Máster Interuniversitario en Seguridad de las TIC (MISTIC)

Trabajo de Fin de Master

1er semestre, curso 2017-18

Enero de 2018

Título: Ciberseguridad en Sistemas de Control Industrial o ICSs

Alumno: Henry Alfonso Romero Mestre

henryromero@hotmail.com

Director: Angela María García Valdés

agarciavald@uoc.edu

Empresa: INCIBE

DEDICATORIA

El gran esfuerzo y la dedicación que se necesita para alcanzar cualquier meta en la vida está acompañado por una red de personas que a su vez te dan parte de su vida, sin pedir nada a cambio, para que tu obtengas todo lo que deseas, es mi caso.

En primer lugar está mi esposa, Victoria, quien con su gran tesón, entrega y ganas de hacer bien todo lo que emprende; me ha impulsado a superarme en los momentos en que he deseado desfallecer.

En segundo lugar mis hijos Cristian Karen y Carlos, pensar en ellos me anima, porque es mi deseo ser el mejor ejemplo de padre que la vida les haya podido dar, sé que al ver todo lo que realizo estoy aportando a su propio buen vivir.

Por último, y no menos importante, a mi madre Marina y a mis hermanos y demás familiares quienes con acciones pequeñas y grandes aportaron en la consecución de esta meta.

AGRADECIMIENTOS

Agradezco en primer lugar a Dios por dar la posibilidad de que mi energía esté en este mundo y particularmente por darme la posibilidad física y mental de afrontar el reto de ser magister en seguridad informática.

Durante la maestría me encontré en con muchas temáticas que me fueron difíciles de asimilar, pero con ayuda de los excelentes profesores del master interuniversitario y de los pocos compañeros de carrera con los que interactué, pude superarlas, ellos fueron mi gran soporte en esta carrera.

Un agradecimiento a parte a mi tutor de master, Juan Jose Murgui, por su ánimo y apoyo contínuo durante los semestres que estuve en el master, y a mi tutora de tesis, Angela María García Valdés, por su paciencia y apoyo.

También debo agradecer a los profesores y alumnos de la universidad Distrital en Bogotá D.C., lugar donde laboro, y de la UPC de Valledupar, por darme luz en muchos de los temas que les consulté y que no conseguía comprender.

RESUMEN

Los sistemas informáticos están presentes en casi todas las actividades del ser humano. Permiten que se manipule información de forma digital, transmitiéndola, almacenándola, modificándola y recuperándola. Usamos estos sistemas a diario para trabajar, interactuar socialmente, para ocio, etc; y en general lo hacemos para nuestro beneficio y sin pensar en dañar al otro, sea persona o empresa. Sin embargo, existen muchas personas/empresas criminales cuyos objetivos son los de amenazar y/o vulnerar la información privada, de otras empresas y personas, para obtener ventajas o beneficios, dejando detrás suyo daños en lo moral, en lo económico, en la propiedad intelectual, entre otros.

Los sistemas de control industrial o por sus siglas en inglés ICSs no escapan a lo dicho anteriormente, es más, son de los sistemas informáticos con más riesgos ya que: existe una falsa confianza de que no es fácil que estos riesgos se presenten por lo secreto y cerrado de su hardware, software y estándares que los rigen (diversidad de fabricantes que no les interesa mucho compartir información); el hardware usado típicamente es de baja capacidad de procesamiento y almacenamiento; los protocolos usados no soportan comunicaciones seguras; un mal diseño del tipo de red y su estructura de seguridad. Se presenta, entonces, un rezago en la securización de redes y equipos activos de red, computadores y equipos de campo, que puede ser aprovechado por atacantes maliciosos para causar daños desde mínimos hasta irreparables.

Durante el desarrollo del proyecto se pretende definir, a manera de estudio, cuáles son las diferentes amenazas y vulnerabilidades que se presentan en la actualidad sobre los ICSs, cómo el atacante efectúa los ataques y cuáles son las formas que tienen los afectados para mitigar las intrusiones. Para ello inicialmente se realiza un estudio de la estructura de estos sistemas, desde las configuraciones, tipos, protocolos y estándares existentes; hasta los elementos mínimos del sistema tales como los actuadores y los motores. Además, se estudiarán cómo diferentes amenazas que afectan a las tecnologías de la información TIs, afectan a los ICSs y cuáles son las amenazas particulares en las tecnologías operacionales TOs, estas últimas se dan particularmente el contexto de la industria. Para concluir, se realiza una propuesta de eliminación y mitigación de riesgos en ICSs.

ABSTRACT

Computer systems are present in almost all human activities. They allow you to manipulate information in digital form, transmission, storing, modifying and recovering. We use these systems daily to work, interact socially, for leisure, etc; and in general we do it for our benefit and without thinking of damaging the other person or company. However, there are many criminal people/companies whose objectives are to threaten and/or infringe private information, other companies and individuals, to obtain benefits or benefits, leaving behind their moral, economic, property damage intellectual, among others.

The systems of industrial control or by its acronyms in English ICSs do not escape to the above mentioned, moreover, they are of the computer systems with more risks since: there is a false confidence that it is not easy that these risks are presented by the secret and closed of its hard Ware, software and standards that govern them (diversity of manufacturers who are not very interested in sharing information); The hardware typically used is low processing and storage capacity; The protocols used do not support secure communications; A bad design of the type of network and its security structure. There is, then, a lag in securing networks and active network equipment, computers and field equipment, which can be exploited by malicious attackers to cause damage from minimal to irreparable.

During the development of the project it is intended to define, as a study, what are the different threats and vulnerabilities that are present in the ICSs, how the attacker performs the attacks and what are the forms that have affected them to mitigate intrusions. Initially, a study of the structure of these systems is carried out, from the existing configurations, types, protocols and standards; to the minimum system elements such as actuators and motors. In addition, they will study how different threats affecting the TIs information technologies, affect ICS and what are the particular threats in the operational Technologies TOs, the latter are particularly given the context of the industry. In conclusion, a proposal for the elimination and mitigation of risks is made in ICSs.

CONTENIDO

GLOSARIO

Acceso remoto: acceso a un sistema informático desde un lugar o punto externo a la red donde se encuentra el equipo con el cual se establece la conexión.

Actuador: dispositivo electromecánico que ejecuta las órdenes enviadas desde el centro de control, realizando acciones sobre elementos físicos como puede ser la apertura o el cierre de una válvula.

AGA: American Gas Association, organización sin ánimo de lucro que desarrolla, publica y promueve estándares para la industria del gas natural.

Alarma: aviso o señal que indica la existencia de una situación anormal que requiere atención por parte del personal.

Amenaza: Hecho o acción, intencional o no, que puede comprometer la seguridad o integridad de un sistema.

Ataque: Agresión a la seguridad de un sistema fruto de un acto intencionado y deliberado que viola la política de seguridad de un sistema.

Ataque de denegación de servicio (DoS): ataque informático cuyo objetivo es la interrupción de un equipo o servicio mediante el envío de gran cantidad de peticiones hasta agotar los recursos disponibles del sistema atacado. Una de sus versiones más conocidas es el ataque distribuido de denegación de servicio (DDoS)

Auditoría de seguridad: revisión exhaustiva de la seguridad de algún sistema o procedimiento. Su objetivo es evaluar el nivel de seguridad o cumplimiento para acometer mejoras que solventen las deficiencias encontradas.

Centro Criptológico Nacional (CCN): el CCN-CERT es el Equipo de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional (CCN), dependiente del Centro Nacional de Inteligencia (CNI).

Centro de control: ubicación en la que se encuentra el equipo o conjunto de equipos que permiten la monitorización y/o gestión remota de un proceso de forma centralizada.

Ciberseguridad: también denominada seguridad de la tecnología de la información, se centra en la protección de computadoras, redes, programas y datos, de cambio o destrucción, no intencionados o no, por parte de atacantes no autorizados.

Cifrado: técnica mediante la cual se transforma un texto o mensaje en un conjunto de símbolos ininteligibles. Dicha transformación es reversible únicamente por aquellos que conozcan la clave de cifrado.

CNPIC: el Centro Nacional para la Protección de las Infraestructuras Críticas es el organismo encargado de impulsar, coordinar y supervisar las actuaciones necesarias para garantizar la seguridad de las Infraestructuras Críticas españolas. Depende de la Secretaría de Estado de Seguridad del Ministerio del Interior.

CPNI: Centre for the Protection of National Infrastructure, organismo nacional del Reino Unido para la protección de infraestructuras críticas.

DCS (Distributed Control System): sistema de monitorización y control en el cual cada instalación geográfica cuenta con un sistema propio de control, contando todas ellas con una monitorización común.

Dispositivo de campo: son aquellos equipos que se encuentran en las posiciones de campo, estando dedicados a la medición de parámetros o a la ejecución de órdenes. Engloban principalmente RTUs, PLCs, IEDs y actuadores finales.

ENISA: la European Network and Information Security Agency es una agencia de la Comunidad Europea dedicada a la seguridad de las redes y de la información. Trabaja para las instituciones europeas y los estados miembros, para lo que cuenta con la colaboración de diferentes agentes de toda Europa, tanto públicos como privados.

ICS (Industrial Control System): término genérico que engloba los diferentes tipos de sistemas de control industrial. Incluye sistemas SCADA, DCS y sistemas basados en PLCs.

IEC (International Electrotechnical Commission, Comisión Electrotécnica Internacional): organización líder en el mundo en la preparación y publicación de Normas Internacionales en el campo de la electricidad, la electrónica y tecnologías afines.

IED (Intelligent Electronic Device): dispositivo que incorpora uno o más procesadores con la capacidad de enviar o recibir información u órdenes de control, desde o hacia otros dispositivos.

IT (Information Technology, Tecnología de la Información): Es todo el espectro de tecnologías para el procesamiento de información, incluido software, hardware, tecnologías de comunicaciones y servicios relacionados. En general, TI no incluye tecnologías integradas que no generan datos para uso empresarial.

NERC: La North American Electric Reliability Corporation ha aprobado varias normas de estandarización (CIP-005 y CIP-007) para la protección de las instalaciones energéticas frente a las amenazas de ciberseguridad.

NIST: el National Institute of Standards and Technology es una institución estadounidense dedicada, entre otros aspectos, a la generación de estándares tecnológicos. Es considerada una de las instituciones de referencia más importantes del mundo.

OT (Operational Technology, Tecnología Operacional): Es el hardware y el software que detecta o causa un cambio a través de la supervisión directa y/o control de dispositivos físicos, procesos y eventos en la industria.

Posición de campo: ubicación física, geográfica o lógica en la cual se encuentran los dispositivos finales y dispositivos de campo.

PLC (Programmable Logic Controller): equipo orientado a la ejecución de órdenes específicas, como operaciones de entrada/salida, operaciones lógicas o aritméticas, comunicaciones o envío y ejecución de ficheros.

Riesgo informático: La probabilidad de que una amenaza se materialice, utilizando vulnerabilidad existentes de un activo o un grupo de activos, generando pérdidas o daños.

RTU (Remote Terminal Unit): dispositivo encargado de recolectar información de sensores y actuadores para reenviarla a otro dispositivo.

Sensor: dispositivo que detecta y/o mide una determinada acción o característica (temperatura, presión, etc.) transmitiendo información referente a ella posteriormente.

SCADA (Supervisory Control and Data Acquisition): término genérico que engloba los sistemas capaces de recolectar información, monitorizar y controlar algún proceso en tiempo real y de forma centralizada.

Tecnología de propósito general: hace referencia a aquellos productos tecnológicos de gran difusión en la sociedad frente a los especializados y limitados a ámbitos reducidos.

Vulnerabilidad: Fallo o debilidad en el diseño, la implementación, la operación o la gestión de un sistema, que puede ser explotado con el fin de violar la política de seguridad del sistema.

1. INTRODUCCIÓN

1.1 JUSTIFICACIÓN

Los sistemas de control industrial o ICS hacen parte de nuestra vida cotidiana, están presentes en la generación y suministro de energía eléctrica, gas natural, agua, en el control de edificaciones y viviendas, y también los encontramos en las plantas de producción de empresas de manufactureras, entre otros.
La seguridad informática en los ICSs ha venido tomando mucha importancia en los últimos años ya que las tecnologías operacionales OTs, presentes en los ICSs, y los procesos dentro de ellas están haciendo un mayor uso de estándares comunes presentes en las TICs. Lo anterior ha traído como consecuencia que estos sistemas se vean abocados a las amenazas y vulnerabilidades que se pueden presentar en cualquier sistema informático y por ende a los daños y perjuicios que éstas generan. Los ICSs históricamente no fueron blanco de ataques o amenazas informáticas, ya que eran sistemas muy cerrados que usaban hardware, software, configuraciones, redes y estándares propietarios lo que los hacían de difícil acceso para cualquier atacante, Sin embargo, si la información sobre el ICS se conoce, o si el hardware, software, configuraciones, redes y estándares son típicos, esto puede ser aprovechado por atacantes maliciosos para causar daños desde mínimos hasta irreparables.

1.2 OBJETIVOS

1.2.1 Generales

- Investigar las amenazas, ataques y vulnerabilidades informáticas más comunes en los sistemas de control industrial
- Realizar una propuesta teórica para evitarlas y mitigarlas.

1.2.2 Específicos

- Recopilar la información necesaria que permita conocer a los sistemas de control industrial.
- Realizar un estudio de las vulnerabilidades y amenazas informáticas que más afectan los sistemas de control industrial.
- Realizar un estudio de algunos ataques informáticos relevantes que han sufrido los sistemas de control industrial.
- Analizar las diferentes amenazas con sus contextos en los sistemas de control industrial.
- Realizar una propuesta de alternativas de securización para gestionar diferentes riesgos comunes presentes en sistemas informáticos de sistemas de control industrial.

1.3 METODOLOGÍA

Durante el desarrollo de la investigación de los diferentes riesgos que se presentan en sistemas de control industrial se usarán las siguientes pautas para su desarrollo y conclusión:

- Análisis del problema a resolver.
- Estudio de casos.
- Recopilación de información de los diferentes riesgos:
  - Contextos de los ataques y amenazas
  - Tipos de amenazas.
  - Tipos de ataques.
  - Tipos de vulnerabilidades.
- Recopilación de información de soluciones ante amenazas, ataques y vulnerabilidades.
- Análisis estadístico de información de riesgos y sus soluciones.
- Interpretación de datos estadísticos.
- Estructuración y escritura del documento final que contenga soluciones para el problema planteado.

1.4 TAREAS DEL PROYECTO

Para la obtención de los resultados esperados durante y al final de la investigación se realizaran las siguientes tareas tendientes a cumplir con los objetivos propuestos:

- Realizar un estudio de lo que es un sistema de control industrial.
- Realizar un estudio del estado del arte sobre ciberseguridad en sistemas de control industrial.
- Realizar un estudio y recopilar, información sobre las amenazas más comunes en sistemas informáticos de sistemas de control industrial.
- Realizar un estudio y recopilar, información sobre los ataques más comunes en sistemas informáticos de sistemas de control industrial.
- Realizar un estudio y recopilar, información sobre las vulnerabilidades más comunes en sistemas informáticos de sistemas de control industrial.
- Realizar el procesado la información recopilada en las tareas anteriores.
- Analizar y usar los resultados de la tarea inmediatamente anterior para obtener conclusiones.
- Realizar la propuesta de solución de securización.
- Para todas las tareas anteriores, realizar con mi tutora realimentaciones y correcciones sobre el trabajo parcial o total, si fuese necesario.
- Exponer la propuesta de solución de securización.

1.5 CRONOGRAMA DE ACTIVIDADES

ETAPAS DEL PLAN DE TRABAJO					
Tareas	**Meses de 2017**				**Meses de 2018**
	Septiembre	Octubre	Noviembre	Diciembre	Enero
Gestión del Proyecto					
Recopilación de Información					
Análisis de Riesgos informáticos					
Procesamiento y análisis de la información					
Planteamiento y escritura de la propuesta de solución					
Creación de video y exposición del TFM					

2 ESTADO DEL ARTE

2.1 SEGURIDAD INFORMÁTICA PARA SISTEMAS DE CONTROL INDUSTRIAL EN INSTALACIONES NUCLEARES

EMPRESA: INVAP S. E.

Nikolic, A., Drexler J.

Introducción

Los sistemas de control industrial son cada vez más propensos a ataques informáticos de diversa índole. Se describe la implementación de un programa para aplicar criterios de ciberseguridad en los procesos de diseño y desarrollo de sistemas de control industrial para instalaciones nucleares. Este programa se ha desarrollado en la división de I&C de INVAP SE, y se ha puesto en ejecución en los proyectos que se llevan a cabo en la empresa y que incluyen a un sistema de control.

Antecedentes

Un sistema de control es un conjunto de dispositivos interconectados que es utilizado para manejar, monitorear y comandar a otro conjunto de elementos físicos o sistemas. Un sistema de control industrial es un sistema de control aplicado a un ambiente industrial. Estos sistemas tienen, en general, períodos de operación muy prolongados y se modifican, salvo fallas, cuando requieren una actualización tecnológica o modernización, o necesitan incorporar modificaciones para ampliar sus prestaciones.

Evolución tecnológica

Los sistemas de control industrial evolucionaron de implementaciones con componentes discretos y cableados hacia dispositivos inteligentes distribuidos geográficamente, de gran capacidad de configuración, comunicados con módulos y protocolos estándar. Esta evolución, que pasó de implementaciones, en general propietarias y cerradas, a implementaciones de arquitectura abierta, basada en tecnológica digital con estándares de tecnología de información (TI) de dominio público, hizo que un conjunto de vulnerabilidades, presentes en la plataforma de TI, apareciera en los sistemas de control. Estas vulnerabilidades, si fueran aprovechadas por algún atacante, podrían generar consecuencias muy graves.

Seguridad informática

La seguridad informática en la plataforma de TI ha ido evolucionando a la par de la evolución tecnológica de TI. Esto se debe fundamentalmente a la popularidad de los medios de TI y porque hay cada vez mayor dependencia de las sociedades en esa plataforma. Sin embargo, muchos de los criterios de seguridad desarrollados en el ambiente de TI no son inmediatamente aplicables a los ambientes industriales.

Esto se debe a varias razones, pero dos de ellas son clave:

- Los sistemas de control operan sobre procesos físicos, donde el concepto de tiempo real es de crucial importancia. Un servidor de correo electrónico puede quedar fuera de línea por algunos minutos sin mayores consecuencias, mientras que, en un sistema de control, si un evento no es informado a tiempo, podría llegar a impactar negativamente en el proceso que se está controlando.
- De las tres características a proteger con respecto a la información: confidencialidad, disponibilidad e integridad, el ambiente de TI privilegia la confidencialidad, mientras que el ambiente de control requiere la disponibilidad, por lo que los métodos de protección son distintos.

2.2 SISTEMAS DE CONTROL INDUSTRIAL – UN OBJETIVO DE GRAN VALOR PARA LOS ATACANTES CIBERNÉTICOS

EMPRESA: CYBERARK

Durante décadas los sistemas de control industrial (siglas en inglés ICS) y los sistemas de producción crítica que forman parte del entorno de tecnología operativa (siglas en inglés OT) en empresas industriales, estuvieron apartados de otros sistemas o de Internet. Pero a medida que los sistemas de TI y los entornos de OT aumentan la conectividad entre ellos, los sistemas de control industrial están expuestos ahora a sistemas de TI y a Internet, aumentando de manera importante el riesgo de intrusión por individuos malintencionados.

La adición de equipo comercial disponible (siglas en inglés COTS) a las operaciones y niveles de supervisión de arquitecturas ICS en las que se encuentran las interfaces de máquina humana (siglas en inglés HMI), historiadores, estaciones de trabajo de ingeniería y otros activos informáticos ha introducido nuevos riesgos

asociados con el funcionamiento de sistemas operativos comerciales. Debido a los requerimientos de alta disponibilidad de los activos de ICS, por lo general, siguen sin abordarse en ICS. Algunos de estos riesgos incluyen:

- El elevado número de cuentas administrativas o privilegiadas que permiten acceso del usuario y de la aplicación a ICS.
- El uso de cuentas compartidas que permiten acceso a sistemas críticos sin supervisión individual
- El uso de aplicaciones industriales con credenciales incrustadas codificadas
- El uso de estaciones de trabajo con todos los derechos de administrador

Para mitigar estos riesgos y abordar los requisitos de cumplimiento, las empresas industriales deben proteger y controlar de manera proactiva las cuentas privilegiadas que permiten acceso a los entornos de ICS. La solución de seguridad de cuenta privilegiada de CyberArk sirve de ayuda para que las organizaciones protejan, supervisen y controlen el acceso a cuentas privilegiadas que proporcionan acceso al núcleo de estos sistemas críticos. La solución de CyberArk ofrece protección integral de cuenta privilegiada para sistemas de control industrial que permiten a las organizaciones lo siguiente:

- Descubrir todas las cuentas privilegiadas y relaciones de confianza en los entornos de Windows y Unix
- Eliminar y almacenar de forma segura las credenciales codificadas de las aplicaciones industriales
- Guardar de forma segura y automatizar la rotación de credenciales de cuenta privilegiada (contraseñas y claves SSH), incluidas las utilizadas por usuarios y aplicaciones remotas
- Proteger sesiones privilegiadas, que aíslan a los sistemas críticos de los dispositivos del usuario vulnerables utilizando un servidor de
- salto reforzado que proporciona también grabación de sesión privilegiada y funciones de supervisión en vivo
- Conceder políticas de mínimos privilegios para super-usuarios en sistemas críticos
- Recibir alertas en tiempo real sobre actividad de cuenta privilegiada anómala

La solución de CyberArk está integrada en una sola plataforma, gestionada detrás de un solo panel de vidrio, probada a escala en entornos de OT grandes, complejos y distintos. Esto quiere decir que CyberArk puede ayudar a las organizaciones a llevar a cabo eficacias operativas al gestionar muchas cuentas de usuarios con supervisión pormenorizada y diversos flujos de trabajo de autorización.

Ventajas clave:

- Identificar riesgos de cuenta privilegiada localizando a todos los usuarios privilegiados y cuentas de aplicación, credenciales y relaciones de confianza, incluidas las cuentas asociadas con acceso remoto.
- Reducir el riesgo de acceso desautorizado a sistemas críticos protegiendo y controlando el acceso a cuentas privilegiadas
- Fortalecer la seguridad de la aplicación industrial eliminando el uso de credenciales codificadas
- Permitir el acceso remoto seguro al tiempo de reducir el riesgo de que se propague el malware desde los dispositivos de usuario a los sistemas críticos
- Abordar los requerimientos de cumplimiento con un seguimiento de auditoría completo de acceso a cuenta privilegiada y actividad de usuario
- Reducir el riesgo de abuso intencionado o mal uso accidental de privilegios de usuario elevados
- Acortar considerablemente la ventana de oportunidad de un atacante y reducir el daño alertando en tiempo real priorizado y preciso de ataques en marcha

Normas y reglamentaciones:

- La solución de seguridad de cuenta privilegiada de CyberArk permite a las organizaciones cumplir diversas normas y reglamentaciones de la industria en relación con la seguridad de cuenta privilegiada, entre las que se incluyen las siguientes:
- Corporación Norteamericana de Fiabilidad Eléctrica, Protección de Infraestructura Crítica (siglas en inglés NERC CIP)

- Instituto Nacional de Normas y Tecnología (siglas en inglés NIST) SP-800-82
- Agencia de Seguridad de las Redes y de la Información de la Unión Europea (siglas en inglés (ENISA)

2.3 SEGURIDAD EN PROTOCOLOS DE SISTEMAS DE CONTROL INDUSTRIAL EMPRESA: INCIBE

Ciberseguridad de España

Desde el 28 de octubre de 2014, el Instituto Nacional de Tecnologías de la Comunicación, S.A. (INTECO) pasa a llamarse INCIBE S.A, según el acuerdo adoptado en Junta General del 27 de octubre de 2014. Con dicho cambio de denominación e imagen, INCIBE proyecta una identidad acorde con su orientación estratégica y posicionamiento como centro nacional de referencia en ciberseguridad.

El Instituto Nacional de Ciberseguridad de España (INCIBE), sociedad dependiente del Ministerio de Industria, Energía y Turismo (MINETUR) a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información (SETSI), es la entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de los ciudadanos, la red académica y de investigación española (RedIRIS) y las empresas, especialmente para sectores estratégicos.

Como centro de excelencia, INCIBE es un instrumento del Gobierno para desarrollar la ciberseguridad como motor de transformación social y oportunidad para la innovación. Para ello, con una actividad basada en la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia, INCIBE lidera diferentes actuaciones para la ciberseguridad a nivel nacional e internacional.

El CERT de Seguridad e Industria, centro de respuesta a incidentes de ciberseguridad operado por INCIBE, trabaja para aumentar la capacidad de detección y alerta temprana de nuevas amenazas, la respuesta y análisis de incidentes de seguridad de la información, aumentar la ciberresiliencia de las organizaciones y el diseño de medidas preventivas para atender a las necesidades de la sociedad en general y, en virtud del Convenio de Colaboración suscrito entre la Secretaría de Estado de Seguridad del Ministerio del Interior y la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información,

a las necesidades de seguridad de las infraestructuras críticas, de apoyo en la investigación y lucha frente a ciberdelitos y ciberterrorismo.

En las últimas décadas, el aumento del número de dispositivos con conectividad a internet y con alta capacidad de proceso, ha traído consigo la necesidad de adoptar las medidas de seguridad necesarias. Sin embargo podemos afirmar que, en general, estas adaptaciones de seguridad no han seguido el mismo ritmo de crecimiento que las nuevas tecnologías y nuevos dispositivos han mantenido.

En este sentido, las infraestructuras de Sistemas de Control Industrial no son una excepción y se ven igualmente afectadas por esta corriente evolutiva, incluso con mayor impacto puesto que, los protocolos de comunicación utilizados en este tipo de plataformas son en su mayoría antiguos e intrínsecamente débiles en cuanto a seguridad se refiere.

La tendencia observada en la detección de amenazas deja patente que las infraestructuras industriales han pasado a convertirse en un importante objetivo de ataques informáticos. Prueba de ello, son los cada vez más numerosos incidentes y eventos relacionados con este tipo de infraestructuras que, según el informe de amenazas de DELL en 2014 se dobló el número de incidentes relacionados con estas estructuras. La evolución temporal de algunos hitos importantes se puede ver en la siguiente línea temporal:

Línea temporal de amenazas en SCI

- Línea temporal de principales amenazas descubiertas en sistemas SCI - La imagen tradicional de sistemas de control industrial totalmente aislados ha dejado de ser real debido a las necesidades y circunstancias modernas, tal y como vimos en el artículo de segmentación en ICS. A día de hoy se hace necesaria una reevaluación de los habituales mecanismos de seguridad perimetral y segmentación.

Con este argumento en mente, INCIBE publica un estudio sobre algunos de los protocolos ICS más usuales, con el objetivo de aportar una visión sobre los detalles de seguridad que deben tenerse en cuenta a la hora de desplegar estos protocolos industriales en ecosistemas heterogéneos.

En este estudio se introducen las características generales a tener en cuenta en el diseño de una infraestructura de red ICS haciendo una parada por cada uno de los elementos de seguridad que se pueden encontrar en cualquier implementación de red típica: cifrado, autenticación, control de acceso, políticas de gestión de la seguridad, etc. Siguiendo esta aproximación genérica se pasa a

realizar un análisis de seguridad de algunos de los protocolos ICS más frecuentes: CIP, Modbus, DNP3, Profibus, Profinet, Powerlink Ethernet, OPC y Ethercat.

3 MARCO CONCEPTUAL

A continuación se definirán los diferentes conceptos que son necesarios para la comprensión de los sistemas ICSs, sus tipos y componentes más significativos, y los problemas de securización que le son inherentes y que pueden afectarlos.

3.1 Sistemas de Control Industrial o ICSs

El término sistema de control industrial (ICS) se refiere a una variedad de sistemas compuestos por computadoras, dispositivos eléctricos, hidráulicos y mecánicos, y procesos manuales supervisados por humanos que monitorean y controlan todo tipo de proceso físico. Estos sistemas realizan el control automatizado o parcialmente automatizado de los equipos en las empresas manufactureras, las plantas químicas, las plantas nucleares, los sistemas de la distribución y del transporte de gas, agua y electricidad; y muchas otras industrias.

Los ICs abarcan a varios tipos de sistemas de control, sistemas de control de supervisión y adquisición de datos (SCADA), sistemas de control distribuido (DCS) y otras configuraciones de sistemas de control como Controladores lógicos programables (PLC) encontrados a menudo en los sectores industriales y las infraestructuras críticas.

Un ICS consiste en combinaciones de componentes de control (lógicos, eléctricos, mecánicos, hidráulicos, neumáticos) que actúan conjuntamente para lograr un objetivo industrial (por ejemplo, la fabricación y/o el transporte de materia o energía). La parte del sistema que se refiere principalmente a producir la salida se conoce como el proceso. La parte de control del sistema incluye la especificación de la salida o rendimiento deseado. El control puede ser completamente automatizado o puede incluir a un ser humano en el bucle. Los sistemas se pueden configurar para operar el modo de bucle abierto, de bucle cerrado y manual. En los sistemas de control de bucle abierto la salida es controlada por los ajustes establecidos. En los sistemas de control de bucle cerrado, la salida tiene un efecto en la entrada de manera que se mantenga el objetivo deseado. En modo manual el sistema es controlado totalmente por los seres humanos. La parte del sistema preocupada principalmente por mantener la conformidad con las especificaciones se conoce como el controlador (o control). Un ICS típico puede contener numerosos bucles de control, interfaces humano-máquinas

(HMIs), y herramientas de diagnóstico y mantenimiento remoto creadas mediante una serie de protocolos de red. Los procesos industriales del control de los ICSs se utilizan típicamente en industrias del sector eléctrico, agua y aguas residuales, aceite y gas natural, productos químicos, transporte, farmacéutico, pulpa y papel, alimento y bebida, y fabricación de automotores, aeroespacial, y de mercancías durables.

En la figura siguiente se describe de manera general a un ICSs

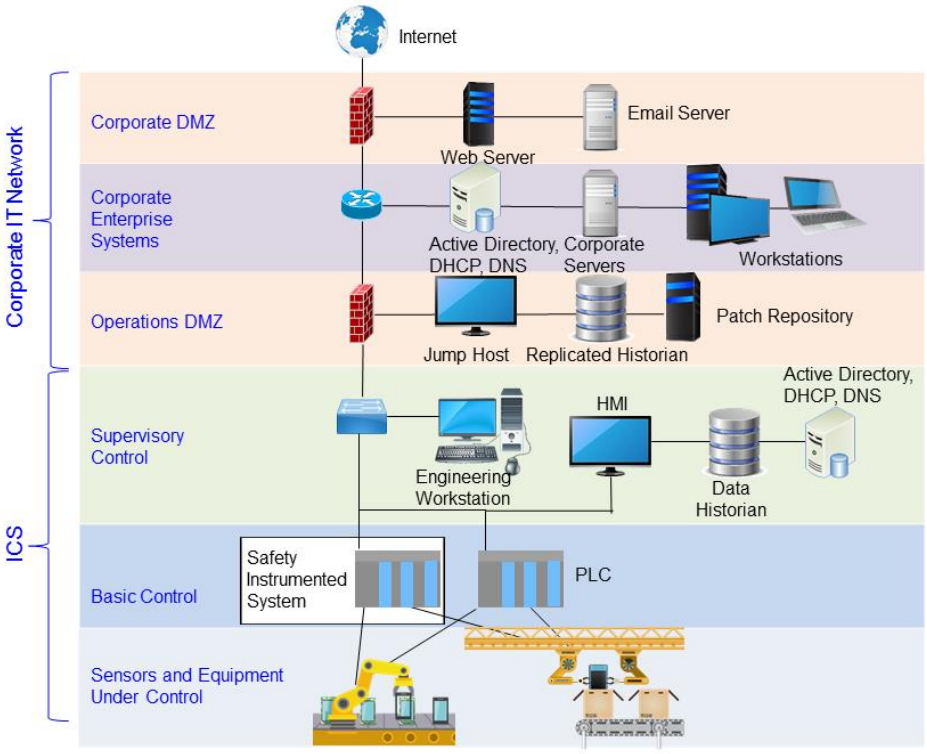


Imagen tomada de https://arxiv.org/ftp/arxiv/papers/1708/1708.07424.pdf

3.2 SCADA

SCADA viene de las siglas de "Supervisory Control And Data Acquisition", es decir: adquisición de datos y control de supervisión. Se trata de una aplicación software especialmente diseñada para funcionar sobre ordenadores en el control de producción, proporcionando comunicación digital con los dispositivos de campo (controladores autónomos, autómatas programables, los instrumentos y actuadores, e interfaz gráfica de alto nivel con el usuario (pantallas táctiles, ratones o cursores, lápices ópticos, etc.…)) que permiten el acceso a datos remotos y controlando el proceso de forma automática desde la pantalla del ordenador, dispositivos móviles o cualquier hardware programable con

posibilidad de establecer interfaz con el humano. Además, provee de toda la información que se genera en el proceso productivo a diversos usuarios, tanto del mismo nivel como de otros supervisores dentro de la empresa: control de calidad, supervisión, mantenimiento, etc.

Los sistemas SCADA integran sistemas de adquisición de datos con sistemas de transmisión de datos y software HMI para proporcionar un sistema de monitoreo y control centralizado para numerosas entradas y salidas de procesos. Los sistemas SCADA están diseñados para recopilar información de campo, transferirla a un centro de cómputo central, y mostrar la información al operador gráfica o textualmente, permitiendo así al operador monitorear o controlar todo un sistema desde una ubicación central en tiempo casi real.

El hardware típico incluye un servidor de control colocado en un centro de control, equipos de comunicaciones (por ejemplo, radio, línea telefónica, cable o satélite), y uno o más sitios de campo distribuidos geográficamente que consisten en unidades terminales remotas (RTUs) y/o PLCs, que controlan a los actuadores y/o monitorizan los sensores. El servidor de control almacena y procesa la información de las entradas y salidas de las RTUs, mientras que las RTUs o los PLCs controlan los procesos locales. El hardware de comunicaciones permite la transferencia de información y datos de un lado a otro entre el servidor de control y los RTUs o PLCs. El software está programado para decirle al sistema qué y cuándo supervisar, qué rangos de parámetros son aceptables y qué respuesta iniciar cuando los parámetros cambian fuera de los valores aceptables. Un dispositivo electrónico inteligente (IED), como un relé de protección, puede comunicarse directamente con el servidor de control, o una RTU local puede sondear los IEDs para recoger los datos y pasarlos al servidor de control. Los IEDs proporcionan una interfaz directa para controlar y monitorear equipos y sensores. Los IEDs pueden ser sondeados y controlados directamente por el servidor de control y en la mayoría de los casos tienen programación local que permite que actúe sin instrucciones directas del centro de control. Los sistemas SCADA generalmente están diseñados para ser sistemas tolerantes a fallas con redundancia significativa incorporada en el sistema. La redundancia puede no ser una contramedida suficiente frente a un ataque malicioso.
Dentro de los componentes y la configuración general de un sistema SCADA encontramos a los siguientes: el centro de control que alberga un servidor de control y los routers de comunicaciones. Otros componentes del centro de

control incluyen la interfaces humano-máquina HMIs, estaciones de trabajo, y el servidor de historial de datos, que están conectados a una LAN. El centro de control recopila y registra la información recopilada por los sitios de campo, muestra información a la HMI y puede generar acciones basadas en eventos detectados. El centro de control también es responsable de alarmas centralizadas, análisis de tendencias y reportes. En el sitio de campo se realiza el control local de los sensores de los actuadores y de los monitores. Los sitios de campo a menudo están equipados con una capacidad de acceso remoto para permitir a los operadores realizar diagnósticos remotos y reparaciones, por lo general usan un módem de marcación separada o una conexión WAN. Los protocolos de comunicación estándar y propietarios que se ejecutan sobre comunicaciones en serie y en red se utilizan para transportar información entre el centro de control y los sitios de campo utilizando técnicas de telemetría como línea telefónica, cable, fibra y frecuencia de radio como la radiodifusión, el microondas y el satélite.

Las topologías de comunicación SCADA varían entre implementaciones. Las diversas topologías utilizadas, incluyendo punto a punto, serie, serie-estrella, y multi-punto. La punto-a-punto es funcionalmente el tipo más simple; sin embargo, es costoso debido a los canales individuales necesarios para cada conexión. En una configuración en serie, se reduce el número de canales utilizados; sin embargo, el intercambio de canales tiene un impacto en la eficiencia y complejidad de las operaciones de SCADA. De manera similar, el uso de un canal por dispositivo en las configuraciones de serie y de multi-punto resulta en una menor eficiencia y una mayor complejidad del sistema.

Ejemplo de un esquema de un sistema SCADA

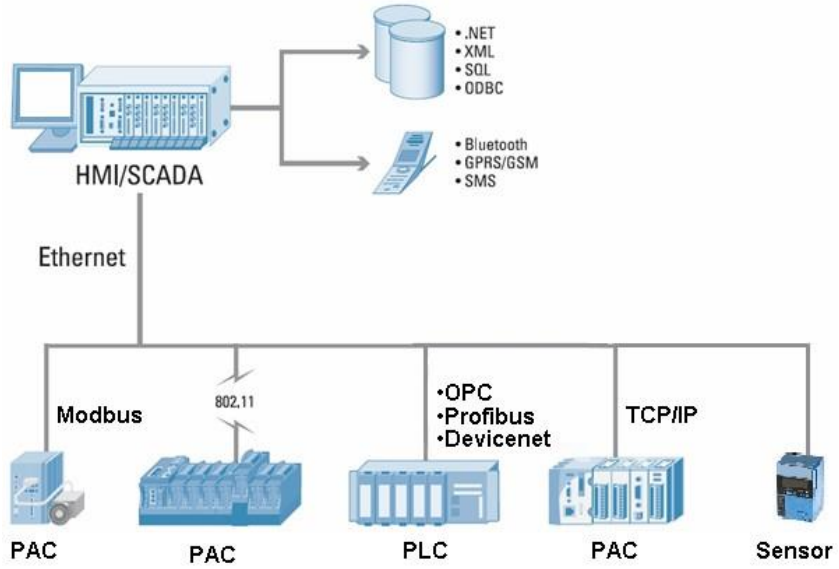


Imagen tomada de http://www.eps-logix.com/wp-content/uploads/2014/07/SCADA.jpg

3.3 DCSs Sistemas de Control Distribuido

Los DCSs se utilizan para controlar procesos industriales como la generación de energía eléctrica, refinerías de petróleo y gas, tratamiento de agua y aguas residuales, y la producción de productos químicos, alimentos y automóviles. Los DCSs se integran a los ICSs como una arquitectura de control que contiene un nivel de supervisión y de control que supervisa múltiples subsistemas integrados que son responsables de controlar los detalles de un proceso localizado. El control del producto y del proceso se consigue generalmente mediante la implementación de bucles de retroalimentación o de compensación mediante los cuales las condiciones clave del producto y/o del proceso se mantienen automáticamente alrededor de un punto de ajuste deseado. Para lograr el producto deseado y/o tolerancia de proceso alrededor de un punto determinado, se emplea un controlador lógico programable específico (PLC) en el campo y los ajustes proporcionales, integrales, y/o diferenciales en el PLC se calibran para proporcionar la tolerancia deseada, así como la tasa de auto-corrección durante el desajuste del proceso. Los DCSs se utilizan ampliamente en industrias basadas en procesos.

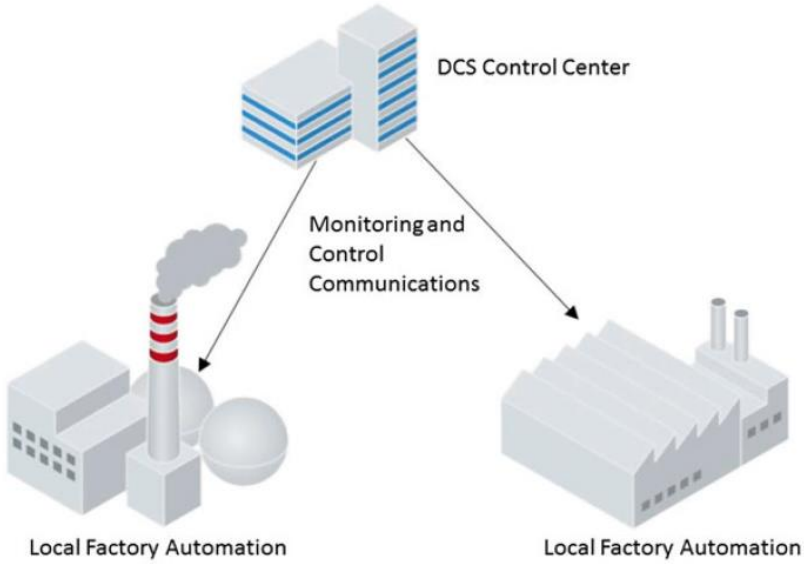


Imagen tomada de http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

3.4 PLCs Controladores Lógicos Programables

Los PLCs son dispositivos de estado sólido basados en computadoras que controlan equipos y procesos industriales. Si bien los PLCs son componentes del sistema de control que se utilizan en los sistemas SCADA y DCS, son a menudo los

componentes principales en configuraciones de sistemas de control más pequeños que se utilizan para proporcionar control regulado de procesos discretos como líneas de ensamblaje de automóviles. Los PLCs se utilizan ampliamente en casi todos los procesos industriales.

Internamente los PLCs son controlados por microprocesadores que leen las señales de entrada de los sensores, ejecutan las instrucciones programadas utilizando estas entradas, así como las órdenes de los controladores de supervisión, y crean señales de salida que pueden cambiar o ajustar el estado de interruptores o activar/desactivar a los actuadores. Un PLC es el primer tipo de controlador de los ICS y es el límite entre el mundo cibernético y el "mundo real".

Un PLC funciona a menudo en localizaciones alejadas y expuesto a condiciones ambientales ásperas (por ej., temperatura, calor, vibración, campos electromagnéticos).

Un PLC opera un sistema operativo en tiempo real (RTOs) que es muy diferente de los sistemas operativos de escritorio como Microsoft Windows. El bucle de control que administra el PLC requiere un ciclo de ejecución y exploración determinista sin bloqueo. El tiempo para leer todas las entradas, ejecutar la lógica y las salidas de escritura sólo dura unos pocos milisegundos. El ciclo se repetirá continuamente. Los PLCs modernos pueden usar un micro-kernel derivado de UNIX y presentar una interfaz web incorporada (sistemas embebidos).

Los PLCs modernos pueden ser programados en un idioma propietario o un lenguaje estándar de la industria.

Existen cinco lenguajes de programación estandardizados para ICS: diagrama del bloque de la función (FBD), diagrama de la escala (LD), texto estructurado (St), lista de la instrucción (IL), y tabla secuencial de la función (SFC) (Comisión electrotécnica internacional [IEC] 61131-3 2003).

Un PLC dispone de una fuente de alimentación, unidad de procesamiento central (CPU), interfaz de comunicaciones y módulo (s) de entrada/salida (I/O). Un módulo de e/s puede ser digital o analógico. Un módulo de entrada digital mide un "1" o "0" según la tensión de entrada.

Un módulo de entrada analógica recibe una medición de corriente o de tensión de un sensor correspondiente al parámetro físico que se está midiendo. Los sensores como termómetros, manómetros, medidores de flujo y velocímetros pueden emitir señales de entrada analógica.

Existen dos tipos de módulos de salida digital. El primer tipo produce una tensión que corresponde a un "1" o "0". El segundo tipo de módulo de salida digital es un

relé electrónico que abre o cierra sus contactos. En contraste con un módulo de salida digital, el módulo de salida analógica PLC ofrece una corriente o voltaje variable que es ajustado por el programa del PLC durante cada ciclo de escaneo. Por otra parte, el empaquetado modular moderno de los componentes del PLC permite las configuraciones modulares de los módulos de la entrada-salida del sistema, el reemplazo rápido en caso de un módulo que falla, y opcionalmente apoya los módulos redundantes de la batería de la CPU y de reserva.
Los PLCs se encuentran en varios tipos de ICSs y típicamente usan una red local para comunicarse con procesos de supervisión usando, por ejemplo, enlaces de serie, óptica o Ethernet.

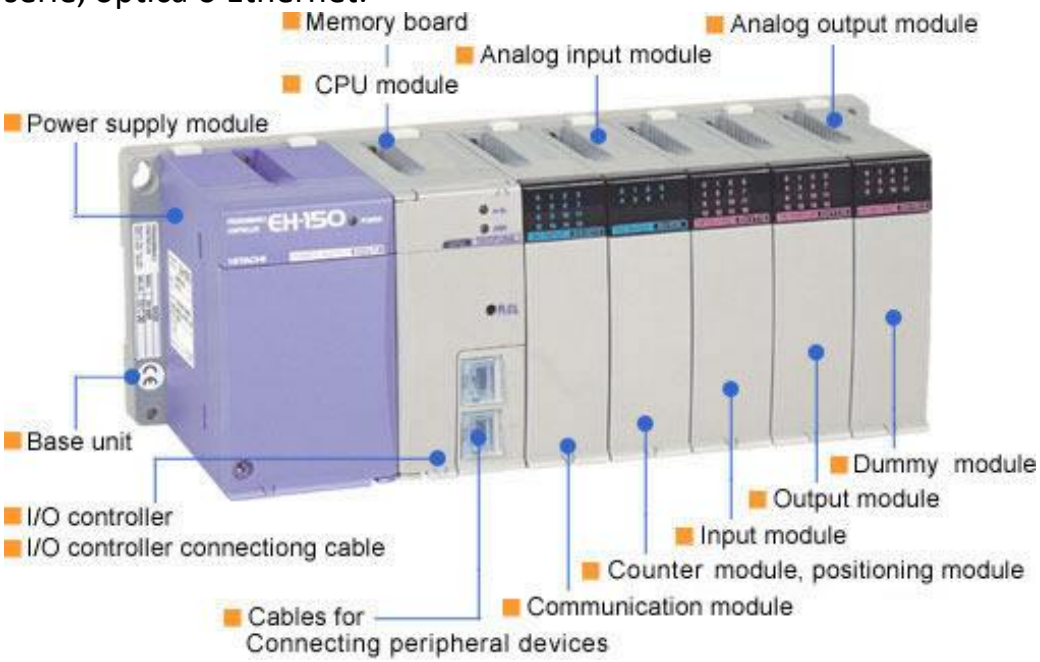


Imagen tomada http://www.instrumentationengineers.org/2013/05/parts-or-components-of-plc.html

3.5 HMIs Interfaces Humano Máquina (Human Machine Interfaces)

Cierto es que todos los sistemas SCADA ofrecen una interfaz gráfica PC-Operario tipo HMI, pero no todos los sistemas de automatización que tienen HMI son SCADA Las HMIs Comprenden los sinópticos de control y los sistemas de presentación gráfica.
HMI (Human Machine Interface) se define como un panel a través del cual el operador es capaz de controlar la maquinaria y ver diferentes procesos en una planta. Las HMI tienen un Panel Sinóptico cuya función es la de representar, de forma simplificada, el sistema bajo control (un sistema de aprovisionamiento de agua, una red de distribución eléctrica, una factoría). En un principio los paneles sinópticos eran de tipo estático, colocados en grandes paneles plagados de

indicadores y luces. Con el tiempo han ido evolucionando, junto al software, en forma de representaciones gráficas en pantallas de visualización (PVD, Pantallas de Visualización de Datos).

En los sistemas complejos suelen aparecer los terminales múltiples, que permiten la visualización, de forma simultánea, de varios sectores del sistema. De todas formas, en ciertos casos, interesa mantener la forma antigua del Panel Sinóptico, pues la representación del sistema completo es más clara para el usuario al tenerla presente y no le afectan los eventuales fallos de alimentación de componentes o de controladores gráficos.

Ejemplo de una interfaz HMI.

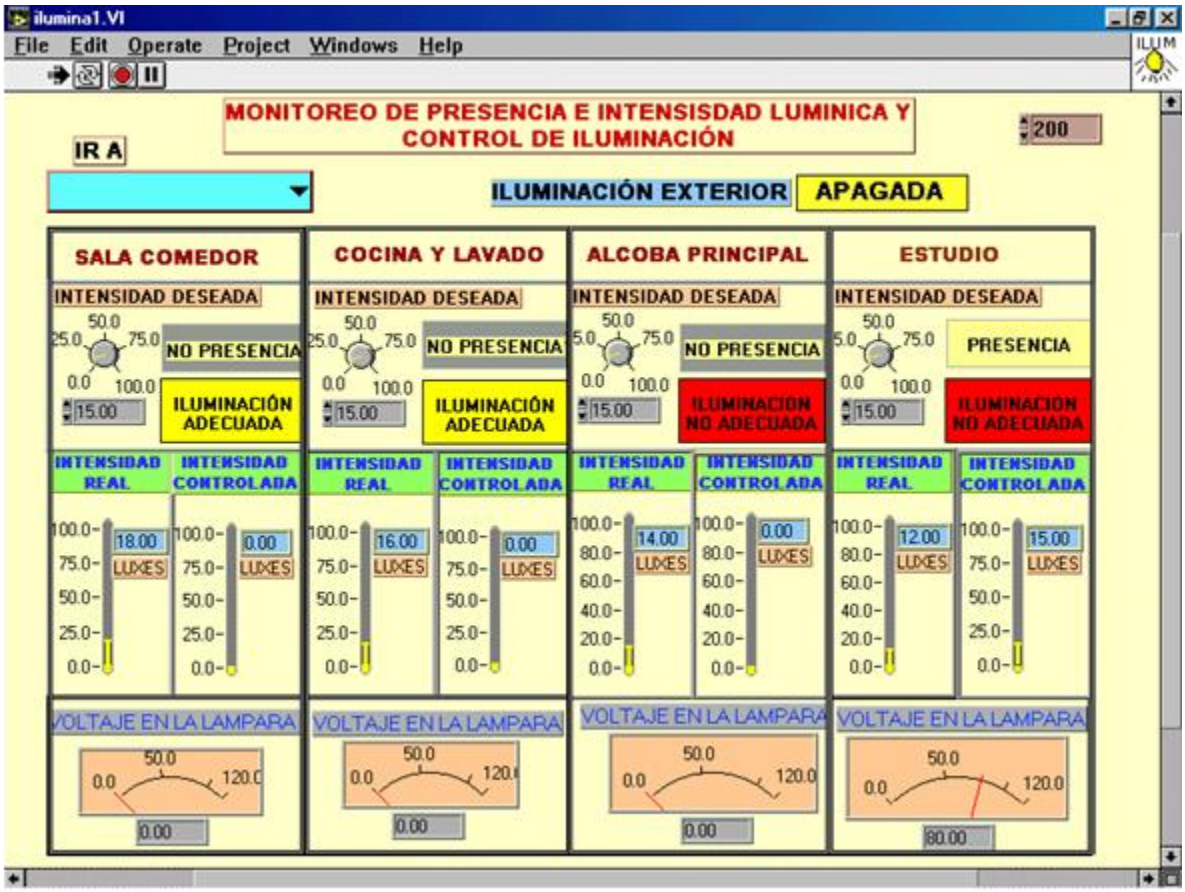


Imagen propia

3.6 RTU Unidad Terminal Remota (Remote Terminal Unit)

Una RTU es un dispositivo electrónico controlado por microprocesadores y está diseñado para entornos agresivos (por ejemplo, temperatura, calor, vibración, campos electromagnéticos). Existen dos tipos de RTUs: Estaciones de RTUs y RTUs de campo. Los RTUs de campo reciben señales de entrada de dispositivos y

sensores y, a continuación, ejecutan la lógica programada con estas entradas. En las RTUs de campo se reúnen los datos mediante el sondeo de los dispositivos/sensores de campo en un intervalo de tiempo predeterminado. Los RTUs de campo son interfaces entre los dispositivos/sensores y las estaciones RTUs.

Las estaciones RTUs también se encuentran en sitios remotos y reciben datos de las RTUs de campo así como órdenes de los controladores de supervisión. A continuación, la estación RTU crea valores de salida para controlar los dispositivos físicos y a través de ellos los procesos físicos. Un centro de control se comunica con una estación RTU. Estos dos tipos de RTUs, las de campo y las estaciones, pueden combinarse en una sola RTU física.

3.7 IED Dispositivo electrónico inteligente (Intelligent Electronic Device)

En el dominio ICS, un dispositivo electrónico inteligente (IED) es cualquier dispositivo que incorpore uno o más procesadores con la capacidad de recibir o enviar datos/control desde o hacia una fuente externa (p. ej., contadores electrónicos de múltiples funciones, relés digitales, controladores). Un IED es el tercer tipo de controlador de ICS. Las empresas de servicios públicos están desplegando IEDs en sus subestaciones para mejorar la automatización y el fl ujo de información a sus redes empresariales. Un IED puede ser sondeado ya sea por un proceso de automatización (controlador o un servidor de aplicaciones desarrollado a la medida) en el centro de control o por una RTU en un sitio de campo a través de comunicación serial, Ethernet o incluso un enlace inalámbrico. Un IED también se conoce como un relé de protección digital o un relé basado en microprocesador. Un IED realiza funciones de protección, control, monitoreo, medición y comunicaciones. Algunos IEDs pueden tener capacidades más avanzadas que otras IEDs.

Dentro de los ejemplos de las funciones de protección de los IEDs están la detección de fallas en una subestación tales como sobrecorriente, fallas de tierra, discontinuidad de fase, así como condiciones de sobretensión y bajo voltaje. Una función de control de los IEDs puede incluir control local y remoto de hasta doce dispositivos de conmutación y proporcionar una visualización y controles al operador en el panel frontal del dispositivo. La capacidad de monitoreo puede informar sobre la condición de interruptores y grabar eventos. Un IED con una función de medición puede rastrear corrientes trifásicas, corriente neutra, potencia activa y otras métricas de corriente, voltaje o potencia. La función de

comunicaciones consiste en las tecnologías de red disponibles para que el IED se comunique con los componentes de supervisión.

3.8 Estación de trabajo de ingeniería

La estación de trabajo de ingeniería es típicamente un ordenador de mesa o un servidor que ejecuta un sistema operativo estándar como Microsoft Windows o Linux. Esta máquina aloja el software de programación para controladores (es decir, PLC, RTU, IED) y sus aplicaciones.

Los ingenieros utilizan esta plataforma para hacer cambios a la lógica del controlador y de las aplicaciones industriales. También pueden desplegar cambios en el firmware de los dispositivos lógicos mediante una tarjeta de memoria. La lógica del proceso de automatización y los datos se almacenan en los archivos de proyecto alojados en la estación de trabajo de ingeniería.

3.9 Historiador de datos

Un historiador de datos (también llamado "historiador operacional") es una aplicación de software que recoge datos de procesos de automatización en tiempo real y los agrega en una base de datos para análisis simultáneos y posteriores. Los mismos datos que se muestran en una HMI se almacenan en el historiador de datos y cada dato es registrado. Un historiador de datos suele ser una estación de trabajo de tipo escritorio o un servidor que ejecuta un sistema operativo estándar como Microsoft Windows o Linux. Algunos historiadores de los datos utilizan una base de datos relacional para el almacenaje de tales datos. Sin embargo, el historiador de datos no es lo mismo que un sistema de base de datos de TI. Un historiador de datos está diseñado para una recopilación muy rápida de datos sin perderlos, no admite integridad referencial en tablas y utiliza protocolos de interfaz industrial. El historiador de datos puede tener interfaces con protocolos industriales como Modbus o comunicaciones de plataforma abierta (OPC) para conectarse directamente a una HMI, PLC o RTU para recuperar datos.

3.10 Pasarelas de comunicaciones

Un Gateway de comunicaciones permite que dos dispositivos con protocolos disímiles se comuniquen. Este dispositivo transforma los datos de un sistema de envío para que coincidan con el protocolo y el medio de transmisión de un host

de destino. Un ejemplo de esta transformación es la traducción de mensajes Modbus en un enlace serie (recomendado estándar-232 [RS-232]/RS-485) a los mensajes OPC en Ethernet.

3.11 Procesador de Front End

Un procesador de front end (FEP) es un procesador de comunicaciones dedicado. Se utiliza un FEP cuando un servidor HMI o de centro de control necesita sondear la información de estado de múltiples RTUs o IEDs. Al usar un FEP, el tiempo de procesamiento y las latencias debidas a los enlaces WAN no interferirá con un operador de planta ejecutando funciones de control en una HMI. Un FEP puede incluir funciones de Gateway de comunicaciones como la conversión de protocolos propietarios de proveedores a los estándares abiertos.

3.12 Dispositivos de Campo

Son los sensores, transductores, actuadores y maquinaria que se conectan directamente con un controlador (es decir, PLC, RTU o IED) a través del módulo de e/s digital o analógico. Un dispositivo de campo también puede utilizar un protocolo industrial como Modbus o PROFIBUS para comunicarse con el controlador. Los sensores miden las características del "mundo real" y representan esta información en señales digitales o analógicas para la entrada del controlador.

Los sensores están disponibles para medir la temperatura, la humedad, la presión, el sonido, la vibración, el voltaje y la corriente, así como otras características físicas. Los ejemplos de los actuadores son los reguladores de la válvula, los reguladores del motor, los convertidores de frecuencia, y los solenoides que están controlando los motores, las bombas, las válvulas, las turbinas, los agitadores, los quemadores y los compresores.

A su vez, los actuadores accionados eléctricamente pueden, por ejemplo, presurizar circuitos hidráulicos para amplificar las fuerzas físicas controladas.

4 Amenazas y Vulnerabilidades en Sistemas de Control Industrial o ICSs

Un ICS moderno es un sistema complejo que depende de muchos componentes y tecnologías diferentes para monitorear y controlar los procesos físicos; junto con muchas de las responsabilidades gerenciales, administrativas y regulatorias asociadas con esta tarea.

El corazón de ICSs es tecnología operacional (TO) que apoya la disponibilidad y la seguridad de procesos críticos. Los ICSs de hoy en día han incorporado tecnología de la información (TI) basada en las funciones del sistema deseadas en el sistema general. TO es hardware y software que detecta o provoca un cambio a través del monitoreo directo y/o control de dispositivos físicos, procesos y eventos en la empresa. TI es la tecnología que involucra el desarrollo, mantenimiento y uso de sistemas informáticos, software y redes para el procesamiento y distribución de datos. Claramente, la diferencia clave es que TO se centra en el monitoreo y control del proceso físico. El foco de TO en apoyar un cierto proceso físico introduce diferencias substanciales en cómo los sistemas TO contrastado con sistemas de TI funcionan y se manejan, junto con las tecnologías usadas para apoyarlos.

La identificación de las diferencias clave entre TI y TO es de vital importancia para comprender los desafíos en la obtención de un ICS, especialmente desde que los métodos de seguridad diseñados originalmente para tecnología de TI se están aplicando ahora a ICSs. TO a menudo tiene limitaciones administrativas, operacionales y tecnológicas adicionales que proporcionan un entorno de seguridad más desafiante. La idea de seguridad para TO no es la misma, ya que la seguridad en TO se centra casi exclusivamente en la disponibilidad y seguridad.

Los ICSs tenían poca semejanza con los sistemas de TI en que ICSs eran sistemas aislados que ejecutaban protocolos de control propietario usando hardware y software especializados. En la actualidad los dispositivos de protocolo de Internet (IP) de bajo costo están ampliamente disponibles y ahora reemplazan las soluciones propietarias, lo que aumenta la posibilidad de vulnerabilidades e incidentes de seguridad cibernética. Como los ICSs están adoptando soluciones de TI para promover la conectividad corporativa y las capacidades de acceso remoto, y están siendo diseñadas e implementadas usando computadoras, sistemas

operativos (SO) y protocolos de red comunes, están comenzando a asemejarse a sistemas de TI. Esta integración soporta nuevas capacidades de TI, pero proporciona significativamente menos aislamiento del mundo exterior para los ICSs que los sistemas predecesores, creando una mayor necesidad de asegurar estos sistemas. Si bien las soluciones de seguridad han sido diseñadas para hacer frente a estos problemas de seguridad en los sistemas de TI típicos, se deben tomar precauciones especiales al introducir estas mismas soluciones a los entornos ICSs. En algunos casos, se necesitan nuevas soluciones de seguridad que se adapten al entorno ICS.

ICSs tiene muchas características que difieren de los sistemas tradicionales de procesamiento de información basados en Internet, incluyendo diferentes riesgos y prioridades. Algunos de ellos incluyen un riesgo significativo para la salud y la seguridad de vidas humanas, graves daños al medio ambiente, y asuntos financieros como pérdidas de producción, impacto negativo en la economía de una nación, y compromiso de información propietaria. Los ICSs tienen diferentes requisitos de rendimiento y fiabilidad y utilizan sistemas operativos y aplicaciones que pueden considerarse no convencionales para el personal de ti típico. Además, los objetivos de seguridad y eficiencia a veces pueden entrar en conflicto con la seguridad en el diseño y funcionamiento de los sistemas de control (por ejemplo, requerir autenticación de contraseña y la autorización no debe obstaculizar las acciones de emergencia para ICSs.) A continuación se enumeran algunas consideraciones especiales al considerar la seguridad de ICSs:

Requisitos de rendimiento. Los ICSs son generalmente tiempo-crítico; los retardos no son aceptables en la entrega de la información, y el alto rendimiento no es tan esencial. En cambio, los sistemas de TI típicamente requieren un alto rendimiento, pero pueden resistir niveles substanciales de retardo y jitter. Los ICSs deben mostrar respuestas deterministas.

Requisitos de disponibilidad. Muchos procesos de ICS son de naturaleza continua. Las interrupciones inesperadas de sistemas que controlan los procesos industriales no son aceptables. Las interrupciones a menudo deben planearse y programarse días/semanas de antemano. Es esencial realizar exhaustivas pruebas previas a la implantación para garantizar una alta disponibilidad para los ICSs. Además de interrupciones inesperadas, muchos sistemas de control no pueden

ser fácilmente detenidos y arrancados sin afectar la producción. En algunos casos, los productos que se están produciendo o el equipo que se está utilizando es más importante que la información que se está retransmitiendo. Por lo tanto, el uso de estrategias de TI típicas, como el reinicio de un componente, generalmente no es aceptable debido al impacto en los requerimientos de alta disponibilidad, confiabilidad y mantenibilidad del ICS.

4.1 Amenazas

En el área de informática, existen varios riesgos tales como: ataque de virus, códigos maliciosos, gusanos, caballos de troya y hackers; no obstante, con la adopción de Internet como instrumento de comunicación y colaboración, los riesgos han evolucionado y, ahora, las empresas deben enfrentar ataques de negación de servicio y amenazas combinadas; es decir, la integración de herramientas automáticas de "hackeo", accesos no autorizados a los sistemas y capacidad de identificar y explotar las vulnerabilidades de los sistemas operativos o aplicaciones para dañar los recursos informáticos.

A continuación, listo las amenazas que comúnmente afectan los sistemas de control industrial.

- **Ataques dirigidos**
- **Incidentes accidentales**
- **Accesos y controles no autorizados**
- **Código malicioso o no autorizado instalado en las máquinas (gusanos, virus, troyanos, spam, phising, bots, etc.).**
- **Espionaje**
  Es la acción de recopilar información de forma legal (publicidad, promociones, muestras de producto), o ilegal (intrusión, vigilancia. robo) acerca de los competidores o posibles clientes, de manera que se obtenga una posición de privilegio a la hora de ofrecer servicios o productos.
- **Sabotaje**
  Originado principalmente, por el deseo de obtener ganancias o ventajas competitivas de tipo personal, político o económico, mediante la destrucción de los medios del competidor.
  Aparece un nuevo cuño en las categorías del sabotaje, el Hactivismo, o el sabotaje llevado a cabo por piratas informáticos (crackers), con la finalidad

de destruir o apropiarse de Información corporativa vital (IT, informaiion Technoiogy) en nombre de algún tipo de Causa.

- **Vandalismo**
  Básicamente es lo mismo que el sabotaje, pero con la única finalidad de destruir información sin ningún tipo de provecho.
- **Intrusión (Crackers)**
  Los crackers, o hackers malos, son aquellos usuarios de ordenador que se introducen, sin permiso, en sistemas informáticos con la finalidad de demostrar que si pueden hacerlo. Por muchas que sean las barreras de seguridad que se implementen, serán capaces de rebasarlas.
  Los buenos, simplemente lo hacen corno un reto personal, limitándose a curiosear o dejar una firma. El lado oscuro es el preocupante.
- **Robo (electrónico)**
  Los datos tienen valor Para un competidor, por ejemplo, la cartera de clientes de la competencia marcaria una ventaja estratégica a la hora de planificar las ventas.
  En el caso de sistemas de control. Hay toda una serie de datos que sería peligroso que estuvieran al alcance de terceros (contraseñas, datos de acceso y configuración, especificaciones técnicas de equipos, etc.). En muchos casos, diseños de características especiales pueden marcar una ventaja competitiva (el know how), y la posibilidad de que alguien de dentro de la empresa pueda facilitar datos a cambio de dinero es tan elevada como la confidencialidad de éstos.
- **Troyanos**
  Ciertas rutinas de programa pueden permanecer ocultas a los usuarios y provocar fallos de funcionamiento o permitir la extracción de datos sin permiso. Por ejemplo, sería posible extraer datos sobre la formulación de fármacos que estuvieran almacenados en una base de datos del laboratorio.
- **Bombas de tiempo**
  Ciertas condiciones pueden activar programas que realicen determinadas acciones de forma automática (y no prevista, por supuesto), o que impidan realizarlas. Por ejemplo, activación de secuencias no permitidas, que puedan alterar el funcionamiento normal de los controles y provocar daños en el equipamiento, o que bloqueen funciones de usuario.

- **Puertas traseras**
  Se denomina así a fallos de seguridad intencionados y no documentados, que pueden permitir el acceso a datos confidenciales sin la autorización necesaria.
- **DOS (Denial of Service)**
  El ataque de negación de servicio se basa en saturar los recursos de una red informática con la finalidad de que los usuarios legítimos de la misma no puedan utilizar sus recursos.
  Su modus operandi se basa en el envío masivo de solicitudes a un servidor determinado, que terminan por agotar Sus recursos de servicio, haciéndolo inutilizable. Cualquier ordenador conectado en red y que haga uso de servicios TCP, es susceptible de un ataque DOS.
  Una forma más elaborada es la que se consigue cuando un pirata informático consigue instalar programas de llamada a en múltiples equipos conectados a Internet. Coordinados desde el equipo del pirata, lanzarán ataques DOS sobre otras máquinas. Esta variante es más elaborada, pues los ataques provienen de múltiples equipos, ninguno del pirata, haciendo muy difícil Su localización. Esta variante se denomina DDoS (Distributed DOS).
- **La falta de supervisión.**
  Sin supervisión de la red activa, es imposible detectar actividades sospechosas, identificar las amenazas potenciales, y reaccionar rápidamente a los ataques cibernéticos.
- **Cambios lentos.**
  A medida que los sistemas SCADA se vuelven más avanzados, también se vuelven más vulnerables a nuevos ataques. El mantenimiento de las actualizaciones de firmware y software puede ser un inconveniente (sin los sistemas adecuados en su lugar), pero son necesarias para una protección máxima.
- **La falta de conocimiento acerca de los dispositivos.**
  Dispositivos de conexión a un sistema SCADA permite el seguimiento y la actualización remota, pero no todos los dispositivos tienen las mismas capacidades de presentación de informes. Como la mayoría de los sistemas SCADA se han desarrollado gradualmente con el tiempo, no es raro ver que la tecnología es de 5 años de edad se combina con la tecnología que tiene

20 años. Esto significa que el conocimiento acerca de los dispositivos conectados a la red es a menudo incompleto.

- **No entender el tráfico.**
  Los gerentes necesitan saber qué tipo de tráfico que está pasando a través de sus redes. Sólo entonces pueden tomar decisiones informadas sobre cómo responder a las amenazas potenciales. Con el análisis avanzado de datos, los gerentes pueden obtener una gran visión de los datos obtenidos de la vigilancia del tráfico, y traducir eso en información procesable. Por ejemplo, un sistema de infiltrado podría comprobar con un servidor exterior una vez cada 30, 45, o 180 días.
- **Agujeros de Autenticación.**
  Las soluciones de autenticación están diseñadas para evitar que intrusos accedan al sistema ICS. Sin embargo, esto puede ser fácilmente vulnerado debido a prácticas inseguras comunes, tales como contraseñas pobres, nombre de usuario compartido y autenticación débil. Además, ahora los proveedores dan soporte remoto a través de enlaces telefónicos o de conexiones a Internet. Los módems rara vez están sujetos a las comprobaciones de seguridad. Un ataque a un sistema no crítico, como es la red de un proveedor, puede suponer de puerta de entrada de virus o ser usado para realizar ataques indirectos.
- El software comercial y el hardware de propósito general se está usando para sustituir el propietario de los sistemas ICSs. Este tipo de software y hardware a menudo no se adapta a la singularidad, complejidad, los requerimientos de tiempo real y seguridad del entorno SCADA. Los sistemas SCADA se vuelven vulnerables a ataques comunes y a malware ampliamente disponible desarrollado para otras plataformas. Aumenta su vulnerabilidad y el rango de posibles atacantes. En Internet es posible encontrar demostraciones de ataques sobre sistemas SCADA comerciales

4.2 Vulnerabilidades

Ya sean ICSs o TIs, las definiciones de disponibilidad, integridad y confidencialidad siguen siendo las mismas:

- Disponibilidad
  La disponibilidad es afectada cuando no se puede acceder a los datos en el momento que sea necesario. Los impactos sobre la disponibilidad pueden

resultar en pérdida o destrucción accidental o deliberada, o retraso en la entrega.

- Integridad
  La integridad se ve afectada cuando los datos cambian sin autorización. Los impactos de integridad pueden resultar en corrupción accidental o deliberada (parcial o total) de los datos, el cambio de los datos.
  La corrupción o el cambio puede ocurrir a través de la eliminación / eliminación parcial o selectiva de partes de un conjunto de datos.
- Confidencialidad
  La confidencialidad se ve afectada cuando los datos se dan a conocer sin autorización. Los impactos de confidencialidad pueden resultar en divulgación no autorizada o inoportuna. La divulgación puede darse a entidades no autorizadas, e incluso al público en general.

En el mundo del ICS, la trinidad de la CIA es menos utilizada, ya que no refleja el orden correcto de énfasis. En el ICS, la disponibilidad requiere la mayor seguridad, seguida muy de cerca por la integridad (especialmente si los problemas de integridad están asociados con la manipulación de vista de las amenazas. Haciendo caso omiso de cualquier aspecto de la tríada de la CIA puede dar lugar a fallos de seguridad desastrosas para ICS. ICS pueden poseer requerimientos y sensibilidades al nivel de milisegundos, por lo que aumentan la degradación del rendimiento y los riesgos. Del mismo modo, en el nivel de disponibilidad, temas complementarios asociados a la integridad entran en juego como la cantidad de retardo y corrupción cuyas consecuencias se ven en la pérdida de la vista o de control, o la negación de vista o control.

Es una creencia común que el ICS y redes SCADA están separadas físicamente de las redes corporativas de TI. Esto podría ser físicamente exacto, en el sentido de que algunas empresas operan redes de área local de sus sistemas de control y sus redes corporativas de manera separada entre sí. En otros casos, las empresas utilizan las mismas redes LAN y WAN, pero encriptan sus ICS y el tráfico SCADA a través de una infraestructura compartida. Con más frecuencia, sin embargo, las redes requieren un cierto nivel de interconectividad con el fin de obtener la entrada operacional de los datos y / o de exportación a sistemas externos de 3 party. Los dispositivos de red SCADA tienen características específicas que pueden ser muy diferentes a los sistemas de TI regulares:

- A menudo se instalan en lugares que son difíciles de acceder físicamente (por ejemplo, en las torres, en una plataforma petrolífera, en maquinaria industrial) y son ambientalmente más afectados que los sistemas de TI regulares (por ejemplo, al aire libre, temperaturas extremas, vibraciones) o requieren voltajes de entrada especiales y opciones de montaje.
- A menudo utilizan sistemas operativos propietarios que no han sido sometidos a un endurecimiento de la seguridad.
- Su software no puede ser actualizado o parcheado con frecuencia, debido a las limitaciones de acceso, la preocupación por el tiempo de inactividad o la necesidad de volver a certificar.
- Ellos usan protocolos propietarios o especiales.

Estas diferencias en el entorno crean problemas como la falta de autenticación y cifrado y almacenamiento de contraseñas débiles que permitiría a los atacantes tener acceso a los sistemas. Mientras que la mayoría de redes SCADA / ISC tienen algún nivel de defensa del perímetro, incluyendo la segmentación de la red y tecnologías cortafuegos, los atacantes siempre están buscando formas alternativas de conseguir entrar - por ejemplo, a través de un puerto que se deja abierto, o por activación de algunas operaciones desde el interior del organización que abre un canal de comunicación con el exterior. Tácticas típicas incluyen:

- El uso de un puerto de acceso remoto utilizado por el proveedor para el mantenimiento
- Hackear un canal legítimo entre los sistemas de TI y sistemas de ICS / SCADA
- Convencer a un usuario interno para hacer clic en un enlace URL en un correo electrónico desde una estación de trabajo conectada tanto a la red SCADA / ICS como a Internet
- Infección de ordenadores portátiles y / o medios extraíbles que estén fuera de la red ICS / SCADA, después infectan los sistemas internos cuando están conectados a la red para la recogida de datos, actualizaciones de software de sensor / control.
- Haciendo uso de errores en la configuración de seguridad o de los dispositivos conectados.

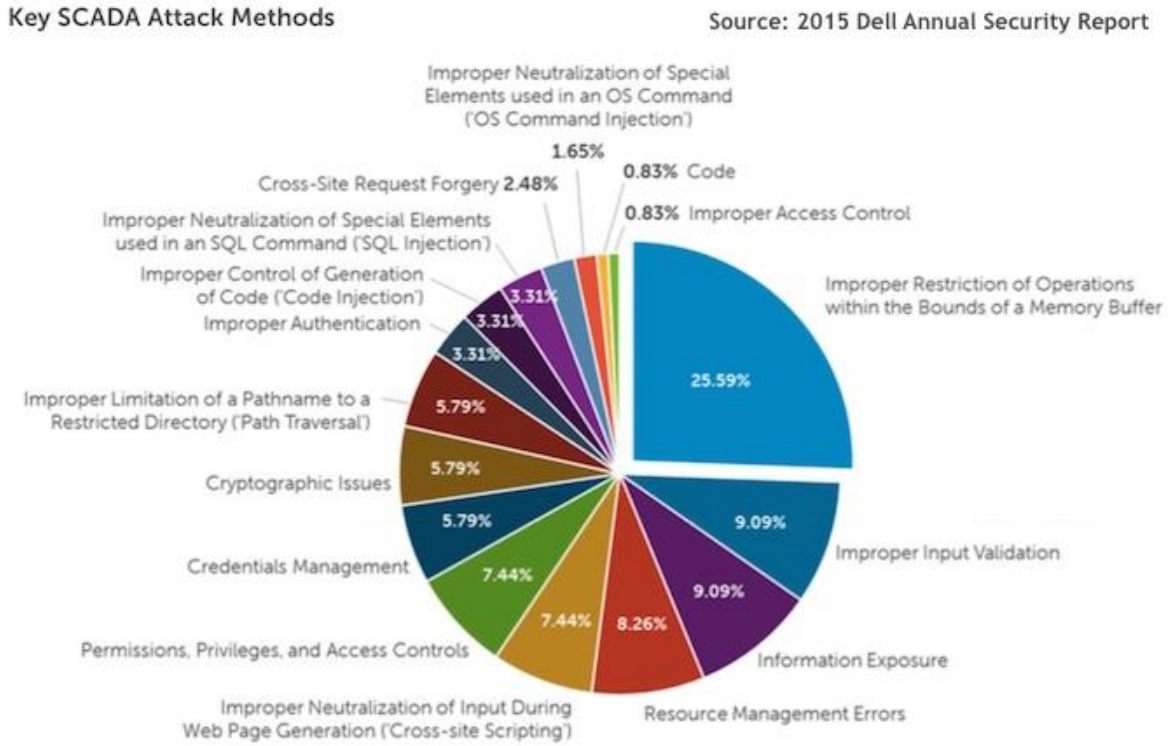
Una vez que un hacker se ha infiltrado en la red SCADA se hace posible enviar comandos maliciosos a los dispositivos con el fin de chocar o detener su actividad,

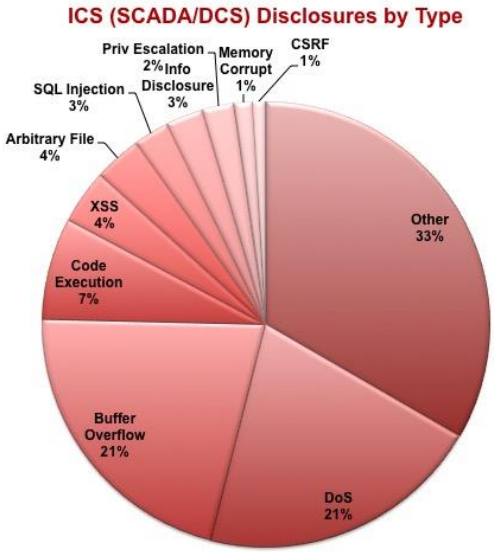
y para interferir con los procesos críticos específicos controlados por ellos, tales como la apertura y cierre de las válvulas.

Dentro de las vulnerabilidades que más se presentan tenemos:

- Vulnerabilidades de cross-site scripting (XSS).
- Vulnerabilidades de Directory traversal.
- Vulnerabilidades de SQL injection.
- Vulnerabilidades de escaladado de privilegios.
- Vulnerabilidades de buffer overflow.
- Vulnerabilidades de ejecución de código arbitrario (arbitrary code).
- Vulnerabilidades de Autenticación.
- Vulnerabilidades de Webtrojans
- Vulnerabilidades de Path Disclosure.
- Vulnerabilidades de DOS.
- Vulnerabilidades de spoof servers.

A continuación, muestro en dos figuras un resumen de vulnerabilidades que más afectan a las TICs y a los ICSs.





Fuente tomada de: https://www.scadahacker.com/images/ics_disclosures_by_type.jpg

Adicionalmente las vulnerabilidades que más se presentaron en ICSs en el 2015 y clasificadas por tipo según Kaspersky Lab se muestran en la figura siguiente.

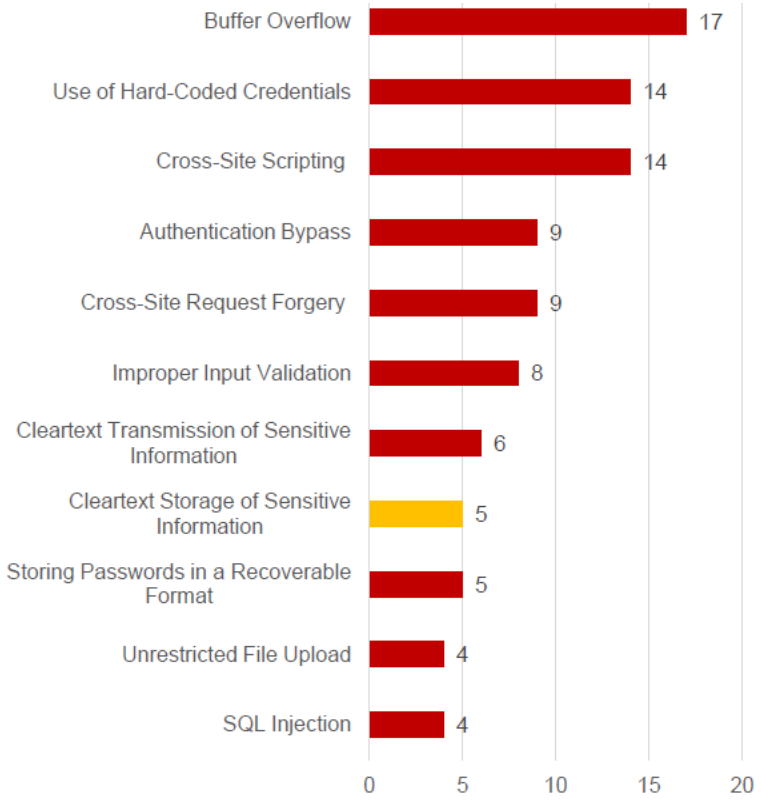


Imagen tomada de https://kasperskycontenthub.com/securelist/files/2016/07/KL_REPORT_ICS_Statistic_vulnerabilities.pdf

Buffer overflow es un error de programación, donde el software, al escribir datos en un búfer, sobrepasa el límite del búfer y sobrescribe las ubicaciones de memoria adyacentes. Escribir fuera de los límites de un bloque de memoria asignada puede dañar los datos, bloquear el programa o causar la ejecución de código malicioso. En total, se encontraron 17 vulnerabilidades de desbordamiento de búfer en los componentes de ICS en 2015, ocho de ellos tienen un alto nivel de riesgo. Estas fallas de seguridad fueron descubiertas en diferentes componentes, incluyendo sistemas SCADA, HMI, controladores, DCS y otros. Cuatro de estas vulnerabilidades tienen la puntuación CVSS más alta: 10, que corresponden al máximo impacto (acceso con privilegios elevados), lo que podría ser realizado por un atacante remoto no autenticado.

Hard-Coded Credentials, tal como una contraseña o clave criptográfica, crean normalmente un hueco de seguridad significativo que permite a un atacante omitir la autenticación configurada por el administrador de software. Esta vulnerabilidad se descubrió en 14 componentes diferentes del ICS (HMI, PLC, dispositivos de red y otros), y en la mayoría de los casos tiene un alto nivel de riesgo. Casi todas las vulnerabilidades identificadas de este tipo podrían ser explotadas por un atacante remoto. Sólo una vulnerabilidad (CVE-2015-0996) en Schneider Electric InduSoft Web Studio y la edición 2014 de InTouch Machine pueden ser explotadas sólo por usuarios locales.

Cross Site Scripting permite a los intrusos inyectar secuencias de comandos de cliente en páginas web vistas por los usuarios, que podrían utilizarse para robar datos de autenticación de usuarios (cookies), realizar ataques de ingeniería social, o difundir malware. Las vulnerabilidades de este tipo están presentes en 14 componentes ICS (la mayoría de ellos son sistemas SCADA).

Cross-Site Request Forgery existe cuando un servidor web está diseñado para recibir una solicitud de un cliente sin ningún mecanismo para verificar que se envió intencionalmente. Entonces, podría ser posible que un atacante engañe a un cliente para que haga una petición involuntaria al servidor Web, el cual será tratado como una petición auténtica. Esto se puede hacer a través de una URL, la carga de imágenes, XMLHttpRequest, etc. y puede resultar en la exposición de los datos o la ejecución de código no intencionado. Cuatro de las nueve vulnerabilidades descubiertas están presentes en los sistemas SCADA.

Los productos que contienen la vulnerabilidad de **validación de entrada incorrecta** no validan ni validan incorrectamente las entradas que pueden afectar al flujo de control o al flujo de datos de un programa. La mayoría de estos defectos están relacionados con la ejecución de código arbitrario. Ocho vulnerabilidades están presentes en el HMI, el sistema SCADA, RTOs y el servidor OPC. Por ejemplo, la vulnerabilidad CVE-2015-0980 (de alto nivel) en el motor SCADA BACnet servidor OPC antes de 2.1.371.24 permite a un atacante ejecutar código arbitrario.

Las vulnerabilidades de **Transmisión de texto no codificada con información sensible** se encontraron en seis diferentes componentes del ICS. Estas vulnerabilidades permiten que un actor no autorizado detecte y/o capture datos sensibles o de seguridad críticos en un canal de comunicación porque el software transmite datos en texto sin codificar. Por ejemplo, debido a que no hay soporte SSL en la estación base de Gateway telemetría de Adcon A840, toda la comunicación está desencriptada, lo que hace que sea fácilmente legible a través de la red (CVE-2015-7932, nivel medio).

El **almacenamiento de contraseñas en un formato recuperable** los hace vulnerable a ataques de reutilización de contraseñas por usuarios malintencionados. De hecho, debe tenerse en cuenta que las contraseñas cifradas recuperables no proporcionan ningún beneficio significativo sobre las contraseñas de texto sin formato, ya que están sujetas no sólo a la reutilización por parte de los atacantes malintencionados, sino también por los intrusos malintencionados. Si un administrador del sistema puede recuperar una contraseña directamente o utilizar una búsqueda de fuerza bruta en la información disponible, el administrador puede utilizar la contraseña en otras cuentas. Las HMIs son las más afectadas por esta vulnerabilidad.

Las vulnerabilidades de **carga de archivos sin restricción** en el software permiten a un atacante cargar o transferir archivos de tipos peligrosos que se pueden procesar automáticamente dentro del ambiente de producción. Estas vulnerabilidades se descubrieron en cuatro componentes ICS, tres de ellos son sistemas SCADA. Por ejemplo, a través de un servlet, es posible cargar código Java arbitrario en la versión 5.21.02 de la plataforma AggreGate y en versiones anteriores, y permitir que las propiedades de las aplicaciones se importen a través de archivos cargados

que podrían permitir la ejecución arbitraria de código y comando (CVE-2015-7912, de alto nivel).

La forma básica de **SQL Injection** describe la inserción directa de datos controlados por el atacante en variables que se utilizan para construir comandos SQL. Como resultado, un atacante puede manipular la consulta original al terminar permanentemente la cadena, anexando nuevos comandos, etc. Las vulnerabilidades de este tipo están presentes en cuatro componentes ICS (tres de ellos son sistemas SCADA).

Si la información se almacena en texto plano (**vulnerabilidad de almacenamiento en texto plano de información sensible**), los atacantes podrían leerlo potencialmente. Incluso si la información está codificada de una manera que no es legible por los seres humanos, ciertas técnicas podrían determinar qué codificación se está utilizando y, a continuación, descodificar la información. Este tipo de vulnerabilidad de nivel medio está presente en diferentes componentes del ICS: HMIS, sistemas SCADA, servidores web y bombas.

Las vulnerabilidades de **autenticación por bypass** se encontraron en ocho tipos diferentes de componentes de ICS, incluyendo HMI, un dispositivo de red, RTU y otros. Un atacante que explote estas vulnerabilidades puede ser capaz de capturar o modificar información privilegiada, inyectar código o eludir el control de acceso. Dependiendo de un sistema vulnerable, tales defectos pueden tener una naturaleza diferente,

En el estudio estadístico realizado por Kaspersky Lab también se identifica a los componentes de un ICS que son los más afectados por los ataques no autorizados. A continuación son descritos en la gráfica.

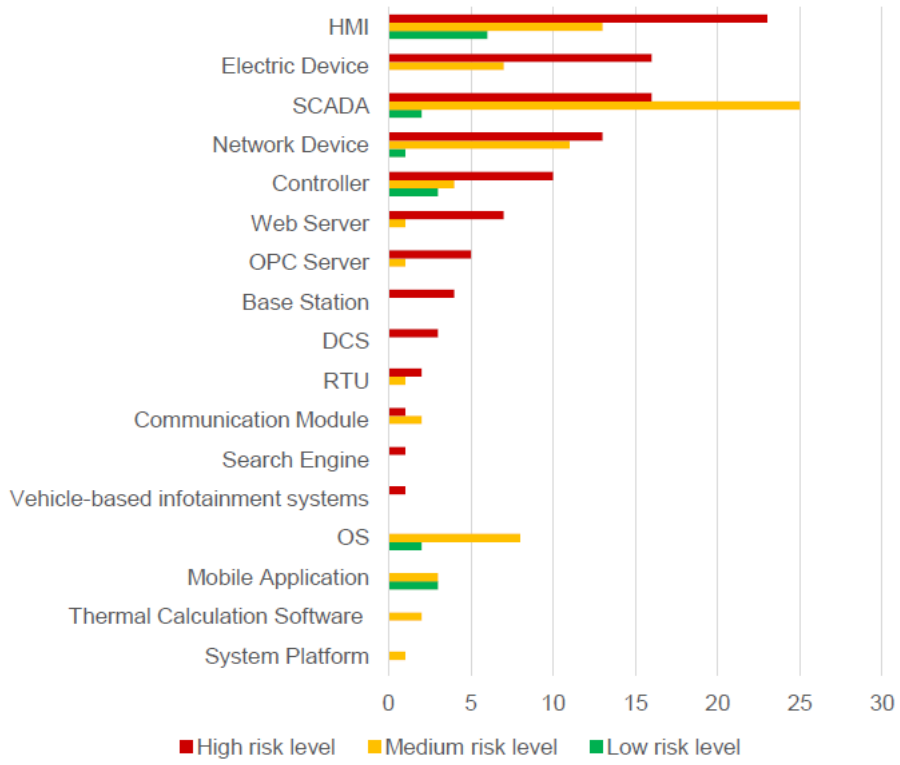


Imagen tomada de https://kasperskycontenthub.com/securelist/files/2016/07/KL_REPORT_ICS_Statistic_vulnerabilities.pdf

Se puede observar que el componente sufre la mayor cantidad de ataques es la HMI debido a su baja capacidad de almacenamiento y procesamiento. Los ataques que más se observaron fueron los de buffer overflow, hard-coded credentials y el de almacenamiento de contraseñas en un formato recuperable. Uno de los ejemplos es la vulnerabilidad de incorrecto control de acceso (CVE-2015-4051, alto nivel de riesgo) en Beckhoff IPC Diagnostics antes 1,8 (HMI) permitiendo que un atacante no autenticado realice una variedad de acciones en el sistema enviando un paquete especialmente diseñado. Estas acciones incluyen reiniciar el dispositivo o inyectar un nuevo usuario que tenga derechos de acceso de administrador tanto en las ventanas incrustadas subyacentes como en un servidor Web.

Para los dispositivos eléctricos, el problema más extendido es el uso de credenciales, hard-coded credentials (tres vulnerabilidades). Por ejemplo, existen siete vulnerabilidades en los productos de sistemas de infusión HOSPIRA Plum A+ y Symbiq, bombas intravenosas que suministran medicamentos a los pacientes: errores de administración de claves (CVE-2015-3957), almacenamiento en texto plano de información sensible (CVE-2015-3952), buffer overflow (CVE-2015-3955), verificación insuficiente de la autenticidad de los datos (CVE-2015-3956), consumo

incontrolado de recursos (CVE-2015-3958), autorización incorrecta (CVE-2015-3954) y uso de contraseña hard-coded (CVE-2015-3953). Cinco de estas vulnerabilidades tienen un alto nivel de riesgo. Todos menos una de estas vulnerabilidades podrían explotarse remotamente. Los usuarios locales sólo pueden utilizar la vulnerabilidad de errores de administración de claves.

Para los sistemas SCADA, los problemas más extendidos son las de cross site scriptig (siete vulnerabilidades), las de buffer overflow (cinco vulnerabilidades), la falsificación de solicitudes entre sitios (cuatro vulnerabilidades), la carga de archivos sin restricción (tres vulnerabilidades) y la inyección de SQL (tres vulnerabilidades). Por ejemplo, una vulnerabilidad de inyección de SQL local (CVE-2015-1008) en el administrador de dispositivos de Emerson AMS antes de la versión 13 permite a los usuarios autenticados obtener privilegios administrativos mediante una entrada malformada.

En el anexo se definen las tablas de vulnerabilidades según el contexto dentro del ICS.

4.3 Fallos de seguridad comunes en ICSs

A continuación se enumeran los fallos más comunes en ICSs.

1. Si un atacante remoto vulnera a algún servidor o equipo dentro de la zona DMZ y escanea los puertos del firewall, que está entre la red corporativa DMZ y la LAN corporativa, y encuentra algún puerto abierto, podría infectar a algún equipos de la red corporativa, violar la seguridad del firewall/router e intentar acceder a los equipos del centro de control y por ende modificar la acción en la red de campo.

2. Si a los usuarios que usan los equipos se les realiza ingeniería social y no han sido formados en la empresa respecto a este tipo de ataques, se podrían encontrar casos en los que se le dé información de acceso o autenticación al atacante y, por ende, acceso a los equipos de la red corporativa segura.

3. Un punto crítico es el uso de un solo router/firewall, entre el bloque red corporativa y el bloque centro de control. Como es sabido, debido a lo que se monitorea y controla, en un sistema SCADA es fundamental la disponibilidad, si se pierde la comunicación entre los bloques antes mencionados, al

inhabilitar el firewall/router, se denegará el servicio y, por ende, el sistema no operará o lo hará de forma limitada.

4. Como los equipos del centro de control son imprescindibles en el sistema, éstos deberían tener una protección mayor, lo que implica que sólo un firewall/router, entre el centro de control y la red corporativa, es insuficiente si un atacante burla la seguridad del primer firewall. Además, falta una zona DMZ con equipos bastión del centro de control que permitan la comunicación de la red corporativa con el centro de control, sin estos no habría la posibilidad de implementar servicios de filtrado de paquetes y de pasarelas a nivel de aplicación (permiten la autenticación de los usuarios que realizan peticiones de conexión y el análisis de conexiones a nivel de aplicación).

5. Por otro lado, el protocolo base de muchos de los sistemas SCADA que hoy están en producción es Modbus, cuyo diseño está pensado para operar sobre líneas de transmisión en serie. El modo bajo el cual se da la comunicación de estas redes es un primitivo esquema “petición-respuesta”, que dificulta la identificación de un eventual ataque pues los sistemas no podrían distinguir entre peticiones legítimas o peticiones provenientes de sistemas infectados.

6. El protocolo Modbus está montado sobre TCP y ese protocolo no realiza autenticación ni tiene funcionalidades de confidencialidad de manera nativa, de forma tal que una vez que el hacker logra entrar a la red puede tomar el control de una sesión.

7. En el centro de control se mueven datos de diferente índole como los de la red corporativa (administrativos), los enviados por los equipos de campo (RTU, módems, etc.) y los propios, al no existir segmentación de estas tres fuentes, un atacante podría usar el único segmento de red para infectar a los routers que se comunican con los equipos de la red de campo.

8. Existe redundancia en los servidores de históricos y de ICSs, pero están ubicados en el mismo segmento de red, falta una redundancia de estos servidores ubicados en otro segmento de red.

9. No se indica si existen equipos que realicen auditoría, que permitan identificar y actuar ante la existencia de vulnerabilidades.

4.4 Propuesta de mejoras en la securización de los ICSs

1. Para securizar el acceso a la red corporativa, se podría implementar un esquema donde la red DMZ corporativa transmita y reciba datos de internet mediante un router que use filtrado y una pasarela a nivel de aplicación, así como un firewall que permite implementar aquellas reglas de la política de seguridad relativas al control de acceso seguro a nivel de red.
2. Tener un plan de actualización periódica de contraseñas y uso de contraseñas robustas.
3. Capacitar a los usuarios de la red corporativa respecto a los riesgos de seguridad que pueden afectar el sistema, tales como Phishing, Vishing, Baiting, entre otros. la Ingeniería social es una técnica que aprovecha los errores humanos para comprometer las seguridad de los sistemas, pero también podríamos decir que es un arte cuyas herramientas principales son el engaño y la confusión. Este fenómeno se magnifica cuando su accionar se centra en los sistemas informáticos empresariales, como el del contexto que se está securizando, en donde la información es valiosa y debería estar siempre al alcance de los entes autorizados para tratarla pero y al mismo tiempo, podría estar expuesta a agentes externos o internos que la desean obtener de manera fraudulenta. Por esta razón, la Ingeniería Social también se aplica a los sistemas computarizados a través de herramientas diseñas específicamente para ello, evidenciándose así su avance en la ciberdelincuencia

4. Se puede obtener alta disponibilidad en el canal de comunicación entre la red corporativa y el centro de control usando la redundancia de equipos y rutas. Se deben agregar routers redundantes y establecer enlaces duales hacia cada uno desde las capas inferiores, tener fuentes de alimentación redundantes, suministros de energía independientes, utilizar motores de enrutamiento/redirección redundantes.

5. La red perimetral del centro de control debe contener equipos que permitan realizar las auditorías, servir como pasarelas a nivel de aplicación y de filtrado de paquetes, equipos que presten servicios de antivirus, actualización de software y de parches.

6. Para evitar vulneraciones del Modbus se podrían encriptar de las comunicaciones, éste encriptado evitaría que al ser esnifado el canal se pueda analizar la información fácilmente.

7. Se podrían actualizar los equipos, por aquellos que soporten IPV6, tales como routers, firewalls, sensores y actuadores en general.

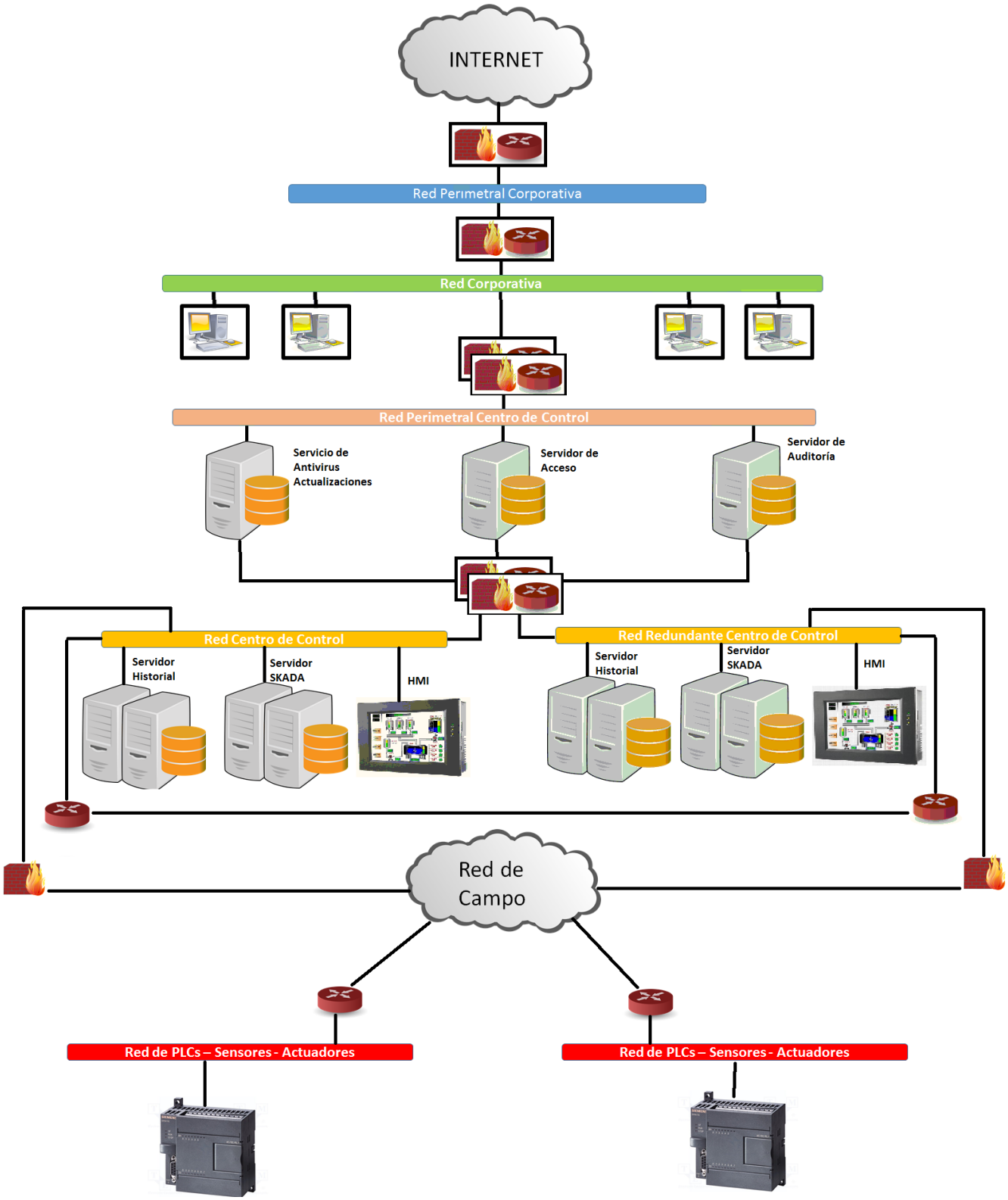
8. Una vez que se obtuvo acceso no autorizado, la segmentación de red o "zonificación" puede proporcionar un control eficaz de mitigar el siguiente paso de una intrusión en la red y para limitar aún más el movimiento a través de la red o propagación de una amenaza. Al segmentar correctamente la red, se está minimizando esencialmente el nivel de acceso a la información sensible para las aplicaciones, los servidores y las personas que no lo necesitan, al tiempo que permite el acceso de los que lo hacen. Mientras tanto se le está haciendo mucho más difícil a un ciber-atacante localizar y acceder a la información más sensible de la compañía eléctrica.

9. Se puede construir un centro de control redundante geográficamente. Este respaldo proporciona servicios de redundancia geográfica de modo que en el caso de una falla completa del centro de control, la información puede ser desviada a otros servidores y HMIs ubicados en otro lugar físico a varios kilómetros de distancia. Esto permite entregar tranquilidad a la empresa y los clientes en caso de que ocurra un desastre natural que afecte al lugar de alojamiento oficial, o un ataque humano que pretenda la DoS.

10. Se deben ubicar en la zona desmilitarizada del centro de control, equipos que permitan la auditoría de los datos de los canales de comunicación con la red corporativa y realizar:
    - Escaneo de vulnerabilidades.
    - Captura y análisis de protocolos.

- Pruebas de penetración.
- Escaneo de puertos.
- Ingeniería social
- Herramientas de gestión de dispositivos de red y gestión remota de servidores y computadoras.
- Reportes de vulnerabilidades en sitios de confianza.

4.5 Solución a modo de diagrama



5 CONCLUSUIONES

- El estudio de la ciberseguridad en ICSs me permitió la aplicación de muchos de los conocimientos adquiridos en las asignaturas cursadas en la maestría MISTIC, desde la regulación en TICs hasta la seguridad en sistemas operativos y redes. Me permitió conocer un contexto en donde la securización se ha desarrollado con menor velocidad que la de un sistema informático típico y se ve la necesidad de realizar estudios profundos para alcanzar niveles similares de seguridad. Los conceptos de seguridad en redes (seguridad en protocolos TCP/IP y en equipos activos de red, etc.), los de vulnerabilidades (Buffer overflow, XSS, DOS, SQL injection, ingeniería social, etc.), los de seguridad en sistemas operativos (seguridad pasiva y activa, configuración de servicios de servidores, etc.) y los de regulación, fueron usados en la solución de las diferentes fases que me permitieron entregar el estudio y alternativa de solución sobre la securización de sistemas ICSs.
- Debido a la importancia de los ICSs tanto para el sector público, respecto al control de infraestructura crítica como la de generación y transporte de gas, electricidad, agua y aguas residuales; y para el sector privado, industria química, manufacturera, de ensamblaje de automóviles, entre otras; atacantes de diversas índoles y motivaciones han puesto su atención en estos y se han dedicado a encontrar deficiencias en su securización para obtener beneficios individuales y colectivos. En ese orden de ideas los gobiernos y las empresas se han unido para contrarrestar a estos adversarios, y la ciberseguridad en ICSs, que históricamente se encontraba rezagada, ha tomado un rol cada vez más relevante.
- En una primera fase del proyecto se definieron los tipos de ICSs, las partes principales que lo conforman y la relación entre las OTs y las ITs. Con este estudio teórico se pudo evidenciar que existen diferentes tipos de amenazas y vulnerabilidades que se pueden presentar en los ICSs y que se derivan de él.
- En el estudio de los ICSs se encuentra que el rezago en su securización se presenta por una multiplicidad de factores, desde los concernientes a los humanos hasta los relacionados componentes presentes en las etapas finales tales como sensores y actuadores. Lo anterior nos debe llevar a la reflexión de la importancia en la capacitación especializada del personal de TI y TO en los temas de ciberseguridad para evitar o mitigar daños en los ICSs. Adicionalmente, en los

diferentes estudios sobre ciberseguridad se ha encontrado que el principal factor de riesgo en la infraestructura de las empresas es el error humano lo que debe llevarnos a pensar en la realización de campañas de capacitación al personal diferente al de las áreas de TI y TO.

- En muchos casos las industrias usaban ICSs con configuraciones, equipos y protocolos de comunicación propietarios, lo anterior llevaba a pensar a los encargados de las TIs y TOs que se encontraban blindados contra ataques y no tomaban medidas de seguridad. Si por algún motivo se perdía la confidencialidad de los ICSs con la posibilidad subsecuentes ataques.
- Dentro de las diferencias críticas entre los sistemas en tiempo real/SCADA frente a la protección y los riesgos asociados a los sistemas de TI empresariales se encuentra que para una empresa es más importante la pérdida de propiedad intelectual, que un atacante obtenga acceso a información financiera o estratégica, o simplemente la denegación de servicio en sistemas informáticos. Mientras que en los sistemas de control industrial ICSs es importante que no se pierdan datos provenientes de los equipos de campo y la respectiva pérdida de control de la planta. Mientras que la afectación por ataques a las TI de las empresas pueden impactar su viabilidad financiera, las posibles consecuencias de los ataques a los ICSs representan una amenaza para la seguridad y la vida humana en un caso extremo. Los sistemas industriales también son vulnerables a la pérdida de registros históricos críticos, pérdida de integridad de datos, pérdida de rendimiento, degradación progresiva y efectos aleatorios.
- En los ICSs se debe tener en cuenta que hay existen otros factores importantes en sus procesos y procedimientos operacionales, así como en las consecuencias de salud, seguridad y medio ambiente debido a un fallo de un sistema o componente.
- Como los sistemas de control industrial tales como SCADA, DCS, PLCs, y otras redes de control de procesos, usan cada vez más equipos que usan internet se exponen a ataques por explotación de vulnerabilidades inherentes a ella, tales como: troyanos, gusanos, puertas trasera, etc. La amenaza de mayor resonancia ha sido el gusano Stuxnet.
- ICSs fueron diseñados tradicionalmente alrededor de confiabilidad y de seguridad; la ciberseguridad no era un diseño y una consideración operacional. La falta de comprensión de la amenaza de ciberseguridad se puede encontrar en todos los niveles de organización. La mayoría de los departamentos de ICS

transmiten sus necesidades al nivel ejecutivo, en el cual hay una falta general de comprensión.

- Dentro de los sistemas ICSs se encontraron vulnerabilidades y amenazas que se detallan a continuación:
    - Falta de firewalls/router entre la red internet y la red DMZ corporativa.
    - Falta de capacitación en el personal de la empresa ante ataques de Ingeniería Social.
    - Falta de redundancia en los firewalls entre el centro de control y la red corporativa.
    - Falta de red DMZ del centro de control.
    - Falta de segmentación en la red del centro de control.
    - Equipos con tecnologías obsoletas (bus modbus) sin posibilidad de securización.
    - Falta de redundancia en los servidores del centro de control.
    - Falta de auditoria.

REFERENCIAS

"Cyber-security of SCADA and Other Industrial Control Systems", Volumen 63, Edward J. M. Colbert y Alexander Kott, Editorial Springer.

Documentos en la web

- https://www.dhs.gov/sites/default/files/publications/csd-nist-guidetosupervisoryanddataccquisition-scadaandindustrialcontrolsystemssecurity-2007.pdf
- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf
- https://ics-cert.us-cert.gov/sites/default/files/Monitors/ICS-CERT_Monitor_Sep-Oct2017_S508C.pdf
- https://kasperskycontenthub.com/securelist/files/2016/07/KL_REPORT_ICS_Statistic_vulnerabilities.pdf
- https://arxiv.org/ftp/arxiv/papers/1708/1708.07424.pdf
- http://www.uco.es/investiga/grupos/eatco/automatica/ihm/descargar/scada.pdf
- http://www.cse.psu.edu/~sem284/cse598e-f11/slides/cse598e-scada.pdf
- http://www.marcombo.com/Descargas/8426714188-SCADA/CAP%C3%8DTULO%20I.pdf
- ftp://ftp.ni.com/pub/branches/latam/nidays_2006/Diseno%20de%20Sistemas%20SCADA%20para%20Monitoreo%20de%20Procesos.pdf
- http://www.etitudela.com/celula/downloads/controldeprocesos.pdf
- http://bibdigital.epn.edu.ec/bitstream/15000/10020/2/PARTE%202.pdf
- http://energy.gov/sites/prod/files/Vulnerability%20Analysis%20of%20Energy%20Delivery%20Control%20Systems.pdf
- http://sas-origin.onstreammedia.com/origin/isaca/LatinCACS/cacs-lat/forSystemUse/papers/212.pdf
- http://redeweb.com/_txt/686/p60.pdf
- https://www.thalesgroup.com/sites/default/files/asset/document/thales-cyber-security-for-scada-systems.pdf
- http://repository.unad.edu.co/bitstream/10596/3629/1/1075210015.pdf
- https://nsrc.org/workshops/2011/walc/routing/raw-attachment/wiki/Agenda/Alta_Disponibilidad.pdf
- http://www.dis.uniroma1.it/~tenace/download/deliverable/Report_tenace.pdf
- http://sas-origin.onstreammedia.com/origin/isaca/LatinCACS/cacs-lat/forSystemUse/papers/212.pdf

- http://redeweb.com/_txt/686/p60.pdf
- http://web.usbmed.edu.co/usbmed/fing/v3n2/v3n2a2.pdf

Páginas web

- https://www.incibe.es/file/5ik7qnpsCJD6GNls9ZYKrA
- https://www.incibe.es/file/DqUev-29M3FtRjmJl-mD6A
- https://es.wikipedia.org/wiki/SCADA
- http://riull.ull.es/xmlui/bitstream/handle/915/657/Evaluacion%20de%20estandares%20HMI%20Aplicacion%20de%20la%20guia%20GEDIS%20a%20los%20Sistemas%20SCADA%20del%20NAP%20(Network%20Access%20Point)%20de%20Canarias..pdf?sequence=1
- https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/205-ccn-stic-480-seguridad-en-sistemas-scada/file.html
- https://seguinfo.wordpress.com/category/scada/
- http://www.controlandlogic.cl/Articulo_Espionaje.html
- http://www.elladodelmal.com/2010/05/shodan-y-sistemas-scada.html
- http://www.silicon.es/seguridad-informatica-en-entornos-industriales-4-85025
- https://archive.org/details/ScadaAulas
- http://www.ingenieriatci.es/productos/control-y-supervision/
- http://pirhua.udep.edu.pe/bitstream/handle/123456789/1739/ING_527.pdf?sequence=1
- http://www.scadaexposure.com/glossary
- https://web.nvd.nist.gov/view/vuln/search-results?query=scada&search_type=all&cves=on&startIndex=80
- https://web.nvd.nist.gov/view/vuln/search-results?query=ICS&search_type=all&cves=on
- http://www.eetimes.com/document.asp?doc_id=1327785
- http://tics166.blogspot.com.co/2011/10/seguridad-y-vulnerabilidad-informatica.html
- https://books.google.com.co/books?id=I6--ib7Uq4QC&pg=PA221&lpg=PA221&dq=amenazas+Scada&source=bl&ots=B9zWNtfgBK&sig=S6PMCaS0wlPV2iQdmr8-4E4b3Fc&hl=es-419&sa=X&ved=0ahUKEwiV2fn-vKrMAhWCox4KHfCQCQ8Q6AEIJzAB#v=onepage&q=amenazas%20Scada&f=false
- https://scadahacker.com/resources/msf-scada.html
- http://www.magazcitum.com.mx/?p=1605#.Vx6SuDDhDIU

- https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/desmontando_modbus
- https://securelist.lat/blog/politicas-de-seguridad/67488/fallas-de-seguridad-en-redes-corporativas-vulnerabilidades-de-redes/
- http://searchdatacenter.techtarget.com/es/cronica/Como-mejorar-la-seguridad-con-una-adecuada-segmentacion-de-redes
- https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/desmontando_modbus
- https://www.inc.cl/blog/hosting/que-es-la-redundancia-y-cual-es-su-importancia
- https://pixabay.com/es/cortafuegos-red-de-seguridad-29503/
- http://www.tiposde.org/informatica/131-tipos-de-servidores/

6 ANEXOS

Tablas de Fuentes de Ataques y de Vulnerabilidades en Sistemas de Control Industrial según el NIST.

Tabla 1: Fuentes de Ataques

Tipo de Fuente de Amenaza	Descripción	Características

• Adversarios
  ○ Individuos
  ▪ Internos
  ▪ Externos
  ▪ Internos confiables
  ▪ Internos con privilegios
  ○ Grupos
  ▪ A medida
  ▪ Establecidos
  ○ Organizaciones
  ▪ Competidor
  ▪ Proveedor
  ▪ Socio
  ▪ Cliente
  ○ Nación-Estado
	Individuos, grupos, organizaciones o Estados que buscan explotar la dependencia de la organización de los recursos cibernéticos (por ejemplo, información en forma electrónica, tecnologías de información y comunicaciones, y el manejo de la información capacidades proporcionadas por esas tecnologías)	Capacidad, intención, segmentación

• Accidental
  ○ Usuario
  ○ Usuario con Privilegio o Administrador
	Acciones erróneas tomadas por las personas en el curso de la ejecución de sus responsabilidades diarias.	Rango de efectos

ESTRUCTURAL
• Tecnologías de la Información TIs
  ○ Equipos
  ○ Almacenamiento
  ○ Procesamiento
  ○ Comunicaciones
  ○ Visualización
  ○ Sensores
  ○ Controladores
	Fallas de equipo, controles ambientales o software debido al envejecimiento, agotamiento de recursos u otras circunstancias que excedan los parámetros de operación esperados.	Rango de efectos

○ Control ambiental ○ Controles de temperatura/humedad ○ Fuente de alimentación ○ Software ○ Sistema operativo ○ Redes ○ Aplicación de propósito general ○ Aplicación de propósito específico		
AMBIENTALES • Desastres naturales o hechos por el hombre • Incendio • Inundación/Tsunami • Vendaval/Tornado • Huracán • Terremoto • Bombardeo • Desbordamiento • Acontecimiento natural inusual (Por ej., manchas solares) • Falla en la infraestructura o apagón • Telecomunicaciones • Energía eléctrica	Desastres naturales y fallas de infraestructuras críticas de las que depende la organización, pero que están fuera del control de la organización. Nota: los desastres naturales y los causados por el hombre también pueden ser caracterizados en términos de su severidad y/o duración. Sin embargo, debido a que la fuente de amenazas y el evento de amenaza se identifican fuertemente, la severidad y la duración pueden incluirse en la descripción del evento de amenaza (por ejemplo, el huracán de la categoría 5 causa daños extensos a las instalaciones que albergan sistemas de misión crítica, haciendo que esos sistemas no estén disponibles	Rango de efectos

	durante tres semanas).	

Tabla 2: Vulnerabilidades de Arquitectura y Diseño y condiciones predispuestas

Vulnerabilidad	Descripción
Incorporación inadecuada de la seguridad a la arquitectura y al diseño.	La incorporación de la seguridad en la arquitectura ICS, el diseño debe comenzar con el presupuesto, y la programación del ICS. La arquitectura de seguridad forma parte de la arquitectura empresarial. Las arquitecturas deben abordar la identificación y autorización de los usuarios, el mecanismo de control de accesos, las topologías de red y los mecanismos de configuración e integridad del sistema.
Arquitectura insegura permite evolucionar	El entorno de infraestructura de red dentro del ICS ha sido desarrollado y modificado a menudo basándose en requerimientos empresariales y operacionales, con poca consideración por los posibles impactos de seguridad de los cambios. Con el tiempo, las brechas de seguridad pueden haber sido introducidas inadvertidamente en determinadas partes de la infraestructura. Si no se remedia, estas brechas pueden representar puertas traseras en el ICS.
No hay seguridad perimetral definida	Si el ICS no tiene una seguridad perimetral claramente definido, entonces no es posible asegurarse de que los controles de seguridad necesarios se desplieguen y configuran correctamente. Esto puede conducir a un acceso no autorizado a los sistemas y a los datos, así como a otros problemas.
Las redes de control utilizadas para el	El control y el no control de tráfico tienen

tráfico no controlo	diferentes requisitos, como el determinismo y la fiabilidad, por lo que tener ambos tipos de tráfico en una sola red dificulta su configuración para que cumpla con los requisitos de control de tráfico. Por ejemplo, el tráfico sin control podría consumir inadvertidamente recursos que controlan las necesidades de tráfico, causando interrupciones en las funciones de ICS.
Los servicios de control de red que no se encuentran dentro de la red controlada	Donde los servicios de TI, el sistema de nombres de dominio (DNS) y el protocolo de configuración dinámica de host (DHCP) son utilizados por las redes de control, a menudo se implementan en la red de TI, causando que la red ICS se vuelva dependiente de la red de TI que puede no tener los requisitos de confiabilidad y disponibilidad necesarios para el ICS.
Recopilación inadecuada del historial de datos del evento	El análisis forense depende de la recopilación y retención de suficientes datos. Sin una recopilación de datos adecuada y precisa, podría ser imposible determinar qué causó un incidente de seguridad. Los incidentes podrían pasar desapercibidos, lo que provocaría daños y/o interrupciones adicionales. También se necesita una supervisión de seguridad continua para identificar problemas con los controles de seguridad, como configuraciones erróneas y fallas.

Tabla 3: Vulnerabilidades de configuración y mantenimiento y condiciones predispuestas

Vulnerabilidad	**Descripción**
Hardware, firmware y software fuera del	La organización no sabe lo que tiene, qué

dominio de la administración de configuración.	versiones tiene, dónde están, o cuál es su estado de revisión, lo que resulta en una postura de defensa inconsistente e ineficaz. Se debe implementar un proceso para controlar las modificaciones del hardware, firmware, software y documentación para garantizar que un ICS esté protegido contra modificaciones inadecuadas o inapropiadas, antes, durante y después de la implementación del sistema. La falta de procedimientos de administración del cambio de configuración puede conducir a descuidos, exposiciones y riesgos de seguridad. Para asegurar correctamente un ICS, debe haber una lista exacta de los activos en el sistema y sus configuraciones actuales. Estos procedimientos son fundamentales para ejecutar los planes de continuidad del negocio y recuperación ante desastres.
Los parches de software del SO y del proveedor no se pueden desarrollar hasta que después de que se encuentren vulnerabilidades de seguridad	Debido a que el acoplamiento entre el software ICS y el ICS subyacente es ajustado, los cambios deben someterse a costosos y largos pruebas de regresión. El tiempo transcurrido para esas pruebas y la posterior distribución del software actualizado proporciona una larga ventana de vulnerabilidad
No se aplican los parches a los OSs y las aplicaciones de seguridad o el proveedor declina a parchear la vulnerabilidad	Fuera de la fecha los OSs y las aplicaciones pueden contener vulnerabilidades recientemente descubiertas que podrían explotarse. Se deben desarrollar procedimientos documentados para saber cómo se mantendrán los parches de seguridad. Es posible que la compatibilidad con parches de seguridad no esté disponible para ICS que utilicen

	sistemas operativos obsoletos, por lo que los procedimientos deben incluir planes de contingencia para mitigar las vulnerabilidades donde los parches nunca estarán disponibles.
Pruebas inadecuadas de cambios de seguridad	Las modificaciones del hardware, firmware y software implementadas sin pruebas podrían comprometer el funcionamiento normal de los ICS. Se deben desarrollar procedimientos documentados para probar todos los cambios de impacto en la seguridad. Los sistemas operativos en vivo nunca deben ser utilizados para la prueba. Es posible que sea necesario coordinar las pruebas de las modificaciones del sistema con los proveedores e integradores de sistemas.
Controles de acceso remoto deficientes	Hay muchas razones por las que es posible que se pueda tener acceso remoto a un ICS, incluidos los proveedores y los integradores de sistemas que realizan funciones de mantenimiento del sistema, y también los ingenieros de ICS que acceden a componentes de sistemas geográficamente remotos. Las capacidades de acceso remoto deben controlarse adecuadamente para evitar que personas no autorizadas accedan al ICS.
Se utilizan configuraciones deficientes	Los sistemas configurados incorrectamente pueden dejar abiertos puertos y protocolos innecesarios, estas funciones innecesarias pueden contener vulnerabilidades que aumentan el riesgo general para el sistema. El uso de configuraciones predeterminadas a

	menudo expone vulnerabilidades y servicios explotables. Todos los ajustes deben ser examinados.
Las configuraciones críticas no se almacenan o se respaldan	Los procedimientos deben estar disponibles para restaurar los ajustes de configuración de los ICS en caso de cambios de configuración iniciados accidental o por un atacante para mantener la disponibilidad del sistema y evitar la pérdida de datos. Se deben desarrollar procedimientos documentados para mantener los ajustes de configuración del ICS.
Datos desprotegidos en dispositivos portables	Si los datos sensibles (por ej., contraseñas, números de teléfono) se almacenan en el texto plano en los dispositivos portables tales como ordenadores portátiles y dispositivos móviles y estos dispositivos se pierden o se roban, la seguridad del sistema podría ser comprometida. Se requieren políticas, procedimientos y mecanismos para su protección.
Generación, uso y protección Contraseñas no se realiza de acuerdo con la política de seguridad	Hay una gran experiencia con el uso de contraseñas que es aplicable a los ICSs. La política y el procedimiento de seguridad para las contraseñas deben ser seguidos para que sean eficaces. Las violaciones de políticas y procedimientos de contraseñas pueden aumentar drásticamente la vulnerabilidad de ICS.
Aplicación de inadecuados Controles de acceso	Los controles de acceso deben coincidir con la forma en que la organización asigna responsabilidades y privilegios a su personal. Los controles de acceso mal especificados pueden dar como resultado que un usuario de ICS tenga demasiados o pocos privilegios. Los siguientes

	ejemplifican cada caso: • El sistema se configura con ajustes de control de acceso predeterminados dando a un operador privilegios administrativos • El sistema se configura incorrectamente y da como resultado que un operador no pueda tomar acciones correctivas en una situación de emergencia
Vínculo incorrecto de datos	Los sistemas de almacenamiento de datos ICS pueden estar vinculados con orígenes de datos que no provienen de sistemas que no son ICS. Un ejemplo de esto son los enlaces de base de datos, que permiten que los datos de una base de datos se repliquen automáticamente a otros. El vínculo de datos puede crear una vulnerabilidad si no está configurado correctamente y puede permitir el acceso o la manipulación de datos no autorizados.
Protección contra malware no instalada o actualizada	La instalación de software malicioso, o malware, es un ataque común. El software de protección contra malware, como el software antivirus, debe mantenerse actualizado en un entorno muy dinámico. El software de protección contra malware y las definiciones obsoletos dejan el sistema abierto a nuevas amenazas de malware.
Protección contra malware implementada sin pruebas suficientes	El software de protección contra malware implementado sin pruebas suficientes podría impactar el funcionamiento normal del ICS y bloquear el sistema para realizar las acciones de control necesarias.
Denegación de servicio (DoS)	El software de los ICSs podría ser vulnerable a los ataques de DoS, lo que

	resultaría en la prevención del acceso autorizado a un recurso del sistema o al retraso en las operaciones y funciones del sistema.
Software de detección/prevención de intrusos no instalados	Los incidentes pueden resultar en la pérdida de la disponibilidad e integridad del sistema; la captura, modificación y supresión de datos; y ejecución incorrecta de comandos de control. El software IDS/IPS puede detener o impedir varios tipos de ataques, incluidos los ataques de DoS, y también identificar hosts internos atacados, como los infectados con gusanos. El software IDS/IPS debe probarse antes de la implementación para determinar que no compromete el funcionamiento normal del ICS.
No mantenimiento de registros	Sin registros apropiados y precisos, puede ser imposible determinar qué causó que ocurriera un evento de seguridad.

Tabla 4: Vulnerabilidades Físicas y condiciones predispuestas

Vulnerabilidad	**Descripción**
El personal no autorizado tiene acceso físico a los equipos	El acceso físico a los equipos del ICS debe limitarse únicamente al personal necesario, teniendo en cuenta los requisitos de seguridad, como el cierre de emergencia o los reinicios. El acceso incorrecto al equipo de ICS puede llevar a cualquiera de los siguientes ataques: • Robo físico de datos y hardware • Daño físico o destrucción de datos y hardware • Cambios no autorizados en el entorno funcional (p. ej., conexiones de datos, uso no autorizado de

	medios removibles, agregar/quitar recursos) • Desconexión de los enlaces de datos físicos • Interceptación indetectable de datos (pulsación de tecla y otro registro de entrada
Radiofrecuencia, pulso electromagnético (EMP), descarga estática, caídas y picos de tensión	El hardware utilizado para los sistemas de control es vulnerable a la radiofrecuencia y pulsos electro-magnéticos (EMP), descarga estática, caídas y picos de tensión.. El impacto puede variar desde la interrupción temporal del mando y control hasta el daño permanente a las placas de circuitos. Se recomienda el blindaje adecuado, la conexión a tierra, el acondicionamiento de energía y/o la supresión de sobretensiones.
Respaldo de las fuentes d poder	Sin respaldo de poder para activos críticos, una pérdida general de poder inhabilitaría all ICS y podría crear una situación insegura. La pérdida de energía también podría llevar a ajustes predeterminados inseguros.
	Pérdida de control ambiental la pérdida de control ambiental (p. ej., temperaturas, humedad) podría ocasionar daños al equipo, tales como el sobrecalentamiento de los procesadores. Algunos procesadores se apagarán para protegerse; algunos pueden continuar operando, pero en una capacidad mínima y pueden producir errores intermitentes, reiniciar continuamente o quedar incapacitados permanentemente.
Puertos físicos inseguros	Los puertos de bus serie universal (USB) y PS/2 pueden permitir la conexión no

	autorizada de las unidades USB, los registradores de teclas, etc.

Tabla 5: vulnerabilidades de desarrollo de software y condiciones predispuestas

Vulnerabilidad	Descripción
Validación incorrecta de datos	El software del ICS puede no validar correctamente entradas de usuario o datos recibidos para asegurar la validez. Los datos no válidos pueden dar lugar a numerosas vulnerabilidades, como buffer overflow, inyecciones de comandos, cross-site scripting y rutas transversales de path.
Capacidades de seguridad instaladas no habilitadas de forma predeterminada	Las capacidades de seguridad que se instalaron con el producto son inútiles si no están habilitadas o al menos identificadas como deshabilitadas.
Software con inadecuada autenticación, privilegios y control de acceso	El acceso no autorizado a software de configuración y programación podría proporcionar la capacidad de corromper un dispositivo.

Tabla 6: Vulnerabilidades de configuración de red y comunicaciones y condiciones predispuestas

No se emplean Controles de flujo de datos	Los controles de flujo de datos, basados en características de datos, son necesarios para restringir qué información se permite entre sistemas. Estos controles pueden prevenir la filtración de información y operaciones ilegales.
Firewalls o Cortafuegos inexistentes o configurados incorrectamente	Una carencia de cortafuegos correctamente configurados podrían permitir que los datos innecesarios pasen entre las redes, tales como control y redes corporativas, permitiendo que los ataques y el malware se difundan entre las redes,

	haciendo sensible datos susceptibles de monitoreo/espionaje, y proporcionar a las personas acceso no autorizado a los sistemas.
Registros inadecuados en firewalls y routers	Sin registros apropiados y precisos, puede ser imposible determinar qué causó un incidente de seguridad.
Los protocolos de comunicación y estándares bien documentados se utilizan en texto sin formato	Los atacantes pueden supervisar la actividad de la red ICS usando un analizador de protocolos u otras utilidades para decodificar los datos transferidos por protocolos como Telnet, protocolo de transferencia de archivos (FTP), Protocolo de transferencia de hipertexto (http) y sistema de archivos de red (NFS). El uso de tales protocolos también hace que sea más fácil para los atacantes realizar ataques contra el ICS y manipular la actividad de la red ICS.
La autenticación de usuarios, datos o dispositivos es deficiente o inexistente	Muchos protocolos ICS no tienen autenticación en ningún nivel. Sin autenticación, existe la posibilidad de reproducir, modificar o falsificar datos o falsificar dispositivos como sensores e identidades de usuario.
	Protección de datos inadecuada entre clientes inalámbricos y puntos de acceso los datos sensibles entre clientes inalámbricos y puntos de acceso deben protegerse mediante un cifrado fuerte para asegurar que los adversarios no puedan obtener acceso no autorizado a los datos no encriptados.
Uso de protocolos ICS inseguros en toda la industria	Los protocolos ICS a menudo tienen pocas o ninguna capacidad de seguridad, como autenticación y encriptación, para proteger los datos contra accesos no

	autorizados o manipulación. Además, la implementación incorrecta de los protocolos puede conducir a vulnerabilidades adicionales.
Falta de comprobación de integridad de las comunicaciones	No hay controles de integridad integrados en la mayoría de los protocolos de control industrial; los adversarios podían manipular las comunicaciones sin ser detectadas. Para garantizar la integridad, el ICS puede utilizar protocolos de capa inferior (por ejemplo, IPSec) que ofrezcan protección de la integridad de los datos.
Autenticación inadecuada entre clientes inalámbricos y puntos de acceso	Se necesita una fuerte autenticación mutua entre clientes inalámbricos y puntos de acceso para asegurar que los clientes no se conecten a un punto de acceso no fiable desplegado por un atacante, y también para asegurarse de que los atacantes no se conectan a ninguna de las redes inalámbricas del ICS.