UNIVERSIDAD PONTIFICIA BOLIVARIANA
Seccional Bucaramanga

TRABAJO DE GRADO PARA ESPECIALIZACION EN TELECOMUNICACIONES

Titulo:

PAUTAS PARA LA INSTAURACIÓN DE SISTEMAS DE COMUNICACIÓN EN SISTEMAS DE CONTROL CRÍTICO

Presentado por:

ING. FABIO JAIMES BELEÑO
ING. ERIKA RANGEL CASTILLO

Dirigido por:

ING. RAUL RESTREPO

Bucaramanga, Mayo de 2008

PAUTAS PARA LA INSTAURACIÓN DE SISTEMAS DE COMUNICACIÓN EN SISTEMAS DE CONTROL CRÍTICO

RESUMEN

La información es uno de los bienes de la empresa y como tal, tienen un valor, por esto debe ser protegida. La seguridad de la información, protege la “
“información” de una diversidad de amenazas, a fin de garantizar la continuidad de las operaciones (y por lo tanto de la producción), minimiza los daños en las corporaciones, maximiza el retorno de la capital invertido, mejorar la eficiencia y eficacia

En el presente articulo, intentaremos dar una visión acerca de las diferencias de los sistemas TI y los sistemas de control; basándonos en la importancia que tiente la seguridad y sus vulnerabilidades en cada uno de estos.

Mostraremos la incidencia que tiene la seguridad en los sistemas de control y su principal importancia, que radica en mantener la disponibilidad de todos los componentes del sistema. Presenta una serie de modelos que pueden ser utilizados en un adecuado diseño de programas de seguridad; además, presentaremos algunos Modelos de la norma ISA99, que tiene como objetivo, identificar las necesidades en materia de seguridad y las características importantes del medio, para hacer frente a las normas y requerimientos de seguridad; por ultimo , mostraremos algunos modelos propuestos para identificar las amenazas y vulnerabilidades, así mismo, adoptar contramedidas más adecuadas para la protección de sistemas de automatización y control y minimizar los riesgos de seguridad en empresas de Control.

Palabras claves:, firewall, switches, router, SCADA, DCS, PLC, VPN, OPC, DMZ, Normas.

RESUMEN

Information is one of the assets of the company and as such, have a value, why should be adequately protected. Information security protects "
"Information" from a variety of threats, to ensure continuity of operations (and therefore production), minimizes damage to corporations, maximizing the return on invested capital, improve efficiency and effectiveness

In this article, we will try to give a vision, about the differences of IT systems and control systems; based on the import tempted security and its vulneranblidades in each of these.

Show the impact of security control systems and its main importance lies in maintaining the availability of all components of the system. presents a series of models that can be used in designing an appropriate security programs, as well as present some models ISA99 standard, which aims to identify security needs and the important features of the environment to cope the rules and security requirements. And finally show some models proposed to identify threats and vulnerabilities, to adopt more appropriate countermeasures to protect automation systems and control and thus minimize the security risks in enterprises of Control.

Keywords: firewalls, switches, routers, SCADA, DCS, PLC, VPN, OPC, DMZ, Models

INDICE

INTRODUCCION:

Durante los últimos años, la seguridad de los sistemas y de la información se ha vuelto una actividad crítica, pero aun mas, en los sectores de la Industrial y de la infraestructura.

Los daños que pueden provocar accidentes en los sistemas de control, pueden ser más peligrosos y tienen peores consecuencias para la gente y para la infraestructura, de lo que imaginamos; por ejemplo: un accidente en una planta de energía nuclear, un apagón eléctrico, un bloqueo de comunicaciones en un aeropuerto, un problema en un reactor químico, en una planta para el control de una represa, en una planta de tratamiento agua, y peor aún en un cruce ferroviario o un hospital.

Proteger sistemas de control y automatización de procesos en Plantas de Producción y Fábricas, suele ser más riesgoso que otros sistemas. Las amenazas y las vulnerabilidades a las están expuestos estos sistemas son a veces desconocidas y muy diferentes de otras organizaciones como bancos y empresas en general.

Como en todas las actividades riesgosas, es necesario "preveer", por lo que se pueden tener diferentes enfoques para enfrentar el problema; Antes de continuar se debe tener algunas consideraciones como:

- Un sistema "seguro" Ahora, puede no serlo mañana o dentro de una hora.
- Los problemas de seguridad no sólo pueden resolverse con la tecnología.
- Un sistema nunca puede ser 100% seguro.
- La seguridad no es un producto envasado, es un proceso, una forma de pensar.
- El comportamiento entre las personas, son la parte preponderante a fin de lograr un sistema seguro.

En los últimos años, la mayoría de las redes de control, sistemas de automatización y control SCADA (Supervisory Control and Data Acquisition), sistemas DCS (Distrubuted Control System), están basando, su tecnología y sus productos, en recursos típicos de ambientes informáticos TI (IT, Information Technology) como por ejemplo Ethernet, TCP/IP, Windows, etc., y se utilizan, en lugares en donde se tienen redes de comunicaciones críticas. El beneficio del uso de esas tecnologías y productos, como el uso de protocolos estándar y de los sistemas operativos del mercado, también, han disminuido el "aislamiento" de los sistemas SCADA, DCS y Redes de Control de Proceso (RCP) que durante mucho tiempo habían basado su protección, principalmente, en mantenerse en ambientes cerrados y de aislamiento. Ahora muchos de estos sistemas corren el riesgo de tener accidentes y ataques.

En general, las arquitecturas en términos de una mejor protección, son aquellas con la presencia de "zonas desmilitarizada" (DMZ, Demilitarized Zone) entre la red empresarial (RE) y red de control de proceso SCADA (RCP).

Generalmente, la solución utilizada para aislar los sistemas SCADA y las RCP, de la conexión directa a Internet y de la red corporativa (RE, Red de la empresa), se logra usando

Firewall. De hecho, el Firewall, pueden ser un poderoso dispositivo, pero también, es complejo para instalar; lo que obliga al administrador a tener un buen conocimiento, de como usarlo de manera efectiva en ambientes industriales. El Firewall para Tecnologías de la Información (TI, Tecnologías de Información), está generalmente diseñado, para los protocolos tradicionales de TI, y a menudo, no es capaz de manejar adecuadamente, los numerosos protocolos que se están moviendo en las redes SCADA/RCP. El Firewall también tiene tiempos de latencia (retrasos), que muchos casos, no son aceptables en aplicaciones de tiempo real, en donde se requieren tiempos de respuesta que deben ser garantizados, especialmente en los sistemas de control. La presentación de los datos y el tratamiento de las alarma y/o información es muy diferente de la típica del mundo (TI). Para hacer las cosas aún más complicadas, todavía es difícil encontrar información sobre cómo debe ser controlado, configurado e instalado el Firewall.

1. SISTEMAS DE CONTROL DE PROCESOS Y AUTOMATIZACIÓN EN PLANTAS DE PRODUCCIÓN.

Las Plantas de Producción y las maquinarias, son administradas por sistemas de automatización y control que cada día, están mas vinculados para interactuar con procesos necesarios para su monitoreo y control desde sitios remotos, comúnmente llamados Cuartos de Control o Cuartos Técnicos. Estos sistemas están a su vez conectados a las empresas por otras redes de datos, por donde se transmitirá la información necesaria, para una gestión completa.

Pero veamos qué dispositivos están en las redes y cuáles son las aplicaciones más comunes de estos sistemas; sin pretender hacer una exposición completa, dado que son muchas las soluciones que existe en empresas de producción como ECOPETROL.

1.1 PLC (Programmable Logic Controller) o controladores lógicos programables.

Son dispositivos, que están en los sistemas de automatización. Están basados en microprocesadores y ejecutan generalmente tareas repetitivas. Están equipados con tarjetas de I/O (entrada/salida), donde pueden estar conectados sensores y actuadores, instalados directamente en plantas de producción o maquinaria controlada.
La multiplicidad de los protocolos utilizados (la mayoría de los cuales no se basan en IP), esconden todavía, muchos de las vulnerabilidades ampliamente difundidas en las redes de TI.

1.2 HMI/SCADA.

Son los puestos de trabajo utilizados por los operadores para observar y evaluar lo que ocurre en las instalaciones (Dado que los PLC son realmente unos dispositivos "ciegos" no están equipados con interfaz para visualización).

1.2.1 **HMI (Human Machine Interface)**: Pueden ser paneles de operador, con pantalla gráfica, microprocesador, a veces, con sistemas operativos y el desarrollo de entornos propietarios (personalizables). En los últimos años ha sido generalizados, los paneles estánda, sobre la base de microprocesadores y WindowsCE, Linux y otras pequeñas versiones (propietarias) de Windows, que soportan las aplicaciones del mercado, para el desarrollo de las interfaces que sirven para presentar datos e información a los operadores en planta. Las HMI usualmente están relacionadas a PLC y redes de PLC, por Puertos Seriales (con comunicación directa con la CPU del PLC) o con el mismo autobús o enlaces vía Ethernet, con el cual utiliza el mismo protocolo.

1.2.2 **SCADA (Supervisory Control and Data Acquisition**): Este es una clase de paquetes de software de aplicaciones, que permite utilizando un PC, desarrollar una interfaz gráfica inteligente para la gestión, incluso compleja de uno o más PLC conectados a la red. Las funciones estándar de un paquete SCADA, para el Monitoreo y supervisión son: la comunicación con el PLC, interfaz gráfica, la

gestión de alarmas, recopilación de datos o cualquier dato disponible de la información proveniente en planta de proceso. Generalmente, utilizan un PC con Windows (rara vez Linux) y en la comunicación con el PLC, son cada vez más frecuente, la utilización de OPC (sobre la base de DCOM), el estándar patrocinado por Microsoft y un grupo de proveedores (www.opcfoundation.org), y con gran acogida en el mercado, para facilitar la configuración y la gestión de los protocolos utilizados.

1.3 DCS (Distributed Control Systems)

Son sistemas de control integrados y distribuidos formados de controladores (similares a PLC) y estaciones para operador (similar a la de los PC SCADA), diseñados para la administración en plantas donde la criticidad, requiere niveles altos de seguridad, en términos de disponibilidad y la fiabilidad de los componentes y la ejecución.

El conjunto **Controlador-PC** es proporcionado por el vendedor con CPU y bus de campo propietario y redundante, y también, las comunicaciones entre los diversos dispositivos en la red, suele ocurrir con redes redundantes y protegidas.

1.4 **Sistemas SCADA (sistemas de Telecontrol**).

Incluso tienen la misma sigla, arriba mencionada (SCADA Supervisory Control & Data Acquisition), los sistemas de Telecontrol, son para la gestión de dispositivos distribuidos, sobre amplios territorios.

Pueden ser utilizados localmente PLC, pero a menudo, se habla también, de RTU (Remote Terminal Unit): Son dispositivos diseñados especialmente para la gestión local, en un número limitado de I/O, cuya funcionalidad es la de transmitir y recibir comandos y datos, sobre el estado de la operación, desde y hacia una sala de control central. Esta transmisión puede ser de muchas formas diferentes: utilizando (costosos) puentes de radio, líneas telefónicas, telefonía móvil GSM/GPRS redes WAN, etc.

En los centros de acopio de información y en las salas de control, existen redes de computadores con SCADA, similares a los que ya se han visto. A menudo, la complejidad de las aplicaciones de Telecontrol, radica principalmente, en la gestión de comunicaciones, ya que en la misma aplicación, se debe combinar una multitud de dispositivos remotos (a menudo cientos y a veces miles), con diferentes métodos de comunicación (módem telefónicos, módem GSM, radio módem, VPN, etc.), para poner a trabajar en épocas y tiempos diferentes e interactuar juntos.

2. VULNERABILIDADES COMUNES EN LAS REDES DE AUTOMATIZACIÓN Y SISTEMAS DE CONTROL DE PROCESO.

En ningún momento, se pretende decir, que esta es una lista completa de vulnerabilidades, solo se dará un esbozó.
A continuación, se presentan algunas de las vulnerabilidades más comunes que pueden surgir en redes y sistemas utilizados en la industria:

- El registro de eventos y accidentes, no están presentes, o no son oportunos.
- Dificultad para controlar y dar métricas sobre la fiabilidad y disponibilidad de la red y sobre los sistemas.
- Política de seguridad inexistente y/o no aplicada.
- Falta de sensibilización (y capacitación) sobre los problemas, como enfrentarlos y las posibles consecuencias.
- Servidores y activos de operación critica no ubicados tras zona desmilitarizada (DMZ, zona desmilitarizada). Es necesario definir las reglas para el acceso a los recursos, computadoras y zonas de la red.
- Documentación de la red y los sistemas, no existentes y/o no actualizada.
- Controles de acceso no presentes o normas no respetadas.
- Separación insuficiente (o inexistentes) entre la red de control y la red del negocio. Separar la red "del negocio" y la red "control" es necesario para evitar que las amenazas y vulnerabilidades pasen de una a la otra.
- Redes "planas" o de pobre segmentación de la red de control. A menudo todos los PC y los PLC están en la misma red de la fábrica, sin segmentación para limitar los problemas de tráfico, daños y las eventuales contaminaciones.
- Mala definición y mantenimiento de los perfiles y la lista de control de acceso al PC y a los recursos de la red. Es necesario limitar el acceso a los recursos, computadores y PLC sólo a quien corresponda.
- Detectores de comportamientos maliciosos (antivirus, etc.) no presente y/o no actualizados. La mayoría de las aplicaciones en tiempo-real se utilizan en equipos que no son compatibles con antivirus de PC: encontrar otras estrategias.
- El computador no está correctamente configurado. Pobres "Afinamiento" de los sistemas operativos y aplicaciones.
- Sistema operativo “viejo” y/o no actualizado (sin parche).
- El PC instalado, "obsoleto" y con poco mantenimiento. Problemas de recursos físicos.
- Gestión de la configuración inexistente o no se actualiza.
- Acceso remoto por defecto o no controlados (para los administradores, los operadores remoto, supervisores, proveedores, etc.) vía módem y/o vía VPN.
- Redes cableadas y/o inalámbricas no controladas.
- Planes y procedimientos para la atención de emergencias/imprevistos inexistentes o no actualizados/probados.
- Planes, procedimientos de back-up (incluyendo PLC), Recuperación y inexistentes o no actualizados/probados.

- Uso de componentes de la red (switch, router, firewall, etc.) no son insuficientes e inadecuados (no industriales).
- Uso de DCS, HMI/SCADA o con sistemas operativos estándar (como Windows, Linux, etc.), sin el parche recomendado para hacer más segura la red.

3. Referencias a las normas y estándares.

3.1 La norma ISO27000 e ISA S99

Algunas normas y estándares puede ayudarnos a decidir cuáles son las mejores políticas para la seguridad de los sistemas y la información, además, para definir las situaciones de riesgo, amenazas, vulnerabilidades y determinar cuáles son los controles y las acciones correctivas que se deben adoptar.

3.2 La ISO/IEC norma 17799, BS 7799 y la serie ISO27000.

Especifica los requerimientos para establecer, implantar y documentar un sistema de gestión de seguridad de la información.
Esta norma da una base común para elaborar las políticas de seguridad de las organizaciones y para el diseño, la ejecución, el mantenimiento de las posibles mejoras de los sistemas utilizados en la empresa, incluidos los de la producción y manejo en plantas.

La Norma **ISO/IEC 17799:2005** "Information Technology Code of practice for Information Security Management", estaba basada en **BS7799-1:1999** (que fue re-emitida como la **ISO 27002** en el 2007) y por lo tanto están alineadas. La **ISO 27002** en el 2007está compuesta por un conjunto de controles/contramedidas de seguridad, que surgieron de **las mejores prácticas** en la seguridad de los sistemas de información y es reconocida a nivel internacional como la norma de referencia para la seguridad de la información.

La serie **ISO27000** se diseño para armonizar con las otras normas de los Sistemas de Gestión, como son la **EN ISO 9001:2000** y el **ES ISO 14001:1996**, proporcionado de manera integrada y coherente los logros y las operaciones de los sistemas de gestión. También introduce el modelo PDCA (Plan-Do-Check-Act) que quiere decir "Planear/Probar-Realizar/Mejorar-Chequear/Monitorear-Actualizar/Asegurar" como parte de los sistemas de gestión para desarrollar, aplicar y mejorar la eficacia del sistema de gestión para la seguridad de la información organización (SGSI).

3.3 La norma ISO 27002

- No es un estándar técnico; una organización puede querer tomar controles adicionales, especialmente sobre la base de análisis y evaluación de riesgos realizada.
- No es un estándar orientado a productos o tecnologías específicas.
- No es un milagro para los ISO.
- Es sólo una referencia.
- No todos los controles descritos son pertinentes a cada situación, ni se tienen en cuenta las limitaciones locales ambientales, tecnológicas, etc.

A menudo los usuarios o la persona responsable de la información y los sistemas de administración quienes tratan/procesan la información, son responsables de la correcta aplicación.

4. **Los Objetivos de seguridad**

La seguridad de la información, se ha enfocado tradicionalmente, en lograr tres objetivos: confidencialidad, la integridad, y disponibilidad." Una estrategia de seguridad típica en TI, “back Office” o para los sistemas del negocio, se puede enfocar principalmente, en la confidencialidad y en los controles necesarios de acceso para lograrlo. La integridad podría catalogarse como la segunda prioridad y la disponibilidad como el más bajo en importancia.

En ambientes de automatización industrial y de sistemas de control, la prioridad general de estos objetivos es a menudo diferente. La seguridad en estos sistemas, está principalmente enfocada a mantener la disponibilidad de todos los componentes del sistema. Hay riesgos inherentes asociados con la maquinaria industrial que se controla, se supervisa y para cumplir estándares de seguridad, es intervenida por otra parte, por sistemas de automatización industrial y de control.

Por consiguiente, la integridad es a menudo la segunda en importancia. Normalmente la confidencialidad es de menor importancia, porque los datos están en un formato “crudo” y deben analizarse dentro del contexto para tener algún valor.
La faceta de la sensibilidad *al tiempo,* es significante. Los sistemas de Control, pueden tener como requisitos de sistema, la sensibilidad en el rango de un (1) milisegundo, en comparación con los sistemas tradicionales de negocio que son capaces de operar con éxito con tiempos de respuesta de uno o múltiples segundos.

En algunas situaciones las prioridades son completamente invertidas, como mostrado en Figura 1

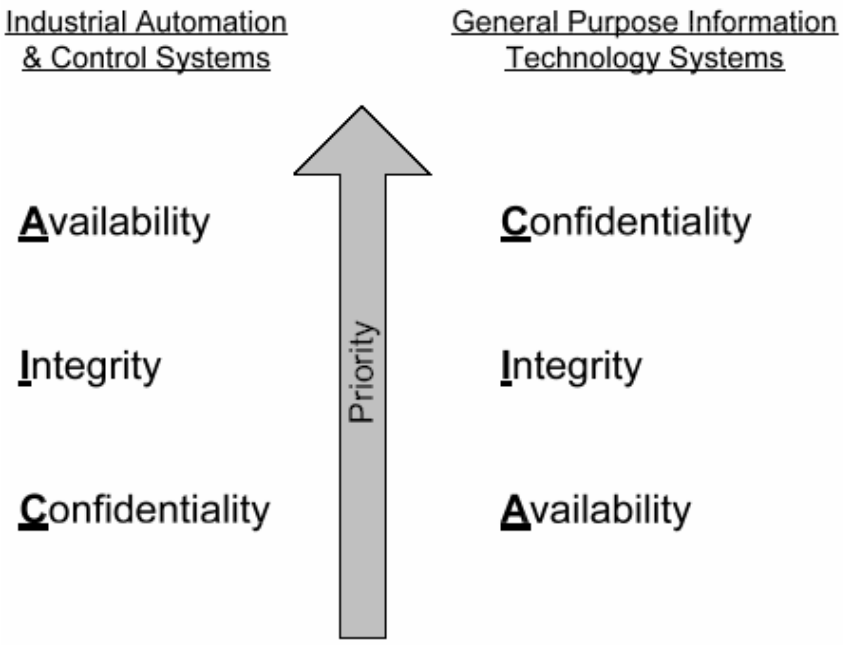

Figura 1 ANSI/ISA–99.00.01–2007 5.2 Comparison of Objectives

En una presentación, que para muchos autores se define como la rueda de la seguridad, la seguridad informática consta de los siguientes macro-procesos:
– proceso 1: Asegurar
– proceso 2: Monitorear
– proceso 3: Probar
– proceso 4: Mejorar

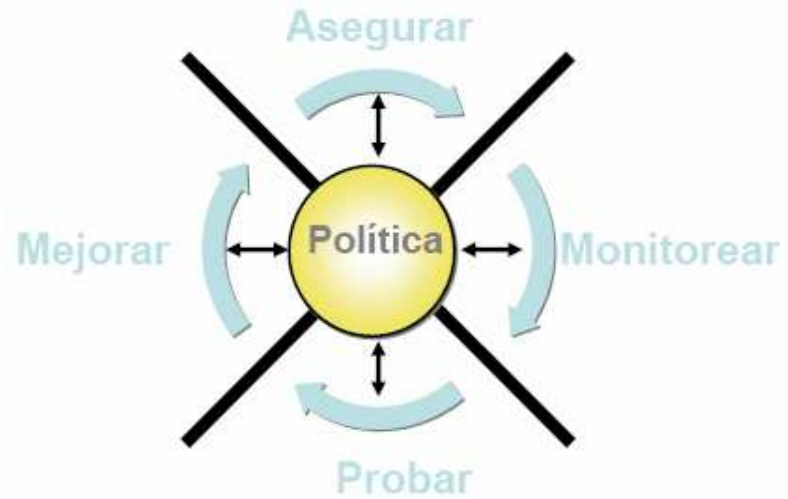

Figura 2. Rueda de la seguridad

4.1 Qué es la seguridad de la información?

La información es uno de los bienes de la empresa y como tal, tienen un valor: por lo tanto debe ser adecuadamente protegida. La seguridad de la información protege la información de una diversidad de amenazas, a fin de garantizar la continuidad de las operaciones (y por lo tanto de la producción), minimizar los daños en las corporaciones, maximizar el retorno de la capital invertido, mejorar la eficiencia y eficacia. La seguridad de la información está vista como la preservación de:

- **Confidencialidad:** Asegurar que la información disponible sólo para quién está autorizado para tener acceso
- **Integridad:** Para salvaguardar la exactitud, la integridad de la información y los bienes conectado cuando sea necesario
- **Disponibilidad:** asegurar que los usuarios autorizados tienen acceso a información y bienes cuando sea necesario
- **No Repudio:**
  Este término se ha introducido en los últimos años como una característica más de los elementos que conforman la seguridad en un sistema informático. Está asociado a la aceptación de un protocolo de comunicación entre emisor y receptor (cliente y servidor) normalmente a través del intercambio de sendos certificados digitales de autenticación.
  Se habla entonces de No Repudio de Origen y No Repudio de Destino, forzando a que se cumplan todas las operaciones por ambas partes en una comunicación.

5. EVALUAR Y GESTIONAR LOS RIESGOS ENTRE LAS FUENTES

Para identificar los requisitos de seguridad en una organización, se hace mediante *El Análisis y la Evaluación de Riesgos*, teniendo en cuenta, la evaluación de las amenazas, el impacto de la vulnerabilidad de la información y las facilidades para procesar la información y la probabilidad de su ocurrencia.

La evaluación del riesgo es por lo tanto una consideración sistemática:
• De los daños que pueden surgir, de deficiencias en materia de seguridad, teniendo en cuenta las posibles consecuencias de la pérdida de confidencialidad, integridad o la disponibilidad de información u otros bienes.
• La posibilidad real de que se produzca un ataque por la falencia de la luz de las amenazas y vulnerabilidades, con los controles/contramedidas ya activos.

Los resultados de la evaluación, conducirán a la **Administración de los Riesgos,** entendida como el proceso para identificar, controlar, reducir o eliminar los riesgos inherentes a la seguridad que pueden afectar los sistemas de información, a un costo aceptable.

6. MODELOS PARA DESARROLLAR UN PROGRAMA DE SEGURIDAD SEGÚN LA NORMA ISA99

6.1 Modelos Generales

La norma ISA S99 del 2007, presenta una serie de modelos que pueden ser utilizados en un adecuado diseño de programas de seguridad. La norma tiene como objetivo, identificar las necesidades en materia de seguridad y las características importantes del medio, para hacer frente a las normas y requerimientos de seguridad. Para llegar a estos modelos, se realiza previamente una estandarización de términos y vocabulario, que genera, un marco de conocimiento común.

Estos modelos vienen en diferentes formas, incluyendo:

a) **Modelos de referencia**: Proporcionan la base conceptual para la información más detallada de los modelos a seguir.

b) **Modelos Activos**: Describen las relaciones entre el activo (dentro del ámbito del sistema de control) y la automatización industrial.

c) **Arquitectura de Referencia**: describe la configuración de los activos. Una arquitectura de referencia puede ser única para cada empresa o un subconjunto de la empresa. Es única para cada situación dependiendo del alcance del sistema de control y la automatización industrial que se esta examinando.

d) **Modelo de Zona**: Agrupa elementos de arquitectura de referencia, de acuerdo con características definidas. Esto proporciona un contexto para la definición de políticas, procedimientos y directrices que a su vez, son aplicados a los activos.

Toda esta información se utiliza para desarrollar un programa detallado de la administración de la seguridad, en un sistema de automatización y control industrial; por esto explicaremos cada uno de una forma mas detallada y sus caracteristicas de sus componentes.

6.1.1 Modelos de Referencia.

El término "modelo de referencia" se hizo popular con el éxito de la ISO del modelo de las "Siete capas", para sistemas de Interconexión abiertos. (OSI, Open Systems Interconnection). La oficina de estándares y tecnología de la NASA (con sigla en ingles, NOST), define el termino como: "Un modelo de referencia es un marco importante para la comprensión de las relaciones entre las entidades de algunos medios para el desarrollo de normas coherentes y especificaciones de apoyo en ese entorno. Un modelo de referencia, se basa en un pequeño número de conceptos unificados y puede ser utilizado como base para la capacitación y explicar las normas a un “no-especialista” en el tema." Un modelo de referencia, describe una vista genérica de un sistema de fabricación o de producción

integrados, expresado en una serie de niveles lógicos. El modelo de referencia utilizado por la ISA99, aparece en la Figura 3. Este modelo se deriva del modelo general utilizado en ANSI/ISA-95.00.01-2000, Enterprise-Control System Integration Parte 1: Terminología y modelos.

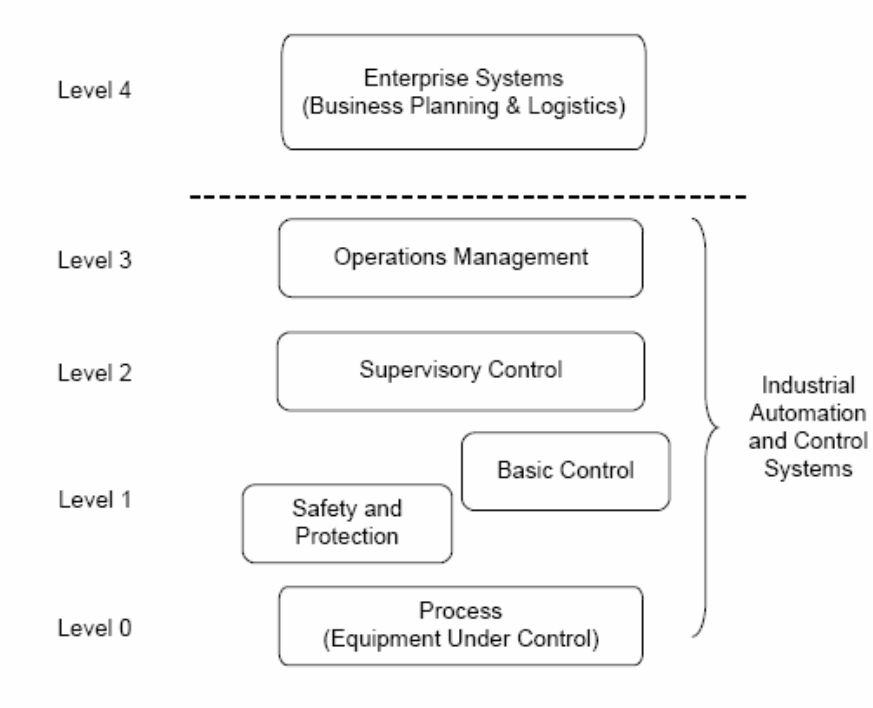

Figura 3 Estandar de Modelo de Referencia

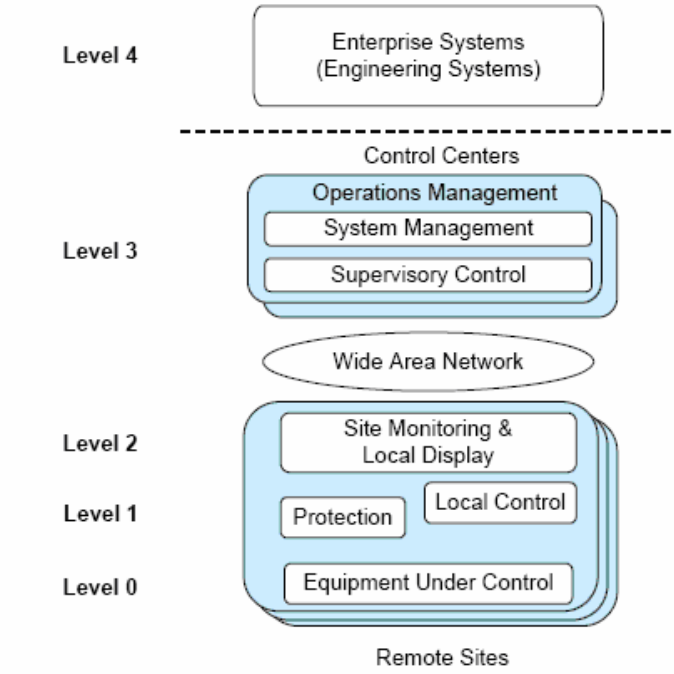

Figura 4 Modelo de Referencia

6.1.1.1. Niveles del Modelo de Referencia

Se describen las funciones y actividades de proceso (nivel 0) hasta la red de la empresa (nivel 4).

- **Nivel 4 – Sistemas de la Empresa**

Este nivel se describe como "La Planificación y Logística del Negocios", se definen las funciones que participan en los negocios relacionados con las actividades necesarias para la administración de la fabricación y la organización. Las funciones incluyen sistemas financieros regionales y empresariales, componentes de la infraestructura como la programación de la producción, gestión operativa y la administración del mantenimiento en general. Para efectos de la norma, la ingeniería de sistemas se encuentra en este nivel.

- **Nivel 3 - Administración de las Operaciones**

Nivel 3 incluye las funciones involucradas en la gestión de los flujos de trabajo, para producir los productos finales. Los ejemplos incluyen el envío de la producción, la programación detallada de producción, garantía de fiabilidad, y control de optimización.

- **Nivel 2 - Control Supervisión**

Nivel 2 incluye las funciones que intervienen en la vigilancia y el control del proceso físico. Hay típicamente varias zonas de producción en planta, como la de destilación, conversión y mezcla en una refinería. Y tiene en cuenta lo siguiente:
a) Interfaz de operador de hombre-máquina.
b) Alarmas y alertas de operador.
c) Las funciones de supervisión de control.
d) Proceso de recogida de los históricos.

- **Nivel 1 - Local o Básica de Control**

Nivel 1 incluye las funciones que participan en detección y manipulación del proceso físico. Proceso de monitoreo de equipos, lectura de datos, desde los sensores, ejecuta los algoritmos en caso necesario, y mantiene el histirico de los procesos. Ejemplos de proceso de sistemas de vigilancia que incluyen los sistemas de medición de tanques, monitores de emisión, la rotación de equipos y sistemas de control, indicando la temperatura y sistemas.
Tiene encuenta lo siguientes:
a) los controladores de DCS
b) PLCs
c) RTU

- **Nivel 0 - Proceso**

Nivel 0, es el proceso físico. El proceso incluye una serie de diferentes tipos de instalaciones de producción, en todos los sectores, pero sin limitarse a las partes de fabricación discreta, procesamiento de hidrocarburos, distribución de productos, productos farmacéuticos, pulpa y papel, y la energía eléctrica. Nivel 0 incluye los sensores y actuadores conectados directamente con el proceso y equipos de proceso.

6.2 Modelos Activos

Los Sistemas de Control Modernos, son complejas, redes de computadores interconectadas con muchos componentes que realizan, una variedad de tareas de forma segura y eficiente.

Por lo tanto, el modelo activo debe comenzar en un nivel alto, hasta el nivel mas bajo de la cadena de operaciones Ver la Figura 5
Estos sistemas se denominan "sistemas instrumentados de seguridad" en normas como la serieANSI/ISA-84.

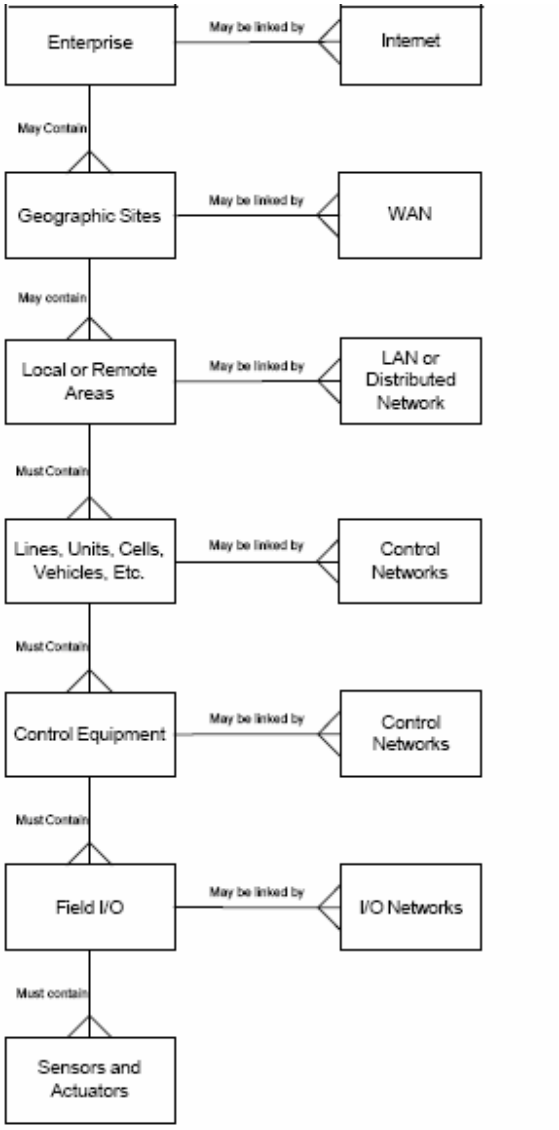

Figura 5 Ejemplo de Modelo Activo en Proceso de Fabricas

Como las redes juegan un papel importante en la seguridad, el modelo activo, explícitamente incluye los elementos de red que típicamente se presentan en cada nivel de la jerarquía. En cada nivel, el equipo (o instalaciones) esta unido, al tipo apropiado de red, aunque en las redes, ellos mismos puedan estar unidos. Este modelo no representa aquel acoplamiento.

6.2.1 Empresa Es una entidad, que produce y transporta productos, opera y mantiene servicios de infraestructura.

6.2.2 Sitios geográficos

. Son un subconjunto de una empresa, físico, geográfico, lógico o grupo de activos. Puede contener áreas, líneas de fabricación, unidades de proceso, centros de control y los vehículos. Un sitio, puede ser conectado a otros sitios de una WAN. Un sitio geográfico, puede incluir sistemas de información, tales como la fabricación, ejecución de las actividades de producción que se coordinan en el sitio.

- **Centro de Control**

Un centro de control, es un tipo especial de sitio. Las industrias de infraestructura suelen utilizar uno o más centros de control, para supervisar o coordinar sus operaciones. Si la empresa tiene varios centros de control (por ejemplo: centro de copia de seguridad en un sitio separado), están normalmente conectados entre sí a través de una WAN. El centro de control contiene el SCADA y los computadores auxiliares del operador de los dispositivos, además, de la información servidores de históricos.

- **Sitio Remoto**

Los sitios Remotos, contienen equipos tales como, PLCs, las unidades terminales remotas (RTU), o dispositivos electrónicos inteligentes (IED), que se encargan de monitorear y controlar las operaciones locales del sitio. Los sitios remotos ,se conectan al centro de control de una red de comunicaciónes (a veces denominado una red de telemetría). Los sitios remotos también pueden ser conectados, unos con otros, para facilitar funciones como la reinstalación de protección entre las subestaciones eléctricas, en una red de transmisión.

6.2.3 Espacio

Un espacio, es un subconjunto de un lugar físico, geográfico, lógico o grupo de activos. Puede contener líneas de fabricación, proceso de las células, y las unidades de producción. Las áreas, en un espacio, pueden estar conectados entre sí, por un sitio LAN y pueden contener, los sistemas de información relacionados con las operaciones realizadas en ese ámbito.

6.2.4 Las líneas, Unidades, Células, Vehículos

Estas zonas están compuestas de elementos de nivel inferior, que llevan a cabo, la fabricación, control de la infraestructura y funciones de vehículo. Entidades en este nivel pueden ser conectados entre sí por una red de control de área y contienen los sistemas de información relacionados con las operaciones realizadas en la empresa.

6.2.5 Equipo de Control de Supervisión

El equipo de control de vigilancia, incluye los servidores informáticos, HMI, redes de área local y dispositivos de comunicación, que permitirán a los operadores, supervisar a distancia y controlar las instalaciones que están repartidas en una amplia área geográfica.

6.2.6 Control de Equipos

El Control de equipos, incluye DCS, PLC, controladores de movimiento, unidades inteligentes, y los operadores de interfaz de consolas, que se utilizan para gestionar y controlar el proceso. También incluye, las redes de bus de campo, donde se ejecuta la lógica de control y algoritmos en los dispositivos de campo, que coordinan sus actividades

6.2.7 Campos de E / S de red

El campo de entrada / salida (I / O), es la red de enlace de comunicaciones (con cable o inalámbrico) que conecta estos elementos, a los sistemas de control.

6.2.8 Sensores y Actuadores

Los sensores y actuadores son los elementos finales, conectados a equipos de control de proceso.

6.2.9 Equipo bajo control

Los activos del sistema de control, son los activos que componen el equipo bajo control. Esto nivel también se conoce como nivel físico o proceso operativo.

6.3 Arquitectura de Referencia:

La arquitectura de referencia, se construye a partir de las entidades definidas en el modelo activo. Una arquitectura de referencia es especifica y particular en cada situación y asi lo será, para el análisis. Cada empresa, crea una o varias arquitecturas de referencia con relación de las funciones desempeñadas. Un ejemplo simplificado de una arquitectura de referencia para una función de fabricación se muestra en la Figura 6

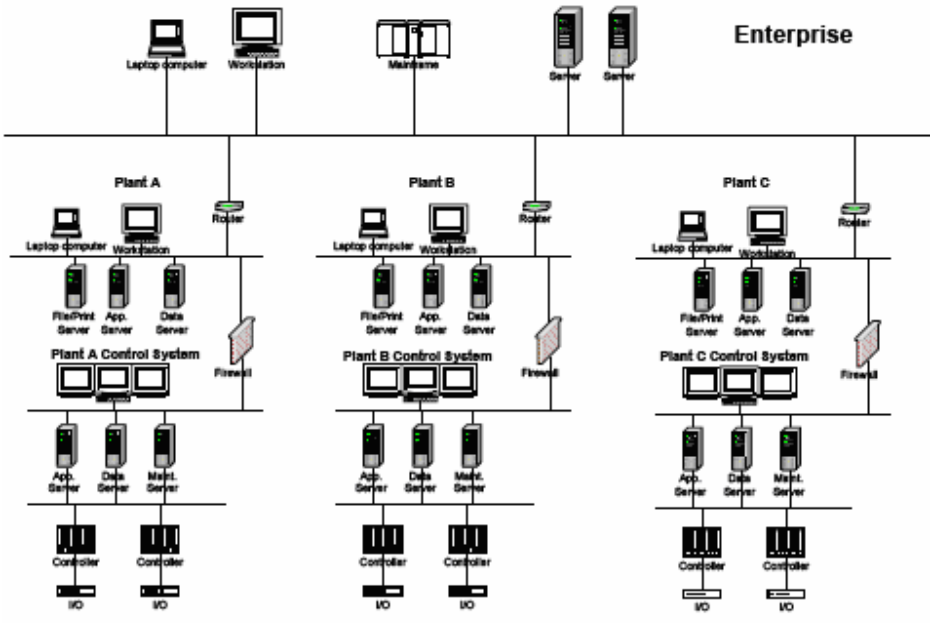

Figura 6 Ejemplo de Arquitectura de Referencia

6.4 Modelo de Zonas

En una zona, se desarrolla el modelo de la arquitectura de referencia. Se utiliza para describir la lógica, agrupaciones de activos dentro de una empresa o un subconjunto de la empresa. Los activos se agrupan en entidades (por ejemplo, las empresas, instalaciones, página web, o por el SIGC) que luego pueden ser analizados por las políticas de seguridad. El modelo ayuda a evaluar las amenazas comunes, vulnerabilidades y lo correspondiente las contramedidas necesarias para alcanzar el nivel de seguridad deseado, (Meta de nivel de seguridad) necesarias para proteger los activos agrupados. Al agrupar los activos de esta manera, una política de seguridad puede definirse para todos los bienes que son miembros de la zona. Este análisis puede usarse, para determinar la protección requerida sobre la base de las actividades realizadas en la zona. **Todos los usos incondicionales de la palabra "zona" en estas normas se deben referir a una zona de seguridad.**

6.4.1 La zonas de seguridad

Al definir las zonas, las organizaciones deben estar seguros de utilizar tanto la arquitectura de referencia como el modelo de activos, para desarrollar la zonas de seguridad adecuadas y los niveles de seguridad, para así, lograr las metas establecidas de seguridad para la automatización y sistemas de control.

6.4.2 Zona de Identificación

Esta Zona, puede ser una agrupación independiente de los activos, una agrupación de subzonas, o una combinación de ambos, independiente de los activos y bienes que también se agrupan en subzonas que figuran en las zonas principales. Las zonas de identificacion, tienen la característica de la herencia, lo que significa una zona niño (o subzona) deben cumplir con todas las necesidades de la zona padre. Una modelo de zona simplificado se muestra en la Figura 7.

Aquí la zona de la empresa es el padre, y cada subzona es un niño..

NOTA: Existe una clara ventaja a ajustar las zonas de seguridad física, con áreas o zonas en una instalación - por ejemplo, una alineación centro de control con una zona de control de seguridad.

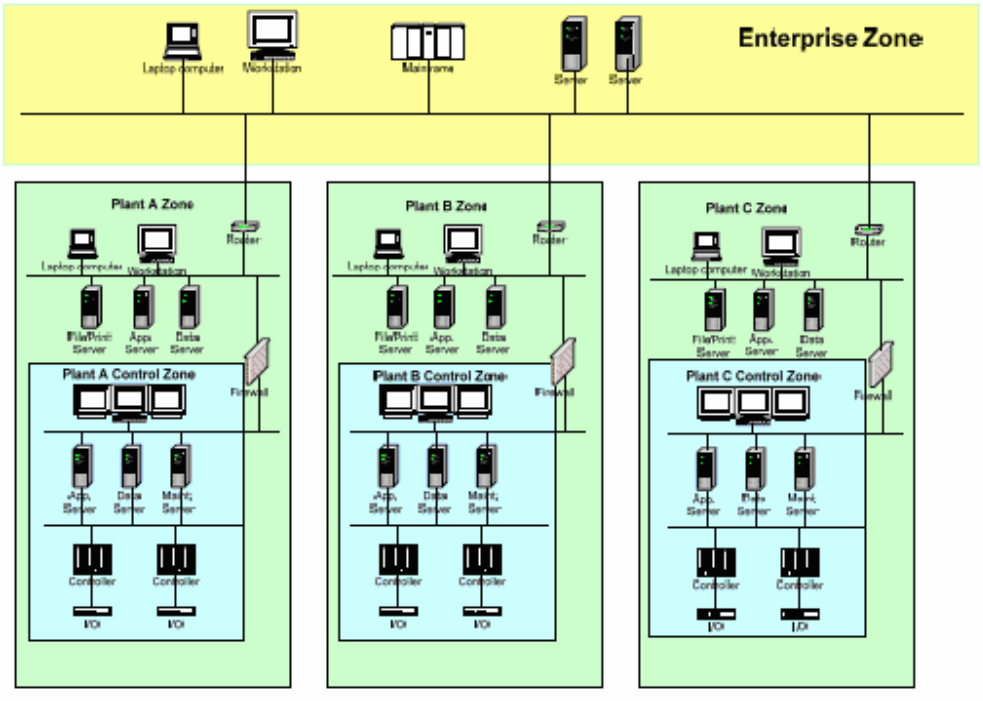

Figura 7 Ejemplo de Zona Multiplantas

La arquitectura misma de la empresa, pueden agruparse en distintas zonas como en la Figura 8. En este modelo, la zona de las políticas serían independientes, y cada zona podría tener totalmente diferentes políticas de seguridad.

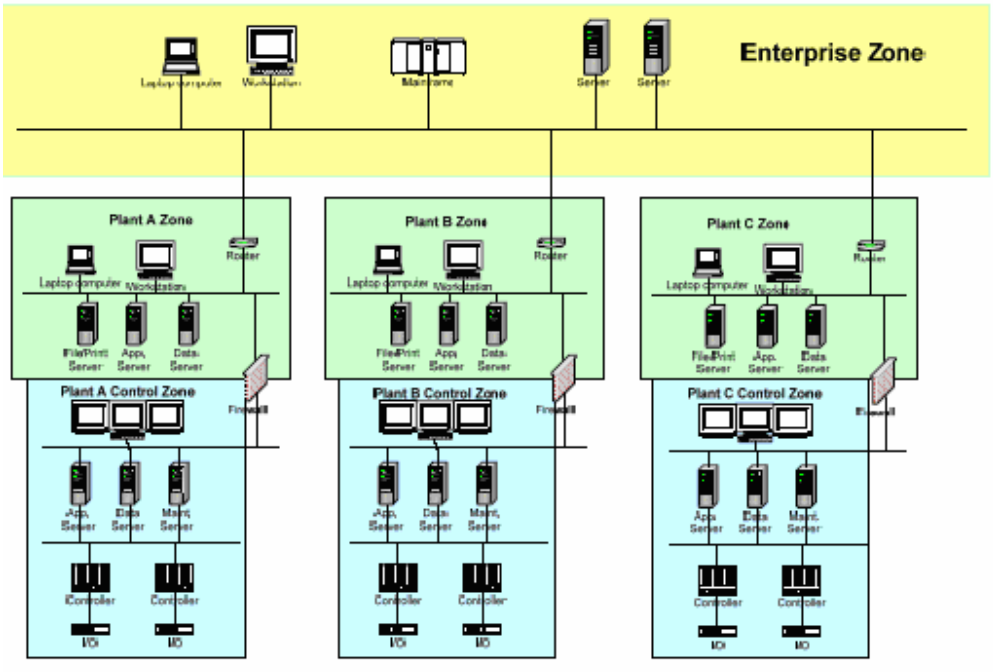

Figura 8 Ejemplo de Zonas separadas

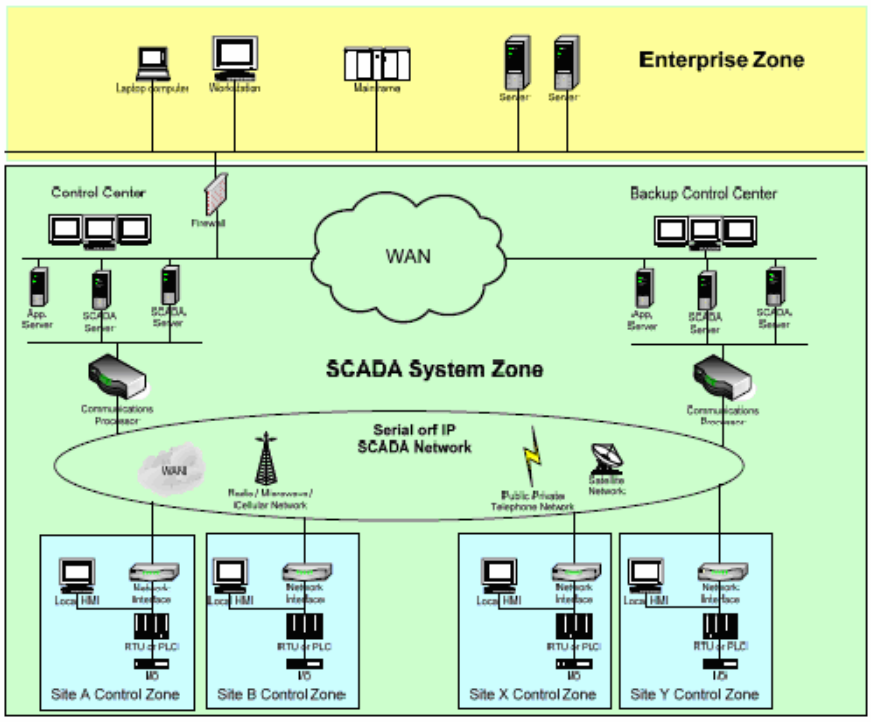

Figura 9 Ejemplo de Zona SCADA

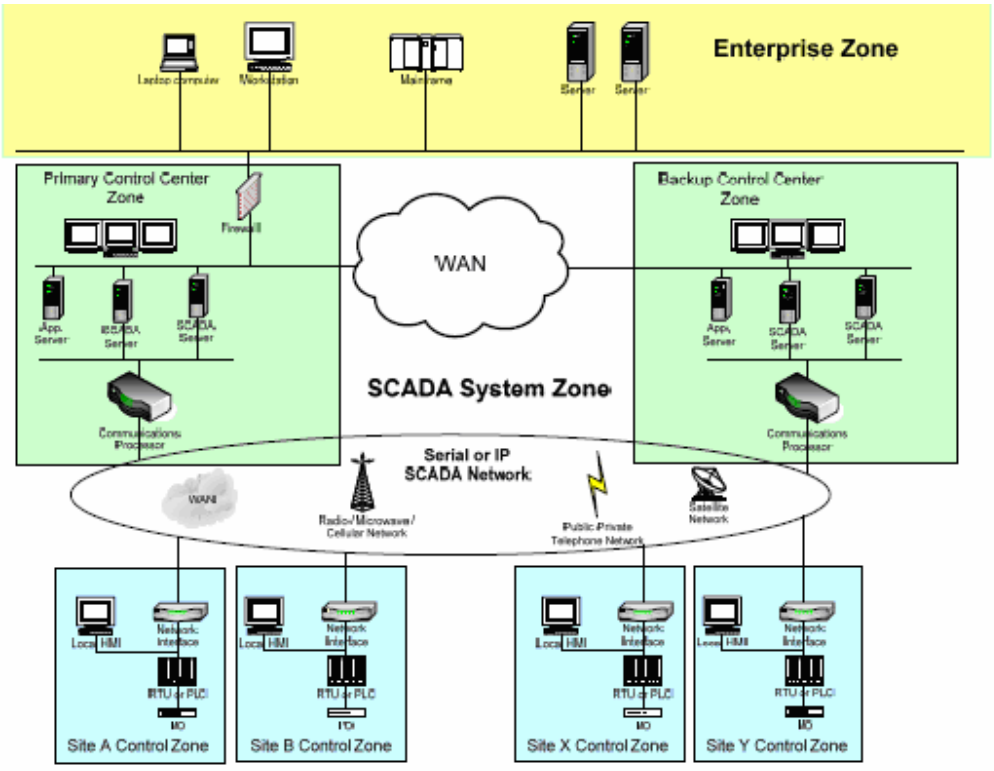

Figura 10 Ejemplo de Zanas separadas SCADA

6.4.3 Zona Características

Cada zona, tiene un conjunto de características y requisitos de seguridad que son sus atributos. Estas tomarán las forma de:
a) Políticas de Seguridad
b) Inventario de Activos
c) requisitos de acceso y controles
d) Amenazas y Vulnerabilidades
e) Las consecuencias de un fallo de seguridad
f) Tecnologías Utilizadas
g) proceso de gestión del cambio.

Cada uno de estos atributos se describe con más detalle en los párrafos siguientes.

- **Políticas de Seguridad**

Cada zona, tiene una participación de control documentos que describe los objetivos de seguridad global y la forma de garantizar, que se cumpla la meta de nivel de seguridad. Esto incluye:
a) la zona de alcance
b) el nivel de seguridad de la zona
c) la estructura organizativa y responsabilidades para hacer cumplir la política de seguridad
d) los riesgos asociados con la zona
e) la estrategia de seguridad para satisfacer los objetivos
f) las medidas de seguridad que debe ejecutarse
g) los tipos de actividades que están permitidas dentro de la zona
h) los tipos de comunicación permitirá el acceso a la zona
i) la documentación de atributos de la zona.
Todo lo anterior se documenta y se combina en la zona de seguridad común, que se utiliza para orientar la construcción y el mantenimiento de los activos que figuran dentro de la zona.

- **Inventario de Activos**

Para mantener la seguridad dentro de una zona, una organización debe mantener una lista de todos los activos (físicos y lógicos). Esta lista, se usa para evaluar los riesgos y vulnerabilidades, así como para determinar y mantener la adecuada las medidas de seguridad necesarias para cumplir los objetivos de la política de seguridad.

- **Requisitos de Acceso y Control**

Por su naturaleza, una zona implica que el acceso está limitado a un pequeño conjunto de todas las posibles entidades que pudieran tener acceso. Una política de seguridad de una zona, debe articular el acceso necesario para la zona a cumplir con sus los objetivos del negocio y cómo este acceso está controlado.

- **Evaluación de la vulnerabilidad y amenazas**

Las organizaciones deben identificar y evaluar estas amenazas y las vulnerabilidades, con el fin de determinar riesgos, que causarían los activos dentro de la zona y no cumplirían con sus objetivos de negocio. El proceso de documentar las amenazas y vulnerabilidades que

sucede en la amenaza y la evaluación de la vulnerabilidad, es parte de la zona de seguridad común.

- **Tecnologías Utilizadas**

Cada una de las tecnologías utilizadas en estos sistemas, trae consigo, un conjunto de vulnerabilidades y riesgos correspondientes. Para reducir al mínimo los riesgos para una zona determinada, la política de seguridad de la zana, debe tener, una lista dinámica de las tecnologías permitidas en la zona, así como las no admitidas.

- **Proceso de gestión de cambio**

Es oficial y preciso, el proceso es necesario para mantener la exactitud de una zona determinada, con el inventario de activos y cómo los cambios afectan la política de seguridad de la zona. Un proceso formal, garantiza que los cambios y adiciones a la zona, no pongan en peligro los objetivos de seguridad. Además, una manera de adaptarse a las nuevas amenazas en la seguridad. Las amenazas y las vulnerabilidades, con sus riesgos asociados, va a cambiar con el tiempo.

6.5 Definición de conductos

Los Conductos, son zonas de seguridad que se aplican a los procesos específicos de las comunicaciones. En las zonas de seguridad, son una consecuencia lógica de agrupamiento de los activos (activos de comunicación en este caso). Un conducto de seguridad protege la seguridad de los canales que contiene, en la misma forma que el conducto físico protege los cables de daños fisicos. Los Conductos, pueden ser considerados como "tubos" que conectan las zonas o que se utilizan, para la comunicación dentro de una zona. Interna (dentro de la zona) y externos (fuera de la zona) o conductos para proteger las comunicaciones "canales" (los cables de vista conceptual) que proporcionan los vínculos entre el activo. La mayoría de las veces en un SIGC medio ambiente el conducto es el mismo de la red. Es decir, el conducto es el cableado, routers, switch, la gestión de la red y los dispositivos que componen las comunicaciones presentadas en virtud del estudio. Los conductos, pueden ser disímiles agrupaciones de tecnologías de red, así como los canales de comunicación que puede ocurrir dentro de un solo ordenador. Los conductos, se utilizan para analizar las amenazas y las vulnerabilidades que pueden existir en las comunicaciones dentro y entre las zonas.

6.5.1 Características de los Conductos

Físicamente un conducto puede ser un cable que conecta las zonas para fines de comunicación. Un conducto es un tipo de zona que no puede tener subzonas, es decir, un conducto no está formado por subconduits. Conductos se define por la lista de todas las zonas que comparten los canales de comunicación dado. El conducto de la empresa ,se pone de relieve en la figura 11.

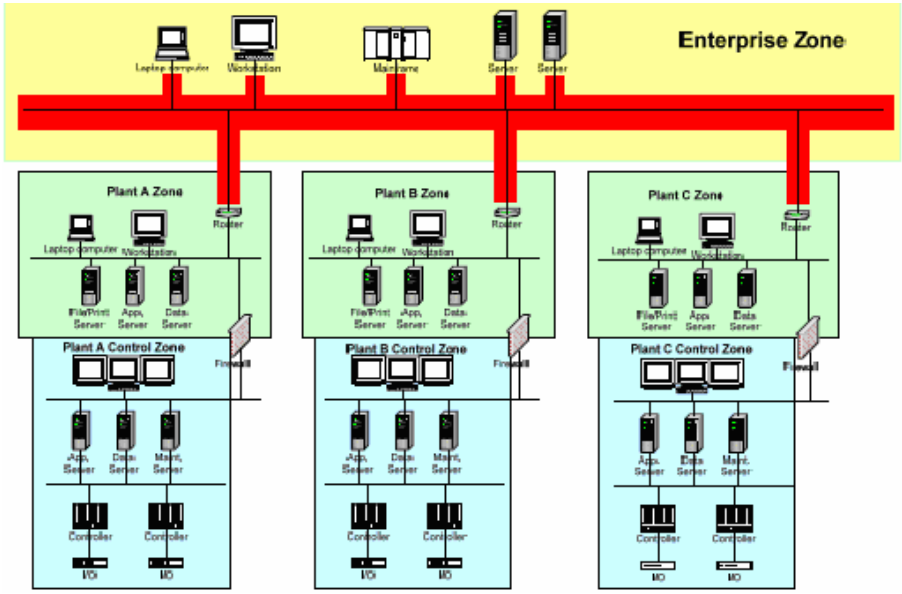

Figura 11 Conducto de la empresa

Al igual que en las zonas, una opinión similar puede ser construido para su uso en aplicaciones SCADA. Un ejemplo de ello, se muestra en la Figura 12.

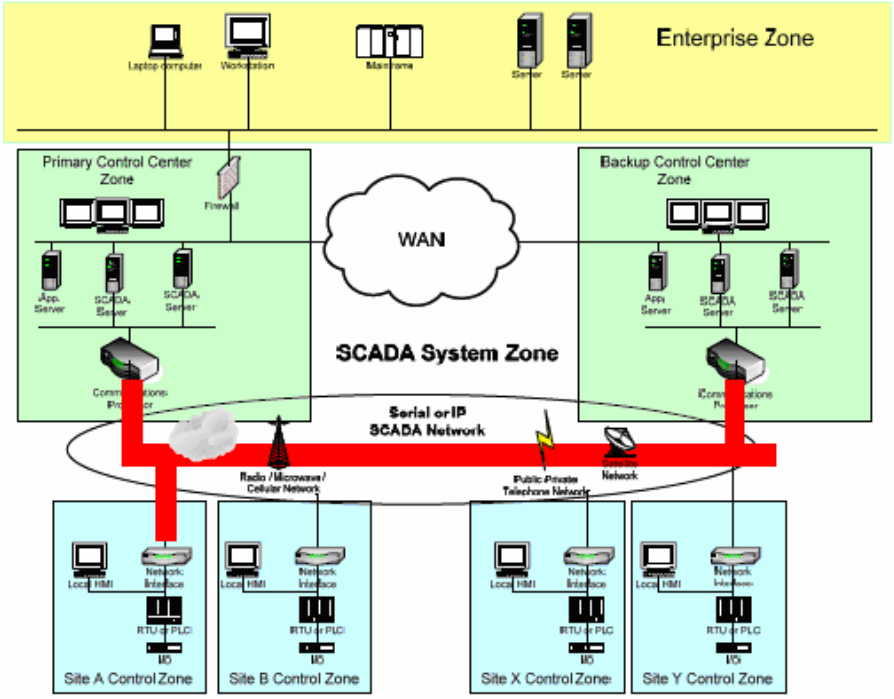

Figura 12 Ejemplo de conducto SCADA.

Al igual que una zona, cada conducto tiene un conjunto de características y requisitos de seguridad que son sus atributos.
Estos se adaptan a:

a) Políticas de Seguridad
b) Inventario de Activos
c) requisitos de acceso y controles
d) Amenazas y Vulnerabilidades
e) Las consecuencias de un fallo de seguridad
f) Autorizado Tecnologías
g) Proceso de Gestión del Cambio
h) Zonas de Conexión.

- **Políticas de Seguridad**

Cada conducto, tiene una participación de control documentos, que describe los objetivos de seguridad global y la forma de garantizar que se cumpla el nivel de seguridad.
Este documento incluye:
a) Alcance del conducto
b) Nivel de Seguridad del Conducto
c) La estructura organizativa y responsabilidades para hacer cumplir la política de seguridad del conducto
d) Los riesgos asociados con el conducto
e) La estrategia de seguridad para satisfacer los objetivos
f) las medidas de seguridad que debe ejecutarse
g) Los tipos de canales que están permitidas dentro de los conductos
h) La documentación de los atributos del conducto.

Todo lo anterior, se documentan y se combinan en el conducto. La política de seguridad se utiliza para guiar y medir la construcción y el mantenimiento de los activos que figuran en el conducto.

- **Inventario de Activos**

Al igual que ocurre con la zona de inventario, es obligatorio tener una lista exacta de las comunicaciones .

- **Requisitos de Acceso y Control**

Por su naturaleza, un conducto implica que el acceso se limita a un pequeño conjunto de todas las posibles entidades que podría tener acceso. Una política de seguridad de un conducto, debe articular el acceso necesario para el conducto y cumplir sus objetivos de negocio y cómo este acceso está controlado.

- **Evaluación de las amenazas y la vulnerabilidad**

Las amenazas y vulnerabilidades correspondientes, existen para un determinado conducto. Las organizaciones deben identificar y evaluar estas amenazas y las vulnerabilidades a fin de determinar el riesgo que causan los activos dentro del conducto para dejar de cumplir sus objetivos de negocio. El proceso de documentar las amenazas y las vulnerabilidades que sucede en la amenaza y la evaluación de la vulnerabilidad, que es parte de la política de seguridad del conducto. Muchas posibilidades, existen para reducir el riesgo de una amenaza, que explotan una vulnerabilidad determinada dentro de un de conducto. La política de seguridad debería indicar qué tipos de contramedidas son apropiadas frente al riesgo.

- **Tecnología Autorizada**

Como la automatización industrial y sistemas de control, evolucionan para satisfacer necesidades empresariales en constante cambio, la tecnología sirve para aplicar los cambios debe ser controlada. Cada una de las tecnologías utilizadas en estos sistemas, trae consigo un conjunto de vulnerabilidades y riesgos correspondientes. Para reducir al mínimo los riesgos para un determinado conducto, la política de seguridad debe tener, una lista dinámica de las tecnologías permitidas en los mismos.

- **Proceso de gestión del cambio**

Este proceso, es necesario para mantener la precisión de un conducto de la política y cómo se realicen cambios. Un proceso formal, garantiza que los cambios y adiciones a los conductos, no comprometen la seguridad de objetivos. Además, una manera de adaptarse a las nuevas amenazas a la seguridad y los objetivos requeridos. Las amenazas y las vulnerabilidades, con sus riesgos asociados, va a cambiar con el tiempo

- **Zonas de Conexión**

Un conducto, también puede ser descrito en términos de las zonas a las que está conectado.

6.6 Modelo de Relaciones

Los modelos descritos en las páginas anteriores están relacionados entre sí, así como las políticas, procedimientos, y directrices que componen un programa de seguridad. Estas relaciones se muestran en el siguiente diagrama.

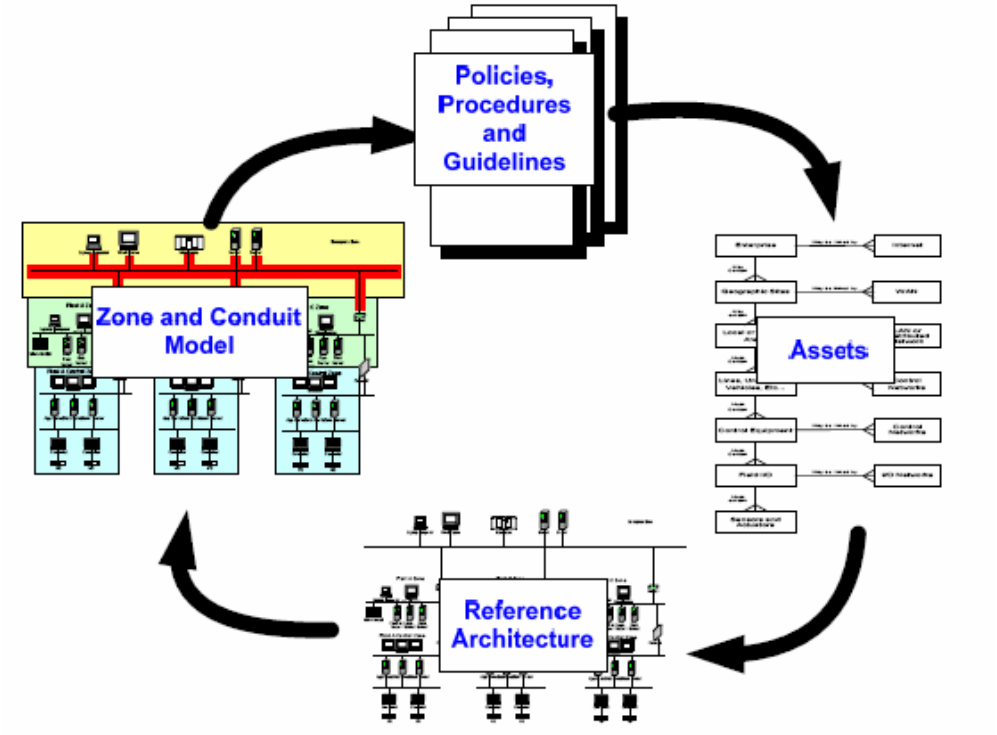

Figura 13 Relaciones de lo Modelos

Más información detallada sobre el proceso de elaboración de dicho programa se dirige a la parte 2 estándar ISA99 en la serie, "El establecimiento de un Industrial Automatización y Control de Sistemas de Seguridad Programa."

7. DIFERENCIAS DE LA SEGURIDAD ENTRE LOS SISTEMAS TI Y SISTEMAS DE CONTROL

7.1 LOS RIESGOS

Sistemas TI: Pérdida de datos e información, archivos y documentos, causando retrasos de transacciones y afectan a la empresa (**recursos, tiempo, dinero**),…

Sistemas de control: además de lo previsto por sistemas informáticos, los sistemas de seguridad no pueden afectar la integridad física de las personas (salud, accidentes de trabajo, riesgo ambiental) y sobre la conservación de plantas de producción y de las elementos (recursos, tiempo, dinero, Maquinaria)

7.2 LA ARQUITECTURA DE LA RED

Sistemas TI: normalment, la arquitectura es cliente-servidor, con especial gestión de la red en puntos críticos (sólo el servidor)

Sistemas de control: Los mismos "clientes" son los "Server" de datos críticos y en tiempo-real distribuidos en la red (Variables/DCS, PLC, SCADA/MHI, CNC, DNC, etc.)

7.3 LOS REQUISITOS DE DISPONIBILIDAD

Sistemas TI: actividades más intensas, en horario normales de oficina y la posibilidad de detener y/o "re-arrancar " por un eventual mantenimiento y reparación (salvo, obviamente como en línea sistemas bancarios o el comercio electrónico).

Sistemas de control: en muchos casos, siempre activos 24/24 horas, 7/7 días de la semana, en plantas de producción continua o de segunda rondas y lotes de producción. Detener los sistemas, no es posible sin parar la producción.

7.4 CONSECUENCIAS EN LAS SITUACIONES DIFÍCILES DE PREDECIR.

Sistemas TI: para los sistemas TI, las consecuencias negativas son limitados, en la gran mayoría de los casos, la información.

Sistemas de control: Las consecuencias dependen del proceso controlado. Todas las funciones deben ser establecidas, para no agregar vulnerabilidad al sistema y el proceso (véase el punto 1 sobre el riesgo)

7.5 MOMENTOS CRÍTICOS PARA LA INTERACCIÓN.

Sistemas TI: en situaciones de emergencia hay procedimientos para la salvaguardar los datos, el cierre de las aplicaciones, el apagado de los sistemas.…

Sistemas de control: las reacciones en situaciones de emergencia deben ser rápidas y eficaces. La información crítica debe ser actualizada bajo la supervisión de los operadores; a veces no hay tiempo para pedir autorización o autenticación de contraseñas.

7.6 LOS TIEMPOS DE RESPUESTA NECESARIA Y EL TRÁFICO DE RED

Sistemas TI: La lentitud y el rendimiento de la red son previsibles y a menudo no son críticos. Las comunicaciones en tiempo real son una excepción, pero el ancho de banda es a menudo un recurso escaso.

Sistemas de Control no son aceptables, las demoras en el tren impulsos, en el reconocimiento de los datos de sensores y controladores. Los tramos de datos son cortos y

frecuentes. A menudo no es necesario un alto "rendimiento" de la red, pero es necesario para garantizar el cumplimiento

7.7 EL SOFTWARE DEL SISTEMA SON DIFERENTES.

Sistemas TI: El software del sistema y los sistemas operativos (Windows, UNIX, Linux), son conocidos y probados, generalmente controlados y actualizado para actividades de administración normal de informática.

Sistemas de control: Los sistemas operativos, pueden ser diferentes (a veces también los mismos sistemas TI), pero son utilizados en forma diferente: las reglas habituales en el mundo TI, con frecuencia no son posible. Por ejemplo: ¿Que el sistema operativo o tarjeta de red tienen un PLC o un DCS? Además la habilidad de las personas es diferente de personal de TI, así como la conciencia y capacitación sobre redes y sistemas.

7.8-LIMITACIONES DE HARDWARE Y SOFTWARE RECURSOS.

Sistemas TI: TI define las necesidades de hardware y software de los sistemas y administra el mantenimiento y la actualización, según las normas y procedimientos de seguridad informática.

Sistemas de control: a menudo hardware y software son "especiales" y acoplados como un todo al sistema. No se puede actualizar el uno o el otro según lo pida seguridad informática. Un cambio sólo en uno de los componentes, como un PC, puede garantizar poner fin al sistema.

7.9 INTEGRIDAD DE LOS DATOS E INFORMACIÓN.

Sistemas TI: La mayor parte de los datos críticos, están en el servidor y defendibles según las "reglas de la “CID” (Confidencialidad, integridad, disponibilidad), con las oportunas medidas por ahora codificadas.

Sistemas de control: los datos e información, provienen directamente de sensores, controladores y subsistemas, su integridad es esencial y muchas veces no controlable. Se necesitan precauciones específicas para eliminar cualquier posible fuente de corrupción de los datos y detección de intrusos.

7.10 LAS COMUNICACIONES

Sistemas TI: los protocolos y los medios de comunicación son usualmente conocidos y vinculados a los estándares de uso universal en el mundo TI (TCP/IP, etc.)

Sistemas de control: Los protocolos, y los medios de comunicación son diferentes, a veces propietarios o específicos para la aplicación: redes entre PLC, DCS, CNC/DNC, las comunicaciones seriales asíncronas con RTU, con enlaces también vía radio, teléfono y bus/redes dedicadas.

7.11 ACTUALIZACIONES DE SOFTWARE (PARCHE).

Sistemas TI: Existe algunas prácticas probadas, para el censo de actualizaciones de software (del sistema o aplicaciones), de los ensayos de mejoras en ambientes de prueba y la instalación de los sistemas productivos, en los momentos de baja utilización. Los sistemas, raramente están sujetos a la reglamentación y validaciones externas.

Sistemas de control: la gestión del parche puede ser muy compleja y por lo tanto a menudo sistemas son "congelados" no actualizado. Es difícil para instalar parche de software del sistema o aplicación; en primer lugar, se necesita una prueba completa de cada

componente para verificar el impacto con otros componentes y módulos del sistema, y en aplicaciones en sectores reglamentados, comprobar guiones de la validación de los sistemas.

8. ESQUEMAS DE SEGURIDAD PARA INTEGRACION

8.1 Por qué uso Firewall para proteger y redes de control sistemas SCADA/DCS?

El Firewall puede ayudar a reducir los riesgos de acceso no autorizado (o de tráfico de red no previstos y/o autorizado) a la RCP y a los componentes de la red y sistemas SCADA y DCS.

Aquí algunos de los objetivos de una estrategia para reducir esos riesgos:

• Eliminar las conexiones directas desde Intranet es y de la red de empresa para controlar y a RCP sistemas SCADA y DCS y viceversa.

• Restringir el acceso al control de la red RCP a los usuarios de la empresa por la red empresarial.

• Hacer más fácil (pero sólo a los usuarios autorizados y autenticados) el acceso por la red empresarial, a la red datos, provienen de la red de control RCP y residentes en el servidor de históricos y servidores Web.

• Acceso abierto remota (para el mantenimiento y/o supervisión) en una forma controlada y sólo a los usuarios autorizados y autenticados.

• si tiene dispositivos inalámbricos, establecer conexiones seguras que no se abren vulnerabilidad frente a la red de control existentes PNC.

• establecer normas para todo el tráfico permitido en red de control PNC

• supervisar el tráfico para impedir acceso no autorizado y el tráfico no quiso sobre el control de la red PNC.

• para establecer conexiones seguras incluso para la gestión de Firewall.

Estas son algunas de las típicas arquitecturas para la segmentación de PNC y sus redes de control segregación por red corporativa es por dispositivos Firewall

8.2 Utilización de Firewall a dos puertos entre la red de control PCN (Proceso Control Network) y la red de la empresa RE (Enterprise Network)

Al proporcionar el uso de un Firewall básico con dos puertos entre la red de la empresa RE y la red de control, podemos ayudar a mejorar la seguridad de las aplicaciones en la fábrica. Muchos Firewall en el mercado ofrecen lo llamado "estado de inspección" para todos los paquetes TCP con la adición de los servicios de Proxy para la protocolos más comunes utilizados en la capa de aplicación tales como ftp, http y SMTP. Si el Firewall está instalado y configurado de forma "agresiva" (limitando así la mayoría de estos protocolos) podemos reducir la posibilidad de que halla un ataque exitoso desde fuera de la red de control RCP. Muchas empresas utilizan esta configuración como estándar para la protección de sistemas SCADA, DCS y RCP

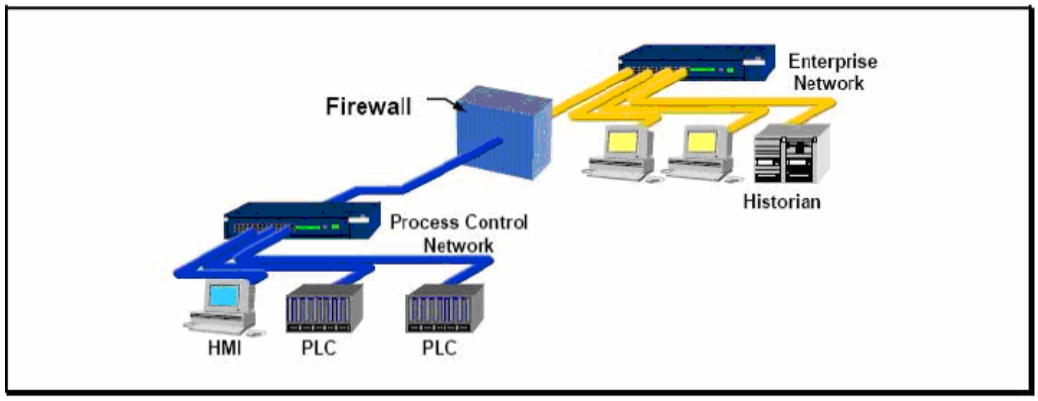

Figura 14 Utilización de Firewall a dos puertos entre la red de control PCN (Proceso Control Network) y la red de la empresa RE (Enterprise Network)

El uso de esta arquitectura de Firewall con dos puertos entre la red de control y la red de la empresa, aunque es una buena elección de protección, exige que existan normas para abrir canales directos de la comunicación entre los dos redes, y esto podría ser riesgoso. Es necesario proporcionar un diseño exacto, la configuración de la red y una supervisión posterior precisa de las anomalías para reducir cualquier riesgo de ataque.

8.3 Separación de la red RCP de RE mediante una combinación de Router y Firewall

Una Configuración un poco más sofisticada que la anterior, se obtiene combinando la funcionalidad del router y del Firewall juntos, donde el router está presente antes que el Firewall y realizar algunos servicios básicos para filtrado de paquetes, mientras que el Firewall administra lo más complejo, utilizando la técnica de estado de inspección o por Proxy.

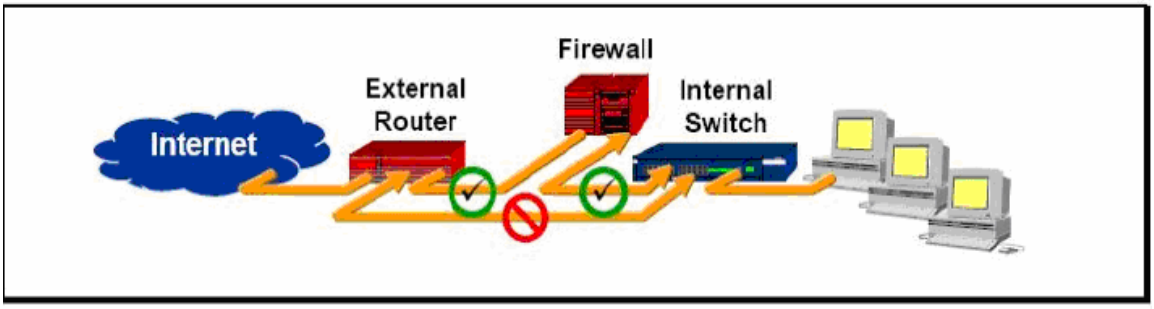

Figura 15 Separación de la red RCP de RE mediante una combinación de Router y Firewall

Esta configuración se presenta cuando se está conectado directamente a Internet, precisamente porque el router es capaz de manejar de forma rápida, grandes volúmenes de paquetes de entrada, especialmente en el caso de los ataques a DOS (denegación de servicio), y por lo tanto reduce la carga del Firewall.

8.4 Firewall con zona desmilitarizada (DMZ) entre la red de control RCP y la red empresa RE.

Una considerable mejora es el caso con el uso de firewall que puede manejar uno o más zona DMZ (zonas desmilitarizada) entre la red de control (RCP) y la red de la empresa (RE).

La DMZ zona desmilitarizada comprende, por ejemplo, el servidor de históricos y servidores Web/Terminal servidor, una base de datos y/o una intranet servidor, un punto de acceso a la red inalámbrica, un punto de acceso está reservado al exterior soporte (remotas), etc.

De hecho, el uso de Firewall con capacidad para segmento y debería algunos zona desmilitarizada, permite la creación de zonas intermedias de la red, que a menudo son identificados como proceso red de información (PIN). Para crear una zona desmilitarizada es necesario que el Firewall tenga tres o más puertos: un típico Firewall básico tiene una interfaz para el exterior (pública) y un hacia adentro (privado).

Para crear distintas zona desmilitarizada, por uno de los puertos está la red corporativa (RE), a un segundo puerto está conectada con la red control SCADA, PLC, DCS, etc. (RCP), mientras que los puertos restantes se conecta la zona desmilitarizada con un servidor de históricos y servidores Web/Terminal servidor, dispositivos "seguros", puntos de acceso inalámbricos, etc. la figura de abajo muestra una configuración típica con red de control zona desmilitarizada entre RCP y red corporativa RE.

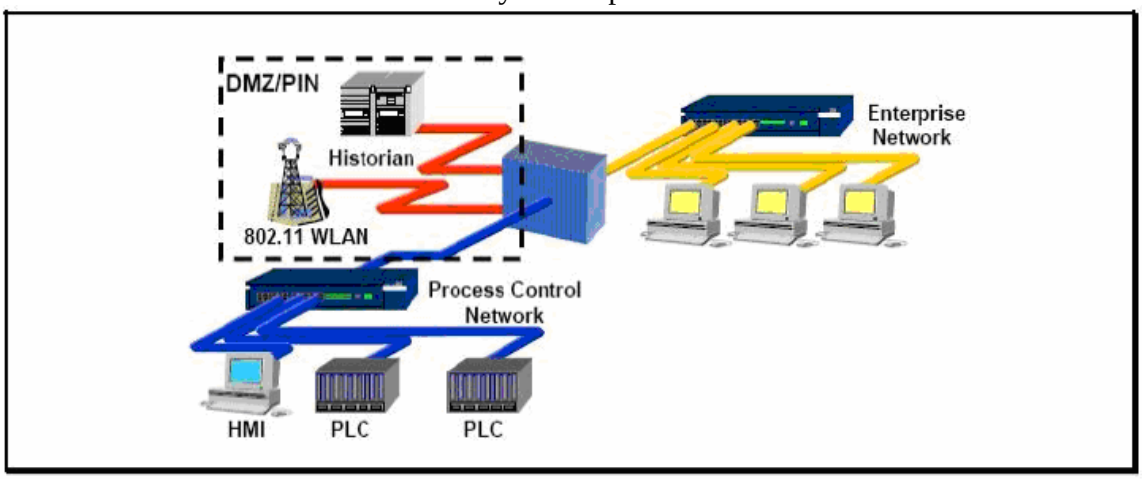

Figura 16 Firewall con zona desmilitarizada (DMZ) entre la red de control RCP y la red empresa RE.

Al adoptar ciertos criterios de la política de seguridad de la organización, se puede definir una lista de control de acceso ACL con una clara delimitación, de los usuarios y los dispositivos de RCP y todos los demás segmentos de la red, con una estrecha supervisión o incluso una prohibición de paso para tráfico a RCP, procedentes de otras zonas.

8.5 Un Par de Firewall en serie entre la red de control RCP y la RED de la empresa RE.

Una variante de configuración anterior (Firewall multipuesto forma una DMZ entre la red de control RCP y red corporativa RE) el uso de un par de Firewall situados entre la red de la empresa RE y red de control RCP, crean una zona desmilitarizada entre las dos redes, donde se encuentran los servidores que serán utilizados en común por los usuarios de los dos redes. Los computadores en esta zona desmilitarizada son generalmente los servidores.

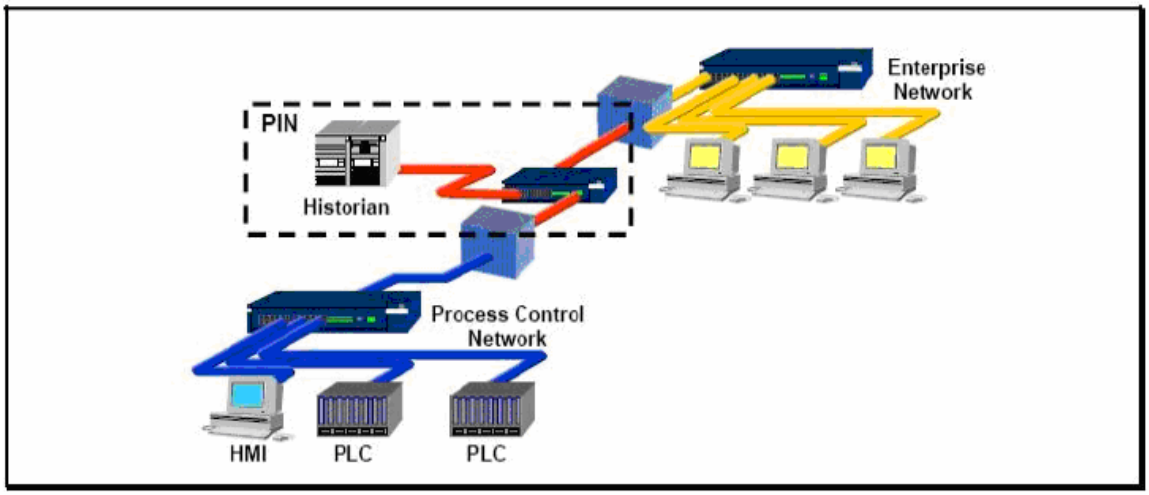

Figura 17 Par de Firewall en serie entre la red de control RCP y la RED de la empresa RE.

Esta configuración permite también a separar claramente la administración por parte del personal de automatización y de las personas que administran la parte TI (tecnologías de la información): en realidad, cada grupo podría administrar su "propio" Firewall que define su propia red y por lo tanto sus fronteras. Esta modelo es recomendado por Ferc USA (Federal Energía Comisión Reguladora) En su documento "propuesta de normas de seguridad".

8.6-Combinación con Firewall y redes de control RCP sobre la base de V-LAN

Hasta ahora hemos analizado situaciones en las que hemos hablado redes de control RCP/SCADA como entidades individuales. Hay muchos casos en que se definen las áreas funcionales, plantas, control células, cada uno con sistemas dedicados RCP o SCADA y donde es necesario tener una comunicación entre los diferentes segmentos de la red, manteniendo la necesidad de cada uno de los dispositivos de estos segmentos puede combinar datos disponibles para el servidor y la concentración de la información de diferentes zonas de las plantas.

para ampliar las arquitecturas que hemos visto hasta ahora con una nueva segmentación de las redes SCADA y RCP en diferentes sub-redes VLAN, podemos controlar y permitir todas las comunicaciones entre las diferentes VLAN utilizando un switch capa-3 con un simple filtrado de paquetes. Bajo el switch de capa-3 hay una serie de switches de capa-2 con estandar 802.Q VLAN, permitiendo que la comunicación directa entre todos los dispositivos de la misma VLAN, para forzar y regular todo el tráfico entre los diferentes VLAN hacia el switch de capa-3 configurado como filtro.

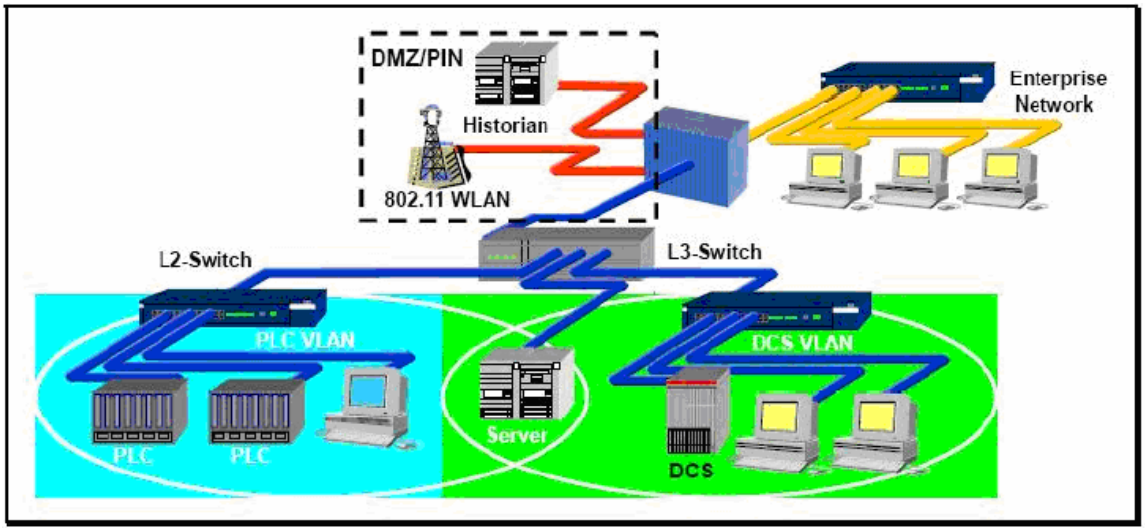

Figura 18 Combinación con Firewall y redes de control RCP sobre la base de V-LAN

Un VLAN impide la propagación del tráfico no deseados en todo el segmento de red: previene por lo tanto que un acceso no controlado desde el interior (por ejemplo un desarrollador o de otra persona con su portátil no controlado) pueda introducir un virus o otros Malware.

Los entornos de la RCP y SCADA están bien controlados y seguros gracias a que el Firewall está entre DMZ, y la red empresa RE; en este nivel pueden ser suficientes estos switches, sin tener que recurrir a sofisticados Firewall.

REFERENCIA/ BIBLIOGRAFICA

[1] NISCC, Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks, Prepared for: National Infrastructure Security Co-ordination Centre (NISCC),By the:British Columbia Institute of Technology (BCIT), Revision Number: 1.4,Document Date: 15th February 2005,INTERNET: www.cpni.gov.uk

[2] "BSQL Slammer Worm Lessons Learned For Consideration By The Electricity Sector", North American Electric Reliability Council, Princeton NJ, June 20, 2003,INTERNET: http://www.esisac.com/publicdocs/SQL_Slammer_2003.pdf

[3] Byres, E, P. Eng. Justin Lowe, "The Myths and Facts behind Cyber Security Risks for Industrial Control Systems", Research Faculty – Critical Infrastructure Security Principal Consultant, British Columbia Institute of Technology PA Consulting Group Burnaby, BC, Canada London, UK

[4] Byres, E. Chauvin, B. Karsch, J. Hoffman, D. Kube, N, "The special needs of SCADA/PCN firewalls: architectures and test results", British Columbia Inst. of Technol., Burnaby, BC, Canada; This paper appears in: Emerging Technologies and Factory Automation, 2005. ETFA 2005. 10th IEEE Conference on Publication Date: 19-22 Sept. 2005, Volume: 2, On page(s): 8 pp.- ISBN: 0-7803-9401-1, INSPEC Accession Number: 9084480, Digital Object Identifier: 10.1109/ETFA.2005.1612765, Posted online: 2006-04-03 15:37:45.0

Papers from Conference Proceedings (Published):

[5] Creery, A. Byres, E.J. "Industrial cybersecurity for power system and SCADA networks", Universal Dynamics Ltd., Richmond, BC, Canada, This paper appears in: Petroleum and Chemical Industry Conference, 2005. Industry Applications Society 52nd Annual, Publication Date: 12-14 Sept. 2005, On page(s): 303- 309, ISSN: 0090-3507, ISBN: 0-7803-9272-8, INSPEC Accession Number: 8606192, Digital Object Identifier: 10.1109/PCICON.2005.1524567, Posted online: 2005-10- 31 10:11:13.0

[6] George D. Jelatis, Joe Weiss, Information Security Primer, Helping the Energy Industry adapt to the Internet Age, without compromising operational security or operating flexibility, Prepared for EPRI, by Secure Computing Corporation

Standards:

[6] AMERICAN NATIONAL STANDARD ANSI/ISA–99.00.01–2007, Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models Approved 29 October 2007, Cap 6 Models

Agradecimientos

A Dios, que me ha permitido encontrar en la UPB el amor por mi hermosa Familia y por mi profesión. Fabio Jaimes Beleño

A Dios, que gracias a el he obtenido todos los logros que me he propuesto y a mi esposo y mi hija que son el motor de todos mis dias. Erika Rangel Castillo