Universidad Acción Pro Educación y Cultura

UNAPEC

Decanato de Ingeniería y Tecnología

SISTEMA DE AUTOMATIZACIÓN DE PARQUEOS EN EL CAMPUS I DE LA UNIVERSIDAD APEC MEDIANTE LA TECNOLOGÍA RFID

Br. Juan Emilio Sepúlveda Hernández 2004-1705

Br. Jenny Esther de Jesús Reyes 2005-0378

Br. Bernardo Rafael Ledesma Polanco 2005-1476

MONOGRAFÍA PARA OPTAR POR EL TÍTULO DE

INGENIERO ELECTRÓNICO, MENCIÓN COMUNICACIONES

Santo Domingo, República Dominicana.

2009

ÍNDICE

1. RESUMEN

Debido a las limitaciones de espacio existentes en el área de parqueo de la Universidad APEC, surge la necesidad de utilizar un método para gestionar dicha área que permita un mejor aprovechamiento del mismo. Una de las alternativas existentes es el uso de la tecnología de Identificación por Radio Frecuencia para automatizar el conteo de los espacios disponibles y como método de control de acceso.

Los RFID constituyen una de las tecnologías mas utilizadas en recientes años debido a la economía de los identificadores y la posibilidad de obtener y registrar datos de forma rápida y remota. La gran cantidad de información generada por los sistemas RFID es manipulable gracias a la existencia de aplicaciones de gestión de los sistemas de RFID. Estos datos generados por el sistema, pueden ser transmitidos a los usuarios del mismo a través de Internet mediante el uso de servicios Web, a la vez que se pueden enviar mediante mensajes SMS con el uso de un módem GSM. El proveer a los usuarios de la información en tiempo sobre la cantidad de espacios disponibles en el parqueo, se traduce en varios beneficios tanto para los usuarios como para la institución.

Además, la implementación de un sistema de monitoreo mediante una red de cámaras de seguridad, se logra la optimización del uso del área de parqueo de la Universidad APEC, al convertirlo en un lugar más seguro para quienes lo usan y al reducir de manera sustancial las congestiones vehiculares en las zonas de acceso.

2. INTRODUCCIÓN

Los parqueos de las Universidades de Santo Domingo no cuentan con un sistema de parqueo eficiente y seguro. UNAPEC no es la excepción a esta regla, es por esto que ha cobrado importancia la implementación de un sistema que ayude a reducir los riesgos de delitos dentro del estacionamiento y aumente la eficiencia de uso del mismo.

Con este fin, es necesario el aprovechamiento de los recursos tecnológicos disponibles como es el caso de la identificación por radio frecuencia (RFID), para automatizar y gestionar de forma eficiente el parqueo de la Universidad APEC.

RFID es una tecnología y sistema que se auxilia de las ondas electromagnéticas para el almacenamiento y la recuperación de datos de forma remota al usar dispositivos denominados etiquetas, transpondedores o tags RFID que realizan esta función por medio de Radio Frecuencia.

Los subsistemas que posee son de seguridad, consistente en una Red de cámaras IP de con el propósito de monitorear el estacionamiento. Un sistema de control de acceso en el cual una barrera permite el paso solo a vehículos autorizados. Y finalmente, otro subsistema encargado de la conexión a las redes externas como Internet y la red de comunicación celular GSM.

3. PLANTEAMIENTO DEL PROBLEMA

En la actualidad, la Universidad APEC cuenta con un sistema de estacionamientos deficiente. Tal situación tiende a incrementarse a medida que la universidad abre las puertas a nuevos estudiantes que poseen vehículos.

Constantemente personas en vehículos no autorizados por la institución tienen acceso al área de parqueo, provocando que la cantidad de parqueos para estudiantes, profesores y empleados sea cada vez menor. Esto crea que en la universidad exista un ambiente de inseguridad. Esto sucede debido a que el personal de seguridad de la universidad permite el ingreso de vehículos no identificados al parqueo de la universidad.

Además, en ocasiones no se sabe con exactitud si hay parqueos disponibles, porque el personal no cuantifica los vehículos que entran y salen del recinto universitario.

Se hace necesario el uso de las tecnologías disponibles como el RFID para la implementación de un sistema de parqueo que le permita a la universidad controlar el acceso de vehículos al estacionamiento. El cual identificará la cantidad de estacionamientos disponibles y los estudiantes tendrán acceso a esta información vía internet.

4. OBJETIVOS DE LA INVESTIGACIÓN

4.1 OBJETIVO GENERAL

Diseñar un sistema de identificación y control de acceso al área de estacionamiento, mediante el uso de la tecnología RFID, que permita a la Universidad APEC mejorar dicho proceso.

4.2 OBJETIVOS ESPECIFICOS.

1. Proporcionar a los usuarios información sobre la disponibilidad existente en el área de estacionamiento de la Universidad APEC.
2. Reducir el número de vehículos no autorizados que ingresa al estacionamiento de la Universidad APEC.
3. Conocer la situación actual de los parques universitarios en la ciudad de Santo Domingo, R.D.
4. Identificar la cantidad de estacionamientos existentes en la Universidad APEC.

5. Analizar los datos estadísticos sobre los vehículos que utilizan el estacionamiento de la Universidad APEC por día.

6. Definir los componentes de un sistema de RFID.

7. Conocer las diferentes aplicaciones de las tecnologías de controles RFID

8. Incrementar la seguridad existente en el área de estacionamientos de la Universidad APEC.

5. HIPÓTESIS

Mediante el uso de la tecnología de la identificación por radio frecuencia (RFID) es posible automatizar el conteo y registro de espacios disponibles para lograr un mejor uso del área de estacionamiento de la Universidad APEC.

6. MARCO TEÓRICO

TEMA 1: INTRODUCCIÓN AL ESTACIONAMIENTO DE LA UNIVERSIDAD APEC.

Las universidades en la ciudad de Santo Domingo presentan un común denominador en lo referido al área de estacionamiento, debido a que casi ninguna presenta un sistema eficiente que permita la gestión de dicha área. El método mas común para el control de acceso a parqueos, es la entrega de tickets y la devuelta de los mismos a la salida del parqueo, siendo la excepción la Universidad Iberoamericana que posee un sistema basado en tarjetas magnéticas.

El campus principal de la universidad APEC está ubicado en la ciudad de Santo Domingo, Distrito Nacional en República Dominicana. El campus cuenta dos áreas de estacionamiento dentro del recinto dependiendo de los usuarios a los que están destinadas:

1. Parqueo exterior: estacionamiento para profesores, personal administrativo, visitantes y estudiantes.
2. Parqueo Principal: dos niveles de estacionamiento para estudiantes, profesores y visitantes.

En total, la cantidad estimada de espacios disponibles como parqueos es superior a los 600 estacionamientos, tomando en cuenta que muchos vehículos que se estacionan en el interior del recinto, son colocados en lugares que no están delimitados como parqueos.

1.1 Características del parqueo de UNAPEC

1.1.1 Ubicación.

La Universidad APEC se encuentra en la ciudad de Santo Domingo, Distrito Nacional, en el sector de El Vergel. Las referencias mas importantes para su ubicación son sus límites en su lado sur por la Avenida México, en su lado este por la Avenida Máximo Gómez, y en su lado oeste por la calle Dr. César Dargam.

Foto de la zona cercana al Campus I de la Universidad APEC.
Fuente: Google Earth.

El parqueo principal de la Universidad APEC tiene como datos geográficos los siguientes:

Latitud 18°28'23.26"N,

Longitud 69°54'50.60"W

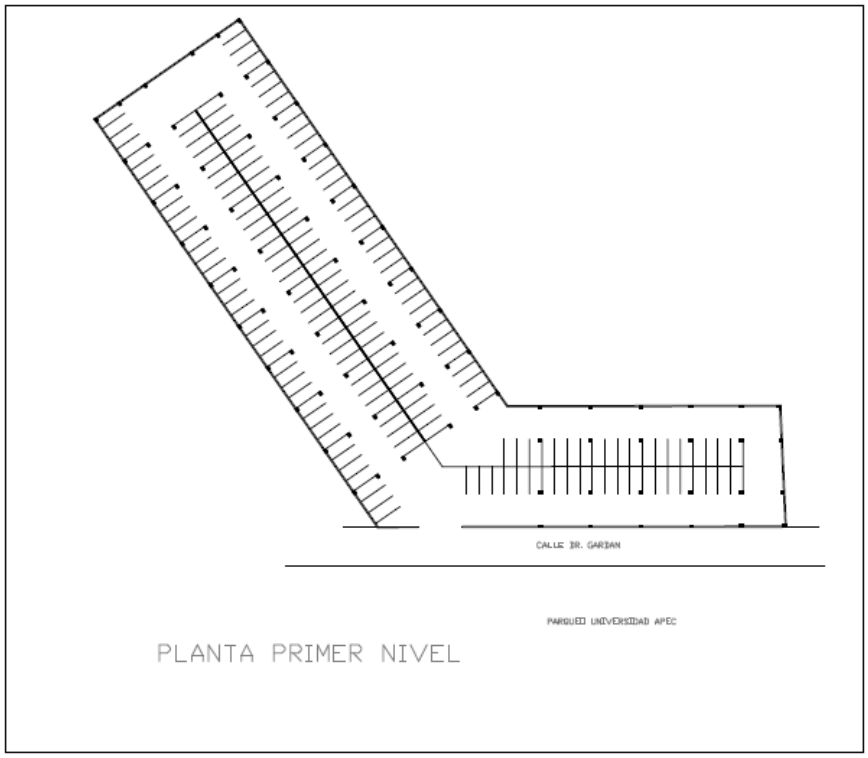
1.1.2 Capacidad estimada del área estacionamiento principal.

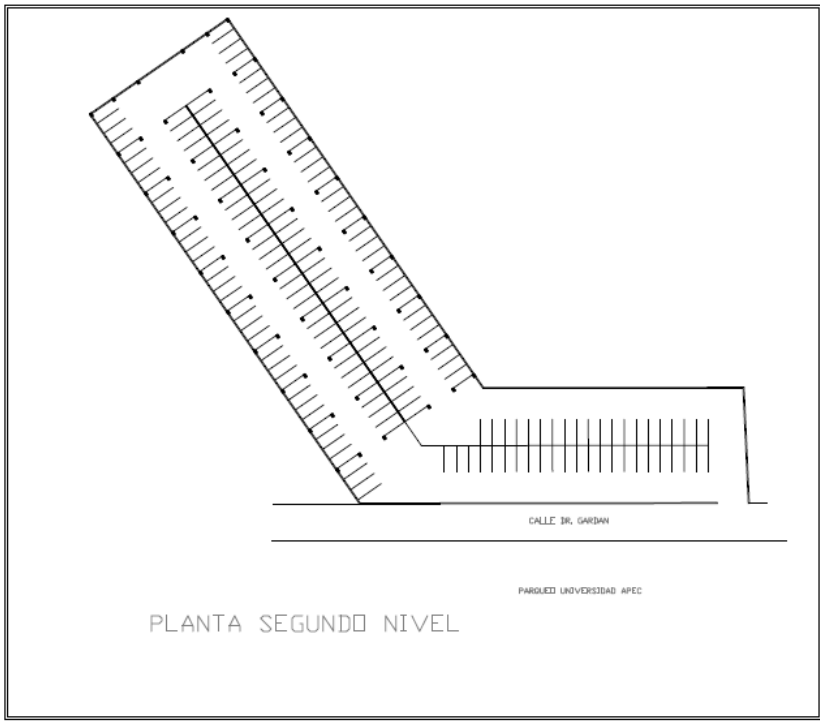
La Universidad APEC cuenta con un lugar de estacionamiento principal, cuyas entradas se sitúan en la calle Dr. Cesar Dargam, el cual es de uso general para estudiantes, visitantes y profesores y tiene una capacidad estimada de 200 vehículos para cada nivel, es decir, una capacidad total estimada de 400 vehículos, sin tomar en consideración las personas que se estacionan en zonas no demarcadas como parqueos.

1.1.3 Planos del estacionamiento principal.

A continuación se presentan algunos planos en dos dimensiones y tres dimensiones sobre la estructura que conforma el estacionamiento principal de la Universidad APEC.

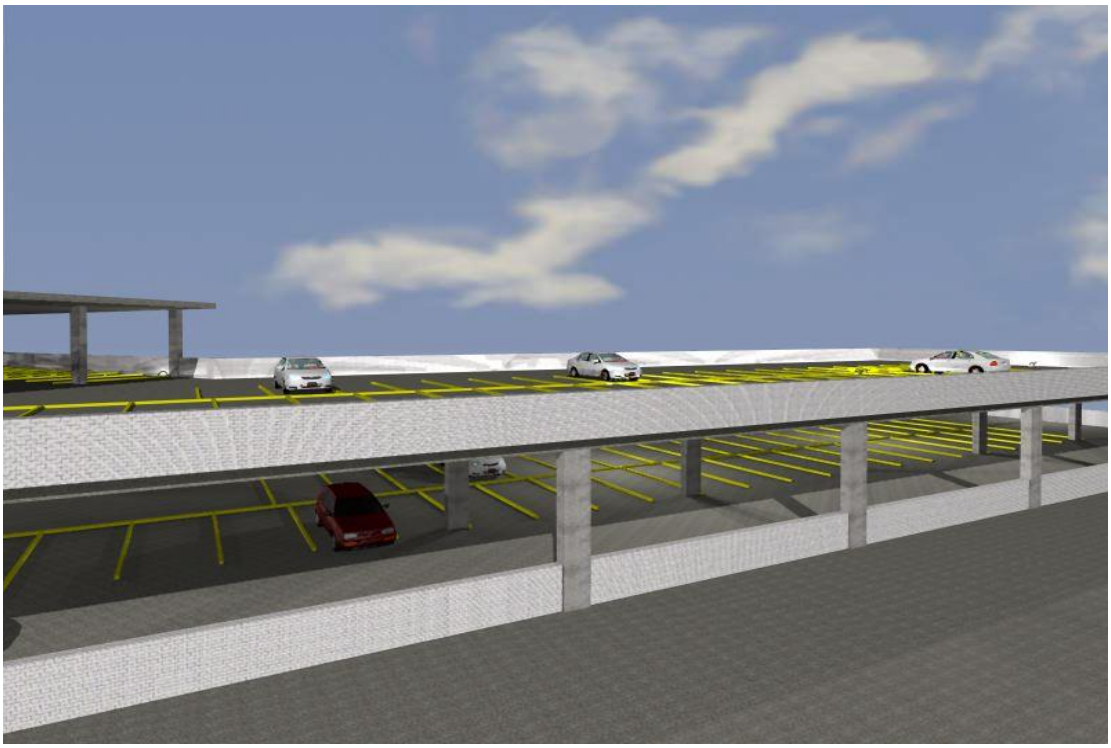
1.1.3.1 Vistas en dos dimensiones (2D).



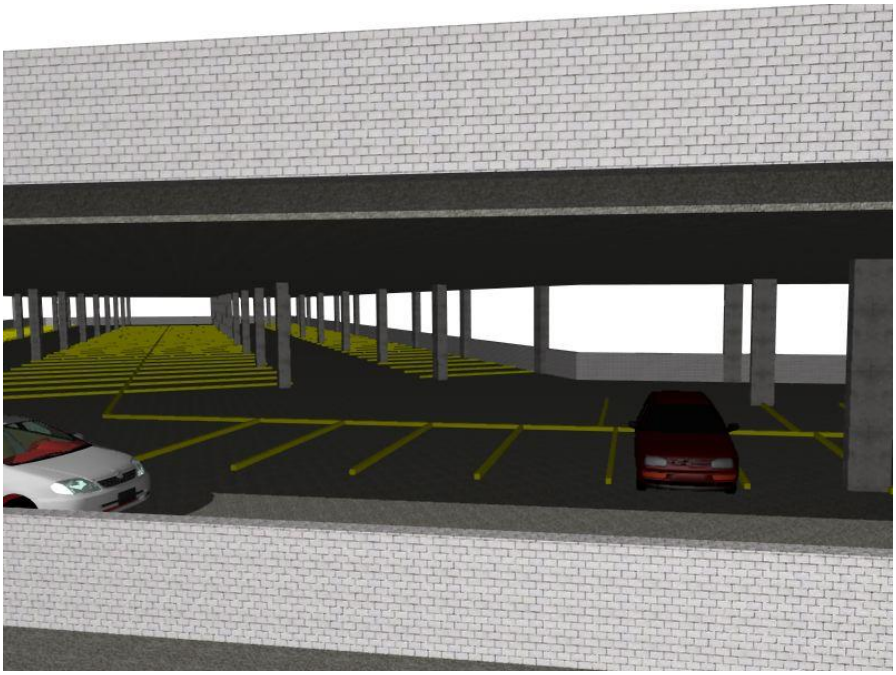


1.1.3.2 Vistas en tres dimensiones (3D).

Vista frontal del área de parqueo de la Universidad APEC



Vista en perspectiva de los dos niveles del parqueo principal de la Universidad APEC.



Vista interior del primer nivel del parqueo de la Universidad APEC.

TEMA 2: LA IDENTIFICACIÓN POR RADIO FRECUENCIA (RFID)

2.1. Conceptos de RFID.

El RFID, Identificación por Radio-Frecuencia (Radio Frequency Identification por sus siglas en inglés) es una tecnología que a grandes rasgos sirve para el almacenamiento y recuperación de información (normalmente poca) de manera remota. El sistema básico RFID está formado por dos componentes el tag o etiqueta y el lector. No obstante, para la utilización real de la tecnología RFID se necesitan una serie de componentes adiciones como antenas, soportes, escritores/programadores, hosts con software de control dependiendo su utilidad.

Una definición más seria sería: RFID es una tecnología y dispositivos que se valen de las ondas electromagnéticas para intercambiar datos de identificación. Normalmente, esto implica la utilización de un pequeño tag o etiqueta que identifica un objeto especifico. El proceso sigue los siguientes pasos: se recibe una señal de radio, se interpreta y se devuelve un número u otro tipo de información identificativa. Adicionalmente este proceso puede ser tan complejo como una comunicación bidireccional pudiendo llegar a ser encriptada e interpretada a través de una base de datos y transportada a través de varios sistemas de comunicaciones.

La potencia de RFID es tan alta que el rango de objetos identificables incluye virtualmente todos las cosas de este planeta e incluso del más allá.

El RFID es un ejemplo de la tecnología de Auto-Identificación, en la cual cualquier objeto es identificado automáticamente. Otro ejemplo de Auto-Identificación son los códigos de barras, biométricos (como huellas dactilares o escaneo de retina) , identificación de voz, OCR, etc

2.2. Historia y Evolución de RFID.

Aunque la historia del RFID pueda estar fechada en los años 1930, esta tecnología encuentra sus raíces en 1897 cuando Guglielmo Marconi invento la radio. El RFID se aplica a los mismos principios físicos que se utilizan en las emisiones de radio, donde las ondas radio, una forma de energía electromagnética, transmite y recibe varios tipos de información.

Léon Theremin en 1946 inventó una herramienta de espionaje para la Unión Soviética incidente que volvió a las ondas de radio con información de audio. Ondas de sonido que vibraba un diafragma ligeramente modificado la forma del resonador, que refleja la modulación de frecuencia de radio. A pesar de este dispositivo es un dispositivo de escucha pasiva encubierta, no una etiqueta de identificación, se considera que es un predecesor de la tecnología RFID.

Tecnología similar, como el FIB transpondedor inventado en el Reino Unido en 1939, fue utilizado habitualmente por los aliados en la Segunda Guerra Mundial para identificar a las aeronaves como amigo o enemigo. Transpondedores están todavía vigentes en la mayoría de aeronaves hasta el día de hoy.

Otro trabajo temprano RFID es explorar el histórico documento de 1948 de Harry Stockman, titulado "Medios de Comunicación de Potencia Reflejada" (Actas del IRE, pp 1196-1204, octubre de 1948). Stockman predijo que "... una considerable labor de investigación y desarrollo tiene que ser hecho antes de que el resto de problemas básicos de energía se refleja en la comunicación son resueltos, y antes de que el campo de aplicaciones útiles se explora".

Mario Cardullo la patente de EE.UU. 3.713.148 en 1973 fue el primer verdadero antepasado de los modernos RFID; un transpondedor pasivo de radio con memoria. El primer dispositivo fue pasiva, con el soporte de la señal de interrogatorio, y se demostró en 1971 a la Autoridad Portuaria de Nueva York y otros usuarios potenciales, y consistió en un transpondedor de 16 bits de memoria para su uso como un dispositivo de telepeaje. Cardullo patente de base se refiere al uso de la RF, el sonido y la luz como medios de transmisión. El plan de negocios original presentado a los inversores en 1969 puso de manifiesto los usos en el transporte (automóvil de identificación del vehículo, sistema de peaje automático, placa electrónica, manifiestos electrónicos, ruteo de vehículos, vehículos de supervisión de la ejecución), el sector bancario (cheque electrónico libro

electrónico, tarjeta de crédito), la seguridad (la identificación del personal, puertas automáticas, vigilancia) y médicos (identificación, la historia del paciente).

A muy temprana refleja la demostración de potencia (modulación de retrodispersión) Las etiquetas RFID, tanto pasivas como semi-pasivas, fue realizado por Steven Depp, Alfred Koelle, y Robert Freyman en el Laboratorio Nacional de Los Alamos en 1973. El sistema portátil operado a 915 MHz y utiliza las etiquetas de 12 bits. Esta técnica es utilizada por la mayoría de los UHFID de hoy y las etiquetas RFID de microondas.

La primera patente de estar asociado con las siglas RFID se otorgó a Charles Walton en 1983 Patente EE.UU. 4.384.288.

El mayor despliegue de la RFID activa es los EE.UU. Departamento de Defensa de la utilización de Savi. Las etiquetas activas en cada uno de sus más de millones de contenedores de transporte que viajar fuera de los Estados Unidos continentales (CONUS) la mayor implantación de la RFID pasiva es la Logística de Defensa Agencia (DLA), el despliegue a través de 72 instalaciones ejecutadas por ODIN, que también realizó la puesta en marcha para Airbus que consiste en 13 proyectos en todo el mundo.

2.3. Componentes de un Sistema de RFID.

El sistema RFID está compuesto por los siguientes componentes:

- Tag: Es un componte esencial del sistema RFID.

- Lector: Es también otro componente esencial.
- Antena del lector: Es también otro componente esencial del sistema, a veces integrada en el mismo lector.
- Controlador: Es también otro componente esencial. Sin embargo, muchos lectores de última generación lo tienen integrado.
- Sensor, actuador, alarma: Son componentes opcionales que son necesarios para interactuar con el sistema.
- Equipo y sistema software: Teóricamente, un sistema RFID puede funcionar independientemente de este componente. Pero un RFID sin estos carece de utilidad.
- Infraestructura de comunicación: Es una parte importante del sistema que conecta los componentes previamente listados, ya sean alámbricos o no, para hacer una comunicación efectiva entre ellos.

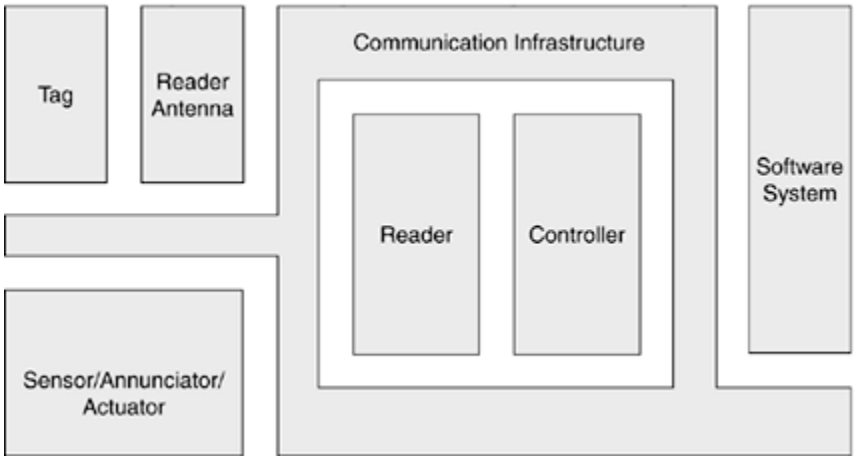


Figura 1. Componentes de un sistema de RFID. Fuente: http://www.gii.upv.es/personal/gbenet/IIN/treballs%200607/RFID%20Por%20Diego%20Contreas%20Jimenez%20y%20Antonio%20Lacasa%20Corral.doc

2.3.1 Etiquetas.

Los transponedores o etiquetas electrónicas se pueden clasificar de maneras diferentes, atendiendo a su alimentación o a su posibilidad de lectura/escritura.

Las tags RFID pueden ser activos, semipasivos (también conocidos como semiactivos o asistidos por batería) o pasivos. Los tags pasivos no requieren ninguna fuente de alimentación interna y son dispositivos puramente pasivos (sólo se activan cuando un lector se encuentra cerca para suministrarles la energía necesaria). Los otros dos tipos necesitan alimentación, típicamente una pila pequeña.

La gran mayoría de las etiquetas RFID son pasivas, que son mucho más baratas de fabricar y no necesitan batería. A pesar de las ventajas en cuanto al coste de las etiquetas RFID pasivas con respecto a las activas son significativas, otros factores; incluyendo exactitud, funcionamiento en ciertos ambientes como cerca del agua o metal, y confiabilidad; hacen que el uso de etiquetas activas sea muy común hoy en día.

Para comunicarse, los tags responden a peticiones o preguntas generando señales que a su vez no deben interferir con las transmisiones del lector, ya que las señales que llegan de los tags pueden ser muy débiles y han de poder distinguirse. Además de la reflexión o *backscatter*, puede manipularse el campo magnético del lector por medio de técnicas de modulación de carga.

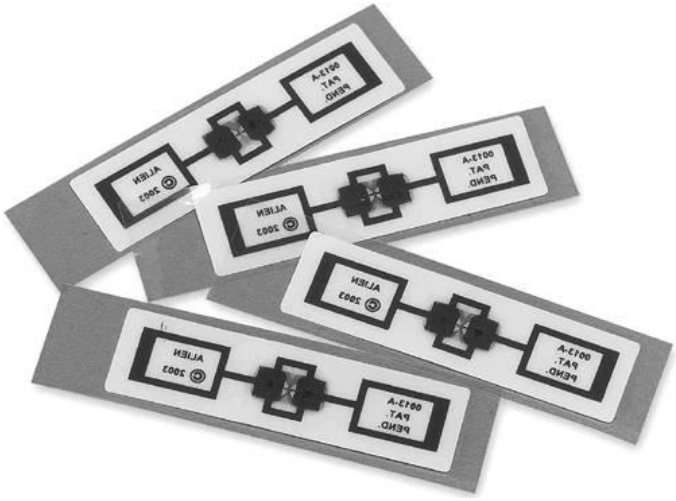


Figura 2. Etiquetas de RFID. Fuente: http://www.gii.upv.es/personal/gbenet/IIN/treballs%200607/RFID%20Por%20Diego%20Contreas%20Jimenez%20y%20Antonio%20Lacasa%20Corral.doc

2.3.1.1. Tags pasivos.

Los tags pasivos no poseen alimentación eléctrica. La señal que les llega de los lectores induce una corriente eléctrica pequeña y suficiente para operar el circuito integrado CMOS del tag, de forma que puede generar y transmitir una respuesta. La mayoría de tags pasivos utiliza *backscatter* sobre la portadora recibida; esto es, la antena ha de estar diseñada para obtener la energía necesaria para funcionar a la vez que para transmitir la respuesta por backscatter. Esta respuesta puede ser cualquier tipo de información, no sólo un código identificador. Un tag puede incluir memoria no volátil, posiblemente escribible.

Por su sencillez conceptual, son obtenibles por medio de un proceso de impresión de las antenas. Como no precisan de alimentación energética, el dispositivo puede resultar muy pequeño: pueden incluirse en una pegatina o insertarse bajo la piel (tags de baja frecuencia).

Debido a las preocupaciones por la energía y el coste, la respuesta de una etiqueta pasiva RFID es necesariamente breve, normalmente apenas un número de identificación (GUID). La falta de una fuente de alimentación propia hace que el dispositivo pueda ser bastante pequeño: existen productos disponibles de forma comercial que pueden ser insertados bajo la piel. En la práctica, las etiquetas pasivas tienen distancias de lectura que varían entre unos 10 milímetros hasta cerca de 6 metros, dependiendo del tamaño de la antena de la etiqueta y de la potencia y frecuencia en la que opera el lector.

2.3.1.2. Tags activos.

A diferencia de los tags pasivos, los activos poseen su propia fuente autónoma de energía, que utilizan para dar corriente a sus circuitos integrados y propagar su señal al lector. Estos tags son mucho más fiables (tienen menos errores) que los pasivos debido a su capacidad de establecer sesiones con el lector. Gracias a su fuente de energía son capaces de transmitir señales más potentes que las de los tags pasivos, lo que les lleva a ser más eficientes en entornos dificultosos para la radiofrecuencia como el agua y metal. También son efectivos a distancias mayores pudiendo generar respuestas claras a partir

de recepciones débiles (lo contrario que los tags pasivos). Por el contrario, suelen ser mayores y más caros, y su vida útil es en general mucho más corta.

Muchos tags activos tienen rangos efectivos de cientos de metros y una vida útil de sus baterías de hasta 10 años. Algunos de ellos integran sensores de registro de temperatura y otras variables que pueden usarse para monitorizar entornos de alimentación o productos farmacéuticos. Otros sensores asociados con RFID Activos incluyen humedad, vibración, luz, radiación, temperatura y componentes atmosféricos como el etileno. Los tags activos, además de mucho más rango (500 m), tienen capacidades de almacenamiento mayores y la habilidad de guardar información adicional enviada por el transceptor.

Actualmente, las etiquetas activas más pequeñas tienen un tamaño aproximado de una moneda. Muchas etiquetas activas tienen rangos prácticos de diez metros, y una duración de batería de hasta varios años.

2.3.1.3. Tags semipasivos.

Los tags semipasivos se parecen a los activos en que poseen una fuente de alimentación propia, aunque en este caso se utiliza principalmente para alimentar el microchip y no para transmitir una señal. La energía contenida en la radiofrecuencia se refleja hacia el lector como en un tag pasivo. Un uso alternativo para la batería es almacenar información propagada desde el lector para emitir una respuesta en el futuro, típicamente usando

backscatter. Los tags sin batería deben responder reflejando energía de la portadora del lector al vuelo.

La batería puede permitir al circuito integrado de la etiqueta estar constantemente alimentado y eliminar la necesidad de diseñar una antena para recoger potencia de una señal entrante. Por ello, las antenas pueden ser optimizadas para utilizar métodos de *backscattering*. Las etiquetas RFID semipasivas responden más rápidamente, por lo que son más fuertes en la razón de lectura que las pasivas.

Este tipo de tags tienen una fiabilidad comparable a la de los tags activos a la vez que pueden mantener el rango operativo de un tag pasivo. También suelen durar más que los tags activos.

2.3.2. Lector.

El lector es un dispositivo que puede leer o incluso escribir datos en tags RFID compatibles. El hecho de escribir en un tag se le llama “crear” un tag, proceso en el cual se le asocia un identificador que lo asociara a un objeto, al asociarlo lo que se esta haciendo es comisionar el tag. En contra, decomisionarlo es desasociarlo del objeto y destruyendo el tag opcionalmente. El tiempo que el lector emite energía RF para leer el tag es el ciclo de espera del lector.

El lector es la espina dorsal del hardware de un sistema RFID y esta compuesto por:

- Transmisor.
- Receptor.
- Microprocesador.
- Memoria.
- Entradas y salidas para los sensores externos / actuadores / alarmas.
- Controlador (suele ser externo).
- Interfaz de comunicación.
- Energía.

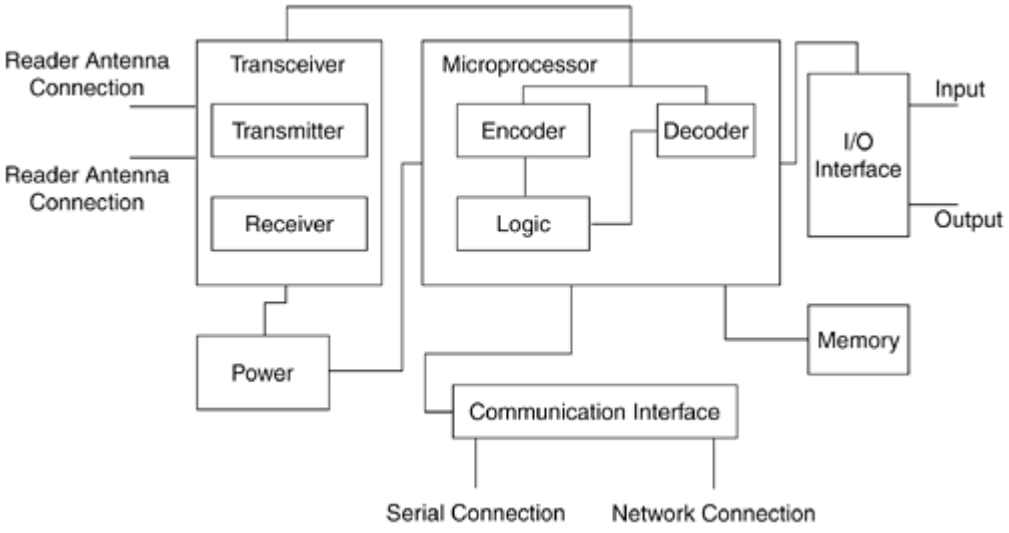


Figura 3. Estructura interna de un lector de RFID. Fuente: http://www.gii.upv.es/personal/gbenet/IIN/treballs%200607/RFID%20Por%20Diego%20Contreas%20Jimenez%20y%20Antonio%20Lacasa%20Corral.doc

2.3.2.1. Antena del lector.

El lector se comunica con los tags a través de de la antena del lector, que suele estar separada físicamente del lector y conectada con esta a través de un cable. La longitud del cable también esta limitada y como se mencionó anteriormente un lector puede soportar varias antenas a la vez. La antena es la que crea el campo electromagnético que induce la corriente el la antena del tag. Por consiguiente para conseguir que se lea un tag deberá estar próximo a la antena del lector. Hay algunos lectores que pueden llevar integrada la antena.

2.3.2.2. Controlador.

Un controlador es un agente intermedio que le permite comunicarse con una entidad externa y controlar el comportamiento de lector junto con los indicadores y los actuadores asociados con este lector. Un controlador es el único componente de un sistema RFID (o un lector, dependiendo del punto de vista) a través del cual las comunicaciones son posibles.

Un controlador también provee (o usa, dependiendo del punto de vista) un interfaz de comunicación para las entidades externas para interactuar con él.

2.3.2.3. Sensor, indicador y actuador.

Un lector no tiene por qué estar conectado todo el tiempo, puede ser encendido y apagado automáticamente si es necesario. Un sensor puede estar añadido con el lector para este objetivo. Este sensor sería el que encendería/apagaría el lector cuando algún evento producido en el exterior que detecte este sensor. Un sensor además puede ser usado para proveer algún tipo de lanzador al lector.

Un indicador es una señal electrónica. Ejemplo de indicadores son las alarmas audibles, señales luminosas, etc. Un conjunto de luces podría ayudar a diferenciar los distintos estados siendo cada estado de un color diferente. Por ejemplo el rojo indicaría que hay una etiqueta inválida o mala en la zona de lectura, verde podría indicar que es un tag válido y ámbar podría decir que se ha interrumpido la conexión entre el lector y el controlador.

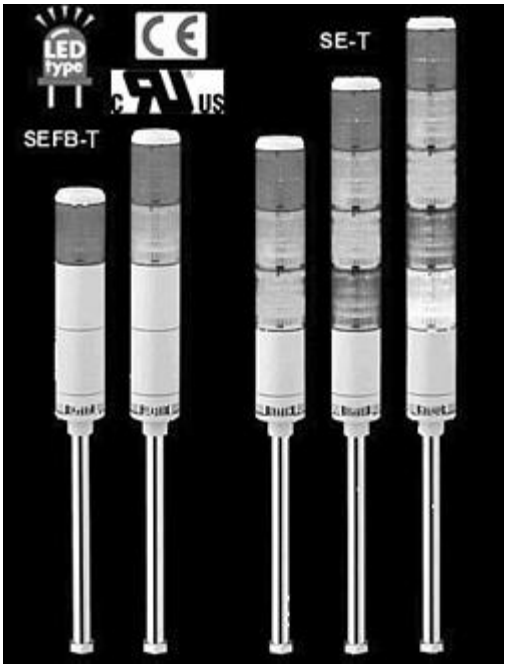


Figura 4. Indicador de RFID. Imagen tomada de http://www.gii.upv.es/personal/gbenet/IIN/treballs%200607/RFID%20Por%20Diego%20Contreas%20Jimenez%20y%20Antonio%20Lacasa%20Corral.doc

Un actuador es un dispositivo mecánico para controlar o mover objetos. PLCs, brazos de robot, brazos mecánicos para el acceso de una entrada, y cosas similares serían ejemplos de actuadores. Un PLC es uno de los actuadores más versátiles, y las PLCs son ampliamente usadas en las plantas de producción. PLCs activan una variedad de acciones para ser realizadas (como monitorizar y controlar una línea de embalaje).

Anunciadores y actuadores pueden también ser usados para proveer algún tipo de salida local desde un sistema RFID, como las alarmas audiovisuales en caso de un error de lectura, abriendo una entrada en caso de un lectura exitosa, y cosas así.

2.4. Equipo y Sistema Software.

El equipo y el sistema software es un término que engloba los componentes hardware y software, y que están separado del hardware propio RFID (eso es el lector, tag y antena); el sistema está compuesto por los siguientes componentes:

- Interfaz/sistema terminal
- Middleware
- Interfaz de la empresa
- Servidor de la empresa

En un sistema RFID no trivial, todos estos componentes pueden o no estar presentes.

2.5. Características de un Sistema RFID.

Las principales características de RFID, que la convierten en una tecnología susceptible de ser utilizada en múltiples aplicaciones, y con múltiples ventajas son:

• *Posibilidad de modificar los datos*. Según el estándar y etiqueta que se utilice.

• *Seguridad de los datos*. En las últimas generaciones de dispositivos RFID es posible cifrar los datos, de forma que no puedan ser leídos con lectores RFID estándar.

• *Cantidad de datos almacenados*. Hasta 1 MB de información en los últimos prototipos.

• *Costes*. En descenso a medida que se aplican los últimos avances tecnológicos.

• *Estándares*. Existen diferentes estándares universalmente aceptados, y relacionados con la banda de frecuencia utilizada, que determina el tipo de sistema RFID. Los dos estándares principales son el estándar EPC y el estándar ISO.

• *Vida útil*. Al no haber necesidad de contacto físico ni de baterías (en las etiquetas pasivas), la vida útil de las etiquetas pasivas es muy grande. Las etiquetas activas tienen limitada su vida útil a la duración de su batería (no obstante, puede ser elevada, del orden de años, dependiendo de la frecuencia de uso de las etiquetas).

• *Tamaño*. En general, desde el tamaño de un botón o un caramelo hasta el tamaño de un paquete de tabaco. Pero la evolución hacia la miniaturización es constante

• *Distancia de lectura*. Las etiquetas pasivas tienen un alcance del orden del metro y las activas pueden tener un alcance de decenas de metros. Además, para realizar la lectura o escritura no se necesita línea de visión directa.

• *Número de elementos que se pueden leer simultáneamente*. Un lector puede leer cientos de etiquetas de forma casi simultánea.

Por el contrario, la única desventaja notable es la posibilidad de interferencias, dado que en función de la frecuencia, los líquidos, madera o metales pueden impedir la propagación de las señales.

2.6. Funcionamiento RFID.

El funcionamiento de un sistema RFID es bastante simple. Enumerando las partes que componen el sistema, se tiene:

- Una antena de escaneo.
- Un transceptor con un descodificador para interpretar los datos.
- Un transpondedor - la etiqueta RFID - que se ha programado con la información.

La antena de escaneo coloca señales de radio-frecuencia en un rango relativamente corto. La radiación de RF hace dos cosas: Ofrece un medio de comunicación con el transpondedor (la etiqueta RFID) y proporciona a la etiqueta RFID la energía para comunicarse (en el caso de las etiquetas RFID pasivas).

Cuando una etiqueta RFID pasa a través del campo de exploración de la antena, se detecta la señal de activación de la antena. Que "despierta" el chip RFID, y se transmite la información sobre su microchip para ser incluida en el escaneo de la antena.

Las etiquetas RFID pueden leerse en una amplia variedad de circunstancias, donde los códigos de barras u otras tecnologías de lectura óptica son inútiles.

2.7. El Middleware.

El middleware es un software de conectividad que ofrece un conjunto de servicios que hacen posible el funcionamiento de aplicaciones distribuidas sobre plataformas heterogéneas. Su papel esencial es la gestión de la complejidad y la heterogeneidad de las infraestructuras distribuidas. Por un lado, el middleware ofrece abstracciones de programación que esconden algunas de las complejidades de la construcción de una aplicación distribuida. Por otra parte, existe una compleja infraestructura de software que implementa estas abstracciones. Con muy pocas excepciones, esta infraestructura tiende a tener una gran huella.

El middleware evita al usuario de enfrentarse a la complejidad y heterogeneidad de las redes de comunicaciones subyacentes, así como de los sistemas operativos y lenguajes de programación, proporcionando una interfaz de programación de aplicaciones para la fácil programación y manejo de aplicaciones distribuidas.

Por lo general el middleware del lado cliente está implementado por el Sistema Operativo subyacente, el cual posee las librerías que implementan todas las funcionalidades para la comunicación a través de la red.

2.7.1 Tipos de middleware.

Se pueden clasificar los diferentes middleware en función de su escalabilidad y su tolerancia a fallos, aunque pueden existir otros tipos de clasificaciones:

Monitores TP En los primeros días de las empresas de Tecnologías de Información, las arquitecturas de computadora se basaban en centrales y la interacción se llevaba a cabo a través de terminales que sólo mostraba la información preparada por el ordenador central.

Los Monitores de procesamiento de transacciones (TP Monitors), también llamados middleware de procesamiento de transacciones o simplemente middleware de transacción, fueron inicialmente diseñadas para permitir que los computadores centrales soportarán al mayor número posible de usuarios concurrentes.

Como parte de esta tarea, los monitores TP también necesitaban tratar con múltiples subprocesos y la coherencia de los datos, extendiendo la funcionalidad básica con el concepto de las transacciones. Son los más antiguos y más conocidos de middleware.

Hoy en día, los monitores de transacción distribuidos prevalecen para habilitar las transacciones de varios sistemas de gestión de bases de datos aislados.

Sistemas basados en RPC (Remote Procedure Call)-Cuando la descentralización de las empresas de TI se llevó a cabo como una consecuencia de la introducción de la PC, la funcionalidad comenzó a ser distribuida a través de unos pocos servidores.

A fin de realizar aplicaciones distribuidas, los desarrolladores estaban en necesidad de un poderoso mecanismo de abstracción para ocultar los tediosos detalles de la comunicación.

La llamada a procedimiento remoto (RPC) respondió a esta necesidad y fue originalmente presentada en como una forma de llamar a un procedimiento transparente situado en otra máquina. La RPC estableció en primer lugar, la noción de un cliente (el programa que llama a un procedimiento remoto) y un servidor (el programa la que se aplica el procedimiento remoto que se invoca). También, introdujo muchos conceptos ampliamente utilizados en la actualidad: el lenguaje de definición de interfaz (IDL), el nombre y directorio de servicios, de interfaces de servicios dinámica y vinculante. Hoy en día, los sistemas de RPC se utilizan como base para casi todas las demás formas de middleware.

Objeto Agente (Object Broker)- RPC fue diseñado y desarrollado en un momento en que los principales lenguajes de programación eran de procedimiento. Con el advenimiento de los lenguajes orientados a objetos el objeto se convirtió en el bloque de construcción del software, encapsulando datos y comportamientos.

Se desarrollaron plataformas de soporte para la invocación de objetos remotos, lo que guió a los objetos agentes. Estas plataformas están más avanzadas en sus especificaciones que la mayoría de los sistemas RPC, pero no difieren en medida significativa en cuanto a la aplicación. En la práctica, la mayoría de utilizan como RPC el mecanismo de fondo para aplicar las llamadas objeto remoto.

Monitores de Objeto. Cuando los agentes trataron de precisar y unificar la funcionalidad de plataformas de middleware, pronto se puso de manifiesto que gran parte de esta funcionalidad ya estaba disponible a partir de los Monitores TP. Al mismo tiempo, los monitores TP, inicialmente desarrollados para lenguajes de procedimiento, tuvieron que ser ampliados para hacer frente a los lenguajes orientados a objetos. El resultado de estas dos tendencias es la convergencia entre los monitores de TP y el objeto agente que dio lugar a los sistemas híbridos objeto llamado monitores de objeto.

Los monitores de objeto son, en su mayor parte, los monitores TP ampliados con interfaces orientadas a objetos. Los vendedores encontraron más fácil hacer parecer un

monitor de TP a un objeto agente que implementar agentes con todas las características de un monitor de TP y de los rendimientos requeridos.

Middleware orientado a mensajes (MOM) Los anteriores tipos de middleware se basaban en el método sincrónico de invocación, donde una aplicación cliente invoca un método ofrecido por un proveedor de servicios. Cuando el servicio proveedor ha concluido su trabajo, devuelve la respuesta al cliente. Esta "estrechamente unida" y "bloqueante" interoperabilidad muy pronto se convirtió en la una limitación para los desarrolladores de software.

La respuesta a este límite fue el middleware orientado a mensajes, que permite clientes y servidores comunicarse a través de mensajes, es decir, conjuntos de datos estructurados, normalmente caracterizados por un tipo de nombre y valor de pares. Este tipo de comunicación es posible gracias a las colas de mensajes controlada por el MOM. Las colas se pueden compartir entre múltiples aplicaciones, los destinatarios pueden decidir cuándo procesar mensajes y de modo que no tienen que sondear continuamente, se pueden asignar prioridades, solo para nombrar sólo algunas ventajas de este enfoque.

2.7.2 Middleware para RFID.

El **Middleware RFID** es una forma diferente de enfocar el clásico middleware conocido en el entorno informático. Así, debido al reciente desarrollo exponencial de la tecnología RFID, las funciones del Middleware RFID no se ajustan a las clásicas funciones informáticas de este tipo de interfaz por lo que compañías como Forrester Research, ABI Research y otras compañías han "consensuado" una definición de lo que se puede considerar un middleware destinado a la gestión de los eventos generados por un sistema RFID:

El RFID Middleware es la plataforma existente entre los lectores de tags y los sistemas de gestión empresariales para trabajar, gobernar y enviar los datos captados por el hardware RFID

A diferencia del middleware clásico, el middleware RFID trabaja en un extremo de la red y mueve los datos en el mismo punto de las transacciones. Las funciones básicas del middleware RFID son la monitorización, la gestión de los datos y de los dispositivos. De hecho, extrae los datos del lector, los filtra, agrega la información y los dirige al sistema de gestión; este sistema de gestión puede ser un ERP o cualquier tipo de aplicación vertical (sistema de producción, almacén, etc.).

No existe un registro histórico sobre el nacimiento y desarrollo de middleware RFID, pero si se conoce las causas que lo hicieron desarrollarse, como que los sistemas informáticos existentes en el año 2.000, no eran capaces de procesar el "torrente" de

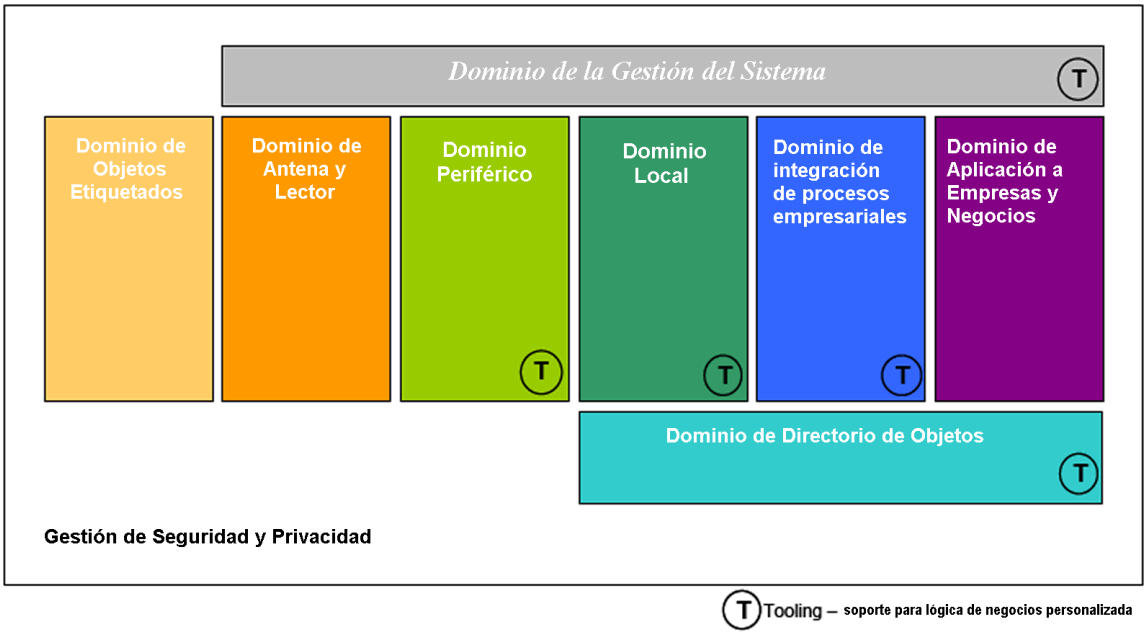
información que generaba un sistema RFID, sistemas capaces de leer más de 300 eventos por segundo. Si la ventaja del RFID era poder tomar decisiones "al momento", los sistemas informáticos existentes no eran capaces de dar respuesta eficiente a 300 lecturas en 1-2 segundos.

Empresas como Oracle, Microsoft, SAP, IBM e Intel se dieron cuenta de la problemática y cada uno de ellos, dentro de su propio campo de actuación, fueron preparando las plataformas para que los desarrolladores en Middleware RFID pudieran crearlos y hacerlos comercialmente viables.

2.7.2.1 Estructura del Middleware de RFID.

Viendo las dimensiones y el desarrollo del middleware destinado a gestionar los eventos RFID, la empresa EPC Global presento una opción globalizada para la estructura que debería tener un Middleware RFID. Esta opción ha sido comúnmente aceptada y es la forma como debe estructurarse un middleware RFID para que un sistema de identificación de productos a través de dicha tecnología, tenga los resultados deseados.

La infraestructura de RFID se puede dividir en distintos dominios. Un dominio es una agrupación de componentes relacionado de hardware y software. La siguiente figura proporciona una representación gráfica de los dominios contenidos en el Marco de Arquitectura de la RFID.



El dominio de objetos etiquetados contiene los productos etiquetados en una cadena de suministro, u otros bienes o lugares que pueden ser rastreados o vigilancia, incluido el uso de sensores en las etiquetas. Como el objeto y la etiqueta están juntos físicamente son considerados como componentes del mismo dominio.

En contraste con otros dominios, la mayoría de los artefactos en El dominio de objetos etiquetados son móviles, es decir, pueden moverse a través de diferentes infraestructuras de la RFID.

Esto impone unos requisitos de interoperabilidad de esos objetos que, idealmente, son abordados a través de estándares abiertos.

El dominio de lector y de la antena es la interfaz entre el mundo físico (objetos, etiquetas, las frecuencias de radio, etc.) y el mundo de las tecnologías de

información. El dominio puede incluir diversas frecuencias y tecnologías, como la de UHF, 13.56, Código de barras, o Puerta de los lectores de paletas.

El lector de la antena y de dominio incluye los dispositivos móviles que están conectados a través de una red inalámbrica. Los dispositivos móviles se conectan siempre al mismo dominio periférico, y por lo tanto, a la misma infraestructura de RFID.

El dominio de periferia incluye la funcionalidad de filtrado y la agregación de volúmenes de datos proporcionada por los lectores, el análisis de los datos y la aplicación de las decisiones locales, elaboración y la inteligencia. Esta actividad está en la periferia de la red antes de transmitir datos a los locales de dominio.

El dominio periférico suele ser un aparato de bajo costo situado antes de los lectores y establece una pila de software en el borde exterior de la infraestructura RFID . Un aparato controla múltiples lectores. Esto está organizado jerárquicamente y proporciona la segura entrega de mensajes en el dominio local, así como descubrimiento automático de lector y de autenticación.

El Dominio Local es el intermediario entre las aplicaciones de empresa y el Dominio Periférico. Comprende el sentido comercial de la lectura obtenida del RFID y permite la

toma de decisiones automática. Además, los filtros y los agregados, monitorean y aumentan los eventos RFID para la detección de operaciones de negocios críticas, o mantiene la ubicación de los objetos físicos.

Asimismo, amacena todos los registros importantes con información sobre los productos y lugares y administra otros componentes en otros dominios, tales como los lectores de RFID o los controladores. El dominio local es más típicamente jerárquico, en el sentido de un jefe de oficina que coordina subordinados locales.

El Dominio de Integración de Procesos de Negocios es un medio para conectar entre las aplicaciones de la empresa y la infraestructura RFID. Mientras que otros dominios proporcionan un nivel razonable de la funcionalidad 'fuera-del-marco', La Integración de Procesos de Negocios suele requerir cierta personalización para que coincida con un determinado entorno empresarial para cumplir su función. Puede por lo tanto, ser descrito como una caja de herramientas para la integración comercial.

El Dominio de Aplicación en Empresas y Negocios de contiene los componentes que requieren información sobre movimiento de los productos que será capturado por la infraestructura de RFID.

Estas capacidades se corresponden con una mezcla única de la organización de la cadena

de suministro, gestión y sistemas de apoyo a las empresas. Incluye el dominio de los sistemas que ayudan a pedidos, la gestión o el suministro de bienes. Ejemplos de ello son sistemas ERP, sistemas de gestión de almacén, Inventario Gestión, depósito de datos, gestión de mercancías, los sistemas de la tienda, y así sucesivamente.

El Dominio de Directorio de Objetos contiene componentes que proporcionan información sobre el objeto físico utilizando el ID como la clave de búsqueda. Puede obtener información sobre un producto y permite a las empresas compartir información a nivel de producto con seguridad. La información puede estar en tres niveles de precisión:

- Sobre el producto / unidad de mantenimiento de existencias (SKU) a nivel
- En instancia, que se conozca en el momento de la fabricación
- Instancia con el seguimiento y la ubicación de la historia

El Directorio de objetos de dominio es un área dinámica, con diferentes normas y evolución de los productos.

El Dominio de Gestión de Sistemas permite a los clientes supervisar a distancia, configurar, y actualizar el software y el firmware de los activos desplegados, tales como antenas, lectores, y servidores. Incluye la capacidad de gestionar y desplegar aplicaciones

de forma remota en un entorno distribuido.

También incluye un "panel" a través de la cual es posible recibir alertas cuando lectores, antenas, servidores se descomponen lo que aumenta la fiabilidad y reduce la gastos de operaciones.

La Gestión de Seguridad y Privacidad permite a los clientes extender la infraestructura de seguridad existente de una empresa hasta llegar a los lectores. Para la funcionalidad del núcleo de seguridad, la infraestructura debe proteger tanto a los datos almacenados como a los datos que están en tránsito.

La infraestructura se asegurará de que los datos almacenados sólo son visitados y modificado por componentes y personas autenticadas y autorizadas, y que los datos transmitidos se envían con controles de integridad y confidencialidad para permitir la detección de alteraciones, y evitar las intercepciones.

2.7.2.2 Funcionalidades Claves.

El middleware tiene muchas funcionalidades y cada uno de los fabricantes o desarrolladores de software le añade características que hacen que cada uno de ellos tenga su propia identidad. Por este motivo aquí se pretende indicar las funcionalidades de

manera genérica.

Gestión de dispositivos: La mayoría de los middleware pueden controlar cualquier tipo de hardware como lectores, tags, sensores, impresoras o dispositivos tipo actuadores (Input/Output). Puede controlar el estado de salud de los lectores, su funcionamiento y alertar a los administradores de su mal funcionamiento cuando este se produce. El software puede tener configurado escenarios de backup o alternativas a un mal funcionamiento como podría ser activar un segundo lector para que el sistema continúe funcionando sin ningún problema. Otra posible función dentro de la gestión es la actualización de los dispositivos que son gestionados, es decir, no hace falta actualizar cada uno de los dispositivos sino decirle al middleware que actualice todos los dispositivos que le indiquemos.

Procesamiento de datos: como es conocido, la RFID facilita la recogida de multitud de datos que permiten obtener en gran detalle lo que está sucediendo. Además estas lecturas son de manera automática, por este motivo es importante gestionar bien este gran volumen de datos. El middleware filtra estos datos recolectados por los lectores para evitar lecturas múltiples del mismo tag y evitar sobrecargar los sistemas de gestión empresarial. Esta característica que puede parecer simple es de gran importancia cuando el tamaño y la complejidad de los sistemas RFID crecen. Además de esta característica, el middleware puede añadir valor a la información antes de traspasarla a los sistemas de gestión empresarial. Puede configurar alertas según el estado de la información. Por

ejemplo, si se detecta que ciertos ductos perecederos están a punto o ya han expirado, el middleware lanzaría un aviso al sistema correspondiente para que los trabajadores realizaran los trabajos definidos en estos casos.

Para facilitar el filtrado de datos, EPCglobal (organización que estandariza la tecnología EPC-RFID), ha configurado una especificación de interfaz de middleware llamada ALE (Application Level Events). La mayoría de proveedores de middleware utilizan el estándar ALE para reducir los datos que se transmiten a los sistemas de back-end.

Conectar la información con las aplicaciones de negocio: los middleware tienen herramientas que incluyen APIs (Interfaces de Programas de Aplicaciones- *Application Program Interfaces*) . Estas interfaces son utilizadas por muchas empresas como puente para conectar los datos con su software de negocio. Por ejemplo, un ERP (Enterprise Resource Planning) se puede configurar para que reciba eventos desde las aplicaciones RFID de los centros de distribución o tiendas. Cuando un sistema de gestión de almacén (SGA o WMS) recibe una orden, lo pasa a través de una API al middleware, quién genera un EPC para cada caja del pedido, asociando la información EPC a la del pedido para crear una etiqueta RFID inteligente que se le ordena imprimir a la impresora correspondiente. Toda esta información puede ser enviada al ERP para que la registre y cree un ASN (Advance Shipment Notice) o aviso anticipado de envío al minorista que debe recibirlo.

2.7.3 Arquitectura del Middleware.

La arquitectura del middleware puede variar según la solución, en este caso se explica la arquitectura más completa. Las otras soluciones son partes de esta ya que la mayoría de middlewares son modulares adaptándose a las características de la empresa.

Se puede diferenciar dos glandes bloques: el Edge Server (ubicación local) y el Enterprise Server (ubicación central). Buscando una definición simple, el primero (Edge Server) es la infraestructura situada a nivel local donde se conectan los dispositivos RFID, en cambio el Enteprise Server se situaría donde la empresa centraliza sus aplicaciones (data center). Los múltiples Edge Servers se conectarían al Enterprise Server, quién se encargaría de trasladar la información a las aplicaciones de negocio a través de un bus empresarial (ESB) o conexión directa.

Su funcionamiento a grandes rasgos sería el siguiente; el lector lee un tag y lo envía al Edge Server, quién verifica y filtra los datos por si fuera una lectura fantasma o duplicada. Si está todo bien se genera un evento y se traspasa al Enterprise Server que registra los datos en el repositorio. Después, si este dato tuviese que generar una acción con otro aplicativo, el Enterprise Server sería el encargado de comunicarse y transferir la información necesaria para el cumplimiento del proceso empresarial. Cuando una aplicación realiza una petición de información es el Enterprise Server quién se encarga de

responder con los datos correctos.

Otro concepto que se debe tener claro es la iniciativa de middleware RFID propuesta por EPCglobal y que es la base de los estándares publicados.

Los componentes de la propuesta de EPCglobal son:

- Reader protocol: estándar joven que pretende tener una base común de comunicación para todos los lectores que firmen EPCglobal compliant.
- Agent Manager (ALE 2.0): gestión y notificación de los eventos RFID/EPC.
- Information Server: Repositorio propietario para cada empresa y de acceso público dónde existe la información de cada EPC leído.
- ONS (Object Name Server): repositorio local dónde estará almacenada la ruta para buscar la información (Information Server) respecto a un EPC leído.

2.7.4 Los retos del Middleware.

La interacción continua de la RFID con los procesos de negocio es muy importante, de aquí que existan retos para el software middleware.

Explosión de datos: la RFID nos puede proporcionar muchos más datos de los actuales pero estos deben ser registrados y gestionados. Depende del nivel de gestión habrá más o menos datos.

Interacción del mundo real con el informático: la gestión de la RFID muchas veces se realiza en ubicaciones que no son donde se producen los procesos operacionales de la empresa (fábricas, centros de distribución o tiendas.

Guardar los datos con significado: las lecturas RFID no son transacciones de negocio, por lo que el middleware les deberá de dar sentido a los datos mediante el filtrado y la agregación de valor.

Distribución geográfica: los despliegues RFID pueden ir más allá que las instalaciones tradicionales de informática al distribuirse geográficamente en múltiples ubicaciones. Esto podría ser el caso de una compañía aérea que trabaja en infinidad de aeropuertos.

Intercambio de datos: para obtener beneficios de negocio, las empresas deberán intercambiarse información.

Extensión e innovación: el impacto futuro de la tecnología es muy diferente a las actuales aplicaciones que hoy demandan las empresas pioneras en RFID, por este motivo es importante que el middleware se anticipe a las futuras necesidades y que independice la arquitectura a cambios de usos o tecnologías.

2.8. Aplicaciones del RFID.

Son muchos los sectores que pueden beneficiarse de las ventajas de la tecnología de auto-identificación por radiofrecuencia. Puede ser utilizado como método de control de calidad, producción y distribución, localización y seguimiento de objetos, identificación de materiales, control de stocks, etc. En este apartado se exponen de forma extensa tres de las aplicaciones más comunes.

2.8.1. Transporte público.

El transporte público es una de las aplicaciones en las que la mayor potencial existe para la uso de sistemas RFID, en particular las tarjetas inteligentes sin contacto. En Europa y los EE.UU. las asociaciones de tráfico operan con una enorme pérdida, a veces tanto como 40% del volumen de negocios, que debe ser constituido por las subvenciones de la comunidad y país en cuestión. Debido a la creciente escasez de recursos, las soluciones a largo plazo deben buscar que se disminuyan las pérdidas por la reducción de los costos y aumentar los ingresos.

El uso de tarjetas inteligentes sin contacto como electrónica de viaje podría aportar una importante contribución a la mejora de la situación (AFC = cobro automático). En el ámbito de la tarifa de gestión, en particular, hay mucho espacio para mejorar.

La malsana situación financiera de las empresas de transporte, naturalmente, tiene muchas diferentes causas. Sin embargo, los siguientes factores son dignos de mención en relación con electrónica de viaje:

• Las empresas de transporte incurren en elevados costes a través de la venta de viajes pasa por automático expendedoras.

• En los vehículos también, se requieren caros billetes electrónicos o dispositivos móviles.

A veces, las entradas se venden incluso por el conductor, lo que provoca largos tiempos de espera mientras que los pasajeros abordan, además del riesgo de seguridad adicional presentada por la continua la distracción del conductor.

• Los boletos se tiran a la basura después de su uso, a pesar de que la fabricación de a prueba de fraude entradas para las empresas de transporte es cada vez más caro.

• En ciudades de Alemania en particular, las pérdidas de hasta un 25% deben tenerse en cuenta debido a la “tarifa dodgers” (Czako, 1997). Esto se debe a que las empresas alemanas de transporte tienen condiciones de viaje muy liberales permiten la entrada en el sistema subterráneo y autobuses que el pase de viajes sea comprobado primero.

• Los descuentos de asociaciones solo pueden ser calculados sobre la base de cuentas de costos al azar, lo que conduce a la imprecisión en el cálculo.

2.8.2. Control de Acceso.

Sistemas electrónicos de control de acceso utilizando los soportes de datos se utilizan para comprobar automáticamente la autorización de acceso de las personas a los edificios, (comercial o evento) locales o habitaciones individuales. En el diseño de tales sistemas en primer lugar debemos diferenciar entre fundamentalmente dos sistemas diferentes con sus correspondientes propiedades: sistemas en línea y sistemas fuera de línea.

2.8.2.1. Sistemas en línea.

Los sistemas en línea tienden a ser utilizados en casos donde se requiere que la autorización de acceso de un gran número de las personas deba ser verificada en unas pocas entradas.

Este es el caso, por ejemplo, en las entradas principales de los edificios de oficinas y locales comerciales. En este tipo de sistema, todos los terminales están conectados a una computadora central por medio de una red.

El ordenador funciona con una base de datos en la que a cada terminal se le asigna todos los portadores de datos autorizados para el acceso a ese terminal. La autorización de los datos generados la base de datos se carga en los terminales (o en una unidad de control de

la puerta intermedia) a través de la red y se guardan allí en una tabla.

Cambios en los datos acceso de una persona pueden ser hechos por una sola entrada en la computadora central del sistema de control de acceso. El soporte de datos en sí no requiere estar presente, ya que sólo una entrada en la base central de datos tiene que ser editado. Esto es ventajoso, ya que significa que las zonas sensibles de seguridad pueden proteger contra el acceso no autorizado, incluso en el caso de pérdida de datos. Los soportes de datos de un sistema en línea sólo tienen que ser capaz de almacenar una pequeña cantidad de datos, por ejemplo, un número único paso. El uso de transpondedores de sólo lectura es también posible.

2.8.2.2. Sistemas fuera de línea.

Los sistemas fuera de línea se han prevalecido principalmente en situaciones en las que muchas habitaciones, a la que sólo unas pocas personas tienen acceso, se han equipado con un sistema de control de acceso electrónico. Cada terminal guarda una lista de identificadores de clave, para las que el acceso a este terminal es que debe autorizarse. No hay ninguna red con otros terminales o un ordenador central.

La información relativa a las habitaciones a los que el portador de datos que puede

proporcionar el acceso es almacenado en el portador mismo en la forma de una tabla de identificadores de clave.

El terminal compara los principales identificadores almacenados sobre un soporte de datos con los datos almacenados en su propia lista y permite el acceso tan pronto como una coincidencia se encuentra. El transpondedor está programado en una estación central de programación.

Sólo en el caso de pérdida de un portador de datos los identificadores deben suprimirse desde la terminal en cuestión mediante un dispositivo de programación. Sistemas fuera de línea ofrecen las siguientes ventajas sobre las convencionales con sistemas de bloqueo de clave.

• Los principios de la especificación de un plan de bloqueo en el sentido normal, no son necesario. El sistema es inicialmente codificado para su uso como un sitio de construcción. Cuando el sitio es entregado, la puerta de terminales es re-codificada para uso comercial por medio de una interfaz de infrarrojos. Posteriores modificaciones y ampliaciones que no plantean ningún problema.

• La opción de programación de tiempo abre nuevas opciones.

• La pérdida de una clave no causa problemas. Los en caso de la pérdida de una clave, se suprimirán las informaciones en las estaciones a leer, una nueva clave se programa, y los datos de esta clave se introducen en los terminales en cuestión.

2.8.2.3. Transpondedores.

El control de acceso mediante tarjetas de PVC ha sido utilizado por mucho tiempo. Se utilizaron inicialmente las tarjetas perforadas, que fueron sustituidos por infrarrojos pasa, magnético pasa banda, pasa Wiegand (tiras magnéticas de metal) y, por último, las tarjetas inteligentes con la incorporación de un microchip. Las principales desventaja de estos procedimientos es la inconveniencia de los procedimientos de operación debido el hecho de que las tarjetas siempre deben ser insertada en un lector de la manera correcta ronda.

El control de acceso sin contacto utilizando sistemas permite mucha más flexibilidad, porque el transpondedor sólo necesita pasar a una corta distancia de la antena del lector. Los pases se pueden efectuar en forma de tarjetas inteligentes sin contacto, llaveros, y hasta relojes de pulsera.

Una gran ventaja de los sistemas de control de acceso sin contacto es que el lector está de mantenimiento libre y no está influenciado por el polvo, la suciedad o la humedad. La antena se puede montar 'en el yeso ", donde es completamente invisible y protegido contra el vandalismo. Manos libres los lectores también están disponibles para el montaje o en los torniquetes para aumentar conveniencia.

2.8.3. La inmovilización electrónica.

El fuerte aumento en el robo de vehículos al comienzo de la 1990 impulsado la demanda de sistemas efectivos para prevenir los robos. Dispositivos de control remoto de con un rango de 5-20m ya habían estado disponibles en el mercado años atrás. Estos son pequeños transmisores de RF o infrarrojos que operan en la frecuencia 433,92 MHz, que se utilizan principalmente para controlar un sistema de bloqueo central y una alarma.

Un inmovilizador también puede ser acoplado junto al mando a distancia de control. En este tipo de dispositivo anti-robo, sin embargo, el seguro mecánico del vehículo todavía ser usado para acceder al vehículo.

Esta es la mayor debilidad de este tipo de sistema, ya que el sistema no puede comprobar si la llave mecánica es la auténtica. Los vehículos no están bien asegurados de esta manera por lo que pueden ser abiertos con una herramienta adecuada y puestos en marcha por una persona no autorizada.

Desde mediados de la década de 1990, la tecnología de los transpondedores ha

proporcionado una solución que puede utilizarse para comprobar la autenticidad, es decir, la autenticidad, de la llave. Esto ofrece una solución ideal para la inmovilización electrónica a través del bloqueo de la función de encendido.

2.8.3.1. La funcionalidad de un sistema de inmovilización.

En un sistema de inmovilización electrónica una llave mecánica se combina con un transpondedor. Un transpondedor miniatura con una antena de ferrita se incorpora directamente en la parte superior de la llave. La antena de lectura está integrada en el seguro de ignición.

El lector de la antena está integrado en la cerradura de encendido, de tal manera que cuando la llave de encendido se inserta, el acoplamiento inductivo entre la antena del lector y la bobina del transpondedor se optimiza. El transpondedor se alimenta con la energía a través del acoplamiento inductivo y, por tanto, esta totalmente libre de mantenimiento.

Los Inmovilizadores electrónicos suelen funcionar con una frecuencia de transmisión en la gama LF 100-135 KHz., la modulación ASK es la preferida para el procedimiento de modulación de la transferencia de datos en el transpondedor, porque permite que los lectores y el transpondedor se fabriquen muy barato. La modulación de carga es el único

procedimiento utilizado para la transmisión de datos desde el transpondedor al lector. Cuando la llave de encendido se enciende en el cerrojo de encendido para iniciar el vehículo, el lector se activa y se intercambian datos con el transpondedor de la llave de encendido.

Tres procedimientos se emplean para comprobar la autenticidad de la clave:

• Comprobación de un número de serie individual.

• Código de procedimiento Rolling. Cada vez que la clave está en funcionamiento un nuevo número está escrito a la tecla del transpondedor de la memoria. Este número es generado por un generador pseudo-aleatorio en el lector del vehículo, por lo cual es imposible duplicar el transpondedor si este sistema es usado.

• Procedimientos criptográficos (autenticación) con llaves fijas.

El lector RFID se comunica ahora con la parte electrónica del motor del vehículo, aunque esta comunicación es protegida por los procedimientos de cifrado. La electrónica del motor controla todas las funciones importantes del vehículo, en particular, el sistema de encendido y sistema de combustible.

La instalación de este tipo de inmovilizador electrónico del motor del sistema de gestión sólo puede ser realizada en la fábrica por el fabricante del vehículo, garantizando así interacción óptima entre el motor y sistema de control de dispositivo de seguridad.

TEMA 3: SISTEMAS DE SEGURIDAD EN ESTACIONAMIENTOS

3.1. Seguridad en Estacionamientos.

La seguridad para estacionamientos ha estado recibiendo bastante importancia en los últimos tiempos. Es interesante observar que cuando un sistema de seguridad para estacionamientos se ha aplicado, aumenta en los usuarios el sentido de seguridad. El aumento del uso de los parqueos por parte de las personas se traduce en un aumento de beneficios para las tiendas y centros comerciales que podrían justificar el aumento de los costos relacionados con mejoras de seguridad. Dos de los factores más importantes que contribuyen a un sistema de seguridad efectivo en los estacionamientos son la iluminación y el diseño del lugar.

3.1.1. Iluminación.

El alumbrado de seguridad se utiliza para aumentar la eficacia de los guardias y de circuito cerrado de televisión, en caso de utilizarse uno, aumentando el alcance visual de los guardias o del circuito cerrado de televisión durante los períodos de oscuridad o aumentando la iluminación de un espacio donde la luz natural no alcanza o es insuficiente. La iluminación también tiene valor como elemento de disuasión a posibles personas en busca de una oportunidad de cometer un delito. Normalmente, las luces de

seguridad requieren menos intensidad que las de las áreas de trabajo. La excepción se encuentra en las puertas normales. La iluminación exterior para áreas como estacionamientos, está obligada a garantizar un nivel mínimo de visibilidad a los guardias cuando se utilizan para realizar tareas de inspección del área protegida. Los guardias de los sistemas de vigilancia y circuito cerrado de televisión deben ser capaces de observar la actividad, inspeccionar los vehículos, los intentos de entrada ilegales, detectar intrusos en el área protegida, y observar las circunstancias inusuales o sospechosas. Cada estacionamiento presenta sus propios problemas particulares sobre la base de la disposición física, el terreno, las condiciones atmosféricas, y los requisitos de seguridad.

El objetivo de la iluminación directa es proporcionar una determinada intensidad en toda la zona como apoyo a los agentes de seguridad o al circuito cerrado de televisión, proporcionando una buena visibilidad para los clientes o empleados y con un mínimo de reflejos.

Los niveles de iluminación en las entradas, salidas, zonas de carga no debería ser inferior a dos veces la iluminación de la zona de aparcamiento adyacente o de la calle adyacente, que cada vez es mayor. Los requisitos de iluminación para CCTV son considerablemente inferiores a las necesarias para la observación visual directa, dependiendo del tipo de sistema seleccionado. Las cámaras de circuito cerrado de televisión deben estar orientadas de modo que no sean cegadas por el aumento o la puesta del sol, los faros de

automóviles y las reflexiones de estacionamiento luminarias.

3.1.2. Diseño.

El diseño de un estacionamiento a veces puede proporcionar una ventaja natural para la vigilancia, la cobertura de un circuito cerrado de televisión y la estructura de vigilancia y respuesta. Los estacionamientos para los centros de venta al por menor son únicos porque no hay forma de controlar quién tiene acceso a diferencia de las zonas de negocio donde se puede controlar el acceso si el riesgo potencial para los empleados así lo justifica. Para la disposición de plazas de estacionamiento para los centros de venta al por menor, es necesario determinar en primer vistazo las posibilidades de aparcamiento en secuencia y si existe una forma natural para optimizar la vigilancia. Normalmente, los clientes minoristas que llegan temprano también se van temprano, siendo entonces las llegadas tardías los espacios menos seguros. Dado que estas llegadas tardías también suelen ser los últimos en salir, también son los más vulnerables a la delincuencia. Al re-direccionar el tráfico entrante y saliente a través del estacionamiento para pasar por las zonas más remotas, aumenta la vigilancia y se reducen los crímenes.

3.2. Sistemas de Seguridad por Cámaras.

3.2.1 CCTV.

El Circuito cerrado de televisión o su acrónimo CCTV, que viene del inglés: Closed Circuit Television, es una tecnología de vídeo vigilancia visual diseñada para supervisar una diversidad de ambientes y actividades.

Se le denomina circuito cerrado ya que, al contrario de lo que pasa con la difusión, todos sus componentes están enlazados. Además, a diferencia de la televisión convencional, este es un sistema pensado para un número limitado de espectadores.

El circuito puede estar compuesto, simplemente, por una o más cámaras de vigilancia conectadas a uno o más monitores o televisores, que reproducen las imágenes capturadas por las cámaras. Aunque, para mejorar el sistema, se suelen conectar directamente o enlazar por red otros componentes como vídeos u ordenadores.

Estos sistemas incluyen visión nocturna, operaciones asistidas por ordenador y detección de movimiento, que facilita al sistema ponerse en estado de alerta cuando algo se mueve delante de las cámaras. La claridad de las imágenes puede ser excelente, se puede transformar de niveles oscuros a claros. Todas estas cualidades hacen que el uso del CCTV haya crecido extraordinariamente en estos últimos años.

3.2.1.1. Historia.

El Circuito Cerrado de Televisión se inicia junto con la televisión misma. De hecho, los primeros sistemas de CCTV se crearon antes que la misma televisión para el público, la cual tuvo mucho más crecimiento.

El primer sistema de circuito cerrado de televisión fue instalado por Siemens, SA en el Banco de pruebas VII en Peenemünde, Alemania, en 1942, para observar el lanzamiento de cohetes V-2. El ingeniero alemán Walter Bruch fue responsable del diseño y la instalación del sistema.

Sistemas de grabación de circuito cerrado de televisión a menudo siguen siendo utilizados en los lugares de lanzamiento de modernos para registrar el vuelo de los cohetes, a fin de encontrar las posibles causas de mal funcionamiento, mientras los cohetes más grandes son a menudo equipados con circuitos cerrado de televisión, lo que permite imágenes de la etapa de separación que se devuelven a la tierra por enlace de radio.

En septiembre de 1968, Olean, Nueva York fue la primera ciudad en Estados Unidos para instalar cámaras de vídeo a lo largo de su calle principal de negocios en un esfuerzo por combatir la delincuencia. El envío de las imágenes de un circuito cerrado de cámaras de televisión al Departamento de Policía de Olean propulsó a Olean a la vanguardia de la

tecnología en lucha contra el crimen.

El uso de circuitos cerrados de televisión se hizo muy común más tarde en los bancos y tiendas de desalentar el robo, mediante el registro de pruebas de actividad delictiva. Su uso popularizó aun más el concepto.

El CCTV tuvo un uso muy especializado durante el siglo pasado, más que nada debido a el precio de las cámaras, el cual limitaba tremendamente las aplicaciones. Con el advenimiento de los nuevos sistemas de captación de imagen en las cámaras, dado a un alto crecimiento del crimen y la inseguridad, provocaron un incremento en la producción y un decremento en los precios.

En la actualidad los sistemas CCTV están al alcance de cualquier organización, empresa o familia, y sus aplicaciones prácticamente no tienen límite. En muchos hogares se utilizan como sistemas de seguridad. En las plantas industriales, los equipos de circuito cerrado de televisión pueden utilizarse para observar las partes de un proceso de una central de control, cuando, por ejemplo, el medio ambiente no es adecuado para los seres humanos. Sistemas de CCTV pueden funcionar continuamente o sólo cuando sea necesario para controlar un evento en particular.

Una forma más avanzada de circuitos cerrados de televisión, la utilización de Digital Video Recorders (DVRs), dispone de grabación para, posiblemente, muchos años, con

una variedad de opciones de calidad y rendimiento y características extra (como la detección de movimiento y alertas por correo electrónico).

Al bajar significativamente su precio las videograbadoras de lapso de tiempo se integraron a los sistemas de CCTV (casi a la 5ª parte en sólo 3 años), y desplazaron al monitor como parte fundamental de un sistema. Las nuevas videograbadoras digitales compiten en precio con las analógicas, y podemos decir que existe equipo para todos los niveles y requerimientos de la sociedad.

3.2.1.2. Componentes de los Sistemas de CCTV.

Los sistemas de CCTV más sencillos están compuestos por 3 componentes básicos:

- La Cámara

Cámara CCD color conmutación día/noche y WDR.
Imagen obtenida de http://www.accesor.com/esp

El punto de generación de video de cualquier sistema de CCTV es la cámara.

Existen cámaras que incluyen un micrófono integrado.

Hay muchísimos tipos de cámara, cada una para diferentes aplicaciones y con diferentes especificaciones, pero se pueden clasificar en dos grandes grupos:

-*Cámaras de vídeo analógicas*

Puede grabar directamente a una grabadora de cintas de vídeo que son capaces de grabar señales analógicas como las imágenes. Si la señal analógica se graba en cinta, entonces la cinta se debe ejecutar en una velocidad muy lenta para operar continuamente. Esto se debe a que, a fin de permitir un recorrido de 3 horas de cinta para correr durante 24 horas, debe estar configurada para ejecutarse en un lapso de tiempo base que suele ser alrededor de 4 fotogramas por segundo.

-*Cámaras de vídeo digitales*

Estas cámaras no requieren una tarjeta de captura de vídeo, ya que trabajan mediante una señal digital que se pueden guardar directamente a un ordenador. La señal se comprime 5:1, pero la calidad de DVD se puede conseguir con más compresión.

Almacenar grabaciones digitales sin comprimir requiere una enorme cantidad de espacio en el disco duro, y un par de horas de vídeo sin comprimir rápidamente podría llenar un disco duro.

Señales analógicas también puede convertirse en una señal digital para que las grabaciones que se almacenen en un ordenador como las grabaciones digitales. En este caso, la cámara de vídeo analógico debe estar conectada directamente a una tarjeta de captura de vídeo en un ordenador, la tarjeta posteriormente convierte la señal analógica a

digital. Estas tarjetas son relativamente baratas, pero inevitablemente, la señal digital resultante se comprime 5:1 (compresión MPEG) para que las grabaciones de vídeo que se guarden en una base continua.

- Lentes:

En los sistemas de CCTV profesionales las cámaras vienen sin lente y únicamente con un conector rosca para que el instalador ensamble el lente que se adapte mejor a los requerimientos, los cuales varían de acuerdo a:

Distancia del objeto.
Angulo mínimo de observación.
Varifocal o fijo.
Intensidad de luz, variable o fijo.
Telefoto variable o fija.

No todos los lentes tienen ajuste de foco e iris. La mayoría debe tener ajuste de iris; algunos lentes de muy amplio ángulo no tienen anillo de enfoque.

- El monitor

La imagen creada por la cámara necesita ser reproducida en la posición de control. Un monitor de CCTV es prácticamente el mismo que un receptor de televisión, excepto que

éste no tiene circuito de sintonía. Pero la característica principal es la durabilidad de su pantalla. El CCTV se requieren 24 horas de trabajo sin perdida de la calidad de la imagen, durante muchos años en ambientes difíciles u hostiles.

Monitor de CCTV. Imagen obtenida de http://www.seguridaddigital.com.mx/

3.2.1.3. Los sistemas de CCTV.

El sistema más simple es una cámara conectada a un monitor a través de un cable coaxial con el suministro de la energía eléctrica para la cámara a través del monitor. Esto es conocido como una cámara energizada por el cable. Los primeros sistemas incluían una sola cámara, luego aparecieron sistemas con 2, 3 y 4 cámaras las cuales eran secuenciadas automáticamente por el monitor, precisamente por un "secuenciador" inter-construido. Estos sistemas últimamente incluyen un sistema quad (cuádruple), el cual permite observar las imágenes de las 4 cámaras en forma simultánea.

El cable coaxial transporta la señal de video desde la cámara hacia el monitor. Sin embargo, se debe tomar en cuenta que la instalación debe cumplir con las regulaciones existentes. Estas conexiones permiten una gran flexibilidad en el diseño de sistemas completos. Cuando se requiere más de una cámara, se debe incluir un conmutador de video

3.2.1.4. Tecnología.

La primera utiliza cámaras de circuito cerrado de televisión en los espacios públicos eran de muy baja definición en blanco y negro, sin sistemas de la capacidad de acercamiento o alejamiento. Las modernas cámaras de circuito cerrado de televisión de alta definición usan pequeñas cámaras en color que no solo pueden centrarse para una resolución minuciosa, pero al vincular el control de las cámaras a un ordenador, se pueden rastrear objetos de forma semiautomática. La tecnología que permite esto es a menudo citada como VCA (Análisis de contenido de vídeo), y actualmente está siendo desarrollada por un gran número de empresas tecnológicas en todo el mundo. La tecnología utilizada en la actualidad en los sistemas permiten reconocer si un objeto en movimiento es una persona a pie, una persona arrastrándose o vehículo. También puede determinar el color del objeto. NEC proclama tener un sistema que puede identificar a una persona de edad, mediante la evaluación de una foto de él / ella. Otras tecnologías claman poder identificar a las personas por sus datos biométricos.

Lo que puede hacer el sistema es básicamente determinar donde está una persona, es decir, cómo se está moviendo y si es una persona o por ejemplo un coche. También es posible dotar al sistema de normas, como por ejemplo "activar la alarma cuando una persona camine cerca de la valla" o en un museo "activar una alarma si una pintura es bajada de la pared".

No hay ninguna limitación tecnológica que prevenga a una red de cámaras de este tipo

dar seguimiento a la circulación de las personas. También se han hecho informes de que lecturas de reconocimiento de placas de erróneas llevaron a multas de personas equivocadas.

Los críticos CCTV ven la más preocupante extensión de esta tecnología en el reconocimiento de rostros con imágenes de alta definición de CCTV. Esto podría determinar la identidad de una persona sin que le adviertan de que su identidad está siendo verificada y registrada. Los sistemas pueden comprobar miles de caras en una base de datos en menos de un segundo.

La combinación de circuitos cerrados de televisión y de reconocimiento facial ha sido juzgado como una forma de vigilancia en masa, pero ha sido ineficaz debido al bajo poder de discriminación de las técnicas de reconocimiento facial y el elevado número de falsos positivos generados. Este tipo de sistema se ha propuesto para comparar rostros en los aeropuertos y puertos marítimos con los de los sospechosos de terrorismo.

En monitoreo computarizado de imágenes de CCTV está en vías de desarrollo, de modo que un operador humano CCTV no tiene que buscar sin cesar en todas las pantallas, lo que permite a un operador que observar muchos más cámaras de CCTV. Estos sistemas no observan la gente directamente. En su lugar, un seguimiento de su comportamiento, mediante la búsqueda de determinados tipos de comportamientos corporales, o

determinados tipos de ropa o equipaje.

La teoría detrás de esto es que en los espacios públicos las personas se comportan de forma previsible. Personas que no son parte de la "multitud", por ejemplo, los ladrones de automóviles, no se comportan de la misma manera. El equipo puede identificar sus movimientos, y alertar al operador que están actuando fuera de lo común.

3.2.2. Retención y almacenamiento.

El almacenamiento a largo plazo de grabaciones de circuito cerrado de televisión es un tema de preocupación en la aplicación de un sistema de circuito cerrado de televisión. Medios reutilizables, tales como las cintas de VHS, se pueden usar a través de un ciclo de grabación a intervalos regulares. Hay límites en la retención de datos.

La grabación del video se convirtió en una aplicación muy común con capacidades para el mercado doméstico desde principios de los 80s. Las videograbadoras en el CCTV aparentemente tiene el mismo diseño que un sistema doméstico, con la diferencia de que cuentan con funciones adicionales diseñadas específicamente para el mercado de la seguridad.

El principio de la funcionalidad de una VCR para seguridad es que deberá de grabar por lo menos 24hrs. La grabación se hará en forma 'periódica' (por un lapso de tiempo), en lugar de 'continua' (grabadoras domésticas).

La videograbadora de seguridad permite seleccionar los intervalos de tiempo en los que se desea grabar, dependiendo de sus requerimientos. Esta forma de grabar en intervalos de tiempo es conocido como "tiempo-lapsado".

Las grabaciones se conservan por varias causas. En primer lugar, el objetivo principal para el que fueron creados (por ejemplo, para supervisar una instalación). En segundo lugar, deben ser conservados durante un período razonable de tiempo para recuperar cualquier tipo de prueba de otras actividades importantes que podrían documentarse (por ejemplo, un grupo de personas pasa por una instalación de la noche se cometió un delito). Por último, las grabaciones pueden ser evaluadas con fines históricos, de investigación o de otras prestaciones a largo plazo de información de valor que puede contener.

3.2.2.1. Los DVRs.

DVR de 16 canales con audio. Imagen obtenida de www.fragaservi.com/admin/productos/1501200812055

Los avances tecnológicos en los sistemas de cómputo y redes han alcanzando a la industria de la Seguridad y los métodos de grabación han implementado tecnologías digitales para lograr una mejor evidencia. Las videograbadoras digitales (DVRs) ahora convierten el video análogo de los sistemas de CCTV en sistemas digitales.

Los DVRs se han convertido en los dispositivos que son ricos en características adicionales y la prestación de servicios excede la simple grabación de imágenes de vídeo que antes se realizaba a través de los VCRs. Un sistema de CCTV DVR ofrece una multitud de funciones avanzadas en tecnología de vídeo de vídeo incluyendo búsquedas por caso, la hora, la fecha y la cámara. También hay mucho más control sobre la calidad y la velocidad de cuadro que permite la utilización del espacio de disco para optimizar el DVR y también se pueden configurar para sobrescribir la más antigua de las imágenes de seguridad en caso de que el disco se llena. DVR en algunos sistemas de seguridad de acceso remoto a las imágenes de seguridad mediante un ordenador también se puede lograr mediante la conexión del DVR a una red LAN o Internet.

3.2.2.2. Los NVRs.

En Network Video Recorder anuncia la llegada del próximo punto natural en el desarrollo de la tecnología de grabación.

Es importante diferenciar entre DVRs y NVRs, ya que ambos a menudo se denominan "digital". Un DVR comprime digitalmente las entradas de vídeo analógico y las almacena en un disco duro, el término "digital" se refiere a la tecnología de compresión y almacenamiento, no de la transmisión de imágenes de vídeo. El DVR, por lo tanto, tiene

que estar situado cerca de los canales analógicos. En contraste un NVR almacena las imágenes digitales directamente desde una red IP.

Sistema de NVR. Imagen obtenida de http://www.channelinsider.com/

Por lo tanto, la diferencia más obvia entre el DVR y NVR es que mientras que el DVR registra líneas de datos análogas provenientes de cámaras analógicas, el NVR registra el vídeo que ya ha sido codificado en las cámaras. Por lo que no se encuentran conectores de vídeo en ningún lugar de una NVR, su entrada y salida son datos IP que comprended videos comprimido y codificados. En general, en formato MPEG-4 que ha gozado de amplia adopción en la industria de circuito cerrado de televisión como la actual tecnología de compresión, debido en gran medida a su eficiencia.

La gran ventaja de la arquitectura basada en NVRs es que pueden estar ubicados en cualquier parte de una red. Su localización es transparente para el operador - él o ella simplemente llama a la secuencia de vídeo grabada para ser vista y, siempre que tengan la autorización necesaria ahí está. Los NVRs graban y reproducen simultáneamente, y las grabaciones en cualquier máquina pueden ser vistas a distancia por un número de operadores autorizados propagados a través de la red al mismo tiempo, totalmente independientes y sin afectar a los demás.

Los NVRs competentes ahora incorporan características tales como:

- Discos intercambiables.
- Simple Network Management Protocol (SNMP)
- Diagnóstico integrado.
- Protección en contra de la supresión de los archives.
- Cortafuegos para la protección de datos contra el acceso no autorizado integrado.
- Función de exportación de archivos que encarna la firma de agua y la firma digital basada en los fotogramas de vídeo y de auditoría de la seguridad
- Sincronización de audio y video en la grabación y la reproducción
- Monitoreo de temperatura del disco duro.
- Fuentes de alimentación y conexiones de red, dobles y totalmente redundantes.

Técnicas "Espejo" son a menudo utilizadas para la grabación de duplicado de vídeo en NVRs adicionales situados en diferentes partes de la red, lo que proporciona un alto nivel de protección contra fallo de red, si una parte se va el otro está allí como una copia de seguridad

3.2.2.3. Las Cámaras IP.

Las cámaras IP son cámaras de circuito cerrado de televisión (CCTV) que utilizan el Protocolo de Internet para transmitir datos de imágenes y señales de control a través de una conexión Fast Ethernet. Como tal, cámaras IP también comúnmente se conoce como red de cámaras. Las cámaras IP se utilizan principalmente para la vigilancia de la misma manera que el CCTV análogo. Una serie de cámaras IP suelen desplegarse junto con una grabadora de vídeo digital (DVR), o una grabadora de vídeo de red (NVR) para formar un sistema de vigilancia por vídeo.


Cámara IP inalámbrica. Imagen obtenida de http://www.tradevv.com

La primera cámara IP fue lanzada en 1996 por Axis Communications. Utilizaba una plataforma de Linux integrada al interior de la cámara.

Al igual que con las cámaras fotográficas digitales, la resolución de cámaras IP se ha incrementado con el tiempo. Cámaras IP para CCTV están disponibles en las

resoluciones de 1, 2, 3, 5 y hasta 11 megapíxeles. Hoy en día hay muchos fabricantes de cámaras IP.

La CCTV analógica usa formatos de CCTV y de televisión establecidos (por ejemplo, CIF, NTSC, PAL y SECAM). Dado que las normas de vídeo analógico han madurado, la preocupación por la incompatibilidad entre las cámaras de vigilancia analógicas y sistemas de registro son poco frecuentes.

Cámaras de vigilancia IP, por otra parte, no se benefician del mismo nivel de la normalización. En términos generales, las marcas de cámaras IP serán diferentes en función de sus características específicas y funciones de codificación de vídeo (compresión), con el apoyo protocolos de red, y la aplicación para ser utilizada por el software de gestión de vídeo.

Con el fin de abordar cuestiones relativas a la normalización de la propiedad intelectual de vigilancia por vídeo, dos grupos de la industria se unieron en 2008. El Foro de Interface de Video de Red Abierta (ONVIF) y la Alianza de Interoperabilidad de Seguridad Física (PSIA). Si bien el PSIA fue fundado por Cisco y ONVIF fue fundado por Axis, Bosch y Sony, cada grupo cuenta actualmente con numerosos miembros. A partir de enero de 2009, cada grupo ha liberado la versión 1.0 de su especificación.

3.2.2.4. Métodos de compresión.

Cuando se digitaliza una secuencia de video analógico cualquiera de acuerdo al estándar ITU-R BT.601 (CCIR 601), se requiere un ancho de banda de 116 Mbit/segundo ó de 116 millones de bits cada segundo. Dado que la mayoría de las redes son sólo de 100 Mbit/segundo, no es posible ni deseable transmitir las secuencias de vídeo sin alguna modificación. Para solucionar este problema se han desarrollado una serie de técnicas denominadas técnicas de compresión de vídeo e imágenes, que reducen el alto nivel de bits precisos para transmisión y almacenamiento.

La compresión de imágenes se aplica sobre una imagen individual haciendo uso de las similitudes entre píxels próximos en la imagen y de las limitaciones del sistema de visión humana. JPEG es un ejemplo de una técnica de compresión de imágenes. La compresión de video se aplica sobre series consecutivas de imágenes en una secuencia de video, haciendo uso de las similitudes entre imágenes próximas. Un ejemplo de este tipo de técnicas es MPEG.

La efectividad de una técnica de compresión de imágenes viene dada por la relación de compresión, calculado como el tamaño del archivo de la imagen original (sin comprimir) dividido por el tamaño del archivo de imagen resultante (comprimida). A mayor relación de compresión se consume menos ancho de banda manteniendo un número de imágenes por segundo determinado. O si el ancho de banda se mantiene constante se aumenta el

número de imágenes por segundo. Al mismo tiempo, un mayor nivel de compresión implica menor nivel de calidad de imagen para cada imagen individual.

3.2.2.4.1. Compresión de imágenes JPEG.

JPEG es un conocido método de compresión, que fue originalmente estandarizado a mediados de los años 80 en un proceso iniciado por el Joint Photographic Experts Group.

La compresión JPEG puede realizarse a diferentes niveles definidos por el usuario y que determinan cuanto tiene que comprimirse una imagen. El nivel de compresión seleccionado tiene una relación directa con la calidad de imagen obtenida. Además del nivel de compresión la escena de la imagen en sí misma también tiene un impacto en el nivel de compresión resultante. Mientras que un muro blanco, por ejemplo, puede producir un archivo de imagen relativamente pequeño (y aceptar un mayor nivel de compresión), el mismo nivel de compresión aplicado a una escena compleja producirá un archivo de mayor tamaño y con un nivel de compresión menor.

3.2.2.4.2. El video como una secuencia de imágenes JPEG (Motion JPEG o M-JPEG).

Al igual que una cámara fotográfica digital, una cámara de red captura imágenes individuales y las comprime en formato JPEG. La cámara de red puede capturar y comprimir las imágenes, por ejemplo 30 imágenes o cuadros individuales por segundo (30 cps), y después hacerlas disponibles como un flujo continuo de imágenes sobre una red a una estación de visualización. Nosotros denominamos a este método como Motion JPEG o M-JPEG.

Dado que cada imagen individual es una imagen JPEG comprimida todas tendrán garantizada la misma calidad, determinada por el nivel de compresión definido en la cámara de red o el servidor de vídeo en red.

3.2.2.4.3. Compresión de vídeo – MPEG.

Una de las técnicas de vídeo y audio más conocidas es el estándar denominado MPEG (iniciado por el Motion Picture Experts Groups a finales de los años 80). Este documento se centra en la parte de video de los estándares de vídeo MPEG.

Descrito de forma sencilla, el principio básico de MPEG es comparar entre dos imágenes para que puedan ser transmitidas a través de la red, y usar la primera imagen como imagen de referencia (denominada I-frame), enviando tan solo las partes de las siguientes imágenes (denominadas B y P –frames) que difieren de la imagen original. La estación de

visualización de red reconstruirá todas las imágenes basándose en la imagen de referencia y en los "datos diferentes"; contenidos en los B- y P- frames

MPEG es de hecho bastante más complejo que lo indicado anteriormente, e incluye parámetros como la predicción de movimiento en una escena y la identificación de objetos que son técnicas o herramientas que utiliza MPEG. Además, diferentes aplicaciones pueden hacer uso de herramientas diferentes, por ejemplo comparar una aplicación de vigilancia en tiempo real con una película de animación. Existe un número de estándares MPEG diferentes: MPEG-1, MPEG-2 y MPEG-4.

3.2.2.4.3.1. MPEG-1.

El estándar MPEG-1 fue presentado en 1993 y está dirigido a aplicaciones de almacenamiento de vídeo digital en CD. Por esta circunstancia, la mayoría de los codificadores y decodificadores (codecs) MPEG-1 precisan un ancho de banda de aproximadamente 1.5 Mbit/segundo a resolución CIF (352x288 píxeles). Para MPEG-1 el objetivo es mantener el consumo de ancho de banda relativamente constante aunque varíe la calidad de la imagen, que es típicamente comparable a la calidad del video VHS. El número de imágenes o cuadros por segundo (cps) en MPEG-1 está bloqueado a 25 (PAL)/30 (NTSC) cuadros por segundo (cps).

3.2.2.4.3.2. MPEG-2.

MPEG-2 fue aprobado en 1994 como estándar y fue diseñado para video digital de alta calidad (DVD), TV digital de alta definición (HDTV), medios de almacenamiento interactivo (ISM), retransmisión de vídeo digital (Digital Vídeo Broadcasting, DVB) y Televisión por cable (CATV). El proyecto MPEG-2 se centró en ampliar la técnica de compresión MPEG-1 para cubrir imágenes más grandes y de mayor calidad en detrimento de un nivel de compresión menor y un consumo de ancho de banda mayor. MPEG-2 también proporciona herramientas adicionales para mejorar la calidad del video consumiendo el mismo ancho de banda, con lo que se producen imágenes de muy alta calidad cuando lo comparamos con otras tecnologías de compresión. La relación de cuadros por segundo está bloqueado a 25 (PAL)/30 (NTSC) cps, al igual que en MPEG-1.

3.2.2.4.3.3. MPEG-4.

El estándar MPEG-4 fue aprobado en 2000 y es uno de los desarrollos principales de MPEG- 2.

Cuando la gente habla de MPEG-4 generalmente se está refiriendo a MPEG-4 parte 2. Este es el estándar de transmisión de vídeo clásico MPEG-4, también denominado MPEG-4 Visual.

Como uno de los desarrollos principales de MPEG-2, MPEG-4 incorpora muchas más herramientas para reducir el ancho de banda preciso en la transmisión para ajustar una cierta calidad de imagen a una determinada aplicación o escena de la imagen. Además la relación de imágenes por segundo no está bloqueado a 25 (PAL)/30 (NTSC) cps.

Otra mejora de MPEG-4 es el amplio número de perfiles y niveles de perfiles que cubren una variedad más amplia de aplicaciones desde todo lo relacionado con transmisiones con poco ancho de banda para dispositivos móviles a aplicaciones con una calidad extremadamente amplia y demandas casi ilimitadas de ancho de banda. La realización de películas de animación es sólo un ejemplo de esto.

3.2.2.4.4. Perfiles MPEG-4.

En uno de los extremos del sistema, tiene lugar la codificación al formato MPEG en la cámara de vídeo. Obviamente en el otro extremo, esta secuencia MPEG necesita ser decodificada y posteriormente mostrada como video en la estación de visualización.

Dado que hay un gran número de técnicas (herramientas) disponibles en MPEG (especialmente en MPEG-4) para reducir el consumo de ancho de banda en la transmisión, la variable complejidad de estas herramientas y el hecho de que no todas las herramientas sean aplicables a todas las aplicaciones, sería irreal e innecesario especificar que todos los codificadores y decodificadores MPEG deberían soportar todas las herramientas disponibles. Por consiguiente se han definido subconjuntos de estas

herramientas para diferentes formatos de imágenes dirigidos a diferentes consumos de ancho de banda en la transmisión.

Hay diferentes subconjuntos definidos para cada una de las versiones de MPEG. Por ejemplo hay un subconjunto de herramientas denominados MPEG Profile. Un MPEG Profile específico establece exactamente qué herramientas debería soportar un decodificador MPEG. De hecho los requerimientos en el codificador y el decodificador no tienen porque hacer uso de todas las herramientas disponibles.

Además, para cada perfil existen a diferentes niveles. El nivel especifica parámetros como por ejemplo la relación de bits máximo a usar en la transmisión y las resoluciones soportadas. Al especificar el Nivel y el Perfil MPEG es posible diseñar un sistema que solo use las herramientas MPEG que son aplicables para un tipo concreto de aplicación.

MPEG-4 tiene un amplio número de perfiles diferentes. Entre ellos se encuentran el Simple Profile y el Advanced Profile que son los más utilizados en aplicaciones de seguridad.

3.2.2.4.4.1. Constant bit-rate (CBR) y Variable bit-rate (VBR).

Otro aspecto importante de MPEG es el modo en el que se usa el ancho de banda disponible. En la mayoría de los sistemas MPEG es posible seleccionar si el ratio de bits

debe ejecutarse en modo CBR (constante) o VBR (variable). La selección óptima depende de la aplicación y de la infraestructura de red disponible.

Con la única limitación del ancho de banda disponible el modo preferido es normalmente CBR, dado que este modo consume un ancho de banda constante en la transmisión. La desventaja es que la calidad de la imagen variará y, aunque se mantendrá relativamente alta cuando no hay movimiento en la escena, la calidad bajará significativamente cuando aumente el movimiento.

El modo VBR, por otra parte, mantendrá una alta calidad de imagen, si así se define, sin tener en cuenta si hay movimiento o no en la escena. Esto es a menudo deseable en aplicaciones de seguridad y vigilancia en las que hay la necesidad de una alta calidad, especialmente si no hay movimiento en la escena. Dado que el consumo de ancho de banda puede variar, incluso si se define una media de ratio de bits objetivo, la infraestructura de red (el ancho de banda disponible) necesitará tener esta capacidad para un sistema de este tipo.

3.2.2.4.5. Ventajas y desventajas para M-JPEG, MPEG-2 y MPEG-4.

Dada su simplicidad, M-JPEG es una buena elección para su uso en múltiples aplicaciones. JPEG es un estándar muy popular y en muchos sistemas se usa por defecto.

Es una técnica simple de compresión/descompresión, lo que significa que los costes, tanto en tiempo del sistema como en inversión total son reducidos. El aspecto del tiempo significa que hay un retraso limitado entre el momento en el que la cámara captura la imagen, la codificación, la transmisión a través de la red, la decodificación y finalmente el mostrar la imagen en la pantalla de la estación de visualización. En otras palabras, M-JPEG proporciona una baja latencia debido a su simplicidad (compresión de imágenes e imágenes individuales completas), y por esta razón es también idóneo para cuando se necesita realizar procesamiento de imágenes, por ejemplo para la detección de movimiento o el seguimiento de objetos.

M-JPEG es válido para cualquier resolución de imagen, desde la pantalla de un teléfono móvil hasta imágenes de video (4CIF, 704x480 píxeles en PAL). También garantiza la calidad de la imagen sin importar el movimiento o la complejidad de las escenas de las imágenes. Además ofrece la flexibilidad de poder seleccionar por un lado imágenes de alta calidad (baja compresión) o menor calidad de imagen (alta compresión) con el beneficio de que imágenes menores producen ficheros más pequeños, lo que permite usar un menor volumen de bits en la transmisión y un menor uso del ancho de banda. Al mismo tiempo el número de imágenes por segundo se puede controlar fácilmente, proporcionando una referencia para limitar el uso del ancho de banda al reducir el número de imágenes por segundo, aunque manteniendo una calidad de imagen garantizada.

Dado que M-JPEG no hace uso de una técnica de compresión de vídeo genera una cantidad de datos de imágenes relativamente alto que se envía a través de la red. Por esta razón con un nivel de compresión de imagen determinado (definiendo la calidad de la imagen del I-frame y de la imagen JPEG respectivamente), un número de imágenes por segundo y la escena de la imagen, la cantidad de datos por unidad de tiempo que envía por la red (bit rate, ratio de bits) es menor para MPEG que para M-JPEG.

Lo siguiente resume claramente el beneficio de MPEG: la capacidad para dar una calidad de imagen relativamente alta con un consumo de ancho de banda reducido (un ratio de bits de transmisión bajo). Esto puede ser especialmente importante cuando está limitado el ancho de banda disponible en la red, o si el video debe ser almacenado (grabado) con un alto número de imágenes por segundo. Estas menores demandas de ancho de banda son a costa de una mayor complejidad en la codificación/decodificación, lo que por otra parte contribuye a una latencia mayor si se compara con M-JPEG.

Otro elemento a tener en cuenta: tanto MPEG-2 como MPEG-4 están sujetos al pago de licencias.

TEMA 4: CONEXIÓN A REDES EXTERNAS

4.1 Conexión a Red Eléctrica.

4.1.1 Introducción a las redes eléctricas.

La distribución de la energía eléctrica desde las subestaciones de transformación de la red de transporte se realiza en dos etapas.

La primera está constituida por la red de reparto, que, partiendo de las subestaciones de transformación, reparte la energía hasta llegar a las estaciones transformadoras de distribución. Las tensiones utilizadas están comprendidas entre 25 y 132 kV. Intercaladas en estos anillos están las estaciones transformadoras de distribución, encargadas de reducir la tensión desde el nivel de reparto al de distribución en media tensión.

La segunda etapa la constituye la red de distribución propiamente dicha, con tensiones de funcionamiento de 3 a 30 kV y con una característica muy radial. Esta red cubre la superficie de los grandes centros de consumo (población, gran industria, etc.), uniendo las estaciones transformadoras de distribución con los centros de transformación, que son la última etapa del suministro en media tensión, ya que las tensiones a la salida de estos centros es de baja tensión (125/220 ó 220/380).

En República Dominicana la distribución esta a cargo de tres Empresas de Distribución de Electricidad, las cuales se encargan de proveer la energía a las regiones Norte, Sur y Este del país.

La Empresa Distribuidora de Electricidad del Norte S.A. EDENORTE Dominicana S.A. tiene la concesión de la comercialización y distribución de energía eléctrica en las 14 provincias de la Zona Norte de la Republica Dominicana: Santiago, La Vega, Duarte, Puerto Plata, Espaillat, Maria Trinidad Sánchez, Monseñor Nouel, Sánchez Ramírez, Valverde, Santiago Rodríguez, Montecristi, Samaná, Salcedo y Dajabón.

La Empresa Distribuidora de Electricidad del Este, S.A, EDEESTE, cubre desde la acera Este de la Av. Máximo Gómez, incluyendo Monte Plata y todas las provincias del Este.

La Empresa Distribuidora de Electricidad del Sur, S.A, EDESUR tiene un área de concesión que se inicia en la acera oeste de la avenida Máximo Gómez, en el Distrito Nacional y termina en la provincia fronteriza de Elías Piña.

La Red de Distribución de la Energía Eléctrica o Sistema de Distribución de Energía Eléctrica es un subsistema del Sistema Eléctrico de Potencia cuya función es el suministro de energía desde la subestación de distribución hasta los usuarios finales.

4.1.2 Defectos de la señal eléctrica.

Un corte de energía se define como una condición de cero tensión en la alimentación eléctrica que dura más de dos ciclos (40 ms). Puede ser causado por la apertura de un interruptor, un problema en la instalación del usuario, un fallo en la distribución eléctrica o un fallo de la red comercial.

Una baja tensión es un estado continuo de baja tensión de red. Un ejemplo de ello es la baja tensión producida durante la gran demanda energética del verano, en el cual las centrales generadoras no alcanzan a satisfacerla, debiendo entonces bajar la tensión para limitar la potencia máxima requerida.

Una variación de frecuencia involucra un cambio en la frecuencia nominal de la alimentación del equipo, el cual es comúnmente estable en 50 ó 60 Hz dependiendo esto de la ubicación geográfica. Esto puede ser causado por el funcionamiento errático de grupos electrógenos o por inestabilidad en las fuentes de suministro eléctrico.

El ruido eléctrico de línea se define como interferencia de Radio Frecuencia (RFI) e Interferencia Electromagnética (EMI) y causa efectos indeseables en los circuitos electrónicos de los sistemas informáticos. Las fuentes del problema incluyen motores eléctricos, relés, dispositivos de control de motores, transmisiones de radiodifusión, radiación de microondas y tormentas eléctricas distantes. RFI, EMI y otros problemas de

frecuencia pueden causar errores o pérdida de datos almacenados, interferencia en las comunicaciones, bloqueo del teclado y del sistema.

Los picos de alta tensión ocurren cuando hay repentinos incrementos de tensión en pocos microsegundos. Estos picos normalmente son el resultado de la caída cercana de un rayo, pero pueden existir otras causas también.

Una sobretensión tiene lugar cuando la tensión supera el 110% del valor nominal. La causa más común es la desconexión o el apagado de grandes cargas en la red. Bajo esta condición, los equipos informáticos pueden experimentar pérdidas de memoria, errores en los datos, apagado del equipo y envejecimiento prematuro de componentes electrónicos.

Una caída de tensión comprende valores de tensión inferiores al 80% ó 85% de la tensión normal durante un corto período de tiempo. Las posibles causas son; encendido de equipamiento de gran magnitud o de motores eléctricos de gran potencia y la conmutación de interruptores principales de la alimentación (interna o de la usina). Una caída de tensión puede tener efectos similares a los de una sobretensión.

Un transitorio de tensión tiene lugar cuando hay picos de tensión de hasta 20.000 voltios con una duración entre 10 y 100 us. Normalmente son causados por arcos eléctricos y descargas estáticas. Las maniobras de las usinas para corregir defectos en la red que generan estos transitorios, pueden ocurrir varias veces al día. Los efectos de transitorios

de este tipo pueden incluir pérdida de datos en memoria, error en los datos, pérdida de los mismos y solicitaciones extremas en los componentes electrónicos.

4.1.3 Sistemas de Alimentación Ininterrumpida.

Un SAI (Sistema de Alimentación Ininterrumpida), también conocido por sus siglas en inglés UPS (*Uninterruptible Power Supply:* 'suministro de energía ininterrumpible') es un dispositivo que puede proporcionar energía eléctrica tras un corte de energía a todos los dispositivos que tenga conectados. Otra de las funciones de los SAI es la de mejorar la calidad de la energía eléctrica que llega a los aparatos, filtrando subidas y bajadas de tensión y eliminando armónicos de la red en el caso de Corriente Alterna.

Los SAI dan energía eléctrica a equipos llamados cargas críticas, que pueden ser aparatos médicos, industriales o informáticos, que requieren tener siempre alimentación y que ésta sea de regulada debido a la necesidad de estar en todo momento operativos y sin fallos.

Existen diversos tipos de Topología de UPS y cada una de ellas tiene sus ventajas y desventajas, continuación se enumeran dos cada una de estas topologías y la discutiremos ampliamente:

4.1.3.1 Sistema Fuera de Línea.

Se le llama Off-Line porque contiene un circuito inversor (convierte la tensión continua de la batería en tensión alterna para alimentar una carga) se encuentra fuera del camino principal de la corriente, y se le llama Stand-By porque el inversor se encuentra apagado "en espera" de que sea requerido para encender.

El UPS Off-Line es el tipo de UPS más económico ya que integra muy pocos componentes, pero a la vez, el nivel de protección obtenido con este tipo de equipos se muy limitado.

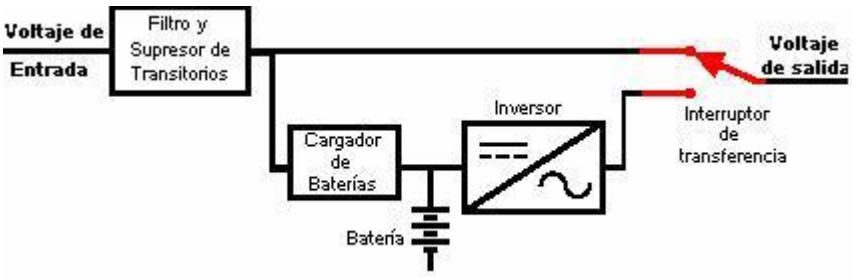


Diagrama en bloques de un UPS Offline. Fuente: http://www.unicrom.com/Tut_TopologiasUPS1.asp

4.1.3.1.1 Filtro y Supresor de Transitorios.

El Filtro de Línea reduce las variaciones transitorias de voltaje debidas al encendido y apagado de ciertos aparatos como por ejemplo motores eléctricos, además reduce el ruido eléctrico que viene con el voltaje de alimentación del UPS para que aparezca en niveles

más seguros en la carga. Cabe hacer la aclaración que el Filtro de Línea sólo reduce problemas de variación de voltaje que son de tiempo muy corto; por el rango de los milisegundos y nanosegundos. No es su función regular el voltaje.

El Filtro de Línea consiste en Bobinas las cuales rechazan voltajes de alta frecuencia y capacitores conectados a tierra para que cualquier alta frecuencia sea drenada a tierra. El Supresor de Transitorios lo que hace es Recortar los picos de voltaje que aparecen en la Línea a niveles más seguros. Un Transitorio de voltaje usualmente anda por el orden de los milisegundos a los nanosegundos y en valor, puede alcanzar desde los 200 hasta varios miles de volts. Consiste esta etapa generalmente de los llamados Varistores de Oxido Metálico (MOV).

Al Supresor de Picos se le llama comúnmente TVSS que significa Supresor de Voltaje Transitorio por sus siglas en inglés (Transient Voltage Surge Suppresor).
El nivel de protección del filtro de Entrada de este tipo de equipos es limitado.

4.1.3.1.2 Batería.

La batería es uno de los componentes más importantes en un UPS, es la que va a hacer posible que los aparatos continúen encendidos aún y cuando haya un corte de energía. La mayoría de las baterías utilizadas en los UPS son del tipo Selladas ó tipo Gel ó VRLA.

Una batería sellada funciona de la misma manera que una de auto, consiste en placas de Plomo y Antimonio sumergidas en un electrolito que en este caso es ácido sulfúrico.

4.1.3.1.3 Cargador de Baterías.

El cargador de baterías es una fuente de voltaje que tendrá dos funciones:

1.- Dar a la batería el voltaje de flotación necesario para asegurar que la batería está cargada al 100%.

2.- Recargar la batería después que fue utilizada al haber un corte de energía. Es decir, al regresar la energía comercial, el cargador de baterías aplicará el mismo voltaje de flotación y la batería se empezará a recargar; una vez que la batería esté recargada completamente la corriente que fluya del cargador de baterías hacia la batería será mínima.

Físicamente el cargador de Baterías consiste en un devanado adicional del transformador de Salida además de un puente de diodos para convertir la Corriente Alterna en Corriente Directa y un Mosfet el cual conecta y desconecta la “Carga” a las baterías y esto comandado por una tarjeta de Control. El Mosfet generalmente tiene disipador de calor.

4.1.3.1.4 El Inversor.

El Inversor se representa por un bloque donde le entra Corriente Directa y sale Corriente Alterna: La forma de Onda que se utiliza en UPS del tipo Off-Line es la Cuasisenoidal y es de la siguiente forma:

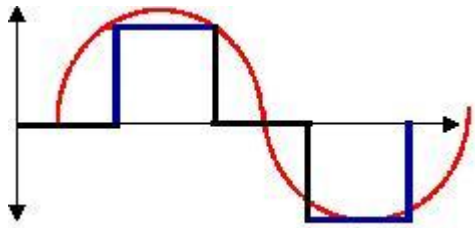


Imagen de distintos tipos de onda.
Fuente: http://www.unicrom.com/Tut_TopologiasUPS2.asp

La Forma de Onda Cuasisenoidal es la de color Negro y se antepuso una Senoidal para que se pueda comparar ambas ondas. Esta forma de Onda es recomendada para Equipo electrónico y de cómputo aunque si el equipo es muy delicado por ejemplo para equipos PLC se recomienda que la forma de onda del inversor sea Senoidal.

4.1.3.1.5 El Interruptor de Transferencia.

Cuando hay un corte de energía ó el voltaje es muy alto ó muy bajo a niveles inadecuados para seguir operando la carga, es necesario desconectar el voltaje de entrada que en ese momento se dirige hacia la carga y encender el Inversor para rápidamente conmutar el

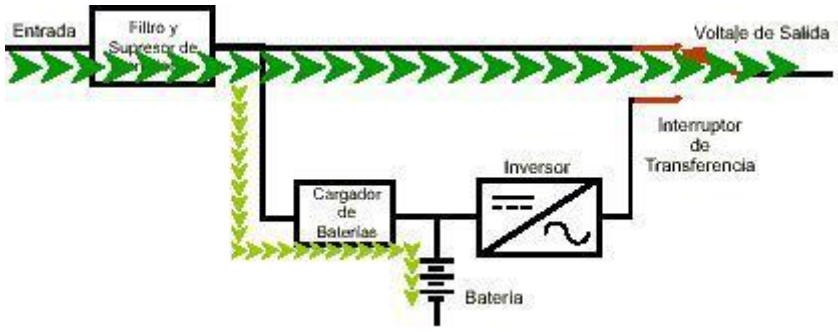
voltaje de Inversor a la carga.

Esto tiene que ser muy rápido de modo que se imperceptible para la carga que el voltaje se interrumpió, esta es la función del interruptor de transferencia que generalmente es un relevador; el tiempo de transferencia típicamente es de 4 mseg. Pero en ocasiones dependiendo del fabricante puede ser hasta de 10 mseg.; Estos valores de tiempo de transferencia se consideran adecuados para la mayoría de las cargas electrónicas. Sin embargo hay cargas muy delicadas que aún un tiempo tan corto de interrupción puede hacer que operen incorrectamente por lo que este tipo de UPS no es adecuado para este tipo de cargas.

4.1.3.1.6 Funcionamiento de un UPS offline.

4.1.3.1.6.1 Modo normal.

En el modo Normal de operación, el voltaje de alimentación es de un nivel tal que no hay necesidad que entre el Inversor a funcionar; por lo tanto el voltaje de Entrada pasa por el filtro y después energiza la carga a través del Switch de Transferencia el cual está normalmente cerrado tomando en cuenta que es un relevador.
La corriente fluye desde la Entrada y hacia la carga y una pequeña cantidad de corriente es rectificada por el cargador de baterías y utilizada para mantener la batería en "flotación". El Inversor se encuentra apagado (en stand-by).

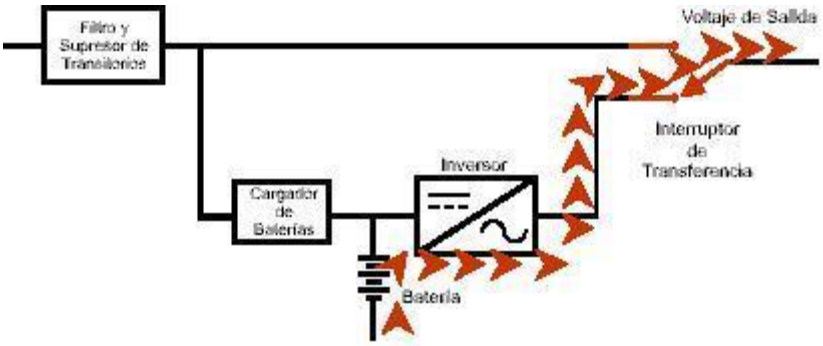


Flujo de la corriente.
Fuente: http://www.unicrom.com/Tut_TopologiasUPS3.asp

4.1.3.1.6.2 Modo baterías.

Cuando el voltaje de alimentación del UPS se sale de la ventana predeterminada de operación, el UPS se va a Modo Baterías. El voltaje de Entrada tiene una ventana "aceptable de operación" que suele ser de un +/- 15% aproximadamente, esta ventana se escoge tomando en cuenta que voltaje es adecuado para alimentar la carga.

Es importante hacer notar que el voltaje del Inversor es regulado y entrega un voltaje de 120 VCA +/-3% a 60.0 Hz (la frecuencia controlada por cristal) aún y cuando inicialmente el voltaje de baterías inicia en unos 14.0 volts y cuando la batería está totalmente descargada el voltaje es de 10.5 volts. (Esto para en caso de que la batería del UPS sea solamente una de 12 volts).



Flujo de la corriente en modo de baterías.
Fuente: http://www.unicrom.com/Tut_TopologiasUPS3.asp

4.1.3.1.6.3 Regreso a operación normal.

Una vez que el voltaje regresa a los límites permitidos, el switch de transferencia ó relevador de transferencia se desenergiza y el UPS regresa a operación Normal donde la carga es nuevamente alimentada por el voltaje de Entrada. El Inversor se apaga al mismo tiempo y la batería se comienza a recargar hasta que llegue nuevamente a su estado de carga al 100%.

El tiempo que tarde en recargarse al 100% la batería depende del tiempo que el equipo duró en baterías y generalmente es de 10 veces el tiempo que duró la descarga, es decir que si el UPS estuvo por 5 minutos en baterías la batería estará casi totalmente recargada en unos 50 minutos. Esto varía dependiendo del fabricante del UPS.

4.1.3.2 Sistema en línea.

Este tipo de equipos es llamado “En Línea” debido a que el Inversor se encuentra dentro de la línea principal de energía ya que siempre se encuentra operando. Esta tecnología es la más cara de todas pero es la que ofrece el mayor nivel de protección.

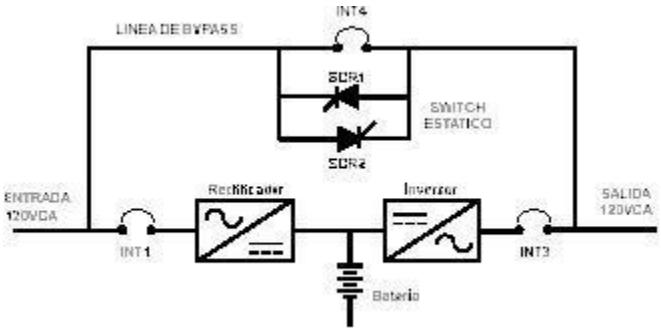


Diagrama de un UPS en línea. Fuente: http://www.unicrom.com/Tut_TopologiasUPS5.asp

Esta topología es muy diferente a la anterior. El voltaje de Entrada pasa por medio del Interruptor “INT1” al primer bloque que es el rectificador. Rectificador.- El Rectificador del UPS On Line consiste de la etapa de rectificación con SCR generalmente con el objeto de poder variar el ángulo de disparo de los SCR y de esta manera poder regular el voltaje de CD a obtener a la salida, obviamente después de ser rectificado el voltaje de Entrada se filtra con Capacitores para obtener un voltaje continuo y regulado. El voltaje regulado de corriente directa obtenido en el Rectificador, tiene dos objetivos:

-El primero es mantener las baterías en flotación e incluso recargarlas después de un corte de energía.

-El segundo es alimentar al Inversor para que este a su vez convierta la corriente directa del rectificador en corriente alterna.

4.1.3.2.1 Funcionamiento de un UPS online.

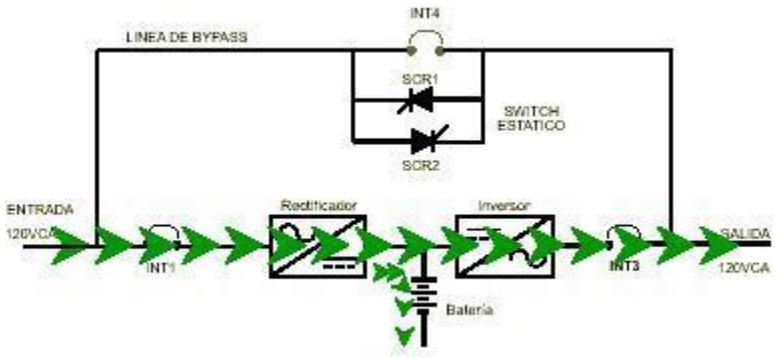
4.1.3.2.1.1 Modo normal.

En el Modo Normal, el interruptor de entrada está cerrado alimentando el Rectificador, éste a su vez proporciona un voltaje de continuo regulado para alimentar el Inversor y a su vez mantener las Baterías en flotación. El voltaje del Rectificador es convertido por el Inversor en un voltaje de Corriente Alterna Regulado en Voltaje y en Frecuencia para por medio del interruptor de salida alimentar la carga. En este instante el interruptor de switch estático está abierto y el "Switch Estático" está apagado. El voltaje de la Línea Comercial es descompuesto al ser convertido en Corriente Directa y cualquier variación de Voltaje, Frecuencia, Pico de Voltaje, etc. es eliminado durante la conversión a Corriente Directa.

El Inversor a partir de esta Corriente Directa genera una nueva señal de voltaje de la cual es totalmente diferente a la que entró al UPS de la Línea Comercial y es por eso que aún y cuando haya en la entrada todo tipo de problemas de variación de voltaje ó picos de

voltaje, en la salida no se verán reflejados porque el voltaje de salida es un voltaje nuevo creado por el Inversor.

En el diagrama siguiente se observa la trayectoria de la corriente, la línea más gruesa representa el camino por el cual circula la corriente hacia la carga y la línea más delgada representa la corriente de flotación para mantener cargadas las baterías.



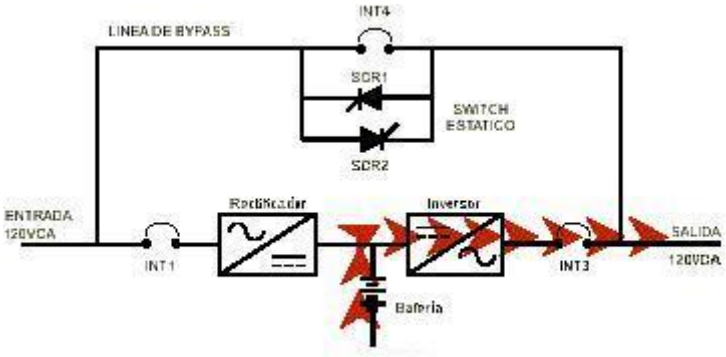
Flujo de corriente en modo normal. Fuente: http://www.unicrom.com/Tut_TopologiasUPS5_modo_normal.asp

4.1.3.2.1.2 Modo baterías.

Cuando el voltaje a la entrada del rectificador es lo suficientemente alto ó bajo como para que ya no pueda seguir entregando un voltaje de CD regulado, el Rectificador se apaga pero como en las baterías están conectadas en paralelo, el Inversor sólo detecta cuando el voltaje baja ya que está operando ahora la batería; sin embargo esa variación de voltaje no importa ya que el Inversor regula el voltaje y en la carga el voltaje permanece sin variación e incluso no hay ningún instante en el que se interrumpa el voltaje como sucede en la topología Off-Line.

Si el corte de energía se prolonga tanto de tal manera que las baterías se descarguen completamente, entonces el UPS se apaga al no tener ya manera de seguir alimentando la carga.

Si antes de que se terminen las baterías, el voltaje de entrada del Rectificador vuelve a la normalidad; entonces el Rectificador enciende y alimenta nuevamente el Inversor y a la vez comienza a recargar las baterías. Este cambio de operación Baterías a operación Normal también es transparente para la carga y permanece en todo momento alimentada sin interrupción alguna.



Flujo de corriente en modo batería. Fuente:
http://www.unicrom.com/Tut_TopologiasUPS5-modo-baterias.asp

En el diagrama anterior se puede observar el camino de la corriente desde las baterías pasando por el Inversor y hacia la carga, el rectificador se representa en color gris para hacer notar que está apagado

4.1.3.2.1.3 Modo BYPASS.

Existe la posibilidad de que por algún motivo el Inversor no pueda seguir alimentando la carga, las principales razones son las siguientes:

- Hay un daño en el Inversor
- Hay una sobrecarga en el Inversor
- Hay sobre temperatura en el equipo
- Hay un daño en la lógica del equipo

Por tal motivo, el UPS On-Line incorpora lo que se llama la línea de Bypass que no es más que una forma de alimentar la carga con la Línea Comercial.
Cuando el UPS está en Bypass el interruptor de salida se encuentra abierto para desconectar el Inversor de la carga, el interruptor de switch estático está cerrado para alimentar la carga directamente de la Línea Comercial.

Cuando la lógica detecta que por alguno de los motivos mencionados anteriormente el Inversor no puede seguir alimentando la carga, ejecuta una transferencia de la carga a Bypass de la manera siguiente:

- Manda encender el Switch Estático el cual consiste en dos SCR en paralelo inverso para poder conducir Corriente Alterna.
- Manda cerrar el interruptor del switch estático el cual consiste en un contactor ó un

Interruptor operado por Motor.

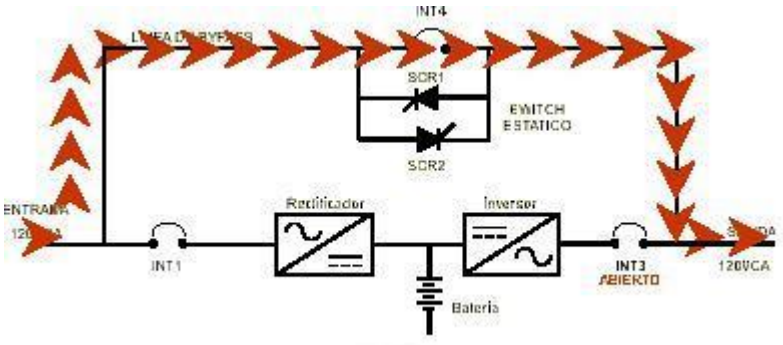
- Manda apagar el Switch Estático.

- Manda abrir el interruptor de salida que también consiste en contactor ó Interruptor operado por Motor.

Ahora la carga está soportada por la Línea Comercial a través de interruptor del switch estático y no a través del Inversor.

Es importante hacer notar que cuando se transfiere a Bypass en un instante quedan en paralelo Inversor y Línea Comercial eso para evitar desconectar el voltaje a la carga. Además hay que notar que siempre va a haber sólo un interruptor cerrado al mismo tiempo y ya sea el interruptor de salida ó el interruptor del switch estático con excepción de cuando se hace una transferencia.

Cuando se requiere transferir a Bypass se necesita una gran velocidad y por ello se utiliza el Switch Estático el cual al ser electrónico es de muy alta velocidad.



Flujo de corriente en modo bypass.
Fuente: http://www.unicrom.com/Tut_TopologiasUPS6.asp

En el diagrama anterior se puede observar la trayectoria de la corriente en Modo Bypass, el Rectificador y el Inversor pueden o no estar encendidos. Cuando el UPS está en el modo Bypass, no hay protección alguna para la carga.

El modo Bypass lo utiliza el UPS para evitar al máximo que el voltaje se vea interrumpido en la carga, por tal razón inmediatamente manda una alarma para alertar que se está en modo Bypass y que la carga esta desprotegida incluso si hay corte de energía no habrá protección de Baterías en virtud de que la carga no está por el Inversor.

4.1.3.3 Otros tipos de UPS.

4.1.3.3.1 La UPS Interactiva.

Una importante mejora a la UPS tipo Standby, fue el agregado de un regulador de voltaje de entrada, constituido por un transformador con derivaciones seleccionables. La Figura muestra el esquema de la UPS resultante, llamada UPS de Potencia Interactiva.

El regulador de voltaje , a la entrada del sistema, permite operar al sistema en "Modo Normal", cuando se producen caídas ó sobre elevaciones en la tensión de línea, sin que sea necesario conmutar al Modo Batería.

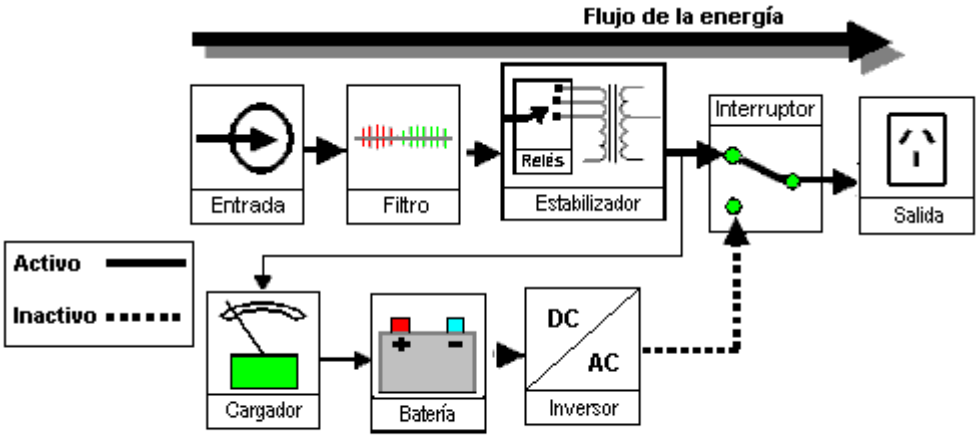


Fig. 8 **UPS Interactiva / Funcionamiento con red normal**

Fuente: http://www.unicrom.com/Tut_tipos-configuraciones-sistemas-ups-definiciones-ByPass-Interactiva.asp

La operación de una UPS Interactiva, en modo Batería es idéntica al de las UPS Standby. El inversor arranca, el relé de conmutación se activa, y la energía es provista por la batería.

En diseños de baja potencia y costo, el transformador tiene solamente dos derivaciones, mientras que en equipos de mayor potencia y mejores prestaciones suelen tener tres ó cuatro, lo que permite obtener un mejor rango de regulación y precisión de la tensión de salida.

La salida varía conjuntamente con la entrada hasta que se produce un cambio de derivación en el transformador. Estos pequeños cambios en la tensión de salida no afectarán a la mayoría de las cargas.

4.1.3.3.2 UPS tipo Ferroresonante.

Otras dos topologías de UPS bastante comunes en el mercado, las cuales son esencialmente de operación Off-Line son las del tipo Ferroresonante y Triport.

Las UPS del tipo Ferroresonate utilizan un transformador especial a la salida, el cual está sintonizado a 50 ó 60 Hz (dependiendo de la frecuencia de la red donde se encuentren instaladas).

Este transformador con tres bobinados regula la tensión de salida, y puede ser visto como un estabilizador de tensión. Uno de los bobinados es utilizado para el Inversor.

Cuando la energía de la línea falla, el relé de transferencia conmuta, el inversor arranca y alimenta a la carga. Como vemos el Inversor está en modo standby, y es energizado solo cuando la línea falla. El transformador, debido a sus especiales características, tiene la capacidad de almacenar energía, lo que hace que durante el período de transferencia no se manifieste un micro corte de energía tan importante como en la UPS Standby.

La aislación del transformador también provee una alta atenuación de ruidos y picos transitorios, igual o mejor que cualquier otro filtro disponible, pero el transformador mismo puede crear severas distorsiones en la tensión de salida (fundamentalmente con cargas no lineales), que pueden llegar a ser peores que una mala conexión de línea.

En la Figura se puede observar el diagrama en bloques de una UPS de éstas características, funcionando en Modo Normal.

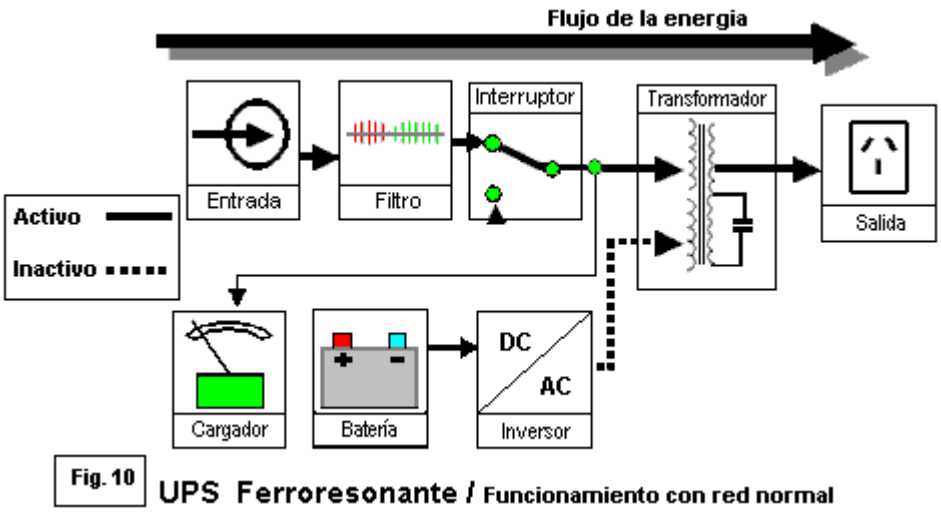
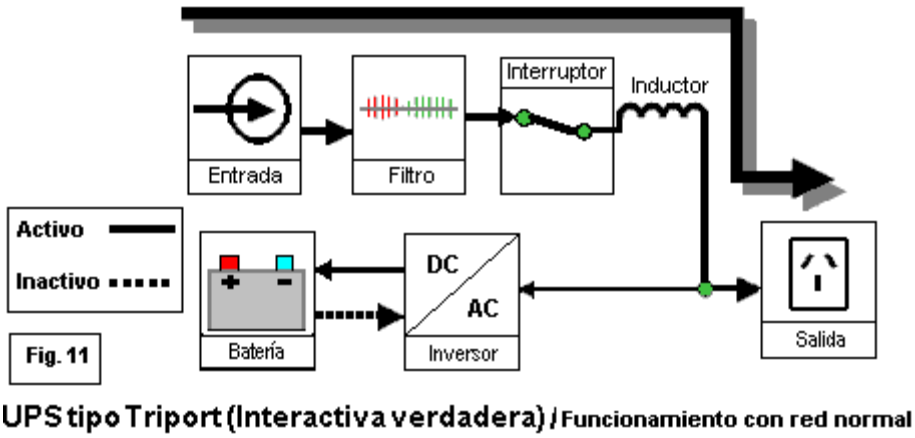


Fig. 10 UPS Ferroresonante / Funcionamiento con red normal

Fuente: http://www.unicrom.com/Tut_tipos-configuraciones-sistemas-ups-off-line-otros-disenos.asp

4.1.3.3.3 UPS tipo Triport.

La UPS denominada Triport (unity three phase, silcon) es realmente una UPS Interactiva. En éste sistema el inversor está interactuando permanentemente con la línea. En la Figura se puede notar que hay un inductor intercalado entre la entrada de la línea y la salida del Inversor. Este inductor es el que distingue a la UPS tipo Triport de las otras tecnologías



UPS tipo Triport (Interactiva verdadera) / Funcionamiento con red normal

Fuente: http://www.unicrom.com/Tut_tipos-configuraciones-sistemas-ups-off-line-otros-disenos.asp

El nombre Triport (tres puertos) es debido a que realmente, el inversor, la línea, y la carga configuran los tres puertos.

Operando en modo normal (con línea presente), hay una caída de tensión en el inductor, y es necesario el funcionamiento del inversor para regular la tensión de salida a la carga.

El inversor también toma parte de energía de la línea y además mantiene la carga de las baterías. Si el inversor tomara la energía desde las baterías, éstas se descargarían y no estarían disponibles en el caso de un corte de tensión de entrada.

Cuando la entrada falla, el interruptor se abre y el inversor alimenta a la carga con la energía de las baterías. El diseño Triport es algunas veces comercializado como UPS de Simple Conversión, pero realmente ésta tecnología sigue encuadrándose dentro de las UPS Off-Line. Estas UPS pueden presentar un incorrecto funcionamiento cuando se las opera con generadores o plantas de energía que tengan una frecuencia inestable.

4.1.3.3.4 PS Redundantes de diseño modular (tolerantes a las Fallas).

Este tipo de UPS, fue utilizado hace tiempo sólo para grandes instalaciones.

Desde el lanzamiento al mercado de UPS de mediana potencia con el mismo concepto de redundancia y modularidad, nos encontramos con una alternativa que nos ofrece una importante cantidad de ventajas.

La Figura es un simple diagrama que muestra múltiples UPS modulares, y un gabinete para las conexiones de entrada y salida.

Cada módulo, es en realidad una UPS completa, usando las últimas tecnologías: doble conversión, salida perfectamente sinusoidal, cargador de baterías incorporado, factor de potencia de entrada corregido, etc.

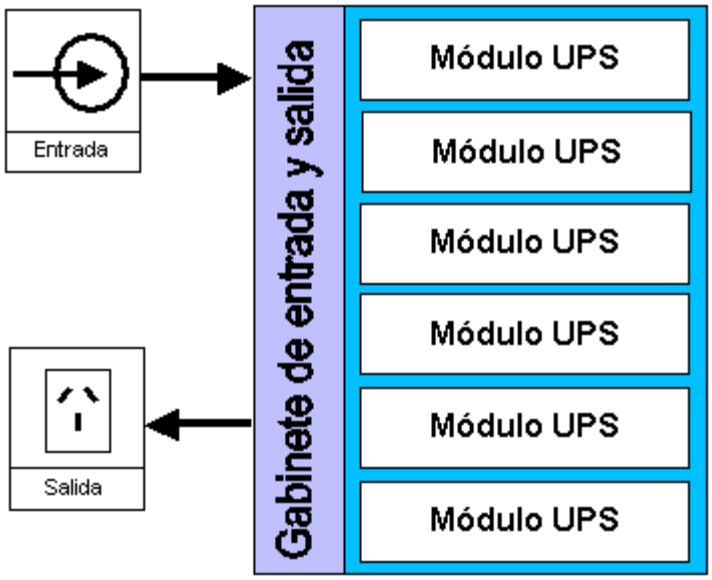


Fig.12 **UPS Modular y Redundante**

Fuente: http://www.unicrom.com/Tut_UPS-redundante-tipos-configuraciones-sistemas-ups.asp

En una UPS de tipo redundante, al menos un módulo se encuentra en reserva. Si un módulo falla, es excluido del sistema y la UPS continua operando normalmente. Algunas de las fundamentales ventajas de éste tipo de UPS son:

- La posibilidad de ampliación (por crecimiento de los sistemas a proteger),
- La facilidad de cambio del módulo con fallas (tiempos mínimos de reparación sin perder la protección de la UPS), y
- Su muy alta confiabilidad.

El UPS debe ser seleccionado por los diferentes parámetros esenciales: Seguridad, Potencia, Autonomía, Entorno y mantenimiento.

Seguridad: es el grado de confiabilidad de operación basado en la selección de nivel de protección requerido.

Potencia: es la capacidad que debe suministrar el UPS en KVA/KW y dependerá de las cargas a conectar y un valor de reserva y seguridad.

Autonomía: es el tiempo que requerimos del UPS para operar en caso de falla total de red.

Entorno: se define como situaciones de instalación, temperatura, existencia de generador, distribución eléctrica y tipo y grado de seguridad de la instalación.

Mantenimiento: en general los UPS dependiendo del tipo de baterías y control de parámetros no requieren mantenimiento pero en determinadas instalaciones esta consideración deberá ser tenida en cuenta por la imposibilidad de un control periódico y deberá ser soportado por comunicación monitorizada.

4.2 Conexión a Red Celular.

En las últimas décadas el área de las telecomunicaciones ha alcanzado un acelerado y notable desarrollo, tanto en las transmisiones libres como en los enlaces de punto a punto. Uno de los sectores de las telecomunicaciones que ha alcanzado mayor desarrollo es el de las comunicaciones móviles, tanto que para 2008 se estimaba que alrededor del mundo existían cerca de 4.1 billones de personas suscritos a servicios de red celular.

Uno de los principales servicios de las redes celulares en esta época es el de mensajería instantánea SMS que será tratado a continuación.

4.2.1 Servicio de Mensajes Cortos (SMS).

El servicio de mensajes cortos o SMS (Short Message Service) es un servicio disponible en los teléfonos móviles que permite el envío de mensajes cortos entre teléfonos móviles, teléfonos fijos y otros dispositivos de mano. SMS fue diseñado originariamente como parte del estándar de telefonía móvil digital GSM, pero en la actualidad está disponible en una amplia variedad de redes, incluyendo las redes 3G.

En un principio, los mensajes SMS se definieron en el estándar GSM como un medio para que los operadores de red enviaran información sobre el servicio a los abonados, sin que éstos pudieran responder ni enviar mensajes a otros clientes. Este tipo de mensajes se denominaban MT-SM *(Mobile Terminated-Short Message,* es decir, mensajes que llegan al terminal del usuario).

Los mensajes de texto son procesados por un SMSC o centro de mensajes cortos *(Short Message Service Center)* que se encarga de almacenarlos hasta que son enviados y de conectar con el resto de elementos de la red GSM.

Un mensaje SMS es una cadena alfanumérica de hasta 160 caracteres de 7 bits, y cuyo encapsulado incluye una serie de parámetros. En principio, se emplean para enviar y recibir mensajes de texto normal, pero existen extensiones del protocolo básico que permiten incluir otros tipos de contenido, dar formato a los mensajes o encadenar varios mensajes de texto para permitir mayor longitud.

4.2.2 Mensajería en masa.

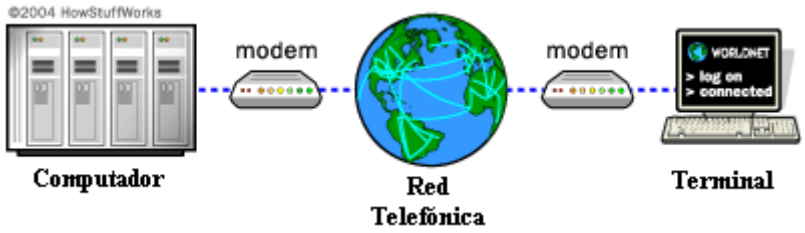
La mensajería en masa es la difusión de un gran número de mensajes SMS para la entrega a las terminales de telefonía móvil. Se usa principalmente por empresas de medios de comunicación, empresas, bancos (para la comercialización y control del fraude) y marcas de consumo para una variedad de propósitos, incluyendo el entretenimiento, la empresa y el marketing móvil. A su vez proveen las siguientes ventajas:

- Reducción de costos de llamadas.
- Reduce el tiempo de contacto con las personas.
- Envío por grupos.
- Ofrece imagen de modernidad a las empresas que lo utilizan.
- Fechas y horarios de envío son programables.

El envío masivo de mensajes de texto usualmente se logra mediante software que realizan esta operación mediante distintas formas de comunicación, ya sea utilizando una conexión a internet o a través de una conexión a una red GSM mediante un teléfono móvil o un modem GSM/GPRS.

4.2.3 Los Módems.

La palabra "módem" es una contracción de las palabras modulador-demodulador. Un módem es típicamente usado para enviar los datos digitales a través de una línea telefónica. El modem transmisor modula los datos en una señal de que es compatible con la línea telefónica, módem y receptor de-modula la señal de nuevo en datos digitales. Los Módems inalámbricos convierten los datos digitales en señales de radio y viceversa. Los módems existen desde la década de 1960 como una manera de permitir que terminales se conectaran a computadores a través de las líneas telefónicas.



Arreglo de conexión simple mediante módem.
Tomada del artículo. http://computer.howstuffworks.com/modem1.htm

En una configuración como esta, una terminal tonta en una oficina o tienda podría "marcar" a una gran computadora central. El 1960 fue la edad de tiempo compartido de los ordenadores, por lo que una empresa solía comprar tiempo de computadora de una instalación de tiempo compartido y conectarse a él a través de un modem de 300-bits por segundo (bps).

Una terminal tonta no es más que un teclado y una pantalla. Una terminal tonta muy

común en el momento fue la DEC VT-100, y se convirtió en una norma del día. El VT-100 podía mostrar 25 líneas de 80 caracteres cada uno. Cuando el usuario escribía un carácter en la terminal, el módem enviaba el código ASCII para el carácter a la computadora. El ordenador entonces enviaba el carácter de regreso a la computadora por lo que aparecía en la pantalla.

Cuando las computadoras personales comenzaron a aparecer en la década de 1970, los sistemas de tablón de anuncios (BBS) se convirtieron en la norma. Una persona configuraba un equipo con un módem y algún software de BBS, y otras personas marcaban para conectar con el tablón de anuncios. Los usuarios ejecutaban emuladores de terminales en sus ordenadores para emular una terminal tonta.

La gente se trabajó con 300 bps por bastante tiempo. La razón por la cual esta velocidad era tolerable se debía a que 300 bps representan alrededor de 30 caracteres por segundo, que es mucho más caracteres por segundo que una persona puede escribir o leer. Una vez que la gente comenzó a transferir grandes programas y las imágenes hacia y desde los sistemas de tablón de anuncios, sin embargo, 300 bps se convirtió en intolerable.

4.2.4 Módems GSM.

Un módem GSM es un módem inalámbrico que funciona con una red inalámbrica GSM. Un módem inalámbrico se comporta como un módem de acceso telefónico. La principal

diferencia entre ellos es que un módem envía y recibe datos a través de una línea telefónica fija, mientras que un módem inalámbrico envía y recibe datos a través de ondas de radio.

Un módem GSM puede ser un dispositivo externo o una tarjeta PC Card / PCMCIA Card. Normalmente, un módem GSM externo está conectado a un ordenador mediante un cable serial o un cable USB. Un módem GSM en la forma de una tarjeta PC Card / PCMCIA Card está diseñado para su uso con un ordenador portátil.

Al igual que un teléfono móvil GSM, un módem GSM requiere una tarjeta SIM de un operador de red para operar.

Los equipos utilizan comandos para controlar módems. Ambos modems GSM y dial-up módems soportan un set común de comandos AT. Se puede utilizar un módem GSM al igual que un módem de acceso telefónico.

Además de los comandos AT estándar, los modems GSM soportan una amplia serie de comandos. Estos comandos ampliados se definen en las normas del GSM. Con la ampliación de los comandos AT, puede hacer cosas como:

- Lectura, escritura y borrado de mensajes SMS.
- Envío de mensajes SMS.

- Control de la fuerza de la señal.
- Vigilancia el estado de carga y nivel de carga de la batería.
- La lectura, la escritura y la búsqueda de entradas de la libreta de teléfonos.
- El número de mensajes SMS que pueden ser procesados por un módem GSM por minuto es muy bajo - sólo unos seis a diez mensajes SMS por minuto.

Un módem GPRS es un módem GSM que además apoya la tecnología GPRS para la transmisión de datos. GPRS significa General Packet Radio Service. Se trata de una tecnología de conmutación de paquetes que es una extensión del GSM. (GSM es una tecnología de conmutación de circuitos). Una de las principales ventajas de GPRS a través del GSM es que GPRS tiene una mayor velocidad de transmisión de datos.


Modem GSM/GPRS.
http://www.made-in-china.com/

GPRS se puede utilizar como portador de SMS. Si se usa SMS a través de GPRS, se obtiene una velocidad de transmisión de SMS de alrededor de 30 mensajes SMS por minuto. Esto es mucho más rápido que el normal uso de SMS a través del GSM. Se requiere un módem GPRS para enviar y recibir SMS a través de GPRS. Sin embargo, hay que notara que algunos operadores móviles no soportan el envío y recepción de SMS a través de GPRS.

En general, un módem GSM / GPRS está recomendado para uso con un ordenador para enviar y recibir mensajes. Esto se debe a que algunos teléfonos móviles tienen ciertas limitaciones en comparación con GSM / GPRS módems. Algunas de las limitaciones que se describen a continuación:

- Algunos modelos de teléfonos móviles no se puede utilizar con un ordenador para recibir mensajes SMS concatenados (tienen mas de 140 bytes).

- Muchos modelos de teléfonos móviles no se puede utilizar con un ordenador para recibir mensajes MMS. Porque cuando reciben una notificación de MMS, la manejan de manera automática en lugar de transmitirla a la computadora.

- Un teléfono móvil no admite algunos comandos AT, parámetros de comando y valores de los parámetros. Por ejemplo, algunos teléfonos móviles no soportan el envío y recepción de mensajes SMS en modo texto. Por lo tanto, el comando AT "AT + CMGF = 1" (que encarga al teléfono móvil para uso en modo texto) provocará un mensaje de error al ser devueltos. Por lo general, GSM / GPRS módems apoyar un conjunto más completo de comandos AT que los teléfonos móviles.

- La mayoría de aplicaciones de mensajería SMS tienen que estar disponibles las 24 horas del día. Si estas aplicaciones de mensajería SMS de los teléfonos móviles se

utilizan para enviar y recibir mensajes SMS, los teléfonos móviles tienen que estar encendidos todo el tiempo. Sin embargo, algunos modelos de teléfonos móviles no pueden funcionar con la bacteria removida, incluso cuando está conectado a un adaptador de CA, lo que significa que la batería se cargará 24 horas del día.

Además de las cuestiones antes mencionadas, los teléfonos móviles GSM / GPRS módems son más o menos lo mismo para enviar y recibir mensajes SMS desde un ordenador. En realidad, se puede considerar un comando AT-teléfono móvil como "GSM / GPRS modem + teclado + pantalla".

No hay mucha diferencia entre los teléfonos móviles y GSM / GPRS módems en términos de tasa de transmisión de SMS, ya que el factor determinante para la tasa de transmisión de SMS es la red inalámbrica.

4.2.4.1 Envío de mensajes SMS desde mediante módems GSM / GPRS.

Las especificaciones del SMS han definido una forma en que un ordenador puede enviar mensajes SMS a través de un teléfono móvil o módem GSM / GPRS.

Un módem inalámbrico es similar a un módem de acceso telefónico. La principal diferencia es que un módem inalámbrico transmite datos a través de una red inalámbrica que un módem transmite datos a través de una línea telefónica de cobre. La mayoría de

los teléfonos móviles pueden ser utilizados como un módem inalámbrico. Sin embargo, algunos teléfonos móviles tienen ciertas limitaciones en comparación con los módems GSM / GPRS.

Para enviar mensajes SMS, en primer lugar, se necesita una tarjeta SIM válida de un operador de red en un teléfono móvil o módem GSM / GPRS, que luego se conecta a un ordenador. Hay varias maneras de conectar un teléfono móvil o GSM / GPRS módem a un ordenador. Por ejemplo, se puede conectar a través de un cable serial, un cable USB, la conexión Bluetooth o una conexión de infrarrojos. La forma de uso depende de la capacidad del teléfono móvil o GSM / GPRS modem.

Después de conectar un teléfono móvil o GSM / GPRS módem a un ordenador, puede controlar el teléfono móvil o GSM / GPRS módem mediante el envío de instrucciones a él. Las instrucciones utilizadas para controlar el teléfono móvil o GSM / GPRS módem son llamados comandos AT. (Comandos AT también se utilizan para el control de módems dial-up para sistemas de teléfono cableado.) Dial-up módems, teléfonos móviles y GSM / GPRS módems apoyo común un conjunto de comandos AT. Además de este conjunto de comandos AT estándar, y los teléfonos móviles GSM / GPRS módems apoyar una amplia serie de comandos AT. Uno de los usos de la ampliación de los comandos AT es controlar el envío y recepción de mensajes SMS.

Una forma de enviar comandos AT a un teléfono móvil o módem GSM / GPRS es usar un programa terminal. Un programa de terminal funciona de la manera siguiente: Se

envía los caracteres escritos para el teléfono móvil o módem GSM / GPRS. A continuación se muestra la respuesta que recibe desde el teléfono móvil o módem GSM / GPRS en la pantalla.

En la mayoría de los casos, la mayor opción en lugar de utilizar programas terminales y escribir el código para interactuar con el teléfono móvil o módem GSM / GPRS a través de comandos AT, es usar librerías de mensajería SMS API (Application Programming Interface) / SDK (Software Development Kit)de alto nivel. La librería API / SDK encapsula el bajo nivel de detalles. Así, un desarrollador de aplicaciones de SMS no necesita saber los comandos AT y la composición de mensajes SMS en el nivel de bits.

4.3 Conexión a Internet.

4.3.1 C SHARP (C#).

Es un lenguaje de programación orientado a objetos(programación orientada a objeto es un paradigma de programación que usa objetos y sus interacciones para diseñar aplicaciones y programas de computadora) desarrollado y estandarizado por Microsoft como parte de su plataforma .NET(.net es un proyecto de Microsoft para crear una nueva plataforma de desarrollo de software con énfasis en transparencia de redes, con independencia de plataforma de hardware y que permita un rápido desarrollo de

aplicaciones), que después fue aprobado como un estándar por la ECMA (es una organización internacional basada en membrecías de estándares para la comunicación y la información) e ISO(organización internacional para la estandarización).

Su sintaxis básica deriva de C/C++ y utiliza el modelo de objetos de la plataforma.NET el cual es similar al de Java aunque incluye mejoras derivadas de otros lenguajes (entre ellos Delphi).

La creación del nombre del lenguaje, C#, proviene de dibujar dos signos positivos encima de los dos signos positivos de "C++", queriendo dar una imagen de salto evolutivo del mismo modo que ocurrió con el paso de C a C++.

C#, como parte de la plataforma.NET, está normalizado por ECMA desde diciembre de 2001 (ECMA-334 "Especificación del lenguaje C#"). El 7 de noviembre de 2005 salió la versión 2.0 del lenguaje que incluía mejoras tales como tipos genéricos, métodos anónimos, iteradores, tipos parciales y tipos anulables. El 19 de noviembre de 2007 salió la versión 3.0 de C# destacando entre las mejoras los tipos implícitos, tipos anónimos y LINQ (Language Integrated Query -consulta integrada en el lenguaje).

Aunque C# forma parte de la plataforma.NET, ésta es una interfaz de programación de aplicaciones (**API**); mientras que C# es un lenguaje de programación independiente diseñado para generar programas sobre dicha plataforma. Ya existe un compilador implementado que provee el marco de DotGNU - Mono que genera programas para distintas plataformas como Win32, UNIX y Linux.

4.3.2 Servicio web.

Un **servicio web** (en inglés, Web service) es un conjunto de protocolos y estándares que sirven para intercambiar datos entre aplicaciones. Distintas aplicaciones de software desarrolladas en lenguajes de programación diferentes, y ejecutadas sobre cualquier plataforma, pueden utilizar los servicios web para intercambiar datos en redes de ordenadores como Internet. La interoperabilidad se consigue mediante la adopción de estándares abiertos. Las organizaciones OASIS (acrónimo de (Organization for the Advancement of Structured Information Standards) es un consorcio internacional sin fines de lucro que orienta el desarrollo, la convergencia y la adopción de los estándares de comercio electrónico y servicios web.) y W3C(El **World Wide Web Consortium**, abreviado **W3C**, es un consorcio internacional que produce recomendaciones para la World Wide Web.) son los comités responsables de la arquitectura y reglamentación de los servicios Web. Para mejorar la interoperabilidad entre distintas implementaciones de servicios Web se ha creado el organismo WS-I, encargado de desarrollar diversos perfiles para definir de manera más exhaustiva estos estándares.

4.3.2.1 Estándares empleados.

- Web Services Protocol Stack: Así se denomina al conjunto de servicios y protocolos de los servicios Web.
- XML (Extensible Markup Language): Es el formato estándar para los datos que se vayan a intercambiar.
- SOAP (Simple Object Access Protocol) o XML-RPC (XML Remote Procedure Call): Protocolos sobre los que se establece el intercambio.
- Otros protocolos: los datos en XML también pueden enviarse de una aplicación a otra mediante protocolos normales como HTTP (Hypertext Transfer Protocol), FTP (File Transfer Protocol), o SMTP (Simple Mail Transfer Protocol).
- WSDL (Web Services Description Language): Es el lenguaje de la interfaz pública para los servicios Web. Es una descripción basada en XML de los requisitos funcionales necesarios para establecer una comunicación con los servicios Web.
- UDDI (Universal Description, Discovery and Integration): Protocolo para publicar la información de los servicios Web. Permite comprobar qué servicios web están disponibles.
- WS-Security (Web Service Security): Protocolo de seguridad aceptado como estándar por OASIS (Organization for the Advancement of Structured Information Standards). Garantiza la autenticación de los actores y la confidencialidad de los mensajes enviados.

4.3.2.2 Ventajas de los servicios Web.

Aportan interoperabilidad entre aplicaciones de software independientemente de sus propiedades o de las plataformas sobre las que se instalen.

- Los servicios Web fomentan los estándares y protocolos basados en texto, que hacen más fácil acceder a su contenido y entender su funcionamiento.
- Al apoyarse en HTTP, los servicios Web pueden aprovecharse de los sistemas de seguridad firewall sin necesidad de cambiar las reglas de filtrado.
- Permiten que servicios y software de diferentes compañías ubicadas en diferentes lugares geográficos puedan ser combinados fácilmente para proveer servicios integrados.
- Permiten la interoperabilidad entre plataformas de distintos fabricantes por medio de protocolos estándar y abiertos. Las especificaciones son gestionadas por una organización abierta, la W3C, por tanto no hay secretismos por intereses particulares de fabricantes concretos y se garantiza la plena interoperabilidad entre aplicaciones

4.3.3 SOAP.

Son las siglas de Simple Object Access Protocol. Este protocolo deriva de un protocolo creado por David Winer, XML-RPC en 1998. Con este protocolo se pedían realizar RPC

o remote procedure calls, es decir, podíamos bien en cliente o servidor realizar peticiones mediante http a un servidor web. Los mensajes debían tener un formato determinado empleando XML para encapsular los parámetros de la petición. Con el paso del tiempo el proyecto iniciado por David Winer interesó a Importantes multinacionales entre las que se encuentran IBM y Microsoft y de este interés por XML-RPC se desarrollo SOAP."

En el núcleo de los servicios Web se encuentra el protocolo simple de acceso a datos SOAP, que proporciona un mecanismo estándar de empaquetar mensajes. SOAP ha recibido gran atención debido a que facilita una comunicación del estilo RPC entre un cliente y un servidor remoto. Pero existen multitud de protocolos creados para facilitar la comunicación entre aplicaciones, incluyendo RPC de Sum, DCE de Microsoft, RMI de Java y ORPC de CORBA. ¿Por qué se presta tanta atención a SOAP?

Una de las razones principales es que SOAP ha recibido un increíble apoyo por parte de la industria. SOAP es el primer protocolo de su tipo que ha sido aceptado prácticamente por todas las grandes compañías de software del mundo. Compañías que en raras ocasiones cooperan entre sí están ofreciendo su apoyo a este protocolo. Algunas de las mayores Compañías que soportan SOAP son Microsoft, IBM, SUN, Microsystems, SAP y Ariba.

Algunas de las Ventajas de SOAP son:

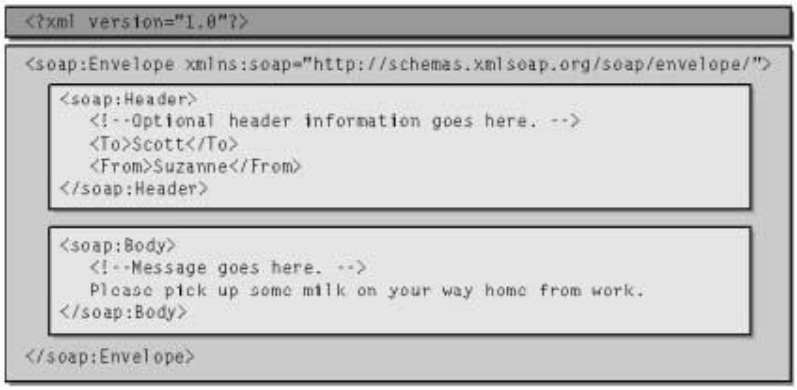
- **No esta asociado con ningún lenguaje**: los desarrolladores involucrados en nuevos proyectos pueden elegir desarrollar con el ultimo y mejor lenguaje de programación que exista pero los desarrolladores responsables de mantener antiguas aflicciones heredadas podrían no poder hacer esta elección sobre el lenguaje de programación que utilizan. SOAP no especifica una API, por lo que la implementación de la API se deja al lenguaje de programación, como en Java, y la plataforma como Microsoft .Net.
- **No se encuentra fuertemente asociado a ningún protocolo de transporte**: La especificación de SOAP no describe como se deberían asociar los mensajes de SOAP con HTTP. Un mensaje de SOAP no es más que un documento XML, por lo que puede transportarse utilizando cualquier protocolo capaz de transmitir texto.
- **No está atado a ninguna infraestructura de objeto distribuido** La mayoría de los sistemas de objetos distribuidos se pueden extender, y ya lo están alguno de ellos para que admitan SOAP.
- **Aprovecha los estándares existentes en la industria**: Los principales contribuyentes a la especificación SOAP evitaron, intencionadamente, reinventar las cosas. Optaron por extender los estándares existentes para que coincidieran con sus necesidades. Por ejemplo, SOAP aprovecha XML para la codificación de los mensajes, en lugar de utilizar su propio sistema de tipo que ya están definidas en la especificación esquema de XML. Y como ya se ha mencionado SOAP no

define un medio de trasporte de los mensajes; los mensajes de SOAP se pueden asociar a los protocolos de transporte existentes como HTTP y SMTP.

- **Permite la interoperabilidad entre múltiples entornos**: SOAP se desarrollo sobre los estándares existentes de la industria, por lo que las aplicaciones que se ejecuten en plataformas con dicho estándares pueden comunicarse mediante mensaje SOAP con aplicaciones que se ejecuten en otras plataformas. Por ejemplo, una aplicación de escritorio que se ejecute en una PC puede comunicarse con una aplicación del back-end ejecutándose en un mainframe capaz de enviar y recibir XML sobre HTTP.

4.2.3.1 Anatomía de un mensaje de SOAP.

SOAP proporciona un mecanismo estándar de empaquetar un mensaje. Un mensaje SOAP se compone de un sobre que contiene el cuerpo del mensaje y cualquier información de cabecera que se utiliza para describir le mensaje. A continuación tiene un ejemplo:



"Anatomía de un mensaje SOAP"

El elemento raíz del documento es el elemento Envelope. El ejemplo contiene dos subelementos, Body y Header. Un ejemplo de SOAP valido también puede contener otros elementos hijo en el sobre.

El sobre puede contener un elemento Header opcional que contiene información sobre el mensaje. En el ejemplo anterior, la cabecera contiene dos elementos que describen a quien compuso el mensaje, y posible receptor del mismo. El sobre debe contener un elemento body el elemento body (cuerpo) contiene la carga de datos del mensaje. En el ejemplo el cuerpo contiene una simple cadena de caracteres.

Un mensaje debe estar dentro de sobre de SOAP bien construido. Un sobre se compone de un único elemento envelope el sobre puede contener un elemento Header y puede contener un elemento body. Si existe, la cabecera debe ser el elemento hijo inmediato del sobre, con el cuerpo siguiendo inmediatamente a la cabecera. El cuerpo contiene la carga

de datos del mensaje y la cabecera contiene los datos adicionales que no pertenecen necesariamente al cuerpo del mensaje.

Además de definir un sobre de SOAP, la especificación de SOAP define una forma de codificar los datos contenidos en un mensaje. La codificación de SOAP proporciona un mecanismo estándar para serializar tipos de datos no definidos en la parte 1 de la especificación del esquema de XML.

La especificación de SOAP también proporciona un patrón de mensaje estándar para facilitar el comportamiento de tipo RPC. Se emparejan dos mensajes de SOAP para facilitar la asociación de un mensaje de petición con un mensaje de respuesta.

La llamada a un método y sus parámetros se serializan en el cuerpo del mensaje de petición en forma de una estructura. El elemento raíz tiene el mismo nombre que el método objetivo, con cada uno de los parámetros codificado como un subelemento.

El mensaje de respuesta puede contener los resultados de la llamada al método o una estructura de fallo bien definida. Los resultados de la llamada a un método se serializan en el cuerpo de la petición como una estructura. Por convenio, el elemento raíz tiene el mismo nombre que el método original al que se añade resultados. Los parámetros de retorno se serializan como elementos hijo, con el parámetro de retorno en primer lugar. Si se encuentra un error el cuerpo del mensaje de respuesta contendrá una estructura de fallo bien definida.

4.3.4 ASP.NET.

Es un framework para aplicaciones web desarrollado y comercializado por Microsoft. Es usado por programadores para construir sitios web dinámicos, aplicaciones web y servicios web XML. Apareció en enero de 2002 con la versión 1.0 del .NET Framework, y es la tecnología sucesora de la tecnología Active Server Pages (ASP). ASP.NET está construido sobre el Common Language Runtime, permitiendo a los programadores escribir código ASP.NET usando cualquier lenguaje admitido por el .NET Framework.

Cualquier persona que está familiarizada con el desarrollo de aplicaciones web sabrá que el desarrollo web no es una tarea simple. Ya que mientras que un modelo de programación para aplicaciones de uso común está muy bien establecido y soportado por un gran número de lenguajes, herramientas de desarrollo, la programación web es una mezcla de varios lenguajes de etiquetas, un gran uso de lenguajes de script y plataformas de servidor. Por desgracia para el programador de nivel intermedio, el conocimiento y habilidades que se necesitan para desarrollar aplicaciones web tienen muy poco en común con las que son necesarias en el desarrollo tradicional de aplicaciones.

4.3.4.1 El protocolo RS-232.

El protocolo RS-232 es una norma o estándar mundial que rige los parámetros de uno de los modos de comunicación serial. Por medio de este protocolo se estandarizan las

velocidades de transferencia de datos, la forma de control que utiliza dicha transferencia, los niveles de voltajes utilizados, el tipo de cable permitido, las distancias entre equipos, los conectores, etc.

Además de las líneas de transmisión (Tx) y recepción (Rx), las comunicaciones seriales poseen otras líneas de control de flujo (Hands-hake), donde su uso es opcional dependiendo del dispositivo a conectar.

4.3.4.2 Señales de la RS-232.

Request To Send (RTS) Esta señal se envía de la computadora (DTE) al módem (DCE) para indicar que se quieren transmitir datos. Si el módem decide que esta OK, asiente por la línea CTS. Una vez la computadora prende la señal RTS, esperará que el módem asiente la línea CTS. Cuando la señal CTS es afirmado por el módem, la computadora empezará a transmitir datos.

Clear To Send (CTS) Afirmado por el módem después de recibir la señal de RTS indica que la computadora puede transmitir.

Data Terminal Ready (DTR) Esta línea de señal es afirmada por la computadora, e informa al módem que la computadora está lista para recibir datos.

Data Set Ready (DSR) Esta línea de señal es afirmada por el módem en respuesta a una señal de DTR de la computadora. La computadora supervisa el estado de esta línea después de afirmar DTR para descubrir si el módem esta encendido.

Receive Signal Line Detect (RSLD) Esta línea de control es afirmada por el módem e informa a la computadora que se ha establecido una conexión física con otro módem. A veces se conoce como detector de portadora (CD). Sería un error que una computadora transmita información a un módem si esta línea no está prendida, es decir si la conexión física no funciona.

Transmit Data (TD) es la línea por donde el dato se transmite de un bit a la vez

Receive Data (RD) es la línea por donde el dato se recibe de un bits a la vez.

7. MARCO METODOLÓGICO.

CAPITULO 5: APLICACIÓN DEL SISTEMA RFID AL PROCESO DE AUTOMATIZACIÓN DEL PARQUEO DE UNAPEC.

- Universo, población y variables del estudio.

El universo de la investigación presente se reduce al parqueo de la Universidad APEC, específicamente al área que es accesible a través de la calle Dr. Cesar Dargam, la cual corresponde al parqueo principal del recinto.

La población a la que va dirigida el estudio son los estudiantes, profesores y empleados de la Universidad APEC, tomando como muestra aquellos estudiantes profesores y empleados de la universidad los cuales tienen al menos un vehiculo de motor.

Las variables a tomar en cuenta para el estudio realizado son la seguridad del parqueo, el diseño y capacidad del mismo, así como la disponibilidad de lugares para estacionamiento.

- Fuentes utilizadas para la recolección de la información.

Las fuentes que se utilizaron para el desarrollo de la presente investigación incluye:

- Libros.
- Internet.
- Investigaciones anteriores.

- Tutoriales.
- Manuales.

- Instrumentos y técnicas utilizadas para realizar la investigación.

Las principales técnicas y herramientas de investigación que se utilizaron para el proceso de recolección, análisis y depuración de los datos presentados fueron:

Entrevistas.

Se realizaron entrevistas a personas expertas en área de las telecomunicaciones, familiarizadas con el diseño e implementación de aplicaciones para gestión de datos y para páginas Web.

Observación.

Este método nos permitió identificar la cantidad identificar las condiciones existentes en el parqueo de la Universidad APEC, así como la capacidad estimada del mismo.

Método Inductivo

A partir de lo observado, con este método se pudo obtener información sobre los diferentes factores que influyen en el estado del parqueo en la universidad y llegar a conclusiones generales sobre el problema de investigación.

Método Deductivo

Se utilizó este método a partir de los resultados obtenidos por medio de entrevistas y la documentación existente, de las cuales se obtuvo información sobre la manera en que se podría implementar el sistema para automatizar el parqueo de la Universidad APEC.

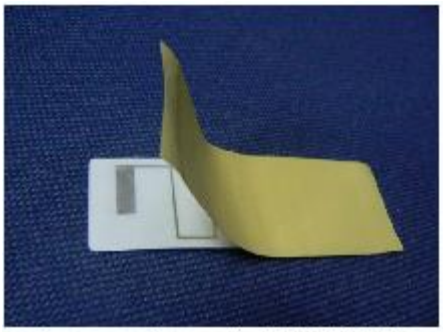
Técnica Documental

Se empleó esta técnica para la revisión, análisis y selección de la literatura disponible sobre los temas relacionados con la investigación desarrollada.

5.1 Sistema de Control de Acceso mediante RFID.

Para acceder al estacionamiento de la Universidad APEC por la calle Dr. Cesar Dargam el vehículo que requiere el acceso debe de estar identificado con un tag pasivo, estos no tienen fuente de alimentación (batería) integrada, utilizan la energía emitida por el lector para autoalimentarse y transmitir su información almacenada al lector. Se seleccionaron los tags pasivos por que el rango que alcanzan es unos pocos centímetros hasta nueve metros lo cual es suficiente para lo deseado y el precio es menor al de los demás tags.

Los tags pasivos a utilizar serán el modelo MR6780 de la compañía Shenzhen Marktrace Technology Co., Ltd.



Tag pasivo modelo MR6780

5.1.1 Características.

- Etiqueta de papel de la frecuencia ultra elevada de la etiqueta de RFID, etiqueta de la voz pasiva del RFID

- Protocolo: ISO18000-6B, ISO18000-6C (EPC GEN2)
- Gama de frecuencia: ISMO 920~925MHz (China) y ISMO 902~928MHz (FCC) Permitido a menos de 4 watts sin licencia.
- Modo de operación de frecuencia fija o software de FHSS programable
- Gama de la lectura: más el de 12m relacionado con el lector y la antena
- Temperatura de la operación: 20C a 80C

El dispositivo tag incorporado al vehículo lleva asociado unos datos identificativos que hacen único al automóvil. Cuando dicho tag está expuesto al alcance del lector RFID, el tag le transmite la información a través de la antena del lector. Esta está conectada al componente receptor / emisor.

El transmisor se utiliza para transmitir la corriente alterna y el ciclo de reloj por las antenas hacia los tags a leer. Es parte del modulo emisor/receptor que se encarga de enviar la señal del lector al entorno y recibir la respuesta por la antena.

El receptor forma parte del componente emisor/receptor y es el encargado de recibir la señal analógica del tag por la antena y traspasarla al microprocesador del lector donde se transformara a señal digital.

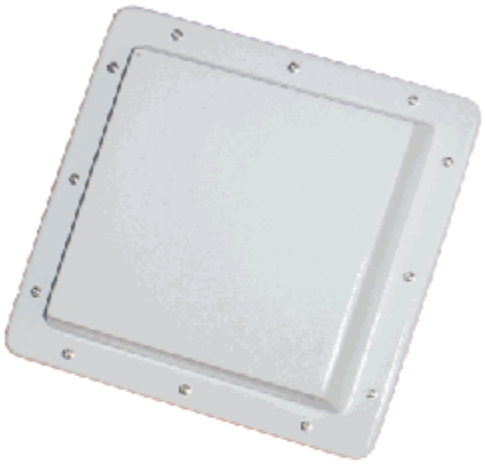
UHF Long Range Reader -- DL910

El lector está compuesto por transmisor, receptor, memoria, interfaces de salida y un microprocesador.

Características del Reader DL910

- Protocolo soportado ISO18000-6B, ISO18000-6C (EPC GEN2)
- Gama de frecuencia: ISMO 920~925MHz (China) y ISMO 902~928MHz (FCC)
- Distancia de lectura 8m-15m (según el tag y el medio ambiente)
- Puertos de interface Rs232, Rs485
- Dimensiones 450mm*450mm*60mm

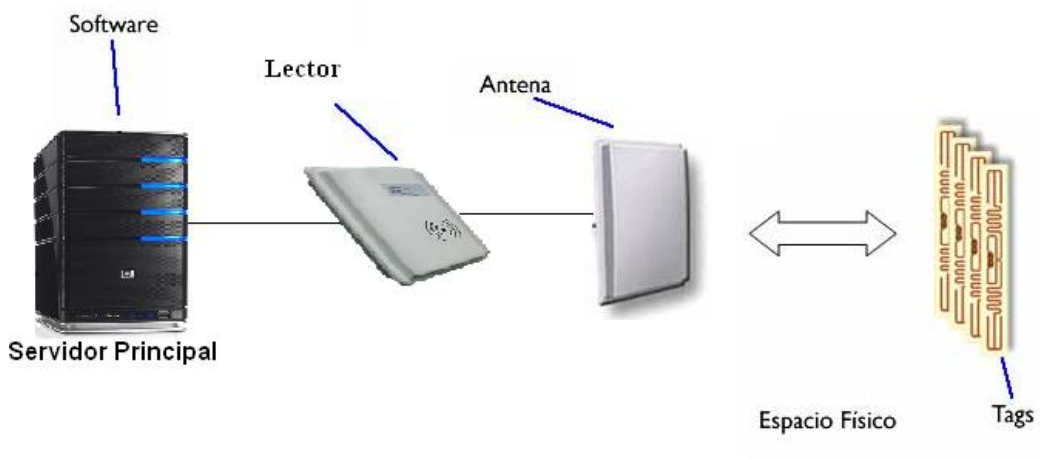
La antena utilizada será de polarización circular modelo 32600.



UHF 902 MHz. RFID Antenna – Circular
Model 326001

Características

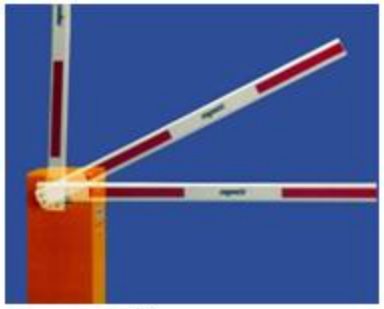
- Rango de operación 902mhz-928mhz
- Ganancia 7.15dbi
- Impedancia 50ohms
- Dimensiones 220mm*220mm*44mm



5.1.2 Gestión de los Datos.

Una vez el lector adquiera la información, este la transferirá por medio una conexión serie a un computador que será el servidor central del sistema. Un software (middleware) instalado en dicho servidor se encarga de almacenar los datos de identificación del objeto, verificar la permisión de acceso al área de estacionamiento y enviar instrucciones al un dispositivo actuador que permita o prohíba el paso de los vehículos.

Este dispositivo tendrá la función de levantar una barrera (ver grafica Barrera) que estará a la entrada del estacionamiento de la UNAPEC.



Barrera

El Middleware además, se encarga del conteo de espacios disponibles y utilizados en el parqueo y de enviar dicha información a otro computador que hace de enlace entre el sistema con las redes de comunicación externas (Red Celular, Internet). Este último, tiene como propósito enviar la información sobre la disponibilidad del parqueo a través de mensajes de texto y de una pagina web.

5.2 Alimentación del Sistema.

Un sistema de RFID es de poco consumo. Tomando en cuenta que la alimentación se limita a los lectores de RFID y a los ordenadores y que el consumo de una PC oscila entre los 300W y 400W, además de utilizar transpondedores pasivos, debido a que estos no

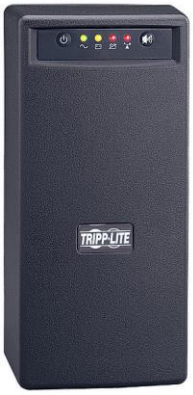
necesitan de una fuente externa de alimentación, por lo que el sistema consume un estimado de 500W.

Para la alimentación del sistema utilizaremos como fuente de energía primaria la suplida por EDESUR, debido a que es mas favorable dado las condiciones económicas. En caso de falla eléctrica, el sistema contará con una fuente de respaldo mediante sistemas UPS capaces de suplir la demanda de energía exigida por el sistema. Y para el peor de los casos, se utilizará una conexión a la planta eléctrica de la universidad como sistema de resguardo.

5.2.1 Características de los dispositivos de alimentación.

Debido a las exigencias del sistema que se está analizando, se usará un UPS con las siguientes características:

- Fabricante: Tripp Lite
- Voltaje de entrada: 120V/15A
- Voltaje de salida: 120V
- Potencia: 1kVA / 500W
- Rango de frecuencia: 50 a 60Hz



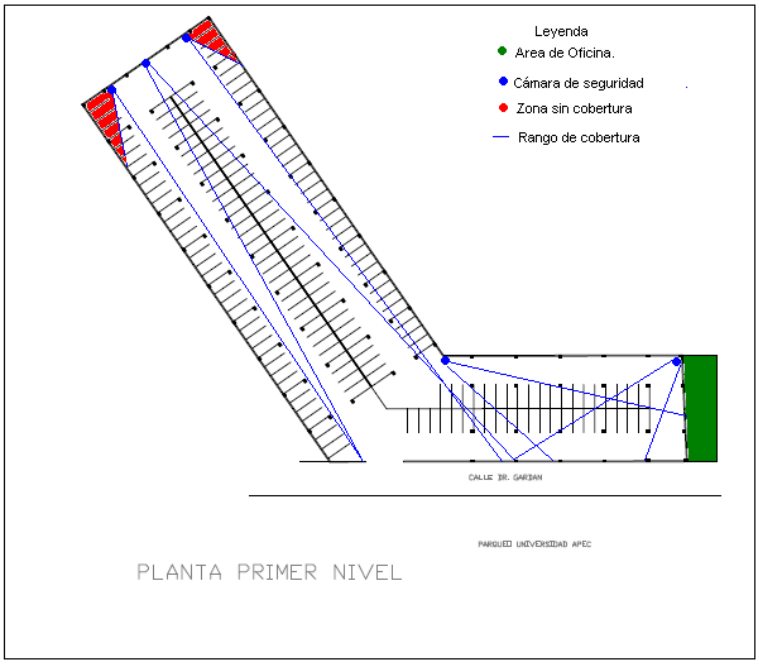
Este equipo ofrece protección para los sistemas de TI. La unidad se ha construido en un regulador automático de tensión (AVR). El AVR corrige automáticamente las altas y bajas de las fluctuaciones de tensión, asegurando que el equipo recibe energía limpia y constante. Además viene con un sistema de vigilancia, Winpower, que permite al usuario administrar y supervisar el UPS a través de una conexión USB (cable incluido).

Este aparato se encargará de mantener alimentado tanto a los lectores, como el servidor principal. En el caso del servidor de comunicaciones, su conexión será incluida al UPS principal del recinto.

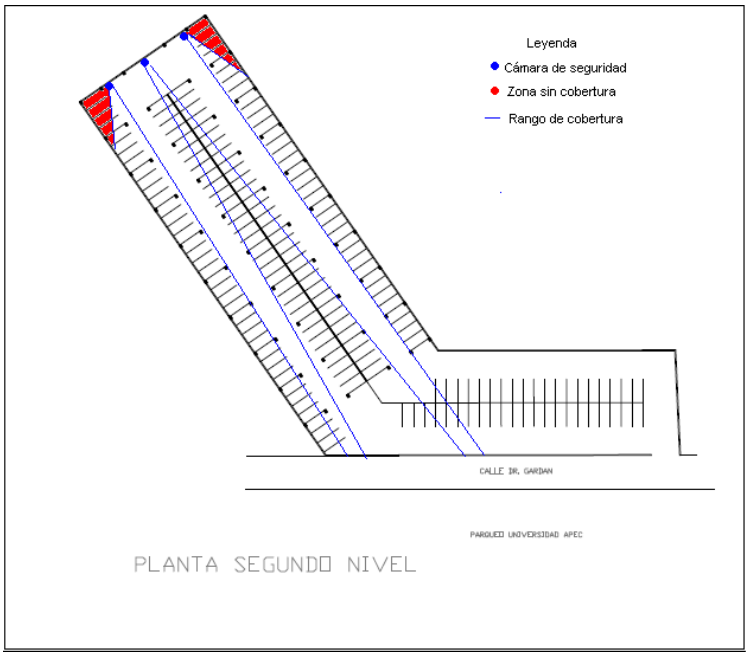
5.3 Seguridad en el estacionamiento de UNAPEC.

Con el fin de mejorar la seguridad existente en el parqueo, se utilizará una red de cámaras colocadas a lo largo del área, que estarán distribuidas a lo largo de todo el estacionamiento, de modo que se obtenga el mayor rango de visión posible. Para los casos de las horas nocturnas en que la luz disponible en el área es reducida, las cámaras contarán con un accesorio de luz infrarroja que permitirá grabar aún en condiciones de iluminación casi nula.

La disposición en el primer nivel será la siguiente:



En el segundo nivel, la distribución será como sigue:



Todas las cámaras estarán conectadas en red a un computador mediante un switch. Tanto el computador como el switch estarán ubicados en el área de oficina que se encuentra en el primer nivel. Es notable el hecho de que ciertas zonas no son cubiertas por las cámaras de seguridad debido a su ubicación, sin embargo, la cobertura es casi total para el área de parqueos que se encuentra bajo techo.

5.3.1 Características de dispositivos de seguridad.

Las cámaras que forman parte del sistema de seguridad y monitoreo del estacionamiento son DCS-3320 de la marca D-Link. La cual cuenta con las siguientes características principales:

- Resolución: 380 Líneas (TV)-
- Control automático de ganancia (AGC): 24 dB-
- Exposición Automática (AE)-
- Iluminación mínima: 1.0 Lux @ f2.0
- Lente con tipo de montaje CS

- Focal fijo (6mm, f1.8) con afinación de precisión

- Resoluciones de hasta 30 fps (176 x 120) en NTSC

- Trabaja con formato MPEG4 como modo de compresión corta para video y JPEG como compresor de imágenes- Radio de compresión: 5 niveles

- Modulación: NTSC y PAL

- 3 ventanas para detección de movimiento

Para la protección de la cámara se cuenta con un encapsulado protector DCS-45 de la empresa D-Link, con las siguientes características:

• Dimensiones: 36,7 (largo) x 14,0 (ancho) cms

• Peso: 1,48 Kg

• Housing de aluminio y bisagras de acero

La DCS-45 incluye además un diseño de barrera termal para evitar las fluctuaciones de temperatura.

Para la conexión de la red de cámaras se utiliza un enrutador D-Link DES-1316.

Características Generales:

- 16 Puertas RJ-45 100Base-TX

- 8 Puertas con soporte PoE

- Estándares: IEEE 802.3af/ 802.3/ 802.3u/ 802.3x

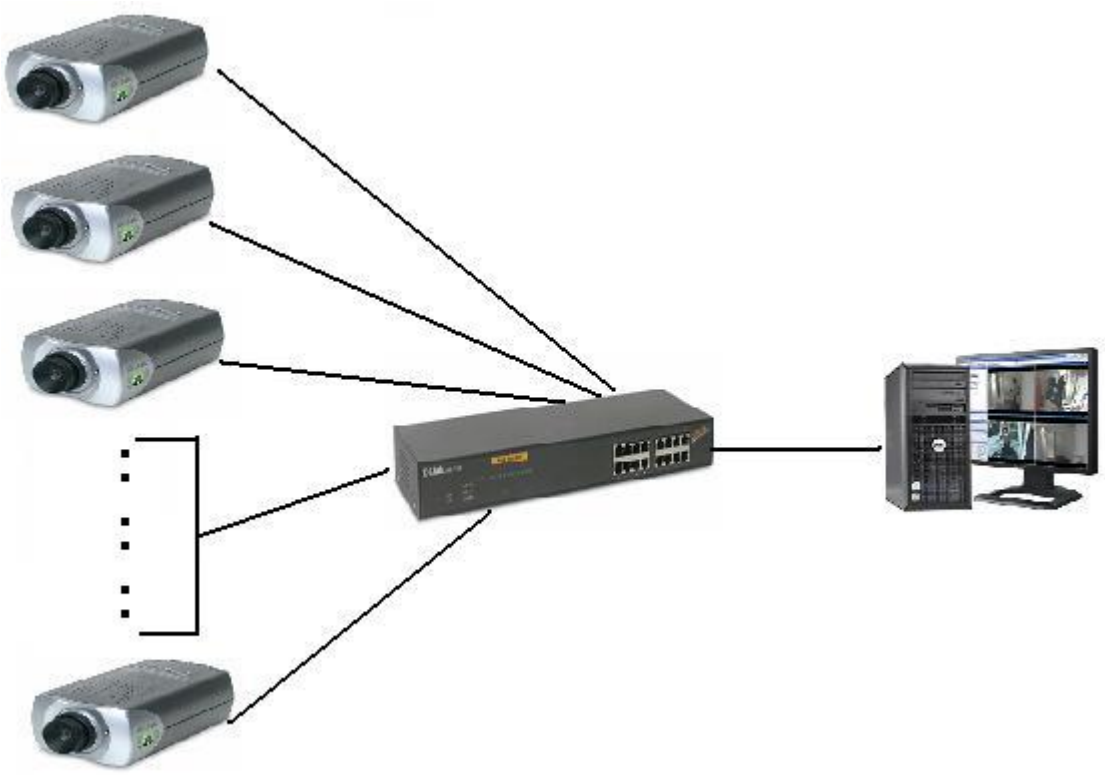
- Protocolo: CSMA/CD

- Conexión : UTP Cat. 5, Cat.5e

- Full/half duplex para velocidades 10/100Mbps

5.3.2 Configuración de Red de cámaras.

La seguridad esta fundamentado en un sistema de NVR en el cual las cámaras son conectadas en una red de por medio de cables de par trenzado (UTP). La conexión entre cámaras es posible mediante un conmutador (Switch) de red que coordina y organiza las direcciones IP de las cámaras y a su vez las conecta a un computador donde se controla todo el sistema mediante un software.



Las grabaciones de las cámaras están codificadas utilizando el formato MPEG-4, debido a la alta resolución de la imagen que provee y su bajo consumo en ancho de banda de la red.

Con fines de asegurar la integridad del sistema y evitar posibles intercepciones, el acceso a la red de cámaras estará restringido sólo a los operadores del parqueo y se llevará a cabo mediante la discriminación de las direcciones MAC de cada tarjeta de red. La red de seguridad además, estará conectada con el servidor principal del sistema completo con fines de copias de seguridad e incluso la supervisión de forma remota.

5.4 Conexión a redes de comunicación.

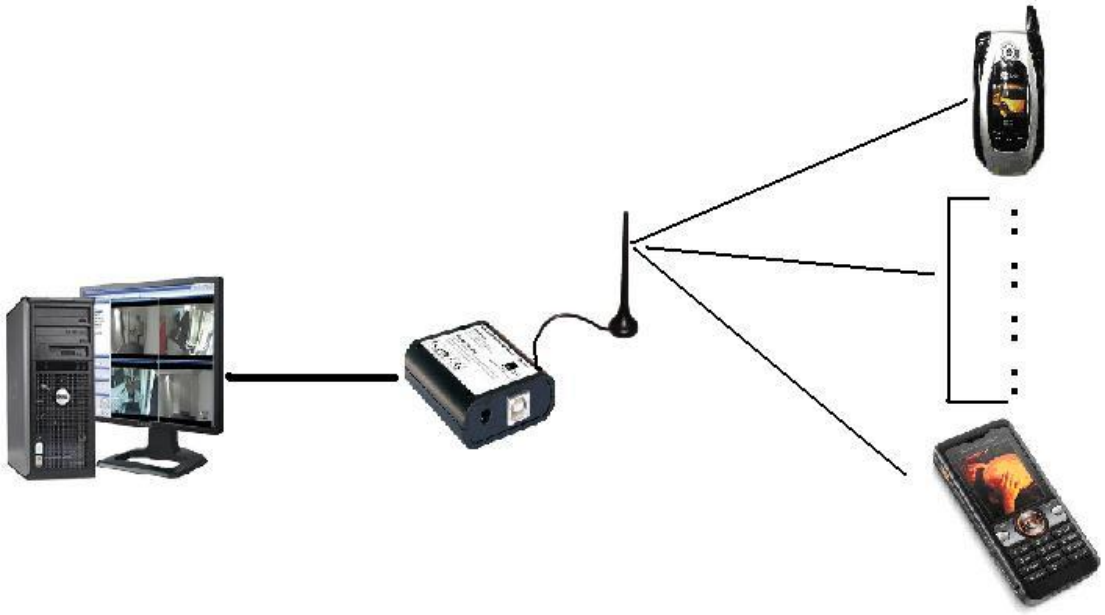
5.4.1 Red Celular.

Debido a que la mayor parte de la población perteneciente a la Universidad pertenece a la clase media y media-baja, es necesario un sistema para que estos se mantengan informados sobre el estado del parqueo sin la necesidad de estar conectados a la Internet en todo momento. Por eso, se cuenta con un sistema de mensajería a través de la red celular.

La conexión del establecimiento con la red celular se logra mediante el envío masivo de mensajes de texto cortos (SMS). Un software instalado en un computador se encarga de registrar los números telefónicos de los usuarios conectados a este servicio, así como de los horarios en que se realizará el envió de mensajes.

La información contenida en los mensajes es una proviene de una aplicación que capta la información al momento sobre el estado de disponibilidad del parqueo desde el software de gestión de datos. Esta aplicación luego introduce esa información en el software destinado al envío masivo de mensajes cortos (SMS).

El envío de la información a la red celular se lleva a cabo mediante un MODEM GSM que se conecta mediante USB al computador, y envía estos datos mediante ondas de radiofrecuencia. Para su funcionamiento es necesario que dicho MODEM GSM cuente con una tarjeta SIM activada por un proveedor de servicios de telefonía.



5.4.1.1 Característica de los dispositivos de red celular.

El dispositivo a utilizar es un MODEM GPRS/GSM Dualband de la empresa ConiuGo GMBH. Este es un dispositivo diseñada para redes en los rangos de banda de: 900/1800 Mhz y 850/1900 Mhz, para transferencias de datos inalámbricas. Este aparato cuenta con las siguientes características:

- Transmisión de datos desde el Módem GSM para redes de 900 y 1800 MHz o 850 y 1900 Mhz para transferencia de datos inalámbricos en todo el mundo (USB o

RS232).

- Interfaces estándar para aplicaciones industriales y lector de tarjetas SIM integrado.

- Uso de todos los servicios GSM (voz, fax, datos, SMS)

- Clase GPRS: Multi-slot clase 8 (4 down, 1 up)

- Tasa de Baudios: 2400 hasta 574000 bps

5.2.3 Conexión a Internet.

Tendremos una aplicación de consola realizada en C Sharp.net, que es un lenguaje de programación orientado a objetos desarrollado y estandarizado por Microsoft como parte de su plataforma .NET. La aplicación va a trabajar en la computadora que estará conectada al modulo RFID (el lector), la aplicación se encargara de leer la información proveniente del modulo RFID, esta información será transmitida por un puerto RS232.

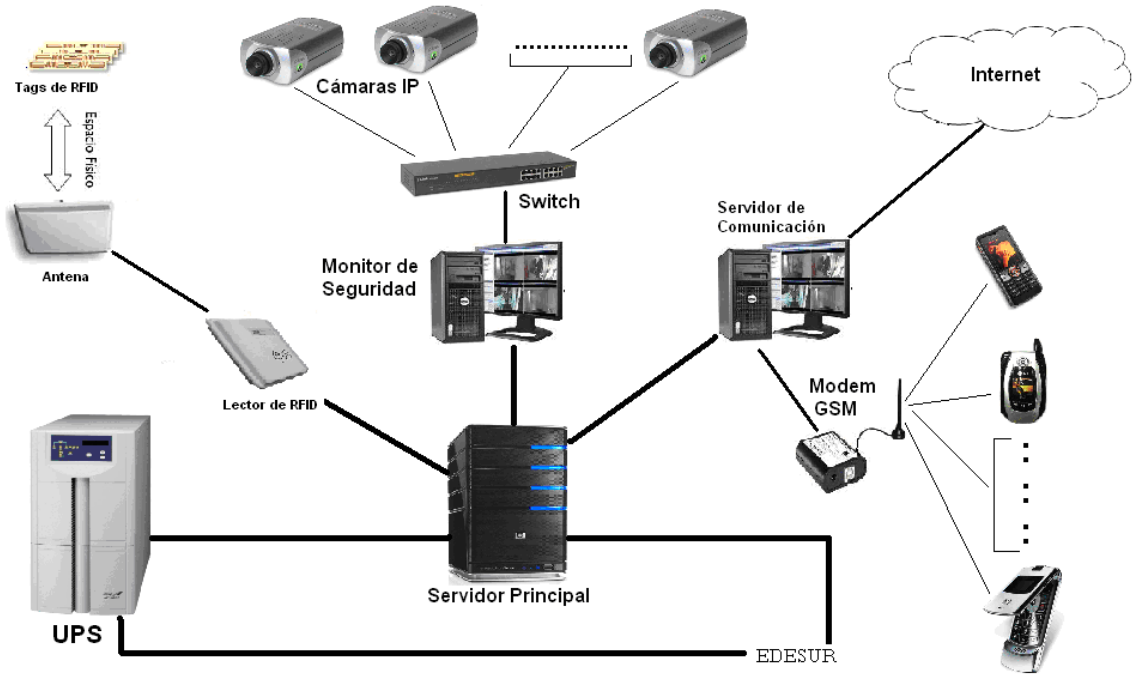
En el servidor de UNAPEC habrá un web service que es un conjunto de protocolos y estándares que sirven para intercambiar datos entre aplicaciones. Distintas aplicaciones de software desarrolladas en lenguajes de programación diferentes, y ejecutadas sobre cualquier plataforma, pueden utilizar los servicios web para intercambiar datos en redes de ordenadores como Internet. El web service se encargará de recibir la información proveniente de la aplicación de consola y la va almacenar en un archivo XML.

La aplicación de consola es a la vez un cliente del web service, por esto podrá enviar la información hacia el web service que se encontrará en el servidor de la Universidad APEC.

Una aplicación web va a leer a cada cierto tiempo la información que tenga el archivo XML y la va presentar en una página web (HTML) la cual será la página web de UNAPEC.

5.5 Esquema general del sistema.

A continuación se presenta un esquema general de la disposición de los diversos componentes dentro del sistema:



8. MARCO JURÍDICO

Las frecuencias son recursos escasos. Los avances espectaculares acontecidos en los servicios de comunicaciones móviles han generado un fuerte incremento de la demanda referida al uso radiofrecuencias.

La tecnología RFID está basada en el uso de frecuencias para su operación. El espectro electromagnético en el cual reside RFID es regulado por instituciones gubernamentales locales. El espectro electromagnético es un recurso natural, limitado y mesurable que permite transportar energía, enviar y recibir mensajes de distinta naturaleza a distancia, a través de un mecanismo de propagación por el espacio sin el concurso de una guía artificial.

Los estándares globales definen la plataforma más eficiente en la cual una industria puede operar y alcanzar sus objetivos. La asignación de radiofrecuencias se realiza en el marco de organismos internacionales, en particular por la Conferencia Mundial de Radiocomunicaciones (CMR), de la Unión Internacional de Telecomunicaciones (UIT), la Organización Internacional de Estandarización (ISO) y la EPC, las cuales han estado ampliamente activas desarrollando los estándares para esta tecnología.

ISO tiene 3 estándares para RFID: ISO 14443, para sistemas sin contacto, ISO15693 para sistema de proximidad e ISO 18000 para especificar la interfaz aérea para una variedad de aplicaciones.

EPC global es una organización sin fines de lucro que ha desarrollado una amplia gama de estándares para la identificación de productos. Los estándares EPC están enfocados a la cadena de suministro y particularmente definen la metodología para la interfaz aérea; el formato de los datos almacenados en una etiqueta RFID, para la identificación de un producto, captura, transferencia, almacenamiento y acceso de estos datos; así como el middleware y la base de datos que almacena esta información.

EPC es un esquema de identificación para identificar objetos físicos de manera universal por medio de etiquetas RFID. El código EPC en una etiqueta RFID puede identificar al fabricante, producto, versión y número de serie, y adicionalmente provee un grupo de dígitos extra para identificar objetos únicos.

La tecnología RFID involucra colocar las etiquetas RFID en los objetos, la lectura de etiquetas (idealmente sin intervención humana) y el paso de la información a un sistema dedicado de infraestructura de Tecnologías de la Información. Con dicha infraestructura

se pueden identificar objetos automáticamente, rastrear, monitorear y activar eventos relevantes.

En República Dominicana, la institución que se encarga del uso racional del espectro electromagnético es el Instituto Dominicano de las Telecomunicaciones (INDOTEL), mediante la ley No. 153-98. Su misión es regular y promover la prestación de servicios de telecomunicaciones en beneficio de la sociedad, en un marco de libre, leal y efectiva competencia.

Las siguientes son algunas organizaciones que han producido algún estándar relacionado con RFID, o han desarrollado alguna función regulatoria al respecto:

□□□ANSI (American National Standards Institute)

□□□AIAG (Automative Industry Action Group)

□□□EAN.UCC (European Article Numbering Association International, Uniform Code council)

□□□EPCglobal

□□□CEN (Comité Européen Normalisation)

□□□ETSI (European Telecommunications Standards Institute)

□□□ERO (European Radocommunications Office)

□□□UPU (Universal Postal Union)

□□□ASTM (American Society for Testing Materials)

9. RESULTADOS.

El objetivo de este estudio es el diseño e implementación de un sistema de identificación y control de acceso para el área de estacionamientos de la Universidad APEC haciendo uso de la tecnología RFID, de modo que sea posible automatizar el conteo del espacio disponible y a la vez, proveer a los principales usuarios de dicha información.

El sistema de seguridad vigente en el estacionamiento de UNAPEC, consiste en la entrega de un ticket a las personas que desean ingresar el cual, al salir la persona devolverá, este solo debe entregarse a vehículos previamente identificados, situación que no sucede.

Con la implementación del sistema, el parqueo contará con una red de cámaras de vigilancia mediante IP, mediante la cual se monitoreara todo el tiempo el estacionamiento y se almacenará la información con esto se tendrá disponible para cualquier investigación que se necesitara realizar. El monitoreo constante ayuda a tener más control del parqueo, además de ofrecer mayor seguridad a los usuarios.

Como en la entrada y salida del estacionamiento posee un barrera que solo permite el paso de vehículos autorizados por la institución, se controla el acceso de cualquier otra persona no perteneciente a la Universidad. A la salida del parqueo se contará con un desgarrador de llantas que podrá ser activado por el operador del sistema RFID o por el

encargado de monitorear de cámaras, con el fin de obligar al automóvil a detenerse en caso halla una sospecha sobre el mismo.

Debido a que solo tendrán acceso al parqueo las personas debidamente identificadas por UNAPEC sin excepción, se aprovechará mejor el espacio existente en esa área. Con esto, a la vez se logra destinar los parqueos exclusivamente a los tienen derecho al mismo.

Ya que se cuenta con la información de que cantidad de parqueos disponibles en tiempo real en la página de la UNAPEC, además de un servicio de mensajería a celulares para el mismo fin, se provee un medio para que los usuarios puedan conocer antes de tiempo la disponibilidad de los estacionamientos antes de tiempo las personas tendrán la oportunidad de evaluar las posibilidades que tienen de ingresar al estacionamiento y de no ser así, ubicar de antemano buscar espacio en otro lugar.

Esto trae ciertos beneficios no cuantificables a los usuarios del parqueo y a la universidad misma como es el ahorro de combustible, la reducción de emisión de gases contaminantes en zonas cercanas al parqueo y sobre todo la reducción de las largas colas que se crean en la calle que da acceso a la entrada y salida del parqueo.

No obstante estas ventajas, es necesario hacer notar algunas desventajas que surgen con la automatización del parqueo de la Universidad APEC, como el hecho de que requiere inversión inicial considerable cuyos beneficios tardan algunos años en ser vistos, además de que no resuelve el problema de la falta de espacio en los estacionamientos, sino que propone una forma alternativa de administrar el espacio disponible.

8.1 Análisis Económico.

La inversión inicial requerida para el sistema propuesto asciende a RD$ 478,481.00, detallados en la siguiente tabla.

Inversión Inicial del Proyecto		
Item	Precio Unitario (RD$)	Precio Total
Cámara de seguridad D-Link 3320	$11,419.00	$137,028.00
D-Link DES-1316 Net Switch	$11,520.00	$11,520.00
Protector de Cámara DCS-45	$2,880.00	$34,560.00
Modem GSM Dualband	$7,977.00	$7,977.00
Lector RFID DL910	$30,600.00	$122,400.00
Etiqueta RFID MR6780	$20.00	$50,000.00
UPS Tripp Lite SU750XL	$16,524.00	$16,524.00
Middleware de RFID.	$130,000.00	$130,000.00
Computador Servidor Principal	$27,000.00	$27,000.00
Computador Red Externa	$18,500.00	$18,500.00
Mano de obra para implementación	$60,000.00	$60,000.00
Total	$305,021.00	$478,481.00

Tomando en cuenta que el servicio de conexión a Internet del sistema, así como el hecho de que la mayor parte de los equipos requieren poco mantenimiento, los gastos estimados del estacionamiento con la implementación del antes mencionado sistema ascienden a RD$851,753.28, detallados en la siguiente tabla:

Gastos Proyecto		
Item	Gastos Mensuales	Gastos Anuales
Paquete SMS	$4,260.00	$42,600.00
Nómina	$60,000.00	$780,000.00
Consumo eléctrico	$1,229.44	$14,753.28
Mantenimiento	$1,200.00	$14,400.00
Total	$2,429.44	$851,753.28

La estimación de los gastos vigentes en que incurre la institución con la zona destinada a parqueos sin la existencia del sistema propuesto es de RD$ 990,984.00, con lo que se evidencia que la implementación de dicho sistema puede llegar a reducir los gastos de estacionamiento en un RD$ 139,230.72 anual que corresponde a un 14.05% de los gastos en que se incurren en la actualidad.

Gastos UNAPEC Parqueo Principal		
Item	Gasto Mensual	Gasto Anual
Consumo de Electricidad	$532.00	$6,384.00
Mantenimiento	$800.00	$9,600.00
Nómina	$75,000.00	$975,000.00
Total	$76,332.00	$990,984.00

Este ahorro se debe en su mayor parte a la reducción de personal necesario para trabajar en el estacionamiento, ya que el sistema solo requiere de tres operadores: dos operadores en las entradas y salidas del estacionamiento y un encargado de monitoreo y supervisión a través de la red de cámaras.

Se podría hacer una proyección económica para los siguientes 10 años luego de iniciado el proyecto y se obtendría un Valor Actual Neto de $546,227.78, asumiendo una tasa de interés de un 22%. Esto significa que en 10 años los ahorros obtenidos por la implementación de este sistema será suficiente para duplicar la inversión realizada.

Proyección económica						
Períodos (años)	0	1	2	...	9	10
Ingresos (estimados)		139,230.72	139,230.72	139,230.72	139,230.72	139,230.72
Inversión Inicial	-$478,481.00					
TIR	26%					
VAN	$546,227.78					

Otro factor a tomar en cuenta es la Tasa Interna de Retorno de la inversión realizada, la cual se estima es de un 26%, como se puede observar en la tabla anterior. Este dato en conjunto con el resultado del Valor Actual Neto, demuestran que la inversión en este proyecto es rentable a largo plazo, pues genera recursos de índole económica al reducir los posibles gastos durante ese período.

10. RECOMENDACIONES.

A continuación se mencionan algunas recomendaciones sobre aspectos generales relacionados con el parqueo de la Universidad APEC, con el fin de proponer una forma de lograr un mejor aprovechamiento del mismo:

Control de Acceso.

Es necesario que la universidad implemente nuevas políticas para el uso del estacionamiento, limitando su uso a estudiantes, profesores y empleados durante aquellas horas del día donde la mayoría de los usuarios tienen la tendencia a entrar al recinto.

Gestión del espacio disponible.

En vista de la situación existente en la Universidad APEC, en cuanto a la escasez de lugares para parqueo dentro del recinto, la solución más lógica a simple vista es la adquisición de espacios cercanos a la Universidad y destinarlos a este fin. Sin embargo, esto no asegura que se resuelva el problema de forma definitiva a largo plazo. Por eso es vital que la universidad implemente un método de gestión de estos espacios que le permita aprovecharlos al máximo.

El sistema de automatización por RFID no es una solución definitiva para el problema de la falta de espacio para parqueo dentro del recinto. Sin embargo es una alternativa a largo plazo para la administración del área de parqueo del que si se dispone. Esto se debe al largo tiempo de vida de la mayoría de los equipos que se usan en dicho sistema y a la posibilidad de expandirlo en caso de que se amplíe el área de parqueo de la institución.

Seguridad.

A causa de la situación social presente en la República Dominicana, es necesario diseñar y utilizar un sistema de seguridad que brinde protección y confianza a los usuarios de la universidad, ya sea mediante redes de cámaras, supervisión humana u otro método. La Universidad APEC cuenta con sistemas de CCTV en ciertas áreas con el mismo fin, sin embargo, esto no es notable en el área de parqueos, lo cual debe ser tomado en cuenta.

11. CONCLUSIONES.

En la Universidad APEC con la implementación del Sistema Automatización mediante RFID, se reduce el acceso de vehículos no autorizados al estacionamiento de UNAPEC, esto se logra gracias los tags de RFID que identifican a cada vehículo como único, lo cual significa que los usuarios tienen acceso luego que el sistema procese la información almacenada en el tag, y proceda a subir la barrera que impide el paso.

La cantidad de vehículos dentro del recinto es un dato que se puede conocer con exactitud debido al conteo que lleva el sistema RFID, con esto se tiene siempre a disposición la cantidad disponibles de parqueos.

Para proporcionar a los usuarios del parqueo la información de disponibilidad existente en el área de parqueo, el sistema RFID posee conexiones con el servidor de UNAPEC el cual, a través de un web service que trabaja en conjunto con una aplicación de consola situada en el computador principal del sistema, la cual envía la información al web service y este la almacena en un archivo XML, la aplicación es cliente del servicio web. Con esto se logra la colocación de esta información en la página web de UNAPEC a

través de una aplicación web, así los usuarios tienen acceso a la información en tiempo real en cualquier momento.

También se utiliza una conexión a la red GSM con lo cual se envía, por medio de un servicio de mensajería corta, la información perteneciente al parqueo a las personas activen este servicio.

La seguridad es un factor importante y es necesario tomarla en cuenta como tal, por esto, se provee un una red de cámaras de vigilancias mediante IP, con esto el estacionamiento es monitoreado todo el tiempo. Además se utiliza un desgarrador de llantas que se activará cuando ocurra algún incidente que lo amerite. Con estos avances la seguridad incrementa significativamente en el área de parqueo.

Al unir todos subsistemas se logra una estructura sólida de gestión de parqueos mediante RFID para identificación y control de acceso, al mismo tiempo que se mantienen informados a los usuarios de la disponibilidad y aumenta la seguridad del estacionamiento.

12. LÍNEAS DE INVESTIGACIÓN.

Las líneas de investigación que surgen del proyecto propuesto son:

- La obtención de la posición real de vehículos u otros objetos dentro de un espacio determinado, utilizando la tecnología de RFID y la triangulación de antenas direccionales.

- Rastreo de productos y mercancía utilizando tecnología RFID en conjunto con las redes GSM.

- La evolución de los sistemas de Identificación por Radio Frecuencia (RFID) en sistemas de Tecnología de la Información por Radio Frecuencia (RFIT).

13. BIBLIOGRAFÍA

1. Entrevista al Ing. Francisco Sánchez Ledesma, Ingeniero el Electrónica y Comunicaciones. Realizada el 25 de Julio del 2009.

2. Cook, G. (n.d). Parking Lot Security. Consultada el 12 de Julio del 2009 en: http://www.crimewise.com/library/parking.html

3. Gimeno J. (2004). RFID, el código de barras del futuro (I Parte). La Flecha. Consultada en 13 de Julio del 2009 en: http://www.laflecha.net/articulos/ciencia/rfid/

4. Goleniew, L. (2006). *Telecommunications Essentials*. (Segunda Edición). Estados Unidos: Addison Wesley Professional.

5. Hunt, V, Puglia, A. y Puglia, M. (2007). *RFID: A guide to radio frequency identification.* Estados Unidos: John Wiley & Sons, Inc.

6. Lidman, T. (2008). *Parking Management: Strategies, Evaluation and Planning.* Canadá. Victoria Transport Policy Institute.

7. Brain, M. (n.d). How Modems work. Consultada el 18 Julio 2009 en: http://computer.howstuffworks.com/modem1.htm

8. Miles, S., Sarma, S. y Williams, J. (2008). *RFID Technology and Applications.* Estados Unidos : Cambridge University Press.

9. Moore, B (2009, Mayo). RFID is Dead… Long Live RFIT. *Association of Automatic Identification and Mobility.* Consultada el 08 de Julio del 2009. http://www.aimglobal.org/members/news/templates/template.aspx?articleid=3482&zoneid=43

10. Oberle, D. (2006). Semantic *Management of Middleware. Springer Science+Business Media, Inc*.

11. S. Fuentes (2008). *Análisis de la tecnología RFID: Ventajas y Limitaciones.* Consultado el 15 Julio de 2009.

12. Syed, A. y Mohammad I. (2006). *RFID Handbook*. Estados Unidos: CRC Press.

13. Thornton, F. (2006). *RFID Security.* Canadá. Syngress Publishing, Inc.

14. Closed Circuit Televisión Camera (2009). Consultada el 11 de Julio en: http://en.wikipedia.org/wiki/Closed-circuit_television_camera

15. Closed Circuit Television (2009). Consultada el 11 de Julio de 2009 en: http://en.wikipedia.org/wiki/Closed-circuit_television

16. Closed-Circuit Television (n.d). Obtenida el 20 Julio 2009, de http://en.wikipedia.org/wiki/Closed-circuit_television#Privacy

17. Componentes de un sistema de RFID básico (2009). Consultado el 13 de Julio del 2009 en: http://www.idautomatica.com/.../componentes-de-un-sistema-rfid-basico.php

18. Compresión Digital de Video (n.d). *Revisión de los métodos y estándares a usar para la transmisión y almacenamiento de video*. Consultada el 23 Julio 2009, de http://www.voxdata.com.ar/voxcompresionvideo.html

19. Digital Video Recorder (2009). Consultada el 11 de Julio del 2009 en: http://en.wikipedia.org/wiki/Digital_video_recorder

20. Digital Video Recorder (n.d) *Digital Video Recorder*. Obtenida el 15 Julio 2009, de http://en.wikipedia.org/wiki/Digital_Video_Recorders#Security_applications

21. DVR vs NVR – Digital Video Recording for Enterprise Systems (n.d). Consultada el 20 Julio 2009, de http://www.indigovision.com/learnabout-dvrvsnvr.php

22. Instituto Dominicano de las Telecomunicaciones (n.d). *Uso del Espectro Radioeléctrico*. Consultado el 13 Julio 2009, de http://www.indotel.gob.do/documentos/reglamentos/

23. Introducción a los sistemas RFID (n.d.). *Servicios Informáticos Kifer S.I*. Consultada en 13 de Julio del 2009 en: http://www.kifer.es/Recursos/Pdf/RFID.pdf

24. IP Camera (2009). Consultada el 11 de Julio de 2009 en: http://en.wikipedia.org/wiki/IP_camera

25. ¿Qué es CCTV? (n.d.). *Sistemas y Servicios de Comunicación S.A. (SYSCOM*). Consultada en 11 Julio 2009 en: http://www.syscomcctv.com.mx/que_es_cctv.htm

26. Servicio de Mensajes Cortos (2009). Consultada el 11 de Julio del 2009 en: http://es.wikipedia.org/wiki/Servicio_de_mensajes_cortos

27. Short Message Service / SMS Tutorial (n.d.*). Developer's Home*. Consultada el 11 de Julio del 2009 en: http://www.developershome.com/sms/

28. La identificación por radiofrecuencia (RFID) en Europa: pasos hacia un marco político (2009). *Síntesis de la legislación de la UE*. Consultada el 13 de Julio del 2009 en: http://europa.eu/legislation_summaries/index_es.htm

29. La identificación por Radiofrecuencia en Europa (2008). *Pasos hacia un Marco Político*. Consultado el 12 Julio 2009, de http://europa.eu/legislation_summaries/information_society/l24120a_es.htm

30. Middleware (n.d) *Middleware [version electrónica]*. Consultada el 15 Julio 2009 en http://www.rfid-magazine.com/recursos/imprimible.php?id=1164

31. Middleware RFID (n.d). Consultada el 17 Julio 2009, de http://es.wikipedia.org/wiki/Middleware_RFID

32. Middleware (n.d). Consultada el 18 Julio 2009, de http://es.wikipedia.org/wiki/Middleware

33. ¿Qué es CCTV? (2008). *Circuito Cerrado de Televisión [versión electrónica]*. Consultada el 16 Julio 2009, de http://www.syscomcctv.com.mx/que_es_cctv.htm

34. RFID, el código de barras del futuro (n.d). Consultado el 17 Julio 2009, de http://www.laflecha.net/articulos/ciencia/rfid

35. Sistemas de Parqueo (n.d). Consultada el 15 Julio 2009, de http://autogard.czechtrade.es/sistemas-de-parqueo

36. UHF Long Range Reader (n.d). Consultada el 17 Julio 2009, de http://www.rfid-in-china.com/2008-11-05/products_detail_2158.html

37. UHF 902 MHz. RFID Antenna (n.d). Consultada el 18 Julio 2009, de http://www.gaorfid.com/index.php?main_page=product_info&products_id=556

14. ANEXOS