Amenazas a la Seguridad informática en sistemas de control y supervisión industriales

Mag. Ermilso Díaz Benachi
Corporación Universitaria Unicomfacauca
ediaz@unicomfacauca.edu.co

Mag. Diana Jimena López
Corporación Universitaria Unicomfacauca
dlopez@unicomfacauca.edu.co

Esp. Jhon Alexander Guerrero
Corporación Universitaria Unicomfacauca
jguerrero@unicomfacauca.edu.co

Fecha Recepción: 07/11/15 - Fecha Aprobación: 12/11/15

Resumen: Este artículo establece un análisis reflexivo sobre las diferentes amenazas que se presentan en los sistemas de control industrial y, en general, los sistemas de información utilizados en la industria para apoyo de actividades. Este interés surge por la creciente apertura de las redes que soportan estos sistemas y que en la actualidad se ve potenciada debido a la incorporación de internet dentro de las instalaciones industriales. Los elementos que se muestran generalizan las amenazas a las que se expone la industria cuando utiliza redes abiertas o cómo se ven expuestas sus propias redes ante diferentes vulnerabilidades, además de qué esfuerzos deben considerarse para mitigarlas, así como los campos en los cuales aún no se generan estrategias de choque.

Palabras clave: Sistemas de control industrial, riesgo, amenazas, vulnerabilidades.

Abstract: This article makes a thoughtful research on the different threats that arise in industrial control systems and general information systems used in the industry to support their activities. This interest arises from the increasing openness of the networks that support these systems and today is enhanced due to the incorporation of internet within industrial facilities. The items shown widespread threats to which the industry is exposed when using open networks or how their networks are exposed to different vulnerabilities and what efforts should consider to mitigate and fields which have not yet strategies shock are generated.

Keywords: Industrial control systems, risk, threats, vulnerabilities.

1. Introducción

Las tecnologías de la información y las comunicaciones (TIC), junto con la inclusión de internet como herramienta para compartir información, han impactado en todos los campos comerciales y productivos de las empresas, tanto de servicios como de manufactura. Hasta hace un tiempo, los sistemas productivos poseían sistemas de información cerrados y la apertura hacia redes públicas no era considerado, mucho más si se trataba de integrar a los sistemas de control, con los sistemas de gestión [1] [2].

Los sistemas de control han tenido una evolución desde los sistemas basados en relés electromecánicos hasta sistemas basados en controladores lógicos programables, equipos con microprocesadores y memoria programable y, últimamente, la utilización de computadores industriales [3]. La singularización de los productos alrededor de las necesidades de los clientes hace que se deban incorporar nuevas tecnologías en los sistemas de producción y que en muchas ocasiones el mismo cliente quiera hacer parte activa del bien que está adquiriendo [4].

Estas redes de control se denominan buses de campo, que inicialmente fueron la mejor forma de reemplazar los efectivos pero voluptuosos lazos de control de 4 a 20 mA, debido a que los sistemas de control requerían una conexión física por cada variable controlada, esto insertaba una gran cantidad de problemas cuando se requería configurar cambios en los procesos, junto con

un enorme gasto en mantenimiento y en instalaciones de cableado [5]; los buses de campo surgieron como una solución a este tipo de inconvenientes, incluyendo dentro de sus ventajas una disminución del cableado al permitir comunicar y alimentar los dispositivos, mayor conexión de dispositivos, posibilidades de diagnóstico y reconfiguración de los equipos, entre otras. La Figura 1 muestra cómo se han posicionado diferentes sistemas para gestionar información en los diferentes niveles en una empresa de manufactura.

Por lo tanto, dentro de una empresa de manufactura generalmente coexisten dos tipos de redes, la red de gestión, que soporta todas las actividades comerciales y administrativas de la empresa que se apoyan en Tecnologías de información (IT), y la red de control que soporta todas las actividades de operación propias de la producción basada en hardware y software para tal fin (OT) [6].

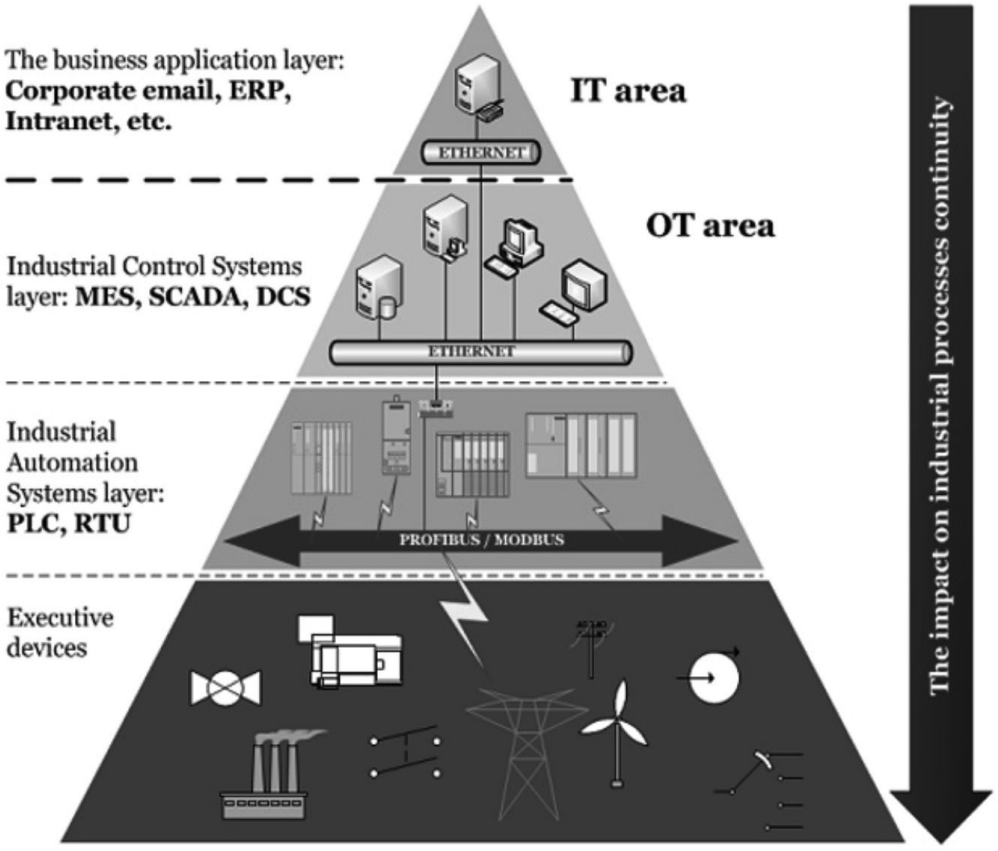

Figura 1. Uso de tecnologías en la industria [6]

Estas dos redes estaban plenamente diferenciadas y separadas a través de firewalls y medios, para una separación lógica entre cada una de ellas y así aislar los sistemas de control.

Los buses de campo, por lo tanto, generan redes cerradas mediante protocolos y componentes físicos propietarios. Esta característica que daba al sistema una mayor robustez es lo que ahora incrementa la vulnerabilidad al incluir protocolos comunes como Ethernet a este tipo de procesos [7]. Por otro lado, la globalización de las economías y la competitividad obliga a la reducción de costos, lo que hace que generalmente las empresas ya no consideren un solo sitio de fabricación, sino que un producto es el resultado de unir diferentes piezas que se fabrican en diversas partes del mundo, buscando mano de obra más competitiva o porque alguna materia prima necesaria es más fácil de conseguir.

El artículo está organizado a partir de la siguiente estructura: en la primera sección se realiza un acercamiento a los conceptos de ICS (Sistemas de Control Industrial), posteriormente, se definen los conceptos básicos de seguridad informática relevantes al tema. En la tercera parte, se realiza una identificación de las diferentes amenazas a las cuales se enfrentan los diferentes sistemas ICS; y, por último, se realizan algunas consideraciones y conclusiones finales.

2. ICS (*Information Control Systems*)

La inclusión del procesador en la industria, a través de los Controladores Lógicos Programables, generó la necesidad de establecer sistemas que fueran capaces de gestionar la información que estos producen; en la actualidad, se conocen dos grandes arquitecturas de control [8], por una parte están los sistemas de control y adquisición de datos (SCADA) y, por el otro, los sistemas de control distribuido (DCS), a continuación se establecen las particularidades de cada una de ellas.

2.1. Sistemas de Control y Adquisición de Datos (SCADA).

Un SCADA es un conjunto de aplicaciones software especialmente diseñada para funcionar sobre hardware, representado en computadores industriales y/o Controladores Lógicos Programables (PLC), con acceso al proceso mediante comunicación digital con los instrumentos y actuadores, e interfaz gráfica de alto nivel con el usuario (pantallas táctiles, ratones o cursores, lápices ópticos) [9][10].

Aunque inicialmente solo era un programa que permitía la supervisión y adquisición de datos en procesos de control, actualmente han ido surgiendo una serie de productos hardware y buses especialmente diseñados o adaptados para éste tipo de sistemas [11]. La interconexión de los sistemas SCADA también es propia, se realiza una interfaz del PC a la planta centralizada, cerrando el lazo sobre el ordenador principal de supervisión [12].

Las prestaciones que puede ofrecer un sistema SCADA son las siguientes:

- Posibilidad de crear paneles de alarma, los cuales exigen la presencia de un computador para reconocer una parada o situación de alarma, con registro de incidencias.
- Generación de históricos de señal de planta que pueden ser volcados para su proceso sobre una hoja de cálculo.
- Creación de informes, avisos y documentos en general.
- Ejecución de programas que modifican la ley de control o incluso el programa total sobre el PLC.
- Posibilidad de programación numérica que permite realizar cálculos aritméticos de elevada resolución sobre la CPU del ordenador, y no sobre el controlador, etc.

Con éstas se pueden desarrollar aplicaciones basadas en un computador, con captura de datos, análisis de señales, presentaciones en pantalla, envío de resultados a disco o impresora, control de actuadores, etc. [13].

2.2. Sistemas de Control Distribuidos (DCS)

Un proceso industrial tiene una gran cantidad de etapas de proceso que deben ser ejecutadas para obtener el producto final; el sistema de control implementado debe contar con los recursos necesarios para cumplir con esta necesidad. Sin embargo, centralizar el control y supervisión a un solo dispositivo hace que la fiabilidad del proceso dependa de lo confiable que sea el equipo, por esta razón se hace necesario distribuir la regulación de las variables a diferentes dispositivos y separar la capa de supervisión de la de control [14].

Al distribuir las tareas en varios equipos como se muestra en la Figura 2. Se implementa una arquitectura de control distribuido. En este tipo de arquitectura el procesador que ejecuta las estrategias de control presenta comunicación vertical entre los diferentes niveles del proceso de producción, permitiendo establecer control directo con el proceso o parte operativa y horizontal con los dispositivos de control, estableciendo comunicación con otros dispositivos de control del sistema. Adicionalmente, un equipo servidor ejecuta las tareas de supervisión, configuración y gestión de alarmas [15] [16].

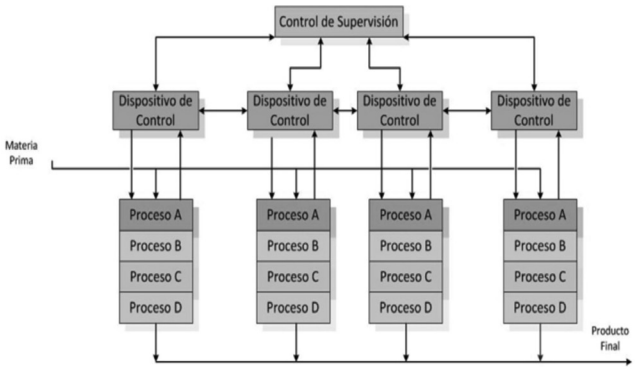

Figura 2. Arquitectura de un sistema DCS [14]

Una de las ventajas con este tipo de esquema es poder hacer una derivación (*Bypass*) a las unidades

con problemas o que necesiten mantenimiento, evitando paradas en toda la planta. Además exige que los diferentes controladores tengan una asignación dinámica de las tareas, por lo tanto requiere gran capacidad debido a los retardos, posibles desbordamientos en el procesamiento de datos en cada nivel y falta de flujo de información directa entre controladores. Necesidades que son solucionadas con la incorporación de buses de campo, o redes de comunicación industrial como Ethernet [7], Profibus [17], Devicenet [18], entre otras.

Al presentar distribución de las tareas del proceso por equipos de control se establece comunicación horizontal solo entre procesadores redundantes, quienes finalmente manejan cada unidad de proceso. En el concepto inicial se contempla que si un dispositivo de control entra en falla y le impide cumplir las funciones asignadas, cualquiera de los controladores adjuntos al sistema debe estar en la capacidad de retomar las tareas del dispositivo que sale de operación. La Tabla 1 resume las principales diferencias entre un sistema SCADA y un DCS.

Tabla 1. Comparativa entre sistemas DCS y SCADA

ASPECTO	SCADA	DCS
Base de datos	Distribuida	Centralizada
Subsistemas	Dispersos geográficamente en los sitios de campo	Ubicados dentro de un área de la fábrica o centrados
Comunicación	Sistemas de comunicación de larga distancia tipo WAN	Se requiere tecnología de red que suela ser más fiable y de alta velocidad Tipo LAN
Flexibilidad	Si se cambia una entrada en una nueva dirección o Tag, el cambio debe ser realizado manualmente en todo el sistema.	Cuando se efectúan cambios, los datos en la lógica de control son propagados automáticamente a todos los aspectos del sistema

3. Conceptos básicos de Seguridad informática

La seguridad informática según [19] es la actividad que consiste mantener los recursos de información de una empresa con una alta disponibilidad y permitiendo el acceso y modificación de ésta solo a personal autorizado, considerando los privilegios que tenga cada usuario. Por lo tanto, la seguridad informática intenta identificar y subsanar los vacíos que existen en los sistemas informáticos que limitan o niegan el acceso a los recursos. A continuación se muestran algunos conceptos relacionados con la seguridad informática y los sistemas ICS.

3.1. Vulnerabilidad

Una vulnerabilidad según [20] es una debilidad del sistema que sustenta los recursos de información, o los procesos relacionados con ella, por lo tanto se pueden identificar de tipo software como hardware incluido, componentes como el talento humano y la seguridad física que contiene el sistema.

3.2. Amenaza

Se define como la situación o evento que previa identificación de una vulnerabilidad genera la posibilidad de afectar los recursos de información, afectando la disponibilidad e integridad de ésta [20]. La materialización de una amenaza que aprovecha una vulnerabilidad se constituye en riesgo para el sistema y un siguiente nivel como un ataque.

3.3. Ataque informático

La utilización de las tecnologías de la información y la comunicación hace uso expansivo de las redes de comunicación, en la redes IT existen diferentes ataques y amenazas a las cuales están expuestas tanto las empresas como cualquier persona desde el punto de vista de los datos. Según [21], un ataque es el aprovechamiento de vulnerabilidades con fines delictivos en sistemas de información, este tipo de actividad se puede realizar a nivel software o hardware o inclusive a nivel físico. También incluye vulnerabilidades en el personal de la empresa a través de comportamiento y/o hábitos riesgosos; generalmente un ataque genera daños al interior de las empresas tanto a nivel comercial como organizacional. Estos ataques pueden ser de diferentes tipo como se planteará a continuación.

3.4. Fabricación

En este tipo de ataque el atacante se hace pasar por quien el usuario necesita comunicarse o existe algún tipo de relación, para esto se utiliza el engaño como fuente de información [22]. Una de las técnicas para

lograr un ataque de este tipo es la ingeniería social, en este se aprovecha una de las vulnerabilidades más grandes que tiene cualquier sistema y es el factor humano. Se soporta en el engaño o la inducción a las personas a realizar una determinada actividad dentro del sistema [23].

3.5. Interrupción

Este tipo de ataque generalmente busca saturar el servicio prestado por algún servidor, el cual el equipo atacado este accediendo, en este caso se genera daño a las actividades del negocio por una empresa por ejemplo si se trata de un modelo de negocio *on line*. Una de las técnicas más usadas se denomina DoS (*Denial of Service*), la cual representa exactamente este tipo de ataque, para realizarlo el atacante comienza a enviar solicitudes del servicio con niveles de cargas más altas a la que normalmente maneja el servidor, esto lo lleva a la saturación y su posterior caída con el resultado que se empieza a negar el servicio hacia clientes legítimos [22].

3.6. Tampering o Data Didding

Se refiere a la modificación, alteración de los datos y software que se encuentran instalados en un sistema, además borrado de archivos. Este tipo de ataque es serio una vez quien lo realiza ha obtenido derechos de administrador, con la capacidad de ejecutar cualquier comando y alterar cualquier información incluso dar de baja el equipo atacado [22].

3.7. Snooping y Downloading

Los ataques de este tipo tienen el mismo objetivo que el sniffing, obtener la información sin modificar nada, sin embargo, los métodos son diferentes. Además de interceptar contraseñas, el atacante ingresa a los documentos, mensajes de e-mail y otra información guardada, realizando un downloading o descargas de ésta información a su propia computadora. El Snooping es también realizado con fines de espionaje o robo de información o software [22].

3.8. OSINT (*Open Source Intelligence*)

Las organizaciones también están expuestos a atacantes externos, quienes perfeccionan sus técnicas de ataque para penetrar los sistemas de seguridad, esto lo realizan mediante diferentes fases una de ellas es la recolección de información a través de diferentes técnicas y la obtención de información desde fuentes públicas y abiertas. El modo de ataque es una detallada investigación sobre el objetivo enfocada a obtener toda la información pública disponible sobre la organización desde recursos públicos. En este aspecto, un atacante gastará más de su tiempo en actividades de reconocimiento y obtención de información porque cuanto más aprende el atacante sobre el objetivo, más fácil será llevar a cabo con éxito el ataque [23].

3.9. Troyanos

Es un software malicioso que permite la administración remota de una computadora de forma oculta y sin el consentimiento del propietario. Generalmente están disfrazados como algo atractivo o inocuo que invitan al usuario a ejecutarlo. Pueden tener un efecto inmediato y tener consecuencias como el borrado de archivos del usuario e instalar más programas maliciosos [26].

4. Amenazas en los Sistemas de Control Industrial

Las amenazas son un problema real en los sistemas SCADA y DCS en la actualidad. Desde Stuxnet, primer gusano conocido que atacó las instalaciones nucleares en Irán y que salto todas la protecciones instaladas [24], evidenciando que en términos de protección de instalaciones muchas de las estrategias de las redes de datos deben establecer una serie de actividades complementarias, las cuales conlleven a lograr una mejora en los problemas de seguridad.

Aun no es clara una clasificación de las diferentes amenazas con que se puede ver afectado un sistema ICS, en [20] se muestra la clasificación de amenazas para cualquier sistema en general, organizándolos en 4 elementos claves así:

- Factores humanos
- Fallas en los sistemas de información
- Desastres naturales
- Actos maliciosos o malintencionados

Sin embargo, la generalidad de estas amenazas debe ser caracterizada a las particularidades de un sistema ICS. La Tabla 2, resume algunas diferencias entre los sistemas TI y los sistemas ICS.

Tabla 2. Comparativa de requisitos entre sistemas IT e ICS [21].

REQUISITOS	TI	ICS
De comportamiento.	No requiere tiempo real.	Requiere tiempo real
	Retardos de tiempo pueden ser aceptables.	Retardos de tiempo resultan en problemas graves.
Disponibilidad	El reinicio del sistema es viable bajo ciertos procedimientos.	El reinicio del sistema puede no ser aceptable. Cada cambio, parada etc., debe ser planeada tiempo atrás.
Riesgos	No se requiere tolerancia a fallos , los tiempos muertos son aceptables	La tolerancia a fallos es un requisito primordial.
Funcionamiento del sistema.	Utiliza sistemas operativos típicos	Se basa en sistemas operativos singulares que no tienen en cuenta la seguridad del sistema.
Vida útil	De 3-5 años	De 15-20 años

En [22] se clasifican las amenazas de acuerdo a los siguientes enunciados:

- Posibilidad de una intrusión cuando el sistema ICS se enlace a un sistema de información empresarial o de gestión.
- Posibilidad de una intrusión de manera remota utilizando herramientas de ingeniería social o de fuerza bruta.
- Posibilidad de una intrusión por parte de los proveedores de software y hardware para los sistemas de control, dejando puertos abiertos para accesos remotos y así brindar soporte.
- Posibilidad de una intrusión cuando personal de operación acceda y/u opere el sistema de control de manera remota.
-

También en [25], se puede encontrar la siguiente propuesta en cuanto a amenazas en sistemas SCADA se refiere, considerando que existen dos grandes grupos de amenazas:

- Las amenazas directas como sabotaje industrial realizado mediante ataques coordinados terroristas.
- Las amenazas indirectas como errores operacionales y virus por parte de los operadores del sistema y que, a través de ingeniería social, pueden generar que se vulnere el sistema.

El impacto de cualquiera de estos tipos puede generar en un sistema SCADA la afectación de una infraestructura crítica, que lleve a una pérdida de la disponibilidad del sistema, así como la interrupción del proceso, acompañado de afectaciones a los equipos y, en algunos casos, al personal de operación; perdida de instalaciones así como de datos. Todo esto puede acarrear sanciones de índole personal y la pérdida de confianza del público.

La generalidad de algunas clasificaciones establece un campo amplio por cubrir cada vez que se quiera identificar amenazas en un sistema de control. En [26], se muestra una clasificación detallada de amenazas, clasificándolas como se muestra en la Tabla 3.

Tabla 3. Amenazas en un sistema de control [26]

AMENAZA	INCIDENTE
Operadores	Dirigido al mediante ingeniería social o interrupción del servicio accidentalmente.
Falla del sistema	Por pérdida de energía y falla de fuentes de respaldo.
Falla en la Red	Ocasiona la denegación del servicio, y pérdida de control sobre el proceso.
Hacker	Intrusión o interrupción del servicio.
Malware	Interrupción del servicio o daños a los sistemas
Espías	Extracción de información

Otra clasificación de las amenazas las organiza en categorías como terrorismo, criminal, personal interno, ambientales, etc.

5. Conclusiones

La inclusión de protocolos abiertos al interior de los sistemas de control ha incluido factores de seguridad que antes no eran considerados, inclusive aunque no se usen protocolos abiertos el uso de tecnologías móviles genera un riesgo en la instalación de aplicaciones no deseadas en los dispositivos de control, ejemplo de ello

son las actualizaciones de los proveedores o firmwares de los equipos.

La diferencia entre un ataque a una red de un área IT y una OT es que en la primera solo se verán comprometidas fuentes de información críticas en la empresa y aunque esto puede parecer grave, un ataque en un área OT comprometería no solamente la información sino la maquinaria, los procesos físicos y, lo más importante, la integridad física de las personas dentro del proceso productivo.

La estandarización en la implementación de sistemas de control inserta factores de riesgo que aún necesitan ser suplidos. Utilizar estrategia de IT es un primer avance pero debido a las características propias de los sistemas ICS se deben complementar con otras estrategias para alcanzar mejores niveles de seguridad.

Por último, como se muestra en el presente trabajo, no existe una categorización o clasificación fuerte de las diferentes amenazas que pueden presentar los sistemas ICS, por lo tanto, se debe crear un marco de referencia para generar estrategias de mitigación más efectivas.

Bibliografía

[1] C. Garzón, "Sistemas integrados de información para producción". Facultad de ingeniería. Universidad Nacional, Bogotá. 2000.

[2] J. Prado. "ETHERNET INDUSTRIAL: Modelos y conectividad en el ámbito de procesos industriales", Tesis de Maestría en Redes de Datos. Facultad de informática. Universidad nacional de la plata. Argentina. 2010.

[3] E. Jiménez. "Implementación de las automatizaciones en los dispositivos industriales de control automático". Departamento de ingeniería eléctrica. Universidad de la Rioja. 2010.

[4] Y. Koren, "The global manufacturing revolution", Editorial Wiley. New Jersey.2010.

[5] C. Orsini. "El bus de campo: una aproximación al usuario". Cuaderno Técnico nº 197. Schneider Electric. Pág. 7-10. España. 2003.

[6] Price waterhouse Coopers (PcW), Industrial Security [online]. Romania: PcW.Ro, 2014. Disponible en: http://www.pwc.ro/en/services/ras/assets/industrial_security.pdf

[7] C. E. Spurgeon. "Ethernet: The Definitive Guide" Editorial O'Reilly. USA. 2000.

[8] J.P. Ferrari, "Sistemas de Control Distribuidos," Departamento de Sistemas e Informática. Universidad Nacional del Rosario, 2005.

[9] J. Park, S. Mackay and E. Wright. "Practical Data Communications for Instrumentation and Control". Elsevier. Pág. 7-9. UK. 2003

[10] A. Rodríguez. "Sistemas SCADA". Editorial Marcombo. Tercera edición. Pág. 16-55. España. 2012.

[11] J. Park. S. Mackay. "Practical Data Acquisition for instrumentation and Control system". Elsevier. Pág. 67-96. UK. 2003

[12] B. Hollifield, D Oliver, I.et al. "The High Performance HMI Handbook" Fist Edition. Pág. 47-51. Houston. 2008.

[13] P. Gallagher. "Guide To Industrial Control Systems (ICS) Security". Computer Security Division. Information Technology Laboratory. National Institute of Standards and Technology (NIST). USA. 2011.

[14] B. Forero, "Caracterización del Sistema de Control Distribuido DCS HONEYWELL EXPERION de la unidad central del norte de la gerencia refinería de Barrancabermeja de Ecopetrol S.A,". Tesis de grado. Facultad de Ingeniería Electrónica. Universidad Pontificia Bolivariana, Bucaramanga. 2011.

[15] M.G. Sánchez, "Implementación de sistemas empotrados de control distribuidos bajo el estándar IEC-61499."pp. 1–57, 2013

[16] A. Rosado, "SISTEMAS INDUSTRIALES DISTRIBUIDOS : Una filosofía de automatización," Universidad de Valencia. Notas de Clase. Pag.3–17. España. 2014.

[17] Online. Disponible en http://www.profibus.com/

[18] Online. Disponible http://ab.rockwellautomation.com/es/Networks-and-Communications/DeviceNet-Network.

[19] J. Costas. Seguridad y Alta disponibilidad. Editorial RA-MA. ISBN – 9788499640891, Pág. 10. 2011.

[20] C. Tarazona. Amenazas informáticas y seguridad de la información. Derecho penal y Criminología. Vol. 28, Núm. 84. Pp. 137-146. 2007.

[21] W. Stallings, "Fundamentos de seguridad en redes Aplicaciones y estándares," 2 Edición. Editorial Pearson - Prentice hall, pp. 5, 2004.

[22] J. Roa Buendía. "Seguridad informática", 1 Edición, Editorial McGraw-Hill, pp. 20. 2013.

[23] C. Tori. "Hacking Etico". Argeniss, pp. 88-106. 2008.

[24] OIEA, " Seguridad informática en las instalaciones nucleares," Organismo Internacional de energía atómica, Viena, manual de referencia, No. 17, 2013.

[25] T. Cruz, P. Simões. "Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures". A European FP7 Project – CockpitCI. Informe técnico. Pág. 62-63. 2013.

[26] G. Francia et al. "Security Best Practices and Risk Assessment of SCADA and Industrial Control Systems". Jacksonville State University. USA. 2012.