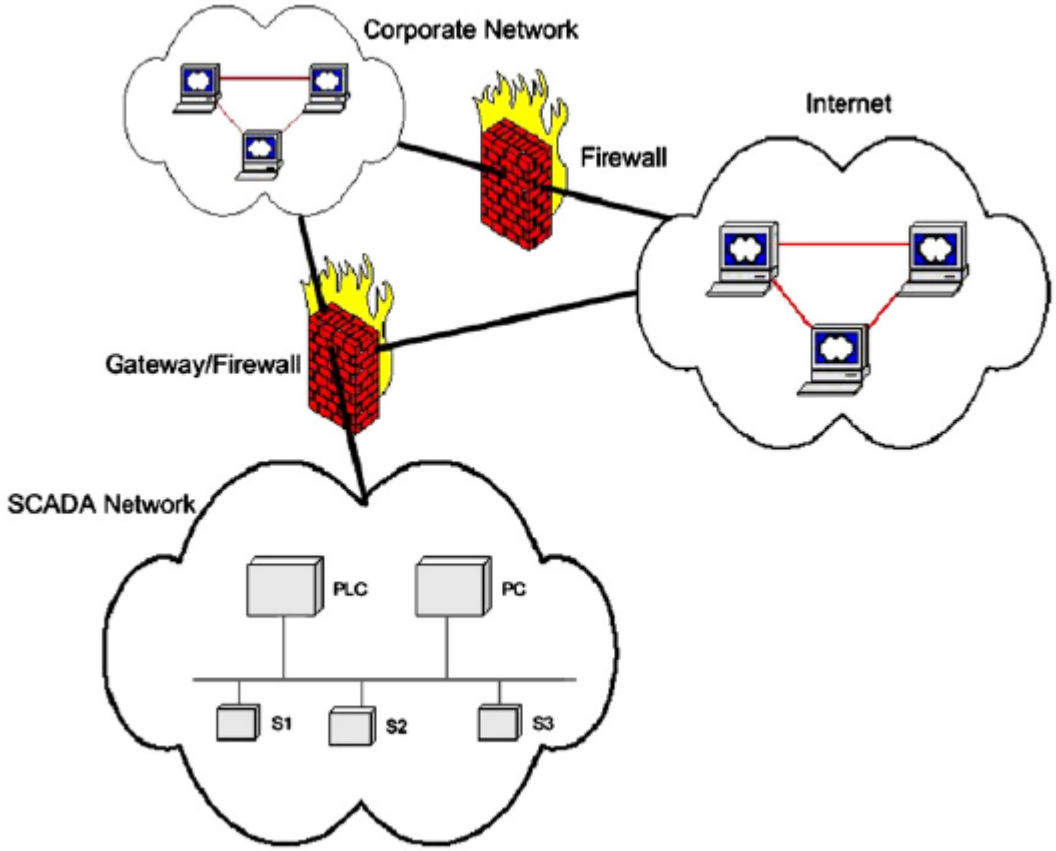
Ciber Seguridad en Redes Industriales

Jhon Jairo Padilla Aguilar, PhD.

El problema

- La conectividad expone las redes industriales críticamente seguras a una gran cantidad de problemas del Internet.
- Debido a que los procesos son monitoreados y controlados por dispositivos conectados a redes SCADA, los potenciales ataques sobre estas redes pueden causar daños significativos sobre la planta:
  - Daños físicos
  - Pérdidas económicas
  - Daños que pueden afectar el medio ambiente
  - Peligros para la seguridad pública.

Arquitectura de red SCADA típica



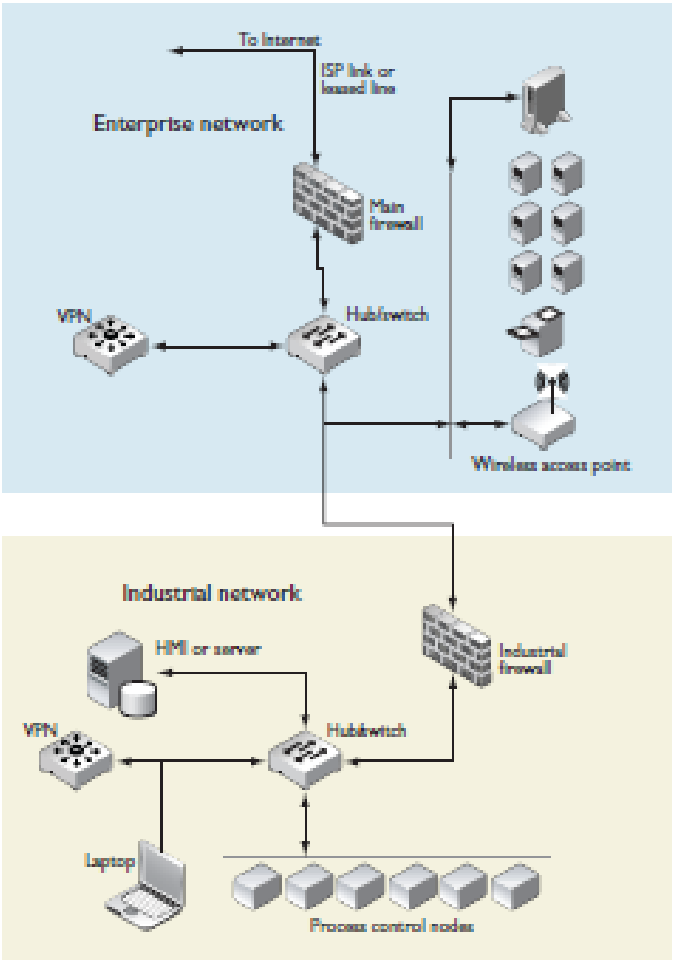
Vulnerabilidades de redes SCADA

Introducción

- Los protocolos estándares de redes industriales fueron diseñados buscando un buen rendimiento y que las tareas se hiciesen en los tiempos críticos de los procesos a controlar.
- Sin embargo, la seguridad informática estuvo lejos de estos objetivos de diseño.

Puntos de Acceso a la red

- Se partió de que las redes SCADA estarían aisladas físicamente del resto de la red de la empresa. Por tanto, los atacantes no podrían tener acceso físico.
- Sin embargo, ahora la planta de producción se encuentra interconectada a una red compleja compuesta por diferentes departamentos de la empresa.

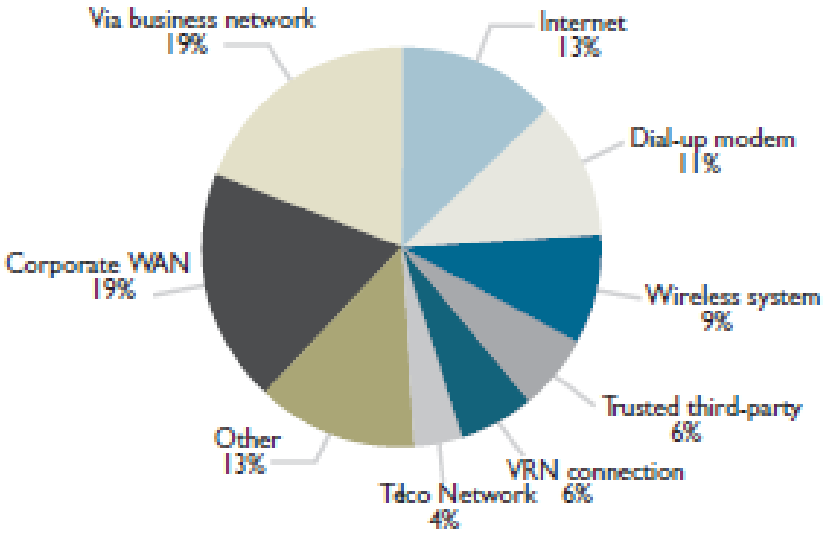


Fuente: Eric Byres,David Leversage and Nate Kube"Security incidents and trends in SCADA and process industries"

Puntos de Acceso a la red

- La interconexión a redes complejas hace que haya múltiples puntos de acceso a la red SCADA (ya no se puede garantizar el aislamiento físico):
  - Líneas telefónicas
  - Intranet
  - Canal de Internet
  - Etc.

Fig. 5. Remote points of entry charted as a percentage from 2002 to 2006(47 records)



Fuente: Eric Byres,David Leversage and Nate Kube"Security incidents and trends in SCADA and process industries"

Crecimiento de los ciber-ataques

- Un atacante decidido, podría utilizar cualquiera de estos puntos de acceso y ganar el acceso a máquinas dentro de la red de producción

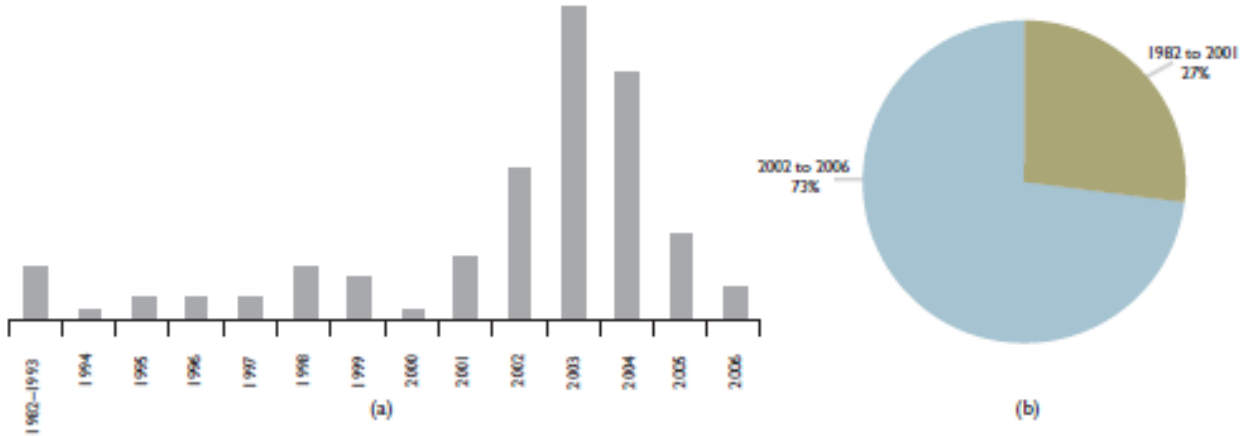


Fig. 1. Incident events by date from 1982 to June 1, 2006: (a) graphed as a frequency distribution; (b) charted as a percentage (105 records)

Fuente: Eric Byres,David Leversage and Nate Kube"Security incidents and trends in SCADA and process industries"

Crecimiento de los ciber-ataques

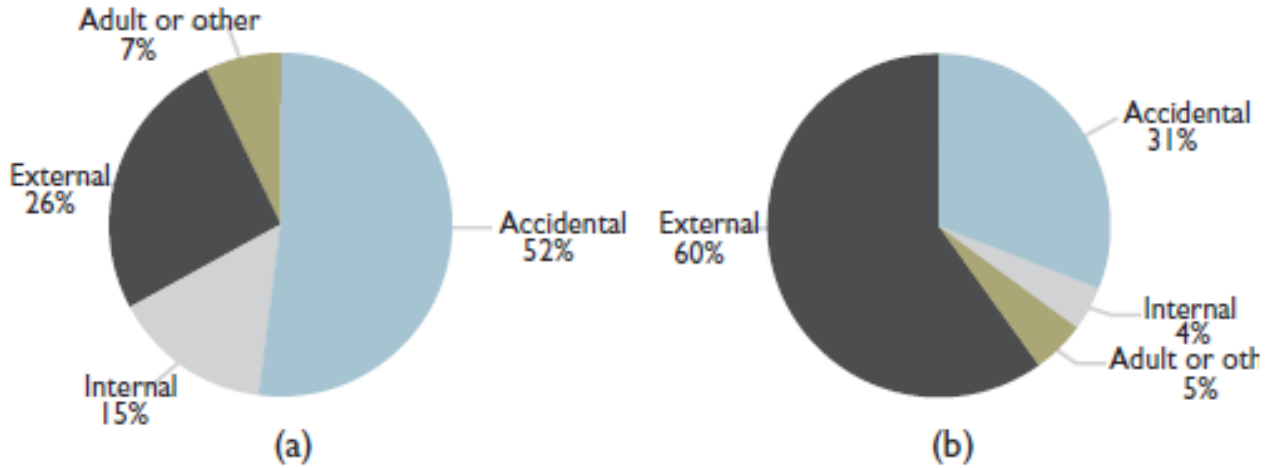


Fig. 3. (a) Incident types percentage charted as a from 1982 to 2001 (27 records); and (b) Incident types from 2002 to June 2006 (78 records)

Fuente: Eric Byres,David Leversage and Nate Kube"Security incidents and trends in SCADA and process industries"

Uso de estándares abiertos

- El uso de estándares abiertos para los protocolos hace que un atacante pueda tener profundo conocimiento de la operación de las redes SCADA.
- El uso de hardware y software comercial y de dominio público (COTS) para desarrollo de dispositivos de red:
  - Reduce el tiempo de desarrollo
  - Permite la interconexión a redes Ethernet usando la pila de protocolos TCP/IP
  - Pero compromete la seguridad de la red.
- Los dispositivos en red son diseñados para ser seguros ante fallos, pero los mecanismos de seguridad ante fallos pueden ser anulados por un atacante.

Uso de Interfaces Web

- La información viaja sobre la pila de protocolos TCP/IP
- Los protocolos de control son transportados sobre paquetes TCP
- Los protocolos de comunicaciones industriales se ven obligados a abandonar su filosofía de operación de tipo Maestro/Esclavo
- En este entorno los dispositivos de control poseen otras aplicaciones más allá del envío de mensajes de control (aplicaciones que permiten la gestión de alto nivel).
- Todo esto hace las redes SCADA vulnerables a los ataques populares a las aplicaciones y a los protocolos TCP/IP

Consecuencias de los ciber-ataques

- Pérdidas en la capacidad de producción
- Pérdidas financieras
- Pérdida de vidas

Tipos de ciber-ataques

- Integridad
- Confidencialidad
- Autenticación
- Disponibilidad

Ataques a la Confidencialidad

- Las redes industriales no soportan cifrado (Encripción) de los datos
- Un atacante puede usar un Sniffer (programa para escuchar lo que pasa por un segmento de la red)
- El atacante puede aprender sobre los datos y los mensajes de control
- Esta información podría usarse para enviar mensajes falsos posteriormente
- Las vulnerabilidades en sistemas operativos de los dispositivos pueden permitir que se implante código malicioso
- El código malicioso podría permitir a los atacantes acceso no permitido a la red y causar otros daños.

Ataques a la Disponibilidad

- El atacante puede cambiar señales de control y causar malos funcionamientos de los dispositivos
- Esto podría afectar la disponibilidad de la red
- Se pueden bloquear o re-enrutar comunicaciones para causar ataques de denegación de servicio (DoS attacks)

Ataques a la Integridad

- Los mensajes de control podrían ser manipulados y así comprometer la integridad
- Podrían atacarse las bases de datos
- Con un acceso no autenticado, el atacante podría cambiar los Set Points (las referencias):
  - Esto podría causar que fallen ciertos dispositivos en un valor de umbral muy bajo
  - Podría hacer que se dispare una alarma cuando no debe
  - Podría hacer que se apague una alarma en rangos de señal que son peligrosos y que el operador humano no se entere.
  - Esto haría que se retrasen las acciones de control para las alarmas en una emergencia, lo que podría afectar la seguridad de las personas en la vecindad de la planta.

Desafíos para la investigación en redes SCADA

Desafíos

- *Mejorar los controles de Acceso:* La idea es endurecer los controles para evitar accesos no autorizados
- *Mejorar la seguridad interna de la red SCADA:* Si un atacante logra penetrar la red SCADA, debe dificultársele llevar a cabo cualquier otro tipo de ataque.
- *Desarrollar herramientas de monitoreo de seguridad eficiente:* Estas herramientas ayudan a la detección de intrusos y otras actividades sospechosas en la red.
- *Mejorar la gestión de la seguridad en la red SCADA.*
- Deben tenerse en cuenta las características propias de redes FieldBus (buses de campo).

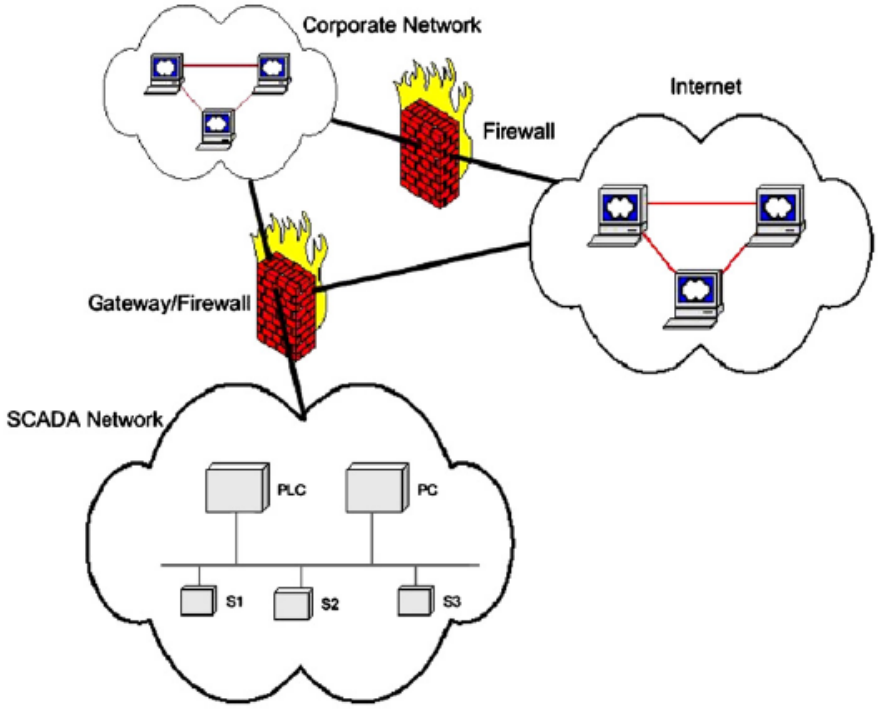
Características de las redes Fieldbus

- Velocidades de transmisión bajas
- Paquetes pequeños para los mensajes
- Requerimientos de operación en tiempo real

Mecanismos de Seguridad en redes SCADA

Control de Acceso

- Se debe asegurar que entidades no autorizadas no tengan acceso a la red
- El primer tropiezo es la dificultad en definir el perímetro de la red SCADA
- Muchas veces se usan Gateways con capacidades de Firewall para interconectar la red SCADA al segmento de red corporativa o a Internet.



Control de Acceso

- Además de los dispositivos tecnológicos para el control de acceso, debe contarse con:
  - Políticas de seguridad de la compañía
  - Buenas prácticas de gestión de la seguridad
- Algunos Gateways no proveen mecanismos de seguridad
- Los Firewalls deben permitir diferentes protocolos SCADA.

Mecanismos de prevención de accesos no autorizados

- Autenticación de usuarios basada en password:
  - Vulnerable a ataques de ingeniería social
  - Uso de passwords inseguros y fáciles de crackear
- Se pueden usar tarjetas inteligentes (Smart Cards):
  - Pueden almacenar los password de manera segura
  - Ayudan a mejorar la gestión de claves de la red
  - No resuelven completamente el problema de autenticación

Firewalls y sistemas de detección de intrusos

- *Función básica del Firewall:* prevenir accesos no autorizados a la red SCADA a través de conexiones directas por el enlace de Internet o la red corporativa de la empresa.
- Los Firewalls pueden configurarse para:
  - Permitir el ingreso de sólo ciertas clases de protocolos (p.ej. Profibus)
  - Monitorear y controlar las actividades de entidades autorizadas para acceder a la red.
  - Autorizar a ciertas entidades para tener acceso sólo a ciertos servicios de la red SCADA. El Firewall puede asegurar que estas entidades no den mal uso a sus permisos.

Arquitectura de red (recomendación del NISCC, 2005)

- Debe dividirse la red en 3 zonas separadas físicamente y lógicamente:
  - Red SCADA o de control de procesos
  - Red corporativa
  - Zona desmilitarizada (DMZ) como buffer entre las otras dos zonas.

Firewalls en la práctica

- Hay pocos Firewalls que detectan protocolos SCADA.
- Cisco desarrolló un Firewall open-source basado en Linux capaz de filtrar paquetes MODBUS (en la herramienta netfilter)
- Se han desarrollado micro-firewalls que pueden embeberse en los dispositivos SCADA:
  - Pueden configurarse para reconocer sólo el tráfico relevante al dispositivo y bloquear todo tráfico sospechoso
  - El problema es que muchos dispositivos SCADA no tienen suficiente capacidad computacional para soportar los firewalls embebidos.
  - Deben primero identificarse cuáles dispositivos de la red SCADA pueden beneficiarse de los micro-firewalls.

IDS (Intrusion Detection Systems)

- Por lo general complementan los Firewalls
- El problema es que los IDS comerciales no tienen capacidad de detección de comportamientos sospechosos con protocolos SCADA
- Los IDS requieren el conocimiento de las vulnerabilidades en los protocolos SCADA.
- Debe hacerse un estudio completo de estas vulnerabilidades.

Análisis de vulnerabilidades de los Protocolos

Introducción

- Los protocolos SCADA actuales son estándares bien establecidos y gestionados por entidades internacionales de estandarización
- La incorporación de cambios en los protocolos SCADA puede ser un proceso muy lento debido a la resistencia a la alteración de los estándares.
- La comprensión de las vulnerabilidades de los protocolos SCADA permite el desarrollo de sistemas IDS: Se pueden desarrollar perfiles de los ataques.

Tipos de vulnerabilidades en los protocolos

- Inherentes a la especificación misma del protocolo
- Debidas a la Implementación inapropiada del protocolo

- No hay metodologías para realizar estudios de vulnerabilidades de protocolos SCADA
- Un paso interesante es desarrollar una taxonomía de las vulnerabilidades

Criptografía y gestion de claves

- Los protocolos SCADA no realizan ningún tipo de criptografía
- Limitantes para hacer criptografía en protocolos SCADA:
  - Capacidades computacionales limitadas de los dispositivos SCADA
  - Velocidades de transmisión de datos bajas
  - Necesidad de respuesta en tiempo real de los dispositivos
- Estos limitantes impiden que se haga una criptografía compleja
- Sin embargo, se podrían aplicar técnicas criptográficas usadas en redes de Sensores Inalámbricos (WSNs)

Criptografía

- Estándar AGA-12: (American Gas Association)
  - Provee una revisión de los problemas para hacer criptografía en redes SCADA
  - Propone una técnica denominada Retrofit Criptography para los enlaces seriales SCADA.
  - Esta técnica provee aseguramiento de la integridad de los mensajes SCADA y a la vez mantiene el rendimiento de la red SCADA.
  - Position Embedded Criptography:
    - Un mensaje SCADA se compone de varios paquetes
    - El transmisor asigna un número de posición a cada paquete dentro del mensaje SCADA.
    - Luego se encripta cada paquete con su número de posición y la posición del paquete anterior
    - Así, se dificulta al atacante insertar paquetes maliciosos en el mensaje SCADA.
    - Se protege la integridad de los mensajes en la red SCADA

Criptografía y gestión de claves

- Se requiere de un método de distribución de etiquetas (es un problema abierto en redes SCADA)
- Desafíos de las redes SCADA:
  - En redes como las eléctricas o las redes de distribución de combustibles, muchos dispositivos permanecen en campo abierto, lo que dificulta el almacenamiento seguro de las claves.

Seguridad de los dispositivos y el Sistema Operativo

- Muchos dispositivos en redes SCADA corren Sistemas Operativos de tiempo real (RTOS)
- Los RTOS son más susceptibles a ataques de Denegación de Servicio (DoS) ya que cualquier retraso en una respuesta puede ser grave.
- Se deben realizar estudios de vulnerabilidad de los RTOS
- También se debe estudiar la interacción entre los RTOS y los dispositivos COTS (abiertos y comerciales)

Seguridad de los dispositivos y el Sistema Operativo

- En redes con muchos nodos (p.ej. Redes de distribución de energía eléctrica) no es práctico proteger todos los nodos. Muchos pueden ser manipulados.
- Podrían construirse dispositivos que tengan protección física contra manipulación (Envolturas especiales). Estos pueden ser muy costosos.
- Se deben desarrollar procedimientos para sobrevivir a un ataque de unos pocos dispositivos comprometidos. Uso de criptografía.

Gestión de la Seguridad

- Las compañías deben definir un conjunto de objetivos de seguridad en redes SCADA que vayan en congruencia con los objetivos del negocio de la empresa.
- Estos objetivos se conocen como Estructura de Control (Control Framework)
- Los objetivos pueden asegurarse con:
  - Unas buenas políticas de seguridad, seguidas de un plan de seguridad y guías de implantación de las mismas.

Gestión de la Seguridad

- La seguridad es un proceso continuo que no termina con la implantación de las tecnologías de seguridad
- Una red SCADA debe ser monitoreada constantemente en busca de vulnerabilidades
- El SW y el HW debe ser actualizado constantemente y asegurado con los últimos parches.
- Debe hacerse una auditoría regular en que se paga a terceros para descubrir vulnerabilidades y malas prácticas. Los auditores deben ser entidades de confianza (esto es delicado y genera controversia).

Estandarización

- Entidades de estandarización de seguridad informática en redes SCADA:
  - ISA: Instrumentation Systems and Automation Society
  - NIST: National Institute for Standards and Technology
  - OPC Foundation
  - AGA: American Gas Association
  - NISC (UK government)
  - IEEE Power Engineering Society (PES)
  - EPRI: Electric Power Research Institute