UNIVERSIDAD DE ORIENTE

Trabajo final presentado en opción al Título de Máster en Automática

Autora: Ing. Yelena Pérez Zamora

Tutores: Dr.C. Israel Francisco Benítez Pina

MSc. Luisa Villafruela Loperena

Santiago de Cuba

2021

UNIVERSIDAD DE ORIENTE

Facultad de Ingeniería Eléctrica

Departamento de Ingeniería en Automática

Trabajo final presentado en opción al Título de Máster en Automática

Título: Propuesta de diseño de seguridad para Supervisión Industrial Integrada.

Autora: Ing. Yelena Pérez Zamora

Tutores: Dr.C. Israel Francisco Benítez Pina

MSc. Luisa Villafruela Loperena

Pensamientos

El futuro tiene muchos nombres. Para los débiles es lo inalcanzable. Para los temerosos, lo desconocido. Para los valientes es la oportunidad.

Hugo, Victor

Dedicatoria

A mis padres, abuelos y tíos por la educación y paciencia de toda una vida. A mi esposo por ser el motor impulsor de mis logros y a mi ángel en el cielo.

Agradecimientos

A mis familiares, compañeros y amigos por su paciencia y comprensión, a mis tutores por su preciado tiempo y a todo el que de una manera u otra me ha transmitido conocimientos; a todos gracias por estar o haber estado en mi vida.

Resumen

Cada día, las empresas están más conectadas y la tecnología se hace imprescindible para que esto sea posible. Tratándose de la industria, la inserción de tecnología en los últimos años ha motivado la aparición del término industria 4.0, que representa toda la automatización y conectividad entre las personas, el software y el hardware; que permiten alcanzar niveles cada vez mayores de excelencia y productividad. Gran parte de la automatización de los procesos industriales está asociado al auge del concepto de Internet de las Cosas (IoT, *Internet of Things*). Muchas empresas ya utilizan el IoT en sus estructuras, pero una pequeña parte aplica recursos para mantener los principios básicos de seguridad digital en estas estructuras. En la actualidad, los datos y variables de un sistema de control son los elementos más importantes a salvaguardar en una red industrial, por lo que resulta de vital importancia garantizar su seguridad. En este trabajo se presenta el diseño y simulación de una Red Desmilitarizada (DMZ, *Demilitarized Zone*) utilizando cortafuegos, para controlar el acceso a la información que se encuentra almacenada en servidores de la red industrial. Se muestran características, configuraciones, métodos y reglas de las DMZ y los cortafuegos, seleccionando la configuración con tres cortafuegos de múltiples patas como la adecuada para la industria, ya que permite el intercambio de datos añadiendo seguridad y evitando en cierta medida la violación del Sistema de Control. También se explican los resultados de la simulación de la red propuesta para la Refinería de Santiago de Cuba como caso de estudio.

Abstract

Every day, companies are more connected and technology is essential for this to be possible. When it comes to industry, the insertion of technology in recent years has led to the appearance of the term industry 4.0, which represents all automation and connectivity between people, software and hardware; that allow reaching ever higher levels of excellence and productivity. Much of the automation of industrial processes is associated with the rise of the concept of the Internet of Things (IoT, Internet of Things). Many companies already use the IoT in their structures, but a small part apply resources to maintain the basic principles of digital security in these structures. At present, the data and variables of a control system are the most important elements to safeguard in an industrial network, so it is vitally important to guarantee its security. This paper presents the design and simulation of a Demilitarized Zone (DMZ) using firewalls to control access to the information that is stored in servers of the industrial network. Characteristics, configurations, methods and rules of DMZs and firewalls are shown, selecting the configuration with three multi-legged firewalls as suitable for the industry, since it allows the exchange of data adding security and avoiding to a certain extent the violation of the System of control. The results of the simulation of the network proposed for the Santiago de Cuba Refinery as a case study are also explained.

Índice

Lista de símbolos, términos especiales y abreviaturas no normalizadas

IoT : Internet de las Cosas, *Internet of Things*.

DMZ: Red Desmilitarizada, *Demilitarized Zone*.

TCP/IP: Protocolo de control de transmisión/Protocolo de Internet, *Transmission Control Protocol/Internet Protocol.*

RCI: Redes de Comunicación Industriales, *Industrial Communication Networks.*

ICS: Sistemas de Control Industrial, *Industrial Control System*.

SCADA: Sistemas de Supervisión Control y Adquisición de Datos, *Supervisory Control And Data Acquisition.*

IT: Tecnología de la Información, *Information technology.*

OT: Tecnología Operativa, *Operational technology.*

DCS: Sistemas de Control Distribuido, *Distributed Control System*.

CIM: Manufactura Integrada por Computadores, *Computer Integrated Manufacturing.*

HMI: Interfaz Hombre-Máquina, *Human Machine Interface*.

QoS: Calidad de Servicio, *Quality of Service*.

LAN: Red de Área Local, *Local Area Network*.

WAN: Red de Área Amplia, *Wide Area Network*.

RTU: Unidad de Terminal Remoto, *Remote Terminal* Unit.

RAP: Puntos de Acceso Remoto, *Remote Access Point.*

PLC: Controlador Lógico Programable, *Programmable Logic Controller*.

CIP: Protocolo Industrial Común, *Common Industrial Protocol*.

IIoT: Internet industrial de las cosas, *Industrial Internet of Things.*

TLS: Seguridad de la Capa de Transporte, *Transport Layer Security*.

ODVA: Asociación abierta de proveedores de DeviceNet, *Open DeviceNet Vendors Association*.

DoS: Denegación de Servicios, *Denial of Service*.

MTU: Unidad de Terminal Maestro, *Master Terminal Unit*.

NISCC: Centro Nacional de Coordinación de Seguridad de Infraestructura.

IEC: Comisión Electrotécnica Internacional, *International Electrotechnical Commission.*

INTRODUCCIÓN

La evolución de la informática y de las computadoras propició la necesidad de establecer vías de comunicación entre ellas, surgiendo de esta forma las conocidas redes LAN, MAN, WAN. La estructura y el modo de funcionamiento de estas redes están definidos en varios estándares, siendo el más importante y extendido de todos ellos el modelo TCP/IP [1], basado en el modelo de referencia OSI [2]; este último estructurado en siete capas con funciones concretas pero relacionadas entre sí; donde TCP/IP se reduce a sólo cuatro capas. Existen multitud de protocolos repartidos por cada capa, los cuales también están regidos por sus respectivos estándares.

En la búsqueda de la integración de las comunicaciones industriales fueron desarrolladas las redes de comunicaciones industriales basadas en los estándares FIELDBUS [3] , que realizan el proceso de adquisición de datos y luego los transmiten a niveles gerenciales comunicándose a través de Ethernet; además de realizar aplicaciones en Novell Net o TCP/IP en paralelo y sin producir interferencias entre ellas.

El desarrollo de las redes informáticas en el ámbito industrial, trajo consigo la necesidad de políticas de seguridad para la prevención de ataques informáticos, debido a las múltiples vulnerabilidades en el sistema; acceso indebido que provocaría fatales consecuencias; daños en las comunicaciones, en el proceso industrial y en el personal técnico.

Los Sistemas de Control Industrial (ICS, *Industrial Control System*) [4] hacen parte de nuestra vida cotidiana, están presentes en la generación y suministro de la energía eléctrica, gas natural, agua, plantas químicas, alimenticias, farmacéuticas, en el control de edificaciones y viviendas y también los encontramos en las plantas de producción manufactureras, entre otros.

Históricamente los Sistemas de Control Industrial y los Sistemas de Supervisión, Control y Adquisición de Datos (SCADA, *Supervisory Control And Data Acquisition*) [4]; sistemas de gestión y toma de decisiones industriales, se han basado en entornos cerrados construidos alrededor de protocolos y sistemas propietarios para aplicaciones específicas, en muchos de los casos estos se han declarado sistemas

seguros, porque estaban aislados del resto de la red corporativa y eran diseñados a medida, donde muy pocas personas conocían como funcionaban en detalle.

Con el tiempo las políticas de reducción de gastos provocaron que paulatinamente se haya ido optando por la estandarización de los protocolos y plataformas SCADA, para facilitar la interoperabilidad entre distintas marcas en los distintos niveles de operación de estos sistemas; generando así una competencia más intensa entre fabricantes y por ende abaratando los costos en su implementación. Esta tendencia de estandarización ha llevado a la mayoría de los fabricantes a migrar hacia redes conocidas como TCP/IP, intentando aprovechar al máximo la infraestructura existente en las empresas.

De esta manera los SCADA han dejado de ser un sistema desconocido y la excusa de que son seguros debido a que no están expuestos ya no es cierta; cualquiera que pueda adquirir el conocimiento sobre cómo está implementada la red, podría aplicar técnicas de explotación e intrusión tradicionales sobre estas plataformas abiertas de hardware y software con vulnerabilidades heredadas de los viejos sistemas aislados.

Aunque en muchos entornos sigue existiendo la sensación de que los SCADA son una red cerrada, la realidad indica que cada vez tienen más interconexiones tanto por necesidades de negocios como para reducir gastos; por ejemplo la unificación de la red de control o industrial con la red de usuarios o comercial, el mantenimiento remoto, la automatización del monitoreo, etc. En definitiva, se han ido eliminando aquellos puntos que hacían del SCADA un sistema único, independiente e inviolable y las bases sobre las que construíamos los conceptos de seguridad en SCADA; dejando así al descubierto y con total vulnerabilidad las redes de las que dependemos para concebir el mundo industrializado como lo conocemos hasta el momento.

Aún existen en la actualidad sistemas SCADA que se encuentran entrelazados con las redes comerciales de la empresa sin total separación o control de acceso; o sea, que carecen de dispositivos de seguridad como cortafuegos [5], mecanismos de cifrado [6] o software antivirus entre otros. En muchos casos los ordenadores tienen dos tarjetas de red conectadas, por un lado a la red de la empresa y por otro al sistema SCADA, en otros casos están conectadas a través de dispositivos inalámbricos y muchas veces se encuentran simplemente aisladas totalmente.

En el caso de que se encuentren conectadas a través de tarjetas de red o dispositivos inalámbricos solamente, esto crea una puerta de enlace potencial entre ambas, ya que basta comprometer alguna máquina para poder acceder de una red a otra. Los atacantes no necesitan ser expertos en redes de control de procesos, basta con atacar una máquina de la red local de la empresa que tenga acceso a la red SCADA para poder causar daños.

La seguridad informática en los ICS [7] ha venido tomando mucha importancia en los últimos años, ya que las tecnologías operacionales presentes en los ICS y los procesos dentro de ella están haciendo un mayor uso de estándares comunes presentes en las tecnologías de la información y las comunicaciones; trayendo 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 estas generan.

En una red empresarial típica, los sistemas se gestionan continuamente en un intento por mantenerse a la vanguardia de esta amenaza que evoluciona rápidamente, pero estos métodos a menudo entran en conflicto con los requisitos básicos de confiabilidad y disponibilidad de una red industrial. Debido a la importancia de las redes industriales y a las consecuencias potencialmente devastadoras de un ataque, es necesario adoptar nuevos métodos de seguridad. Las redes industriales son objetivos de un nuevo perfil de amenaza que utiliza ataques más sofisticados y específicos que nunca. Una tendencia igualmente inquietante es el aumento de eventos accidentales que se verán con más detalle en el capítulo 1, que han llevado a consecuencias significativas causadas cuando un usuario del sistema autorizado sin saberlo introduce amenazas en la red, durante su interacción normal y de rutina. Esta interacción puede ser una administración normal del sistema local o mediante una operación remota del sistema. Muchos sistemas industriales se construyen utilizando dispositivos heredados y, en algunos casos, ejecutan protocolos heredados que han evolucionado para operar en redes enrutables. Los sistemas de automatización fueron construidos para la confiabilidad mucho antes de la proliferación de conectividad de Internet, aplicaciones basadas en web y sistemas de información de negocios en tiempo real. La seguridad física siempre fue una preocupación, pero la seguridad de la información no era

típicamente una prioridad porque los sistemas de control estaban a cielo abierto, es decir, físicamente separados sin ningún sistema común (electrónico u otro) que cruzara esa brecha.

Los ICS 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 los ICS se conoce, o si el hardware, software, configuraciones, redes y estándares son típicos; esto puede ser aprovechado por atacantes, para causar daños desde mínimos hasta irreparables.

Una carencia de estos sistemas es que aún en la actualidad son escasas las medidas de seguridad básica que se han implementado en sus niveles tales como cifrado, autenticación, almacenamiento de datos críticos en textos planos, redundancia e incluso hay implementaciones cuya pila TCP/IP es defectuosa, lo que las hace vulnerable a una variedad de ataques plenamente conocidos. Por ejemplo, los sistemas SCADA son muy sensibles a escaneos de red, por lo tanto es bastante arriesgado ejecutar un proceso de auditoría de seguridad, ya que los resultados son impredecibles. Los mismos van desde ralentización de la red hasta denegaciones de servicio, es decir, que muchos de los controles de seguridad empleados en otro tipo de entornos no son directamente trasladables a los sistemas SCADA. Por lo tanto es necesario analizar la seguridad a nivel de red, tanto del software como de las aplicaciones e instalaciones de carácter industrial que coexistan. Dentro de este análisis, es necesario incluir no sólo las necesidades de protección de la información y autentificación de los accesos a las distintas entidades que componen una red industrial, sino que también se deben tener en cuenta las necesidades funcionales de un sistema de automatización, tanto en funcionamiento normal como en caso de averías, mantenimiento y modernización de la instalación.

Con la integración entre el SCADA y las redes comerciales, la seguridad de los ICS [4] se ha vuelto cada vez más importante. Las políticas tradicionales de seguridad de la Tecnología de la Información (TI) [8], se centran principalmente en la confidencialidad de los datos, en donde la disponibilidad de la red es la prioridad de seguridad más baja. Por el contrario los ICS, especialmente aquellos que se consideran

infraestructura crítica, deben mantener un alto nivel de disponibilidad del sistema por muchas razones, incluyendo la seguridad económica, ambiental, humana y nacional. Para muchos procesos, sería inaceptable degradar el rendimiento por razones de seguridad, lo que requiere un análisis de riesgo para que cada sistema haga tal determinación. Las protecciones de seguridad deben ser implementadas de una manera que mantenga la integridad del sistema durante el funcionamiento normal, así como durante los tiempos de ciberataque.

En diferentes entornos industriales en nuestro país, las medidas de seguridad adoptadas van desde pocas a casi nulas, donde existen algunos proyectos entre distintas empresas como Copextel, que se encargan del montaje o de realizar propuestas cuyos costos son elevadísimos, ya que la tecnología utilizada para la ejecución de estos proyectos de seguridad se realizan con tecnología importada. De especial importancia en el ámbito industrial cubano está el software SCADA EROS XD [9], porque su uso va incrementándose en nuestras industrias. Por lo anterior, es importante que los desarrolladores de aplicaciones de automatización industrial integrada con estos dispositivos, conozcan lo que deben tener en cuenta para elevar la ciberseguridad de la aplicación específica.

Por lo antes expuesto se puede definir el **problema de la investigación** como la necesidad de acceder de manera segura a los datos de una red industrial, con vistas a lograr la interconexión de una red empresarial con una red industrial.

En base a lo anteriormente planteado se define como **objeto de la investigación** la ciberseguridad en redes industriales, precisándose como **campo de acción** los mecanismos de ciberseguridad en redes industriales.

El **objetivo de la investigación** consiste en diseñar un sistema de seguridad que permita la interconexión de una red empresarial con una red industrial, utilizando redes desmilitarizadas y cortafuegos, como soporte de supervisión industrial integrada.

Como **hipótesis** se plantea que si se logra diseñar un sistema de seguridad que permita la interconexión de una red empresarial con una red industrial, utilizando redes desmilitarizadas y cortafuegos como soporte de supervisión industrial integrada, existirían mecanismos de seguridad que permitan dicha interconexión asegurando los datos almacenados en la red industrial, para una eficiente integración empresarial.

Las **tareas** para dar cumplimiento al objetivo de la presente investigación se relacionan a continuación:

1. Definir los aspectos teóricos referentes a la Automatización Industrial, las diferencias entre las redes empresariales e industriales, la seguridad en los Sistemas de Control Industrial, así como los mecanismos de ciberseguridad propuestos para estos sistemas.
2. Realizar una propuesta de diseño en cuanto a seguridad para Sistemas de Control Industrial, que cumpla con los requerimientos y exigencias de las aplicaciones modernas de automatización.
3. Simular la propuesta de diseño de seguridad, empleando como caso de estudio la “Refinería Hermanos Díaz”.
4. Proponer otros mecanismos de seguridad a tener en cuenta a la hora de integrar SCADA a IT.

En el transcurso de la investigación se utilizaron las siguientes **técnicas y métodos:**

- Análisis de fuentes documentales.
- Técnicas y Métodos Empíricos: Observación, Encuestas y Entrevistas.
- Método Histórico-lógico.
- Método de Análisis y Síntesis.
- Métodos Experimentales: Diseño y Simulación.

Significación práctica de la investigación

La propuesta de diseño y simulación de una red DMZ usando cortafuegos, permite crear un perímetro de defensa entre las redes externas de una organización y la red de control, con el objetivo de asegurar los datos almacenados en esta última, aumentando así la protección de los sistemas supervisorios integrados modernos.

El trabajo se encuentra organizado de la siguiente forma: una introducción general en la que se exponen las principales motivaciones que llevaron a la realización de esta investigación y en la que además se encuentra la fundamentación de su diseño metodológico; dos capítulos que constan de introducciones parciales para la mejor comprensión de sus objetivos, los que a su vez, se encuentran organizados por

epígrafes, de manera que se facilite su revisión por parte del lector. Se brindan además, las conclusiones de cada capítulo, aparte de las conclusiones generales, recomendaciones, bibliografía y anexos.

En el capítulo 1 se presenta el estudio teórico de la presente investigación. Para ello se aborda sobre la automatización de procesos industriales dando paso a la automatización basada en computadores. Además, se analiza el valor de los sistemas supervisorios para los atacantes y se hace una comparativa de estos sistemas con las redes empresariales tradicionales. Se analiza la importancia de la seguridad en los sistemas supervisorios y se exponen las características de seguridad de algunos de los protocolos industriales; además de clasificar las amenazas de seguridad que presentan estos sistemas y algunas de las medidas preventivas contra esas amenazas o vulnerabilidades.

El capítulo 2 muestra el diseño y la simulación de la red DMZ propuesta basada en la configuración de una DMZ con 3 costafuegos de múltiples patas, que se integran con cortafuegos ubicados entre las redes externas e internas. Se realiza la descripción del diseño y se muestra la configuración de la red DMZ propuesta para la red empresarial e industrial, de conjunto con la configuración de los cortafuegos establecida, las definiciones de las políticas de seguridad y las reglas de filtrado de paquetes. También se presentan recomendaciones necesarias para garantizar la creación de Supervisorios Industriales ciberseguros, soportados sobre esta arquitectura de red con DMZ y cortafuegos, lo cual complementa la implementación eficiente de dichos sistemas industriales modernos.

CAPÍTULO 1. CARACTERÍSTICAS Y TECNOLOGÍAS DE LOS ICS INTEGRADOS MODERNOS

En la industria moderna, la convergencia entre los sistemas de información y redes de operaciones (OT, *Operational Technology*) que interconectan los distintos elementos de producción en planta y los sistemas de información corporativos (IT, *Information technology*) de una industria, plantea nuevos retos de ciberseguridad en el contexto de transformación de la industria 4.0 [7]. La digitalización de prácticamente la totalidad de los sectores industriales y la globalización de los modelos de producción son dos catalizadores que hacen inevitable la convergencia en las políticas de seguridad entre los sistemas de información del ámbito OT y los sistemas corporativos IT de las industrias. Un reto crucial de la Industria 4.0 es dicha convergencia, garantizando en todo momento el intercambio de datos e información, de manera estandarizada y segura entre dispositivos, máquinas, sistemas y servicios.

1. AUTOMATIZACIÓN DE PROCESOS

La sustitución del quehacer humano en los procesos técnicos por equipos mecánicos, eléctricos, electrónicos, con el fin de optimizar el uso de los recursos y la continuidad de los procesos, recibe el nombre de automatización. El desarrollo tecnológico y la existencia de información al alcance de todos, ha llevado a la humanidad a idear metodologías y prácticas para estructurar las organizaciones empresariales, de la comunicación y el manejo de datos desarrollados en diferentes plataformas, así como técnicas y arquitecturas de automatización [10].

Para el modelado de procesos industriales se definen requerimientos comunes para todas las implementaciones, independientemente de los requisitos específicos del proceso. La automatización debe proveer una infraestructura que permita cubrir los aspectos del proceso productivo con el fin de lograr un incremento de la producción, manteniendo o reduciendo costos. Por tanto, en estos modelos se encuentran presentes actividades como la Optimización, Planificación, Supervisión y el Control. En función del proceso industrial, se organizan e integran estas actividades definiendo arquitecturas jerárquicas, heterárquicas e inclusive híbridas, donde se toman las características convenientes de algunos modelos referenciales de automatización [10].

La digitalización ha pasado de ser un elemento relevante en la evolución de los sistemas de automatización industrial a convertirse en el epicentro de una nueva etapa, conocida como industria 4.0 [7]. Es una transformación que viene caracterizada por la unión entre el mundo físico y el digital, un escenario global donde se diluyen conceptos como fronteras sectores, empresas o la propia distinción entre producto y servicio. La digitalización industrial, además de constituir un reto para los actuales modelos productivos, proporcionará nuevas oportunidades de crecimiento económico, así como mejoras sustanciales a la competitividad, flexibilidad y eficiencia de los procesos de producción industrial. La integración de la tecnología de la información se traducirá en la optimización e interacción de los procesos de investigación y desarrollo, diseño, producción, logística y prestación de servicios asociados.

1.1 Automatización Industrial

La Automatización Industrial combina ingenierías como la eléctrica, electrónica, mecánica, química, de comunicaciones, computacional y de software. Constituye un conjunto de técnicas que involucran la aplicación e integración de sistemas industriales de forma autónoma, área en la que confluyen disciplinas para la solución de problemas de procesos productivos tales como la eficiencia, productividad, calidad y diseño de procesos a nivel de producción, planta y nivel gerencial [10]. Por tanto, aborda problemas técnicos y operacionales en todos los niveles de los sistemas productivos.

El proceso de automatización consiste en diseñar sistemas capaces de ejecutar tareas repetitivas y de controlar operaciones con la mínima intervención del operador. Debe permitir la disposición de elementos para supervisar y controlar cada proceso dentro de la cadena de producción, almacenamiento y distribución; así como diferentes servicios ofrecidos a los clientes por parte de las fábricas, empresas y proveedores. Implica la implantación de instrumentación, dispositivos de maniobra, máquinas mecánicas o hidráulicas, autómatas, paneles, SCADAs y redes de comunicación que enlacen todos los elementos que componen el sistema de automatización [10].

Mediante la implementación de sistemas automatizados se logra:

- Mejorar la productividad de la empresa, reduciendo los costes de la producción y mejorando la calidad de la misma.

- Mejorar las condiciones de trabajo del personal, suprimiendo los trabajos peligrosos incrementando así la seguridad.
- Realizar las operaciones imposibles de controlar intelectual o manualmente.
- Mejorar la disponibilidad de productos, proporcionando las cantidades necesarias en el momento preciso.
- Simplificar el mantenimiento de forma que el operario no requiera grandes conocimientos para la manipulación del proceso productivo.
- Integrar los sistemas de gestión y los sistemas de apoyo a la producción.

Independientemente de la arquitectura utilizada, la automatización debe permitir implantar un sistema capaz de realizar la adquisición, control y supervisión de los elementos, procesos y servicios llevados a cabo en las industrias y empresas; posibilitando al personal encargado la monitorización de los procesos.

1.1.1 La Automatización basada en computadores

Con el desarrollo de minicomputadoras a mediados de los 60's y microcomputadores en los 70's, tareas relativas al control de procesos industriales cambian a favor de implementar técnicas de optimización, en función de la potencia de cálculos de los dispositivos microprocesadores y microcontroladores. El computador en un ambiente de control de procesos, cumple funciones de Adquisición de datos, Control digital directo, supervisorio y jerárquico [10]. Este no tan solo puede controlar directamente la operación de las plantas, sino que también proporciona a los ingenieros el estado de las operaciones de los procesos. Es en este rol supervisorio y en la forma de presentación de la información, que se han hecho los mayores cambios actualmente comenzando con los SCADA [11] y los Sistemas de Control Distribuido (DCS, *Distributed Control System*), basados en la filosofía de modelos de Manufactura Integrada por Computadores (CIM, *Computer Integrated Manufacturing*) [12], la cual permite la integración total de los procesos. La Figura 1.1 muestra gráficamente el concepto de control supervisorio.

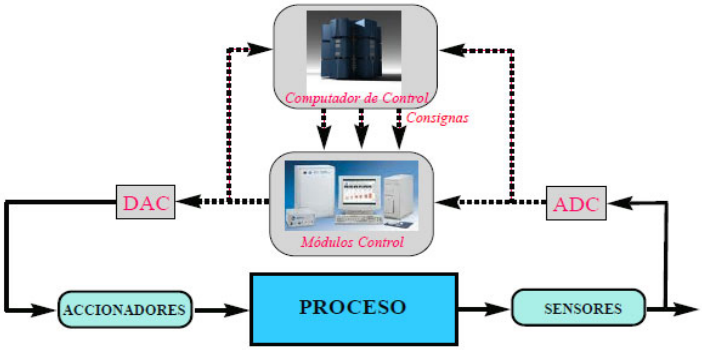

Figura 1.1. Control Supervisorio [10]

Muchas de las aplicaciones del control supervisorio están basadas en el conocimiento de las características del estado estacionario de la planta. En la actualidad existe la tendencia para la implementación de sistemas complejos como la optimización multivariable, el control predictivo multivariable robusto, control multivariable robusto, sistemas inteligentes, entre otros [13].

1.1.2 Sistemas supervisorios. Un objetivo de gran valor para los atacantes cibernéticos dentro de la red industrial

Durante décadas los ICS entre los que se encuentran los sistemas de supervisión y de producción crítica, que forman parte del entorno de OT [14] en empresas industriales, estuvieron apartados de otros sistemas o de Internet. Pero a medida que los sistemas de IT [8] y los entornos de OT aumentan la conectividad entre ellos, los sistemas supervisorios están expuestos ahora a sistemas de IT y a Internet, aumentando el riesgo de intrusión por individuos malintencionados.

El equipamiento comercial para las operaciones de supervisión en las que se encuentran las Interfaces Hombre-Máquina (HMI, *Human Machine Interface*), historiadores, estaciones de trabajo y otros activos informáticos, introduce nuevos riesgos asociados al funcionamiento de los sistemas operativos comerciales [4]. Para mitigar algunos de estos riesgos y abordar los requisitos de cumplimiento, las empresas industriales deben utilizar mecanismos de seguridad en los entornos industriales. Otro aspecto importante para evaluar la vulnerabilidad de los ICS integrados a la gestión empresarial, es tener en cuenta las diferencias entre las redes que soportan ambos sistemas, como veremos a continuación.

1.2 Diferencias entre las Redes Industriales y Empresariales

Con el desarrollo de la automatización industrial, se ha percibido la necesidad de vínculo con el desarrollo de los sistemas computacionales. Inicialmente, la automatización sólo ocurría a nivel de máquinas y supervisión, siendo incorporada posteriormente al proceso de planificación y optimización, para la creación de nuevos modelos de automatización, de acuerdo a las estructuras del sistema de producción. En los últimos años, los avances en la creación de redes industriales [3] tales como la incorporación de la tecnología Ethernet [15] [16], han comenzado a desdibujar la línea entre las redes industriales y empresariales, donde cada una de ellas tiene requisitos fundamentalmente diferentes.

La diferencia más relevante, es que las redes industriales se usan para controlar y monitorear las acciones y condiciones del mundo real [17]. Esto ha dado como resultado el énfasis en un conjunto diferente de consideraciones de Calidad de Servicio (QoS, *Quality of Service*) [18], como la necesidad de un fuerte determinismo y la transferencia de datos en tiempo real. Algunas diferencias entre las redes típicas convencionales y las industriales mencionadas anteriormente, se amplían en detalle a continuación:

- Arquitectura: las redes empresariales pueden consistir en Redes de Área Local (LAN) de sucursales u oficinas conectadas por una red troncal o una Red de Área Amplia (WAN) [19], mientras que las redes industriales tienden a tener una jerarquía de tres o cuatro niveles [20]. La conexión de los instrumentos a los controladores puede ocurrir en un nivel, la interconexión de los controladores en el siguiente y la IHM se puede situar por encima de eso, con una red final para la recopilación de datos y comunicación externa en la parte superior. A menudo se utilizan diferentes protocolos y / o medios físicos en cada nivel, requiriendo dispositivos de pasarela para la comunicación.
- Gravedad de la falla: las redes industriales están conectadas a equipos físicos, por lo que el fallo de un sistema tiene un impacto más severo que el de los sistemas ubicados en redes empresariales. Los diferentes efectos del fracaso de una red industrial, pueden incluir daños a equipos, pérdidas de producción, daños ambientales, pérdida de reputación e incluso de vidas; no siempre causado por fallas en el sistema de control. Desastres industriales como el

nuclear de Fukashima Daiichi en 2011 [21], son ejemplos del impacto severo de un fracaso industrial. Las redes empresariales desvinculadas del sistema físico no crean fallos físicos, sino informáticos y de gestión empresarial.

- Requisitos en tiempo real: la velocidad a la que operan los procesos y equipos en una red industrial requiere que los datos sean transmitidos, procesados y respondidos tan rápido como sea posible; una regla general es que el tiempo de respuesta debe ser menor que el tiempo de muestreo de los datos recopilados [22]. Los retrasos en la entrega de información pueden afectar el rendimiento de los lazos de control, especialmente en el caso de los sistemas a lazo cerrado. Para el caso de las redes empresariales, estas tienden a no tener ningún requisito de tiempo de respuesta y si lo hacen, suelen estar en el rango de decenas de cientos de milisegundos [19].
- Determinismo: no sólo se deben transmitir los datos utilizados en los niveles más bajos de una red industrial en tiempo real, sino que también debe hacerse de manera predecible o determinista, por lo que debe ser posible predecir cuándo una respuesta a una transmisión será recibida[22]. Mientras, las redes empresariales no son afectadas por la inestabilidad tan severamente [19].
- Tamaño de los datos: los paquetes de datos transmitidos en niveles industriales son generalmente muy pequeños a niveles bajos en la arquitectura, donde sólo se necesita transmitir una única medición o valor digital, junto con algunas informaciones generales; estas transmisiones son a menudo unos pocos bytes de tamaño, como la transmisión de un estado binario o un valor de 16 bits [20]. Por otra parte, las redes empresariales transmiten regularmente kilobytes o más de datos, con tamaños de paquete que comienzan en un mínimo de 64 bytes. Esta diferencia requiere protocolos diferentes dentro de la pila de red [19].
- Tráfico periódico y aperiódico: las redes industriales requieren la transmisión de datos muestreados periódica y aperiódicamente, tales como cambios de estado o condiciones de alarma. El período de muestreo para recopilar y transmitir datos puede variar de un dispositivo a otro de acuerdo con los requisitos de control [3]. En las redes empresariales, la transmisión de datos puede implicar un retardo aleatorio antes de que se transmitan los datos [19].

- Robustez: las redes industriales se implementan en una amplia variedad de ubicaciones físicas, a menudo experimentando condiciones adversas tales como humedad, polvo, calor y vibración. Ante estas condiciones, el equipo debe ser resistente y con altas clasificaciones de protección, para evitar daños al equipo [23]. Esto contrasta con las redes empresariales que, en su conjunto, están situadas en ambientes limpios y con temperatura controlada [19].

A pesar de estas diferencias, con la introducción del protocolo Ethernet en las redes industriales y con la necesidad de integración de estas a las redes empresariales, para lograr los niveles de competitividad del mercado globalizado moderno, se requiere homogenizar estas diferencias sin afectar la cyberseguridad del sistema integrado.

1.3 Componentes de un Sistema de Control Industrial

Las redes industriales que soportan sistemas supervisorios, están compuestas de componentes y aplicaciones especializadas capaces de mantener la comunicación [24]. Algunos de estos componentes son los Controladores Lógicos Programables (PLC, *Programmable Logic Controller*), servidor SCADA y los DCS. Es de la comunicación dentro y entre estos componentes y sistemas que las redes industriales se preocupan principalmente [25].

Un ICS se jerarquiza en diferentes capas de red: *red de empresa, red de control y red de campo*. Los componentes de un ICS que se mencionan anteriormente están interconectados en esos diferentes niveles para proporcionar varias funcionalidades. La evolución de los componentes de control para soportar los protocolos basados en IT, llevó a la personalización de los componentes de esta última para satisfacer los requisitos de los ICS tales como disponibilidad, rendimiento, etc. Otra razón detrás del uso de tecnologías de redes basadas en IT, es fusionar las redes empresariales con las redes de control y permitir a los ingenieros controlar y supervisar remotamente el control del proceso fuera de la instalación [24].

En el paradigma de la industria 4.0, a menudo, una máquina de producción moderna está interconectada de distintos modos, ya sea a Internet para el mantenimiento remoto, a la red empresarial para el intercambio de datos de producción, o a otras máquinas y sistemas para una producción automatizada. Una mayor interconexión

significa redes más grandes, un aumento de la comunicación y más requisitos en cuanto a la seguridad.

En el mundo hoy en día, prácticamente no existe ninguna instalación que no esté interconectada mediante Ethernet. La disponibilidad de estas redes, el apoyo de estándares y protocolos de comunicación específicos de aplicación, la superación de grandes distancias y la función fiable bajo condiciones ambientales adversas, son sólo algunos de estos requisitos; por lo que la protección de la comunicación frente a ataques y manipulación, requiere redes protegidas.

1.4 Seguridad en los Sistemas de Control Industrial

El entorno de los ICS se ha vuelto progresivamente más abierto. Los desarrolladores de mercado algunas veces requieren que la información de los sistemas de supervisión y control, sea provista a departamentos comerciales dentro de una empresa, o a terceros por redes de comunicación públicas. Desde una perspectiva operacional, conviene a menudo implementar facilidades remotas de acceso, permitiendo a los operadores de sistema reaccionar a las alarmas de los sistemas de control desde casa, mientras los integradores de sistema y los ingenieros de mantenimiento pueden acceder remotamente a la red de control para monitorear el estatus de los equipos, implementar cambios en el sistema y efectuar mantenimiento remoto.

Las organizaciones deben estar conscientes de las ciberamenazas y factores de riesgo para los sistemas supervisorios, introducidos por empleados externos y sus actividades. Los diseñadores, proveedores e integradores por lo general están más enfocados en el desarrollo de características nuevas que en el desarrollo de sistemas que son intrínsecamente más seguros. Una falta de demanda armonizada del cliente y los requisitos reguladores para la ciberseguridad amplifican la falta de foco en ciberasegurar las redes de control industrial. Sólo recientemente, la necesidad para la ciberseguridad en redes industriales se ha vuelto más prominente [26].

Los ICS se enfrentan a numerosas amenazas de ciberseguridad con diferentes grados de pérdida potencial, que van desde el incumplimiento hasta la interrupción de las operaciones que podrían resultar en la destrucción de la propiedad y desgraciadamente, la pérdida potencial de vidas humanas.

Ejemplos de amenazas potenciales relacionadas con los ICS son:

- Amenazas Persistentes Avanzadas.
- El desborde involuntario de los compromisos de la red corporativa.
- Interrupción de los servicios de red de voz y datos.
- Combate físico y cibernético coordinado.
- Sabotaje interno.
- Interrupción o compromiso de la cadena de suministro.
- Negación de servicios distribuidos.

Dados estos retos, es importante el desarrollo de arquitecturas de seguridad para la protección de infraestructura crítica, que siga una estrategia de defensa en profundidad. La defensa en profundidad define la implementación de controles por niveles para defender un sistema en contra de los diferentes tipos de ataques. La meta es reducir riesgo de información al conservar la disponibilidad y la integridad del ambiente industrial y sobre todo, para proteger vidas humanas.

Para facilitar la conectividad y estabilidad de los ICS, la mayoría de los protocolos de comunicación raramente incorporan consideraciones de seguridad (entre los más difundidos: DNP3, Modbus-TCP, etc.). En el artículo "Cyber Security for Corporate and Industrial Control Systems" [26], mencionan que todos estos protocolos presentan vulnerabilidades, brindando en casi todos los casos gran cantidad de información en texto plano que permite obtener datos relevantes de la infraestructura. A continuación se clasifican las amenazas y se definen algunas medidas preventivas para los ICS.

1.4.1 Problemas de seguridad en sistemas SCADA como principal objetivo dentro de los Sistemas de Control Industrial

Desde el momento que se introduce en el mercado nuevas tecnologías basadas en entornos distribuidos, comienzan a surgir en paralelo nuevos problemas de seguridad en los sistemas SCADA. Un sistema SCADA es un sistema complejo cuyo objetivo principal es el de llevar a cabo los procesos de supervisión y gestión de otros sistemas complejos, cuyos recursos son considerados críticos (por ejemplo el agua, gas o la electricidad). Estos sistemas de control han evolucionado, estando actualmente basados en entornos distribuidos y con componentes (hardware y software) muy

variados. Esta interacción de componentes, junto con la apertura de sus conexiones hacia redes externas como Internet, podría conllevar a vulnerabilidad en estos sistemas críticos. Además, un fallo o interrupción en alguno de sus componentes podría suponer un impacto importante sobre la continuidad de otras infraestructuras, repercutiendo incluso económicamente a una región, a una nación o naciones [27].

Un sistema SCADA está compuesto por dos tipos de redes básicas (ver figura 1.3), la red corporativa y la red de control. En la red corporativa, las operaciones están más relacionadas con la supervisión general del sistema y cuyos empleados requieren de procedimientos de autentificación fuertes, para interactuar con las bases de datos (históricos, alarmas, etc.) y servidores críticos del sistema. En cambio, en la red de control se realizan todas aquellas tareas relacionadas con la supervisión. Estas tareas son gestionadas por un HMI, localizado en el centro principal de control SCADA o subestaciones, y transmitidas a un dispositivo de campo como por ejemplo un RTU, localizado físicamente en la propia planta industrial, o en alguna subestación remota.

Estos dispositivos son capaces de establecer comunicaciones con otras subestaciones, o sea, con otras RTUs y/o con otros dispositivos de campo, por ejemplo un PLC para la supervisión de un control local eficiente. Pueden soportar múltiples sesiones con TCP/IP, por lo que podrían procesar y responder simultáneamente a mensajes provenientes de múltiples fuentes, e igualmente, una misma fuente podría entablar conexión con varias RTUs. Para el control remoto, son capaces de interpretar protocolos específicos como Modbus/TCP [28] o DNP3 [29], y algunas RTUs manejan Linux/Unix o Microsoft Windows para dar soporte a aplicaciones Web, y así proveer mediante interfaces gráficas informes a los operarios.

Para la gestión remota desde cualquier punto de localización física, es necesario utilizar infraestructuras de comunicación versátiles, desde una red Ethernet o una línea de teléfono hasta el uso de Satélite, Microondas, fibra óptica, WiFi, etc., e incluso, algunos sistemas SCADA podrían proveer servicios Web y móviles para reducir las tareas de mantenimiento y minimizar los costes de operación. Además, en estos sistemas de control pueden convivir los protocolos propios de automatización industrial basados en TCP/IP para el control remoto mencionados anteriormente, o aquellos pertenecientes a la familia de Protoclo Industrial Común (CIP, *Common Industrial*

Protocol), mantenido por la Asosiación abierta de Proveedores de DeviceNet (ODVA, *Open DeviceNet Vendors Association*) [30] como: Ethernet/IP, DeviceNet, CompoNet y ControlNet. No obstante, la mayoría presentan vulnerabilidades al carecer de mecanismos de seguridad.

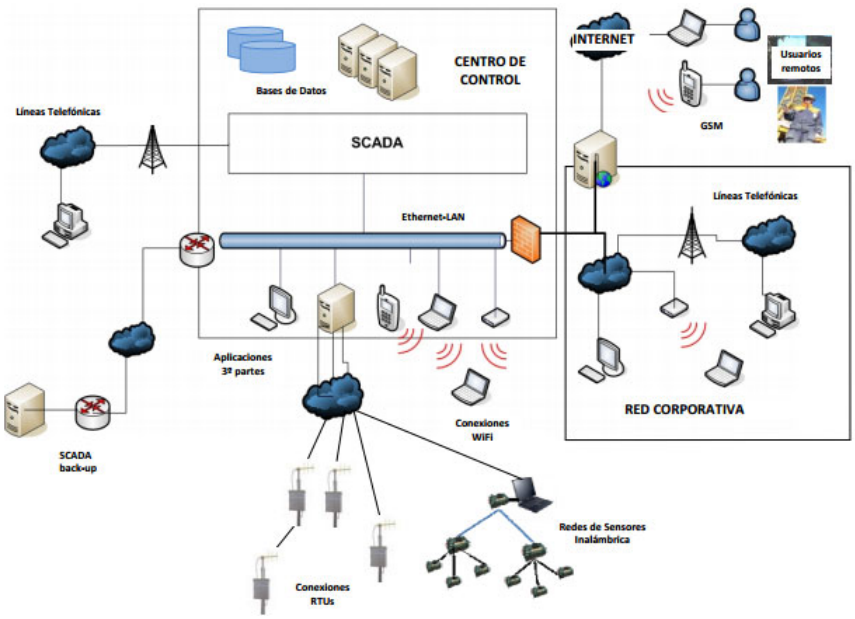

Figura 1.2: Arquitectura de un sistema de red SCADA [27].

Esta arquitectura (Figura 1.2) presenta un riesgo importante desde el punto de vista de la seguridad y disponibilidad del sistema, ya que no sólo suman los diversos ataques conocidos cuando el sistema era cerrado, sino que también se le suman todos aquellos asociados con el estándar TCP/IP y el uso de nuevas tecnologías. Muchas de estas debilidades están registradas en bases de datos públicas, como es el caso de CERT, *Computer Emergency Response Team* [31], el cual tiene publicado desde 1998 alrededor de 2.500 vulnerabilidades y 150 informes técnicos de seguridad, o ISID (Industrial Security Incidents Data) [32]. De hecho, ISID permitió a Byres et.al. [32] concluir que el índice de vulnerabilidades desde el año 2001 eran la mayoría causadas por amenazas externas.

Es importante mencionar que muchos de los sistemas SCADA tienden a utilizar en sus arquitecturas servicios Web no sólo para acceder al sistema desde Internet sino para realizar operaciones de control (recibir datos de campo o enviar órdenes de control) en tiempo real desde cualquier IHM. Generalmente, estas páginas web interactúan con

las bases de datos relacionales para realizar los procesos de autorización. En caso extremo de que estos servicios Web presenten deficiencias de seguridad, existe la posibilidad de que las bases de datos se vean comprometidas. Por lo tanto, se hace casi inevitable adoptar técnicas de desarrollos que prevengan futuros ataques, haciendo uso de herramientas de filtrado de paquetes.

1.4.1.1 Políticas de Seguridad en sistemas SCADA dentro de los Sistemas de Control Industrial

Las políticas de seguridad trasladan los requerimientos de seguridad y fiabilidad de cada sistema SCADA particular, a una serie de procedimientos auditable, los cuales permiten salvaguardar la seguridad en su diseño, implementación, y posterior funcionamiento. A la hora de desarrollar políticas de seguridad para sistemas SCADA, es recomendable seguir las normativas que contemplen controles de seguridad genéricos para sistemas de información. Entre otras, se encuentran las normas NIST 800-53 [33] e ISO/IEC 17799 [34]. No obstante, los requerimientos específicos de los sistemas SCADA, tales como una alta disponibilidad, fiabilidad, y tiempo de reacción, requieren de un conjunto de normas y políticas adaptadas especialmente a sus necesidades [35]. Con este fin, se han extendido normas existentes [33], desarrollando normas como la NIST 800-82 [36].

Para cada sistema SCADA, hay que tener en cuenta principalmente las siguientes políticas de seguridad [37]: protección de datos (acceso y almacenaje), configuración del hardware y software (virus, detección de intrusos, control de acceso, cifrado), seguridad en las comunicaciones (acceso inalámbrico, local, remoto), recursos humanos (uso del sistema, preparación y reciclaje), auditorías, seguridad física (acceso a equipamiento, destrucción de material), y ejecución de operaciones de forma manual en caso de fallo. Todas estas políticas de seguridad están influenciadas por los siguientes factores: las interdependencias existentes dentro de la organización, los roles de los diversos recursos humanos, la arquitectura del sistema de información, los datos manejados dentro de SCADA, y los riesgos asociados al sistema.

1.4.1.2 Protección de las redes SCADA como principal objetivo dentro de los Sistemas de Control Industrial

Para llevar a cabo procesos de gestión de una red SCADA segura será necesario previamente identificar y gestionar todas aquellas conexiones abiertas y directas desde Internet hacia y desde la red SCADA, y desde la red corporativa hacia la red de control mediante mecanismos especializados y restrictivos, tales como: firewalls, IDS (Intrusion Detection System), IPS (Intrusion Prevention Systems), antivirus, protocolos VPN (Virtual Private Networks). Cada uno de estos componentes deberá estar bien configurado y distribuido estratégicamente por todo el sistema con el fin de alcanzar protección. Además, será necesario controlar los accesos desde la red corporativa hacia la red de control y hacia diversos servidores críticos, e igualmente, se deberá proteger los enlaces de comunicaciones mediante cifrado de datos.

En el año 2005, el National Infrastructure Security Co-ordination Centre (NISCC) [38] del BCIT presentó una guía para la configuración y gestión de firewalls para sistemas de control. Dicha guía describe una posible arquitectura de red segura y escalable basada en una división de tres zonas principales, con el objetivo de delimitar cada una de las entidades del sistema, siendo la primera línea de defensa el firewall, los IDS y la DMZ.

El firewall deberá filtrar por un lado direcciones de red, de forma que cada componente SCADA tendrá asignada una dirección IP y uno (o varios) puertos TCP/UDP, y por otro lado, filtrar también a nivel de aplicación, centrando su uso en aquellos servicios de mayor riesgo en una red SCADA. Para poder resumir y estudiar las vulnerabilidades y posibles soluciones en los SCADA dentro de los ICS integrados modernos, se estudian en más detalles los protocolos industriales modernos compatibles con TCP/IP, para luego analizar las posibles amenazas y medidas de prevención existentes.

1.5 Protocolos de comunicación industrial modernos. Ethernet en las redes industriales

Es importante mencionar que los sistemas de supervisión y control tradicionales utilizaban protocolos de comunicación con menos seguridad como MODBUS, FIELDBUS, etc; basados principalmente en la comunicación y prestando menor atención a la seguridad. A partir de la necesidad de integración de las redes industriales a las empresariales, los protocolos de comunicación están evolucionando para incorporar mejoras de seguridad: DNP3 se convierte en DNPV5 [39], OPC en

OPC-UA [40], Modbus evoluciona hacia Modbus seguro [41] y EtherNET/IP se convierte en EtherNET/IP seguro [30].

La introducción de Ethernet en el campo de las redes industriales presentó algunos desafíos. Las normas Ethernet existentes debían ampliarse o modificarse para satisfacer los estrictos requisitos de las redes industriales. Esto se logró en varios niveles de la pila IP utilizando varios enfoques. La mayoría de los buses de campo de serie, incluyendo todos los definidos en la Comisión Electrotécnica Internacional (IEC, *International Electrotechnical Commission)* 61158 [42], funcionan según el modelo reducido definido en MAP / EPA. El modelo MAP / EPA consta de sólo tres capas: *física, enlace de datos y aplicación*, como se muestra en la Figura 1.3.

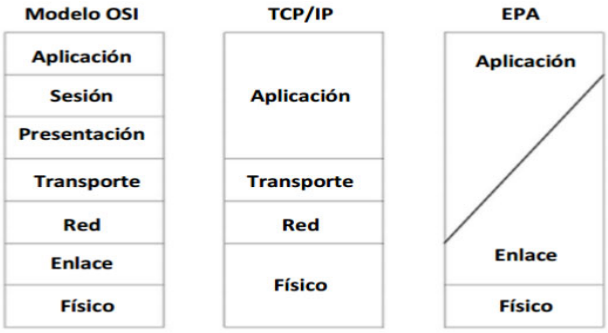

Figura 1.3. Modelos de referencia OSI, TCP/IP y EPA.

Las implementaciones de Ethernet en tiempo real, se basan en el modelo TCP/IP de cuatro capas, con algunas modificaciones para lograr el determinismo. Los requisitos en tiempo real se pueden lograr a través de uno de los tres enfoques.

Los sistemas de Internet industrial de las cosas (IIoT) [43], presentan nuevas técnicas de conexión que requieren protocolos de comunicación seguros. La tecnología Industria 4.0 [44], mantiene su evolución en el sector industrial, y refuerza la necesidad de nuevas medidas de ciberseguridad en el sector de la supervisión industrial inteligente moderna. En el próximo punto daremos atención a algunos de los protocolos industriales modernos, que soportan la comunicación de los sistemas supervisorios actuales y futuros.

1.5.1 Protocolos Industriales como soporte de comunicación

Históricamente, los protocolos eran específicos del proveedor, pero protocolos independientes del proveedor como Modbus-TCP [28] o DNP3 [29] son cada vez más

populares. Estos satisfacen los requerimientos de bajo tiempo de latencia y cómputo de los sistemas supervisorios [45]. Algunos de estos protocolos industriales son:

DNP3: el IEEE 1815 DNP3 [46] es un protocolo abierto, con dos clases de dispositivos definidos. Las estaciones maestras suelen ser dispositivos con alguna potencia de procesamiento y almacenamiento de información, y las estaciones exteriores son dispositivos ubicados en el campo (como líneas de transmisión, subestaciones, transformadores, etc.), encargados de recopilar información de los sensores y enviarla a la estación maestra. Es un protocolo simplificado de tres capas llamado EPA (*Enhanced Performance Architecture*), y su topología ofrece tres tipos de arquitecturas que son: *punto a punto, multipunto* y *concentrador de datos en niveles* [47].

DNP3 es un protocolo diseñado para maximizar disponibilidad de sistema, y pone menos cautela en los factores de confidencialidad e integridad de los datos. El estándar tiene un modelo de operaciones basado en solicitud y respuesta, entonces cuando una petición es hecha para una función que requiere autenticación, la petición no es tramitada a menos que la solicitud de autenticación se resuelva. La recomendación principal en trabajo “Enfoque de seguridad en Sistemas de Control Industrial” [18], sería desplegar sólo DNP3 seguro. Es válido aclarar que esta implementación puede no ser posible por un número de factores diferentes como el soporte lógico informático del fabricante, donde puede ser recomendable el uso de DNP3 encapsulado, dentro de un protocolo seguro de transporte como el protocolo de Seguridad de la Capa de Transporte (TLS) [48] .

Modbus-TCP: diseñado para aplicaciones en tiempo real. Se encuentra en la capa de aplicación en la parte superior de TCP/IP y se basa en los componentes estándar de Ethernet. Tiene un puerto TCP bien conocido (502) para transmitir datos y por lo tanto puede ser controlado a distancia; además es muy fácil de configurar. Se implementa como una arquitectura cliente-servidor por lo que cada dispositivo puede convertirse en cliente o servidor [28].

Modbus no implementa ninguna característica de seguridad, por lo que la comunicación entre dispositivos usando este protocolo debe controlarse. En un trabajo realizado en la Universidad de las Villas titulado: “Enfoque de seguridad en Sistemas de Control Industrial” [18], el autor recomienda que la implementación de un analizador

de tráfico para comprobar que el tráfico Modbus es permitido sólo entre dispositivos específicos y sólo con funciones permitidas, podría ayudar a mitigar problemas de comunicaciones cuando se usa este protocolo. Para este caso puede ser recomendable no sólo el uso de herramientas que analicen el tráfico, sino que lo controlen para no permitir accesos indebidos.

Ethernet-IP: se basa en el Protocolo Común Industrial, que se encuentra en la parte superior de TCP / IP y UDP / IP. Para la transmisión de datos de proceso en tiempo real, UDP / IP se utiliza, posibilitando una comunicación directa entre todos los dispositivos. Básicamente, Ethernet/IP se puede utilizar con todos los protocolos en la capa de la aplicación y sin la limitación del número de dispositivos. Por otra parte, la sincronización de tiempo tiene que ser implementado en hardware por medio de conmutadores especiales con el soporte de una función IEEE 1588 [49]. Para complicar las cosas, los enrutadores tienen características de control de multidifusión/difusión disponibles y no existe un estándar para implementar o configurar estas características [50].

Ethernet /IP es susceptible a ser afectado por las vulnerabilidades de Ethernet como robo de identidad o captura de tráfico. Además, como utiliza UDP para sus mensajes implícitos y esto carece de controles de transmisión, es posible la inyección de tráfico malicioso y manipular la ruta de transmisión usando IGMP. En el trabajo “Enfoque de seguridad en Sistemas de Control Industrial” [18], se aconseja emprender un monitoreo pasivo de la red a fin de asegurar que el tráfico de Ethernet -IP no viene de fuera de la misma [51]. Como Ethernet-IP es un protocolo basado en Ethernet, hay que proveer a la red de todos los mecanismos de seguridad posibles que se basan en Ethernet e IP.

Profinet: la comunicación en este tipo de red tiene lugar cíclicamente y se divide en varias fases. Cada ciclo comienza con la fase isócrona, en el que se trasmiten tramas en tiempo real isócronas (IRT), configuradas ya durante la instalación de la red por medio de relojes sincronizados y esta sincronización se lleva a cabo por un maestro. Después de la fase isócrona, otra fase RT sigue y por último, se proporciona una fase de datos de tiempo de transmisión a través de UDP o TCP. Profinet IRT es un sistema

complejo de planificación, pero ha ganado una cuota de mercado notablemente alta debido a que Siemens apoya su desarrollo [52].

En el artículo enumerado anteriormente, mencionan que el equipamiento Profinet carece de cualquier función de seguridad nativa. Las medidas incorporadas en el protocolo se concentran en la mejora de la disponibilidad del sistema y la fiabilidad operacional, conjuntamente con la robustez del equipamiento cuándo afronta volúmenes altos de tráfico en ciertos puntos. En el trabajo "Enfoque de seguridad en Sistemas de Control Industrial" [18], también se menciona que al igual que con otros protocolos originalmente creados la comunicación a través de Fieldbus, la ausencia de autenticación y la falta de seguridad en el protocolo requieren aislamiento del resto de la red. A la hora de trabajar con este protocolo, sería bueno el uso de métodos de tecnología de la información para autenticar componentes en la red, conjuntamente con mecanismos de control de acceso dentro de ésta.

EtherCAT: es un sistema Ethernet Industrial que se basa en el principio maestro-esclavo y aplica un procedimiento para el tratamiento de los datos de proceso cíclicos en los dispositivos de campo (esclavos). Para la comunicación, se crea una imagen de proceso en el maestro, que representa el estado de varias entradas y salidas del sistema general que comprende varios esclavos. Para cambiar el estado de las salidas específicas de un esclavo, la parte correspondiente de la imagen del proceso junto con una orden de cambio, tienen que ser enviados. Los esclavos por si mismos pueden enviar partes de la imagen de proceso al maestro durante el intercambio cíclico de datos para actualizar la información de estado de sus entradas [53].

Como EtherCAT es un protocolo derivado de Ethernet es susceptible a todas sus vulnerabilidades, y por ende presenta un gran riesgo de ataques de negación de servicio. Los servicios EtherCAT fácilmente pueden ser modificados a través de la inserción de paquetes de Ethernet en la red, de tal manera que interfieren con la sincronización y por tanto son vulnerables a la falsificación a consecuencia de la falta de autenticación, así que se aconseja separar la red EtherCAT de cualquier otro sistema Ethernet. Se aconseja en el mismo trabajo mencionado anteriormente, llevar a cabo un monitoreo de la red para asegurar su integridad, chequeando que el tráfico EtherCAT se origina exclusivamente en dispositivos que están explícitamente

autorizados. Esto sería una buena práctica ya que el acceso a los dispositivos de campo debe ser controlado sólo por personal autorizado y con conocimiento previo.
En resumen, queda claro que los protocolos de redes industriales no están totalmente preparados para los niveles de ciberseguridad requeridos por los supervisorios industriales integrados modernos, de aquí la necesidad de un soporte seguro para estos sistemas.

1.6 Clasificación de las amenazas a la seguridad de los sistemas supervisorios como principal objetivo dentro de los Sistemas de Control Industrial

En el artículo "Seguridad en Sistemas SCADA" [54], se clasifican algunas de las amenazas a la seguridad que presentan los sistemas supervisorios como:

- Malware: incluye todo tipo de virus, troyanos, spywares y gusanos. Estos ataques no necesariamente son dirigidos a los SCADA, pero si un computador de control es afectado por alguna de estas amenazas, bien podría afectar al sistema entero.
- Ataques internos: este puede ser un tipo de amenaza frecuente, ya sea intencional o involuntario (errores operacionales). Cuando ocurre una de estas amenazas suele ser bastante crítica, pues al estar dentro de la red operacional se tiene acceso directo a los equipos críticos del sistema.
- Hackers: esta es una amenaza creciente ya que existen herramientas automatizadas para perpetrar estos ataques.

Algunos autores como Juan Anabalón y Eric Donders, en su artículo "Seguridad en sistemas SCADA" [54] argumentan que en los sistemas supervisorios, las vulnerabilidades pueden ser explotadas a través de distintos vectores de ataques comunes como:

- Puertas traseras y agujeros en el perímetro de la red.
- Vulnerabilidades en protocolos comunes.
- Ataques a dispositivos de campo, remotos (por ejemplo, PLCs).
- Ataques a bases de datos.
- Secuestros de sesiones.

Desde el punto de vista de un ingeniero de control, posibles ataques pueden agruparse en las siguientes categorías:

- Manipulación de datos de entrada introducidos a través de sensores comprometidos y/o enlaces de red entre sensores y controladores.
- Manipulación de datos de salida de sensores y controladores.
- Controlar archivos históricos.
- Ataques de Denegación de Servicios (DoS, *Denial of Service*).

Se han analizado que los problemas de seguridad en sistemas supervisorios más comunes incluyen una inadecuada o la falta de políticas de seguridad organizacional, falta de segmentación de redes, ausencia de *logs* de acceso, acceso a internet desde estaciones de trabajo de operadores, software no relacionado en las estaciones de trabajo y falta de revisión en los sistemas de control por parte de los fabricantes. Por lo anterior, se proponen a continuación algunas medidas preventivas para los sistemas supervisorios.

CONCLUSIONES PARCIALES DEL CAPÍTULO

En este capítulo se han analizado y estudiado las características y tecnologías de los ICS integrados modernos, que necesitan fortalezas que garanticen su ascenso a los nuevos retos de integración de las automatizaciones industriales desde el control local, la supervisión remota, la planificación y control de la producción, el control de la calidad, la implementación del mantenimiento predictivo y hasta la gestión de negocios de la empresa. El estudio ha demostrado que las estructuras y protocolos de redes tradicionales no son capaces de garantizar esta integración y que requieren nuevas estructuras y protocolos para evitar las afectaciones que se han comentado al final del capítulo y la necesidad de seguir las recomendaciones.

Todo esto nos permite diseñar una estructura de red y realizar recomendaciones de diseño de los supervisorios industriales integrados modernos, que permitan elevar los niveles de ciberseguridad que requieren nuestras industrias, lo cual se verá en detalle en el próximo capítulo.

CAPÍTULO 2. PROPUESTA DE DISEÑO DE SEGURIDAD PARA SUPERVISIÓN INDUSTRIAL INTEGRADA

Con el desarrollo y amplio uso de las Redes de Comunicaciones Industriales, como soporte de la integracion SCI-Gestión Empresarial en la industria moderna, se necesita crear una política de seguridad que prevenga posibles ataques informáticos. Las políticas tradicionales de seguridad de las Tecnologías de la Información se centran principalmente en la confidencialidad de los datos, dejando la disponibilidad de la red como la prioridad de seguridad más baja. Por el contrario los SCI integrados modernos, especialmente aquellos que se consideran infraestructura crítica, deben mantener un alto nivel de disponibilidad del sistema por muchas razones, incluyendo la seguridad económica, ambiental, humana y nacional.

En el presente capítulo se realiza la propuesta de diseño y simulación de una red Desmilitarizada utilizando cortafuegos, que permita el intercambio de los datos de una red industrial (red interna) hacia redes externas (empresarial o Internet) y viceversa, brindando seguridad a los datos y evitando así la violación del Sistema de Control. Se propone la utilización de este soporte de red industrial para crear sistemas supervisorios integrados más seguros, que permitan el intercambio de datos, acciones y tomas de decisiones que garanticen la eficiencia, productividad y competitividad de las empresas modernas.

2. METODOLOGIA DE CYBERSEGURIDAD INDUSTRIAL

Una red de control industrial integrada, presenta infraestructuras atractivas a sujetos amenazadores o piratas informáticos, cuya finalidad es adentrarse en el sistema para recopilar diversa información, como pueden ser: diseño de la instalación, umbrales críticos de trabajo, ajustes de dispositivos, tomas de decisiones empresariales, entre otros. Estas acciones de sabotaje pueden provocar, entre otros factores, la interrupción de los servicios, el desenlace de situaciones peligrosas e incluso letales.

En la industria, la red general de comunicaciones está integrada por la red empresarial y por la red de control. La red empresarial desarrolla operaciones de supervisión del sistema y de los usuarios que a ella acceden; además, requiere de procedimientos de autenticación rigurosos para acceder a la información de las bases de datos y así

conocer las alarmas generadas, realizar estudios de tendencia, comportamiento de variables, entre otras ventajas [55].En la industria moderna se integran la red industrial y la empresarial, para que el procesamiento de los datos de los procesos industriales permita respaldar la toma de decisiones inteligente [10], y para crear las bases de la Industria 4.0 [56], [57], [58].

La red de control desarrolla actividades de configuración, mantenimiento y operación de sensores y actuadores, lectura de variables, monitoreo del proceso, etcétera. La comunicación entre los diversos dispositivos que conforman la red utiliza diferentes protocolos como HART, PROFIBUS, FOUNDATION FIELDBUS, MODBUS/TCP [59]; y en ocasiones soportan otras tecnologías como líneas telefónicas, satélites, microondas, fibra óptica, entre otras [60], [61], [62]. La incorporación de equipos comerciales e informáticos ha introducido riesgos asociados al funcionamiento de los sistemas de comunicaciones industriales, unido a la necesidad de realizar acciones del sistema integrado que contribuyen a la toma de decisiones de la gerencia empresarial desde la automática local.

En una red de control interactúan protocolos de automatización industrial basados en TCP/IP para el control remoto, o basados en el Protocolo Industrial Común (CIP), bajo la organización ODVA [30], como pueden ser: Ethernet/IP, DeviceNet, CompoNet y ControlNet. No obstante, la mayoría de estos protocolos presentan vulnerabilidades en la protección y seguridad de los datos [63], [64]. Existen métodos para evitar algunas de estas vulnerabilidades como puede ser el uso de las redes Desmilitarizadas.

Las redes DMZ son redes locales ubicadas entre las redes internas y externas de una organización, que permite implementar políticas de seguridad contra ataques informáticos. Su principal ventaja radica en que la red DMZ permite una conexión directa de la red interna y externa hacia ella, mientras que desde la DMZ sólo se permiten las comunicaciones a la red externa, es decir, los equipos locales (*hosts*) en la DMZ no se pueden conectar con la red interna, permitiendo que los *hosts* en la DMZ puedan brindar servicios a la red externa, a la vez que protegen la interna en caso de que intrusos comprometan la seguridad de los *host* en la zona DMZ [65].

MEDIDAS PREVENTIVAS CONTRA VULNERABILIDADES EN LOS SISTEMAS

SUPERVISORIOS COMO PRINCIPAL OBJETIVO DENTRO DE LOS SISTEMAS DE CONTROL INDUSTRIAL

El principal riesgo de una falla en los sistemas supervisorios dentro de los ICS, es el daño en la infraestructura empresarial como operaciones detenidas, daños costosos y tiempo de recuperación elevado. En muchos casos las vulnerabilidades están asociadas con la antigüedad de los equipos, sistemas operativos viejos y que además no tienen los parches de seguridad.

Algunas vulnerabilidades comunes en relación a incidentes en:

- Permisos, privilegios y control de acceso: son los permisos y controles de acceso indebidos de los usuarios. El usuario sólo debe acceder a lo estrictamente necesario.
- Gestión de credenciales-identidades: son las contraseñas débiles (pocos caracteres y sólo minúsculas) y las políticas de contraseñas no adecuadas que no obliguen a cambiar de contraseña o que permitan introducir sin penalización (poner límite de reintentos) contraseñas hasta craquear por fuerza bruta.
- Configuración y mantenimiento de la seguridad del sistema de control industrial: son la gestión de parches y actualizaciones inadecuada o no existente.
- Debilidad del diseño de red: son la carencia de segmentación de red y zonas de cuarentena, no existencia de zonas funcionales DMZ (Zonas Desmilitarizadas), carencia de elementos de protección como firewalls/UTM.
- Auditoría, responsabilidad y monitorización de eventos: son la carencia de logging, la implantación de prácticas de logging inadecuadas/pobres, el no entendimiento sobre la arquitectura de red que deja sin monitorización zonas vulnerables.

Algunas medidas preventivas útiles son: comunicar a través de mecanismos de seguridad las redes de supervisión con las redes empresariales que a su vez están conectadas a Internet, instalar los últimos parches de seguridad para software, sistemas operativos y actualizar las herramientas de seguridad, cifrar los datos, configurar profesionalmente firewalls (utilizar IDS/IPS/IMS/AV para reconfiguración automática), realizar exploraciones de virus malware, configurar adecuadamente permisos y autenticación de usuarios, sólo permitir contraseñas robustas, utilizar

tarjetas inteligentes, limitar la disponibilidad de información técnica sobre el sistema supervisorio, proteger los sistemas operativos eliminando cuentas por defecto y cerrar servicios/puertos no utilizados, analizar y eliminar puertas traseras del sistema a nivel de software, firmware y hardware, eliminar servicios que utilizan canales subliminares. Algunos métodos de detección (capacidad para reconocer la ocurrencia de un incidente de seguridad) útiles son [54]:

- Recoger en una BD histórica los datos de campo.
- Implantar mecanismos de alerta de seguridad hardware-firmware y software.
- Utilizar registros de auditoría y adquisición de *logs* en software de aplicaciones.
- Analizar los ficheros de *log* de sistemas operativos.

Algunos métodos de recuperación (capacidad para restaurar el sistema comprometido a su estado operacional) útiles son [54]:

- Utilizar hardware redundante tolerante a fallos.
- Emplear herramientas para valorar el impacto de pérdida o desconexión de uno o más componentes del sistema.
- Aplicar procedimientos de *backup* del sistema probados y no ambiguos.
- Implantar procedimientos para revisar y aprender de incidentes de seguridad existentes.

Algunas recomendaciones y contramedidas útiles para mejorar la seguridad de las redes de supervisión son [54]:

- Monitorizar no sólo las conexiones de entrada sino también las de salida. Implantar herramientas de sniffers [66].
- Implantar fuertes medidas de seguridad a usuarios y activos de alto valor por ejemplo utilizar autenticación mutua multi-factor (lo que uno: sabe, tiene, es, se comporta, está geográficamente o lugar GPS, el cuándo o instante de tiempo, etc.).
- Desplegar sistemas multi-funcionales de defensa en profundidad UTM (Unified Threats Management), IDS/IPS [67], anti-malware, VPN, *router*, filtrado URL, gestión identidades y firewall con estados, con firmas que se actualicen para nuevas amenazas y mecanismos heurísticos para amenazas del día cero.
- Protegerse contra ataques DoS/DDoS basados en IP.

- Protegerse contra la indisponibilidad utilizando redundancias, virtualización, backups, reubicación, hot-site y coldsite, etc.
- Segregación de red. Se deben utilizar mecanismos de seguridad para integrar los sistemas de supervisión a las redes LAN corporativas-intranets, redes WLANs-WiFi o incluso directa e indirectamente de Internet.
- Utilizar sistemas operativos basados en arquitectura micro-kernel cuyos servicios son recortados al máximo impidiendo el ataque a servicios superfluos: limita el número de líneas de código e implícitamente el número de fallos, lo cual potencia una mayor fiabilidad.
- Mejorar la protección de las redes de sensores o implantar nuevas tecnologías más robustas para redes de sensores: las redes de sensores permiten monitorizar la instrumentación de la factoría, determinar los niveles de contaminación, etc. y estas constan de cientos o miles de nodos sensor. Cada nodo representa un punto potencial de ataque y securizar cada uno, puede no ser sencillo y practicable. Los detectores de sensor ofrecen defensa contra ataques y tienen la capacidad para diferenciar entre la transmisión de redes autorizadas y no autorizadas, así como otros dispositivos.
- Identificar todas las conexiones a las redes SCADA: desconectar las conexiones innecesarias y evaluar la robustez en seguridad de las que queden. Considerar conexiones con socios corporativos, fabricantes, agencias de cumplimiento, redes inalámbricas, redes corporativas, módems, etc.
- Eliminar o inhabilitar los servicios no necesarios: es necesario analizar la necesidad de los servicios de Internet, mantenimiento remoto (tanto software como hardware) y suprimir o evaluar puertos de entrada como USB, DVD, etc.
- No utilizar protocolos propietarios para proteger la red SCADA ni configuraciones por defecto que salen de fábrica: rastrear posibles puertas traseras o interfaces secretos que dejan algunos fabricantes.
- Implantar las características de seguridad personalizadas proporcionadas por los fabricantes de dispositivos y sistemas.
- Establecer fuertes controles contra cualquier medio utilizado como puerta trasera en la red SCADA.

- Implantar sistemas de detección/prevención/gestión de intrusiones y establecer una monitorización y gestión de incidentes continua 7x24 horas.
- Realizar auditorías técnicas de dispositivos y redes SCADA, así como de otras redes conectadas para identificar problemas de seguridad.
- Analizar y valorar la seguridad física de todos los sitios remotos conectados a la red SCADA para evaluar su nivel de seguridad. Así mismo realizar tests de penetración/intrusión, para identificar y evaluar posibles escenarios de ataque y vulnerabilidades.
- Definir claramente los roles de seguridad, las responsabilidades y autoridades de gestores, administradores del sistema y usuarios.
- Documentar la arquitectura de red e identificar los sistemas que realizan funciones críticas o contienen información sensible que requiera de unos niveles de protección adicionales.
- Identificar claramente los requisitos de seguridad para minimizar las amenazas desde dentro: limitar los privilegios de red, aplicar acuerdos de usuario, notificaciones y avisos/warnings.
- Establecer backup del sistema y planes de recuperación de desastres frente a emergencias: utilización de copias de seguridad y hardware de respaldo cold-site/hot-site con procesadores y aplicaciones duplicadas.
- Establecer políticas y realizar planes de formación para minimizar que el personal de la organización revele inadvertidamente información sensible relacionada con el diseño, operaciones o controles de seguridad del sistema SCADA.
- Establecer un proceso continuo de gestión de la seguridad consistente en un ciclo cerrado formado por: (i) prevenir, disuadir y estar a la defensiva. (ii) detectar y monitorizar ataques. (iii) actuar según planes-procedimientos-técnicas para detener-bloquear ataques. (iv) recuperarse de forma conocida y probada. (v) documentar, informar y aprender de los ataques sufridos y vuelta al comienzo.

2.1 ¿QUÉ ES UNA RED DMZ?

Una red DMZ es una red local perimetral que se ubica entre la red interna de una organización y una o varias redes externas, generalmente una red de empresa e Internet. El objetivo de una DMZ es que las conexiones desde la red interna (en nuestro caso la red de control o red industrial) a la DMZ, y desde las redes externas (red empresarial e Internet) a la DMZ, estén permitidas, mientras que en general las conexiones desde la DMZ solamente se permitan a las redes externas; de este modo, se impide generalmente que los equipos de la DMZ se conecten directamente con la red interna [68].

En cualquier empresa, es habitual ofrecer distintos servicios accesibles hacia y desde Internet, ya sea para empleados o clientes, tales como una página web, correo electrónico o simplemente un servidor de ficheros. Estos servicios pueden subcontratarse a una empresa especializada o se pueden afrontar de forma interna, desde la organización, mediante recursos propios. La principal ventaja de abordarlo de forma interna será ostentar el control de su propia información, sin exponerla a terceros, lo que redundará en preservar la privacidad. Otra ventaja es que el servidor puede diseñarse a medida en función de las necesidades de la propia empresa . Un ejemplo de red local usando DMZ puede observarse en la Figura 2.1:

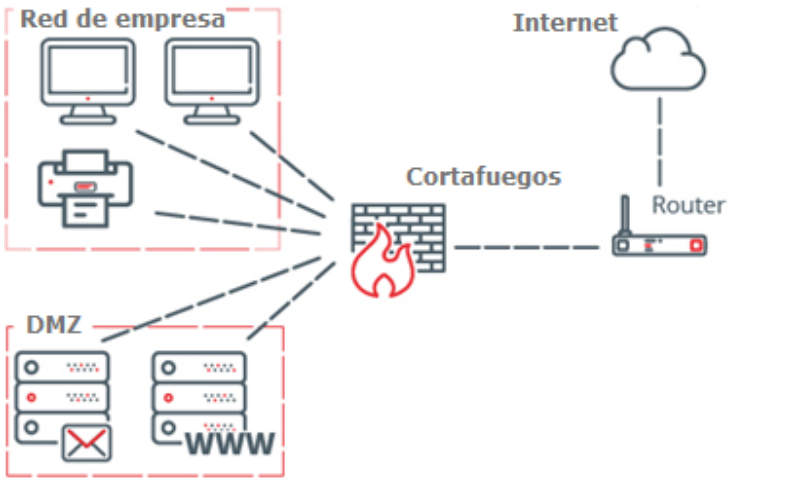

Figura 2.1: Ubicación de red DMZ dentro de una empresa

2.1.1 Riesgos de utilizar servidores propios

Cuando se permite el acceso desde o hacia Internet a una página web, servidor de correo, servidor de ficheros, red privada virtual, red industrial, etc., aumenta el riesgo

de sufrir un incidente de seguridad [69]. Si un ciberdelincuente consigue vulnerar la seguridad de uno de estos servidores, podría comprometer el resto de dispositivos conectados a la red, incluso aquellos que no son accesibles desde Internet. Un acceso no deseado podría derivar en comunicaciones espiadas, ficheros robados, caídas de servicio, etc.

2.1.2 Configuraciones y características de una DMZ

Una zona DMZ hace referencia a una red de dispositivos con un rango de direcciones IP privadas que sirve como franja de seguridad entre dos o más redes, separándolas mediante estrictas reglas de acceso. Aunque físicamente los servidores dentro de una DMZ se encuentran en la misma organización, no están conectados directamente con los equipos de las redes externas y la red interna. La estructura del nivel de protección más alto consiste en el uso de cortafuegos, que separan la zona desmilitarizada de las redes externas, interna e Internet. Hay muchas formas diferentes de diseñar una red DMZ [68].

Características de una red DMZ.

- El tráfico de la red externa a la DMZ está autorizado.
- El tráfico de la red externa a la red interna está prohibido.
- El tráfico de la red interna a la DMZ y a la red externa está autorizado.
- El tráfico de la DMZ a la red interna está prohibido.
- El tráfico de la DMZ a la red externa está denegado.

De esta manera las redes DMZ poseen un nivel de seguridad intermedio, ya que no son suficiente para almacenar datos imprescindibles de una red industrial. Para ello es necesario un diseño más seguro que consiste en la integración de una red DMZ y el uso de cortafuegos, ayudando a prevenir el acceso desde las redes externas a la interna, también llamado cortafuegos de subred monitorizada. Se pueden usar dos cortafuegos para crear una red DMZ, el primero, llamado "front-end", que permite el tráfico únicamente de la red externa a la red DMZ y el segundo, llamado "back-end", que permite el tráfico únicamente desde la red DMZ a la red interna [70].

Existen varias configuraciones para implementar una red DMZ usando cortafuegos, algunas de estas pueden ser [71]:

- DMZ con 1 cortafuegos de tres patas.

- DMZ con 2 cortafuegos de cinco patas.
- DMZ con 3 cortafuegos de múltiples patas.

2.1.3 Ventajas y Desventajas del uso de DMZ y cortafuegos

Las arquitecturas de seguridad perimetral con el empleo de DMZ, engloban diferentes esquemas en los que es posible configurar varias soluciones para cumplir con distintos niveles de seguridad requeridos. Para la implementación de alguna arquitectura, se requiere evaluar las necesidades de la organización, analizando su operación ininterrumpida, sus recursos y los servicios que se brindan, además de su distribución geográfica [68].

Algunos sistemas que hay que tomar en cuenta son: Intranets e Internet, sitios de comercio electrónico, conmutadores, video vigilancia IP, Planificación de Recursos Empresariales (ERP, *Enterprise Resource Planning*), Gestión de Relaciones con Clientes (CRM, *Customer Relationship Management*), bases de datos, entre otros. Una vez identificados todos estos puntos se debe de considerar también a qué usuarios se les brindaran los servicios, es decir, si son usuarios de la red interna, si son usuarios en Internet, o si son usuarios de la red empresarial. Con estos datos es posible diseñar una arquitectura adecuada para la DMZ, y en este sentido, incluso combinarlas, para maximizar sus ventajas y disminuir sus inconvenientes.

Algunas de las ventajas y desventajas de cada tipo de arquitectura de DMZ utilizando cortafuegos son:

Ventajas:

- Administración simple o compleja para mayor seguridad.
- Publicación de servicios de una manera más segura.
- Estructura recomendada para puntos remotos donde se alojan sólo algunos servicios críticos, sin acceso directo a una red de usuarios.
- Mejor política de accesos y reglas de filtrado.
- Independencia total de redes y equipamiento.

Desventajas:

- Menor o mayor complejidad en la administración del cortafuegos.
- Si se compromete el cortafuegos, toda la red se puede ver afectada según la distribución y confieguración de los cortafuegos.

- Costos más elevados según su complejidad.

2.1.4 SEGURIDAD EN DMZ

Existen por lo general, varios consejos para ayudar a garantizar que una DMZ sea segura [68]:

1. Preservar el aislamiento tanto como sea posible: consiste en mantener las reglas que permiten el tráfico entre la DMZ y una red interna lo más estrictas posible. Con frecuencia, los administradores que buscan solucionar un problema crean una regla que permite el acceso completo entre un sistema DMZ y un servidor *back-end* en la red interna (o toda la red interna); esto frustra el propósito de la DMZ y la fusiona efectivamente con la red interna. En su lugar, es necesario crear reglas de cortafuegos que permitan la comunicación solo entre servidores específicos en puertos puntuales necesarios para cumplir con los requisitos comerciales.
2. Practicar una buena gestión de la vulnerabilidad: los servidores DMZ están expuestos al mundo, así que es necesario asumir medidas adicionales para asegurar de que estén completamente actualizados, a fin de hacer frente a las últimas vulnerabilidades de seguridad. Se recomienda la automatización de alertas de vulnerabilidades que comprometan el funcionamiento de la DMZ, considerando aplicar parches a los sistemas DMZ con mucha más frecuencia que a los sistemas protegidos, para reducir la ventana de vulnerabilidad entre el momento en que se lanza un parche y su aplicación en los servidores DMZ.
3. Utilizar defensas de la capa de aplicación para los servicios expuestos: es necesario elegir un cortafuegos de red que tenga una sólida protección en la capa de aplicación, en lugar de solo un filtro de puerto. Un cortafuegos debe tener la capacidad de inspeccionar el contenido del tráfico y bloquear solicitudes maliciosas.
4. Monitorear: la DMZ debe ser uno de los principales focos de los esfuerzos de monitoreo de redes de una organización. En este sentido, utilizar Sistemas de Detección de Intrusos (IDS, *Intrusion Detection System*), Sistemas de Gestión de Eventos e Incidentes de Seguridad (SIEM, *Security Information and Event Managent*), supervisión de registros y otras herramientas para mantenerse alerta a

las señales de un ataque, debe formar parte del buen hacer de las políticas de la organización.

De forma general, los sistemas en la DMZ están en el extremo puntiagudo de la lanza de seguridad de la red, y sujetos siempre a ataques externos a diario. Por esta razón, es importante invertir esfuerzos en garantizar rigurosamente de que se encuentren entre los servidores más seguros de una organización.

2.2 ¿Qué es un cortafuegos?

Los cortafuegos son unos dispositivos de seguridad cuya función principal es la de filtrar el tráfico de red entrante y saliente por medio de una serie de reglas, que permitirán su paso o lo rechazarán. Una vez que una comunicación llega al cortafuegos, por ejemplo una petición al servidor web de una empresa, esta podrá ser aceptada o rechazada, según se hayan configurado las reglas [69]. Este tipo de herramientas pueden ser tanto dispositivos específicos dedicados, o software, como el integrado por defecto en el sistema operativo Windows. Los dispositivos dedicados, por lo general, cuentan con más capacidades de procesamiento que los basados en software, ya que se han diseñado específicamente para esa tarea, aunque por el contrario, su coste económico es superior. En la Figura 2.2 se muestra la red de una empresa que cuenta con un cortafuegos.

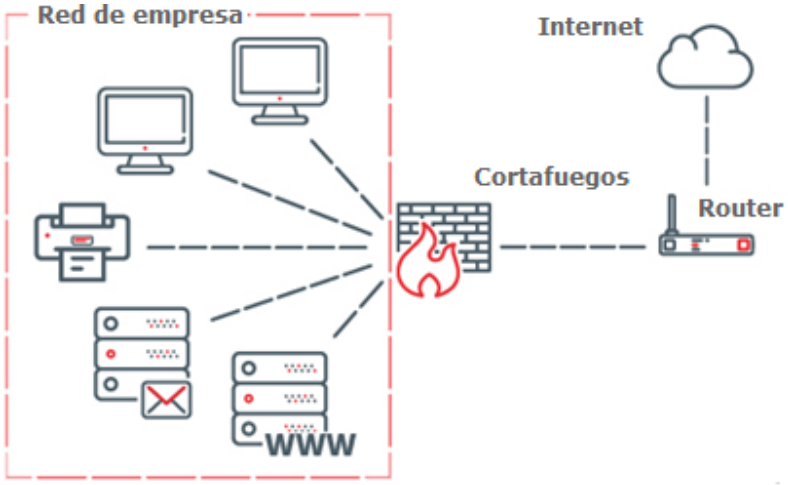

Figura 2.2: Ubicación de cortafuegos dentro de una empresa.

Por lo general, una DMZ permite las conexiones procedentes tanto de Internet, como de una red local de una empresa donde están los equipos de los trabajadores y una

red de control; pero las conexiones que van desde la DMZ a una red de empresa o red de control no están permitidas. Esto se debe a que los servidores que son accesibles desde Internet son más susceptibles a sufrir un ataque que pueda comprometer su seguridad. Si un ciberdelincuente comprometiera un servidor de la zona desmilitarizada, tendría muchos más complicado acceder a la red local de la organización y de control, ya que las conexiones procedentes de la DMZ se encuentran bloqueadas [69]. Ver figura 2.3:

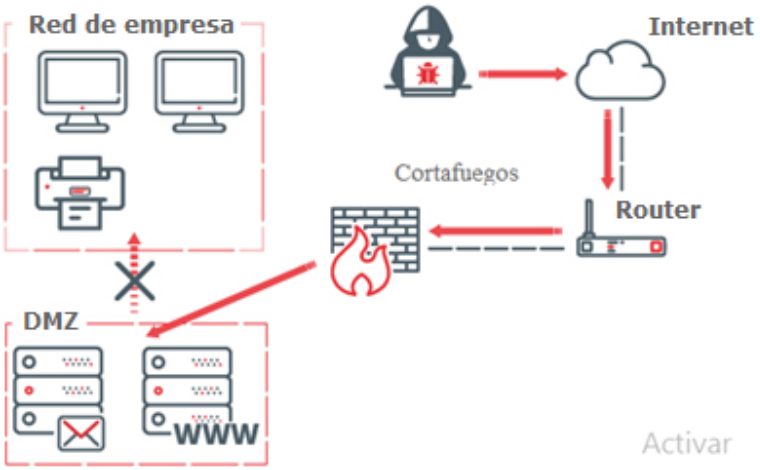

Figura 2.3: Conexiones procedentes de la DMZ a una empresa

A pesar de que el uso de DMZ con cortafuegos menciona que no se debe permitir que desde la red de control hacia la DMZ exista flujo de datos, en la industria 4.4 se aboga porque exista una retroalimentación desde la red de control hacia la empresa [57]. En este trabajo solo se propone un diseño utilizando DMZ y cortafuegos como primera barrera de seguridad, a la hora de integrar la red de control con la red empresarial de una industria cubana. La manera de permitir el flujo entre la red de control y la DMZ de manera segura para cumplir con las exigencias de la industria 4.0 se encuentra en desarrollo.

2.2.1 Configuración básica de un cortafuegos con DMZ

Como hemos analizado para configurar una zona desmilitarizada en la red de una organización, es necesario contar con cortafuegos. Este dispositivo, será el encargado de segmentar la red y permitir o denegar las conexiones. En la siguiente tabla, se muestra el tipo de conexiones recomendables que permitiría o denegaría el cortafuegos dependiendo su origen y destino. Ver figura 2.4:

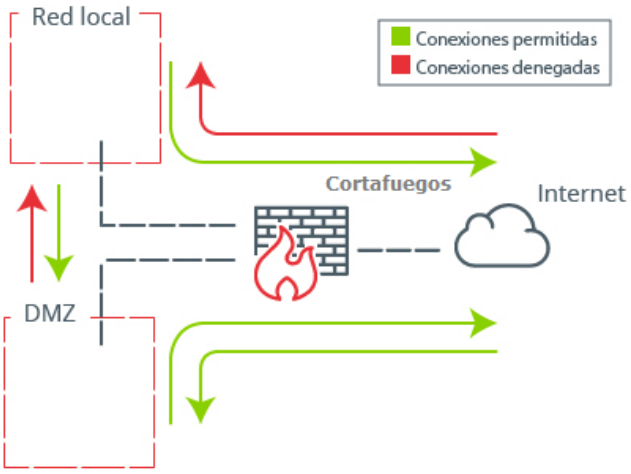

Figura 2.4: Muestra gráfica del tráfico permitido y denegado por el cortafuegos

No obstante, si se quiere aumentar aún más la seguridad de la red interna frente a un ataque proveniente de la DMZ, se pueden ubicar dos o más cortafuegos.

2.2.2 Generalidades de un cortafuegos

Existen tres parámetros a tener en cuenta en cuanto a la configuración de cortafuegos. El primero y más importante tiene en cuenta la política de seguridad de la empresa donde se va a montar, el segundo analiza el nivel de monitorización que se desea y el tercero se basa en la parte económica. Una vez que se haya decidido cual configuración de red DMZ usando cortafuegos se va a implementar, se debe elegir qué elementos físicos utilizar.

Los elementos para los cuales se pueden implementar mecanismos de protección son el filtrado de paquetes, el proxy de aplicación, y la monitorización y detección de actividad sospechosa [72]. Conceptualmente existen dos tipos de cortafuegos que brindan mayor robustez y seguridad, el de nivel de red llamado cortafuegos de filtrado de paquetes y el de nivel de aplicación [73], que se explican a continuación.

2.2.2.1 Cortafuegos de filtrado de paquetes

El término en inglés por el que se los conoce es Packet Filter Firewalls. Analizan el tráfico de la red fundamentalmente en la capa 3 del modelo OSI, teniendo en cuenta a veces algunas características del tráfico generado en las capas 2 y/o 4 y algunas características físicas propias de la capa 1. Los elementos de decisión con que cuentan a la hora de decidir si un paquete es válido o no son los siguientes:

- La dirección de origen desde donde, supuestamente, viene el paquete (capa 3).

- La dirección del *host* de destino del paquete (capa 3).
- El protocolo específico que está siendo usado para la comunicación, frecuentemente Ethernet o IP, aunque existen cortafuegos capaces de desenvolverse con otros protocolos como IPX, NetBios, etc (capas 2 y 3).
- El tipo de tráfico: TCP, UDP o ICMP (capas 3 y 4).
- Los puertos de origen y destino de la sesión (capa 4).
- El interface físico del cortafuegos a través del que el paquete llega y por el que habría que darle salida (capa 1), en dispositivos con 3 o más interfaces de red.

Con todas o algunas de estas características se forman dos listas de reglas: las permitidas y denegadas. La forma en que un paquete recibido se procesa difiere según el modelo, el fabricante, o el modo de actuación configurado, y define en gran medida la permisividad del cortafuegos. Otras veces existe una única lista de reglas y el paquete es procesado, según la primera regla que encontramos. Otros cortafuegos usan la última regla que encuentran como acción a efectuar. Por último, también encontramos diferencias en cuanto a qué hacer cuando no se encuentra ninguna regla válida: algunos productos aceptan el paquete y otros lo rechazan.

Las principales bondades de este tipo de cortafuegos están en su rapidez, transparencia y flexibilidad. Proporcionan un alto rendimiento y escalabilidad y muy bajo coste, y son muy útiles para bloquear la mayoría de los ataques de DoS. Otra de sus ventajas es la protección de información privada, donde define que usuarios de la red y que información va a obtener cada uno de ellos. En cuanto a la optimización de acceso: define de manera directa los protocolos a utilizarse, y para la protección de intrusos: protege de intrusos externos restringiendo los accesos a la red.

Su principal inconveniente es su dificultad a la hora de configurarlos y mantenerlos. No pueden prevenir ataques que exploten vulnerabilidades específicas de determinadas aplicaciones, puesto que no examinan las capas altas del modelo OSI. No protege de ataques que no pasen a través del firewall. No protege de la copia de datos importantes si se ha obtenido acceso a ellos. No protege de ataques de ingeniería social. No son efectivos como medida única de seguridad, pero sí muy prácticos como primera barrera, en la que se bloquean ataques y se filtran protocolos no deseados.

2.2.2.2 CORTAFUEGOS DE NIVEL DE APLICACIÓN

Este cortafuegos, evalúa los paquetes realizando una validación en la capa de aplicación (capa 7) antes de permitir una conexión. Adicionalmente, suelen prestar servicios de autenticación de usuarios y de Proxy.

Las principales ventajas de este tipo de cortafuegos son sus detallados registros de tráfico (ya que pueden examinar la totalidad del paquete de datos), el valor añadido que supone tener un servicio de autenticación de cara a dar seguridad a nuestra red, y la casi nula vulnerabilidad que presentan ante ataques de suplantación (spoofing), el aislamiento que realizan de nuestra red, la seguridad que proporciona la comprensión a alto nivel de los protocolos que inspeccionan y los servicios añadidos, como caché y filtro de URL's, que prácticamente todos implementan.

Entre los inconvenientes están sus menores prestaciones en cuanto a velocidad de inspección se refiere, la imposibilidad de ejecutar muchos otros servicios puesto que escucha en los mismos puertos, la imposibilidad de inspeccionar protocolos como UDP, RPC y otros servicios comunes y lo vulnerables que resultan ante ataques directos al sistema operativo sobre el que se suelen ejecutar.

2.2.3 Topología de los cortafuegos

- Dual-Homed Host: cortafuegos que se instala en un *host* con dos tarjetas de red y actúa como *router* entre las dos redes [74].
- Screened Host: cortafuegos que se combina con un *host* bastión situado en la red externa y un *host* bastión situado en la red interna [74].
- Screened Subnet (DMZ): cortafuegos que se emplea en una red Desmilitarizada donde se utilizan dos *routers*, uno en la red externa y otro en la interna, y entre ellos se incluye el *host* bastión [74].

Los sistemas Dual-Homed Host y Screened Host por separado, tienen la desventaja de ser no transparentes para el usuario, y a veces se debe instalar algún tipo de aplicación especializada para lograr la comunicación. Se suma a esto que generalmente son más lentos porque deben revisar todo el tráfico de la red. Así mismo pueden ser complicados de configurar y comprobar, lo que puede dar lugar paradójicamente a agujeros de seguridad en toda la red. En cambio, si se combinan, se encuentran bien configurados y administrados pueden brindar un alto grado de protección y ciertas ventajas como:

- Ocultamiento de la información: los sistemas externos no deben conocer el nombre de los sistemas internos. El *gateway* de aplicaciones es el único autorizado a conectarse con el exterior y el encargado de bloquear la información no solicitada o sospechosa.
- Registro de actividades y autenticación robusta: el *gateway* requiere de autenticación cuando se realiza un pedido de datos externos. El registro de actividades se realiza en base a estas solicitudes.
- Reglas de filtrado menos complejas: las reglas del filtrado de los paquetes por parte del *router* serán menos compleja, dado a que él sólo debe atender las solicitudes del *gateway*.

2.3 METODOLOGÍA DE DISEÑO DE UNA RED DMZ UTILIZANDO CORTAFUEGOS PARA INTEGRAR UNA RED INDUSTRIAL A UNA RED EMPRESARIAL

La automatización integrada de procesos es un sistema de automatización soportado en redes de comunicación que permite integrar las funciones de la automática local, la supervisión de procesos y el gerenciamiento de la empresa para lograr eficiencia de la sincronización de todos ellos. En el nivel de automática local se incluyen las funciones de control secuencial, control de procesos y protecciones automáticas hasta sistemas inteligentes de auto-diagnóstico, tolerancia a fallos, tomas de decisiones sobre adaptabilidad y optimización de parámetros del proceso.

La supervisión de procesos constituye el eslabón central integrando las funciones de operación remota, tratamiento de alarmas, tendencias y reportes, integradas a la supervisión operacional, al mantenimiento del sistema, a las protecciones automáticas y a la seguridad del proceso. Es por esto que se considera juega un papel fundamental en cualquier tipo de automatización integrada, porque establece el enlace de las dos partes fundamentales.

La gerencia empresarial se ocupa de la gestión inteligente para optimizar su funcionamiento, reducir consumo energético, evitar afectaciones al medio ambiente, garantizar productividad, eficiencia y rentabilidad con altos niveles de calidad en productos y/o servicios del sistema automatizado. Integrar las funciones de la automática local, la supervisión de procesos y el gerenciamiento de la empresa en la

automatización moderna es fundamental, para poder lograr esa competitividad de las futuras empresas orientadas a integrarse en las Smart Grids y Smart Cities.

En nuestro país en general, la red industrial se encuentra aislada de las redes externas de una organización (internet y empresarial), por lo que los servidores ubicados en la red industrial no son accesibles desde ningún cliente (PC) ubicado en la redes externas, o simplemente son accesibles sin mecanismos de seguridad. Esto da lugar a que no se tenga acceso a los datos involucrados en los procesos, o se generen vulnerabilidades en cuanto a seguridad de los datos, ya que se pudiera recibir un ataque informático en cualquier momento y desde cualquier cliente. Para lograr la integración entre la red interna de una empresa y las redes externas, se realizaron investigaciones con el objetivo de encontrar mecanismos de seguridad informática que se puedan adaptar a las condiciones de la industria, donde se analizaron diversas opciones de protección. Entre estas opciones, hay trabajos donde se propone el uso de redes DMZ y cortafuegos [70], [75], [76], [77].

Es importante destacar que aunque el objetivo de esta investigación es integrar la red interna con las redes externas de una empresa, para poder aplicar mecanismos de seguridad, se hace necesario dividir la red de la organización en tres redes (ver figura 2.5): dos redes externas (internet y empresarial) y una red interna (industrial o de control, con datos y variables de proceso). Los sistemas de división dan a las empresas la capacidad de priorizar la seguridad de las redes que contienen datos altamente sensibles sobre aquellos con datos bajos o incluso moderadamente sensibles. Por lo tanto, tener una red segmentada hace que sea difícil para atacantes y/o personas no autorizadas, navegar a través de redes que transportan datos confidenciales como lo son las redes industriales.

El objetivo de la segmentación y segregación de la red, es minimizar el acceso a información sensible para aquellos sistemas y personas que no lo necesitan, asegurando al mismo tiempo que la organización pueda seguir operando de manera efectiva. Esto ayuda a aumentar la protección de los datos de los procesos, cuando el acceso proviene de una de las redes externas. La separación entre las dos redes externas y la inserción de una red DMZ, ayuda a limitar aún más el acceso hacia la red interna de una empresa, porque la toma de decisiones empresariales requieren de

datos industriales para su efectividad, por lo que es importante la seguridad de los mismos.

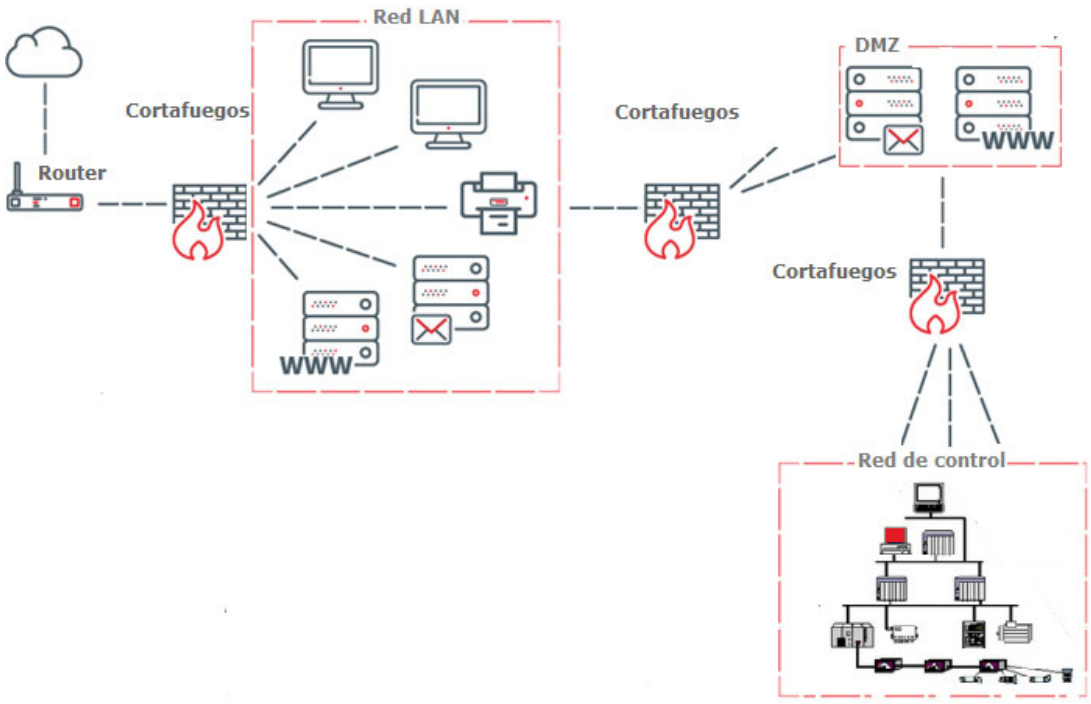

Figura 2.5: Propuesta de diseño de red de una organización segmentada para lograr mejor seguridad

Analizando las políticas de seguridad que debe cumplir la industria y las funciones de la automatización integrada de procesos, para la realización de esta investigación se selecciona la configuración de una DMZ con 3 cortafuegos de múltiples patas, debido a que es la más confiable para garantizar los protocolos de protección necesarios analizados en el punto anterior. Se segmentaron las redes de una organización para minimizar el acceso a información sensible, para aquellos sistemas y personas que no lo necesitan, asegurando al mismo tiempo que la organización pueda seguir operando de manera efectiva. Esto ayuda a aumentar la protección de los datos de los procesos, cuando el acceso proviene de una de las redes externas. La diferenciación de las dos redes externas ayuda a limitar más el acceso desde Internet que desde la red empresarial, porque para el caso de la red empresarial es necesario tener en cuenta que la toma de decisiones empresariales requieren de datos industriales para su efectividad.

2.4 Propuesta de diseño de seguridad integrando DMZ y Cortafuegos

Para el diseño de una red DMZ utilizando cortafuegos, que sea capaz de brindar seguridad a los datos y variables en una red industrial, se adoptaron medidas de seguridad que brindan una mayor defensa contra intrusos. La red DMZ cuenta con equipos tecnológicos como autómatas programables y *routers* con fibra óptica, que garantizan la comunicación con los servidores. Los buses de campo y la periferia descentralizada son Profibus PA y DP o protocolos similiares, conectados a los servidores que almacenan los datos. Las conexiones entre los dispositivos de una red industrial se realizan de forma redundante; permitiendo que si ocurre una falla, los procesos sigan funcionando dando al operador la posibilidad de solucionar el fallo sin detener el proceso [78], [79]; ya que esto provocaría pérdidas en la producción y por ende pérdidas materiales y económicas.

Analizando que a los servidores que almacenan los datos y las variables de procesos industriales, se puede acceder desde cualquier dispositivo conectado en esa u otra red; se realizó un estudio exhaustivo de las políticas de seguridad que debe cumplir la industria para garantizar los protocolos de protección necesarios; seleccionándose la configuración de una DMZ con 3 cortafuegos de múltiples patas, debido a que es la más confiable y garantiza una alta seguridad contra accesos indebidos y ataques informáticos. Las topologías de los cortafuegos se distribuirán entre la *Screened Subnet* y la *Dual-Homed Host* [74]. Los cortafuegos se ubicaron entre las redes externas y la interna de la siguiente manera:

1. Entre la conexión externa (puede ser Internet u otra empresa) y una red empresarial dentro de la industria.
2. Entre la red empresarial dentro de la industria y la DMZ.

Como cortafuegos se proponen *routers* con seguridad intrínseca, ya que poseen cortafuegos internos y de filtrado de paquetes utilizando el *iptables* de Linux [80], aumentando aún más los mecanismos de seguridad. Cuentan también con la herramienta de NetFilter que permite al administrador definir reglas aplicables a los paquetes IP que entran y/o salen de un *host*. Es importante destacar que cuanto más *routers* se instalen en la red, más seguridad se brindará, haciendo casi imposible burlar tantos protocolos.

En la propuesta de diseño se instalaron servidores que prohíben el tráfico de red exterior (toda red que no sea la industrial), hacia la red industrial y viceversa. Si un cliente necesita ver, por ejemplo, el proceso de combustión de una caldera, deberá acceder al servidor correspondiente en la red DMZ, y no al servidor real de la red industrial; garantizando que no se puedan realizar cambios en las variables reales de los procesos [81], [82], [83].

Con base en este marco teórico, se estudia el caso de aplicación de la Refinería de Santiago de Cuba para crear un sistema de comunicaciones industriales seguro, que garantice el uso de la información de la planta en la gestión empresarial. A continuación se detallan la arquitectura de red integrada, internet-empresarial-industrial, y las pruebas de simulación realizadas sobre seguridad informática en la refinería.

2.4.1 Descripción del diseño y configuración de la red DMZ propuesta para la red empresarial e industrial.

La Figura 2.5 muestra la red empresarial donde se adoptaron medidas de seguridad informática para la instalación de la red DMZ. Entre la red empresarial y la red externa (en el caso de Internet), se instaló un *router* configurado por el administrador que representa un cortafuegos de tipo aplicación desarrollado en Linux llamado *iptables*, utilizado para el filtrado de paquetes.

Entre la red empresarial y la DMZ, se ubicó otro *router* que representa otro cortafuegos del tipo de aplicación, también utilizado para el filtrado de paquetes. Esta herramienta de cortafuegos se considera una de las más eficaces y sólidas contra la intrusión de un intruso. Para lograr la seguridad requerida en el tráfico de información, se definieron las reglas de filtrado de paquetes que se exponen en el próximo epígrafe, que aprueban o no la solicitud hacia o desde los servidores de la red DMZ propuesta.

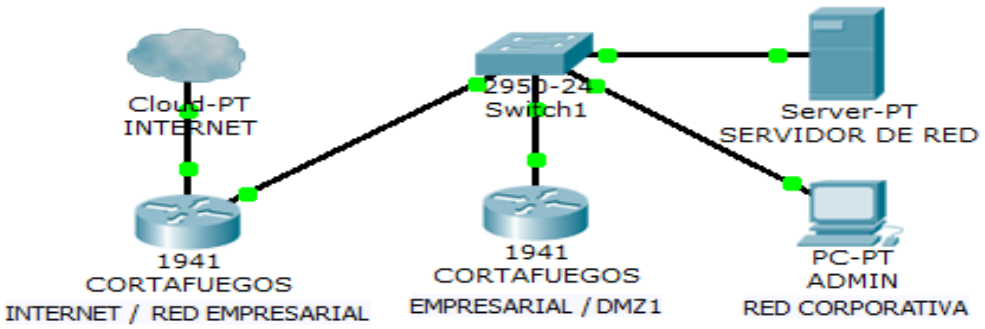

Figura 2.5. Comunicación entre la Red Empresarial e Internet

La red DMZ propuesta se muestra en la Figura 2.6 y es el frente contra ataques informáticos, ubicada entre la red empresarial y la red industrial como vía de acceso entre ellas de forma indirecta. Si un *host* de la red empresarial desea acceder a un proceso que ocurre en la planta en tiempo real, debe acceder al servidor correspondiente en la DMZ y no al de la red industrial directamente. De esta manera, se demuestra la importancia de la red DMZ como *host* bastión, que no son más que una aplicación que se localiza en un servidor con el fin de ofrecer seguridad a la red interna, ya que ha sido especialmente configurado para la recepción de ataques. En esta red, se establecen servidores como FTP, WEB, WEB MONITOR, DATA MONITOR y PROCESS HISTORIAL, etc.

Es importante señalar que para lograr el objetivo de la red DMZ, el tráfico debe ser de las redes externas (internet y/o empresarial) e interna (industrial) hacia ella, todo lo demás será prohibido. La red DMZ se conecta a la red industrial a través de un router y luego el cortafuegos es configurado bajo el protocolo de seguridad establecido más abajo, regulando así el tráfico de los datos.

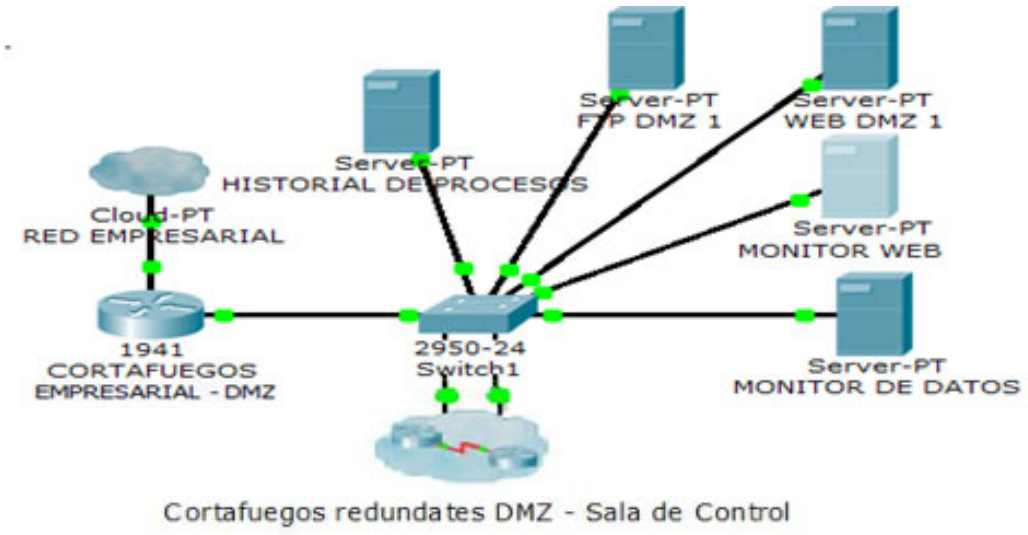

Figura 2.6. Red DMZ propuesta.

En la red Industrial ya conectada a la Empresarial (ver figura 2.7), se ubica el anillo de una red Ofimática. A la entrada de la misma se encuentran dos routers comunicados entre sí vía en serie, a través de las interfaces WAN (Serial0) de cada uno de ellos, representando así los cortafuegos ubicados entre la red DMZ y la red industrial.

Para la comunicación entre la red empresarial y la red industrial, las conexiones se establecen a través de cuatro conmutadores (switches) a través de sus interfaces LAN (GigaEthernet). Dichos conmutadores, a su vez, pueden estar conectando a algunas PC cliente o servidores, que puedan estar conectados a otros PC cliente y servidores dentro de la red de la planta (red industrial).

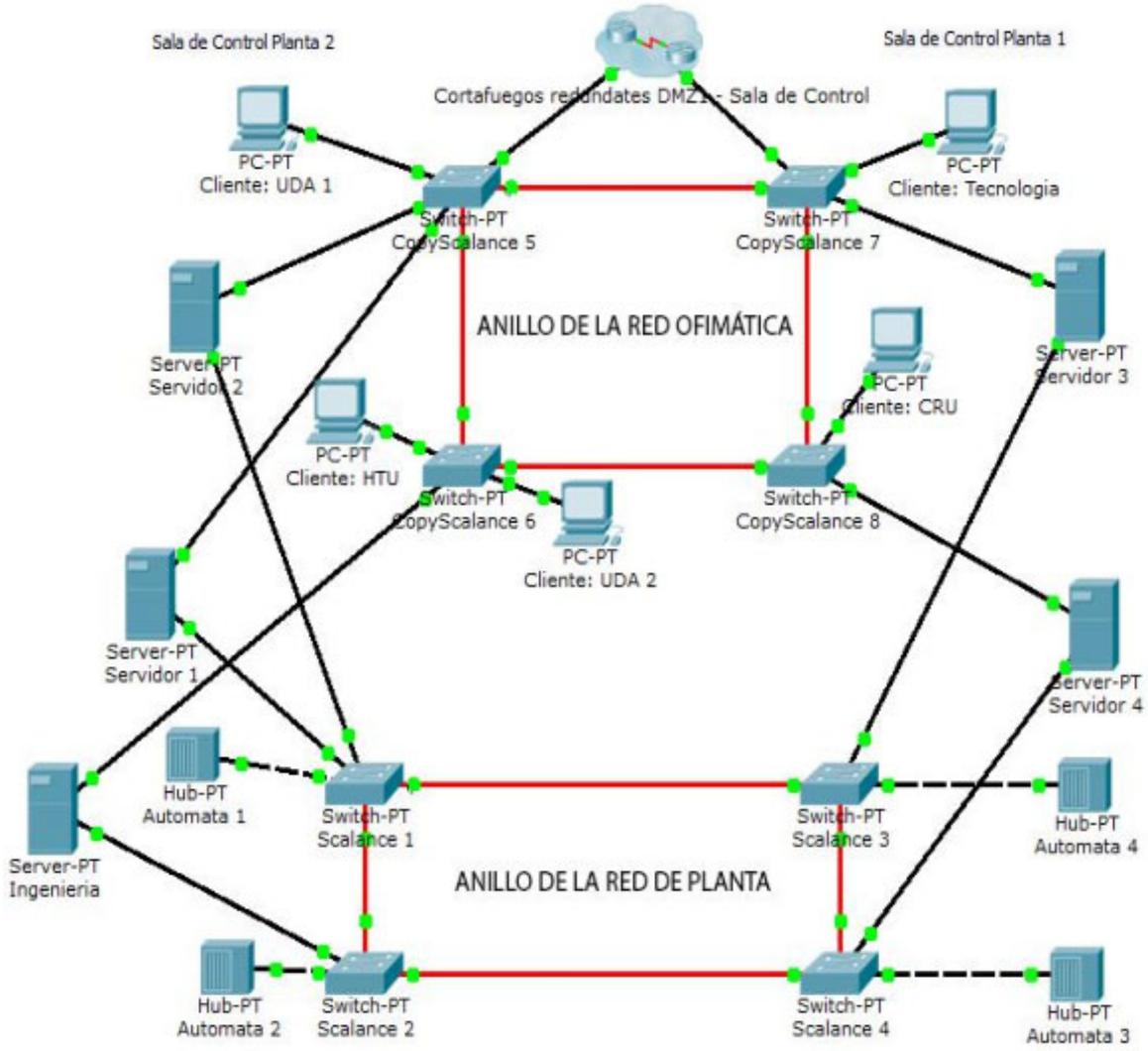

Figura 2.7. Red industrial propuesta

2.4.2 Configuración de los cortafuegos en iptables Linux

A la hora de configurar los cortafuegos, entre las redes externas se propuso el uso de cortafuegos de tipo aplización, que tiene como objetivo supervisar, filtrar o bloquear el tráfico HTTP que pasa a través de una aplicación web.

Para definir las reglas de cortafuegos de tipo aplicación se utilizó la herramienta *iptables* de Linux [80], que define las políticas de seguridad para el filtrado de paquete y que tiene en cuenta 2 premisas fundamentales:

1. Permitir todo el tráfico y luego irlo prohibiendo de acuerdo a las necesidades de seguridad.
2. Prohibir todo el tráfico y luego irlo permitiendo de acuerdo a las necesidades de seguridad.

2.4.2.1 DEFINIENDO POLÍTICAS POR DEFECTO ANTE CUALQUIER CONEXIÓN

Las reglas, definen cómo deben ser tratados los paquetes de datos entrantes y salientes. Estos paquetes enviados pasan por una cadena de regla en regla, donde cada regla provoca una acción o genera un cambio a otra cadena.

Las acciones que se producen cuando una regla se corresponde con un paquete de datos incluyen:

- ACCEPT: el paquete será aceptado.
- DROP: el paquete será descartado.
- QUEUE: mueve el paquete a los procesos de usuario y requiere un intermediario que reenvíe todos los paquetes a una aplicación.
- RETURN: el paquete se envía de nuevo a la cadena anterior en caso de que esta haya sido definida por el usuario. Las cadenas estándar se guían por la directriz de la cadena (por defecto y sin necesidad de configuración: ACCEPT).

Las cadenas estándar mencionadas en la acción *RETURN* están especificadas, por defecto, en las tablas de filtrado de iptables. Estas cadenas son: *INPUT, FORWARD y OUTPUT* como hemos mencionado. La primera se encarga de paquetes que deben ser entregados al sistema y la segunda procesa los paquetes de datos entrantes destinados a ser reenviados. La cadena *OUTPUT* es la cadena de salida que controla el tráfico generado a partir del propio equipo. Además de la tabla de filtros existe una tabla *NAT* para la traducción de las direcciones de red y una *MANGLE* para la manipulación de paquetes [84] [85]. Para regular el tráfico puedes crear tu propia cadena o utilizar las tres cadenas estándar (*INPUT, OUTPUT* y *FORWARD*).

Por las características de la industria, para la realización de este trabajo se utilizó la segunda premisa de la herramienta de *iptables*. Esta garantiza mayor seguridad por

admitir prohibir todo el tráfico y luego irlo permitiendo de acuerdo a las necesidades de seguridad de la organización donde se vaya a implementar.

El primer paso consiste en añadir la regla para descartar (*DROP*) a cada una de las tres cadenas, con el fin de asegurarse de que los paquetes de datos van a ser bloqueados en caso de que la implementación de cualquiera de las reglas de filtrado no arroje un resultado positivo. Por tanto se descartan los paquetes de entrada, salida y reenvío de la siguiente manera:

iptables -P INPUT DROP #se descartan los paquetes de entrada.

iptables -P OUTPUT DROP #se descartan los paquetes de salida.

iptables -P FORWARD DROP #se descartan los paquetes de reenvío.

2.4.2.2 DEFINIENDO REGLAS DE FILTRADO DE PAQUETES

A continuación, se expanden las cadenas *INPUT* y *OUTPUT* con la regla (-A) para ir habilitando el sistema (*ACCEPT*) [80]. A partir de acá se habilitan las conexiones entrantes y/o salientes según las necesidades de la empresa:

iptables -t filter -A INPUT -p tcp --dport 3000 -j ACCEPT #se acepta la entrada de paquetes con destino al puerto 3000 el cual es de una web en la DMZ.

iptables -t filter -A OUTPUT -p tcp --sport 3000 -j ACCEPT #se acepta la salida de paquetes con origen del puerto 3000.

iptables -t filter -A INPUT -p tcp --dport 80 -j ACCEPT # se abre el puerto 80 para el web monitor de una planta.

#abriendo los puertos 25 y 110 para brindar los servicios de correo.

iptables -t filter -A INPUT -p tcp --dport 110 -j ACCEPT #se abre el puerto 110 para habilitar el protocolo de correo.

iptables -t filter -A INPUT -p tcp --dport 25 -j ACCEPT #se abre el puerto 25 para habilitar el protocolo de transferencia de correo electrónico (SMTP).

iptables -t filter -A INPUT -s 192.168.0.0/24 -d 192.168.1.0/24 -j ACCEPT

#se permite la conexión de la red empresarial a la DMZ.

iptables -t filter -A INPUT -s 192.168.2.0/24 -d 192.168.1.0/24 -j ACCEPT

#se permite comunicación desde la red industrial para el envío de los datos de procesos hacia la DMZ.

La Figura 2.8 muestra la configuración donde se permite la conexión de la red empresarial a la DMZ y de la red industrial a la DMZ respectivamente.

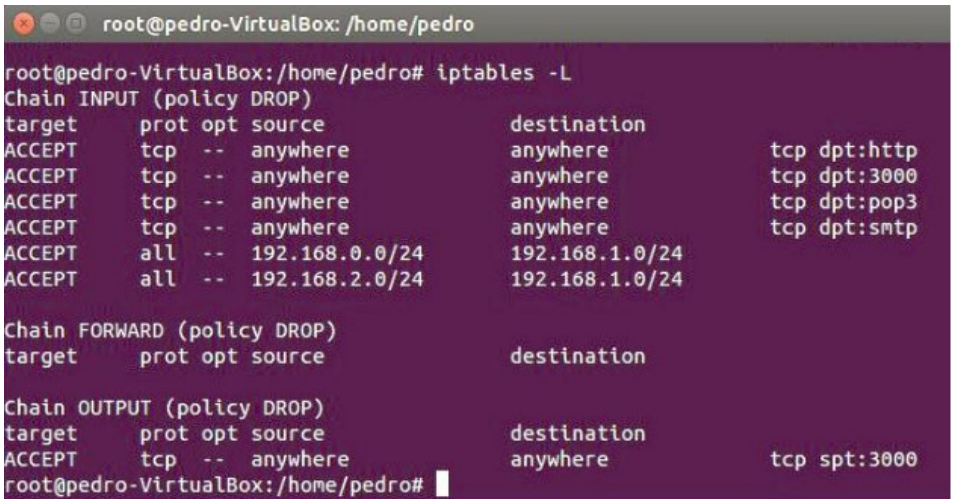

Figure 2.8. Configuración de cortafuegos usando iptables de Linux.

Para verificar que el resultado de la propuesta de diseño sea correcto, se realizaron pruebas utilizando la configuración anterior, ver Figura 2.9, donde se ejecutaron envíos de paquetes a la red empresarial desde la DMZ, evidenciándose que el envío se realiza satisfactoriamente.

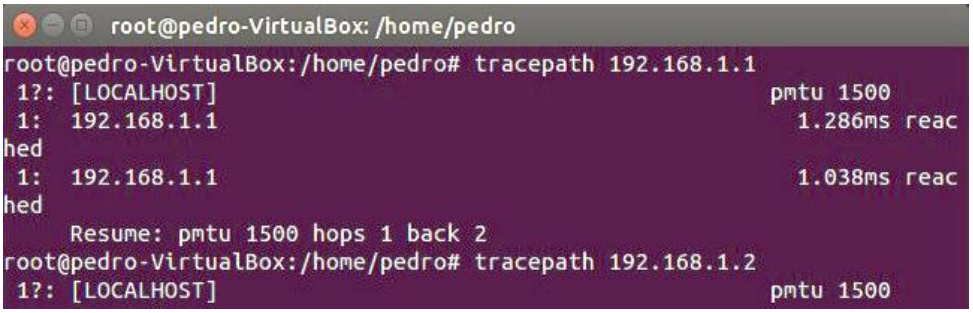

Figura2.9. Paquetes enviados hacia una red empresarial desde una red DMZ.

Para confirmar que no existe tráfico directo entre la red industrial y la red empresarial, se realizaron envíos de paquetes, como se muestra en la Figura 2.10, entre host de ambas redes, donde se evidencia que el envío no se realiza y que no existe respuesta entre ellos, demostrando que el diseño propuesto de red DMZ uzando cortafuegos es adecuado.

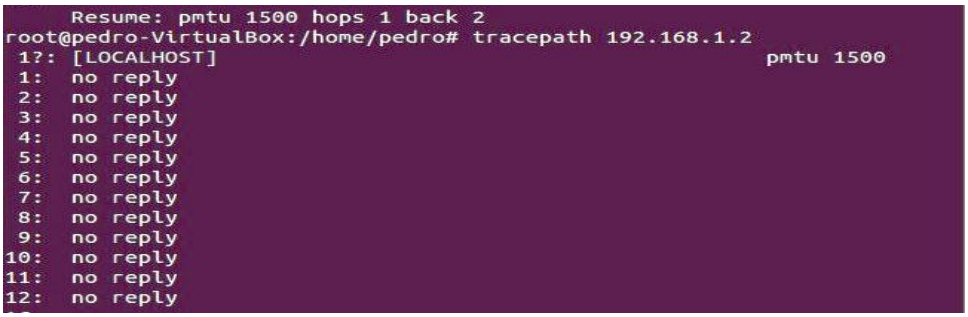

Figura 2.10. Intento de envío de paquetes desde una red industrial a una empresarial.

Al utilizar este soporte de red con DMZ y cortafuegos en las aplicaciones que soporten sistemas de automatización industrial integrada, se logra garantizar como primera barrera elevar el nivel de ciberseguridad de dichas aplicaciones. Como los SCADA son ampliamente utilizados para supervisión industrial y están absorviendo funcionalidades de los sistemas de gerencia de producción, mantenimiento predictivo y gerencia empresarial, es muy importante garantizar que estos sistemas se soporten en estructuras similares a la propuesta realizada en este trabajo. Para esto se deben estudiar las características del SCADA integrado y sus funcionalidades, para poder analizar como cumplir sus funciones de manera más segura, utilizando las medidas propuestas en este trabajo.

2.5 Recomendaciones a la hora de integrar SCADA a IT

A pesar de que en la presente investigación se propone un diseño usando DMZ y cortafuegos para integrar una red industrial a una red empresarial, fue necesario analizar otros mecanismos de seguridad existentes que se puedan aplicar a la industria para aumentar la seguridad de los datos de los procesos industriales, teniedo en cuenta la integración SCADA con los sistemas IT.

El fin de la integración de los sistemas SCADA y los sistemas IT, es conseguir que la estructura corporativa funcione como un todo, adecuando el funcionamiento de toda la estructura empresarial a las necesidades reales de cada momento. Algunos puntos suceptibles de dicha integración pueden ser las Unidades de Terminal Maestro (MTU, *Master Terminal Unit*), redes de comunicación, datos y aplicaciones [86].

La red empresarial ya suele existir cuando se piensa en integrar un sistema SCADA en la estructura general de la empresa. La vía más fácil sería integrar la estación en la red corporativa, a través de la red informática de ésta, ya existente. Si se realiza el

soporte de red SCADA sin las medidas antes previstas, se sentarían las bases de alta vulnerabilidad. En base a lo anterior, se recomienda utilizar estructuras de red DMZ utilizando cortafuegos explicado en el punto anterior, garantizando el soporte tecnológico de ciberseguridad requerida como primera barrera de seguridad, para sistemas de automatización integrada moderna.

Si utilizamos protocolos de comunicación estandarizados como TCP/IP, debemos asegurarnos de que usuarios sin permisos no puedan afectar al tráfico SCADA. Conseguir que los datos de las aplicación SCADA esten disponibles para la red empresarial, es lo que hace interesante el concepto de integración. Se pueden llevar a cabo acciones comerciales basándose en los datos del sistema de producción, o adecuar la producción a las directrices del departamento de ventas.

La arquitectura del sistema SCADA permite distribuir de manera sencilla los datos dentro de la empresa, gracias a las utilidades de que disponen (bases de datos relacionales, servicio web, etc.). Los usuarios pueden acceder a los datos de forma rápida y sencilla, para su posterior tratamiento (hojas de cálculo, documentación, etc.) [86]. Pero si se permite dicha integración sin la utilización de medidas de seguridad como la propuesta anteriormente utilizando DMZ y cortafuegos, no sería posible garantizar la seguridad de la aplicación integrada. Por tanto, la comunicación en cualquier aplicación de SCADAs industriales, debe contar como primera barrera con un soporte de red DMZ utilizando cortafuegos, que limite las posibilidades de intercomunicación garantizando que la información llegue a su destino de manera segura.

Simplemente, los diseñadores de las aplicaciones con SCADAs deben tener en cuenta los posibles bloqueos de intercomunicaciones no seguras, que realizan estos soportes de red ciberseguros a la hora de definir las comunicaciones y el tiempo de ejecución de funciones integradas, como la toma de decisiones inteligentes que utilizan mediciones auxiliares directas desde la automática local, y pueden asesorar o directamente actuar sobre algunas señales de control local del sistema.

El efecto de compartir los datos es el de mejorar el negocio, pues la empresa podrá adecuar sus acciones al estado real del sistema. La integración pone al alcance de cualquiera los datos de producción, por lo que sería muy sencillo integrar los datos a

una hoja de cálculo y enviarlos por correo electrónico. Ahora todo se basa en los estándares, las comunicaciones, el control, las bases de datos, etc. El problema es que estos estándares están al alcance de cualquier persona, ya que si se conoce un protocolo se puede robar información.

Para lograr la seguridad requerida a la hora de perfeccionar el negocio empresarial, integrando funciones en modo seguro, se propone en este trabajo el uso de un cortafuegos de tipo aplicación, capaz de evaluar los paquetes antes de permitir una conexión [72]. Estos además suelen prestar servicios de autenticación de usuarios y de proxy, manteniendo de esta forma la integración desde el control local hasta el nivel de negocio empresarial, pero con mayor ciberseguridad.

2.5.1 Políticas de Seguridad recomendadas para Sistemas SCADA integrados

Dentro de los sistemas SCADA, es esencial definir una serie de políticas de seguridad. Las políticas de seguridad trasladan los requerimientos de seguridad y fiabilidad de cada sistema SCADA particular a una serie de procedimientos auditable, los cuales permiten salvaguardar la seguridad en su diseño, implementación, y posterior funcionamiento. El alcance de las políticas de seguridad es muy amplio: éstas definen qué acciones pueden o no pueden ser realizadas por los diversos elementos físicos (por ejemplo, los operarios) y lógicos (por ejemplo, el subsistema de comunicaciones), los pasos a seguir durante las operaciones de mantenimiento y gestión de incidencias, además de la cadena de mando y las responsabilidades de cada uno de los miembros de la organización con respecto a la seguridad del sistema.

A la hora de desarrollar políticas de seguridad para sistemas SCADA, es recomendable seguir las normativas que contemplen controles de seguridad genéricos para sistemas de información. Entre otras, se encuentran las normas NIST 800-53 [33, 87] e ISO/IEC 17799 [88]. No obstante, los requerimientos específicos de los sistemas SCADA tales como una alta disponibilidad, fiabilidad, y tiempo de reacción, requieren de un conjunto de normas y políticas adaptadas especialmente a sus necesidades [9]. Con este fin, se han extendido normas existentes como la NIST 800-82, y definiendo diversos esquemas de políticas de seguridad dentro del ámbito académico [26]. Por

tanto, para cada sistema SCADA, recomendamos tener en cuenta principalmente las siguientes políticas de seguridad:

- protección de datos (acceso y almacenaje).
- configuración del hardware y software (virus, detección de intrusos, control de acceso, cifrado).
- seguridad en las comunicaciones (acceso inalámbrico, local, remoto), recursos humanos (uso del sistema, preparación y reciclaje), auditorías, seguridad física (acceso a equipamiento, destrucción de material), y ejecución de operaciones de forma manual en caso de fallo.

Todas las políticas de seguridad anteriores están influenciadas por los siguientes factores: las interdependencias existentes dentro de la organización, los roles de los diversos recursos humanos, la arquitectura del sistema de información, los datos manejados dentro de SCADA, y los riesgos asociados al sistema.

Como ejemplo de dichas políticas, es posible mencionar las políticas de gestión de incidencias. Un sistema SCADA debe recuperar su funcionamiento lo antes posible ante situaciones anómalas. Por lo tanto, hay que definir tanto el almacenamiento como el acceso a los eventos ocurridos dentro del sistema. También hay que controlar la visibilidad de dichos eventos, así como forzar que operarios con suficientes privilegios conozcan de su existencia. Estos operarios deben disponer de suficiente información (número de teléfonos, correo, claves de cifrado e instrucciones para verificar su identidad) con el fin de contactar con los encargados de la respuesta frente a incidentes. Finalmente, junto con procedimientos de recuperación y puesta en marcha, deben existir accesorios para recopilar y analizar pruebas de evidencias, las cuales pueden preservarse en previsión de posibles acciones legales.

En nuestro país contamos con el SCADA EROS-XD, por lo que recomendamos tener en cuenta el uso de normas como la NIST 800-82, que define diversos esquemas dentro del ámbito académico.

2.5.2 Recomendaciones como primera línea de defensa en redes de comunicación SCADA

En el año 2005, el NISCC [89] presentó una guía para la configuración y gestión de cortafuegos para sistemas de control. Dicha guía describe una posible arquitectura de

red segura y escalable basada en una división de tres zonas principales (ver figura 2.9), con el objetivo de delimitar cada una de las entidades del sistema, siendo la primera línea de defensa el cortafuegos, los IDS y la DMZ.

El cortafuegos deberá filtrar, por un lado las direcciones de red, de forma que cada componente SCADA tendrá asignada una dirección IP y uno (o varios) puertos TCP/UDP, y por otro lado, filtrar también a nivel de aplicación, centrando su uso en aquellos servicios de mayor riesgo en una red SCADA.

Actualmente, existen varios cortafuegos exclusivos para entornos industriales, como por ejemplo MODBUS-aware [90] para la familia IEC 60870-5 (101, 103 y 104) [91]. También, el NISCC propuso dentro de esta guía el desarrollo de cortafuegos embebidos en cada uno de los dispositivos de campo, conocidos con el nombre de micro-cortafuegos. Obviamente, hay que seguir investigando, ya que en general las RTU y PLC carecen de suficiente capacidades computacionales como para analizar continuamente el tráfico entrante y saliente.

Con respecto a los IDS [67], éstos son los encargados de monitorizar el tráfico de red basándose en patrones y reglas definidas en base a un conocimiento previo de vulnerabilidades y ataques. Esta tarea no es fácil de mantener en un sistema SCADA, ya que se requiere de una persistente actualización de dicho conocimiento. Actualmente, existen algunas herramientas IDS para entornos críticos como, [92], [93], [94], y cualquier tipo de incidencia detectada por éstos deberá ser registrado para realizar investigaciones en caso de que se requiera.

2.5.3 Recomendaciones para protección en los canales de comunicación de redes SCADA

Para garantizar disponibilidad y mantenimiento en los sistemas SCADA, las operaciones de control deben ser gestionadas desde cualquier punto de conexión y localización geográfica. Independientemente del tipo de red, los procesos de encriptación deben ser fuertes y los procesos de autentificación restrictivos, y en el caso de que la red de control tenga conexión directa a Internet implementar una VPN basada en SSL [95].

Cuando las operaciones de control deben llegar hacia los dispositivos de campo, se debe hacer uso de protocolos específicos como Modbus o DNP3, los cuales carecen

de mecanismos de seguridad. Si la comunicación es en serie, el sistema deberá tener instalado un dispositivo mediador entre el puerto EIA-232 de la RTU y el modem para gestionar las operaciones de encriptación de forma transparente; este dispositivo es conocido con el nombre de Bump-in-the-Wire [96].

Por el contrario, si la comunicación se realiza bajo el estándar TCP/IP, sólo será necesario instalar y configurar aquellos mecanismos de seguridad asociados al estándar. Igualmente, cuando el tráfico de control proviene de otro centro de telecontrol, éste hace uso del protocolo ICCP/TASE 2.0 [27, 97], el cual provee alta disponibilidad y rendimiento en la transmisión de datos, pero carece también de mecanismos de seguridad. Esto obliga que su diseño esté definido bajo el estándar IEC-62351 del TC57 [98], el cual incluye los protocolos TLS/SSL (para maximizar la interoperabilidad entre sistemas SCADA), MMS/IEC-62351-4 y una tabla bilateral para registrar los enlaces asociados. Todos estos protocolos proveerán al sistema de un soporte para la gestión de certificados, código de autentificación de mensajes, renegociación de cifrados, intercambio de claves de al menos 1024 bits, y firma digital con RSA y DSS, además de habilitar el puerto TCP 3782 para establecer comunicaciones seguras.

Por último, la criptografía y los sistemas de gestión de claves podrían resolver muchos de los problemas de seguridad en los canales de comunicación de redes SCADA. Sin embargo, esto no es relativamente fácil de conseguir, ya que existen múltiples e importantes limitaciones asociadas a las capacidades computaciones y de transmisión de datos de los dispositivos de campo. Uno de los primeros informes que agrupó un conjunto de estándares para la implementación de criptografía fue desarrollado por *American Gas Association* (AGA) con AGA-12 Part 1 [99]. Más tarde, presentaron el AGA-12 Part 2 [100], para describir una técnica de implementación criptográfica en canales de comunicación en serie, y quedan aún pendientes AGA-12 Part 3 y Part 4, donde especifican la protección de los sistemas de redes y la seguridad de dispositivos embebidos en componentes SCADA.

Este mismo grupo de trabajo también estuvo involucrado en desarrollar estándares para la gestión de claves en sistemas de control, y actualmente existen varios grupos de trabajo que están poniéndolo en práctica, como *TC57WG15* (IEC62351), *IEEE*

Power Engineering Society Substations Committee con P1689 y *DNP3 User Group* (DNP3 v1.0). Actualmente, existen varias técnicas propuestas, como por ejemplo, hacer uso de Criptografía de Clave Elíptica [101], y es necesario aplicar una metodología de selección [102] apropiada según el tipo de red SCADA diseñado.

2.6 *Valoración de aplicabilidad de la Metodología de cyberseguridad industrial en aplicaciones reales*

En la Refinería de Petróleo Hermanos Díaz en Santiago de Cuba que es nuestro caso de estudio, existe una infraestructura implementada a través de una red industrial y empresarial, aisladas entre sí. La red empresarial cuenta con servicios de Correo, Jabber, Internet, Dominio, Telefonía VoIP, Intranet, WEB y FTP. La red industrial desde 2007, cuenta con un sistema de control distribuido SIEMENS PCS7, basado en el uso de buses de campo, redes de comunicación Profibus PA y Profibus DP, tarjetas de comunicación ET 200, así como una amplia gama de equipos e instrumentación de campo capaces de proporcionar/procesar datos. Esta red se apoya en un banco de servidores redundantes en tiempo real.

Dada la necesidad de comunicar la red industrial con la red empresarial e Internet, y su importancia en la toma de decisiones acertadas, se hizo necesario utilizar mecanismos de seguridad entre estas redes. Estos mecanismos deben garantizar que la información se suministre digitalmente de manera segura a todos los clientes que necesiten utilizar los datos, lo que redundaría en un proceso más rápido y un mejor análisis de la información. De esta forma, se podría evitar un posible error humano a la hora de rellenar la hoja de ejecución, o utilizarse en la toma de decisiones automatizada del sistema de automatización integrado inteligente que se pretende implementar.

La red industrial de la Refinería "Hermanos Díaz" fue aislada en su momento de las redes externas, por lo que los servidores ubicados en la red industrial no eran accesibles desde ningún cliente (PC) ubicado en la refinería. Esto derivó en que no hubo acceso a los datos involucrados en el proceso, lo que evidenció la necesidad de integrar la red industrial con la red empresarial y esta a su vez a Internet. Dicha integración generó vulnerabilidades en cuanto a la seguridad de los datos ya que se podía recibir un ataque informático en cualquier momento y desde cualquier cliente.

Para lograr dicha integración entre estas redes, se realizaron investigaciones con el objetivo de lograr mecanismos de seguridad informática en la Refinería, donde se analizaron diversas opciones de protección aplicadas en refinerías a nivel mundial. Entre estas opciones, hay trabajos donde se propone el uso de redes DMZ y otros donde se propone el uso de firewalls. También se tuvo en cuenta la necesidad de subdividir las redes de refinería en tres redes: dos redes externas (Internet y negocios) y una red interna (industrial o de control, con datos y variables de proceso). Esto ayuda a aumentar la protección de la computadora cuando el acceso proviene de una red externa.

La Refinería Hermanos Díaz se encuentra en proceso de actualización de sus sistemas de seguridad informática para proteger el sistema de control y supervisión. Como cada empresa debe cumplir con diversas políticas de seguridad para cumplir con los protocolos de protección y dado que los procesos que se llevan a cabo en una refinería son críticos, se realizó un análisis en profundidad donde se llegó a la propuesta de implementación de una red. DMZ integrada con 3 firewalls de múltiples patas. Con la integración de los mecanismos de protección proporcionados por la red DMZ y el uso de cortafuegos, se logra una primera barrera de seguridad para los datos alamacenados en los servidores del sistema de control.

Finalmente, la propuesta de diseño permitió evaluar el nivel de seguridad que brinda la integración de redes DMZ con cortafuegos de diferentes fabricantes, demostrando sus ventajas frente a intentos de intrusión en las pruebas realizadas. El resultado logrado permitió la interconexión de la red empresarial con la red industrial de la refinería de una forma más segura, logrando la transmisión de los datos de procesos registrados en el sistema de control a la red empresarial con la seguridad requerida, evitando así la vulneración del sistema de control.

El acceso seguro a la información de la red industrial desde la red empresarial permite la creación de sistemas inteligentes distribuidos que utilizan los resultados del procesamiento automatizado de variables de proceso, para la toma inteligente de decisiones comerciales, con el objetivo de garantizar la eficiencia del sistema integrado para planificación y control de la producción, mantenimiento predictivo, logística, finanzas y negocios de la empresa. Todo esto abre las posibilidades de aplicar de

forma segura las ventajas del Internet de las Cosas (IoT) para la industria (Industria 4.0) en la Refinería de Santiago de Cuba. Todo el diseño y configuración de la propuesta fue puesto a prueba en la refinería en Santiago de Cuba, a través del proyecto de adquisición de un sistema que permita la unión de la red industrial con la red empresarial. El sistema propuesto y los resultados obtenidos en materia de seguridad de los datos sirven de base para continuar con la modernización de los sistemas automatizados y aumentar la protección de los sistemas de control de la planta. De esta forma, es posible el procesamiento seguro de variables, datos e información de proceso en tiempo real, lo que ayudaría a tomar decisiones precisas y acertadas utilizando inteligencia artificial y crearía las condiciones para implementar las ventajas de la Industria 4.0 en el futuro.

CONCLUSIONES DEL CAPÍTULO.

Las recomendaciones que se incluyen en este capítulo permiten crear sistemas integrados de supervisión y gerencia empresarial con un mayor nivel de ciberseguirdad. En este trabajo el diseño de la red DMZ propuesto brinda seguridad a los datos en una red industrial.

La propuesta de diseño brinda buenos resultados basados en la configuración seleccionada de una red DMZ integrada con 3 cortafuegos de múltiples patas, ya que la misma utiliza cortafuegos físicos aplicando la configuración conocida como cortafuegos de subred monitorizada, creando una barrera entre la red empresarial y la red DMZ, y luego brindando protección entre la DMZ y la red industrial. El diseño también tuvo en cuenta que los cortafuegos propuestos deben ser de diferentes fabricantes, para evitar que aunque se viole uno de ellos, no puedan aplicar la misma metodología para violar otro, y con ello continuar aumentando la seguridad.

Además de la estructura de soporte de red con seguridad, se deben tener en cuenta las medidas propuestas para un sistema supervisorio industrial integrado y evitar en cierta medida, algunas de las afectaciones que mencionadas en el capítulo 1.

Nuestro software profesional SCADA EROS-XD tiene posibilidades de cumplir con estas recomendaciones al desarrolar sus aplicaciones particulares, por tanto debe ser de conocimiento de todos los desarrolladores de aplicaciones en nuestro país el cumplimineto de las recomendaciones indicadas en este trabajo.

CONCLUSIONES

La aspectos teóricos referentes a la Automatización Industrial, las diferencias entre las redes empresariales e industriales, la seguridad en los Sistemas de Control Industrial, así como los mecanismos de ciberseguridad propuestos para estos sistemas, permitieron la obtención de conocimientos que posibilitaron la selección de una configuración capaz de brindar seguridad a los datos de los procesos de una red industrial.

La caracterización de la red Empresarial e Industrial situadas en la Refinería de Petróleo “Hermanos Díaz”, permitió encontrar las vulnerabilidades existentes en las mismas en cuanto a la seguridad de los datos de los procesos, a la hora de conectar ambas redes.

El diseño, simulación y programación de una red DMZ, integrada con tres cortafuegos de múltiples patas, permitió brindar seguridad a los datos de la red industrial de la Refinería de Petróleo “Hermanos Díaz”, demostrando ser una configuración que permite el intercambio de los datos entre la red empresarial y la industrial, a la vez que brinda seguridad a los datos de esta última, evitando en cierta medida la violación del Sistema de Control.

El estudio de los mecanismos de ciberseguridad industrial, permitió recomendar otros aspectos a tener en cuenta a la hora de integrar SCADA a IT, para así crear sistemas integrados de supervisión y gerencia empresarial con un mayor nivel de ciberseguridad.

RECOMENDACIONES

Para darle continuidad a esta investigación se recomienda implementar la propuesta de diseño en la Refinería de petróleo “Hermanos Díaz” de Santiago de Cuba, para la verificación de su funcionamiento.

Implementar en la industria políticas de seguridad como la protección de datos en cuanto al acceso y almacenaje de estos, la detección de intrusos, control de acceso, cifrado y seguridad en las comunicaciones.

BIBLIOGRAFÍA

[1] L. M. Crespo Martínez and F. A. Candelas-Herías, *Introducción a TCP/IP: sistemas de transporte de datos*: Universidad de Alicante, 1998.

[2] J. Edwards and R. Bramante, *Networking self-teaching guide: OSI, TCP/IP, LANs, MANs, WANs, implementation, management, and maintenance*: John Wiley & Sons, 2015.

[3] N. O. Alonso, *Redes de comunicaciones industriales*: Editorial UNED, 2013.

[4] E. J. Colbert and A. Kott, *Cyber-security of SCADA and other industrial control systems* vol. 66: Springer, 2016.

[5] Miguel_Soriano, "Seguridad en redes y seguridad de la información," vol. 2019, ed: České_vysoké_učení_technické_v_Praze, 2014.

[6] Y. F. Chala, "Importancia de la aplicación del mecanismo de cifrado de información en las empresas para la prevención de riesgos como ataques, plagio y pérdida de la confidencialidad."

[7] J. A. Lecuit, "Hacia la fusión entre la ciberseguridad industrial y los sistemas de información corporativos," *Análisis del Real Instituto Elcano (ARI),* p. 1, 2019.

[8] J. R. A. Yupanqui and S. B. Oré, "Políticas de Seguridad de la Información: Revisión sistemática de las teorías que explican su cumplimiento," *RISTI-Revista Ibérica de Sistemas e Tecnologias de Informação,* pp. 112-134, 2017.

[9] R. A. T. C. Miguel Luis Sojo Hernández , Mónica Rodríguez Dobarganes, and C. M. C. Eduardo Pérez Gómez , Marcel Mesa Martínez, Liuba M. Barroso Revilla "ENTORNO PARA EL DESARROLLO DE SISTEMAS SCADAS "EROS-XD"," in *Informática XVIII Convención y Feria Internacional 2020*, La Habana, Cuba 2020.

[10] J. Aguilar, A. R. BOLIVAR, F. Hidrobo, and M. Cerrada, *Sistemas MultiAgentes y sus Aplicaciones en Automatizaci on Industrial*, 2012.

[11] S. A. Boyer, *SCADA: supervisory control and data acquisition*: International Society of Automation, 2009.

[12] T. J. Williams, "A reference model for computer integrated manufacturing (CIM)," *International Purdue Works,* 1989.

[13] J. A. Martín, *Inteligencia artificial para la supervisión de procesos industriales*: Universidad Los Andes, 2007.

[14] C. A. Ospina Ardila, "Convergencia de seguridad IT y OT."

[15] P. S. Marshall, *Industrial Ethernet: a pocket guide: how to plan, install, and maintain TCP/IP Ethernet networks: the basic reference guide for automation and process control engineers*: ISA, 2002.

[16] J. F. Kurose, K. W. Ross, and W. L. Zucchi, *Redes de Computadores ea Internet: uma abordagem top-down*: Pearson Addison Wesley, 2007.

[17] P. Neumann, "Communication in industrial automation—What is going on?," *Control Engineering Practice,* vol. 15, pp. 1332-1347, 2007.

[18] N. Molly Melitafa, "Enfoque de seguridad en sistemas de control industrial," Universidad Central" Marta Abreu" de Las Villas, Facultad de Ingeniería …, 2017.

[19] J. J. R. Jalca, V. F. R. Castro, M. D. J. A. Menéndez, L. R. M. Quimiz, G. R. P. Anzúles, Y. H. C. Pilay*, et al.*, *Redes de Computadoras* vol. 32: 3Ciencias, 2018.

[20] J. C. Caicedo-Erasoa, D. R. Varón-Sernab, and F. Díaz Arango, "Redes industriales," ed: Vector, 2012.
[21] J. A. Nieto, "El accidente nuclear de Fukushima-Daiichi, Japón."
[22] L. Moreno, C. Geymonat, and J. M. Urriza, "Conceptos de tiempo real aplicados a la informática industrial," in *XVII Congreso Argentino de Ciencias de la Computación*, 2011.
[23] Á. R. Rojas Castro, "Protección en infraestructuras críticas: análisis de seguridad de los sistemas de control industrial," 2019.
[24] A. R. Penin, *Sistemas Scada*: Marcombo, 2012.
[25] C. A. Smith, A. B. Corripio, and S. D. M. Basurto, *Control automático de procesos: teoría y práctica*: Limusa México, 1991.
[26] H. Luiijf and B. J. te Paske, "Cyber security of industrial control systems," 2015.
[27] C. Alcaraz, G. Fernández, R. Román, Á. Balastegui, and J. López, "Gestión segura de redes SCADA," *Nuevas tendencias en gestión de redes, Novática,* 2008.
[28] P. Ackerman, *Industrial Cybersecurity: Efficiently secure critical infrastructure systems*: Packt Publishing Ltd, 2017.
[29] G. Clarke, D. Reynders, and E. Wright, *Practical modern SCADA protocols: DNP3, 60870.5 and related systems*: Newnes, 2004.
[30] Open_DeviceNet_Vendors_Association. (2019, 05/12/2019). *The_Future_of_Industrial_Automation*. Available: http://www.odva.org/
[31] G. J. Touhill. (2019, 17/12/2019). *Division_Research_Supports_National_Cybersecurity_Awareness_Month*. Available: https://www.sei.cmu.edu/about/divisions/cert/index.cfm
[32] E. Byres, P. Eng, and D. Leversage, "The Industrial Security Incident Database," *Retrieved on February,* vol. 20, p. 2008, 2006.
[33] K. A. Stouffer, J. A. Falco, and K. A. Scarfone, "Sp 800-82. guide to industrial control systems (ics) security: Supervisory control and data acquisition (scada) systems, distributed control systems (dcs), and other control system configurations such as programmable logic controllers (plc)," ed: National Institute of Standards & Technology, 2011.
[34] R. Lepofsky, "ISO/IEC 17799: 2005 and the ISO/IEC 27000: 2014 Series," in *The Manager's Guide to Web Application Security:*, ed: Springer, 2014, pp. 161-163.
[35] A. A. Cárdenas, S. Amin, and S. Sastry, "Research Challenges for the Security of Control Systems," *HotSec,* vol. 5, p. 15, 2008.
[36] K. Stouffer, S. Lightman, V. Pillitteri, M. Abrams, and A. Hahn, "NIST special publication 800-82, revision 2: Guide to industrial control systems (ICS) security," *National Institute of Standards and Technology,* 2014.
[37] D. Kilman and J. Stamp, "Framework for SCADA security policy," *Sandia National Laboratories report SAND2005-1002C,* 2005.
[38] E. Byres, J. Karsch, and J. Carter, "NISCC good practice guide on firewall deployment for SCADA and process control networks," *National Infrastructure Security Co-Ordination Centre,* vol. 2, p. 2005, 2005.

[39] S. Jeschke, C. Brecher, T. Meisen, D. Özdemir, and T. Eschert, "Industrial internet of things and cyber manufacturing systems," in *Industrial internet of things*, ed: Springer, 2017, pp. 3-19.

[40] A. Chowdhury and S. A Raut, "Benefits, Challenges, and Opportunities in Adoption of Industrial IoT," *International Journal of Computational Intelligence & IoT,* vol. 2, 2019.

[41] P. F. Tampering, "Modbus Protocol Based on the Characteristics," in *Advances in Intelligent Information Hiding and Multimedia Signal Processing: Proceedings of the 15th International Conference on IIH-MSP in conjunction with the 12th International Conference on FITAT, July 18-20, Jilin, China, Volume 1*, 2019, p. 335.

[42] L. Wang, M. Li, J. Qi, and Q. Zhang, "Design approach based on EtherCAT protocol for a networked motion control system," *International Journal of Distributed Sensor Networks,* vol. 10, p. 750601, 2014.

[43] H. F. Atlam, A. Alenezi, M. O. Alassafi, and G. Wills, "Blockchain with internet of things: Benefits, challenges, and future directions," *International Journal of Intelligent Systems and Applications,* vol. 10, pp. 40-48, 2018.

[44] S. Mantravadi, R. Schnyder, C. Møller, and T. D. Brunoe, "Securing IT/OT Links for Low Power IIoT Devices: Design Considerations for Industry 4.0," *Ieee Access,* vol. 8, pp. 200305-200321, 2020.

[45] I. N. Fovino, M. Masera, L. Guidi, and G. Carpi, "An experimental platform for assessing SCADA vulnerabilities and countermeasures in power plants," in *3rd International Conference on Human System Interaction*, 2010, pp. 679-686.

[46] Y. Wang, "sSCADA: securing SCADA infrastructure communications," *International journal of communication networks and distributed systems,* vol. 6, pp. 59-78, 2011.

[47] A. Ortega, C. M. Schweitzer, A. A. Shinoda, and A. V. Ortega, "Simulation of the DNP3 protocol over TCP/IP on a network IEEE 802.11 g ad-hoc with smart meter," in *2016 IEEE ANDESCON*, 2016, pp. 1-4.

[48] D. Hercog, "Communication Protocols."

[49] J. C. Eidson, *Measurement, control, and communication using IEEE 1588*: Springer Science & Business Media, 2006.

[50] J. Robert, J.-P. Georges, E. Rondeau, and T. Divoux, "Minimum Cycle Time Analysis of Ethernet-Based Real-Time Protocols," *INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL,* vol. 7, pp. 744-758, 2014.

[51] M. H. Collantes and A. L. Padilla, "Protocols and network security in ICS infrastructures," *Tech. Rep.,* 2015.

[52] M. Yang and G. Li, "Analysis of PROFINET IO communication protocol," in *2014 Fourth International Conference on Instrumentation and Measurement, Computer, Communication and Control*, 2014, pp. 945-949.

[53] P. Danielis, J. Skodzik, V. Altmann, E. B. Schweissguth, F. Golatowski, D. Timmermann*, et al.*, "Survey on real-time communication via ethernet in industrial automation environments," in *Proceedings of the 2014 IEEE Emerging Technology and Factory Automation (ETFA)*, 2014, pp. 1-8.

[54] J. Anabalón and E. Donders, "Seguridad en Sistemas SCADA un Acercamiento Práctico a Través de EH e ISO 27001–2005," *de MonkeysLab Research, Universidad de Santiago de Chile, Departamento de Ingeniería Informática, Chile,* 2014.

[55] J. R. Núñez Alvarez, I. F. Benítez, R. Proenza, L. Vázquez, and D. Díaz, "Metodología de diagnóstico de fallos para sistemas fotovoltaicos de conexión a red," *https://doi. org/10.4995/riai. 2017.7133,* 2019.

[56] H. Hosseinian, H. Shahinzadeh, G. B. Gharehpetian, Z. Azani, and M. Shaneh, "Blockchain outlook for deployment of IoT in distribution networks and smart homes," *International Journal of Electrical and Computer Engineering,* vol. 10, pp. 2787-2796, 2020.

[57] D. Korčok, "Industry 4.0: The future concepts and new visions of factory of the future development," in *Sinteza 2016-International Scientific Conference on ICT and E-Business Related Research*, 2016, pp. 293-298.

[58] C. G. Machado, M. P. Winroth, and E. H. D. Ribeiro da Silva, "Sustainable manufacturing in Industry 4.0: an emerging research agenda," *International Journal of Production Research,* vol. 58, pp. 1462-1484, 2020.

[59] F. Cavallin, "Estudo sobre redes de comunicação para automação industrial," 2016.

[60] J. Zhang, Y. Kuai, S. Zhou, G. Hou, and M. Ren, "Improved minimum entropy control for two-input and two-output networked control systems," in *2016 UKACC 11th International Conference on Control (CONTROL)*, 2016, pp. 1-5.

[61] M. M. B. Gaid, A. Cela, and Y. Hamam, "Optimal integrated control and scheduling of networked control systems with communication constraints: Application to a car suspension system," *IEEE Transactions on Control Systems Technology,* vol. 14, pp. 776-787, 2006.

[62] B. Rahmani and A. H. Markazi, "Variable selective control method for networked control systems," *IEEE transactions on control systems technology,* vol. 21, pp. 975-982, 2012.

[63] J. Nuñez, I. F. B. Pina, A. R. Martínez, S. D. Pérez, and D. L. de Oliveira, "Tools for the implementation of a SCADA system in a desalination process," *IEEE Latin America Transactions,* vol. 17, pp. 1858-1864, 2019.

[64] S. McLaughlin, C. Konstantinou, X. Wang, L. Davi, A.-R. Sadeghi, M. Maniatakos*, et al.*, "The cybersecurity landscape in industrial control systems," *Proceedings of the IEEE,* vol. 104, pp. 1039-1057, 2016.

[65] Instituto_Nacional_de_Ciberseguridad. (2019, 12/09/2020). *Qué es una DMZ y cómo te puede ayudar a proteger tu empresa* Available: https://www.barracuda.com/glossary/dmz-network

[66] C. G. M. Alonso, D. O. Gabriel, A. A. Ignacio, and S. R. Elio, *Procesos y herramientas para la seguridad de redes*: Editorial UNED, 2014.

[67] B. O. Páez Sotomonte, "Sistemas de detección de intrusiones: IDS vs sistemas de prevención de intrusiones: IPS," 2020.

[68] Infotecs. (2020). *DMZ: Zona Desmilitarizada*. Available: https://infotecs.mx/blog/dmz_zona_desmilitarizada.html

[69] I. N. D. C. INCIBE. (2019). *Qué es una DMZ y cómo te puede ayudar a proteger tu empresa*. Available: https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

[70] K. Dadheech, A. Choudhary, and G. Bhatia, "De-Militarized Zone: A Next Level to Network Security," in *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*, 2018, pp. 595-600.

[71] H. R. M. Rabanales, "Title," unpublished|.

[72] J. M. M. Vázquez, "Cortafuegos. Comparativa entre las Distintas Generaciones y Funcionalidades Adicionales," 2002.

[73] S. Amin, G. A. Schwartz, and S. S. Sastry, "Security of interdependent and identical networked control systems," *Automatica,* vol. 49, pp. 186-192, 2013.

[74] J. G. Delgado, "Title," unpublished|.

[75] I. Ahmad, S. Namal, M. Ylianttila, and A. Gurtov, "Security in software defined networks: A survey," *IEEE Communications Surveys & Tutorials,* vol. 17, pp. 2317-2346, 2015.

[76] Z. Chen, W. Dong, H. Li, P. Zhang, X. Chen, and J. Cao, "Collaborative network security in multi-tenant data center for cloud computing," *Tsinghua Science and Technology,* vol. 19, pp. 82-94, 2014.

[77] N. Cauvery, "Trust-based secure routing against lethal behavior of nodes in wireless adhoc network," *International Journal of Electrical & Computer Engineering (2088-8708),* vol. 10, 2020.

[78] J. Ponniah, "A clean slate approach to secure wireless networking," University of Illinois at Urbana-Champaign, 2014.

[79] J. Zhu, Z. Ge, Z. Song, and F. Gao, "Review and big data perspectives on robust data mining approaches for industrial process modeling with outliers and missing data," *Annual Reviews in Control,* vol. 46, pp. 107-133, 2018.

[80] J. Andreu, *Interconexión de red (Servicios en red)*: Editex, 2011.

[81] A. Mungekar, Y. Solanki, and R. Swarnalatha, "Augmentation of a SCADA based firewall against foreign hacking devices," *International Journal of Electrical and Computer Engineering (IJECE),* vol. 10, pp. 1359-1366, 2020.

[82] C. Shen, C. Liu, H. Tan, Z. Wang, D. Xu, and X. Su, "Hybrid-augmented device fingerprinting for intrusion detection in industrial control system networks," *IEEE Wireless Communications,* vol. 25, pp. 26-31, 2018.

[83] Y.-S. Jeong and J. H. Park, "Artificial intelligence for the fourth industrial revolution," *Journal of Information Processing Systems,* vol. 14, pp. 1301-1306, 2018.

[84] D. P. Serral, "El módulo Netfilter de Linux: iptables."

[85] E. M. Gonzaga Gonzaga, "Tutorial para la implementación de un Firewall usando Linux como sistema operativo e iptables y control de ancho de banda," Universidad del Azuay, 2008.

[86] A. R. Penin, *Sistemas Scada*: Marcombo, 2011.

[87] D. Bodeau and R. Graubart, "Cyber resiliency and NIST special publication 800-53 Rev. 4 controls," *MITRE, Tech. Rep.,* 2013.

[88] I. E. Commission, "Industrial communication networks-Profiles-Part 2: Additional fieldbus profiles for real-time networks based on ISO/IEC 8802-3," *Standard IEC,* pp. 61784-2, 2014.

[89] NISCC. *NISCC, National Infrastructure Security Co-ordination Centre, NISCC Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks, British Columbia Institute of Technology (BCIT)*.

[90] W. Shang, Q. Qiao, M. Wan, and P. Zeng, "Design and Implementation of Industrial Firewall for Modbus/TCP," *J. Comput.,* vol. 11, pp. 432-438, 2016.

[91] R. Kirkman, "Development in substation automation systems," in *2008 Third International Conference on Electric Utility Deregulation and Restructuring and Power Technologies*, 2008, pp. 598-603.

[92] INCIBE_Instituto_Nacional_de_Ciberseguridad. (2017). *Diseño y Configuración de IPS, IDS y SIEM en Sistemas de Control Industrial* Available: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjtuvvM5-j0AhUuSzABHZIpAVcQFnoECAoQAQ&url=https%3A%2F%2Fwww.incibe-cert.es%2Fsites%2Fdefault%2Ffiles%2Fcontenidos%2Fguias%2Fdoc%2Fcertsi_diseno_configuracion_ips_ids_siem_en_sci.pdf&usg=AOvVaw0ulV4XmW71BtLOOu_J3Jvv

[93] Digital_Bond, "IDS Signatures " 2007.

[94] A. Yang, L. Sun, X. Wang, and Z. Shi, "Intrusion detection techniques for industrial control systems," *Journal of Computer Research and Development,* vol. 53, p. 2039, 2016.

[95] M. E. C. Hurtado and D. J. A. Sarango, "Análisis de Certificados SSL/TLS gratuitos y su implementación como Mecanismo de seguridad en Servidores de Aplicación," *Enfoque UTE,* vol. 8, pp. 273-286, 2017.

[96] P. P. Tsang and S. W. Smith, "YASIR: A Low-Latency, High-Integrity Security Retrofit for Legacy SCADA Systems (Extended Version)," 2008.

[97] A. F. Narváez Portillo, "Aplicación de los enlaces ICCP en el intercambio de información entre los centros de control en tiempo real," 2006.

[98] R. Schlegel, S. Obermeier, and J. Schneider, "A security evaluation of IEC 62351," *Journal of Information Security and Applications,* vol. 34, pp. 197-204, 2017.

[99] A. G. Association, "Cryptographic protection of SCADA communications part 1: Background, policies and test plan," Technical Report AGA Report2005.

[100] M. Hadley, K. Huston, and T. Edgar, "AGA-12, part 2 performance test results," *Pacific Northwest National Laboratories,* 2007.

[101] R. Lambert, "Ecc and scada key management," in *S4 (SCADA Security Scientific Symposium) Conference*, 2007.

[102] L. Pièrre-Cambacédès and P. Sitbon, "Cryptographic key management for SCADA systems-issues and perspectives," in *2008 International Conference on Information Security and Assurance (ISA 2008)*, 2008, pp. 156-161.

ANEXOS

Anexo 1. Direccionamiento IP de los dispositivos

Equipos	Direccionamiento IP Gigabit Ethernet	Puertas de enlace	Red
Servidor de Red	192.168.0.2/24	192.168.0.1	Red Empresarial
PC0	192.168.0.3/24	192.168.0.1	Red Empresarial
PC Admin Red Corporativa	192.168.0.4/24	192.168.0.1	Red Empresarial
Servidor Historial de Procesos	192.168.1.2/24	192.168.1.1	DMZ
Servidor FTP	192.168.1.3/24	192.168.1.1	DMZ
Servidor WEB DMZ	192.168.1.4/24	192.168.1.1	DMZ
Servidor Web Monitor	192.168.1.5/24	192.168.1.1	DMZ
Servidor Monitor de Datos	192.168.1.6/24	192.168.1.1	DMZ
Cliente UDA 1	192.168.2.3/24	192.168.2.1	Red Ofimática
Cliente Tecnología	192.168.2.2/24	192.168.2.1	Red Ofimática
Cliente UDA 2	192.168.2.4/24	192.168.2.1	Red Ofimática
Cliente CRU	192.168.2.5/24	192.168.2.1	Red Ofimática
Cliente HTU	192.168.2.6/24	192.168.2.1	Red Ofimática
Servidor 1	192.168.2.250/24 - 192.168.3.1/24	192.168.2.1 - Autómata	Red Ofimática - Red de la Planta
Servidor 2	192.168.2.251/24 - 192.168.3.1/24	192.168.2.1 - Autómata	Red Ofimática - Red de Planta
Servidor 3	192.168.2.252/24 - 192.168.3.2/24	192.168.2.1 - Autómata	Red Ofimática - Red de Planta
Servidor 4	192.168.2.253/24 - 192.168.3.3/24	192.168.2.1 - Autómata	Red Ofimática - Red de Planta
Servidor Ingeniería	192.168.2.254/24 - 192.168.3.4/24	192.168.2.1 - Autómata	Red Ofimática - Red de Planta
Autómata 1	Filtrado por MAC		Red de Planta

Autómata 2	Filtrado por MAC		Red de Planta
Autómata 3	Filtrado por MAC		Red de Planta
Autómata 4	Filtrado por MAC		Red de Planta

Anexo 2. Direccionamiento IP de los cortafuegos

Cortafuegos	**Direccionamiento IP Gigabit Ethernet**	**Direccionamiento Puerto Serie**		**Red**
Cortafuegos Internet – Red Empresarial	110.10.20.1/8 - 192.168.0.1/24			Internet - Red Empresarial
Cortafuegos Empresarial – DMZ	192.168.0.1/24 - 192.168.1.1/24			Red Empresarial - DMZ
Cortafuegos redundantes DMZ – Sala de Control	192.168.1.1/24 - 192.168.2.1/24	Cortafuegos 1 10.30.1.3	Cortafuegos 2 10.30.1.4	DMZ -- Red Ofimática