UF1864: Pruebas y verificación de los dispositivos de transporte y transmisión y de los servicios de conectividad asociados

Elaborado por: Francisco Castro Báez

Edición: 5.1

EDITORIAL ELEARNING

ISBN: 978-84-16492-74-9

Impreso en España - Printed in Spain

Presentación

Identificación de la Unidad Formativa:

Bienvenidos a la Unidad Formativa UF1864: Pruebas y verificación de los dispositivos de transporte y transmisión y de los servicios de conectividad asociados. Esta unidad formativa pertenece al Módulo Formativo MF0960_2: Implementación de equipos de acceso a redes de comunicaciones, que forma parte del certificado de profesionalidad IFCM0110: Operación en sistemas de comunicaciones de voz y datos, de la familia profesional de Informática y comunicaciones.

Presentación de los contenidos:

La finalidad de esta unidad formativa es enseñar al alumno a realizar los procedimientos de verificación de los dispositivos de transporte y transmisión de datos, para asegurar la continuidad en la prestación de los servicios de comunicaciones según procedimientos establecidos.

Para ello, se analizarán las pruebas de instalación de equipos de transmisión.

Objetivos del módulo o unidad formativa:

Al finalizar este módulo formativo aprenderás a:

– Aplicar procedimientos de prueba de dispositivos de transporte y transmisión de datos, utilizando técnicas y herramientas específicas.

UF1864: Pruebas y verificación de los dispositivos de transporte y transmisión y de los servicios de conectividad asociados

Índice

UD1

Pruebas de instalación de equipos de transmisión

1.1. Procedimientos de prueba de seguridad mecánica
  1.1.1. Pruebas de estabilidad y nivelación
  1.1.2. Pruebas de nivel de refrigeración/disipación
  1.1.3. Resistencia a vibraciones
1.2. Procedimientos de prueba de cableado, alimentación, seguridad eléctrica y EMC (compatibilidad electromagnética)
  1.2.1. Verificación de continuidad y distribución eléctrica
  1.2.2. Verificación de estado de seguridad eléctrica. Tierras
  1.2.3. Compatibilidad electromagnética (normativa IEC y normas de producto)
1.3. Procedimientos de pruebas de señales de sincronismo
  1.3.1. Verificación de la generación/recepción de señales de sincronismo
  1.3.2. Verificación de continuidad y distribución de la señal de sincronismo
1.4. Pruebas funcionales de unidad y sistema
  1.4.1. Pruebas funcionales de alimentación interna y externa. Nivel de unidad funcional y global
  1.4.2. Pruebas de sincronismo y distribución de señal de reloj. Nivel de unidad funcional y global
  1.4.3. Pruebas de conectividad interna (unidad funcional) y externa (nivel sistema) y operatividad

1.1. Procedimientos de prueba de seguridad mecánica

¿Qué es seguridad?

Podemos entender como seguridad, una característica de cualquier sistema (informático o no) que nos asegura que está libre de todo peligro, que dicho sistema no corre riesgo alguno, es en cierta manera infalible.

En el caso de sistemas operativos o redes de ordenadores, esta característica es muy difícil de conseguir por no decir que es imposible, podemos suavizar la definición de seguridad y podemos hablar de **fiabilidad** más que de seguridad; por tanto, se habla de sistemas fiables en lugar de hacerlo de sistemas seguros.

Fiabilidad es la probabilidad de que un sistema se comporte tal y como se espera de él.

A grandes rasgos se entiende que mantener un sistema seguro (o fiable) consiste básicamente en garantizar tres aspectos:

– Integridad.

  La integridad permite que los objetos del sistema sólo se puedan modificar por elementos autorizados por la organización, y de una manera controlada.

– Disponibilidad.

  La disponibilidad indica que los objetos de un sistema tienen que ser accesibles a elementos autorizados por la empresa; es decir, lo contrario a la negación de servicio.

– Confidencialidad.

  La confidencialidad indica que solamente los elementos autorizados por la empresa u organización pueden acceder a los objetos de un sistema. El uso de la información a la que se accede está sujeta a las normas establecidas por la empresa.

Generalmente tienen que cumplirse los tres requisitos antes descritos para que haya seguridad en un sistema. Por ejemplo,: se puede conseguir confidencialidad para un fichero determinado impidiendo que todos los usuarios (incluido el root) puedan leerlo, pero este mecanismo no proporciona disponibilidad alguna.

Dependiendo del entorno en que el sistema trabaje, interesará dar prioridad a un aspecto o a otro de la seguridad.

Ejemplo

En un sistema militar se antepondrá la confidencialidad de los datos almacenados o transmitidos a su disponibilidad: es decir, es preferible que alguien borre información confidencial (que se recuperará después desde cualquier sistema de backup) a que ese mismo elemento ajeno pueda leerla. Incluso se sacrificará la disponibilidad de esa información para los usuarios autorizados.

En cambio, en un servidor NFS de un departamento se premiará la disponibilidad frente a la confidencialidad: No importa que un extraño lea una unidad, pero si no tienen acceso los usuarios autorizados se producirán pérdidas de tiempo y dinero importantes.

En un entorno bancario, la prioridad de los responsables del sistema es mantener la integridad de los datos, frente a su disponibilidad o su confidenciali-

dad: Se impedirá que un usuario pueda modificar el saldo de otro, ahora bien, no es tan grave que lo pueda leer.

Para garantizar la seguridad física de los sistemas informáticos es necesario aplicar barreras físicas y procedimientos de control para prevenir cualquier amenaza o posible ataque bien a los recursos o bien a la confidencialidad de la información.

Definición

Entendemos por Seguridad Física todos aquellos procedimientos - generalmente de prevención y detección - destinados a la protección física de todos y cada uno de los recursos del sistema. Aquí podemos contemplar un teclado, un ratón, incluso la CPU de la máquina.

Seguridad Informática.

Los procedimientos de protección física del sistema están destinados a: acceso a personas, consecuencias de un incendio, agua, terremoto, etc.

Desafortunadamente, la seguridad física es un aspecto olvidado, con mucha frecuencia, a la hora de hablar de seguridad informática; en muchas organizaciones se toman medidas para prevenir o detectar accesos no autorizados al sistema, pero rara vez se tiene en cuenta que pueden ocurrir ataques físicos tanto al espacio donde están localizados dichos sistemas como al sistema en sí, es decir a cada uno de sus componentes.

Hay que tener en cuenta que incluso el deterioro del más insignificante de los componentes puede ser fatal para el funcionamiento de toda una organización.

Seguridad Informática

Por todos estos motivos, en determinadas situaciones, el ataque a un sistema aprovechará las posibles vulnerabilidades físicas en lugar de las lógicas. Posiblemente sea más fácil robar una cinta, cualquier dispositivo de almacenamiento, con una copia completa del sistema, que intentar acceder a él mediante fallos en el software mucho más tedioso de localizar.

Protección del hardware

El hardware es normalmente el elemento más caro de todo sistema informático. Por lo tanto, las medidas dedicadas a asegurar su integridad son la una parte más importante de la **seguridad física** de cualquier organización, especialmente en las dedicadas a I+D: universidades, centros de investigación, institutos tecnológicos...

Estos suelen poseer, entre sus equipos, máquinas muy caras, desde servidores con una gran potencia de cálculo hasta Routers de última tecnología, pasando por modernos sistemas de transmisión de datos como la fibra óptica.

La amenazas al hardware de una instalación informática pueden ser variadas; aquí se van a presentar algunas de ellas, sus posibles efectos y algunas soluciones, si no para evitar los problemas sí al menos para minimizar sus efectos.

La seguridad del hardware se refiere a la protección de objetos frente a intromisiones externas provocadas por el uso del hardware.

Seguridad del Hardware

A su vez, la seguridad del hardware puede dividirse en:

– Seguridad física.

Se dedicará a la protección de los equipos hardware frente a amenazas externas como manipulación o robo. Todo el equipamiento que almacene o trabaje con información sensible necesita ser protegido, de forma que resulte imposible a una persona ajena al sistema acceder físicamente a él. La solución más común es la ubicación del sistema en un entorno seguro, para lo que no se dudará en utilizar alarmas, cámaras, dispositivos de vigilancia, etc.

– Seguridad de difusión.

Consiste en la protección contra la emisión de señales del hardware. Un ejemplo sencillo son las pantallas de ordenador visibles a través de las ventanas de una oficina, por las que se puede obtener información muy sensible. O bien, las emisiones electromagnéticas de algunos elementos del hardware que una vez capturadas y tratadas adecuadamente pueden convertirse en información igualmente privilegiada.

La solución hay que buscarla en la adecuación de entornos seguros.

Además de los desastres naturales, incendios, siniestros, sabotajes, etc., hemos de tener en cuenta, los siguientes riesgos que pueden afectar a un sistema informático:

– Cableado

Los cables que se utilizan para construir las redes locales pueden ser cable telefónico normal, cable coaxial o bien fibra óptica. Hoy en día algunos edificios de oficinas ya se construyen con los cables instalados para evitar la pérdida de tiempo y el gasto posterior, así se minimiza el riesgo de un corte en el cable, de una rozadura u otro daño accidental.

Los riesgos más comunes que afectan al cableado son los siguientes:

– Interferencias

Estas modificaciones, o ruidos eléctricos, pueden estar generadas por cables de alimentación de maquinaria pesada o por equipos de radio o microondas. Los dispositivos emisores de ondas como los móviles pueden afectar al sistema.

Los datos que viajan a través de fibra óptica no se ven alterados por la acción de los campos eléctricos, problema que si sufren los cables metálicos.

– Corte del cable

La conexión establecida se rompe, con lo que el flujo de datos que circula a través del cable se ve interrumpido.

Este problema es muy frecuente en instalaciones antiguas.

– Daños en el cable

Los daños normales con el uso pueden afectar al apantallamiento, que preserva la integridad de los datos transmitidos. Cualquier problema hace que las comunicaciones dejen de ser fiables.

Cable dañado.

En la mayor parte de las organizaciones, estos problemas entran dentro de la categoría de daños naturales, de accidentes fortuitos. Sin embargo también se pueden considerar como un sabotaje, una forma de alterar la red, con el objetivo de interferir en su funcionamiento.

El cable de red también es un punto muy vulnerable para un ataque externo, para un intruso que intentase acceder a los datos, a la información que circula a través de ella.

Hay varias técnicas utilizadas para tal fin:

– Desviando o estableciendo una conexión no autorizada en la red.

Será necesario un sistema de administración adecuado y un procedimiento de identificación correcto para conseguir un acceso seguro, de forma que un agente externo no pueda conseguir privilegios de usuarios en la red, pero los datos que fluyen a través del cable pueden estar en peligro.

– Haciendo una escucha sin establecer conexión.

Los datos se pueden seguir y pueden verse comprometidos, peligrará su integridad. Por lo tanto, no hace falta penetrar en los cables físicamente para acceder a los datos que transportan.

– Cableado de Alto Nivel de Seguridad

Son cableados de redes que se recomiendan para instalaciones militares con alto grado de seguridad. El objetivo es impedir infiltraciones, accesos ilegales y monitorizaciones de información que circula por el cable.

Consta de un sistema de tubos (herméticamente cerrados) por cuyo interior circula aire a presión que rodea al cable. A lo largo de la tubería hay sensores conectados a un ordenador. Si se detecta alguna variación de presión a lo largo de este circuito se dispara un sistema de alarma.

– Picos y ruidos electromagnéticos

Las subidas (picos) y caídas de tensión no son el único problema eléctrico que sufrirán los usuarios. También está el problema añadido del ruido que afecta al funcionamiento de los componentes electrónicos.

El ruido interfiere en la transmisión de los datos, además de favorecer las escuchas electrónicas, aumentando así la fragilidad del sistema.

– Techos y suelos de Placas Extraíbles

Los cables de alimentación, comunicaciones, interconexión de equipos, receptáculos asociados con los ordenadores y equipos de procesamiento de datos pueden ser alojados en el espacio dispuesto para ello en los techos de placas extraíbles o bien debajo del propio suelo.

– Sistema de Aire Acondicionado

Es importante disponer de un sistema de calefacción, ventilación y aire acondicionado propio, dedicado exclusivamente al recinto donde se encuentran los ordenadores y equipos de proceso de datos.

Uno de los problemas más grandes que suele haber en los mainframes de los grandes servidores cloud es precisamente la refrigeración de la sala en la que se encuentran estos.

Teniendo en cuenta que los aparatos de aire acondicionado son causa potencial de incendios e inundaciones, se recomienda sistemas de protección y detección de fugas en todo el sistema de cañería al interior y al exterior, detectores y extintores de incendios, monitores y alarmas efectivas, etc.

Picos y ruidos electromagnéticos
Cableado
Cableado de alto nivel de seguridad
Techos y suelos de placas extraíbles
Sistema de aire acondicionado

Aspectos de seguridad a tener en cuenta

1.1.1. Pruebas de estabilidad y nivelación

En primer lugar estructurado, los niveladores.

Tipos de niveles

Plomada
Nivel de manguera
Nivel de burbuja de aire
Nivel láser
Teodolito

Tipos de niveladores

La plomada

Es el método más arcaico y menos preciso. Se usa principalmente en albañilería.

La plomada es el instrumento que se utiliza para tomar el nivel vertical, emplea la ley de la gravedad.

Se basa en un principio bastante sencillo, una cuerda suspendida con un peso al final, será perpendicular y vertical a cualquier plano de nivel que atraviese.

Esta herramienta consta de las siguientes partes:

– Una pesa de metal, preferiblemente hierro, plomo, bronce, u otro metal, de forma cilíndrica, cónica o una mezcla de ambas. Las plomadas equilibradas suelen terminar con un extremo en punta.

– Una pieza llamada nuez, parecida a un carrete que suele ser de madera, metal o incluso de metal imantado: tendrá el mismo espesor que la pesa y tiene un orificio en el centro.

– Una cuerda de algodón o nylon que atraviesa la nuez por el orificio y une ambas piezas.

– Las cuerdas de nylon soportan mejor la humedad por lo que se utilizan más en albañilería.

Plomada.

Ejemplo

Cuando se está levantando un muro, para que el plano de una hilada esté correcto colocamos la nuez en cualquiera de las piezas que constituyen el muro, ya sea bloque o ladrillo; el kilo debe quedar colgado a la distancia requerida (aproximadamente el espesor de una moneda) de la cara de la pieza correspondiente a la hilada de replanteo.

Si queda a mayor distancia, se diría que la pared está despierta, esto es, con desplome hacia afuera.

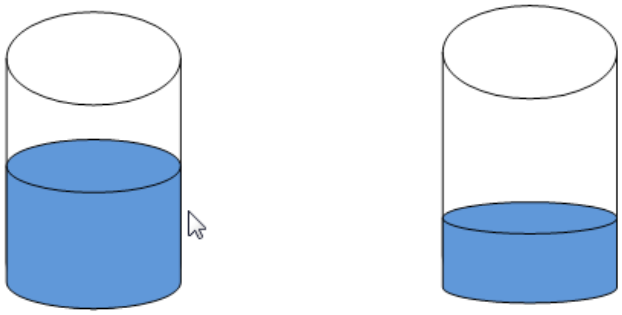
Si queda sin separación, entonces la pared estará dormida, esto es, con desplome hacia dentro.

Nivel de Manguera

Es también muy antiguo y poco preciso. Se usa principalmente en albañilería.

El nivel de manguera se basa en el principio la los vasos comunicantes, enunciado por Galileo Galilei.

"Si en un conjunto de vasos comunicantes se vierte un líquido homogéneo cualquiera, y se deja en reposo, se observa que, sin importar la forma o el volumen de los vasos, la superficie superior del líquido en todos ellos alcanza el mismo nivel."



Vasos no comunicados