

Unidad IV

Parámetros característicos de los sistemas inalámbricos

4.1. Interferencia y confiabilidad.

Las tecnologías que empleamos garantizan la completa y continua confiabilidad de todos nuestros productos y han sido demostradas en terreno como las más eficaces por lo que se refiere a cobertura del espectro de interferencia y confiabilidad en todo tiempo y terreno.

No tercerizamos ningún aspecto de nuestra producción. Cada producto que vendemos es fabricado internamente por nuestro equipo técnico de ingenieros mecánicos y electrónicos en RF, altamente especializado. Incluso nuestros componentes accesorios, como las antenas, son diseñados y fabricados en forma interna a fin de garantizar el más alto grado de desempeño, confiabilidad y compatibilidad con nuestros sistemas de alta potencia patentados.

Nuestro activo departamento de investigación y desarrollo mejora continuamente nuestras tecnologías y productos y se esfuerza constantemente por introducir innovadores productos para satisfacer la demanda siempre creciente de protección de tropas.

Nuestro equipo de ingenieros de diseño sobresale en enfrentar cualquier desafío que se presente en el diseño de soluciones de interferencia especiales para responder a los requerimientos específicos de cada cliente.

Esperamos tener la oportunidad de darle otros detalles sobre nuestra exclusiva tecnología de avanzada, cómo puede responder idealmente a sus aplicaciones de interferencia de RF y sus ventajas sobre los productos de nuestro competidor.

4.2. Consumo de energía.

La eficiencia energética es una consideración importante en el desarrollo de todos los equipos inalámbricos y componentes de red de Emerson con la meta de maximizar el tiempo entre mantenimientos. Nuestros ingenieros de desarrollo tratan la energía como si fuera oro — un bien escaso que se debe tomar y conservar en todo momento, y se debe gastar únicamente en las funcionalidades que valora el usuario, como los diagnósticos. El resultado es que los usuarios obtienen los beneficios de nuestras capacidades SmartPower™, que incluyen técnicas avanzadas de gestión de energía, tiempos más rápidos de activación de equipos, equipos electrónicos de bajo consumo de energía y tecnologías de recolección de energía.

Las aplicaciones de red de campo inalámbrica difieren de las aplicaciones de Red

de planta inalámbrica y los requisitos de energía asociados con cada una son muy diferentes. Las aplicaciones de red de planta como vídeo inalámbrico y aplicaciones para trabajadores móviles pueden alimentarse por línea o recargados diariamente. Sin embargo, uno de los requisitos más importantes que caracteriza a los equipos de red de campo es que éstos “no se conectan”. Los dispositivos de red de campo se alimentan por batería y tienen un requisito de consumo de energía extremadamente bajo. La energía que consumen estos equipos es 10 veces más baja que otras soluciones de conectividad inalámbrica que se consideran “de bajo consumo de energía”. Aunque el requisito de consumo es bajo, es aún un componente muy importante, y las baterías deben durar de 5 a 10 años en entornos exigentes de planta.

4.3. Interoperabilidad.

La gestión de emergencias se basa en la unión de los modos de organización, de las técnicas y de los medios que permiten a los servicios de seguridad civil estar preparados y hacer frente a situaciones de urgencia tales como catástrofes naturales o industriales (inundaciones, terremotos, incendios, etc.) o atentados terroristas. Esta gestión necesita que las autoridades responsables sean capaces de organizar los esfuerzos de las distintas partes implicadas con diferente nivel y naturaleza (bomberos, servicios de urgencias, policía, seguridad civil y, en algunos casos, el ejército), tanto en el plano nacional como el internacional, con la compleja problemática del funcionamiento conjunto de los distintos sistemas de comunicaciones inalámbricos (interoperabilidad) y las altas exigencias de calidad de servicio, latencia, ancho de banda, enrutamiento y restricciones de movilidad. En los últimos años, el aumento del número de catástrofes de gran calibre ha creado nuevas necesidades en materia de protección civil, que exigen nuevos medios de comunicación de gran ancho de banda capaces de incrementar las capacidades de diagnóstico, intercambio de información, decisión e implementación de dichas decisiones. El vídeo para los informes de intervención o la visualización del estado de las zonas siniestradas, geo localización, la telemedicina, la imagen de alta definición, la consulta de bases de datos son algunos ejemplos de los nuevos servicios requeridos por las transmisiones de información de alto ancho de banda (orden de varios Mb/s).

4.4. Seguridad.

A nivel de la red de planta inalámbrica, la seguridad es fundamental para la Red inalámbrica unificada Cisco. La solución de auto defensa de red de Cisco basada en normas ofrece la confianza de que su planta y los datos de su empresa se mantendrán privados y seguros. Las capacidades de control de amenazas controlan y contienen amenazas conocidas y desconocidas, y el control de admisión de red le ayuda a hacer cumplir las políticas de seguridad de la organización para permitir el acceso únicamente a dispositivos fiables.

Dentro de la red inalámbrica, Cisco ofrece capas de protección adicionales y múltiples, que incluyen:

Seguridad RF:

Detecta y evita interferencia de frecuencia de radio 802.11i y controla la propagación de señales no deseadas.

Localización y prevención de intrusión WLAN: Detecta y sitúa dispositivos de campo o puntos de acceso malintencionados, así como posibles amenazas inalámbricas tales como un intento de escucha sin autorización, lo que ayuda a los administradores IT a evaluar rápidamente el nivel de amenaza y tomar acción inmediata. Los ataques de réplica se previenen tanto en la capa de enlace como en la capa de red con el uso de contadores de replicación sin repetición. El protocolo de salto de canales espaciados reduce los riesgos de un ataque DOS por medio del uso de todo el espacio de radio.

Control de acceso de red (NAC):

Hace cumplir las políticas relacionadas con la configuración y comportamiento de puntos de acceso para ayudar a asegurar que únicamente sensores reconocidos pueden obtener acceso a la red.

Movilidad segura: Mantiene el nivel más alto de seguridad en ambientes móviles con Proactive Key Caching de Cisco, una extensión de la norma 802.11i y precursor de los Certificados 802.11r: Uso de certificados X.509 y encriptación AES para transacciones LWAPP. Esta encriptación AES y X.509 está integrada dentro de la solución de malla inalámbrica con cada transacción LWAPP y todo el tráfico encriptado.