PROPUESTA DE GESTIÓN DE RIESGOS PARA SCADA EN SISTEMAS ELÉCTRICOS

María J. Bernal Zuluaga
Central Hidroeléctrica de Caldas SA. Manizales
mjbernalz@yahoo.com

Diego F. Jimenez Mendoza
Universidad de San Buenaventura, Medellín
diegof.jimenez@gmail.com

(Tipo de Artículo: **Investigación**. Recibido el 14/10/2012. Aprobado el 11/12/2012)

RESUMEN
En la actualidad los ataques cibernéticos son uno de los principales aspectos a considerar por parte de los entes gubernamentales y por las empresas prestadoras de servicios públicos, dado que dichas entidades son el blanco preferido para desestabilizar el normal desempeño de las actividades de un sector determinado. En particular, la prestación del servicio eléctrico es fundamental para la operación de la mayor parte de las actividades diarias a nivel comercial, industrial y social de nuestro país.

Los centros de control eléctricos cuentan con el Sistema SCADA para tener información en tiempo real que facilite la supervisión, control y toma de decisiones necesarias para garantizar la seguridad y calidad en la prestación del servicio eléctrico.

Este artículo trata de la gestión de riesgos del sistema SCADA y la definición de un plan de tratamiento en el cual se exponen las medidas de control que deben ser implementadas para la mitigación de los riesgos a los cuales está expuesto dicho sistema.

Palabras clave
Front End, HMI, Protocolo, RTU/IED, SCADA, Sistema Eléctrico.

RISK MANAGEMENT PROPOSAL FOR SCADA IN ELECTRICAL SYSTEMS

ABSTRACT
Nowadays cyber-attacks are one of the major concerns to be considered by government agencies and utilities because they are sensitive targets in order to disrupt the normal performance of the activities of a particular sector. One of the most important services is electricity because of its crucial role for commercial, industrial and social activities in our country.

In order to have real time information that make easier supervision, control and decision making for ensuring safety and quality in the provision of electricity service, the control centers have the SCADA system (Supervisory Control And Data Acquisition).

This article deals with risk management of the SCADA system and the definition of a treatment plan which proposes control measures that should be implemented in order to minimize the risks and attacks for the system.

Keywords
Front End, HMI, Protocol, RTU/IED, SCADA, Electric System.

UNE PROPOSITION DE GESTION DE RISQUES POUR SCADA DANS SYSTÈMES ÉLECTRIQUES

Résumé
Aujourd'hui les attaques cybernétiques sont une des aspects essentiels à considérer par les organismes gouvernementaux et par les services publics, étant donné que ces organismes sont un point de mire pour déstabiliser la performance normal des activités d'un secteur particulier. De manière ponctuelle, le service électrique est fondamental pour le fonctionnement de la plupart des activités quotidiennes à l'échelle commercial, industrielle et social de notre pays.

Les centres de contrôle électrique ont le système SCADA pour avoir information en temps réel pour faciliter la surveillance, le contrôle et la prise des décisions nécessaires pour garantir la sécurité et qualité dans les services publics.

Cet article s'occupe de la gestion de risques du système SCADA et de la définition d'un plan d'un traitement dans lequel on expose les mesures de contrôle qu'on doit implémenter pour la mitigation des risques pour le système.

Mots-clés
Front-end, Interface Homme-Machine (HMI), Protocole, Unité terminale distante/Dispositif Electronique intelligent (RTU/IED), Télésurveillance et acquisition de données (SCADA), Système électrique.

1. INTRODUCCIÓN

Un Centro de control Eléctrico es el responsable de la operación y supervisión coordinada en tiempo real de las instalaciones de generación y de transporte del sistema eléctrico. Para que exista un equilibrio constante entre la demanda y la oferta de energía, se requiere realizar previsiones de demanda y mantener márgenes de generación suficientes para hacer frente a posibles cambios del consumo previsto [1].

Para cumplir con lo anterior y garantizar la seguridad y calidad del suministro eléctrico, los centros de control deben operar sin interrupción el sistema de producción y transporte de energía por medio de los Sistemas SCADA (Supervisory Control And Data Acquisition).

El sistema SCADA utiliza equipos de cómputo y tecnologías de comunicación para automatizar el monitoreo y control de procesos industriales. Estos sistemas son parte integral en la mayoría de los ambientes industriales complejos y geográficamente dispersos, ya que pueden recoger la información de una gran cantidad de fuentes muy rápidamente y presentarla al operador en una forma amigable.

La importancia de los sistemas SCADA en el control de servicios como la energía eléctrica hace que se conviertan en sistemas estratégicos o incluso en sistemas dignos de ser considerados como de seguridad nacional, ya que una falla en ellos puede acarrear consecuencias catastróficas para una región e incluso para un país, con pérdidas económicas, pérdidas de imagen, implicaciones legales y afectación ambiental, entre otras [2].

Este articulo tiene como objetivo comprender el sistema SCADA, identificar y valorar los activos de información que lo componen y proponer una gestión de riesgos que nos da como resultado un plan de tratamiento, en el cual se describen los controles que ayudan a prevenir, detectar y mitigar dichos riesgos.

2. SCADA Y SUS ELEMENTOS PRINCIPALES

El SCADA consiste típicamente en una colección de equipos de cómputo conectados vía LAN donde cada máquina realiza una tarea especializada, como es la recolección de datos, la visualización y así sucesivamente. Para alcanzar un nivel aceptable de tolerancia de fallas con estos sistemas, es común tener computadores SCADA redundantes operando en paralelo en el centro de control. El SCADA de los sistemas eléctricos recibe toda la información de las subestaciones, se comprueba el funcionamiento del sistema eléctrico en su conjunto y se toman las decisiones para modificarlo o corregirlo si es del caso.

Los principales elementos que componen los Sistemas SCADA son:

2.1. Remote Terminal Units (RTU´s) o Estaciones remotas o Intelligent Electronics Device (IED's)

La RTU es un pequeño y robusto computador que proporciona inteligencia en el campo para permitir que se comunique con los instrumentos. Es una unidad independiente (stand−alone) de adquisición y control de datos, cuya función es controlar el equipamiento del proceso en el sitio remoto, adquirir datos del mismo explorando las entradas de información de campo conectadas con ellos y transferirlos al sistema central SCADA [3].

Las RTU's tienen la capacidad de comunicarse por radio, microonda, satélite, fibra óptica, etc., y algunos estándares de comunicación han comenzado recientemente a emerger para RTU's, como son el DNP3 e IEC60870-5-104.

Las RTU´s han evolucionado a IED´s que corresponden a dispositivos electrónicos inteligentes capaces de supervisar y controlar procesos con funciones de Interfaz ser humano y máquina (HMI) y comunicación a sistemas superiores, es decir, sistemas SCADA sobre los estándares de comunicación mencionados.

Entre los elementos que las RTU's/IED's supervisan a nivel eléctrico son:

- Transformador de potencia
- Interruptor
- Seccionador
- Transformador de potencial
- Transformador de corriente

2.2. Master Terminal Unit (MTU) o HMI en Subestaciones y en Estación Principal

La parte más visible y "centro neurálgico" del sistema es llamado Master Terminal Unit (MTU) o Interfaz ser humano y máquina (HMI − Human Machine Interface), cuyas funciones principales son recolectar datos de las RTU's o IED's, salvar los datos en una base de datos, ponerlos a disposición de los operadores en forma de gráficos, analizar los datos recogidos para ver si han ocurrido condiciones anormales, alertar al personal de operaciones sobre las mismas, generar los informes requeridos y transferir los datos hacia y desde otros sistemas corporativos.

La MTU de SCADA se puede ejecutar en la mayoría de las plataformas y su tendencia es migrar hacia estándares abiertos como ODBC, INTEL PCs, sistemas estándares de gráficos y sistemas de computación corrientes.

La mayoría de los soluciones SCADA cuentan con HMI en las subestaciones (S/E) y HMI en el Centro de Control o Estación principal. Normalmente, los IED se comunican al HMI de S/E los que a su vez se comunican con el HMI principal.

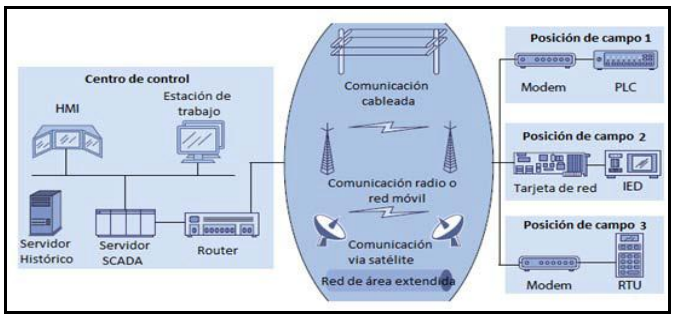

Fig. 1. Estructura de los sistemas SCADA [4]

2.3. Procesadores de Comunicaciones Front End

La interfaz a la red de comunicaciones es una función asignada a un computador llamado Front End, el cual maneja toda la interconexión especializada a los canales de comunicaciones y realiza la conversión de protocolos de modo que el sistema principal pueda contar con datos en un formato estándar.

Debido a que los SCADA cubren áreas geográficas grandes, normalmente depende de una variedad de sistemas de comunicación: LAN normalmente confiables y de alta velocidad, y WAN menos confiables y de mas baja velocidad; por lo que se han desarrollado técnicas para la transmisión confiable sobre diferentes medios. Los progresos recientes han considerado la aparición de un número apreciable de protocolos "abiertos".

2.4. Aplicaciones especiales

Casi todos los sistemas SCADA tienen software de aplicación especial, asociado generalmente al monitoreo y al control.

3. PROTOCOLOS DE COMUNICACIÓN DEL SCADA

Los protocolos utilizados van de acuerdo con cada uno de los medios disponibles en la comunicación. Algunos de los más comunes son:

3.1. Protocolo IEC 61850

La norma IEC 61850 es un estándar internacional de comunicación para subestaciones automatizadas que se extiende a otros elementos del sistema eléctrico. El objetivo de la norma IEC 61850 es comunicar IEDs de diferentes fabricantes buscando interoperabilidad entre funciones y elementos, y la armonización de las propiedades generales de todo el sistema. Para lograrlo, la norma no solo define las comunicaciones, sino que también define un lenguaje de configuración del sistema, condiciones ambientales y especificaciones de calidad de los equipos, y procedimientos para probar equipos.

La norma IEC 61850 adopta como red de área local la red Ethernet y define diversos niveles lógicos y físicos en una subestación, como nivel estación, nivel campo y nivel proceso, no define ninguna topología en particular [5].

La posibilidad de implementar una instalación bajo IEC 61850, permite reducir el cableado entre los distintos aparatos de maniobra y protección, debido al remplazo de señales eléctricas por mensajes, que envían información digital o análoga.

Las tendencias en la automatización de las compañías eléctricas, especialmente de las subestaciones, convergen en una arquitectura de comunicaciones común con el objetivo de tener la interoperabilidad entre una variedad de IEDs encontrados en las subestaciones, que puede:

- Desarrollar un estándar internacional para las comunicaciones en el interior de una subestación automatizada.
- Conseguir interoperabilidad entre equipos de diferentes proveedores.
- Permitir la comunicación cerca de los equipos de potencia.
- Reducir el cableado convencional.

3.2. Protocolo Distributed Network Protocol - DNP3

La telemetría de radio es probablemente la tecnología base de SCADA. Una red de radio típica consiste en una conversación a través del repetidor situado en algún punto elevado y un número de RTU's que comparten la red. Todas las RTU's "hablan" sobre una frecuencia (F1) y escuchan en una segunda frecuencia (F2). El repetidor escucha en F1, y retransmite esto en F2, de modo que una RTU que transmite un mensaje en F1, lo tiene retransmitido en F2, tal que el resto de RTU's pueda oírlo. Los mensajes del Master viajan sobre un enlace de comunicación dedicado hacia el repetidor y son difundidos desde el repetidor en F2 a todas las RTU's. Si el protocolo de comunicaciones usado entre el Master y el repetidor es diferente al usado en la red de radio, entonces debe haber un "Gateway" en el sitio del repetidor [6].

DNP3 se ha utilizado con éxito sobre la red de radio, que encapsulado en TCP/IP, permite que una red de fines generales lleve los datos al Master. DNP3 es un protocolo SCADA moderno, en capas, abierto, inteligente, robusto y eficiente, que puede [3]:

- Solicitar y responder con múltiples tipos de dato en un solo mensaje.
- Segmentar mensajes en múltiples frames para asegurar excelente detección y recuperación de errores.
- Incluir en una respuesta, sólo datos cambiados.
- Asignar prioridad a los ítems de datos y solicitarlos periódicamente basado en su prioridad.
- Responder sin solicitud previa.
- Utilizar sincronización de tiempo con un formato estándar.
- Permitir múltiples operaciones punto a punto y al Master.
- Permitir objetos definibles por el usuario incluyendo transferencia de archivos.

A continuación veremos la relación entre el modelo de capas OSI y el Enhanced Performance Architecture (EPA) del protocolo DNP3.

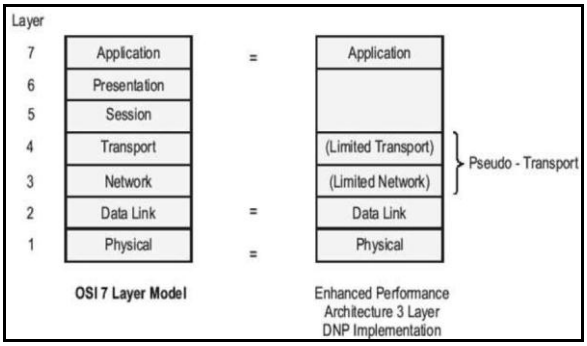

Fig. 2. Relación Modelo OSI y el Enhanced performance Architecture (EPA) del DNP3. Fuente: Practical Industrial Data Communications [3]

El siguiente gráfico presenta el frame del Protocolo DNP3:

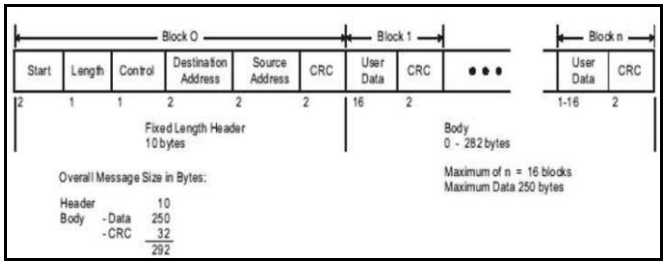

Fig. 3: Frame Format Protocolo DNP3. Fuente: Practical Industrial Data Communications [3]

3.3. Protocolo IEC 60870-5-104

El protocolo IEC 60870-5-104 o IEC 104 es un estándar basado en el IEC 60870-5-101 o IEC 101. Utiliza la interfaz de red TCP/IP para disponer de conectividad a la red LAN y para conectarse a la WAN. La capa de aplicación IEC 104 se conserva igual a la de IEC 101 con algunos de los tipos de datos y los servicios utilizados.

Generalmente para los sistemas de energía, se utiliza el protocolo IEC 104 para el centro de control y el protocolo IEC 101 para la interacción con los IEDs.

La ventaja más grande del protocolo IEC 60870-5-104 es que habilita la comunicación a través de una red estándar y permite la transmisión de datos simultáneos entre varios dispositivos y servicios, debido a que el protocolo IEC 60870-5-104 define el uso de una red TCP como medio de comunicación [7].

La Fig. 4 muestra las arquitecturas de los protocolos IEC 101 y IEC 104.

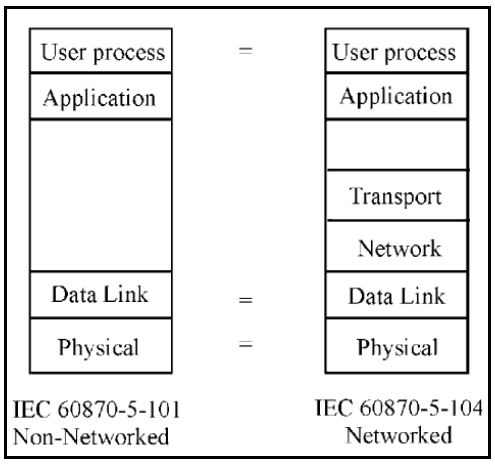

Fig. 4. Arquitecturas de los Protocolos IEC 101 e IEC 104. Fuente: Practical Industrial Data Communications [3]

La Fig. 5 muestra la relación entre el modelo de capas OSI y el Enhanced Performance Architecture (EPA) del protocolo IEC 104:

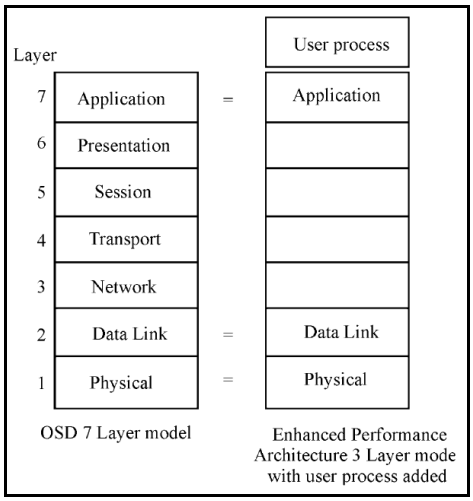

Fig. 5. Relación Modelo OSI y el EPA del IEC 104. Fuente: Practical Industrial Data Communications [3]

La Fig. 6 y la Fig. 7 nos permiten ver el campo de control del protocolo IEC-104 en transmisiones balanceadas y no balanceadas:

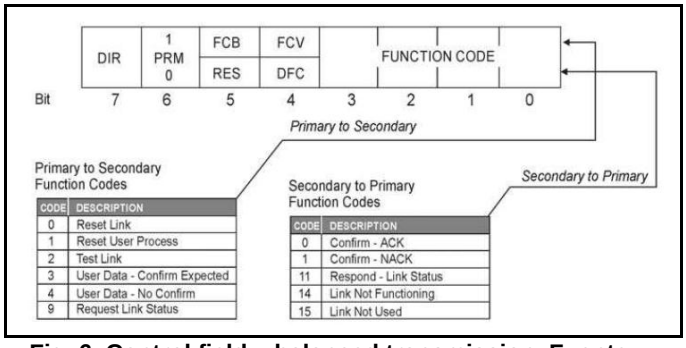

Fig. 6. Control field – balanced transmission. Fuente: Practical Industrial Data Communications [3]

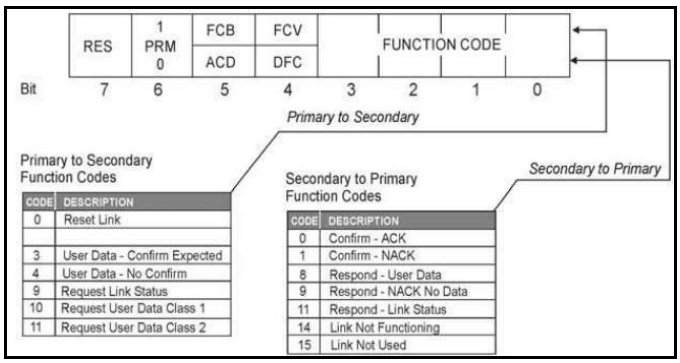

Fig. 7. Control field – unbalanced transmission. Fuente: Practical Industrial Data Communications [3]

4. IDENTIFICACIÓN Y VALORACIÓN DE ACTIVOS DE INFORMACIÓN

Los activos mas importantes a tener en cuenta para el análisis de riesgos para un sistema SCADA son los siguientes: IED, HMI en S/E (HMI S/E), HMI en principal (HMI P/L), Front End (FE) y Protocolos (PT).

Los activos se valoran con base en los elementos principales para la seguridad de la información: Confidencialidad, Integridad, Disponibilidad, Trazabilidad y No repudio.

La valoración de los activos se puede realizar de acuerdo con la siguiente Tabla:

Tabla I. Valoración de Activos

VALORACION DE ACTIVOS
CATASTROFICO
MAYOR
MODERADO
MENOR
INSIGNIFICANTE

En la Tabla II se presenta el resultado de esta valoración y su correspondiente justificación.

Tabla II Identificación y Valoración de Activos de Información

Activo	Confidencialidad		Integridad		Disponibilidad		Trazabilidad		No Repudio	
	Valoración	Justificación	Valoración	Justificación	Valoración	Justificación	Valoración	Justificación	Valoración	Justificación
IED	Moderado	Información operativa convencional que no merece ser confidencial	Catastrófico	Por ser la unidad básica de recepción/envió de información, su integridad es de muy alta valoración.	Moderado	Indisponible la supervisión sobre el elemento o la función que realice el elemento indisponible	Catastrófica	Los cambios en IED realizados deben ser registrados para determinar los cambios a efectuar en HMI S/E y HMI Principal	Menor	Los cambios y quien los realiza en IED deben ser registrados, Pero estas actividades son realizadas por personal especializado y su responsabilidad formalizada.
HMI S/E	Moderado	Información operativa convencional que no merece ser confidencial	Moderado	Si su funcionamiento no es adecuado se realiza manejo del IED directamente	Mayor	La supervisión y control de la S/E se hace muy dispendiosa y la información no estaría disponible	Catastrófica	Los cambios en HMI S/E realizados deben ser registrados para determinar los cambios a efectuar en IED y HMI Principal	Menor	Los cambios y quien los realiza en HMI S/E deben ser registrados, Pero estas actividades son realizadas por personal especializado y su responsabilidad formalizada.
HMI Principal	Moderado	Información operativa convencional que no merece ser confidencial	Mayor	Si su funcionamiento no es adecuado se realiza manejo del HMI de todas las S/E o IED directamente	Catastrófica	La supervisión y control del Sistema eléctrico no podría realizarse.	Catastrófica	Los cambios en HMI principal realizados deben ser registrados para determinar los cambios a efectuar en IED y HMI de S/E	Menor	Los cambios y quien los realiza en HMI Principal deben ser registrados, Pero estas actividades son realizadas por personal especializado y su responsabilidad formalizada.
Front End	Moderado	Información operativa convencional que no merece ser confidencial	Mayor	Si su funcionamiento no es adecuado se realiza manejo del HMI de todas las S/E o IED directamente	Catastrófica	La supervisión y control del Sistema eléctrico no podría realizarse.	Catastrófica	Los cambios en Front End realizados deben ser registrados para determinar los cambios a efectuar en HMI Principal y HMI de S/E	Menor	Los cambios y quien los realiza en Front End deben ser registrados, Pero estas actividades son realizadas por personal especializado y su responsabilidad formalizada.
Protocolos	Insignificante	Protocolos utilizados son estándares	Menor	Los protocolos utilizados son confiables	Insignificante	No aplica el concepto de disponibilidad	Menor	No se ha visto la necesidad de verificar logs de estos protocolos	Insignificante	No aplica el concepto de no repudio

5. IDENTIFICACIÓN Y VALORACIÓN DE RIESGOS

Al igual que los activos, los riegos deben ser identificados y valorados con base en los elementos principales para la seguridad de la información: Confidencialidad, Integridad, Disponibilidad, Trazabilidad y No repudio.

En este paso se determinan los riesgos con base en las vulnerabilidades que se tienen y que son explotadas por las amenazas.

La valoración se identifica con los siguientes símbolos y colores:

Tabla III Valoración de Riesgos

IA	INACEPTABLE
ID	INADMISIBLE
TO	TOLERABLE
AC	ACEPTABLE

Las Tablas IV, V, VI y VII presentan el resultado de la valoración de riesgos de acuerdo con su confidencialidad, integridad, disponibilidad y trazabilidad correspondientemente.
La valoración de riesgos según la característica de “No Repudio” no se considera en este punto, debido a que en la valoración de activos esta característica dio menor e insignificante.

Tabla IV Valoración del Riesgo – Pérdida de Confidencialidad del Activo

VALORACION RIESGO - PERDIDA DE **CONFIDENCIALIDAD** DEL ACTIVO						
VULNERABILIDAD	**AMENAZA**	**IED**	**HMI S/E**	**HMI P/L**	**FE**	**PT**
Controles inadecuados de acceso físico/lógico	Abuso de Privilegios	IA		TO	TO	
	Acceso no autorizado	IA		IA	IA	
	Escaneos de red (I)	IA			IA	
	Análisis de trafico			IA		
Configuración incorrecta o Inadecuada	Abuso de privilegios	IA		TO	IA	
	Acceso no autorizado	IA	IA	IA	IA	
	Escaneos de red (I)	IA			ID	
	Análisis de trafico		IA	IA		
	Escapes de información			IA		
Poca conciencia sobre la seguridad de la información	Divulgación de información			IA		
	Ataque de ingeniería social			IA		
	Fuga/Robo de información			IA		
Inadecuado procedimiento de actualizaciones de seguridad y antivirus	Errores del administrador		IA	IA		
	Vulnerabilidad de programas		TO	IA		
	Difusión sw dañino		IA	IA		

Tabla V Valoración del Riesgo – Pérdida de Integridad del Activo

VALORACION RIESGO - PERDIDA DE **INTEGRIDAD** DEL ACTIVO						
VULNERABILIDAD	**AMENAZA**	**IED**	**HMI S/E**	**HMI P/L**	**FE**	**PT**
Controles inadecuados de acceso físico/lógico	Abuso de Privilegios	IA	IA	IA		TO
	Acceso no autorizado	IA	ID	ID		IA
	Ataque dirigido	IA	ID	ID		
	Manipulación de la configuración		ID	ID	ID	TO
	Manipulación de programas		IA	IA		
Configuración incorrecta o Inadecuada	Errores de administrador	IA	ID	ID		IA
	Abuso de privilegios	IA	IA	IA	IA	
	Acceso no autorizado	IA		IA		
	Difusión sw dañino		ID	ID		
	Fallas de software		ID	ID		IA
	Errores de los usuarios			IA		
	Fallas de hardware				ID	
	Ataque dirigido				ID	
	Vulnerabilidad de los programas					IA
Inadecuados esquemas de reposición de activos obsoletos	Acceso no autorizado		ID	ID	ID	
	Abuso de privilegios		IA	IA		
	Ataque dirigido		ID	ID	ID	ID
	Difusión sw dañino		ID	ID		
Insuficientes o inadecuados mantenimientos predictivos, preventivos y/o correctivos	Fallas de hardware				ID	
	Degradación de los soportes de almacenamiento				ID	

Tabla VI Valoración del Riesgo – Pérdida de Disponibilidad del Activo

VALORACION RIESGO - PERDIDA DE **DISPONIBILIDAD** DEL ACTIVO						
VULNERABILIDAD	**AMENAZA**	**IED**	**HMI S/E**	**HMI P/L**	**FE**	**PT**
Controles inadecuados de acceso físico/lógico	Abuso de privilegios	IA	IA	IA		
	Acceso no autorizado	ID	ID	ID		
	Denegación de Servicios	ID	ID	ID		
	Ataque dirigido		ID	ID	ID	
Configuración incorrecta o Inadecuada	Acceso no autorizado	ID	ID	ID		
	Ataque dirigido		ID	ID	ID	
	Caída del sistema por agotamiento de recursos		ID	IA	ID	
	Denegación de servicios	ID	ID	ID	ID	
Insuficiente protección contra virus y código malicioso	Fallas de sw		ID	ID		
	Vulnerabilidad de los programas		ID	ID		
	Denegación de servicios		ID	ID		
Punto único de fallo	Fallas de hardware				ID	
	Caídas del sistema por agotamiento de recursos				ID	
	Ataque dirigido				ID	
Insuficientes o inadecuados mantenimientos predictivos, preventivos y/o correctivos	Fallas de hardware				ID	
	Degradación de los soportes de almacenamiento				ID	
	Avería de origen físico/lógico				ID	

Tabla VII Valoración del Riesgo – Pérdida de Trazabilidad del Activo

VALORACION RIESGO - PERDIDA DE **TRAZABILIDAD** DEL ACTIVO						
VULNERABILIDAD	**AMENAZA**	**IED**	**HMI S/E**	**HMI P/L**	**FE**	**PT**
Escasos registros en logs o variables auditables	Fallas de hardware	IA				
	Errores de administrador	IA	IA	ID	IA	IA
	Acceso no autorizado	IA			IA	
	Ataque dirigido				IA	
	Abuso de privilegios				IA	
	Manipulación de la configuración		IA			IA
	Errores de configuración					IA
	Errores de monitorización					IA
	Destrucción de información		IA	ID		
Pocos mecanismos de control y Monitoreo	Errores de administrador	IA	IA	ID	IA	
	Errores de configuración	IA			IA	
	Ataque dirigido	IA	IA	ID		
	Errores de monitorización		ID	ID		

6. PLAN DE TRATAMIENTO Y CONTROLES

La Tabla VIII nos permite ver cada uno de los controles propuestos para mitigar los riesgos detectados.

Al igual que para cualquier sistema, el aseguramiento de los sistemas SCADA es un proceso continuo y permanente. Día a día aparecen nuevas amenazas que deben ser analizadas y revisadas frente a las vulnerabilidades del sistema. Así mismo, se debe ser consiente que la implementación de los controles no es solo una actividad puntual, sino un proceso que debe ser implementado gradualmente y en diferentes fases.

A continuación son descritos los controles definidos para los sistemas SCADA y que pueden ser considerados de acuerdo con la gestión de riesgos que se presenta en este artículo, teniendo en cuenta que algunas medidas mitigan más de un escenario de riesgo.

Para limitar las conexiones al SCADA con el fin que únicamente las necesarias se lleven a cabo, se debe restringir el acceso lógico e implementar una arquitectura de red segura, que incluya, al menos: **la Segmentación de redes** de modo que cada subred tenga un propósito específico y ofrezca acceso solo a aquellos usuarios que lo requieran, la instalación de un **Firewall** para habilitar única y exclusivamente las conexiones necesarias, denegando todo el tráfico que no haya sido autorizado explícitamente, la Instalación de un **Sistema de Detección de Intrusos y/o Sistema de Prevención de Intrusos - IDS/IPS** en la red que permita detectar situaciones anómalas a partir de patrones de funcionamiento de la red SCADA, solución que también puede ser complementada incluyendo la **solución de HIPS** (el mismo IPS a nivel de equipo o host). Además, la implementación de una **Solución Network Access Control – NAC** para control de acceso a la red a través de políticas, incluyendo condiciones de admisión, chequeo de políticas de seguridad en el usuario final (antivirus actualizado, sistema operativo parcheado, etc.) y controles sobre

los recursos a los que pueden acceder en la red los usuarios y dispositivos, y lo que pueden hacer en ella [4].

Para monitorear el acceso a los activos de la red SCADA, se debe contar con un **Sistema SOC (Security Operation Center) y un correlacionador de eventos**, donde se centralicen, estandarice y relacionen logs, se haga tratamiento a situaciones anómalas y se identifiquen y manejen oportunamente los incidentes de seguridad.

Para eliminar lo que se denomina puntos únicos de fallo, se deben considerar **Sistemas redundantes** cuya disponibilidad se considere esencial para el SCADA en caso de que ocurra un fallo lógico o físico, sin prescindir de los **esquemas de mantenimiento preventivo y correctivo** para la prevención y atención de cualquier daño a los activos.

Un factor y no menos importante para la seguridad del sistema y una adecuada toma de decisiones es el **Entrenamiento al personal** que maneja el SCADA. La capacitación debe incluir temas de seguridad física y lógica, informática y telecomunicaciones. Cursos o sesiones de concienciación sobre seguridad son claves para fomentar una cultura de seguridad entre los empleados. Igualmente se debe considerar este aspecto al momento de contratar el personal, con el fin de tener parámetros claros sobre capacidad de actuación tanto profesional como ética.

Dado que la seguridad no es exclusivamente un problema técnico, es necesario desarrollar e implantar adecuadamente políticas y procedimientos por medio de los cuales se implementan y evalúan los controles: **Auditorias de seguridad y procedimientos para la revisión de registros de auditoria y monitorización**: se debe definir y establecer una serie de auditorías de seguridad periódicas que afecten los sistemas SCADA, los elementos de red y las comunicaciones, así como su alcance y enfoque. Adicionalmente formalizar el procedimiento de revisión de los registros de auditoría y de monitorización de la red, con el objetivo de detectar anomalías, ya sean funcionales o de seguridad. En este punto, vale la pena mencionar que se deben tomar medidas para la **protección de archivos** incluidos los registros de auditoria. **Procedimiento para administración de roles y privilegios**: esta administración se debe realizar de acuerdo con la segregación de funciones y responsabilidades de cada empleado, para minimizar la posibilidad de ocurrencia de errores humanos y de ataques internos, y también facilitar la trazabilidad de las acciones en caso de un incidente. **Procedimiento de pruebas y control de cambios**: define los pasos a seguir a la hora de afrontar cambios en los activos de información y pruebas de validación antes de aplicarlos en producción, lo que amerita contar con entornos de pruebas diferentes a los entornos productivos. **Procedimiento de aplicación de actualizaciones (parches)**: establece los requisitos y pasos a seguir para la aplicación de parches de seguridad. Es imprescindible aplicarlo en un entorno de pruebas para detectar posibles conflictos o malfuncionamientos en el sistema como consecuencia de dicha aplicación. **Procedimiento de control de accesos físicos**: este procedimiento debe establecer, al menos, los siguientes aspectos: requisitos para conceder acceso físico a las instalaciones, registro de datos del personal, identificación del personal, personal que autoriza el acceso y periodo de validez de la autorización.

Aunque idealmente las redes SCADA deberían permanecer aisladas, se recomienda realizar aseguramiento de los accesos remotos para evitar accesos no autorizados. En todo caso, se deben utilizar **Protocolos Seguros** que cifren todas las comunicaciones con algoritmos robustos, empleando claves complejas y tunelizando todo el tráfico relativo al acceso remoto. Adicionalmente, emplear un **mecanismo de acceso y autenticación fuerte** de doble factor.

Una medida que se debe aplicar antes de realizar el despliegue de una aplicación, sistema operativo o equipo en el entorno productivo, es la realización de un aseguramiento de dicho elemento, es decir la tarea de configuración segura del nuevo elemento. Los parámetros de aseguramiento de los activos son las denominadas **líneas base de seguridad** cuyo objetivo es que ese elemento cuente con un nivel de seguridad razonable, sin que por ello se vea afectada su funcionalidad. Este proceso de aseguramiento suele contar al menos con: Eliminación o desactivación de servicios innecesarios y/o inseguros, sustitución de cuentas por defecto por cuentas personales y biunívocas, alteración de la configuración por defecto, eliminando aquellos valores que sean considerados inseguros, activación de mecanismos y controles de seguridad, como puede ser el establecimiento de una política de contraseñas robustas y la configuración de la ejecución de actualizaciones automáticas. Para la construcción y aplicación de las líneas base de seguridad se pueden utilizar como base y referencia las guías de buenas prácticas y seguridad que ofrecen organizaciones especializadas, teniendo en cuenta también las necesidades operativas del sistema SCADA.

Debido a la constante evolución que sufren los sistemas de información, y concretamente el surgimiento de amenazas relativas a la infección con malware, la **Implementación de sistemas de antimalware y actualización de firmas de los antivirus,** es un control esencial para los Sistemas SCADA. Así como lo hemos mencionado, realizando las pruebas correspondientes que garanticen que las aplicaciones no tienen inconvenientes con estas firmas.

De igual manera y debido al desarrollo de la tecnología, es necesario asumir programas de **renovación tecnológica**, tanto a nivel de hardware como de software, que ofrezcan más funcionalidades y mayor seguridad. Estos programas de renovación deberán ser

sustentados con base en los resultados que arrojen los **análisis de capacidad y rendimiento** de los equipos y aplicativos que deben realizarse con anterioridad, con el objetivo que cumplan con los requerimientos del sistema.

Tabla VIII - Identificación De Riesgos y Controles

Riesgo	Activo	Amenaza	Vulnerabilidad	CONTROLES
Pérdida de disponibilidad del hardware	Front End	Ataque Dirigido	Controles inadecuados de acceso físico/lógico a un activo de información	- Implementación IPS y HOST IPS - Implementación de firewall - Líneas base de seguridad
		Caída del sistema por agotamiento de recursos	Configuración incorrecta o inadecuada	- Análisis de capacidad y rendimiento
		Denegación de servicio		- Entrenamiento al personal
		Ataque Dirigido		- Implementación IPS y HOST IPS - Implementación de firewall - Segmentación de Red en VLANS - Utilización Protocolos seguros - Implementación de Control de acceso a la Red - NAC
		Falla del Hardware	Punto único de fallo	- Sistemas redundantes
		Caída del sistema por agotamiento de recursos		- Análisis de capacidad y rendimiento
		Ataque Dirigido		- Implementación IPS y HOST IPS - Implementación de firewall - Líneas base de seguridad
		Falla del Hardware	Insuficientes o inadecuados mantenimientos predictivos, preventivos y/o correctivos	- Esquemas de mantenimiento preventivo y correctivo
		Degradación de los soportes de almacenamiento		- Esquemas de mantenimiento preventivo y correctivo
		Avería de origen físico o lógico		- Programas de renovación tecnológica
Pérdida de disponibilidad del hardware	IED	Acceso no autorizado	Configuración incorrecta o inadecuada	- Sistema de autenticación fuerte - Procedimiento de control de accesos físicos - Administración de roles y privilegios
		Denegación de servicio		- Entrenamiento al personal
		Acceso no autorizado	Controles inadecuados de acceso físico/lógico a un activo de información	- Sistema de autenticación fuerte - Procedimiento de control de accesos físicos - Administración de roles y privilegios
		Denegación de servicio		- Implementación IPS y HOST IPS - Implementación de firewall - Líneas base de seguridad
Pérdida de disponibilidad del software	HMI Principal	Acceso no autorizado	Controles inadecuados de acceso físico/lógico a un activo de información	- Sistema de autenticación fuerte - Administración de roles y privilegios
		Ataque Dirigido		- Implementación IPS y HOST IPS - Implementación de firewall - Líneas base de seguridad
		Denegación de servicio		- Implementación IPS y HOST IPS - Implementación de firewall - Líneas base de seguridad
		Acceso no autorizado	Configuración incorrecta o inadecuada	- Sistema de autenticación fuerte - Administración de roles y privilegios
		Ataque Dirigido		- Implementación IPS y HOST IPS - Implementación de firewall - Líneas base de seguridad
		Denegación de servicio		- Implementación IPS y HOST IPS - Implementación de firewall - Líneas base de seguridad
		Falla del Software	Insuficiente protección contra virus y código malicioso	- Implementación de sistemas de antimalware - Esquemas de pruebas y control de cambios
		Vulnerabilidades de los programas (software)		- Implementación de sistemas de antimalware - Esquemas de pruebas y control de cambios - Procedimiento de aplicación de parches
		Denegación de servicio		- Implementación de sistemas de antimalware
Pérdida de disponibilidad del software	HMI S/E	Acceso no autorizado	Controles inadecuados de acceso físico/lógico a un activo de información	- Sistema de autenticación fuerte - Administración de roles y privilegios
		Ataque Dirigido		- Implementación IPS y HOST IPS - Implementación de firewall - Líneas base de seguridad
		Denegación de servicio		- Implementación IPS y HOST IPS - Implementación de firewall - Líneas base de seguridad
		Caída del sistema por agotamiento de recursos	Configuración incorrecta o inadecuada	- Entrenamiento al personal
		Acceso no autorizado		- Sistema de autenticación fuerte - Administración de roles y privilegios
		Ataque Dirigido		- Implementación IPS y HOST IPS - Implementación de firewall - Líneas base de seguridad
		Denegación de servicio		- Implementación IPS y HOST IPS - Implementación de firewall - Líneas base de seguridad
		Falla del Software	Insuficiente protección contra virus y código malicioso	- Implementación de sistemas de antimalware - Esquemas de pruebas y control de cambios - Procedimiento de aplicación de parches
		Vulnerabilidades de los programas (software)		- Implementación de sistemas de antimalware - Esquemas de pruebas y control de cambios - Procedimiento de aplicación de parches
				- Implementación IPS y HOST IPS - Implementación de firewall

Tabla VIII - Identificación de Riesgos y Controles

	Activo	Amenaza	Vulnerabilidad	CONTROLES
Pérdida de la confidencialidad del hardware	Front End	Escaneo de red	Configuración incorrecta o inadecuada	- Implementación IPS y HOST IPS - Implementación de firewall - Segmentación de Red en VLANS - Utilización Protocolos seguros - Implementación de Control de acceso a la Red - NAC
Pérdida de la integridad del hardware	Front End	Manipulación de la configuración	Controles inadecuados de acceso físico/lógico a un activo de información	- Esquemas de pruebas y control de cambios
		Falla del Hardware	Configuración incorrecta o inadecuada	- Esquemas de mantenimiento preventivo y correctivo
		Ataque Dirigido		- Implementación IPS y HOST IPS - Implementación de firewall - Líneas base de seguridad
		Acceso no autorizado	Inadecuados esquemas periódicos de reposición de Activos Obsoletos	- Sistema de autenticación fuerte - Procedimiento de control de accesos físicos - Administración de roles y privilegios
		Ataque Dirigido		- Implementación IPS y HOST IPS - Implementación de firewall - Líneas base de seguridad
		Falla del Hardware	Insuficientes o inadecuados mantenimientos predictivos, preventivos y/o correctivos	- Esquemas de mantenimiento preventivo y correctivo
		Degradación de los soportes de almacenamiento		- Programas de renovación tecnológica
Pérdida de la integridad del software	HMI Principal	Manipulación de la configuración	Controles inadecuados de acceso físico/lógico a un activo de información	- Esquemas de pruebas y control de cambios
		Acceso no autorizado		- Sistema de autenticación fuerte - Administración de roles y privilegios
		Manipulación de programas		- Esquemas de pruebas y control de cambios
		Ataque Dirigido		- Implementación IPS y HOST IPS - Implementación de firewall - Líneas base de seguridad
		Falla del Software	Configuración incorrecta o inadecuada	- Esquemas de pruebas y control de cambios - Sistemas Redundantes
		Errores del administrador		- Entrenamiento al personal - Esquemas de pruebas y control de cambios
		Difusión de software dañino		- Implementación de sistemas de antimalware
		Acceso no autorizado		- Sistema de autenticación fuerte - Administración de roles y privilegios
		Difusión de software dañino	Inadecuados esquemas periódicos de reposición de Activos Obsoletos	- Implementación de sistemas de antimalware
		Acceso no autorizado		- Sistema de autenticación fuerte - Administración de roles y privilegios
		Ataque Dirigido		- Implementación IPS y HOST IPS - Implementación de firewall - Líneas base de seguridad
Pérdida de la integridad del software	HMI S/E	Manipulación de la configuración	Controles inadecuados de acceso físico/lógico a un activo de información	- Esquemas de pruebas y control de cambios
		Acceso no autorizado		- Sistema de autenticación fuerte - Administración de roles y privilegios
		Ataque Dirigido		- Implementación IPS y HOST IPS - Implementación de firewall - Líneas base de seguridad
		Falla del Software	Configuración incorrecta o inadecuada	- Esquemas de pruebas y control de cambios - Sistemas Redundantes
		Errores del administrador		- Entrenamiento al personal - Esquemas de pruebas y control de cambios
		Difusión de software dañino		- Implementación de sistemas de antimalware
		Difusión de software dañino	Inadecuados esquemas periódicos de reposición de Activos Obsoletos	- Implementación de sistemas de antimalware - Programas de renovación tecnológica
		Acceso no autorizado		- Sistema de autenticación fuerte - Administración de roles y privilegios - Programas de renovación tecnológica
		Ataque Dirigido		- Implementación IPS y HOST IPS - Implementación de firewall - Líneas base de seguridad
Pérdida de la integridad del software	Protocolos	Ataque Dirigido	Inadecuados esquemas periódicos de reposición de Activos Obsoletos	- Implementación IPS y HOST IPS - Implementación de firewall - Líneas base de seguridad
Pérdida de trazabilidad del software	HMI Principal	Errores del administrador	Escasos registros en logs o variables auditables	- Entrenamiento al personal - Procedimientos de revisión y auditorias
		Destrucción de información		- Protección de archivos
		Errores del administrador	Pocos mecanismos de control y monitoreo	- Entrenamiento al personal
		Errores de monitorización (log)		- Entrenamiento al personal - Implementación Sistemas SOC y correlacionalor de eventos - Procedimientos de revisión y auditorias
		Ataque Dirigido		- Implementación IPS y HOST IPS - Implementación de firewall - Líneas base de seguridad
Pérdida de			Pocos mecanismos de	- Entrenamiento al personal - Implementación Sistemas SOC y correlacionalor de

7. CONCLUSIONES

Debido al incremento de las posibilidades de ataques a los sistemas SCADA, este proceso de análisis de riesgos e implementación de medidas de control es un proceso que debe ser asumido por la dirección de las Empresas con compromiso, involucrando a equipos interdisciplinarios en su implementación y asignando los recursos requeridos.

El análisis de riesgos debe ser un proceso periódico que permita a cada empresa conocer cuál es su estado actual, con el objetivo de marcarse hitos y priorizar las tareas, atendiendo en primer lugar aquellas que sean consideradas como críticas.

Una vez que los controles estén siendo gestionados para los Sistemas SCADA, las Empresas estarán acercándose al cumplimiento de la Norma NERC CIP, norma que es el marco de trabajo que tiene como función identificar y proteger los recursos cibernéticos críticos y garantizar el funcionamiento del sistema Eléctrico.

REFERENCIAS

[1] CECOEL - Centro de Control Eléctrico. Online [Jul. 2012].
[2] E. San Román. CISSP, CISA y CEH. *"Los sistemas SCADA y su exposición ante ataques informáticos".* Online [May. 2012].
[3] G. Clarke, D. Reynders & E. Wright. "*Practical Moderm SCADA Protocols: DNP3, 60870.5 and Related Systems*". Great Britain, 2004.
[4] P. Pablo, A. Eduardo, D. Susana, G. Laura & G. Cristina. "*Estudio sobre la seguridad de los sistemas de monitorización y control de procesos e infraestructuras (SCADA)". Instituto Nacional de Tecnologías de la Comunicación* – INTECO. España. Marzo 2012.
[5] R. Vignoni, R. Pellizzoni & L. Funes. "*Sistemas de automatización de subestaciones con IEDs IEC 61850: Comunicaciones, topologías"*. Argentina, Mayo, 2009.
[6] D. G. Hernán. *"Implementación de Un sistema SCADA para la mezcla de dos sustancias en una industria química".* Online [En. 2012].
[7] Protocols IEC 60870-5-104. Online [Mar. 2012].