilizarse y la máxima cantidad de información que ésta puede transmitir, de acuerdo con esto las bandas RF se dividen en canales cuyo tamaño depende del uso del espectro. Es muy importante tener en cuenta la modulación utilizada en cada tecnología, ya que ésta influye enormemente en el rango de cobertura y puede determinar la ubicación y el número de estaciones necesarias en un área determinada.

2.1 Modulación Compleja

Las primeras técnicas de modulación fueron las ya conocidas, AM, FM y PM, las cuales proporcionaron maneras simples de transportar la única información disponible en el momento en el que fueron inventadas, el audio. Sin embargo, a medida que la información digital se hizo disponible, estas técnicas debieron modificarse o adaptarse para poder prestar el servicio de transmisión de la información en este nuevo formato.

Una portadora RF es una onda sinusoidal y por lo tanto es de naturaleza analógica, debido a esto, para realizar una transmisión de información digital es necesario convertir los datos del mundo digital al mundo analógico. Gracias a esta necesidad, surgieron las técnicas de modulación digital, las cuales aún utilizan la fase y la amplitud como las características a ser moduladas, pero se han implementado de manera más compleja con el fin de incrementar el rendimiento del canal, estas técnicas son las utilizadas tanto por la norma IEEE 802.11 como la norma IEEE 802.16 para poner la información en el aire.

En la Tabla 1, se puede ver un resumen de las técnicas de modulación digital más utilizadas, es de particular interés desde el punto de vista de diseño, el número de bits por transición que cada una de ellas puede representar, este factor determina la eficiencia de transmisión de bits por segundo, pero al mismo tiempo establece el grado de susceptibilidad a pérdida de información dependiendo de si la técnica se utilizará en un medio de transmisión ruidoso y congestionado.

Por ejemplo, en 256 QAM, la incertidumbre asociada con la correcta recepción e interpretación de un estado especifico de entre 256, es extremadamente alta. De hecho, la portadora debe ser de al menos 30 dB, o 1000 veces más fuerte que el ruido presente en el canal, para que la señal sea escuchada y correctamente demodulada por el receptor (1). Estas técnicas tan complejas pueden ser utilizadas solamente en los medios más limpios y con niveles de potencia mucho mayores que modulaciones de menor rango.

Por estas razones, el diseño de un sistema de radiocomunicaciones muchas veces se basa en la técnica de modulación más simple que pueda realizar bien el trabajo, siempre teniendo en cuenta el balance entre potencia versus el ancho de banda espectral para un determinado rendimiento.

Tabla 1. Técnicas de modulación digital

Modulación	Bits por Transición	Cambios
BPSK (*BiPhase Shift Keying*)	1	2 cambios de fase opuestos 180º
QPSK (*Quadrature Phase Shift Keying*)	2	4 cambios de fase separados 90º
8PSK (*8 Phase Shift Keying*)	3	8 cambios de fase separados 45º
QAM (*Quadrature Amplitud Modulation*)	2	2 estados de fase separados 180º, cada fase con 2 cambios de amplitud
16 QAM (*Quadrature Amplitud Modulation*)	4	4 estados de fase/ amplitud
64 QAM (*Quadrature Amplitud Modulation*)	6	6 estados de fase/amplitud
256 QAM (*Quadrature Amplitud Modulation*)	8	16 estados de fase/amplitud

Las técnicas de modulación más simples requieren menos potencia para cubrir efectivamente un área determinada, sin embargo, proporcionan una tasa de rendimiento menor. Por otra parte, las modulaciones complejas necesitan mayor potencia para cubrir esa misma área, pero ofrecen velocidades de transmisión mucho mayores. Si la modulación utilizada es de este tipo, puede darse el caso de que el sistema exija tanta potencia al dispositivo cliente, el cual puede ser un dispositivo portátil, que ocasione una disminución en la vida de su batería. En general, un sistema que haga uso de una modulación tan elevada puede tener serias restricciones de cobertura, o en el peor de los casos, puede ser tan frágil y sufrir tantos errores que una comunicación efectiva puede ser imposible sobre el área de cobertura deseada. La Figura 5 (3), ilustra las características y desventajas asociadas con el incremento en la complejidad de la modulación.

Hay que mencionar que existen métodos que utilizan técnicas de modulación adaptativa que provocan un cambio automático de la codificación dependiendo de las condiciones del canal. De este modo, cuanto más cerca se encuentren las estaciones cliente de la estación base, más probabilidades tendrán de poder transmitir a una mayor velocidad.

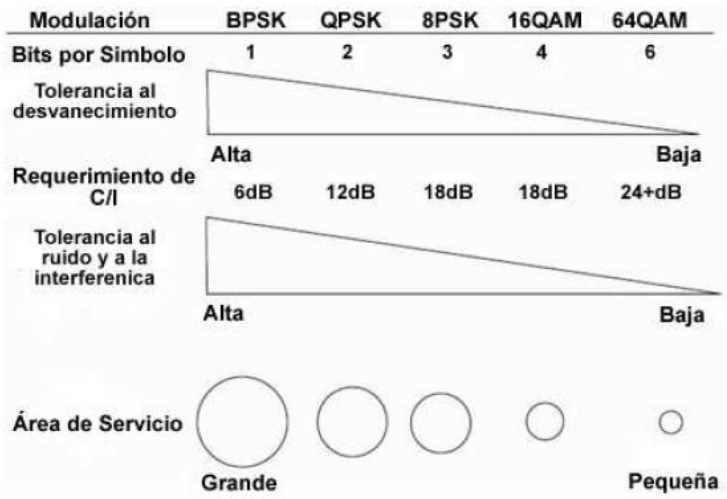

Figura 5. Comparación de modulaciones

Sin embargo, cuando se emplea una modulación de señal de orden superior, la probabilidad de errores se incrementa, por lo que se hace necesario algún sistema que permita al receptor detectar y corregir un cierto porcentaje de los errores encontrados. La técnica que permite realizar esto, se denomina corrección de error hacia delante (FEC, *Forward Error Correction*) y consiste en la adición de bits redundantes en la transmisión. Esta inclusión de bits requiere una tasa de transmisión mayor, siendo el impacto general un mejor desempeño de la red. El enlace radio 802.11b original de WiFi no incluyó FEC, pero se incorporó una codificación convolucional FEC en 802.11a y 802.11g. WiMAX emplea dos sistemas FEC: Codificación Convolucional y Reed-Solomon.

En la Tabla 2 (4), se puede encontrar información de las diferentes enmiendas que cobija el estándar WLAN y su determinado tipo de modulación.

Tabla 2. IEEE 802.11 como estándar WLAN

Estándar	Frecuencia	Técnica de modulación	Tasa de transmisión nominal	Descripción
802.11a	5 GHz	ODFM	54 Mbps	8 Canales no solapados. No ofrece QoS
802.11b	2.4 GHz	DSSS, CCK	11 Mbps	14 canales solapados
802.11g	2.4 GHz	OFDM, CCK, DSSS	54 Mbps	14 canales solapados. Compatibilidad con el 802.11b
802.11n	2.4 GHz	OFDM	360/540 Mbps	Mejora los estándares anteriores agregando MIMO que aprovecha transmisores múltiples para aumentar el rendimiento mediante multiplexación espacial

3. DUPLEXACIÓN

Debido a que los sistemas de comunicación inalámbricos deben ser bidireccionales, o sistemas *duplex*, es decir, permitir una transmisión y recepción en los dos extremos, debe existir algún mecanismo que controle el acceso al medio y que permita las dos formas de comunicaciones. Existen dos técnicas de Duplexación disponibles: Duplexación por División en Frecuencia (FDD, *Frequency Division Duplexing*) y Duplexación por División de Tiempo (TDD, *Time Division Duplexing*).

Para el caso particular de Colombia, el Ministerio de Comunicaciones ha asignado la banda de 3.5 GHz para la otorgación de licencias de operación nacional y departamental WiMAX, con equipos que utilizan Duplexación FDD.

- **FDD:** La Duplexación por división de frecuencia se lleva a cabo asignando dos frecuencias distintas al canal de comunicación. Una de ellas es transmitida por la estación base y recibida por la estación cliente, y la otra es transmitida por la estación cliente y recibida por la estación base. Debido a que los sistemas *dúplex* comparten una antena común, las dos frecuencias asignadas deben tener una gran separación entre ellas, 45 MHz o más, con el fin de asegurar que la energía transmitida sea filtrada fácilmente de la energía recibida. Esta técnica es utilizada en aquellos sistemas que esperan tener un tráfico simétrico, debido a que los dos canales asignados tienen el mismo ancho de banda.

- **TDD:** Esta técnica permite la utilización de una sola frecuencia para transmitir y recibir señales en ambos extremos del enlace. Esto se lleva a cabo dividiendo el canal en ranuras de tiempo lo suficientemente rápido como para que los trasmisores y receptores vean un flujo continuo de información. Por lo tanto, el canal es dividido temporalmente en ranuras para la transmisión y recepción con pequeños tiempos de guarda entre ellas. El estándar IEEE 802.11 utiliza TDD basado en contención, donde el AP y todas las estaciones móviles compiten por el uso del canal, lo cual hace que sea un sistema *half-duplex*. Esta técnica es útil en sistemas que tienen patrones de tráfico asimétricos, debido a que los *slots* de tiempo pueden ser asignados de forma irregular.

Sin importar el método de Duplexación utilizado, tanto la estación base como la estación cliente necesitan de un transmisor y un receptor, es decir un *transceiver.* Todos los bloques y capacidades discutidas anteriormente son implementados por los fabricantes en los equipos de radio que venden en el mercado, algunos productos presentan más limitaciones que otros, por lo tanto no existe una solución que satisfaga todos los escenarios. Es en este aspecto donde el conocimiento del diseñador de la red entra en juego para realizar una selección apropiada de la solución hardware que mejor cumpla

con los requerimientos y necesidades de los usuarios. El costo, capacidad, cobertura y confiabilidad son algunas de las variables que deberán ser consideradas para realizar un correcto diseño de una red inalámbrica.

4. OFDM

Los estándares 802.11a, 802.11g, 802.16 y 802.20 basan su funcionamiento en una técnica de modulación relativamente nueva conocida como OFDM o Modulación Ortogonal por División de Frecuencia. OFDM utiliza un gran número de canales traslapados para transmitir la información, cada uno de estos sub-canales (también llamados tonos) tiene su propio módem y se comporta como una portadora independiente, siendo el modem un dispositivo que sirve para enviar la señal *portadora* mediante otra señal de entrada llamada *moduladora*. En la Figura 6 se puede ver lo antes dicho.

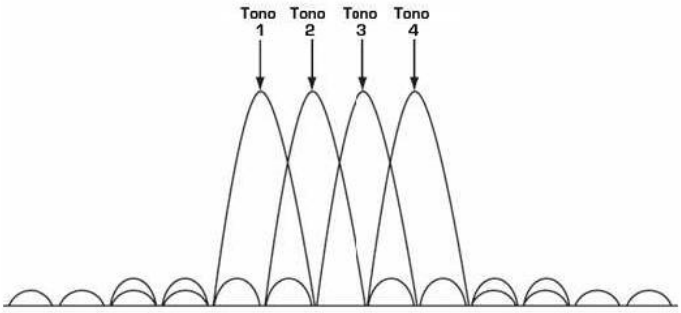

Figura 6. OFDM

Estas portadoras se traslapan, pero están espaciadas a frecuencias precisas de tal forma que sean ortogonales, así, el centro de una portadora está ubicado en el borde de la portadora adyacente, evitando que los diferentes demoduladores capten frecuencias distintas a la propia. Los beneficios de OFDM son una alta eficiencia espectral, gran flexibilidad para adaptarse al ancho de banda disponible del canal y una baja susceptibilidad al desvanecimiento por multi-trayecto. Esto es de gran utilidad en un ambiente de propagación terrestre, donde existen reflexiones de la señal que pueden distorsionar la señal recibida. En esta técnica, cada portadora ortogonal puede ser modulada independientemente con una señal BPSK o QAM, debido a que son tratadas como canales independientes, la modulación seleccionada en cada uno puede ajustarse a los desvanecimientos del medio de propagación. La implementación de esta flexibilidad añade complejidad al sistema, pero a cambio permite alcanzar el máximo rendimiento debido a que puede adaptarse dinámicamente a las condiciones del canal, por ejemplo, si una sub-portadora ocupa una frecuencia que está afectada por el desvanecimiento, puede cambiar a una modulación de orden más bajo. Los equipos actuales de 802.11a y 802.11g utilizan OFDM de 64 canales y solo hacen uso de una técnica de modulación en todas las sub-portadoras.

ANEXO B. WIRELESS SENSOR NETWORK

1. WSN EN EL MUNDO DE LA AUTOMATIZACIÓN INDUSTRIAL

En el mundo industrial, este tipo de redes cumplen una función muy importante es por ello que se debe tener muy en cuenta todos los aspectos que se relacionen con ellas. Como se dijo en la sección 1.8 es de vital importancia, que todos los sensores deben estar disponibles o en condiciones óptimas de funcionamiento ya que son una parte importante para la operación de la planta. Esto significa que no se puede admitir la pérdida de un nodo aunque la red global siga siendo operativa.

Un paquete de datos en una WSN estándar puede emplear un tiempo indeterminado desde su origen hasta su destino, a diferencia de esto, una aplicación industrial requerirá frecuentemente límites rigurosos de la demora máxima permitida cambiando así los parámetros de configuración de la red, por ejemplo la frecuencia de envió de datos, fuentes de energía entre otros. Las soluciones inalámbricas en la industria suelen tener una infraestructura cableada. Los datos emanarán desde los sensores y se propagarán por la red hasta algún punto de unión cableado, desde donde generalmente serán transportados hasta un controlador a través de un bus de alta velocidad.

2. VENTAJAS DE WSN

La comunicación inalámbrica en aplicaciones industriales tiene muchas ventajas, además de una mayor fiabilidad, la ventaja más reconocida es el bajo costo de instalación. Los emplazamientos industriales suelen ser entornos severos, con requisitos muy exigentes en cuanto al tipo y calidad del cableado. Prescindir de los cables significa que las instalaciones son más baratas, sobre todo cuando se trata de modernizar o actualizar versiones antiguas, un caso en que puede ser difícil proyectar los cables adicionales necesarios en una instalación ya de por sí congestionada.

WSN introduce nuevas técnicas de interconexión que ayudan a reducir más el costo de instalación de los sensores inalámbricos. La naturaleza *ad hoc* de WSN permite un sencillo ajuste y configuración, tarea que no debe subestimarse cuando la red es de considerable tamaño. Para apoyar la cobertura de sensores inalámbricos a nivel de planta se ha de minimizar el trabajo manual de configuración de la red. Además, la configuración de tipo ‘plug and produce’ (enchufar y producir) de la red permite desplegar redes temporales de sensores para garantizar el mantenimiento o la localización y corrección de fallos.

En la fabricación discreta, el tiempo de latencia del sistema es vital. Existe un límite estricto del tiempo máximo de latencia, por encima del cual el sistema funcionará mal. Este tiempo suele ser de algunas decenas de milisegundos. Para la monitorización de activos, en cambio, el tiempo de latencia es mucho menos crítico. Esto depende, como es lógico, del activo que se esté supervisando, pero es habitual que los tiempos de actualización sean del orden de minutos o incluso de horas. La fiabilidad es un tercer parámetro de interés. Dependiendo de la aplicación concreta hay varias formas de aumentar la probabilidad de que un mensaje llegue a su destino.

Una forma posible es aumentar la redundancia, lo que puede hacerse de varias maneras. El mensaje se puede transmitir por diferentes caminos (diversidad de espacio), en diferentes frecuencias (diversidad de frecuencias), varias veces en la misma frecuencia (diversidad de tiempos) o, incluso, se puede enviar utilizando diferentes esquemas de modulación (diversidad de esquemas de modulación). Este último es un método complejo que sólo se empleará cuando los requisitos sean extremadamente estrictos y el coste no sea ningún problema.

El sector de productos para oficina y de consumo es hoy en día el principal impulsor de las tecnologías inalámbricas, con aplicaciones de gran volumen en las que se requiere un tiempo de vida relativamente corto de los dispositivos. En cambio, la vida útil de los dispositivos industriales ha de ser mucho más larga que la de los productos de consumo. Esto significa que hay que prestar atención muy especial a la integración de componentes inalámbricos en los dispositivos industriales. El diseño modular (del hardware y el software) es esencial, pues permite un mantenimiento eficaz de los dispositivos hechos con componentes estándar disponibles en el mercado durante toda su vida útil.

3. RETOS DEL DESARROLLO DE SISTEMAS INTEGRADOS

Un sistema integrado se puede definir de varias formas. Un buen ejemplo es un sistema informático especializado que forma parte de un sistema o máquina mayor. Un sistema integrado tiene un solo propósito y ejecuta una tarea única. Por consiguiente, la creación de sistemas dedicados, como un WSN, tiene sus propios requisitos, específicos del problema en cuestión. El diseño del sistema integrado considera tanto los aspectos de hardware como de software. Los dos sistemas están entrelazados y la solución óptima, si realmente se puede hallar una, implica la interacción entre ellos.

4. ELECCIÓN DE LOS BLOQUES FUNCIONALES

Una característica importante de WSN es reducir al mínimo el consumo de energía de los nodos, proporcionando al mismo tiempo el mayor rendimiento posible a los usuarios del

sistema. Diseñar los nodos para un bajo consumo supone elegir componentes de baja potencia, algo que a primera vista puede parecer trivial, pero que suele ser más complejo de lo que parece.

El primer parámetro a considerar es el consumo de energía de la CPU, el sensor, el radiotransceptor y, posiblemente, de otros elementos, como la memoria externa y los periféricos durante el modo normal de operación. La elección de elementos de baja potencia implica normalmente aceptar compromisos sobre el rendimiento medio. Por regla general, una CPU de baja potencia opera en un ciclo reducido de reloj, con menos características en el chip que otras unidades homólogas que consumen más energía.

La solución está en elegir elementos con el rendimiento justo para poder hacer el trabajo. Es importante que el consumo de energía en modo durmiente sea bajo. A menudo se puede incluso desconectar por completo la alimentación del sensor y del transceptor. Sin embargo, la CPU necesitará alguna alimentación en modo durmiente para poder reactivarse. Para el presupuesto de la potencia total es esencial que el consumo en modo durmiente sea bajo.

Otro aspecto que también se suele pasar por alto es el tiempo de activación y desactivación de los elementos. Por ejemplo, el transceptor necesitará un cierto tiempo mínimo hasta que se estabilicen sus osciladores. Durante la espera, tanto el transceptor como la CPU consumen energía, consumo que es necesario minimizar. Lo mismo ocurre, como es lógico, al energizar la CPU y el sensor.

Finalmente, es preciso garantizar el control por la CPU de todos los elementos necesarios. Ésta es la unidad maestra del sistema y necesita controlar por completo todos los bloques funcionales.

5. ASPECTOS DEL SISTEMA

Con frecuencia se proporciona el protocolo de comunicación con objeto de utilizar los recursos disponibles dentro de los límites especificados y que ningún elemento esté energizado, si no es imprescindible.

El trabajo se reduce a activar y desactivar unidades, como el sensor, la CPU y el transceptor, con la temporización apropiada. Suponiendo que un nodo necesita despertar del modo durmiente a intervalos regulares para transmitir el valor de su sensor, pero sólo si el nuevo valor tiene una diferencia mínima dada con el último valor. Una vez enviado el valor por el canal de radio, la unidad espera recibir un mensaje de confirmación que indica que el paquete ha sido recibido correctamente.

El comportamiento requerido del software se explica mejor con un diagrama de estados (Figura 1): una representación esquemática del estado en que se encuentra el software, de los sucesos que lo llevan de un estado a otro y de las acciones asociadas a cada transición de estado. Obsérvese que, en el sistema descrito, las unidades se energizan sólo cuando es necesario, minimizando así la pérdida de energía.

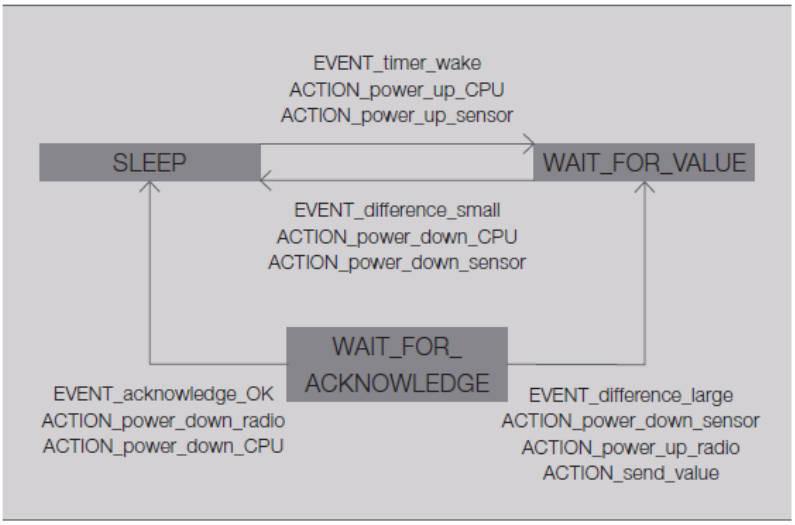

Figura 1. Diagrama de estados

6. Aspectos del protocolo

Además de utilizar componentes electrónicos de baja potencia y un programa inteligente de durmiente/reactivación, el protocolo de comunicación tiene una gran influencia sobre el consumo final de energía del sistema.

En el protocolo de comunicación se determinan los límites inferiores del consumo. Algunos protocolos de comunicación son poco eficientes y ninguna programación integrada inteligente ayudará a reducir el consumo hasta un nivel aceptable.

Otros protocolos se diseñan para conseguir un bajo consumo sin comprometer indebidamente el rendimiento de la comunicación. Uno de estos protocolos de baja potencia es la plataforma tecnológica de interconexión inalámbrica para sensores y actuadores (WISA, Wireless Interface to Sensors and Actuators).

El alto rendimiento se puede atribuir a dos factores: salto simple y multiplexación por división en el tiempo (TDM). El primer factor evita demoras en los nodos intermedios, el segundo garantiza que sólo habrá un nodo en el canal, es decir, que no habrá colisiones. La especificación ZigBee, recientemente desarrollada con el protocolo subyacente

802.15.4, es de tipo más general, pero su rendimiento de comunicación será menor. Incluye multisalto, lo que implica que un mensaje puede utilizar varios saltos en las ondas de radio para llegar a su destino. Los nodos no tienen asignados intervalos específicos de tiempo, sino que han de competir para acceder al canal. Esto permite el acceso de más usuarios al medio inalámbrico, pero introduce incertidumbre en el sistema, ya que la demora y el consumo de energía aumentan cuando un nodo está esperando su turno. Además, los nodos intermedios desconocen el momento en que pueden ser solicitados para encaminar paquetes para otros. Por consiguiente, es aconsejable disponer de nodos intermedios, también conocidos como routers, alimentados desde la red eléctrica. En resumen, el protocolo WISA se adapta bien a los requisitos de la fabricación discreta, siempre que se cumpla la condición de salto simple. Por el contrario, ZigBee resulta ideal para aplicaciones de monitorización de activos, suponiendo que los nodos routers están conectados por cable a la red eléctrica. En la Figura 2 se muestra lo antes dicho.

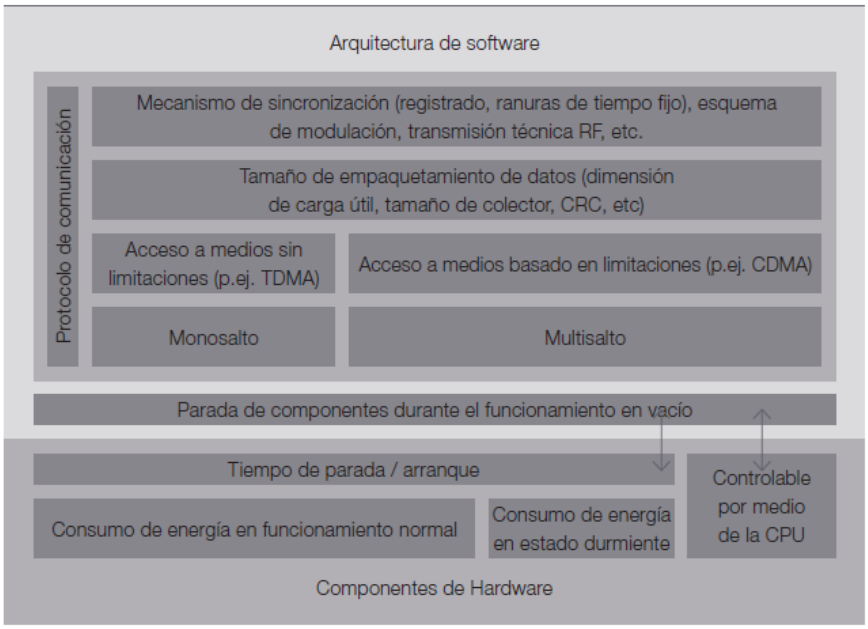

Figura 2. Métodos hardware y software

Los diferentes métodos de hardware y software influyen directamente en el consumo de energía de los dispositivos. Hasta ahora no se han cuantificado los diversos efectos, pero esto dependerá de que se desarrolle la red WSN específica.

7. Modularidad

El diseño modular es necesario con objeto de poder reutilizar los elementos. Sin embargo, la modularidad conlleva limitaciones de diseño y se ha de tener cuidado para garantizar

que las interfaces entre módulos, hardware y software sean suficientemente generales para permitir la portabilidad.

Un ejemplo clásico de la separación de módulos es la división entre el protocolo de comunicación y el software de aplicación. Integrar estos dos componentes en el mismo microcontrolador puede ser difícil. Aún más complejo es manejar versiones nuevas, tratamientos de errores y documentación cuando el software que se ejecuta en el mismo procesador tiene varias fuentes. También es alto el riesgo de suboptimización, es decir, los dos módulos de software están optimizados individualmente (con respecto a potencia, rendimiento, tamaño de código, etc.), pero esto no proporciona necesariamente una solución globalmente óptima.

La modularidad se puede conseguir también a un nivel inferior. El protocolo de comunicación puede considerarse formado por varios bloques, conocidos como capas OSI (Open Standards Interface). Dado un procedimiento correcto de diseño, cabe la posibilidad de cambiar una capa individual por otra de una fuente diferente. Como es obvio, cuanto más dividido esté el código tanto más modular resulta. Al mismo tiempo aumenta la 'suboptimización', de modo que la solución dista de ser perfecta.

8. Normalización

Actualmente hay varias iniciativas en curso que buscan normalizar WSN para el uso industrial. Una de las más conocidas es la norma ZigBee, que es una especificación inalámbrica de baja potencia, bajo coste y baja velocidad de transferencia de datos, destinada a electrodomésticos, juguetes, aplicaciones industriales y otras similares. Zig-Bee Alliance ha empezado a trabajar hace poco en un perfil para la monitorización de plantas industriales.

Otra importante iniciativa, la especificación inalámbrica HART, tiene como objetivo extender este famoso estándar al dominio inalámbrico y abrir el mercado al gran número de usuarios HART. Esta iniciativa especificará perfiles y casos prácticos en los que se podrá aplicar directamente el control inalámbrico.

La tercera iniciativa en marcha es la norma ISA-SP100. En vez de normalizar todos los elementos del sistema, ISASP100 especifica sólo los niveles superiores de la pila, con varias implementaciones posibles a nivel inferior. Estando en los comienzos del proceso es difícil predecir cuál de estas iniciativas prevalecerá. Los clientes finales serán los que decidan en su día basándose en el rendimiento y la disponibilidad de los productos. El reto actual es adoptar óptimamente la norma dominante, es decir, utilizar la norma en la mayor medida posible, satisfaciendo al mismo tiempo los requisitos críticos de la misión y manteniendo/actualizando eficazmente la implementación.

La llegada de las redes de sensores inalámbricos conlleva la introducción de muchas y apasionantes tecnologías nuevas en el mundo de la automatización industrial. El desafío tecnológico fundamental es mantener en un mínimo el consumo de energía de los nodos sensores, proporcionando al mismo tiempo el mayor rendimiento posible a los usuarios del sistema. El segundo reto es crear un diseño modular del sistema que permita el mantenimiento de los dispositivos durante toda su vida útil, satisfaciendo asimismo todos los requisitos de aplicación críticos de la misión.

ANEXO C. RECOMENDACIONES

1. PERSONAL CAPACITADO

Por más de que una red haya sido diseñada de forma adecuada es indispensable que las personas encargadas del mantenimiento y uso de la misma estén lo suficientemente calificados para operarla de manera adecuada, es por eso que se hace especial énfasis en los conocimientos que debe tener el personal.

La teoría de esta sección va orientada hacia el modo en que las empresas deben capacitar su personal, es decir, se hace necesario que la empresa tenga dentro de su estructura planes de acción que aseguren el buen funcionamiento de la red, además, estos planes deberán ser del total conocimiento del personal que administra y usa la red, deben saber que hacer en un caso de emergencia, tener planes de mantenimiento preventivo y correctivo entre otros.

a. ¿Porque capacitar?

Los recursos humanos de una organización constituyen seguramente su mayor patrimonio. Las personas también son la principal fuente de variación e innovación en cualquier ambiente organizacional.

En la actualidad la capacitación de los recursos humanos es la respuesta a la necesidad que tienen las empresas de contar con un personal calificado y productivo capaz de desenvolverse en cualquier situación adversa para la empresa.

La obsolescencia, que es la caída en desuso de máquinas, equipos y tecnologías motivada no por un mal funcionamiento del mismo, sino por un insuficiente desempeño de sus funciones en comparación con las nuevas máquinas, equipos y tecnologías introducidos en el mercado, es también una de las razones por la cual, las empresas se preocupan por capacitar a su personal, pues ésta busca actualizar sus conocimientos con las nuevas técnicas y métodos de trabajo que están en continua evolución gracias a la demanda colosal de los mercados del mundo garantizando eficiencia y competitividad, beneficiando no solo a la empresa si no al personal que recibe la capacitación ya que van a aumentar sus conocimientos, se van a sentir más seguros en su desempeño y con mayor grado de pertenencia por la empresa.

Es indudable, que la capacitación a todos los niveles constituye una de las mejores inversiones en Recursos Humanos y una de las principales fuentes de bienestar para el personal y la empresa en general.

b. Cómo Beneficia la capacitación a las organizaciones

Para las empresas, la capacitación de recursos humanos debe ser de vital importancia porque contribuye al desarrollo personal y profesional de los individuos a la vez que redunda en beneficios para la empresa, ya que está a la vanguardia en las tecnologías usadas en todo el mundo lo cual hace que sea más competitiva.

A continuación se muestra una lista de ventajas generadas por la capacitación de los recursos humanos de una empresa:

- Conduce a rentabilidad más alta y a actitudes más positivas.
- Mejora el conocimiento del puesto a todos los niveles.
- Se obtiene conocimiento más tecnificado.
- Crea mejor imagen.
- Mejora la relación jefes-subordinados.
- Se promueve la comunicación a toda la organización.
- Reduce la tensión y permite el manejo de áreas de conflictos.
- Se agiliza la toma de decisiones y la solución de problemas.
- Promueve el desarrollo con vistas a la promoción.
- Contribuye a la formación de líderes y dirigentes.

Cómo beneficia la capacitación al personal:

A continuación se muestra una lista de ventajas para el personal generadas por la capacitación de los mismos:

- Ayuda al individuo para la toma de decisiones y solución de problemas.
- Alimenta la confianza, la posición asertiva y el desarrollo.
- Contribuye positivamente en el manejo de conflictos y tensiones.
- Forja líderes y mejora las aptitudes comunicativas.
- Sube el nivel de satisfacción con el puesto.
- Permite el logro de metas individuales.
- Desarrolla un sentido de progreso en muchos campos.
- Elimina los temores a la incompetencia o la ignorancia individual.
- Se obtiene conocimiento más tecnificado.

Ya a que el objetivo principal de la capacitación es contribuir a las metas globales de la empresa, es necesario desarrollar programas que no pierdan de vista las metas y estrategias organizacionales y de implementación de nuevas tecnologías. Las operaciones organizacionales abarcan una amplia variedad de metas que comprenden personal de todos los niveles, es por eso, que al implementar una nueva tecnología dentro de una empresa todos deben estar en común acuerdo en el uso de la misma, que es uno

de los aspectos a tener en cuenta a la hora de seleccionar y usar una nueva tecnología dentro de una industria (Tabla 16). A fin de tener programas de capacitación eficaces, se recomienda un enfoque sistemático, el cual consiste en varios pasos:

Detectar las necesidades de capacitación

Es el primer paso en el proceso de capacitación, es detectar las necesidades de capacitación, esto es para que la empresa no corra el riesgo de equivocarse al ofrecer una capacitación inadecuada, lo cual redundaría en gastos innecesarios. Para detectar las necesidades de capacitación deben realizarse tres tipos de análisis, estos son:

Análisis Organizacional: que es aquél que examina a toda la compañía para determinar en qué área, sección o departamento, se debe llevar a cabo la capacitación. Se debe tomar en cuenta las metas y los planes estratégicos de la empresa, así como los resultados de la planeación en recursos humanos.

Análisis de Tareas: se analiza la importancia y rendimiento de las tareas del personal que va a incorporarse en las capacitaciones.

Análisis de la Persona: En el análisis de la persona se deben hacer dos preguntas ¿a quién se necesita capacitar? y ¿qué clase de capacitación necesita?. En este análisis se debe comparar el desempeño del empleado con las normas establecidas de la empresa.

Integración de un plan de capacitación

La Planeación de los Recursos Humanos y el desarrollo del personal centran su atención en el planeamiento formal de dichos recursos. Al planear formalmente, se debe hacer énfasis en:

- Establecer y reconocer requerimientos futuros.
- Asegurar el suministro de participantes calificados.
- El desarrollo de los recursos humanos disponibles.
- La utilización efectiva de los recursos humanos actuales y futuros.

Ejecución de programas de capacitación

Las empresas deben tomar en consideración varios lineamientos para la implementación de programas de capacitación en su organización. Una vez se tenga la planeación de la capacitación puede procederse al diseño de programas de capacitación. A continuación analizaremos brevemente algunos elementos que están considerados en el diseño del programa de capacitación.

- ✓ Establecimiento de objetivos.
- ✓ Contenido del programa.
- ✓ Principios del Aprendizaje.
- ✓ Herramientas De Capacitación.

Se hace especial énfasis en que es necesario para el buen funcionamiento de la red de comunicaciones y de los procesos de la empresa en general, que el personal que hace uso y mantenimiento de ella, tenga los conocimientos necesarios para desempeñar dichas labores y generar beneficios, de lo contrario el esfuerzo dedicado al buen diseño de la red será en vano.

2. RECOMENDACIONES DE INSTALACION INDOOR OUTDOOR

No hay duda que la base de las soluciones de automatización de cualquier tipo, es una red de comunicación fiable. Esta debe ser fácil de instalar y resistente a las duras condiciones de los ambientes industriales. Estas redes deben tener componentes aptos para el uso industrial, de fácil montaje para no elevar los costos y como cada industria tiene sus procesos característicos debe haber una amplia gama de productos para los diferentes requisitos y condiciones ambientales con sus respectivas especificaciones técnicas para una adecuada instalación que combinadas con un buen diseño de red, generaran condiciones optimas de funcionamiento llegando así a una producción constante con parámetros de calidad óptimos generando activos para la empresa.

2.1. Cómo instalar y conectar los dispositivos.

Al hacerlo, hay que seguir los consejos de instalación relativos a las condiciones ambientales, posibilidad de expansión, fuentes de energía, que se encuentran en los datos técnicos del manual de usuario.

Ciertos dispositivos pueden calentarse bastante durante el funcionamiento, hay que asegurarse de que la temperatura ambiente no supere 35 °C para el óptimo funcionamiento del dispositivo. Debe haber ventilación suficiente y en lo posible se recomienda no apilar los dispositivos.

En caso necesario, instalar/conectar antenas adicionales para los dispositivos de transmisión, teniendo en cuenta las recomendaciones sobre la perdida de ganancia generada por el cable para la instalación de la antena, Se recomienda y es preferible que no sea demasiado largo.

Suministrar alimentación eléctrica a través de la fuente de alimentación proporcionada o del cable de alimentación. En los dispositivos con batería, hacer un seguimiento

exhaustivo sobre el consumo de energía y en lo posible configurar los dispositivos en modo de bajo consumo, es decir que estén activos cuando sea necesario esto se aplica mucho en las redes de sensores.

Ciertos dispositivos permiten la alimentación a través de un cable de red (Power-over-Ethernet, PoE), hay que observar las características técnicas del dispositivo que se desea usar.

2.2. Planta de varios pisos

A la hora de instalar un AP en un lugar cerrado, se recomienda posicionarlo a una altura 1.30 metros del nivel del piso para así permitir que las ondas de RF cubran toda la locación, cuando es una planta de una piso.

Cuando físicamente aumentan los niveles de la locación en donde se va a instalar la red es decir se tiene una planta física de varios pisos, es necesario pensar en una configuración más óptima para la instalación de los componentes activos de la red. A continuación en la Figura 1, se muestran unos ejemplos de posibles soluciones de montaje para el caso antes mencionado.

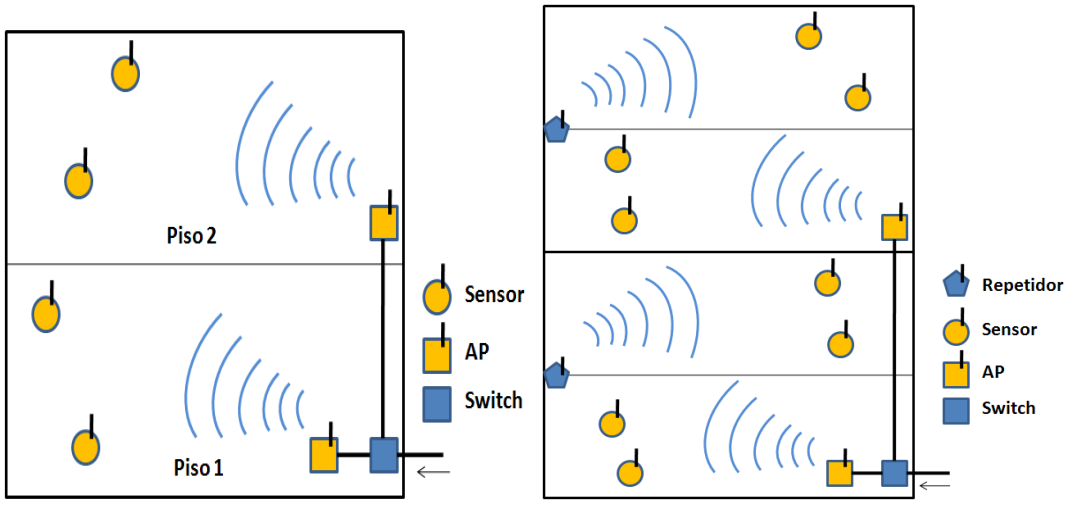

Figura 1. Ejemplos de solución para plantas de varios pisos.

INDOOR

- Análisis de ubicación de clientes.
- Intensidad de tráfico, procesos de roaming.
- Atenuación por paredes o techos.
- Calculo de enlaces.

OUTDOOR

- IEEE 802.11b no especifica solución de planta externa.
- Las soluciones existentes son adaptaciones propietarias de los fabricantes.
- Se requieren antenas externas y opcionalmente amplificadores.
- Debe existir Línea de Vista entre las Antenas.
- Línea de Vista Optica/de Radio
- Desarrollo del Perfil del Trayecto
- Liberación de la Zona de Fresnel
- Cálculo de la Curvatura de la Tierra y Alturas de las Antenas.
- Determinación del SOM/Cálculo de Enlace.

4. TIPOS DE MANTENIMIENTO

A continuación se hará una descripción de las posibilidades existentes sobre el mantenimiento, pero desde un punto de vista global, ya que es un hecho la necesidad de tener dentro de toda empresa, industria o fuerza productiva del tipo que sea que utilice maquinaria, dispositivos electrónicos o cualquier tipo de instalación con alguna función necesaria para el desarrollo del determinado bien o servicio, planes de mantenimiento que contrarresten estas amenazas en contra de la buena productividad y normal desempeño de actividades.

4.1 Mantenimiento Correctivo

Es aquel que se ejecuta a los dispositivos que están en operación después de detectar falla y que requiera de una reparación para su buen funcionamiento ya sea de forma urgente o planificada.

El mantenimiento correctivo o mantenimiento por rotura fue el esbozo de lo que hoy día es el mantenimiento. Esta etapa del mantenimiento va precedida del mantenimiento planificado.

Este, agrupa las acciones a realizar en el software o en los dispositivos ante un funcionamiento incorrecto, deficiente o incompleto que por su naturaleza no puede planificarse en el tiempo.

Estas acciones, que no implican cambios funcionales, corrigen los defectos técnicos de las aplicaciones. Se entiende por defecto una diferencia entre las especificaciones del sistema y su funcionamiento cuando esta diferencia se produce a causa de errores en la configuración del sistema o del desarrollo de programas. Se establecerá un marco de colaboración que contemple las actividades que corresponden a la garantía del actual proveedor y las actividades objeto de este contrato. La corrección de los defectos

funcionales y técnicos de las aplicaciones cubiertas por el servicio de mantenimiento debe incluir:

- Recogida, catalogación y asignación de solicitudes y funciones.
- Análisis del error / problema.
- Análisis de la solución.
- Desarrollo de las modificaciones a los sistemas, incluyendo pruebas unitarias.
- Optimización dentro de las posibilidades.
- Pruebas del sistema documentadas.
- Mantenimiento de las documentaciones técnicas y funcionales del sistema.

Cuando se presenta un error en el funcionamiento ya sea de la planta en general o de sus comunicaciones, es necesario analizar a fondo el problema y la causa de las fallas, para así determinar si los planes implementados para la corrección de errores son eficientes o se quedan cortos ante una situación específica, con el fin de estar en una mejora continua y prever posible fallas futuras, es por ello que estos planes deben estar sujetos a modificaciones y a optimización combinado con una capacitación adecuada del personal encargado del mantenimiento.

4.2 Mantenimiento Preventivo

Es aquel realizado a los equipos con el fin de conservarlos en condiciones óptimas de operación. El mantenimiento preventivo es una actividad programada de inspecciones, tanto de funcionamiento como de seguridad, ajustes, reparaciones, análisis, limpieza, calibración, que deben llevarse a cabo en forma periódica en base a un plan establecido. El propósito es prever averías o desperfectos en su estado inicial y corregirlas para mantener la instalación en completa operación a los niveles y eficiencia óptimos, es decir se prevé el mal funcionamiento.

El mantenimiento preventivo permite detectar fallos repetitivos, disminuir los puntos muertos por paradas, aumenta la vida útil de equipos, disminuye costos de reparaciones, detecta puntos débiles en la instalación, entre una larga lista de ventajas. Algunos de los métodos más habituales para determinar que procesos de mantenimiento preventivo deben llevarse a cabo son las recomendaciones de los fabricantes, la legislación vigente, las recomendaciones de expertos tanto de los equipo como del proceso y las acciones llevadas a cabo sobre activos similares.

4.3 Mantenimiento Predictivo

Es el mantenimiento programado y planificado con base en el análisis, muestreo y registro de variables que determinan el estado de la red o de sus equipos. La Gestión de Mantenimiento Asistido por Computadora u Ordenador, (GMAO). En esencia es una herramienta software que ayuda en la gestión de los servicios de mantenimiento de una

empresa. Básicamente es una base de datos que contiene información sobre la empresa y sus operaciones de mantenimiento. Esta información sirve para que todas las tareas de mantenimiento se realicen de forma más segura y eficaz. También se emplea como herramienta de gestión para la toma de decisiones, es una nueva tendencia que están usando las empresas para gestionar de manera más acertada las operaciones de mantenimiento.

4.1.1. Que es la seguridad en las tecnologías de información y comunicación.

Para muchos, se considera la seguridad un sinónimo para el cifrado de la información y para otros, la seguridad se refiere a la protección contra los virus informáticos. En realidad, la seguridad tiene un alcance mucho más amplio. Existen ocho objetivos de seguridad (36), los cuales son un marco adecuado para la estructuración de los requisitos de seguridad y las propiedades de cualquier tipo de sistema, estos son:

Confidencialidad: Los objetivos de la confidencialidad son impedir la divulgación de información a personas o sistemas no autorizados. Para los sistemas de automatización, esto es de suma importancia, ya que se refiere a información con respecto al proceso específico, tales como recetas de los productos o de rendimiento de la planta, datos de planificación, los secretos específicos de los mecanismos de seguridad propios, tales como contraseñas y claves de cifrado entre otro tipo de información.

Integridad: El objetivo de la integridad es garantizar que las modificaciones de información específica sean hechas por personas o sistemas autorizados. Para los sistemas de automatización esto se aplica a información tal como las recetas de los productos, valores de los sensores o comandos de control. La violación de la integridad puede causar problemas de seguridad, es decir, el equipo, el medio ambiente, o incluso las personas pueden resultar perjudicadas.

Disponibilidad: Hace referencia a que personas o sistemas no autorizados no puedan negar el acceso o uso a personas o sistemas con autorización. En sistemas de automatización, esto hace referencia a todos los elementos de la planta tales como los sistemas de control, sistemas de seguridad, estaciones de operador, estaciones de ingeniería, sistemas MES[1], y los sistemas de comunicación de estos elementos con el mundo de afuera.

La violación de la disponibilidad, también es conocida como *Negación de Servicio* (DoS), la cual no sólo puede causar daños económicos, sino también en cuestiones de seguridad ya que los operadores pueden perder la capacidad de supervisar y controlar los procesos.

Autenticación: La autenticación es la determinación de la verdadera identidad de un usuario del sistema y el mapeo de esta identidad a un sistema principal interno (por

[1] MES: Manufacturing Execution Systems (Sistemas de Ejecución de Manufactura).

ejemplo, cuentas de usuario válidas) en el cual el usuario es conocido, es decir, la autenticación se basa en distinguir entre los usuarios legítimos y los ilegítimos.

Autorización: También conocida como control de acceso, se refiere a la prevención de las personas (o sistemas) que no tienen permiso de acceso al sistema. En el sentido más general, la autorización hace referencia al mecanismo que distingue entre los usuarios legítimos e ilegítimos para todos los objetivos de seguridad, por ejemplo, la confidencialidad, integridad, entre otros. En un sentido más estricto del control de acceso, hace referencia a la restricción de la capacidad de emitir diferentes tipos de comandos para el sistema de control de la planta.

Auditabilidad o Capacidad de verificación: Hace referencia a la posibilidad de reconstruir el historial completo del comportamiento del sistema de registros de todas las acciones llevadas a cabo en él. Este objetivo de seguridad hace referencia sobre todo a descubrir y encontrar razones para el mal funcionamiento del sistema y para establecer el ámbito de aplicación del mal funcionamiento o las consecuencias de un incidente de seguridad. Hay que tener en cuenta que la auditabilidad sin autenticación pueden servir para fines de diagnóstico, pero no establece la rendición de cuentas.

Sin repudiabilidad: Primero que todo, la repudiabilidad es la noción de negar que se ha producido una acción. El objetivo de esto, es ser capaz de proporcionar una prueba irrefutable a un tercero del responsable de una acción determinada en el sistema, incluso si éste actor no está cooperando. Este objetivo de seguridad es importante para establecer la rendición de cuentas y la responsabilidad. En el contexto de los sistemas de automatización, esto es muy importante con respecto a los requisitos reglamentarios. La violación de este objetivo de seguridad puede tener consecuencias jurídicas y comerciales (6).

Protección de Terceras Partes: Un ataque exitoso y un sistema de automatización perturbado pueden utilizarse para diversos ataques contra los sistemas informáticos de terceros, utilizando, por ejemplo, *Ataque de Negación de Servicio Distribuido*[2] (DDoS) o ataques de gusanos. El objetivo de la protección de terceras partes es prevenir que este tipo de daños ocurran.

La importancia de cada objetivo de seguridad depende del sistema, específicamente su propósito y sus activos. En los sistemas de automatización, la confidencialidad es importante para la producción y los datos de rendimiento, mientras que la integridad y la autorización son más importantes para los comandos de operador, los parámetros y funciones de control. Para cada sistema e instalación, se debe diseñar una política de seguridad, indicando los objetivos de seguridad y limitaciones específicas del sistema.

[2] DDoS: Es un tipo especial de DoS consistente en la realización de un ataque conjunto y coordinado entre varios equipos hacia un servidor víctima.

4.1.2. Mecanismos de seguridad.

El riesgo de un ataque existe, si hay alguna vulnerabilidad y una amenaza en el sistema. La vulnerabilidad de un sistema de información puede ser causada por un defecto de diseño lógico por ejemplo, un protocolo diseñado erróneamente, un error de aplicación, lo que permite un desbordamiento de búfer (BO)[3], o de una de las debilidades fundamentales como, contraseñas y claves criptográficas que están tratando de adivinar por todas las permutaciones posibles (7).

A continuación, se muestra una tabla con una lista de mecanismos de seguridad usados para contrarrestar alguna falla, debilidad o posible amenaza que pueda generar una ataque contra el sistema o violación de los objetivos o políticas de seguridad, para ello se han tomado en cuenta cada uno de los objetivos de seguridad antes nombrados y se han clasificado los mecanismos de seguridad según cada uno de ellos (8):

Tabla 1. Mecanismos de Seguridad Según el Objetivo

Objetivos de Seguridad	Mecanismos de seguridad
Confidencialidad	Cifrado, Red Virtual Privada (VPN), Capa de Conexión Segura (SSL)
Integridad	Sumas de Comprobación de Cifrado, Escaneo de Software Malicioso.
Disponibilidad	Redundancia, Diversidad, Escaneo de Software Malicioso.
Autenticación	Contraseñas, Certificados, Fichas / Tarjetas inteligentes, Biometría, Probar Respuesta de los Protocolos.
Autorización	Sistemas Operativos Robustos (Sin servicios inseguros o sin uso), Cuentas de Usuario, Listas de Control de acceso Bien Definidas (ACLs), FireWalls, Servidores de seguridad personales, Filtros de mensajes el nivel de aplicación, LAN virtual (VLAN).
Auditabilidad o Capacidad de verificación	Sistema de Detección de Intrusos (IDS), Registros.
Sin Repudiabilidad	Firmas Digitales.
Protección de Terceras Partes	FireWall (Filtrado de Salida), Escaneo de Software Malicioso (Para datos de salida).

[3] BO: Del inglés *buffer overflow* o *buffer overrun,* es un error de software que se produce cuando se copia una cantidad de datos sobre un área que no es lo suficientemente grande para contenerlos, sobrescribiendo de esta manera otras zonas de memoria.

Ahora se hará una descripción general de los mecanismos de seguridad más relevantes plasmados en la tabla, para así tener una idea de lo provechoso de cada uno de ellos para la seguridad y la integridad de un sistema de comunicaciones.

Cifrado: Para el significado de cifrado se puede hacer una analogía hacia el hecho de guardar algo muy valioso dentro de una caja fuerte cerrada con una llave única. Los datos confidenciales se cifran con un algoritmo de cifrado y una clave que los hace ilegibles si no se conoce dicha clave. Las claves de cifrado de datos se determinan en el momento de realizar la conexión entre los componentes de la red.

El cifrado es tal vez, una de las herramientas más efectivas para el envió de información de forma segura. Existen diferentes sistemas de cifrado, entre ellos (9):

- ***Sistemas de Cifrado Simétrico:*** Los sistemas de cifrado simétrico son aquellos que utilizan la misma clave para cifrar y descifrar un documento. El principal problema de seguridad reside en el intercambio de claves entre el emisor y el receptor ya que ambos deben usar la misma clave. Por lo tanto se tiene que buscar también un canal de comunicación que sea seguro para el intercambio de la clave.

- ***Sistemas de Cifrado Asimétrico:*** También son llamados sistemas de cifrado de clave pública. Este sistema de cifrado usa dos claves diferentes. Una es la clave pública y se puede enviar a cualquier persona y otra que se llama clave privada, que debe guardarse para que nadie tenga acceso a ella. Para enviar un mensaje, el remitente usa la clave pública del destinatario para cifrar el mensaje. Una vez que lo ha cifrado, solamente con la clave privada del destinatario se puede descifrar, ni siquiera el que ha cifrado el mensaje puede volver a descifrarlo. Por ello, se puede dar a conocer perfectamente la clave pública para que todo aquel que se quiera comunicar con el destinatario lo pueda hacer.

- ***Sistemas de Cifrado Híbridos:*** Es el sistema de cifrado que usa tanto los sistemas de clave simétrica como el de clave asimétrica. Funciona mediante el cifrado de clave pública para compartir una clave para el cifrado simétrico. En cada mensaje, la clave simétrica utilizada es diferente por lo que si un atacante pudiera descubrir la clave simétrica, solo le valdría para ese mensaje y no para los restantes. La clave simétrica es cifrada con la clave pública, y el mensaje saliente es cifrado con la clave simétrica, todo combinado automáticamente en un sólo paquete. El destinatario usa su clave privada para descifrar la clave simétrica y luego usa la clave simétrica para descifrar el mensaje.

Red Virtual Privada (VPN): Es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet. Aplicaciones comunes de esta tecnología son, la posibilidad de conectar dos o más sucursales de una

empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa al centro de cómputo, o que un usuario pueda acceder a su equipo desde un sitio remoto. Todo esto con la utilización de la infraestructura de Internet. Para hacerlo posible de manera segura es necesario proporcionar los medios para garantizar la autenticación, integridad y confidencialidad de toda la comunicación, cumpliendo requerimientos básicos como la identificación de usuario, codificación de datos o cifrado y administración de claves de cifrado.

Capa de Conexión Segura (SSL): Proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, sólo el servidor es autenticado mientras que el cliente se mantiene sin autenticar; la autenticación mutua requiere un despliegue de infraestructura de claves públicas (o PKI) para los clientes. Los protocolos permiten a las aplicaciones cliente-servidor comunicarse de una forma diseñada para prevenir escuchas (eavesdropping), la falsificación de la identidad del remitente (phishing) y alterar la integridad del mensaje. SSL implica una serie de fases básicas:

- Negociar entre las partes el algoritmo que se usará en la comunicación.
- Intercambio de claves públicas y autenticación basada en certificados digitales.
- Cifrado del tráfico basado en cifrado simétrico.

Durante la primera fase, el cliente y el servidor negocian qué algoritmos criptográficos se van a usar. Las implementaciones actuales proporcionan las siguientes opciones:

- Para criptografía de clave pública: RSA, Diffie-Hellman, DSA (Digital Signature Algorithm) o Fortezza.
- Para cifrado simétrico: RC2, RC4, IDEA (International Data Encryption Algorithm), DES (Data Encryption Standard), Triple DES o AES (Advanced Encryption Standard);
- Con funciones hash: MD5 o de la familia SHA.

Sistema de Detección de Intrusos (IDS): Es un programa usado para detectar accesos no autorizados a un computador o a una red. Estos accesos pueden ser ataques que usan herramientas automáticas programas y scripts desarrollados para atacar sistemas de computadoras y redes.

El IDS suele tener sensores virtuales con los que el núcleo del IDS puede obtener datos externos generalmente sobre el tráfico de red. El IDS detecta, gracias a dichos sensores, anomalías que pueden ser indicio de la presencia de ataques o falsas alarmas.

Su funcionamiento se basa en el análisis del tráfico de red, el cual al entrar al analizador es comparado con firmas de ataques conocidos, o comportamientos sospechosos, como

puede ser el escaneo de puertos, paquetes malformados, entre otros. El IDS no sólo analiza qué tipo de tráfico es, sino que también revisa el contenido y su comportamiento. Normalmente esta herramienta se integra con un *firewall*.

Firewall: Es un sistema que protege a un ordenador o a una red de ordenadores contra intrusiones provenientes de redes de terceros (generalmente desde internet). Un sistema de *firewall* filtra paquetes de datos que se intercambian a través de internet. Por lo tanto, se puede decir que se trata de una pasarela de filtrado.

El sistema *firewall* es un sistema de software, a menudo sustentado por un hardware de red, que actúa como intermediario entre la red local donde se utiliza el *firewall* y una o más redes externas, también existe el término *firewall* personal, que se utiliza para los casos en que el área protegida se limita al ordenador en el que el *firewall* está instalado. A continuación se muestra Figura 32 (6) donde se ve la ubicación de un *firewall* dentro de una red industrial.

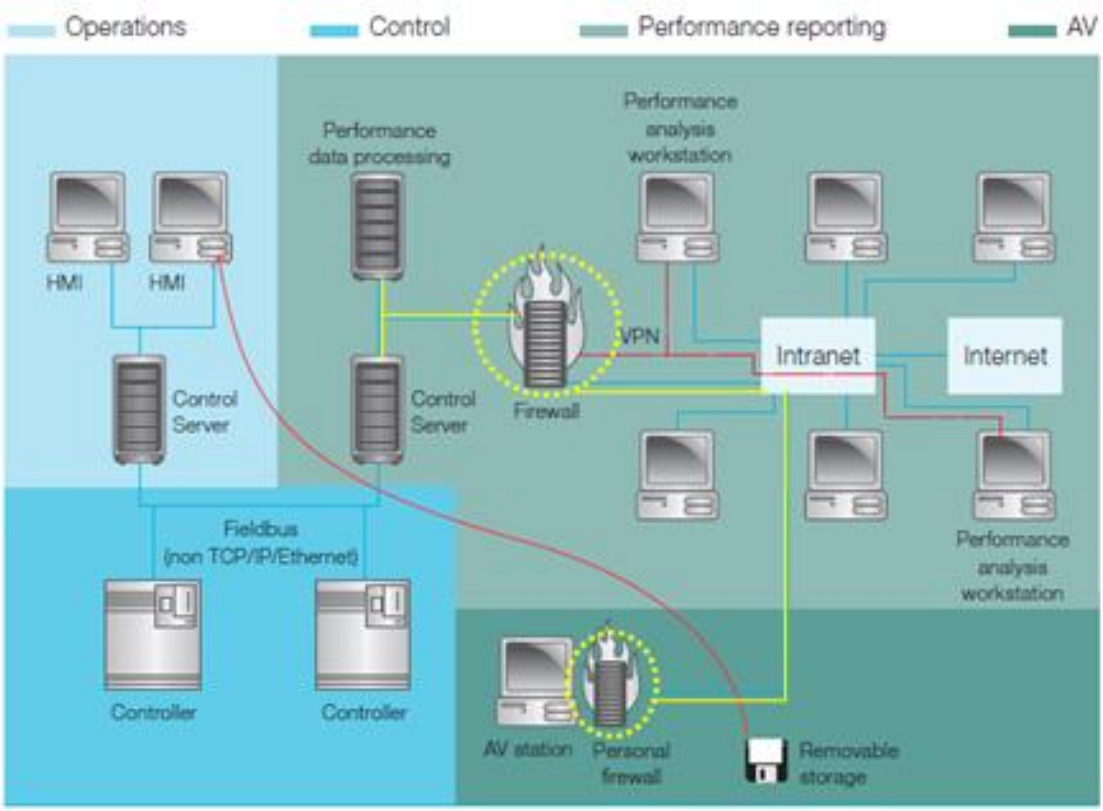

Figura 1. Diagrama de red de un sistema de automatización protegido contra software malicioso o malware

Estos sistemas constan de un conjunto de reglas predeterminadas que le permiten al sistema autorizar la conexión (*permitir*), bloquear la conexión (*denegar*) y rechazar el pedido de conexión sin informar al que lo envió (*negar*), todas estas reglas implementan un método de filtrado que depende de la política de seguridad propia de la organización.

Redundancia: La redundancia en un sistema de comunicación se puede dar de varias formas. Un sistema redundante, es aquel en el que se repiten aquellos datos o hardware de carácter crítico que se quiera asegurar ante los posibles fallos que puedan surgir por su uso constante.

También se puede hablar de redundancia en el sistema eléctrico, un fallo en el suministro eléctrico a un servidor, podría tener consecuencias catastróficas. No solo se necesita un suministro constante, sino que es conveniente que no tenga subidas y bajadas bruscas, para evitar daños en los componentes.

También se puede hablar de redundancia en los componentes de red, ya que si uno de estos componentes falla, la información no llegaría nunca al servidor. Para evitar este fallo, se aconseja crear dos caminos diferentes entre los componentes de la red, basados en la concepción de las formaciones de topologías en malla.

Lista de Control de Acceso (ACLs): Es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto. Las ACLs permiten controlar el flujo del tráfico en equipos de redes, tales como *routers* y *switches* que son los componentes principales del flujo de tráfico de la red. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición preestablecida.

ANEXO D. TOPOLOGÍAS Y COMPONENTES DE RED

A continuación se muestra una descripción general de cada una de las topologías de la Figura 27 del Capítulo 3 sección 3.2 y con ello poder hacerse una idea de cómo y cuándo usar cada una de ellas además de los componentes de red nombrados en la sección 3.5.

1. TOPOLOGÍAS DE RED

Topología en Bus. Es una red cuya topología se caracteriza por tener un único canal de comunicaciones denominado bus, troncal o *backbone*, al cual se conectan los diferentes dispositivos. De esta forma todos los dispositivos comparten el mismo canal para comunicarse entre sí, hay una conexión *full-duplex* es decir se permite la transmisión y recepción simultanea.

Un ejemplo típico en este caso es el *Industrial Ethernet bus*, en el que la red se conecta a través de un acoplador (transmisor, emisor-receptor) con un cable coaxial. El cable de bus termina en ambos extremos con resistencias de terminación los cuales absorben la trama al final de la línea. Segmentos individuales pueden ser conectados entre sí por medio de componentes activos (repetidores), cada uno de estos segmentos puede derivar en un dispositivo que aplique tecnología inalámbrica como se ve en la Figura 1 (5).

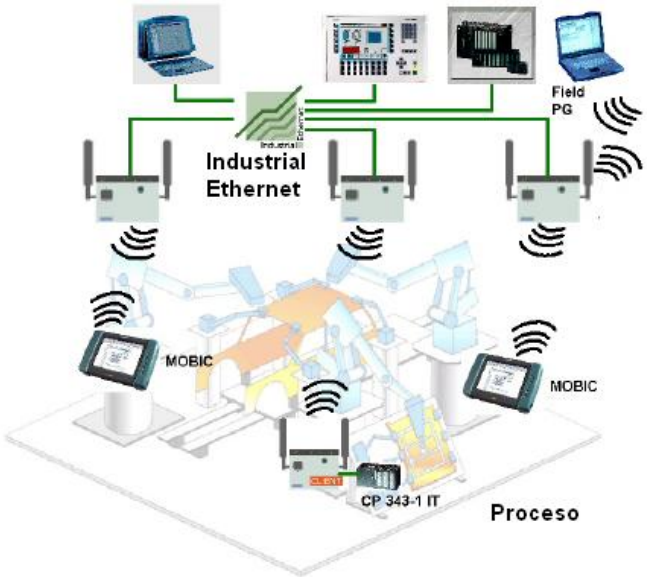

Figura 1. Ejemplo de topología en Bus

Topología en Anillo: Este tipo de topología es muy parecida a la de bus, pero con la diferencia de que el punto final e inicial del bus no tienen terminales si no que están

unidos por un nodo formando un anillo por el cual fluye la información. En este tipo de topologías los terminales actúan como repetidores unidos a cada estación transmisora.

Topología en Estrella. La topología en estrella se caracteriza por el uso de un *hub* o un *switch* central que retransmite los paquetes de datos que recibe desde cualquiera de los otros equipos conectados en esta configuración. Las estaciones de red individuales están conectadas con los componentes activos de la red de forma punto a punto, produciendo así una red en estrella. En este tipo de interconexión cuando se tienen muchos equipos es posible que se eleve el nivel de colisiones y tráfico de red, es necesario identificar los pros y los contras dependiendo de la aplicación. La topología de estrella soporta un sólo coordinador, que para la IEEE 802.15.4 logra conectar hasta 65,536 dispositivos terminales.

Topología en Árbol. La conexión en árbol es parecida a una serie de redes en estrella interconectadas salvo en que no tiene un nodo central. En cambio, tiene un nodo de enlace troncal, generalmente ocupado por un *hub* o *switch*, desde el que se ramifican los demás nodos. Es una variación de la red en bus, la falla de un nodo no implica interrupción en las comunicaciones. Se comparte el mismo canal de comunicaciones por lo tanto como en el bus, todas las terminales escuchan. Tanto la de árbol como la de estrella son similares a la de bus cuando el nodo de interconexión trabaja en modo difusión, pues la información se propaga hacia todas las estaciones, solo que en ésta topología las ramificaciones se extienden a partir de un punto raíz, a tantas ramificaciones como sean posibles, según las características del árbol, en la Figura 2 (6) se puede ver un ejemplo de esta topología.

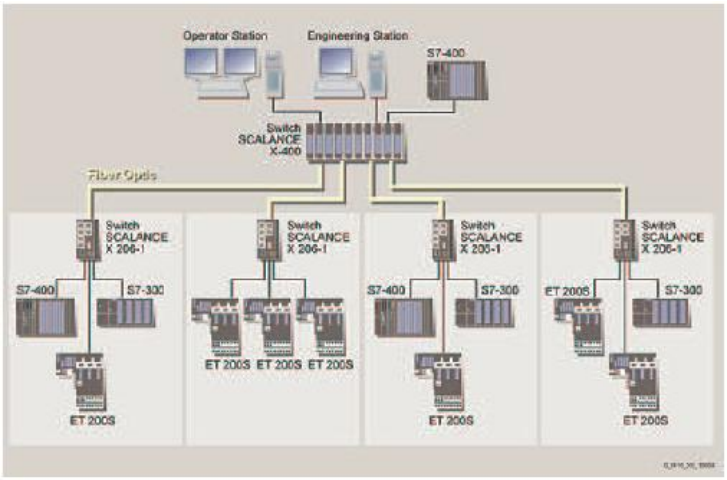

Figura 2. Topología en Árbol

Los problemas asociados a las topologías anteriores radican en que los datos son recibidos por todas las estaciones sin importar para quien vayan dirigidos. Es entonces necesario dotar a la red de un mecanismo que permita identificar al destinatario de los mensajes, para que estos puedan recogerlos a su arribo. Además, debido a la presencia de un medio de transmisión compartido entre muchas estaciones, pueden producirse

interferencia entre las señales cuando dos o más estaciones transmiten al mismo tiempo. Una red en árbol inalámbrica, permite que se establezca una red punto a punto con un mínimo de proceso de ruteo, ya que puede usar ruteo multisalto, donde cualquier par de nodos que desean comunicarse podrán utilizar para ello otros nodos inalámbricos intermedios que se encuentren en el camino.

La solución al primero de estos problemas aparece con la introducción de un identificador de estación destino. Cada estación de la red está unívocamente identificada. Para darle solución al segundo problema (superposición de señales provenientes de varias estaciones), hay que mantener una cooperación entre todas las estaciones, y para eso se utiliza cierta información de control en las tramas que controla quien transmite en cada momento (control de acceso al medio) se pierde por completo la información si no la utilizas.

Topología en Malla. Es una topología de red en la que cada nodo está conectado a todos los nodos. De esta manera es posible llevar los mensajes de un nodo a otro por diferentes caminos. Si la red de malla está completamente conectada, no puede existir absolutamente ninguna interrupción en las comunicaciones. Cada servidor tiene sus propias conexiones con todos los demás servidores. También debe tenerse en cuenta que la capacidad de los enlaces puede verse limitada a medida que aumentan los nodos, y además debido a las múltiples funcionalidades adicionales que deben desempeñar, su diseño es más complejo. Industrialmente, esta red tiene grandes aplicaciones en las redes de sensores/actuadores y controladores. Una topología de malla, permite establecer caminos para la información desde cualquier dispositivo fuente a cualquier dispositivo destino, usando algoritmos de ruteo basados en tablas o árboles de ruteo. En la topología de malla se requiere que los radios de los nodos coordinadores y ruteadores estén encendidos todo el tiempo.

2. COMPONENTES DE RED

En esta sección, se muestra información relativa a los componentes que hacen parte de una red de comunicaciones en general haciendo énfasis en los componentes utilizados en el diseño de la red caso de estudio profundizando lo tratado en la sección 3.5 de la monografia.

Repetidores

Un repetidor o amplificador es un dispositivo que intensifica las señales eléctricas para que puedan viajar grandes distancias entre nodos. Con este dispositivo se pueden conectar un gran número de nodos a una red, además se pueden adaptar a diferentes medios físicos.

En una red cableada, la longitud máxima para el cable UTP por ejemplo es de 100 metros. Si es necesario extender la red más allá de este límite, se debe agregar un dispositivo repetidor a la red. El propósito de este, es regenerar y re temporizar las

señales de red a nivel de los bits para permitir que estos viajen a mayor distancia a través de los medios. En la Figura 3 se puede ver un dispositivo repetidor inalámbrico.

Figura 3. Repetidor inalámbrico.

El término repetidor se refiere tradicionalmente a un dispositivo con un solo puerto de entrada y un solo puerto de salida. Sin embargo, hoy en día estos dispositivos han evolucionado en repetidores multipuerto. En un sistema inalámbrico dentro de una edificación, un repetidor generalmente consiste en una antena externa de alta ganancia combinada con un amplificador de señal bidireccional.

Un repetidor inalámbrico está diseñado para repetir datos digitales entre transmisores inalámbricos y el receptor de destino. Se necesitan enlaces de repetición cuando el receptor de destino está más allá del alcance de algún transmisor inalámbrico o cuando no hay LOS y es por tanto incapaz de recibir transmisiones directamente. Si la distancia entre transmisores y el receptor de destino es demasiado grande para que la cubra un único repetidor, se pueden añadir varios repetidores auxiliares a lo largo del camino de comunicación. De esta forma se crea una red multinivel.

En una red multinivel, un repetidor auxiliar colocado en el camino de comunicación retransmite los datos que recibe de un repetidor de nivel superior a un repetidor de nivel inferior, pero también se puede usar para retransmitir datos de transmisores situados cerca de él, en su área de cobertura local los datos fluyen del repetidor de mayor nivel a través de enlaces de repetidores intermedios hasta el repetidor de menor nivel y finalmente alcanza el receptor de destino.

En conclusión estos dispositivos ayudan a obtener una mayor cobertura y expansión de la red. En el modelo OSI, los repetidores se clasifican como dispositivos de Capa 1 o nivel físico.

Hub o Concentrador

El propósito de un *hub* al igual que un repetidor, es regenerar y re temporizar las señales de red, esto se realiza a nivel de los bits para un gran número de hosts (por ej., 4, 8 o incluso 24) utilizando un proceso denominado concentración. Este dispositivo es muy

similar al repetidor, es por ello que el *hub* también se denomina repetidor multipuerto. La diferencia es la cantidad de puertos disponible en cada uno de ellos. En la Figura 4 se puede ver un dispositivo *hub*.

Figura 4. Concentrador o Hub de 8 puertos.

Un concentrador funciona repitiendo cada paquete de datos en cada uno de los puertos con los que cuenta, excepto en el que ha recibido el paquete, de forma que todos los puntos tienen acceso a los datos.

Los *hubs* se utilizan por dos razones principalmente, para crear un punto de conexión central para los medios de cableado y para aumentar la confiabilidad de la red, esta se ve aumentada al permitir que cualquier cable falle sin provocar una interrupción en toda la red. Este dispositivo es muy común en las configuraciones de red tipo estrella.

Existen distintas clasificaciones para los *hubs*. La primera clasificación corresponde a los *hubs* activos o pasivos. La mayoría de los *hubs* modernos son activos, ya que toman energía desde un suministro de alimentación para regenerar las señales de red a diferencia de los *hubs* pasivos que simplemente dividen la señal entre los puertos que estén en uso. Estos no regeneran los bits, de modo que no ayudan a extender la distancia de transmisión, sino que simplemente permiten que uno o más hosts se conecten al mismo segmento de cable.

Otra clasificación de los *hubs* corresponde a los inteligentes y no inteligentes. Los *hubs* inteligentes tienen puertos de consola, lo que significa que se pueden programar para administrar el tráfico de red. Los *hubs* no inteligentes simplemente toman una señal entrante y la repiten hacia cada uno de los puertos sin la capacidad de realizar ninguna administración. Los *hubs* se consideran dispositivos de Capa 1 dado que sólo regeneran la señal y la envían por medio de una transmisión *Broadcast*[4] a todos los puertos.

Bridge o Puente

Un puente es un dispositivo diseñado para conectar dos segmentos de red. El propósito de un puente es filtrar el tráfico de una red, para que el tráfico local siga siendo local, pero permitiendo la conectividad a otras partes de la red para el envío de datos, esto lo consigue al verificar la dirección local. Cada dispositivo de la red tiene una dirección MAC exclusiva en la NIC (Tarjeta de Interfaz de Red), el puente rastrea cuáles son las

[4] Broadcast: Es un tipo de transmisión en la cual un paquete de datos enviado será recibido por todos los dispositivos que conforman la red.

direcciones MAC que están ubicadas a cada lado del puente y toma sus decisiones basándose en esta lista de direcciones MAC ya aprendidas.

El aspecto de los puentes varía enormemente según el tipo. Aunque los *routers* y los *switches* han adoptado muchas de las funciones del puente, estos siguen teniendo importancia en muchas redes. Para comprender la conmutación/switcheo y el enrutamiento, primero se debe comprender cómo funciona un puente. En la Figura 5, se puede ver dispositivos *bridges* industriales de tecnología cableada e inalámbrica.

Figura 5. Bridges cableados e inalámbricos

Un puente es un dispositivo de hardware utilizado para conectar dos redes que funcionan con el mismo protocolo. A diferencia de un repetidor, que funciona en el nivel físico, el puente funciona en el nivel lógico (Capa 2 del modelo OSI). Esto significa que puede filtrar tramas para permitir sólo el paso de aquellas cuyas direcciones de destino se correspondan con un equipo ubicado del otro lado del puente.

El puente, de esta manera, se utiliza para segmentar una red, ya que retiene las tramas destinadas a la red de área local y transmite aquellas destinadas para otras redes. Esto reduce el tráfico (especialmente las colisiones) en cada una de las redes y aumenta el nivel de privacidad, ya que la información destinada a una red no puede escucharse en el otro extremo.

Sin embargo, el filtrado que lleva a cabo el puente puede provocar una leve demora al ir de una red a otra, razón por la cual los puentes deben ubicarse con buen criterio dentro de una red.

Routers

El *router* es un dispositivo que pertenece a la capa de red del modelo OSI, es decir a la Capa 3. Al trabajar en este nivel, el *router* puede tomar decisiones basadas en grupos de direcciones de red en contraposición con las direcciones MAC de Capa 2 individuales. Los *routers* también pueden conectar distintas tecnologías de Capa 2, como por ejemplo Ethernet, Token-ring y FDDI.

El propósito de un *router* es examinar los paquetes entrantes (datos de Capa 3), elegir cuál es la mejor ruta para ellos a través de la red y luego conmutarlos hacia el puerto de salida adecuado. Los *routers* son los dispositivos de regulación de tráfico más importantes en las redes de gran envergadura.

Un *router* puede tener distintos tipos de puertos de interfaz, por ejemplo puertos seriales, puertos de consola que permiten realizar una conexión directa al *router* para poder configurarlo, puertos Ethernet, puertos para conexión a internet PSTN, ISDN, GSM, GPRS/EDGE entre otros. En la Figura 6, se pueden ver *routers* cableados e inalámbricos y un ejemplo de conexión de aplicación industrial.

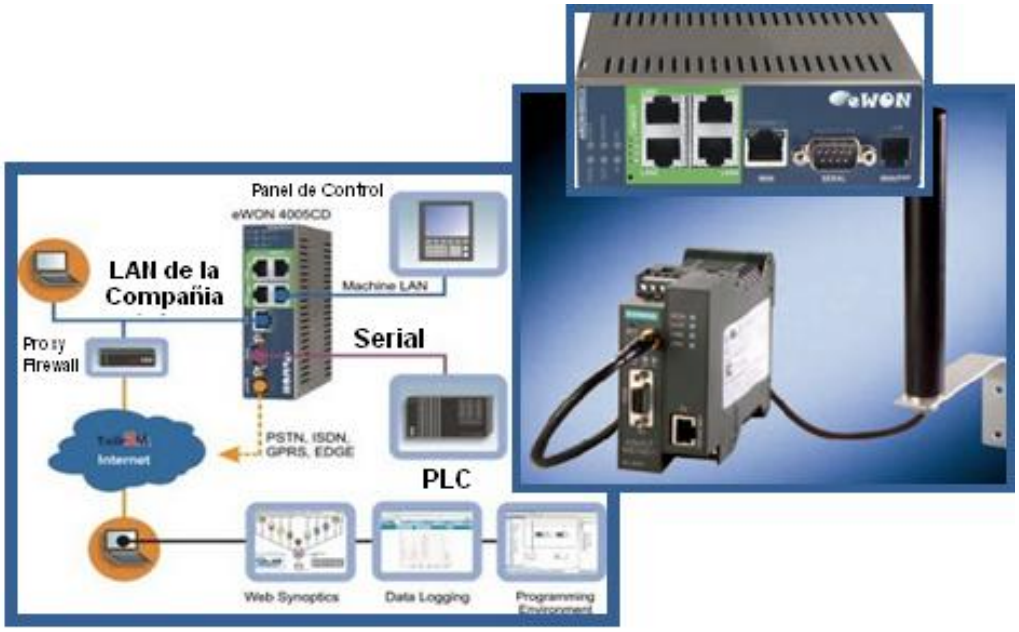

Figura 6. Router industrial Cableado e Inalámbrico

Los *routers*, pueden proporcionar conectividad dentro de las empresas, entre las empresas, entre la empresa e Internet, y en el interior de proveedores de servicios de Internet (ISP), es por ello que se ha convertido en uno de los dispositivos de red más usados en la actualidad.

Gateways

Un *gateway* o puerta de enlace, es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red al protocolo usado en la red de destino.

Figura 7. Gateway wirelessHART

Por ejemplo la familia Anybus X-Gateway tiene gran cantidad de productos diferentes, los cuales permiten conectar prácticamente todas las combinaciones posibles entre dos redes industriales. Este tipo de dispositivos hacen posible interconectar diferentes redes de bus de campo entre las cuales se pueden encontrar Profibus, DeviceNet, CANopen, CC-Link, Ethernet industrial, entre las más conocidas del mercado, como se aprecia en el ejemplo de conexión de la Figura 8 (7), en donde se ve un dispositivo *gateway* permitiendo una conexión de bus de campo a bus de campo, aquí el dispositivo actúa como esclavo en una red CC-Link y como Master / scanner en la red DeviceNet. (Figura 8.A) o una conexión de bus de campo a Ethernet (Figura 8.B), en donde el *gateway* interviene como esclavo / adaptador en la red Ethernet/IP y como maestro en la red ProfibusDP.

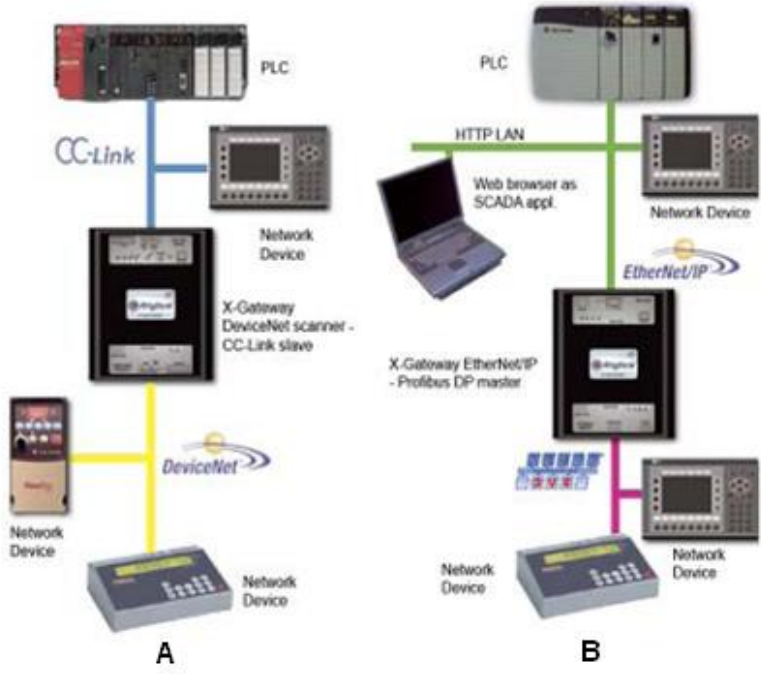

Figura 8. Ejemplo de conexión con un AnyBus X – Gateway

Estos dispositivos están diseñados de forma robusta para su uso exclusivo en plantas industriales en las que cada vez es más habitual el uso de redes industriales de diferentes proveedores, lo cual permite a los ingenieros integradores de sistemas interconectar fácilmente dos redes industriales diferentes, obteniendo un flujo de información transparente y sin pérdida de información vital a través de toda la planta industrial. Estos son dispositivos autónomos e inteligentes capaces de operar en condiciones industriales y permiten crear soluciones más flexibles y versátiles.

Sensor/Transmisor de pH WirelessHART

El modelo 6081 – P es capaz de medir pH y ORP. El transmisor inalámbrico se instala fácilmente y se une rápidamente a la red inalámbrica, lo que permite mediciones analíticas que antes era imposible debido a limitaciones físicas o económicas, o en aplicaciones en donde se necesite hacer mediciones en diferentes sitios de la planta o móviles en las cuales se puede monitorear el estado de los sensores desde el celular. Ahorro de instalación son de hasta un 90 por ciento en comparación con el servicio de cable tradicional (8).

Figura 9. Sensor/Transmisor de pH wirelessHART Modelo 6081-P de Emerson

Sensor/Transmisor de flujo/Nivel wirelessHART

Su innovador diseño, combinado con técnicas de fabricación patentadas proporciona una mejora de 10 órdenes de magnitud en su eficacia, así como una relación de gran magnitud entre los caudales máximo y mínimo con la clase de rendimiento “Ultra for Flow” (9).

Figura 10. Sensor/Transmisor de flujo/Nivel WirelessHART Modelo 3051S_F de Emerson

Sensor/Transmisor de nivel WirelessHART

Brinda eficacia con una precisión de hasta 0,065% y una relación de 100:1 entre los rangos máximo y mínimo a escala completa (“rangedown”) • El sistema soldado de fluido de llenado proporciona la mejor fiabilidad del sistema de su tipo, diafragmas ampliados y al ras de 2, 4 y 6 pulgadas, disponibles múltiples fluidos de llenado y múltiples materiales en contacto con el proceso, alertas de proceso y unidades tanto para nivel como para volumen (9).

Figura 11. Sensor de nivel WirelessHART 3051S_L

Sensor de Turbidez

Es un Sensor para la medida de la turbidez en LINEA Método nefelométrico (luz I.R.). Adecuado para la medida de turbidez con bajos caudales y valores. Diseñado para evitar la formación de burbujas de aire. Fácil limpieza y calibración además de fácil instalación.

Figura 12. Sensor de Turbidez

Sensor de Sólidos en Suspensión

El sensor Turbi-Tech 2000 permite una medida en continuo de la turbidez y los sólidos en suspensión. El sensor incorpora un mecanismo de auto limpieza que permite que la superficie óptica se mantenga limpia en todo momento.

Se encuentra disponible en dos versiones: LA para sistemas de aireación, monitorización de sólidos en suspensión y retorno de fangos activados, y versión LS indicada para monitorización de niveles inferiores de sólidos en suspensión y turbidez, en aplicaciones tales como puntos finales de efluentes (15).

Figura 13. Sensor de Sólidos en Suspensión Turbi-Tech 2000

Adaptador WirelessHART

Es un adaptador inalámbrico que podrá ser añadido a cada instrumento para que la información pueda ser transmitida de forma inalámbrica en una WSN. El adaptador puede ser alimentado a través de bucle de 4 a 20 mA o a través de otra fuente (por ejemplo, baterías, red local, solar). Esta solución constituiría un punto de bajo costo-por-punto (9).

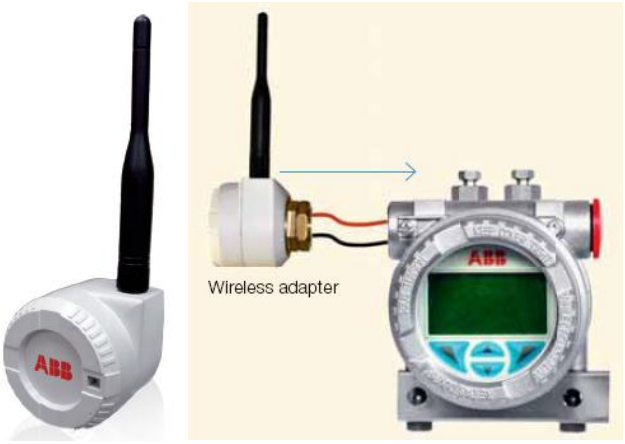

Figura 14. Adaptador WirelessHART de ABB

Dosificador automatico MICRODOS

Gracias a la regulación automática del PH MICRODOS, se decide el PH ideal para el agua a tratar. Una sonda situada en el circuito de filtración mide el PH del agua, si este es diferente al PH que desea, la bomba de inyección se pone en marcha e inyecta en el circuito de filtración la cantidad justa del corrector del PH. La bomba es de tipo peristático,

permitiendo así un funcionamiento silencioso. Tiene una alarma indica si el pH medido es inferior o superior a 8.

Figura 15. Dosificador MICODOS

APs INDOOR – OUTDOOR (11)

Los puntos de acceso de la línea de productos SCALANCE W-780 son ideales para construir redes Industrial Wireless LAN (IWLAN) a 2,4 GHz ó 5 GHz con velocidades de transferencia de hasta 54 Mbits/s. Se pueden utilizar en todas las aplicaciones que requieren gran seguridad funcional, incluso en condiciones ambientales extremadamente adversas. Fiabilidad garantizada por su caja robusta a prueba de golpes, protección contra los efectos del agua y el polvo (IP65), resistencia a choques, vibraciones y campos electromagnéticos. En la Figura 16, se pueden ver los APs INDOOR (A) y OUTDOOR (B) utilizados en el diseño de la red caso de estudio.

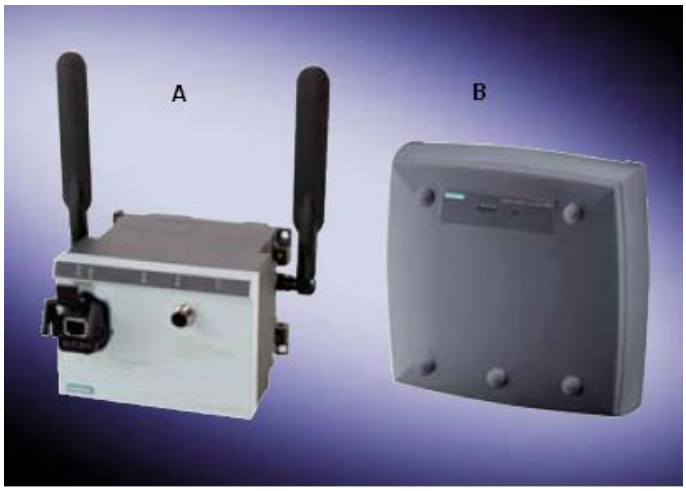

Figura 16. APs SIEMENS SCALANCE W788 (A) & SCALANCE W786 (B)

IWLAN PB Link PN IO

El IWLAN/PB Link PN IO se emplea como elemento de transición (pasarela) entre las redes Industrial Wireles LAN y PROFIBUS. La transferencia inalámbrica brinda una mayor

disponibilidad de la instalación al no estar sujeta a ningún tipo de desgaste con partes que necesiten de mantenimiento continuo.

Gracias a la utilización del IWLAN/PB Link PN IO, bien como interfaz maestro PROFIBUS o como proxy PROFINET IO, el Link es apropiado para la comunicación con sistemas de automatización en aplicaciones móviles. El uso del soporte intercambiable C-Plug para salvar datos de configuración es una gran ventaja ya que facilita el cambio de dispositivos sin necesidad de enchufar una programadora.

Figura 17. IWLAN PB Link PN IO

La posibilidad de usar PROFINET permite disfrutar de sus numerosas ventajas a nivel de sistema, por ejemplo el diagnóstico vía bus (5). En la Figura 17 se puede ver una imagen del dispositivo de comunicación inalámbrica. Es posible la adaptación hasta de dos antenas.

IE/WSN-PA LINK

IE/WSN-PA LINK es una pasarela WirelessHART para conectar una red WirelessHART a un sistema superior como por ejemplo un sistema de control de procesos o una *Maintenance Station*. El administrador de redes integrado permite configurar redes WirelessHART fácilmente y optimizar el rendimiento de la red y los ajustes de seguridad (11).

IE/WSN-PA LINK conecta equipos de campo HART inalámbricos con Industrial Ethernet por vía inalámbrica. Del lado de la conexión inalámbrica, IE/WSN-PA LINK es compatible con el estándar WirelessHART y del lado de Ethernet, con la comunicación TCP/IP y Modbus TCP.IE/WSN-PA LINK permite el diagnóstico, mantenimiento y la observación de procesos de forma inalámbrica. Es posible la adaptación de hasta dos antenas.

Figura 18. IWLAN IE/WSN-PA LINK

FIREWALL SCALANCE S612

Los Módulos de Seguridad *SCALANCE S* representan el núcleo central del concepto de seguridad de Siemens para protección de de redes y datos. La función de protección de SCALANCE S se encarga de controlar el tráfico de datos desde y hacia la célula. Los módulos de seguridad se colocan simplemente como un componente más de red antes del equipo o la red de equipos a proteger.

- Protección contra espionaje
- Protección contra manipulación
- Protege hasta 64 equipos
- Hasta 128 túneles VPN a la vez
- Rango de temperatura ampliado de -20 °C a +70 °C

Figura 19. Firewall Siemens

Antenas y accesorios para antenas

El uso de antenas separadas en los productos SCALANCE permite realizar comunicaciones inalámbricas fiables. Tienen un montaje sencillo, ya que las antenas

vienen con cable de antena y conectores R-SMA (11). Las antenas de SIMATIC NET, que ofrecen grado de protección IP65[5], se diferencian según sus características en orientadas (20° vertical, 20° horizontal) u omnidireccionales (360° horizontal, 30° vertical).

- ANT793-8DR
- ANT795-4MR
- ANT795-6MR

Figura 20. Antenas SIMATIC NET

Accesorios para antenas

Elemento protector contra rayos LP798-1PRO: El elemento de protección contra rayos LP 798-1PRO amplía las posibilidades de uso de los productos SCALANCE W-700 con antenas separadas, especialmente en exteriores

Resistencia terminal de antena TI795-1R: En los productos SCALANCE W-700, cuando se prescinde de la segunda antena, es necesario instalar una resistencia terminal de antena en el segundo conector R-SMA.

Cable de prolongación de antena FRNC: Para optimizar el montaje existe además un cable de prolongación de antena, 5m, pre conectado con dos conectores R-SMA (Disponible sólo para la variante ANT 790).

Figura 21. Protector – Terminal – Cable

Motobomba centrifuga vertical PEERLESS

Para el sistema de bombeo se definieron motobombas PEERLESS PUMP. Son motobombas centrífugas verticales modelo 12MB con motores de 160 HP y 1750 RPM. Tienen capacidad para caudales de 4500 gpm y 27 mts.

[5] Protección IP: Protección contra el contacto y la penetración de agua y suciedad.

Figura 22. Motobomba PEERLESS modelo 12MB

Válvula Hidráulica de Control

La válvula hidráulica de control BERMAD Serie 700 (19) es de un diseño hidrodinámico, con cuerpo ensanchado en forma de "Y", lo que disminuye el factor de cavitacion, con flujo directo, provocando que la perdida de carga sea menor en un 30% que las válvulas globo, y un actuador de doble camara, que permite control suave y preciso.

- La válvula es fabricada en diversas clases de presiones: clase 125, 250 y 400 ANSI B 16.1 estandar, o clase 10, 16, 25 y 40. ISO/DIN/BS 4504 estandar.
- Temperatura máxima de trabajo: 80°C (180°F).
- Diámetros disponiblles: 2" (50 mm) hasta 24" (600 mm).
- Materiales y revestimiento: a pedido especial.
- La Serie 700 BERMAD es fabricada no solo en "Y", sino asimismo en tipo ángulo, en todos los diametros.

Esta válvula cumple funciones tales como regulador de presión Sostenedor de presión, limitador de caudal, control de altura de depósitos, válvula de retención, válvula de control de bombas, válvula anticipadora de onda o contra golpe de ariete Y muchas otras aplicaciones para usos en aguas potables y residuales municipales, industria, petroquimica, edificios, sistemas contra incendio, y fluidos en general.

Figura 23. Válvula de control BERMAD Modelo 730

Por último, se tiene una imagen en la cual se puede ver aplicación de las diferentes tecnologías de comunicación para cada nivel de la pirámide de automatización CIM estudiadas en la monografía (2).

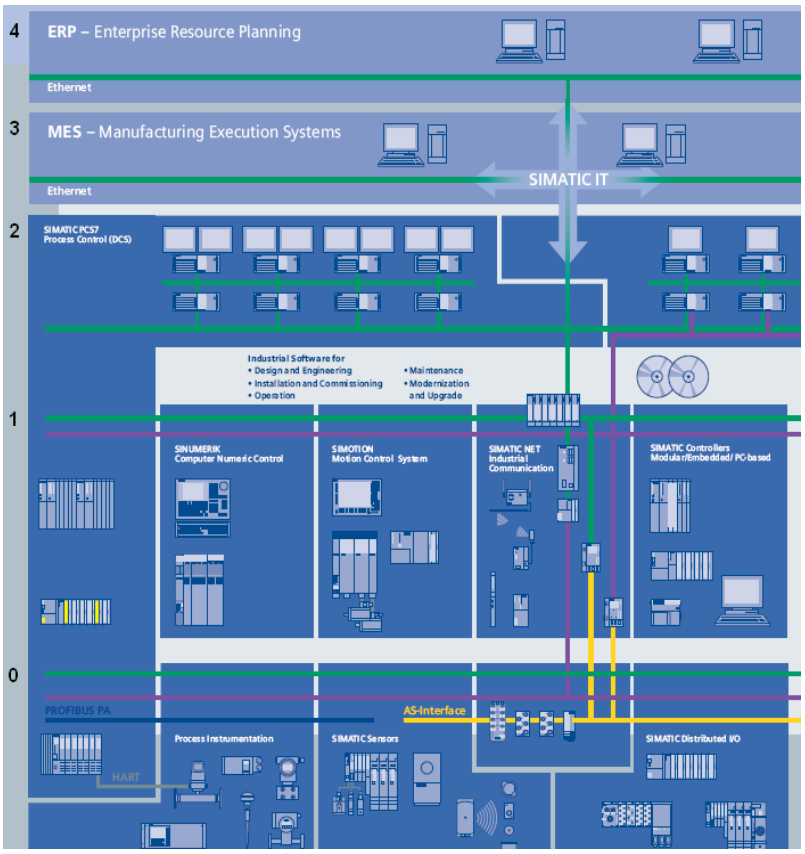

Figura 24. Integración en las Comunicaciones Industriales

ANEXO E. SIMULACIÓN

1. DIBUJOS EN PLANTA

A continuación, se toman las imágenes reales de los planos y las imágenes de los planos digitalizados para dibujar sobre ellos las delimitaciones u obstáculos (paredes, muros, etc.) con las herramientas de dibujo que proporciona el software SINEMA E, como el Editor de Modelado (*floor plan*), que ayudaran a una mejor aproximación de la simulación de las señales de RF y a simplificar la planificación e instalación de la red WLAN. Es recomendable utilizar una imagen de fondo, ya que simplifica tanto la orientación espacial durante las mediciones y la interpretación de los resultados medidos. Los dibujos o ediciones hechas sobre las imágenes de los planos se ven como líneas de color rojo.

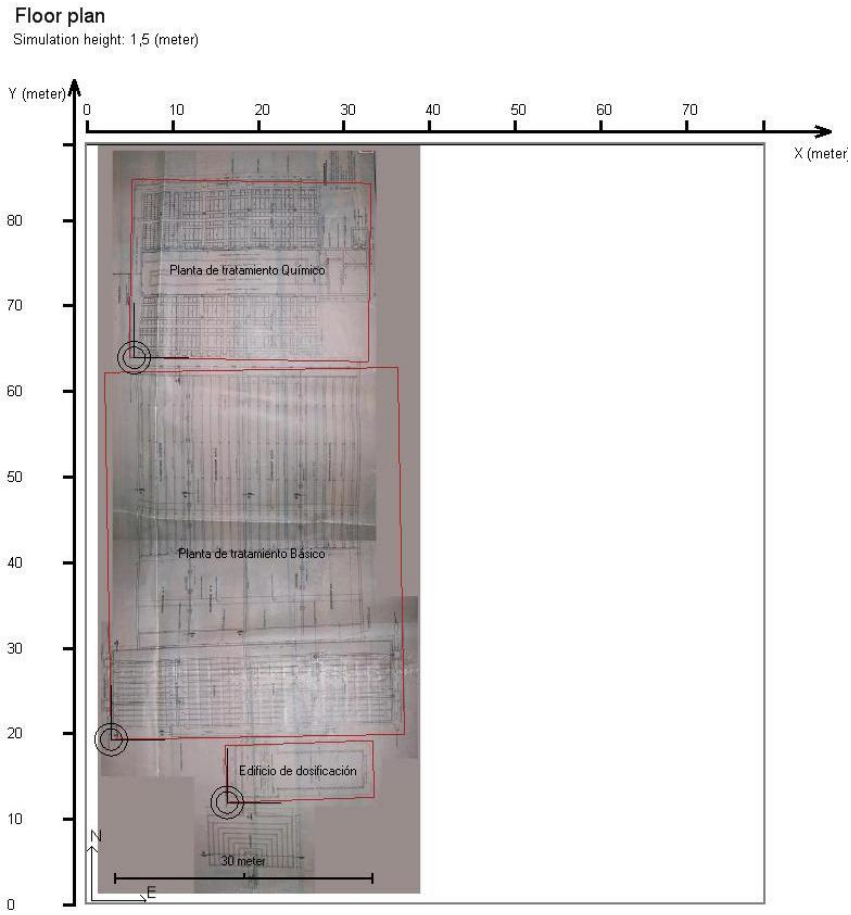

Figura 1. Floor Plan - Planta El Tablazo

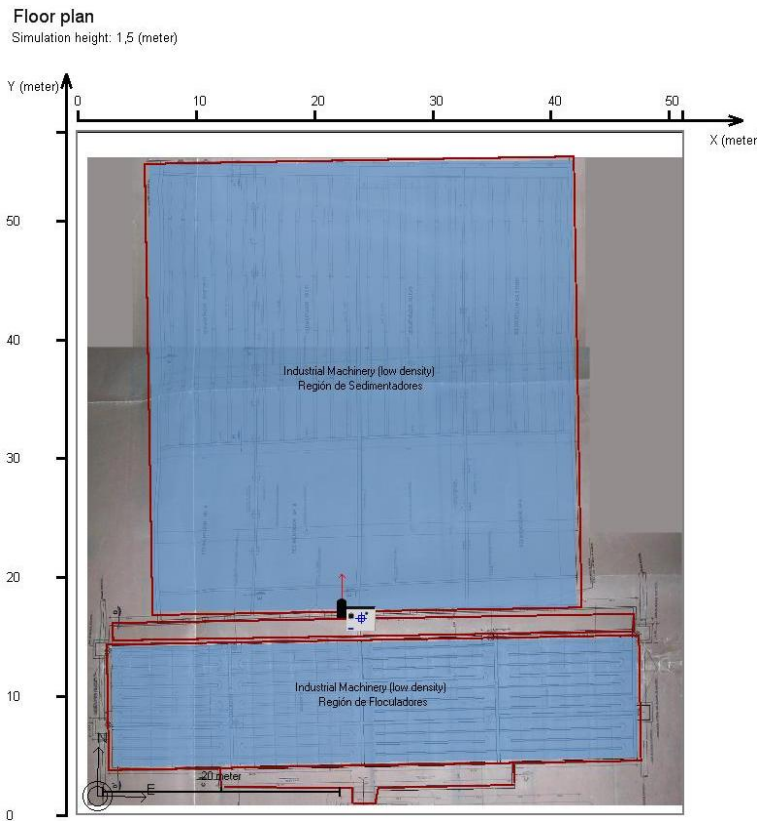

Figura 2. Floor Plan - Floculadores/Sedimentadores planta El Tablazo

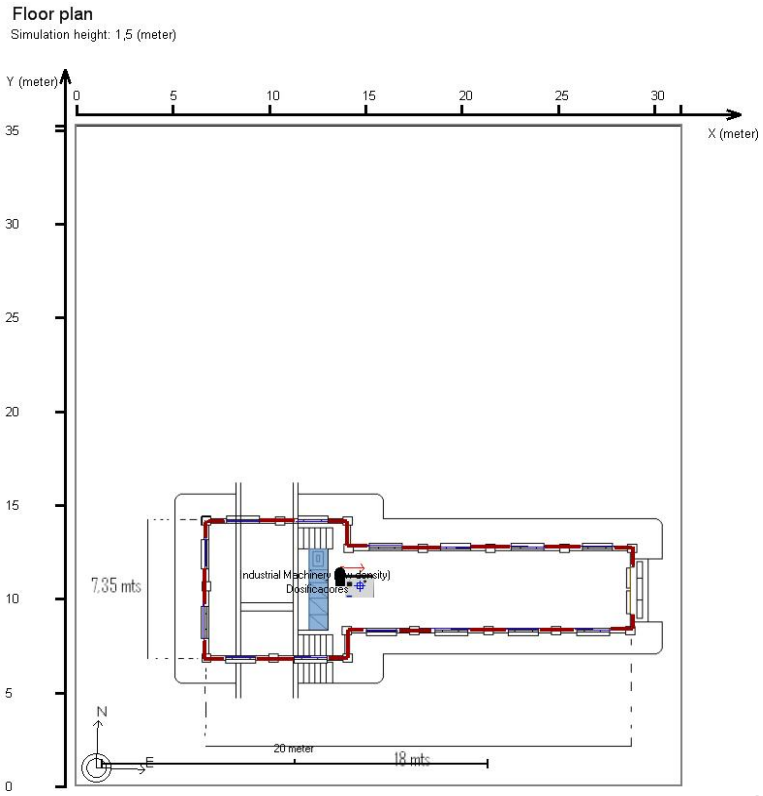

Figura 3. Floor Plan - Planta El Tablazo – Sala de dosificación

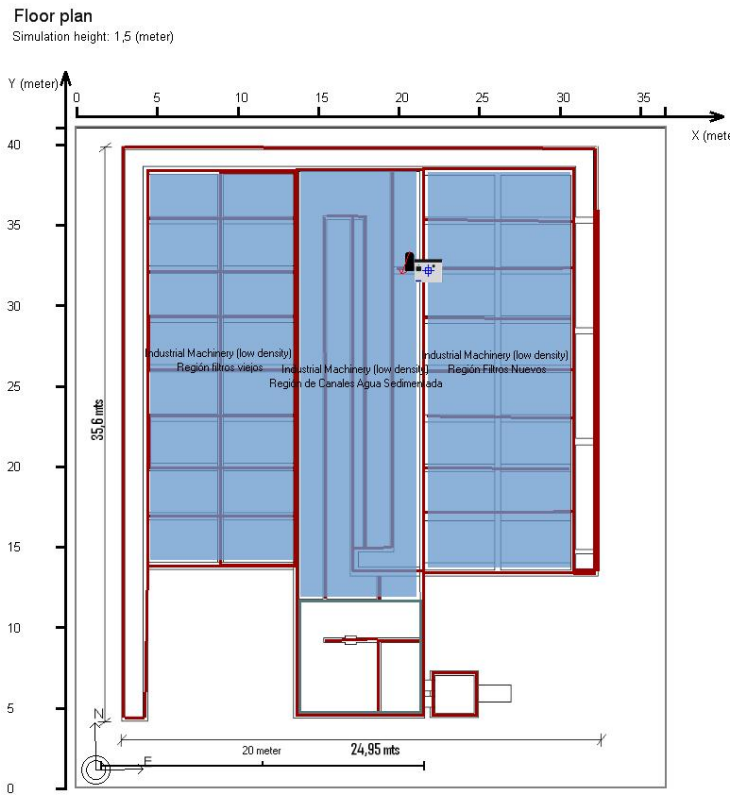

Figura 4. Floor Plan - Planta El Tablazo - Planta tratamiento químico

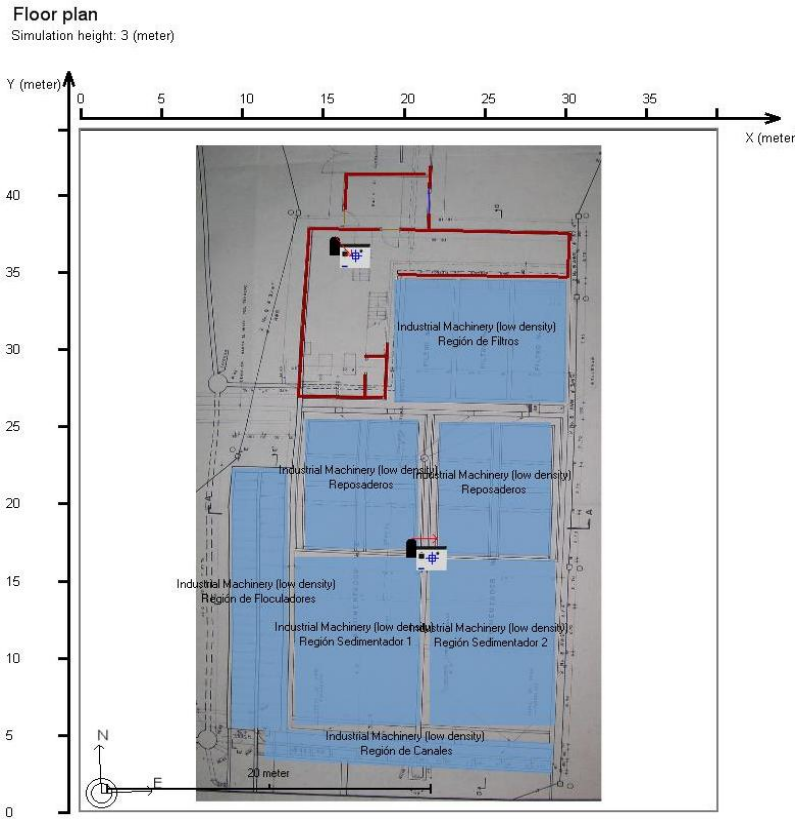

Figura 5. Floor Plan - Planta Tulcán

En las Figuras 1 a la 5, lo que se hace es definir el *floor plan* lo cual consiste en dibujar los posibles obstáculos (paredes, muros, etc.) en los planos de las plantas caso de estudio, que hay que tener en cuenta para la simulación de las señales de RF.

2. Configuración Coverage Filters

En el *Coverage Filter* se puede elegir un filtro de la lista que da el software SINEMA E, mostrando u ocultando el edificio individual, los pisos o las interfaces WLAN de los puntos de acceso. También se tiene la lista modo *wireless* en la cual se puede mostrar u ocultar las bandas de frecuencia individuales / modos WLAN, marcando o desmarcando la cajas (*checking boxes*). La visualización de las bandas de frecuencia relevantes esta entonces en mostrar u ocultar la selección para todos los dispositivos.

Tabla 1. Configuración *coverage filters* - Planta El Tablazo

Access Point Filter:	Planta del Tablazo/Planta de tratamiento Básico/Floor (1)/SCALANCE-W788-1PRO-SIEMENS-1<0> Planta del Tablazo/Edificio de dosificación/Floor (1)/SCALANCE-W788-1PRO-SIEMENS-3<0> Planta del Tablazo/Planta de tratamiento Químico/Floor (1)/SCALANCE-W788-1PRO-SIEMENS-6<0>
Selected Wireless Mode:	802.11b/g
Selected Client Type:	SCALANCE W/IWLAN PB-Link

Tabla 2. Configuración *coverage filters* - Planta Tulcán

Access Point Filter:	Planta de tratamiento/Planta de Tratamiento/Piso Planta/SCALANCE-W788-1PRO-SIEMENS-1<0> Planta de tratamiento/Planta de Tratamiento/Piso Planta/SCALANCE-W788-1PRO-SIEMENS-2<0> Planta de tratamiento/Edifico Oficinas/Piso Oficinas/SCALANCE-W788-1PRO-SIEMENS-3<0> Planta de tratamiento/Edifico Oficinas/Piso Oficinas/SCALANCE-W788-1PRO-SIEMENS-4<0>
Selected Wireless Mode:	802.11b/g
Selected Client Type:	SCALANCE W/IWLAN PB-Link

En las Tablas 1 y 2 se muestra el resultado de la configuración del *coverage filter* con la respectiva tecnología IEEE selecciona. En este caso IEEE 802.11 b/g, Los filtros de protocolos lo que hacen es impedir o permitir el uso de protocolos específicos a través del punto de acceso. Puede configurar filtros de protocolos individuales y permitir que cada filtro para una o más redes VLAN. Se puede filtrar los protocolos para los dispositivos de cliente inalámbrico, los usuarios de la red de cable, o ambos. Por ejemplo, un filtro de SNMP en el puerto de radio del punto de acceso evita que los dispositivos de cliente inalámbrico de utilizar SNMP con el punto de acceso, pero no bloquear el acceso SNMP de la red de cable. Se puede seleccionar un filtro para un edificio individualmente, o para los pisos, o interfaces WLAN de los puntos de acceso.

3. Dispositivos utilizados

Al configurar la red de radio, las coordenadas en las que los dispositivos individuales se van a instalar también puede ser extraídas del informe. Esto facilita una instalación rápida y suave y fiable de los componentes individuales. A continuación se pueden ver las tablas 3 a 6 generadas por el software de simulación, las cuales contienen la información relativa a las antenas y los dispositivos de transmisión en cada una de las plantas.

Tabla3. Access Point - Planta El Tablazo

Access Point	Model	Position
SCALANCE-W788-1PRO-SIEMENS-1	SCALANCE W788-1PRO.SIEMENS (Ver. 3.1)	Planta del Tablazo / Planta de tratamiento Básico / Floor (1)
SCALANCE-W788-1PRO-SIEMENS-3	SCALANCE W788-1PRO.SIEMENS (Ver. 3.1)	Planta del Tablazo / Edificio de dosificación / Floor (1)
SCALANCE-W788-1PRO-SIEMENS-6	SCALANCE W788-1PRO.SIEMENS (Ver. 3.1)	Planta del Tablazo / Planta de tratamiento Químico / Floor (1)

Tabla4. Access Point - Planta Tulcán

Access Point	Model	Position
SCALANCE-W788-1PRO-SIEMENS-1	SCALANCE W788-1PRO.SIEMENS (Ver. 3.1)	Planta de tratamiento / Planta de Tratamiento / Piso Planta
SCALANCE-W788-1PRO-SIEMENS-2	SCALANCE W788-1PRO.SIEMENS (Ver. 3.1)	Planta de tratamiento / Planta de Tratamiento / Piso Planta
SCALANCE-W788-1PRO-SIEMENS-3	SCALANCE W788-1PRO.SIEMENS (Ver. 3.1)	Planta de tratamiento / Edifico Oficinas / Piso Oficinas
SCALANCE-W788-1PRO-SIEMENS-4	SCALANCE W788-1PRO.SIEMENS (Ver. 3.1)	Planta de tratamiento / Edifico Oficinas / Piso Oficinas

Tabla5. Antenas - Planta El Tablazo

Antenna	Access Point	Position
ANT795-4MR	SCALANCE-W788-1PRO-SIEMENS-1	Planta del Tablazo / Planta de tratamiento Básico / Floor (1)
ANT795-4MR	SCALANCE-W788-1PRO-SIEMENS-3	Planta del Tablazo / Edificio de dosificación / Floor (1)
ANT795-4MR	SCALANCE-W788-1PRO-SIEMENS-6	Planta del Tablazo / Planta de tratamiento Químico / Floor (1)

Tabla 6. Antenas - Planta Tulcán

Antenna	Access Point	Position
ANT795-4MR	SCALANCE-W788-1PRO-SIEMENS-1	Planta de tratamiento / Planta de Tratamiento / Piso Planta
ANT795-4MR	SCALANCE-W788-1PRO-SIEMENS-2	Planta de tratamiento / Planta de Tratamiento / Piso Planta
IWLAN Rcoax	SCALANCE-W788-1PRO-SIEMENS-3	Planta de tratamiento / Edifico Oficinas / Piso Oficinas
IWLAN Rcoax	SCALANCE-W788-1PRO-SIEMENS-4	Planta de tratamiento / Edifico Oficinas / Piso Oficinas

En las Tablas 3, 4, 5 y 6, se muestran la lista de dispositivos utilizados para la simulación en cada una de las plantas es decir los APs con sus respectivas.

4. Signal Quality

A continuación se muestran las imágenes arrojadas por la simulación las cuales muestran la calidad de la señal representado por colores en cada una de las zonas de las plantas de tratamiento de agua.

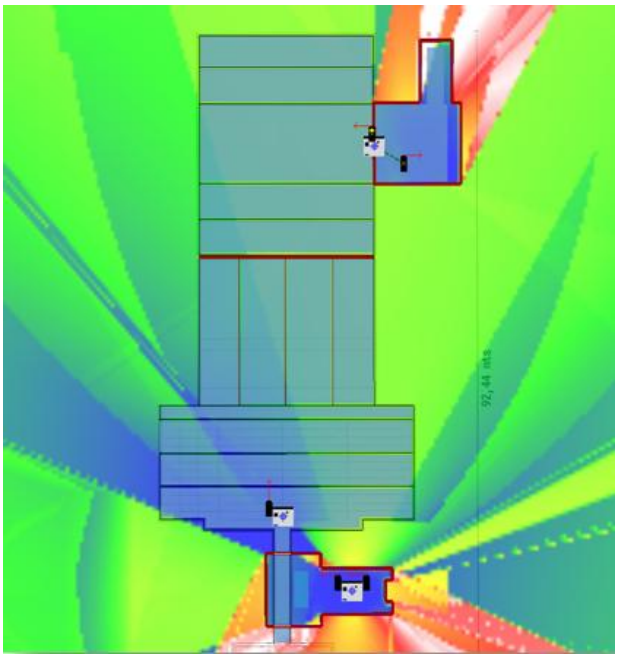

Figura 6. Signal Quality - Floculadores/Sedimentadores planta El Tablazo

La Figura 6 muestra la calidad de señal del AP IE/WSN.PA LINK, aquí se puede apreciar que coincide con el *Signal Strength* mostrado en el capitulo 4 sección 4.8.2.., la calidad de señal está ligada de esta, por lo tanto se puede verificar que las medidas están entre el 90 y el 100 de SIRN, garantizando que la calidad de señal es muy buena, por lo cual no se van a tener problemas de interferencia en esta zona.

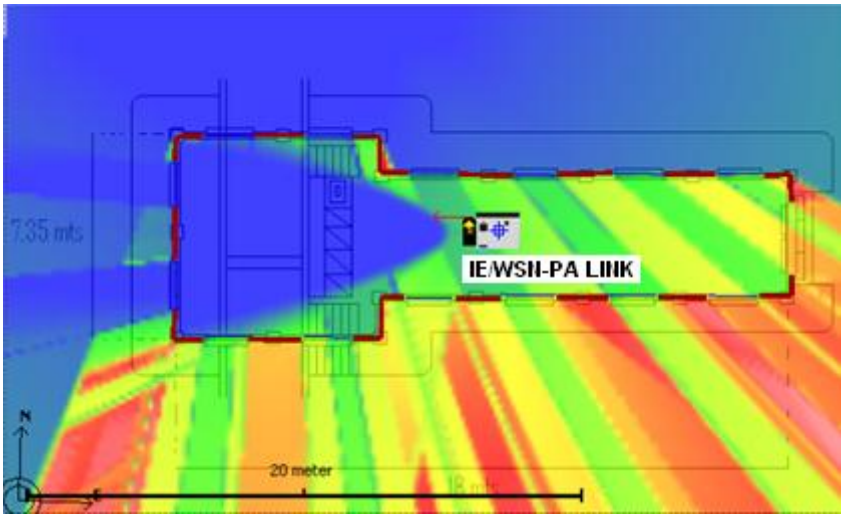

Figura 7. Signal Quality - Sala de Dosificación planta El Tablazo

La Figura 7, muestra la calidad de señal para el proceso de dosificación, se puede observar que los niveles están de casi el 100 dBm (color azul) para la zona de los medidores, se garantiza una vez más que la calidad es muy buena. Para la zona de verde y amarillo también existe una buena calidad que está entre los 60 y 90 dBm, por lo tanto

cumple con los estándares, garantizando pocas posibilidades de interferencia para equipos portátiles de medición.

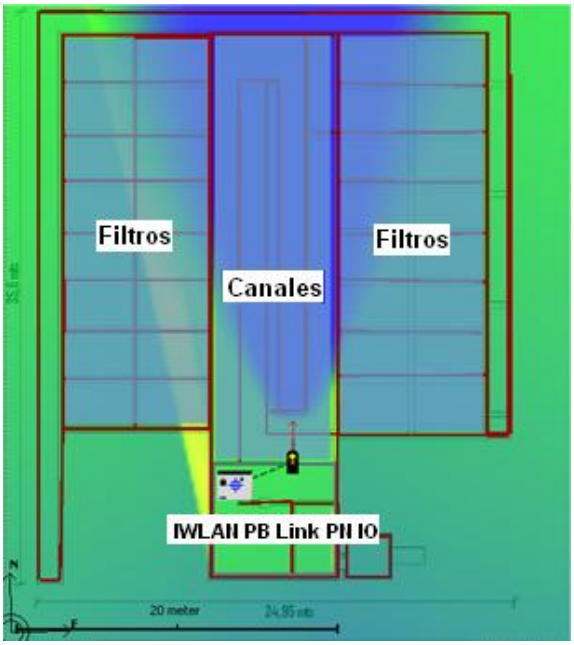

Figura 8. Signal Quality - Filtros planta El Tablazo

La zona de filtros también cumple con los estándares de calidad de señal como se ve en la Figura 8, para las zonas de mediciones de flujo para el control de válvulas corresponde a los estándares permitidos, además en las zonas más alejadas del AP se tienen mediciones que superan los 60 dBm y se garantiza que las interferencias son de poco probables.

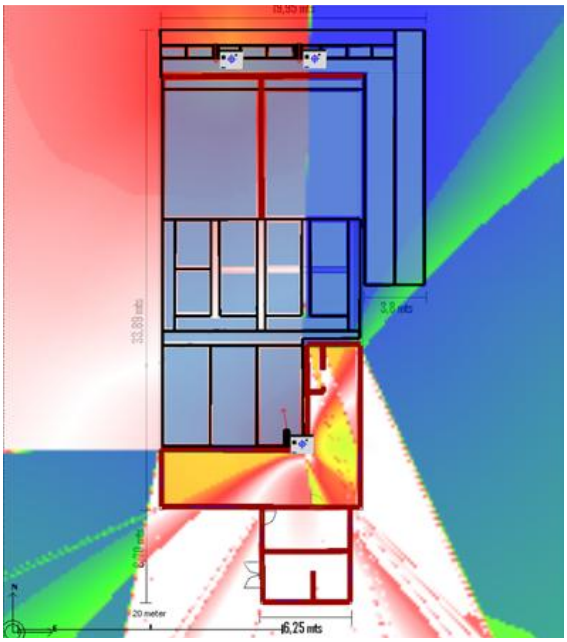

Figura 9. Signal Quality - Planta Tulcán

En la Figura 9 se puede observar la simulación del *Signal Quality* para la planta de Tulcán, en ella hay una zona media donde la señal esta por los 60 dBm aunque estas mediciones garantizan buena calidad siempre es deseable estar por los 100 dBm como se ve en la mayoría de las zonas, si se garantiza que los AP tengan una potencia máxima de -3 dBm, se logra buena calidad de la señal, pero si se lleva la potencia de los AP por encima de -3 dBm no se puede garantizar la buena calidad ya que cada AP podría interferir en el otro. Los valores de la señal según su color se pueden ver en la Figura 10.

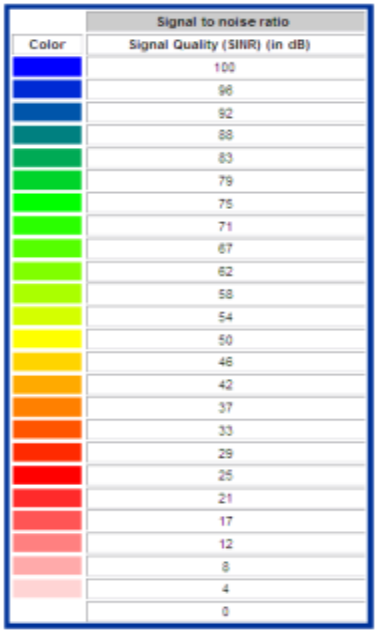

Figura 10. Signal Quality - Leyenda de colores

La leyenda muestra los colores correspondientes a las medidas de la calidad de señal en dBm, las medidas superiores a 30 dBm garantizan una señal muy buena la cual corresponde a los colores por encima del naranja, para medidas entre 20 dBm y 30 dBm la señal es satisfactoria (colores del naranja al amarillo), pero para las señales por debajo de 20 dBm no se puede garantizar una buena calidad de señal según los estándares (por debajo del rojo).

Tabla 7. Niveles de la calidad de recepción

SINR	Calidad de la recepción
≥ 30 dB	Muy buena
20 dB ≤ SINR < 30 dB	Buena a satisfactoria
10 dB ≤ SINR < 20 dB	Adecuada a pobre
< 10 dB	No hay recepción

5. Strongest AP

En esta sección, lo que se pretende es confrontar la fuerza de las señales de RF de cada uno de los APs configurados con respecto a los otros. Esta una opción de simulación muy útil cuando se tienen zonas donde hay más de un AP cerca.

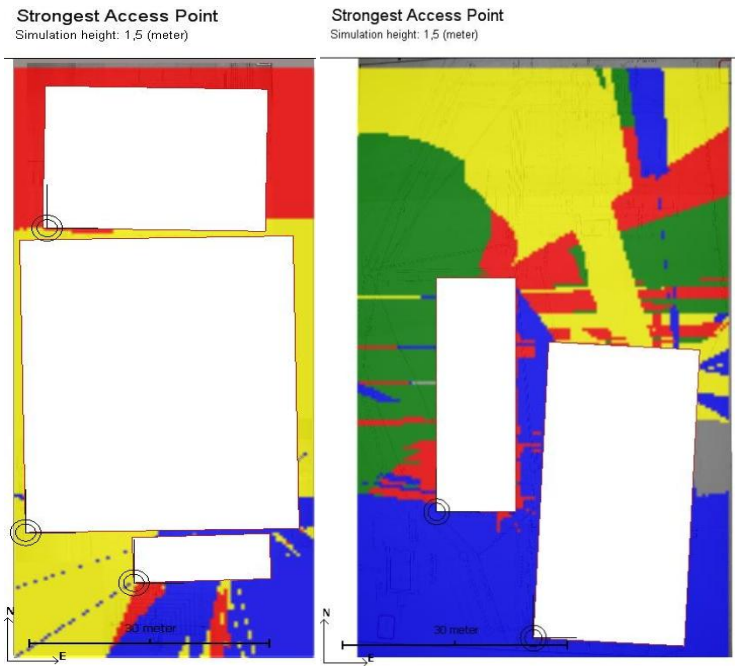

Figura 11. Strongest Access Point Plan de piso - Plantas Tablazo y Tulcán

En la Figura 11, se puede ver la fuerza de las señales de los APs en la totalidad de las plantas, cada APs configurado tiene un color de señal como se ve en la Figura 17.

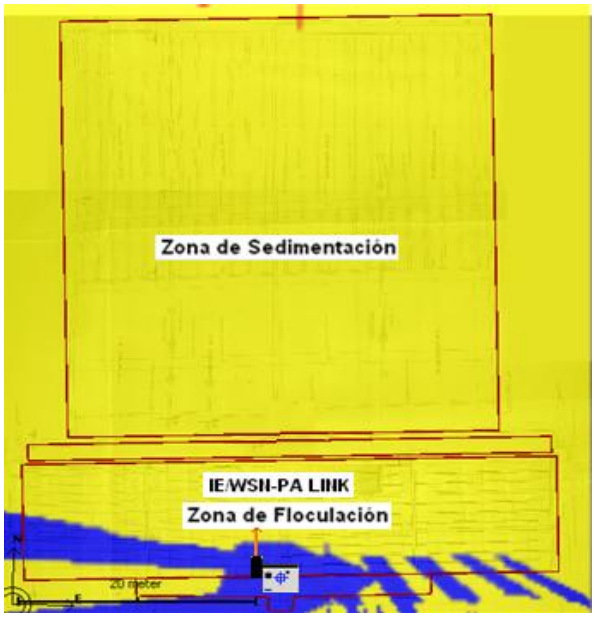

Figura 12. Strongest Access Point - Floculadores/Sedimentadores planta El Tablazo

La Figura 12, muestra el dominio del *Access Point* para el proceso de tratamiento básico (color amarillo), como era de esperarse se puede observar que el AP que se ve en la Figura 12 tiene mayor fuerza en la zona de los Floculadores/Sedimentadores, aunque en la zona inferior se ve influenciado por el AP de la sala de dosificación (color azul), se puede definir entonces que la ubicación del AP como se ve en la grafica de arriba es optima.

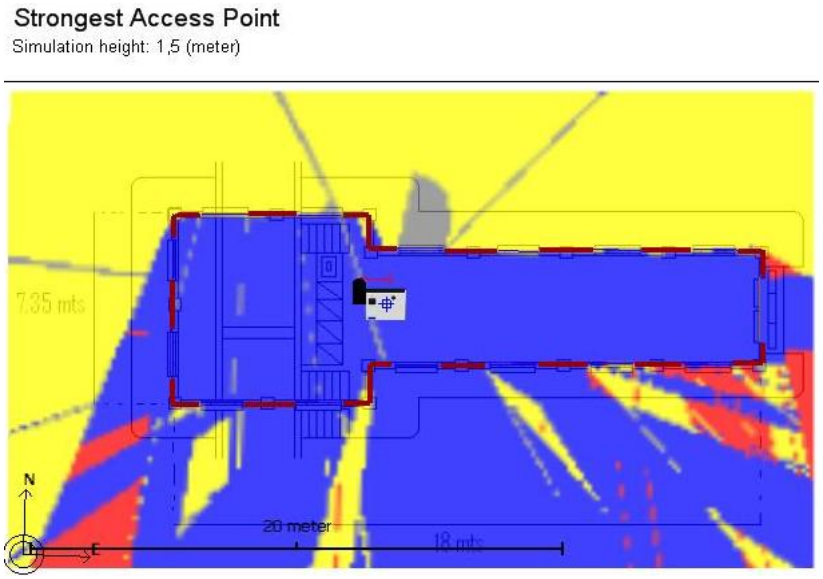

Figura 13. Strongest Access Point - Sala de Dosificación planta El Tablazo

El *Access Point* para el proceso de dosificación (Figura 13) es el mostrado en color azul, en la simulación se garantiza que el AP dominante para la zona de dosificación es el esperado.

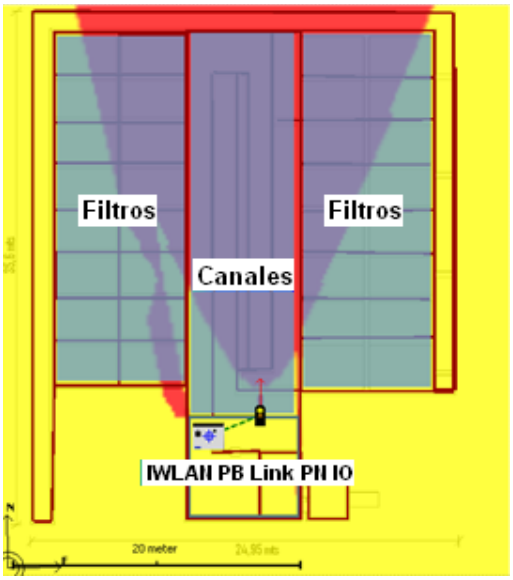

Figura 14. Strongest Access Point - Filtros planta El Tablazo

La Figura 14 muestra la simulación del *Strongest Access Point* para la zona de filtros de la planta El Tablazo, en ella se puede ver que está influenciada por dos APs, el color rojo muestra la influencia del AP determinado para la zona en cuestión, aunque demarca la zona para la cual fue diseñada también se observa la presencia de un segundo AP (color amarillo), se puede observar entonces que en un momento dado se logra cubrir la demanda de potencia de señal para algún mantenimiento o fallo del tercer AP.

La Figura 15, se muestra la zona de dominio del *Access Point* de la planta El Tablazo, si se situara un AP en la sala de cloración (color amarillo) y otro en la zona de los sedimentadores (color azul). Es claro que el AP dominante seria el azul.

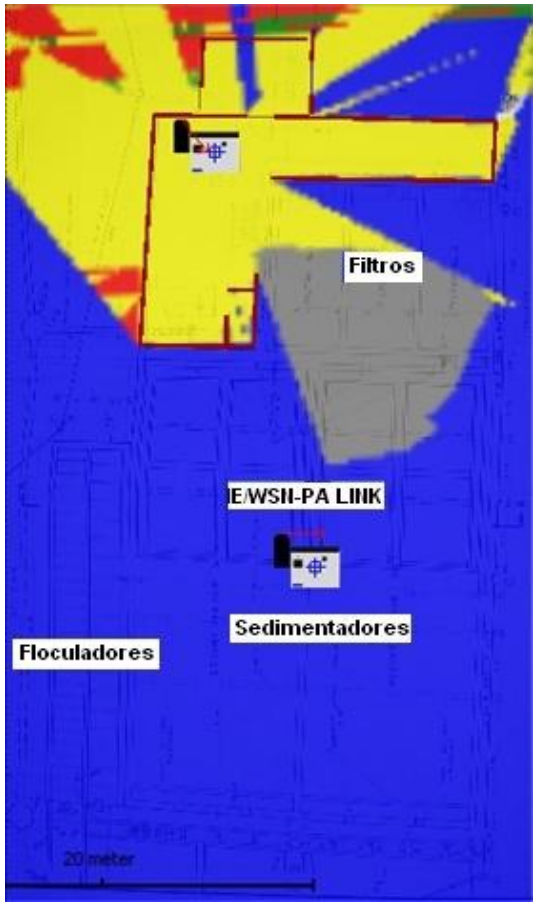

Figura 15. Strongest Access Point - Planta Tulcán

	Strongest access point
Color	Access Point
	SCALANCE-W788-1PRO-SIEMENS-2 <1>
	SCALANCE-W788-1PRO-SIEMENS-3 <1>
	SCALANCE-W788-1PRO-SIEMENS-4 <1>
	SCALANCE-W788-1PRO-SIEMENS-1 <1>
	SCALANCE-W788-1PRO-SIEMENS-2 <1>
	SCALANCE-W788-1PRO-SIEMENS-1 <1>
	SCALANCE-W788-1PRO-SIEMENS-3 <1>
	SCALANCE-W788-1PRO-SIEMENS-4 <1>

Figura 16. Strongest Access Point - Leyenda de colores

Los resultados anteriores indican el área de dominio de un AP particular, dónde el área de cada celda para cada velocidad depende de la potencia de recepción de cada AP. Para la menor velocidad de 10 Mbps se consiguen las celdas más grandes, mientras que para velocidades más grandes se presentan celdas más pequeñas debido a que el nivel umbral aumenta en proporción de la velocidad, concluyendo así que a medida que aumenta la velocidad el tamaño de celdas disminuye y que depende de la intensidad de la señal.

6. Data Rate

En las siguientes simulaciones se puede ver el *data rate* o velocidad de transmisión de datos en cada una de las zonas definidas para la simulación. En la Figura 27, se puede corroborar la velocidad en cada simulación según su color.

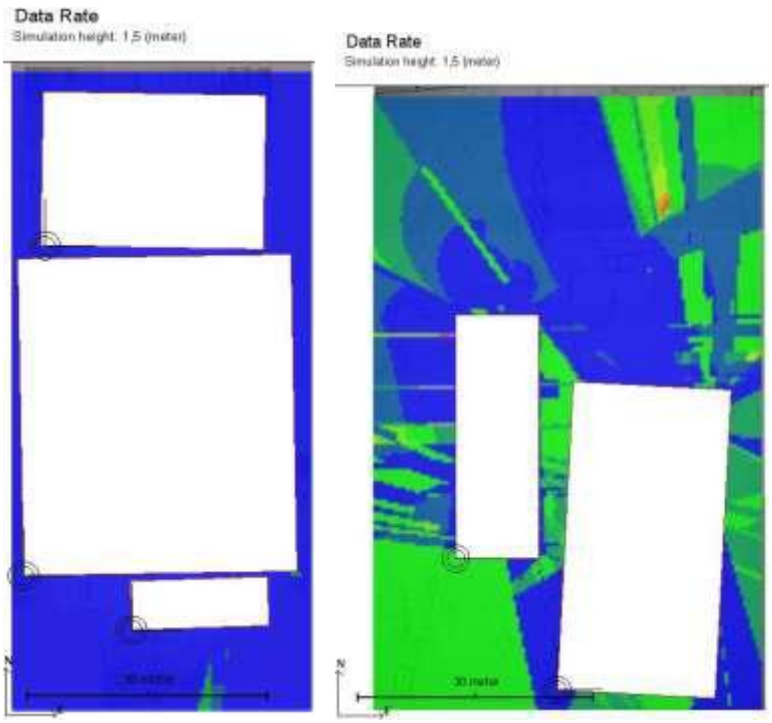

Figura 17. Date Rate Planeación de sitio - Plantas Tablazo y Tulcán

La Figura 17, muestra el *data rate* para las plantas de El Tablazo y Tulcán respectivamente y en la cual se observa que hay un *data rate* optimo el cual va desde los 54 Mbps (azul) y baja hasta los 24 Mbps para algunas pocas zonas.

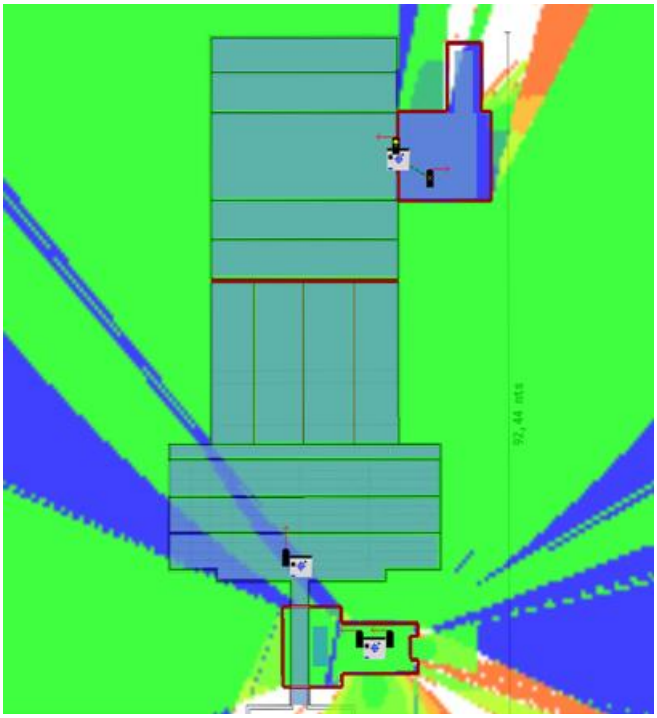

Figura 18. Date Rate - Floculadores/Sedimentadores planta El Tablazo

Figura 19. Date Rate Planeación de sitio - Sala de dosificación - El Tablazo

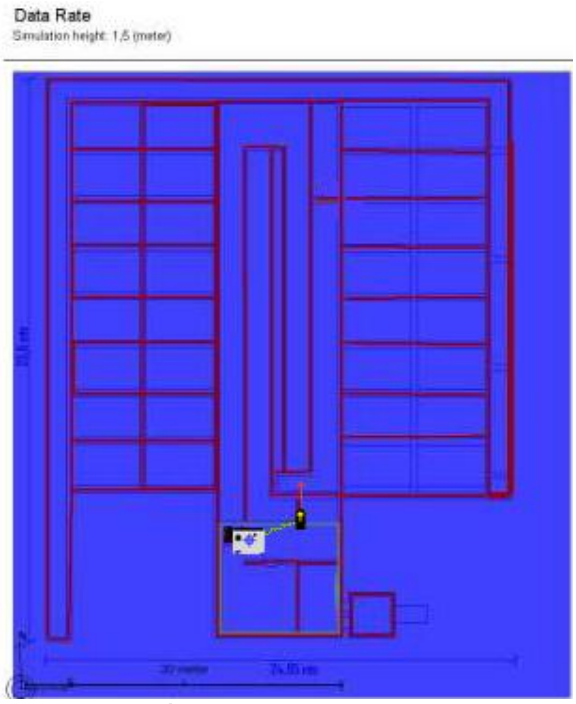

Figura 20. Date Rate Planeación de sitio - Proceso de dosificación – El Tablazo

Figura 21. Date Rate Planeación de sitio - Proceso de dosificación - Tulcan

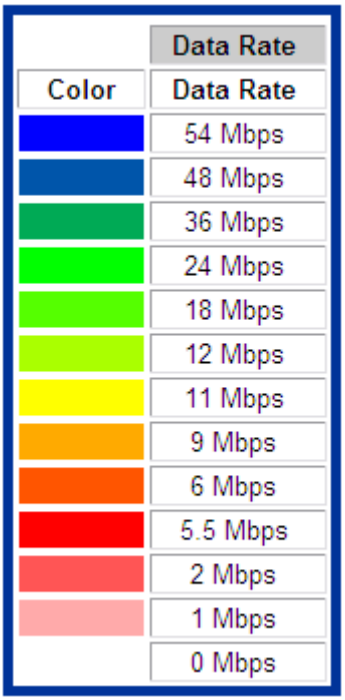

Figura 22. Date Rate - leyenda de colores

Se puede concluir, que para todas las zonas de simulación se obtiene una buena transmisión de datos (*data rate*) optima de 54 Mbps como se ve en las graficas anteriores y disminuye un poco en algunas zonas hasta 24 Mbps pero no más bajo de ahí para los objetivos de la red caso de estudio

ANEXO F. TRATAMIENTO DEL AGUA

1. PROCESO DE TRATAMIENTO DE AGUA

Las diversas actividades agrícolas, ganaderas, industriales y recreacionales del ser humano han traído como consecuencia la contaminación de las aguas superficiales con sustancias químicas y microbiológicas, además del deterioro de sus características estéticas.

Para hacer frente a éste problema, es necesario someter al agua a una serie de operaciones o procesos unitarios, a fin de purificarla o potabilizarla para que pueda ser consumida por los seres humanos.

Este proceso como la mayoría, tiene diferentes fases indispensables a seguir para la obtención de resultados favorables, en este caso lograr que el agua que corre por la ciudad de Popayán sea apta para el consumo de sus habitantes. Estas fases se agrupan en unos determinados procesos de transferencia. Estos son:

- Transferencia de sólidos.
- Transferencia de iones.
- Transferencia de gases.
- Transferencia molecular o de nutrientes.

A continuación se muestra una visión general de dichos procesos y las correspondientes fases que agrupa.

1.1 TRANSFERENCIA DE SÓLIDOS

El proceso de transferencia de sólidos se constituye de las fases siguientes:

FASE 1: CERNIDO

Consiste en hacer pasar el agua a través de rejas o tamices, los cuales retienen los sólidos de tamaño mayor a la separación de las barras, como ramas, palos y toda clase de residuos sólidos que puedan venir con el agua. El agua que se trata en la planta de El Tablazo proviene del Rio las Piedras e ingresa por una bocatoma que está a 10 kilómetros de distancia de la planta. También está considerado en esta clasificación el microcernido, que consiste básicamente en triturar las algas reduciendo su tamaño para que puedan ser removidas mediante sedimentación.

FASE 2: SEDIMENTACIÓN

Consiste en promover condiciones de reposo en el agua, para remover, mediante la fuerza gravitacional, las partículas en suspensión más densas. Este proceso se realiza en

los desarenadores, presedimentadores, sedimentadores y decantadores, en estos últimos, con el auxilio de la coagulación.

FASE 3: FLOTACIÓN

El objetivo de éste proceso es promover condiciones de reposo, para que los sólidos cuya densidad es menor que la del agua asciendan a la superficie de la unidad de donde son retirados por desnatado. Para mejorar la eficiencia del proceso, se emplean agentes de flotación. Mediante este proceso se remueven especialmente grasas, aceites, turbiedad y color. Los agentes de flotación empleados son sustancias espumantes y microburbujas de aire.

FASE 4: FILTRACIÓN

Consiste en hacer pasar el agua a través de un medio poroso, normalmente de arena, en el cual actúan una serie de mecanismos de remoción cuya eficiencia depende de las características de la suspensión (agua más partículas) y del medio poroso. Este proceso se utiliza como único tratamiento cuando las aguas son muy claras o como proceso final de pulimento en el caso de aguas turbias.

Los medios porosos utilizados además de la arena —que es el más común —son la antracita, el granate, la magnetita, el carbón activado, la cáscara de arroz, la cáscara de coco quemada y molida y también el pelo de coco en el caso de los filtros rápidos. En los filtros lentos lo más efectivo es usar exclusivamente arena; no es recomendable el uso de materiales putrescibles.

1.2 TRANSFERENCIA DE IONES

FASE 5: COAGULACIÓN QUÍMICA

La coagulación química consiste en adicionar al agua una sustancia que tiene propiedades coagulantes, la cual transfiere sus iones a la sustancia que se desea remover, lo que neutraliza la carga eléctrica de los coloides para favorecer la formación de flóculos de mayor tamaño y peso. Los coagulantes más efectivos son las sales trivalentes de aluminio y fierro. Las condiciones de pH y alcalinidad del agua influyen en la eficiencia de la coagulación. Este proceso se utiliza principalmente para remover la turbiedad y el color.

FASE 6: PRECIPITACIÓN QUÍMICA

La precipitación química consiste en adicionar al agua una sustancia química soluble cuyos iones reaccionan con los de la sustancia que se desea remover, formando un precipitado. Tal es el caso de la remoción de hierro y de dureza carbonatada (ablandamiento), mediante la adición de cal.

FASE 7: INTERCAMBIO IÓNICO

Como su nombre lo indica, este proceso consiste en un intercambio de iones entre la sustancia que desea remover y un medio sólido a través del cual se hace pasar el flujo de agua. Este es el caso del ablandamiento del agua mediante resinas, en el cual se realiza un intercambio de iones de cal y magnesio por iones de sodio, al pasar el agua a través de un medio poroso constituido por zeolitas de sodio. Cuando la resina se satura de iones de calcio y magnesio, se regenera introduciéndola en un recipiente con una solución saturada de sal.

FASE 8: ABSORCIÓN

La absorción consiste en la remoción de iones y moléculas presentes en la solución, concentrándolos en la superficie de un medio adsorbente, mediante la acción de las fuerzas de interfaz. Este proceso se aplica en la remoción de olores y sabores, mediante la aplicación de carbón activado en polvo.

1.3 TRANSFERENCIA DE GASES

FASE 9: AIREACIÓN DEL AGUA

La aireación se efectúa mediante caídas de agua en escaleras, cascadas, chorros y también aplicando el gas a la masa de agua mediante aspersión o burbujeo. Se usa en la remoción de hierro y manganeso, así como también de anhídrido carbónico, ácido sulfhídrico y sustancias volátiles, para controlar la corrosión y olores.

FASE 10: DESINFECCIÓN

Consiste en la aplicación principalmente de gas cloro y ozono al agua tratada.

FASE 11: RECARBONATACIÓN

Consiste en la aplicación de anhídrido carbónico para bajar el pH del agua, normalmente después del ablandamiento.

1.4 TRANSFERENCIA MOLECULAR

Las bacterias saprofitas degradan la materia orgánica y transforman sustancias complejas en material celular vivo o en sustancias más simples y estables, incluidos los gases de descomposición. También los organismos fotosintéticos convierten sustancias inorgánicas simples en material celular, utilizando la luz solar y el anhídrido carbónico producto de la actividad de las bacterias y, a la vez, generan el oxígeno necesario para la supervivencia de los microorganismos aeróbicos presentes en el agua.

2. TIPOS DE PLANTAS DE TRATAMIENTO DE AGUA O PLANTAS POTABILIZADORAS

Una planta de tratamiento es una secuencia de operaciones o procesos unitarios, convenientemente seleccionados con el fin de remover totalmente los contaminantes microbiológicos presentes en el agua cruda y parcialmente los físicos y químicos, hasta llevarlos a los límites aceptables estipulados por las normas.

Existe una clasificación para las plantas de tratamiento de agua, éstas se pueden dar de acuerdo con el tipo de procesos que las conforman, en:

- Plantas de filtración rápida.
- Plantas de filtración lenta.

2.1 PLANTAS DE FILTRACIÓN RÁPIDA

Estas plantas se denominan así porque los filtros que las integran operan con velocidades altas, entre 80 y 300 m3/m2.d, de acuerdo con las características del agua, del medio filtrante y de los recursos disponibles para operar y mantener estas instalaciones.

Como consecuencia de las altas velocidades con las que operan estos filtros, se colmatan en un lapso de 40 a 50 horas en promedio. En esta situación, se aplica el retrolavado o lavado ascensional de la unidad durante un lapso de 5 a 15 minutos (dependiendo del tipo de sistema de lavado) para descolmatar el medio filtrante devolviéndole su porosidad inicial y reanudar la operación de la unidad.

Las plantas de filtración rápida a su vez se dividen en dos clases de acuerdo con la calidad del agua que se va a tratar, estas son:

- Plantas de filtración rápida completa.
- Plantas de filtración directa.

i. Planta de filtración rápida completa

Una planta de filtración rápida completa normalmente está integrada por los procesos de coagulación, decantación, filtración y desinfección. El proceso de coagulación se realiza en dos etapas: una fuerte agitación del agua para obtener una dispersión instantánea de la sustancia coagulante en toda la masa de agua *(mezcla rápida)* seguida de una agitación lenta para promover la rápida aglomeración y crecimiento del floculo *(etapa de floculación).*

La coagulación tiene la finalidad de mejorar la eficiencia de remoción de partículas coloidales en el proceso de decantación (sedimentación de partículas floculentas). El proceso final de filtración desempeña una labor de acabado, le da el pulimento final al agua.

De acuerdo con las investigaciones realizadas por la Agencia de Protección Ambiental (EPA) de los Estados Unidos, el filtro debe producir un efluente con una turbiedad menor o igual a 0,10 UNT[6] para garantizar que esté libre de huevos de parásitos. Para lograr esta eficiencia en la filtración, es necesario que los decantadores produzcan un agua con 2 UNT como máximo.

Finalmente, se lleva a cabo la desinfección, proceso común a los dos tipos de plantas, las de filtración rápida completa y las de filtración directa. La función principal de éste proceso es completar la remoción de microorganismos patógenos que no quedaron retenidos en el filtro y servir de protección contra la contaminación que el agua pueda encontrar en el sistema de distribución.

Tabla 1. Límites de calidad del agua aceptables para el tratamiento mediante filtración rápida completa

Parámetros	90% del tiempo	80% del tiempo	Esporádicamente
Turbiedad (UNT)	< 1.000	< 800	< 1.500; si excede, considerar presedimentación
Color (UC)	< 150	< 70	
NMP de coliformes termotolerantes/100 mL	< 600		Si excede de 600, se debe considerar predesinfección

La desinfección, en la forma en que normalmente se aplica (esto es, con residual libre de 1 mg/L a la salida de la planta y tiempo de contacto mínimo de 30 minutos), solo tiene la capacidad de remover bacterias. Como se verá detalladamente en el capítulo sobre desinfección, para remover huevos de parásitos se necesitarían aplicar dosis altísimas y disponer de tiempos de contacto muy largos, que hacen impracticable el proceso. Como los huevos de parásitos son grandes, un filtro que opere eficientemente y reciba agua con no más de 2 UNT puede producir un efluente exento de huevos de parásitos (12). En la Tabla 1 se pueden ver los límites óptimos de calidad del agua por medio del tratamiento de filtración rápida completa.

[6] UNT: Unidades Nefelométricas de Turbidez

ii. Plantas de filtración directa

Es una alternativa a la filtración rápida, constituida por los procesos de mezcla rápida y filtración, apropiada solo para aguas claras. Son ideales para este tipo de solución las aguas provenientes de embalses o represas, que operan como grandes pre sedimentadores y proporcionan aguas constantemente claras y poco contaminadas.

Cuando la fuente de abastecimiento es confiable —caso de una cuenca virgen o bien protegida—, en la que la turbiedad del agua no supera de 10 a 20 UNT el 80% del tiempo, y no supera 30 UNT ni 25 UC el 90% del tiempo, puede considerarse la alternativa de emplear *filtración directa descendente.*

Cuando el agua viene directamente del río y aunque clara la mayor parte del año, presenta frecuentes fluctuaciones de turbiedad, normalmente se considera una floculación corta, generalmente de no más de 6 a 8 minutos, para obtener un efluente de calidad constante, aunque con carreras de filtración más cortas. Esta es la alternativa más restringida de todas en cuanto a la calidad de agua que se va a tratar.

Tabla 2. Límites de calidad del agua para plantas de filtración directa

Alternativa	Parámetros	90% del tiempo	80% del tiempo	Esporádicamente
Filtración directa descendente	Turbiedad (UNT)	25 - 30	<20	< 50
	Color verdadero (UC)	< 25		
	NMP de coliformes totales/100 mL	< 2.500		
	Concentración de algas (unidades/mL)	< 200		
Filtración directa ascendente	Turbiedad (UNT)	< 100	< 50	< 200
	Color (UC)	< 60		< 100
Filtración directa ascendente–descendente	Turbiedad (UNT)	< 250	< 150	< 400
	Color (UC)	< 60		< 100

En el caso de aguas que el 90% del tiempo no sobrepasan los 100 UNT y las 60 UC y alcanzan esporádicamente hasta 200 UNT y 100 UC, podrían ser tratadas mediante *filtración directa ascendente.*

La tercera alternativa disponible para aguas relativamente claras es la *filtración directa ascendente–descendente*. Esta alternativa es aplicable a aguas que el 90% del tiempo no sobrepasan las 250 UNT ni las 60 UC, y alcanzan esporádicamente más de 400 UNT y 100 UC. En la Tabla 2, se puede encontrar información referente a los límites de calidad del agua para plantas de filtración lenta.

2.2 PLANTAS DE FILTRACIÓN LENTA

Tabla 3. Límites de calidad del agua para tratamiento mediante filtración lenta

Procesos	Parámetros	90% del tiempo	80% del tiempo	Esporádicamente
Filtro lento	Turbiedad (UNT)	< 20	< 10	< 50
	Color verdadero (UC)	< 15	< 5	
	Concentración de algas (UPA/mL)	250		
	DBO5 (mg/L)	5		
	NMP de coliformes totales/100 mL	1.000		
	NMP de coliformes fecales/100 mL	500		
Filtro lento + prefiltro de grava	Turbiedad (UNT)	25		
	Color (UC)	15	< 5	< 25
	NMP de coliformes totales/100 mL	5.000		
	NMP de coliformes fecales/100 mL	1.000		
	Concentración de algas (UPA/mL)	1.000		
Filtro lento + Prefiltro de grava + sedimentador	Turbiedad (UNT)	100	< 50	< 500
	Color (UC)	< 15	< 5	< 25
	NMP de coliformes totales/100 mL	10.000		
	NMP de coliformes fecales/100 mL	3.000		
	Concentración de algas (UPA/mL)	1.000		
Filtro lento + Prefiltro de grava + sedimentador + presedimentador	Turbiedad (UNT)	100	< 50	< 1.000
	Color (UC)	< 15	< 5	< 25
	NMP de coliformes totales/100 mL	10.000		
	NMP de coliformes fecales/100 mL	3.000		
	Concentración de algas (UPA/mL)	1.000		

Los filtros lentos operan con tasas que normalmente varían entre 0,10 y 0,30 m/h; esto es, con tasas como 100 veces menores que las tasas promedio empleadas en los filtros rápidos, de allí el su nombre.

Los filtros lentos simulan los procesos de tratamiento que se efectúan en la naturaleza en forma espontánea, al percolar el agua proveniente de las lluvias, ríos, lagunas, entre otros, a través de los estratos de la corteza terrestre, atravesando capas de grava, arena y arcilla hasta alcanzar los acuíferos o ríos subterráneos. Al igual que en la naturaleza, los procesos que emplean estos filtros son físicos y biológicos.

Una planta de filtración lenta puede estar constituida solo por filtros lentos, pero dependiendo de la calidad del agua, puede comprender los procesos de desarenado, pre-sedimentación, sedimentación, filtración gruesa o filtración en grava y filtración lenta.

Los procesos previos al filtro lento tienen la función de acondicionar la calidad del agua cruda a los límites aceptables por el filtro lento. Con el tren de procesos indicados se puede remover hasta 500 UNT, teniendo en cuenta que el contenido de material coloidal no debe ser mayor de 50 UNT es decir, que la mayor parte de las partículas deben estar en suspensión para que sean removidas mediante métodos físicos.

En la Tabla 3, se puede encontrar información referente a los límites de calidad del agua mediante el proceso de filtración lenta.

BIBLIOGRAFÍA

1. **Olexa, R.** *Implementing 802.11, 802.16, and 802.20 Wireless Networks Planning, troubleshooting and operations.* s.l. : Ed. Newnes: Elsevier, 2005. ISBN: 0-7506-7808-9., 2005.

2. **SIEMENS.** Comunicación industrial para aplicaciones de automatización. [En línea] 04 de 2007. http://www.automation.siemens.com/download/internet/cache/3/1436552/pub/es/k_schrift_es_0407.pdf.

3. **SR-Telecom-Inc.** WiMAX-Capacity. [En línea] 2006. http://www.srtelecom.com/uploads/File/whitepapers/WiMAX-Capacity.pdf.

4. **Alberto Escudero Pascual, IT +46.** Unidad 02: Estándares en Tecnologías Inalámbricas. [En línea] 2007. http://wirelessu.org/uploads/units/2008/08/28/59/02_es_estandares-inalambricos_guia_v02.pdf.

5. **SIEMENS, Franz Köbinger.** Information Security in Industrial Communications. [En línea] 03 de 2003. http://www.automation.siemens.com/download/internet/cache/3/1105388/pub/en/whitepaper_security_e.pdf.

6. **ABB, Martin Naedele, Dacfey Dzung.** Industrial Information System Security. [En línea] Febrero de 2005. http://search.abb.com/library/Download.aspx?DocumentID=9AKK100580A1770&LanguageCode=en&DocumentPartId=&Action=Launch&IncludeExternalPublicLimited=True.

7. **Mrs.D.Shanmugapriya, Dr.G.Padmavathi &.** A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks. [En línea] 2009. http://arxiv.org/ftp/arxiv/papers/0909/0909.0576.pdf.

8. **IBM.** Política y objetivos de seguridad. [En línea] 2009. http://publib.boulder.ibm.com/infocenter/iseries/v5r3/index.jsp?topic=/rzaj4/rzaj4rzaj40j0securitypolco.htm.

9. **Metropolitana, Universidad Autonoma.** Análisis Comparativo de diferentes algoritmos de cifrado (encriptar). [En línea] 2005. http://docs.google.com/viewer?a=v&q=cache:t21Yhqm32doJ:www.somece.org.mx/simposio06/memorias/titulo/files/4_SanchezGuerreroLourdes_analisis2.pdf+sistemas+de+cifrado+simetrico+de+datos+pdf&hl=es&gl=co&sig=AHIEtbTvi-GdhWq6XaRxDB47Ulnr-1R9AA.

10. **SIEMENS.** IWLAN/PB Link PN IO. [En línea] 2008. http://www.automation.siemens.com/net/html_78/produkte/050_iwlan_pb_link_pn_io.htm.

11. **SIEMENS**. Simatic net Industrial Ethernet, Network Topologies. [En línea] 2005. http://www.automation.siemens.com/download/internet/cache/3/1218442/pub/en/ie_netztopologien_v1_1.pdf.

12. **AnyBus.** Pasarelas industriales (Gateways) diseñadas para conectar DOS redes industriales diferentes. [En línea] http://www.interempresas.net/FeriaVirtual/Catalogos_y_documentos/80595/HMS_ABX1.pdf.

13. **Emerson.** Transmisor de pH wirelessHART modelo 6081-P. [En línea] http://www.emersonprocess.es/excom/16/7/content/9888.

14. **Emerson, Process Magnament.** Transmisor Rosemount Serie 3051S. [En línea] http://www.emersonprocess.com/rosemount/document/pds/4801b09n.pdf.

15. **ABB, Gareth Johnston.** Unlocking stranded information, The ABB WirelessHART upgrade adapter. [En línea] 04 de 2009. http://www05.abb.com/global/scot/scot271.nsf/veritydisplay/9fddd7b3e845ca5ac12576800033fcc8/$File/27-32%204M918_ENG_72dpi.pdf.

16. **SIEMENS.** Industrial Wireless Communication. [En línea] 2009. http://www.automation.siemens.com/mcms/industrial-communication/en/support/catalog/Documents/78/03_IKPI_2009_Industrial_Wireless_Communication_es.pdf.

17. **SIEMENS**. IE/WSN - PA LINK. [En línea] 2008. http://www.automation.siemens.com/mcms/industrial-communication/es/pasarelas/ie-wsn-pa-link/Pages/ie-wsn-pa-link.aspx.

18. **SIEMENS**. Antenas y Accesorios Para Antenas. [En línea] 2008. http://www.automation.siemens.com/net/html_78/produkte/antennen.htm.

19. **BERMAD.** Valvulas de control Sistemas Industriales y Abastecimiento de Agua. [En línea] http://www.medidores.com/pdfs/2_16.pdf.

20. **Vargas, Ing. Lidia de.** *Tratamiento de agua para consumo humano Manual 1: Teoria.* [En línea] 2004. http://www.cepis.org.pe/bvsatr/fulltext/tratamiento/manualI/tomoI/tres.pdf.

21. **SIEMENS.** Comunicación industrial para Automation and Drives. [En línea] 2007. http://www.sispm.com/descargas/04%20Comunicaciones/Catalogos/01_Automation_Drivers.pdf.

22. **SIEMENS**. Gestión de activos a nivel de planta, Productos para el mantenimiento inteligente en la Industria de Procesos. [En línea] Abril de 2008. http://www.automation.siemens.com/w2/efiles/pcs7/pdf/78/maintenance_2sp.pdf.

23. **Pareek, D.** *The Business of WiMAX.* s.l. : Ed. Chichester: John Wiley & Sons. 2006. ISBN: 10-0470-02691, 2006.

24. **SIEMENS.** Applicattions and tool, set up an industrial wireless LAN. [En línea] 2007. https://a248.e.akamai.net/cache.automation.siemens.com/dnl/jIyMzg3AAAA_22681042_Tools/22681042_Aufbau_IWLAN_v11_e.pdf.

25. **Alfredo Rosado, Universidad de Valencia.** Sistemas Industriales Distribuidos. *Tema 2. Redes de Comunicación: Topologías y Enlaces.* [En línea] 2006 - 2007. http://www.uv.es/rosado/sid/Capitulo2_rev0.pdf.

26. **SIEMENS.** Industrial Wireless LAN Features, Applications, Examples. *Industrial Wireless LAN Features, Applications, Examples.* [En línea] 2006. https://www.automation.siemens.com/download/internet/cache/3/1091497/pub/en/ie_wireless.pdf.

27. **ORiNOCO, Technical Bulletin 046/ A.** WDS: Wireless Distribution System. [En línea] Febrero de 2002. http://74.125.47.132/search?q=cache:-jSdp6Xjhj4J:www.pafree.net/media/TB-046.pdf+WDS+(Wireless+Distribution+System) &cd=4&hl=es&ct=clnk&gl=co .

28. **Department of Computer Science & Engineering, Jadavpur University.** Setting up of a Wireless Distribution System (WDS). [En línea] 2002. http://www.cs.ucsb.edu/~sudipto/files/wds.pdf.

29. **Niels Aakvaag, Jan-Erik Frey.** Redes de sensores inalámbricos, Nuevas soluciones de interconexión para la automatización industrial. *Redes de sensores inalámbricos, Nuevas soluciones de interconexión para la automatización industrial.* [En línea] 2006. http://library.abb.com/GLOBAL/SCOT/scot271.nsf/VerityDisplay/A019E9833DCF2819C1257199004E5DD2/$File/39-42%202M631_SPA72dpi.pdf.

30. **ISA, International Society of Automation.** ANSI/ISA–95.00.01–2000 Enterprise-Control System Integration Part 1: Models and Terminology. [En línea] 2000. http://www.isa.org.

31. **Hernández, Miguel.** Introducción a las redes de comunicación industriales. [En línea] 1999. http://isa.umh.es/asignaturas/ci/Tema%201.pdf.

32. **DISA: Departamento de Ingenieria de Sistemas y Automatica, Universidad del Pais Vasco.** Comunicaciones Industriales. [En línea] 1999. http://www.disa.bi.ehu.es/spanish/ftp/material_asignaturas/Laboratorio%20de%20Comunicaciones%20Industriales/Documentaci%F3n/Introducci%F3n%20a%20las%20Comunicaciones%20Industriales.pdf .

33. **SIEMENS.** Industrial Networking. *Febrero.* [En línea] 2007. http://www.automation.siemens.com/download/internet/cache/3/1441710/pub/es/BS_Networking_sp.pdf.

34. **Apprion, Dr. Peter Fuhr.** Coexistence of Devices and Systems in an ISA100 Network. [En línea] 2008. http://www.apprion.com/pdf/ApprionNewsletter.ISA100CoexistenceArticle.pdf.

35. **BrazilFW.** Wireless - Optimización - En Construcción. [En línea] 2006. http://www.brazilfw.com.br/forum/viewtopic.php?f=40&t=65199.

36. **ABB.** Redes de Sensores Inalambricos. [En línea] Febrero de 2006. http://library.abb.com/GLOBAL/SCOT/scot271.nsf/VerityDisplay/A019E9833DCF2819C1257199004E5DD2/$File/39-42%202M631_SPA72dpi.pdf.

37. **Peña, Joan Domingo.** Comunicaciones en el entorno industrial. [En línea] 2003. http://books.google.com.co/books?id=IAAK4pQpaK0C&pg=PA55&lpg=PA55&dq=entornos+industriales+bandas+de+frecuencia&source=bl&ots=NACGkbINkd&sig=NHxcWs-QETsqoTqFpJlv6kbBzaI&hl=es&ei=y1x3Sv_IB4rBlAer_-SACA&sa=X&oi=book_result&ct=result&resnum=2#v=onepage&q=&f=.

38. **Oak, Manali.** Advantages and Disadvantages of Different Network Topologies. [En línea] 25 de 10 de 2008. http://www.buzzle.com/articles/advantages-and-disadvantages-of-different-network-topologies.html.

39. **Soroush Amidi & Alex Chernoguzov, Honeywell.** Wireless Process Control Network Architecture Overview. [En línea] 3 de 2009. http://hpsweb.honeywell.com/NR/rdonlyres/14F08C40-BE14-490C-8E82-8F4D09D3A9DB/76326/WirelessProcessControlNetworkArc_WP_March09.pdf.

40. **FCIT, Florida Center for Instructional Technology.** Chapter 5: Topology. [En línea] 2009. http://fcit.usf.edu/Network/chap5/chap5.htm.

41. **Wikipedia.** Red en estrella. [En línea] http://es.wikipedia.org/wiki/Red_en_estrella.

42. **Bussmann, Cooper.** Wireless Mesh Networks – Reliability and Flexibility. [En línea] http://www.cooperbussmann.com/pdf/df32d995-50e6-42e3-ac41-cb4456c3b9e6.pdf.

43. **SIEMENS.** Comunicación industrial para aplicaciones de automatización. [En línea] 04 de 2007. http://www.automation.siemens.com/download/internet/cache/3/1436552/pub/es/k_schrift_es_0407.pdf.

44. **SIEMENS**. Profinet Success Story. [En línea] 2008. http://www.automation.siemens.com/download/internet/cache/3/1418505/pub/de/E20001-A430-P820-X-7600.pdf.

45. **SIEMENS**. PROFINET Katja Koivistoinen. [En línea] 11 de 7 de 2008. http://www.siemens.fi/CMSADwww.nsf/F7C54CD674F4C012C22574FD00307F61/$file/05_Profinet%20Innovation%202008.pdf.

46. **SIEMENS**. IE/WSN-PA LINK. [En línea] 2008. http://www.automation.siemens.com/mcms/industrial-communication/en/network-transitions/ie-wsn-pa-link/Pages/ie-wsn-pa-link.aspx.

47. **SIEMENS**. Industrial wireless communication creates new prospects for reliable automation. [En línea] 11 de 2009. http://www.automation.siemens.com/download/internet/cache/3/1501203/pub/en/E20001-A530-P820-V1-7600.pdf.

48. **Wikipedia.** Red Industrial. [En línea] http://es.wikipedia.org/wiki/Red_industrial.

49. **Eraso, Julio César Caicedo.** Redes Industriales. [En línea] 2008. http://www.galeon.com/juce/artredind.pdf.

50. **Linkses.** Topologías de Red. [En línea] http://www.linkses.com/articulos/articulo.php?id=472.

51. **Universidad del Cauca, DEIC.** INTRODUCCION A LAS REDES DE COMUNICACIÓN INDUSTRIAL. [En línea] ftp://ftp.unicauca.edu.co/Facultades/FIET/DEIC/docs/Materias/Redes%20Industriales/Redes/Conferencias/Capitulo%201.pdf.

52. **Ignacio Morande**. PROTOCOLOS DE COMUNICACIONES INDUSTRIALES. [En línea] http://www.alumnos.usm.cl/~ignacio.morande/descargas/PROTOCOLOS_INDUSTRIALES.pdf.

53. **HART communication Foundation.** HART Field Communications Protocol Application Guide. [En línea] 1999. http://grupos.emagister.com/ficheros/dspflashview?idFichero=162028.

54. **SIEMENS.** PROFIBUS El bus polivalente para la comunicación en la industria de procesos. [En línea] 2008. http://www.automation.siemens.com/w2/efiles/pcs7/pdf/78/prdbrief/kb_profibus_es.pdf.

55. **red, Seguridad en la.** Criptografia. [En línea] http://www.seguridadenlared.org/es/index25esp.html.

56. **Universidad de Valencia, Alfredo Rosado Muñoz.** Sitemas Industriales Distribuidos: Redes de Comunicaciones Industriales. [En línea] 2004. http://www.uv.es/rosado/sid/Capitulo3_rev0.pdf.

57. **UV**. Sistemas Industriales Distribuidos: Redes de Comunicación (Topologías y enlaces). [En línea] 2004. http://www.uv.es/rosado/sid/Capitulo2_rev0.pdf.