5/11/2018

Julio Alejandro Tejada Nava

ITIW31

Tareas 3.5, 3.6 y 3.7

# Sistemas de tierras basados en la norma ANSI/EIA/TIA-607

Universidad Tecnológica de Ciudad Juárez

Tecnologías de la Información y la Comunicación

Materia: Aplicación de las telecomunicaciones

ApApl

En abril de 2012 ha sido publicado el estándar TIA-607-B, el que fue actualizado en Enero de 2013 como TIA-607-B-1. Esta recomendación está basada en la ANSI/J-STD--607-A-2002 (publicada en octubre de 2002). El propósito de este documento es brindar los criterios de diseño e instalación de las tierras y el sistema de aterramiento para edificios comerciales, con o sin conocimiento previo acerca de los sistemas de telecomunicaciones que serán instalados. Este estándar incluye también recomendaciones acerca de las tierras y los sistemas de

aterramientos para las torres y las antenas. Asimismo, el estándar prevé edificios

compartidos por varias empresas, y ambientes con diversidad de productos de

telecomunicaciones.

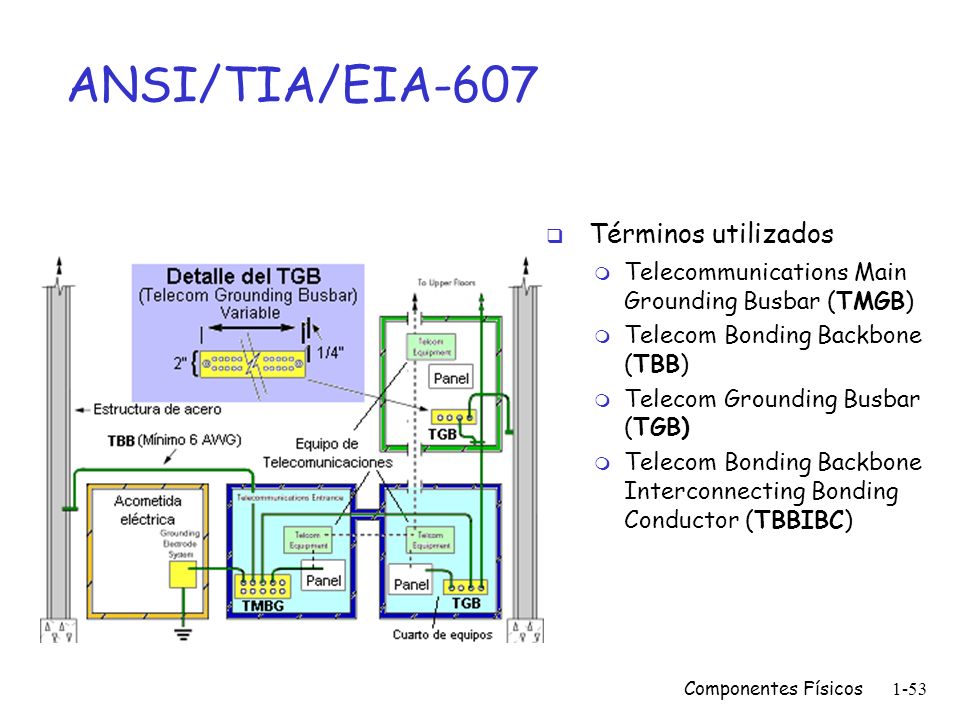
El estándar original ANSI/TIA/EIA-607 fue publicado en Agosto de 1994, y fue

actualizado por las nuevas recomendaciones, incluyendo criterios de

aterramientos para torres y antenas, tablas para el cálculo del diámetro de

conductores y barras de aterramiento, etc.

# Diagrama de un cableado estructurado de tierras, basado en la 607



TMGB (Barra principal de tierra para telecomunicaciones)

Los aterramientos para los sistemas de telecomunicaciones parten del aterramiento principal del edificio (aterramiento eléctrico, jabalinas, etc). Desde este punto, se debe tender un conductor de tierra para telecomunicaciones hasta la “Barra principal de tierra para telecomunicaciones” (TMGB = “Telecomunications Main Grounding Busbar”).

Este conductor de tierra debe estar forrado, preferentemente de color verde, y debe tener una sección mínima de 6 AWG (16 mm2 AWG – mm – mm2 ). Asimismo, debe estar correctamente identificado mediante etiquetas adecuadas.

Es recomendable que el conductor de tierra de telecomunicaciones no sea ubicado dentro de canalizaciones metálicas. En caso de tener que alojarse dentro de canalizaciones metálicas, éstas deben estar eléctricamente conectadas al conductor de tierra en ambos extremos.

La TMGB (“Telecomunications Main Grounding Busbar”) es el punto central de tierra para los sistemas de telecomunicaciones. Se ubica en las “Instalaciones de Entrada”, o en la “Sala de Equipos”. Típicamente hay una única TMGB por edificio, y debe ser ubicada de manera de minimizar la distancia del conductor de tierra hasta el punto de aterramiento principal del edificio.

# Características físicas, funcionamiento y formas de conexión de los siguientes equipos, usados en los centros de datos

## UPS, (con sus cargadores y bancos de baterías)

Sistema de alimentación ininterrumpida (ISAI), en inglés uninterruptible power supply (UPS), es un dispositivo que gracias a sus baterías u otros elementos almacenadores de energía, durante un apagón eléctrico puede proporcionar energía eléctrica por un tiempo limitado a todos los dispositivos que tenga conectados. Otra función que se puede añadir a estos equipos es mejorar la calidad de la energía eléctrica que llega a las cargas, filtrando subidas y bajadas de tensión y eliminando armónicos de la red en caso de usar corriente alterna.

Los UPS (ISAI) proporcionan energía eléctrica a equipos llamados cargas críticas, como aparatos médicos, industriales o informáticos que requieren alimentación permanente y de calidad, para estar siempre operativos y sin fallos (picos o caídas de tensión).

Las cargas conectadas a los UPS requieren una alimentación de corriente continua. Por tanto, éstos transformarán la corriente alterna de la red comercial a corriente continua, y la usarán para alimentar la carga y almacenarla en sus baterías. Por eso, no necesitan convertidores entre las baterías y las cargas.

Tipos de UPS:

UPS offline. Corrige los siguientes fallos eléctricos

1. Fallos de alimentación
2. Caídas de tensión.
3. Picos de corriente, sobretensiones y subtensiones.

UPS Line Interactive. Corrige:

1. Fallos de alimentación
2. Caídas de tensión.
3. Picos de corriente, sobretensiones y subtensiones.
4. Infratensiones prolongadas.
5. Sobretensiones prolongadas.

UPS online. Este tipo de UPS es el más seguro y el que más fallos eléctricos corrige.

1. Fallos de alimentación
2. Caídas de tensión.
3. Picos de corriente, sobretensiones y subtensiones.
4. Infra tensiones prolongadas.
5. Sobretensiones prolongadas.
6. Distorsiones en la onda de la línea.
7. Variaciones en las frecuencias.
8. Micro cortes.
9. Distorsión armónica.

## Tableros de Panel

Denominado bahía de rutas, es el elemento encargado de recibir todos los cables del cableado estructurado. También se puede definir como paneles donde se ubican los puertos de una red o extremos (analógicos o digitales) de una red, normalmente localizados en un bastidor o rack de telecomunicaciones. Todas las líneas de entrada y salida de los equipos (computadoras, servidores, impresoras, entre otros) tendrán su conexión a uno de estos paneles.

Sirve como organizador de las conexiones de la red, para que los elementos relacionados de la red de área local (LAN) y los equipos de conectividad puedan ser fácilmente incorporados al sistema, y además los puertos de conexión de los equipos activos de la red (switch, router, etcétera) no tengan daños por el constante trabajo de retirar e introducir los conectores en sus puertos.

Son paneles electrónicos utilizados en algún punto de una red informática o sistema de comunicaciones (analógico o digital) en donde terminan todos los cables de red.

## Interruptor termo magnético

Es un dispositivo capaz de interrumpir la corriente eléctrica de un circuito cuando ésta sobrepasa ciertos valores máximos. Su funcionamiento se basa en dos de los efectos producidos por la circulación de corriente en un circuito: el magnético y el térmico (efecto Joule). El dispositivo consta, por tanto, de dos partes, un electroimán y una lámina bimetálica, conectadas en serie y por las que circula la corriente que va hacia la carga.

No se debe confundir con un interruptor diferencial. Al igual que los fusibles, los interruptores magnetotérmicos protegen la instalación contra sobrecargas y cortocircuitos.

Al circular la corriente por el electroimán, crea una fuerza que, mediante un dispositivo mecánico adecuado (M), tiende a abrir el contacto C, pero sólo podrá abrirlo si la intensidad I que circula por la carga sobrepasa el límite de intervención fijado. Este nivel de intervención suele estar comprendido entre tres y veinte veces (según la letra B, C, D, etc.) la intensidad nominal (la intensidad de diseño del interruptor magnetotérmico) y su actuación es de aproximadamente unas 25 milésimas de segundo, lo cual lo hace muy seguro por su velocidad de reacción. Esta es la parte destinada a la protección frente a los cortocircuitos, donde se produce un aumento muy rápido y elevado de corriente.

La otra parte está constituida por una lámina bimetálica (representada en rojo) que, al calentarse por encima de un determinado límite, sufre una deformación y pasa a la posición señalada en línea de trazos lo que, mediante el correspondiente dispositivo mecánico (M), provoca la apertura del contacto C. Esta parte es la encargada de proteger de corrientes que, aunque son superiores a las permitidas por la instalación, no llegan al nivel de intervención del dispositivo magnético. Esta situación es típica de una sobrecarga, donde el consumo va aumentando conforme se van conectando aparatos.

Ambos dispositivos se complementan en su acción de protección, el magnético para los cortocircuitos y el térmico para las sobrecargas. Además de esta desconexión automática, el aparato está provisto de una palanca que permite la desconexión manual de la corriente y el rearme del dispositivo automático cuando se ha producido una desconexión. No obstante, este rearme no es posible si persisten las condiciones de sobrecarga o cortocircuito.

## Sistemas de alarma

Un sistema de alarma es un elemento de seguridad pasiva. Esto significa que no evitan una situación anormal, pero sí son capaces de advertir de ella, cumpliendo así, una función disuasoria frente a posibles problemas.

Una vez que la alarma comienza a funcionar, o se activa dependiendo del sistema instalado, esta puede tomar puede mandar un mensaje telefónico a uno o varios números. El uso de la telefonía para enviar mensajes, de señales o eventos se utilizó desde hace 60 años, pero desde el año 2005 con la digitalización de las redes de telefonía, la comunicación deja de ser segura, actualmente la telefonía es solo un vínculo más y se deben enviar mensajes mediante GPRS a direcciones IP de servidores que ofician de receptores de las señales o eventos, también se utiliza la conectividad propia de las redes IP. Si se detecta la presencia de humo, calor o ambos, mandar un mensaje al "servicio de monitoreo" o accionar la apertura de rociadores en el techo, para que apaguen el fuego. Si se detecta la presencia de agentes tóxicos en un área, cerrar las puertas para que no se expanda el problema.

Para esto, la alarma tiene que tener conexiones de entrada, para los distintos tipos de detectores, y conexiones de salida, para activar otros dispositivos que son los que se ocupan de hacer sonar la sirena, abrir los rociadores o cerrar las puertas.

Todos los sistemas de alarmas traen conexiones de entrada para los detectores y por lo menos una de salida para la sirena. Si no hay más conexiones de salida, la operación de comunicar a un servicio de monitoreo, abrir el rociador o cerrar las puertas deberá ser realizada en forma manual por un operador.

Uno de los usos más difundidos de un sistema de alarma es advertir el allanamiento en una vivienda o inmueble. Los equipos de alarma pueden estar conectados con una Central Receptora, también llamada Central de Monitoreo, con el propietario mismo (a través de teléfono o TCP/IP) o bien simplemente cumplir la función disuasoria, activando una sirena localmente (la potencia de la sirena estará regulada por las distintas leyes de seguridad del Estado o región correspondiente).

## Plantas Generadoras de Energía de Respaldo

Una planta generadora es un grupo motor – generador, esto quiere decir que cuenta con un motor de combustión (generalmente que utiliza diésel como combustible), que este acoplado mecánicamente a un generador eléctrico. Dicho motor transmite energía mecánica al generador, el cual produce energía eléctrica por el principio de inducción magnética.

* Plantas eléctricas industriales

Funcionan con la quema de combustibles, generalmente diesel, de la misma forma que lo hace un motor de cualquier vehículo que utilice este tipo de combustible. Pueden ser utilizadas en trabajo continuo o emergencia.

Las plantas industriales son de distintas capacidades en diferentes voltajes y frecuencias. Incluyen un contador de horas de uso. Es posible adaptarles remolques para su transportación y casetas o contenedores acústicos para la disminución del ruido que por su naturaleza producen.

* Planta eléctrica portátil

La planta portátil funciona a gasolina. Incluye un contador de horas de uso y se le puede adaptar ruedas para moverla. Son recomendables para hogares pequeños que tengan pocos aparatos eléctricos.

* Planta eléctrica solar

Es la interconexión de diversos dispositivos que transforman la energía solar en electricidad, también llamados sistemas fotovoltaicos. La planta eléctrica solar permite cubrir la necesidad de electrificación en regiones montañosas, aisladas o de difícil acceso, requieren de un inversor de voltaje y frecuencia, y necesitan un banco de baterías para tener una buena autonomía.

## Sistemas de extinción

Dentro de la gama de extinción, podemos encontrar dos grandes ramas específicamente orientadas a determinados casos: Los sistemas de extinción automática y los sistemas de extinción manual, con el apoyo de hidrantes y columna seca. En grandes instalaciones está indicado el uso de ambas ramas de forma complementaria.

Sistemas de extinción manual:

* Extintores (Hídricos, de polvo seco, por espuma, por gases, ...)
* BIES - Bocas de Incendio Equipadas (abatibles, fijas, especiales,...)

Sistemas de extinción automática:

* Por agua (rociadores de agua nebulizada, pulverizada, ...)
* Por espuma (de baja, media o alta presión)
* Por gases (CO2, gases inertes, gases fluorados,...)
* Por aerosoles (partículas ultra finas de potasio)
* Grupos de presión
* Sistemas de inertización

Los 3 principales objetivos de los sistemas de extinción

1. Salvar vidas: Este es el objetivo que se puede considerar como principal al momento de diseñar, adquirir e instalar los equipos requeridos para el sistema de detección y extinción de incendios.
2. Proteger los activos: Sin duda alguna, un sistema de extinción adecuado ayuda a minimizar las pérdidas económicas en caso de un incendio.
3. Reinicio de las actividades: Si se tuvo una respuesta oportuna en la extinción de un incendio, se podrá comenzar a producir nuevamente en un menor periodo de tiempo.

## Control de acceso

Un sistema de control de acceso es un sistema electrónico que restringe o permite el acceso de un usuario a un área específica validando la identificación por medio de diferentes tipos de lectura (clave por teclado, tags de próximidad o biometría) y a su vez controlando el recurso (puerta, torniquete o talanquera) por medio de un dispositivo eléctrico como un electroimán, cantonera, pestillo o motor.

Tipos de Control de Acceso

Básicamente los controles de acceso se clasifican en dos tipos:

* Sistemas de Control de Acceso Autónomos
* Sistemas de Control de Acceso en Red

Los Sistemas de Control de Acceso Autónomos son sistemas que permiten controlar una o más puertas, sin estar conectados a un PC o un sistema central, por lo tanto, no guardan registro de eventos. Aunque esta es la principal limitante, algunos controles de acceso autónomos tampoco pueden limitar el acceso por horarios o por grupos de puertas, esto depende de la robustez de la marca. Es decir, los más sencillos solo usan el método de identificación (ya sea clave, proximidad o biometría) como una "llave" electrónica.

Los Sistemas de Control de Acceso en Red son sistemas que se integran a traves de un PC local o remoto, donde se hace uso de un software de control que permite llevar un registro de todas las operaciones realizadas sobre el sistema con fecha, horario, autorización, etc. Van desde aplicaciones sencillas hasta sistemas muy complejos y sofisticados según se requiera.

El control de acceso generalmente incluye tres componentes:

1. Un mecanismo de autenticación de la entidad (por ejemplo, contraseña, una mapa, una clave, una biométrica, ...). Este mecanismo no es útil en sí mismo, pero es esencial para el funcionamiento de los dos siguientes:2​
2. Un mecanismo de autorización (la entidad puede ser autenticada, pero no tiene el derecho a acceder a este recurso en un momento dado).
3. Un mecanismo de trazabilidad: a veces el mecanismo de autorización puede ser insuficiente para garantizar que la entidad tiene el derecho de acceso a ese recurso (respecto a un procedimiento, a las horas trabajadas, ...), la trazabilidad compensa esta carencia mediante la introducción de una espada de Damocles responsabilizando a las entidades. También sirve si se desea identificar a posteriori al responsable de una acción.

## Sistemas de detección

Un sistema de detección es un dispositivo o aplicación de software que monitorea una red o sistemas para detectar actividades maliciosas o infracciones de políticas. Cualquier actividad maliciosa o violación generalmente se reporta a un administrador o se recopila de forma centralizada mediante un sistema de gestión de eventos e información de seguridad (SIEM). Un sistema SIEM combina salidas de múltiples fuentes y utiliza técnicas de filtrado de alarmas para distinguir la actividad maliciosa de las falsas alarmas.

Los tipos de IDS varían en alcance desde computadoras individuales hasta redes grandes. [1] Las clasificaciones más comunes son los sistemas de detección de intrusos en la red (NIDS) y los sistemas de detección de intrusos basados ​​en host (HIDS). Un sistema que controla los archivos importantes del sistema operativo es un ejemplo de un HIDS, mientras que un sistema que analiza el tráfico de la red entrante es un ejemplo de un NIDS. También es posible clasificar IDS por enfoque de detección: las variantes más conocidas son la detección basada en firmas (reconociendo patrones incorrectos, como malware); y detección basada en anomalías (detección de desviaciones de un modelo de tráfico "bueno", que a menudo se basa en el aprendizaje automático). Algunos productos IDS tienen la capacidad de responder a las intrusiones detectadas. Los sistemas con capacidades de respuesta suelen denominarse sistemas de prevención de intrusiones.

## Sistemas de climatización

Se denomina sistema de climatización a aquel que es capaz de controlar la calidad del aire interior para que permanezca dentro de unos valores de confort razonables de los siguientes parámetros:

* Temperatura
* Humedad
* Calidad del aire interior

Se introduce en los locales, para conseguir junto con los elementos terminales o equipos, las condiciones adecuadas para el ambiente a climatizar:

* Sistemas todo aire.
* Sistemas toda agua.
* Sistemas aire-agua.
* Sistemas de refrigerante.

Subsistemas:

* Centrales de tratamiento
* Elementos terminales
* Elementos intermedios
* Equipamiento de control y seguridad

En consecuencia, este sistema debe ser capaz de actuar sobre el aire interior para enfriarlo y calentarlo, filtrarlo y renovarlo introduciendo en el local interior aire procedente del exterior.

Los componentes de un sistema de climatización son: a) el Lazo primario, encargado de producir calor y/o frío para ser suministrado a los sistemas terminales del sistema de climatización. También se incluyen dentro del lazo primario los sistemas de distribución y acumulación de energía. b) Lazo secundario, donde se realiza el aprovechamiento del fluido caloportador para calentar o refrigerar el aire.