

# Ciberseguridad, nuevo desafío para la ingeniería de control

## Ingeniería Electromecánica con Orientación en Electrónica

Tomás Indalecio Armoa López ,45729

**Resumen**— Este es un Proyecto del tipo exploratorio en el área de la ciberseguridad, orientado a explicar la importancia de la ciberseguridad para los sistemas de control industrial estableciendo una relación entre las tecnologías de información y comunicación y la Tecnología de Operación. También se evaluará casos de estudio con laboratorios virtuales tal como el propuesto por la empresa Fortiphyd Logic en conjunto con el Instituto tecnológico de Georgia creado para ser una herramienta open source para ayudar al estudio de la ciberseguridad en los sistemas de control industrial.

**Palabras clave**— Entorno Virtualizado, ICS (Sistemas de Control Industrial), industria 4.0, TIC, TO, Ciberseguridad, PoC (Prueba de Concepto), Proyecto Final de Grado

### I. INTRODUCCIÓN

A lo largo de los años los sistemas de control industrial han ayudado a las industrias a poder responder mejor a las exigencias del mercado mejorando la eficiencia de sus procesos, aumentando la seguridad y evitando riesgos. Por lo que siempre estuvo en crecimiento buscando mejorar lo más posible y facilitando más su uso. Hoy en día las industrias están pasando por una transición conocida como la cuarta revolución industrial o mejor conocida como industrias 4.0 donde se plantea la completa digitalización de los procesos y su incorporación al internet, de ahí surgen nuevos conceptos conocidos como Internet of Things (IoT), Tecnología de la información y comunicación (TIC) Cloud, entre otros. Lo que trae bastantes mejoras a las industrias, pero éstas a su vez también representan nuevos riesgos. En este trabajo de Grado se está exponiendo sobre estos nuevos riesgos que se presentan a los sistemas de control industrial y cómo enfrentarlos de manera a poder evitarlos o mitigarlos.

### II INTRODUCCIÓN A LOS SISTEMAS DE CONTROL INDUSTRIAL

#### A. Introducción a los Sistemas de control

Estos llamados Sistemas de control contemplan varios componentes como los son el Supervisory Control And Data Adquisition (SCADA), Human-Machine Interface (HMI), Distributed Control System (DCS), Programmable logic controller (PLC), entre otros. Todos estos están relacionados a

las Tecnología de Operación (TO) ya que entran dentro del concepto de automatización de procesos. Con la nueva tendencia de las industrias de interconectar sus equipos conocida como la cuarta revolución industrial o industria 4.0, nuevos conceptos fueron agregándole como el IoT( Internet of Things), cloud computing, Big Data, todos nuevos conceptos anteriormente mencionados comparten una similitud y es que todos requieren una conexión a internet, que en parte mejorará el servicio brindado por las compañías, pero también se verán afectados por las amenazas que las presentes en el internet como lo son los virus, cibercriminales, etc. [3] Esto presenta una gran amenaza ya que anteriormente las repercusiones que se daban por este ataque se daban solo en ciberespacio, pero como se estará presentando más adelante en los casos de estudio con las nuevas tendencias los daños ocasionados pueden llegar a presentarse en el mundo real. Y esto se da a través de la convergencia de las TO (Tecnologías de la Operación) con las TIC (Tecnologías de la Información y Comunicación) como se puede apreciar en la siguiente ilustración.

#### B. Niveles ISA-95

El Estándar ISA-95 tiene por objetivo el facilitar en las industrias la integración de las funciones empresariales a nivel TIC y los sistemas de control TO. Adicionalmente, aborda los modelos y las terminologías que pueden ser usadas para determinar qué información se debe intercambiar entre las diferentes funciones empresariales durante los procesos de compras, ventas, finanzas, logística, mercadeo.

Nivel 0 – El proceso industrial: En este nivel se encuentran los equipos de campo como lo son las maquinarias, motores, elementos físicos necesarios para el proceso.

Nivel 1 – El automatismo: En este nivel se encuentran los dispositivos que procesan y manipulan el proceso de producción. Tales como los sensores, actuadores y los autómatas. También se encuentran dispositivos con los RTU's que permiten la adquisición remota de datos para traspasarlos a los elementos de Nivel 2 como también a los autómatas de este mismo nivel.

Nivel 2 – Interfaz humana: En este nivel se da la primera interacción Hombre-Máquina. Principalmente con dos elementos el HMI y el SCADA, ambos elementos de monitoreo de procesos donde la diferencia está que el HMI suele ser de un solo PLC donde el operador puede monitorear una parte del proceso y los sistemas SCADA reúnen en una PC todo el proceso productivo, además de poder incorporar funcionalidades avanzadas como Data Logging, control de alarmas o comunicación con el nivel siguiente.

Nivel 3 – Históricos y enlaces con último nivel: En este nivel se encuentran los dispositivos encargados del control del flujo de la producción, las recetas del proceso productivo y que almacenan toda la información sobre los mismos; lotes, trazabilidad, productividad, calidad. Estos son MES, Batch y/o Historian.

También podríamos agregar el Big Data del hardware, por ejemplo, para mejorar la eficiencia energética de la fábrica o similares, este concepto está cada vez más en aumento.

Nivel 4 – El Cerebro empresarial: En este nivel se encuentran los softwares utilizados por la parte directiva de la empresa, softwares destinados a procesos económicos, contables y de marketing que ayudan con el inventario, la facturación, los gatos, la logística y la relación con el cliente a través de los CMR (base de datos de los propios clientes).



Fig. 1. Pirámide ISA-95

### C. La nueva problemática que afronta los ICS

El problema de la ciberseguridad en las infraestructuras críticas es un tema que preocupa mucho últimamente, y no es de exagerar ya que en los últimos años se han presentado varios incidentes, y cada vez van apareciendo más. Y esto no es algo que solo compete a los países de primer mundo, sino que ya está sucediendo en nuestra región, tanto así que la OEA (Organización de Estados Americanos) en conjunto con el BID (Banco Internacional de Desarrollo) emitieron ya varios reportes acerca del estado de la ciberseguridad en Latinoamérica y el caribe. Reportes donde nos mencionan la falta de una legislación para tales crímenes, fomentar la confianza cibernética y la diplomacia en Latinoamérica y el Caribe. [27]

Pero antes, ¿Qué es la Ciberseguridad? Según ISACA (Information Systems Audit and Control Association) se entiende que la ciberseguridad es la "Protección de activos de información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados" y Kaspersky nos dice que la ciberseguridad es "la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, la redes y los datos de ataques maliciosos". ¿Por qué es importante ambas definiciones? Porque la definición estándar de ciberseguridad siempre apunta a las TIC, y sin embargo Kaspersky ya no empieza a hablar también de los sistemas electrónicos. Esto es muy importante ya que como Joseph Weiss nos habla en su libro "Protecting Industrial Control System for Electronic Threats" aún no está bien definida la ciberseguridad dentro de los sistemas de control industrial. Sin embargo, cada día los

sistemas de control industrial o también podríamos llamarlos TO y las TIC están cada vez más relacionados. Más adelante estaremos estableciendo esta relación.

#### D. Deficiencias existentes en los ICS

Para los ICS siempre se priorizó la disponibilidad y la integridad del proceso, por ello, las medidas de seguridad en las mismas son muy escasas, siempre priorizando la producción a la seguridad del sistema, por ello, muchas veces encontramos sistemas con contraseñas de fábrica, conexiones que permiten todo tipo de tráfico entre otros, a continuación, se estará hablando de los errores más comunes. [23]

- Contraseñas fácilmente evitables: muchos PLC y DCS cuentan con la posibilidad de colocar contraseñas para poder evitar el cambio de la programación del sistema. Sin embargo, existen varias formas de pasar por sobre este proceso, ya sea por resets o por métodos de recuperación de contraseñas. También existen fabricantes que, a través de sus servicios de soporte, da la posibilidad de hacer bypass de las contraseñas.
- Protocolos sin autenticación: En un principio los protocolos no contaban con autenticación ni cifrado de la comunicación lo que provoca que cualquier dispositivo externo pudiese conectarse con el sistema (como lo demostraremos más adelante en la PoC). Hoy en día ya existe protocolos que cuentan con autenticación y cifrado como lo son el DNP3 y el OPC UA entre otros, pero a pesar de esto aún siguen siendo utilizados protocolos que no cuentan con ellos como por ejemplo el protocolo Modbus.
- Web server sin contraseña: hoy en día es muy normal que se disponga de un servicio web para el monitoreo, configuración y mantenimiento del sistema (como lo mostraremos más adelante en la PoC) sin embargo algunos no cuentan con un método de autenticación o son de muy fácil acceso como es el ejemplo el OpenPLC server de la PoC que no cuenta con un método de autenticación y es muy accesible por lo que cualquiera puede cambiar las configuraciones de los PLC.
- QoS (Quality of Service) Pobre: la calidad del servicio de la comunicación en las redes industriales muchas veces es opacada por la necesidad de los diseñadores de privar la velocidad de ejecución por sobre la efectividad de las comunicaciones. Dado esto, un ataque DoS podría fácilmente desbordar estas comunicaciones y causar problemas en el funcionamiento del programa de automatización.

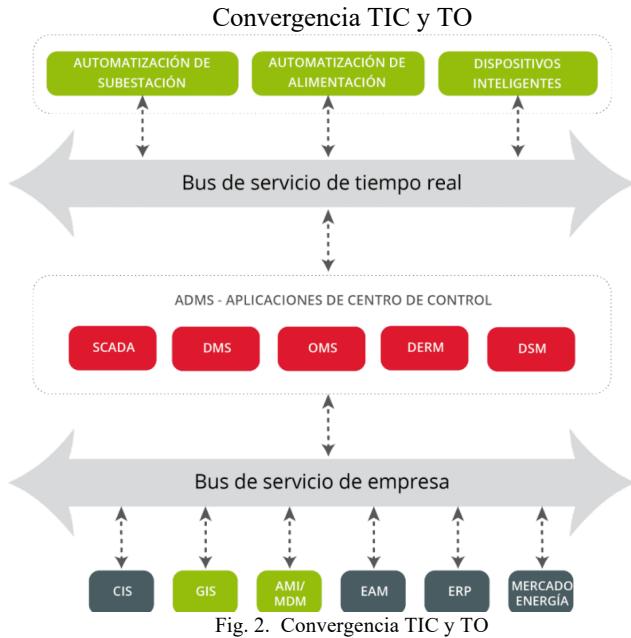
- Dificultad de parcheo: esto es un problema muy común ya que cuando se diseña el proyecto del automatismo se considera que este va a durar por lo menos unos 20 años, y durante ese tiempo se van encontrando nuevas vulnerabilidades sin embargo es muy raro que estas sean parcheadas o se parchen incorrectamente, que esto luego genera aún más problemas, por esta misma razón alguno prefieren no parchear ni actualizar para no desconfigurar el automatismo, dejando vulnerable todo el sistema.

### III CONVERGENCIA TIC Y TO

Estamos pasando por una era de la digitalización de los procesos donde se están adaptando las tecnologías a nuevos procesos para así poder mejorar en el servicio y el producto para el cliente, tecnologías como IoT (Internet of Things), Big

data, Cloud, etc. Pero para poder implementar dichas tecnologías es necesario la integración de los sistemas tanto TIC como TO, pero esto además de generar grandes beneficios también trae consigo nuevas amenazas.

La convergencia de los sistemas TIC con los TO se da a través de las redes de comunicación que generan esta cadena de mando durante su integración en los distintos niveles de la ISA 95, que también funciona como un camino desde la red de gestión empresarial a la red de TO. Camino que, de no ser segmentado y debidamente protegido, los ciberdelincuentes podrían usarlo para llegar a la planta y hacer daño en el mundo real. [42]



En un principio las TO y TIC se encontraban aisladas entre sí, este aislamiento protegía a los sistemas TO de amenazas como los ciberataques, por lo que los dispositivos fueron evolucionando en función a la precisión de sus funciones, mayor producción, mejor manejo, por ello la mayoría de los dispositivos carecen de defensas ante ciberataques.

#### A. Redes Industriales

Dentro de las industrias existen varios tipos de redes de comunicación diseñadas para interconectar desde dispositivos de campo con módulos de Entrada y Salida hasta dispositivos más complejos como computadores por medio de cables ethernet, siguiendo estos un protocolo de comunicación. Cabe resaltar que un protocolo vendría a ser un conjunto de reglas utilizadas en la comunicación entre dos o más dispositivos.

#### B. Buses de Campo:

Protocolo utilizado en una red de control para la comunicación de los distintos dispositivos de campo o de control (sensores, actuadores, PLC, DCS, etc.). Los buses de campo pueden utilizar conexiones y protocolos específicos como Profibus, Profinet o FieldBus, a través de distintas tipologías de redes físicas, incluyendo comunicaciones serie RS-232/485 o Ethernet. Los elementos de control utilizan

protocolos propietarios del fabricante u otros de carácter general como Modbus, DNP3 o OPC-UA. [27]

#### C. Protocolo Modbus

En el año 1979 la empresa MODICON-804 creó el protocolo Modbus para utilizarlo con sus PLCs. Se creó para transmitir información a través de líneas seriales entre dispositivos electrónicos. Este protocolo se creó para integrar los distintos dispositivos de diferentes marcas que existían ya que antes todo se manejaba por protocolos propietarios y solo se podían utilizar dispositivos de la misma marca. Todo esto cambio gracias a Modbus se liberó como un protocolo abierto, lo que provocó que infinitud de dispositivos de rango inferior lo adoptaran, como fueron los variadores de frecuencia, RTU, IEDs. Adoptándose también como segunda opción de comunicación en otros PLCs a través de módulos de comunicación. Por ello Modbus ha sido de los más utilizados en variantes serie (RTU [hex] y ASCII) y TCP (puerto TCP-502). En una red Modbus estándar puede haber un Maestro y hasta 247 esclavos. [12]

#### D. Protocolo DNP3

El DNP3(Distributed Network Protocol, en su versión 3) es un protocolo de comunicación entre IED (Intelligent Electronic Device), RTU (Unidades Remotas) y estaciones de control, Se utiliza mayormente en el sector eléctrico, con mayor presencia en el mercado americano que en Europa.

El DNP3 define las variables datos por tipo y comportamiento, de manera a priorizar las funciones que representen un cambio de variable, también se comunica utilizando un ancho de banda limitado para transportar valores de datos y comandos simples entre los extremos del sistema. Permitiendo el envío de enlaces en serie, multipunto, radioenlaces, conexiones de marcado y a través de redes dedicadas mediante TCP/IP o UDP. Gracias a esta adaptabilidad, se puede gestionar la mayoría de los escenarios de interrupción de conexión, dando como resultado un sistema de comunicación más resiliente con menos errores y fallos. [9]

Este protocolo también se destaca por su seguridad ya que utiliza un sistema de cifrado de comunicación para proteger los datos y un sistema de autenticación para evitar las intervenciones no autorizadas.

El cifrado que utiliza es el cifrado TLS que salvaguarda los sistemas conectados a través de canales TCP/IP cifrando los datos de manera que solo el sistema interno pueda leerlos. Está definido por el estándar DNP3 y la norma IEC 62351-3.

#### E. DNP3 vs IEC 61850

Aunque el protocolo DNP3 es el estándar más utilizado para el mercado energético estadounidense, en instalaciones eléctricas, de agua y aguas residuales, la norma europea IEC 61850 cada vez está abriendose más paso como el referente del futuro de los protocolos de comunicación. Siendo cada vez más adoptada en todo el mundo, muchas empresas que hoy en día tienen DNP3 están optando también por la funcionalidad transversal de ambos. Pero antes de integrarlos es importante primero entender sus diferencias. [9]

De acuerdo con Punzenberger una de sus principales diferencias podría ser el hecho de que DNP3 se centra en el transporte de datos simples de manera segura y ligera,

mientras que la norma IEC 61850 se centra en la comunicación de activos y la protección de los equipos, IED o sistemas HMI/SCCADA ya que esta norma fue creada enfocada para los incidentes relacionados a la Ciberseguridad. Otra diferencia importante es que la norma IEC se centra más en el contexto de los datos, mientras que, el DNP3 se centra en los datos y no tanto en su contextualización dejando este trabajo más a los ingenieros para que lo gestionen.

La norma IEC 61850 contempla las siguientes ventajas sobre el DNP3

- Tiempos de configuración reducidos: se reducen los tiempos necesarios para la configuración de los nuevos sistemas automatizados de la subestación gracias a la disponibilidad de un modelo de datos bien definido para los activos de las subestaciones.
- Mejor estandarización y organización: diseñado con un enfoque orientado a objetos, esto permite que los diseñadores puedan diseñar configuraciones estándar para elementos del sistema energético. Esto implica que se pueden eliminar o añadir bloques individuales sin tener que volver a rediseñar toda la ingeniería del sistema.
- Menos reconfiguración física: en caso de necesitar cambios, se pueden realizar cambios en el software en lugar de proceder a una reconfiguración física. Así se pueden realizar cambios fácilmente o volver a configuraciones anteriores sin necesidad de cambios costosos en los equipos.
- Mayor virtualización: se pueden realizar modelos de subestaciones y realizar pruebas en un entorno virtual antes de su implementación. De esta forma poder tener un mejor diseño inicial más robusto que requiera de menos modificaciones futuras.

#### *F. IEC 61850*

El estándar IEC 61850, desarrollado por la Comisión Electrotécnica Internacional (IEC, International Electrotechnical Commission), define una serie de protocolos de comunicación entre los distintos dispositivos de subestaciones eléctricas. Estos protocolos son Sampled Measured Values (SMV), Simple Network Time Protocol (SNTP), Manufacturing Message Specification (MMS) y Generic Substation Events (GSE), que a su vez se dividen en Generic Object-Oriented Substation Events (GOOSE) y en Generic Substation State Events (GSSE, actualmente en desuso). [18]

##### *1) Los protocolos que conforman el estándar IEC 61850*

- Sampled Measured Values: se utiliza para proporcionar una rápida comunicación de los valores de medición, protección y control. Funciona a través de Ethernet (capa 2 OSI) y los mensajes son encapsulados como multicast.
- GOOSE: se utiliza para la transmisión en tiempo real de eventos críticos, y funciona también a través de mensajes multicast de Ethernet (Capa 2 OSI).
- SNTP: es utilizado para la sincronización de tiempo de los dispositivos. Como su nombre lo indica, se trata de una versión simplificada del protocolo NTP. Se utiliza para la transmisión de protocolo UDP (Capa 4 OSI).
- MMS: se utiliza como base de las comunicaciones de datos de aplicación en el estándar IEC 61850. Sus mensajes son

enviados a través de las conexiones TCP (Capa 4 OSI) y es utilizada para las comunicaciones entre cliente y servidor.

#### IV. AMENAZAS, VULNERABILIDADES Y CASOS DE ESTUDIO RELACIONADOS A LOS ICS

##### A. Amenazas electrónicas o Ciberamenazas a los ICS

Joseph Weiss en su libro "Protecting Industrial Control Sistem from Electronic Threats" del 2010 [3] nos habla sobre que podría constituir a una amenaza electrónica o ciberamenazas para los sistemas de control industrial. Ellos pueden ser rotos de diferentes maneras, entre las más importantes se encuentran:

- Amenazas internas intencionales: esto se da cuando una persona con "información privilegiada" es despedida, no cobra todo lo que se le prometió o simplemente no queda satisfecho de alguna manera con la empresa en cuestión, por lo que buscan venganza de la empresa utilizando la información que tienen para acceder a los sistemas de control y general algún daño.
- Amenazas internas involuntarias: la confusión entre los ICS y los sistemas de información hacen que abunden los impactos no deseados. La mayoría de ellos se da por un diseño, políticas, arquitectura, procedimientos, tecnologías o pruebas inadecuadas. Estos son posiblemente los más frecuentes y los más difíciles de identificar.
- Amenazas externas no dirigidas: en esta categoría se encuentran los virus y gusanos que fueron diseñados y liberados de forma maliciosa para causar daños. No están dirigidos a los ICS, pero si estos se encuentran conectados a las redes TIC de gestión y verse afectados en el proceso. Se vio mucho esto con los USB contaminados que fueron colocados en las computadoras del nivel empresarial y llegaron hasta los ICS.
- Actores Maliciosos: aquí entran los hackers de sombrero negro, los Hacktivistas e incluso otras naciones. Es cuando el actor malicioso como lo dice su nombre busca dañar de alguna manera los ICS, siendo este el peor de las amenazas, ya que, en algunos casos pueden ser muy difíciles de prevenir.

##### *B. Vulnerabilidades en los ICS*

Según la NIST SP 800-82(Guía de seguridad para los ICS) las vulnerabilidades se agrupan según donde existan, como en la política y los procedimientos de la organización, o la insuficiencia de los mecanismos de seguridad implementados en hardware, firmware y software. Los primeros se conocen como pertenecientes a la organización y los segundos como pertenecientes al sistema. Comprender la fuente de las vulnerabilidades puede ayudar a determinar estrategias de mitigación óptimas. Los grupos de vulnerabilidades utilizados en este apéndice son: [10]

- a) Vulnerabilidades pertenecientes a la organización: las vulnerabilidades a menudo son introducidas a los ICS debido a la incompleta, inapropiada o inexistente

política de seguridad, entre ellos la falta de documentación, implementación de guías (por ej. procedimientos) y cumplimientos. Un buen soporte administrativo es la piedra angular de cualquier programa de seguridad ya que ayuda a reducirlas vulnerabilidades al ordenar y hacer cumplir una conducta adecuada. La política y los procedimientos escritos son mecanismos para informar al personal y a las partes interesadas sobre las decisiones sobre el comportamiento que es beneficioso para la organización.

- b)** Vulnerabilidades pertenecientes al Sistema: Las vulnerabilidades de un sistema pueden ocurrir en el hardware, firmware y software utilizado para construir el ICS y sus fuentes de estos pueden ser por fallas de diseño, fallas de desarrollo, configuraciones incorrectas, mantenimiento deficiente administración deficiente y conexiones con otros sistemas y redes. Las posibles vulnerabilidades que se encuentran comúnmente en los ICS se clasifican de la siguiente manera:

- Diseño y arquitectura
- Configuración y Mantenimiento
- Físicos
- Desarrollo de Software
- Redes y Comunicación

## V . ETHICAL HACKING

Para hablar de Ethical Hacking primero debemos definir la palabra hacker, que según la RAE en su segunda aceptación define la palabra hacker como " Persona con grandes habilidades en el manejo de computadoras que investiga un sistema informático para avisar de los fallos y desarrollar técnicas de mejora." [13]

Con esta definición ya descartamos ese conocimiento popular donde el hacker de por si es un criminal, siendo verdad que existe este tipo de hacker también existen los que se dedican a la auditoria de seguridad para los sistemas informáticos de ahí nacen los términos White Hat Hacker o Hacker de sombrero blanco y los Black Hat Hackers o Hackers de sombrero negro, siendo el de sombrero blanco el que se dedica a las buenas prácticas como el pentesting que vendría a ser una auditoria de seguridad para las empresas, y el de sombrero negro vendría a ser el que si utilizas sus habilidades para beneficiarse a sí mismo a través de las malas prácticas. [46]

### A. Pentesting

Dado los fraudes y robos de información que han sufrido varias empresas, surge la práctica ahora conocida como Pentesting que consiste en una auditoría de seguridad, donde el pentester realiza un test de penetración para encontrar los fallos de seguridad en el sistema [48]. Según el autor mencionado anteriormente existen varios tipos de Pentesting según la información con que cuenta el Pentester a la hora de realizar las pruebas de penetración:

- White Box: en este caso al auditor le proporcionan información acerca del sistema ya sea contraseñas, IP, firewalls. Es el más completo
- Black Box: es cuando no se le proporciona ninguna información de la empresa al auditor y este actúa como si fuera un cibercriminal más.
- Grey Box: es una mezcla de los dos anteriores, donde el auditor solo posee cierta información a la hora de realizar la prueba de penetración.

Existen varias metodologías utilizadas a la hora de ejecutar una auditoria de seguridad o pentesting (ISSAF, PCI, PTF, PTES, OWASP, OSSTMM) que se diferencian por el tipo de sistemas a auditar o, incluso, los requerimientos a los que se somete la empresa, pero todas ellas contienen 5 fases: [23]



Fig 3. Fases del Pentesting

### B. Fases del Pentesting:

- a) Recopilación de información: ya sea en una auditoria de caja negra o caja blanca, lo primero siempre será la recopilación de toda la información que se pueda sobre los sistemas que van a atacar. Esto también incluye las actividades de los empleados o directivos en las redes sociales ya que eso también podría revelar el sistema que utilizan. Cuanta más información tengamos disponible más fácil nos resultara la explotación de los sistemas.
- b) Búsqueda de vulnerabilidades: tras recopilar toda la información posible, es cuando procedemos a buscar objetivos, encontrar maneras de conectar con ellos e identificar sus vulnerabilidades. Aquí es donde se demuestra la habilidad del pentester.
- c) Explotación de vulnerabilidades: una vez que hayamos encontrados las vulnerabilidades del sistema pasamos a la explotación del mismo. Para ello se ejecutan exploits contra las vulnerabilidades o se utilizan las credenciales obtenidas previamente para ganar acceso a los sistemas y sacar provecho de él.
- d) Post-exploitacion: esto en una auditoria de seguridad no se llega a realizar siempre. Aquí es donde los atacantes reales harían acciones maliciosas luego de haber obtenido acceso, o dejarían un backdoor o puerta trasera y borrarían los registros de su presencia. De todas formas, una vez dentro, podrían volver a recopilar nueva información y tratar de ganar más privilegios.
- e) Elaboración de informenes: ya que se trata de una "auditoria" se deberá dejar al cliente un reporte o informe de las vulnerabilidades encontradas, como se

explotaron esas vulnerabilidades y consejos de como eliminarlas o al menos paliar sus consecuencias. Siempre se recomienda realizar dos informes, uno informe ejecutivo con explicaciones generales para los directivos, y otro informe más técnico para el personal operativo.

## VI. BUENAS PRÁCTICAS, NORMATIVAS ORGANIZACIONES A FIN DE LA CIBERSEGURIDAD INDUSTRIAL

### A. Aproximaciones a la protección de los ICS

Lo llamamos aproximación ya que en la realidad no existe un sistema completamente seguro e impenetrable. Con el pasar de los años y dado la evolución de los sistemas de control donde estos cada vez más van tomando aspectos de las TIC también se optó por aplicarles los mismos métodos de seguridad como Firewalls, IDS/IPS, VPN, antivirus entre otros.

- Firewalls: los firewalls o cortafuegos siguen siendo las herramientas más útiles a la hora de proteger nuestros dispositivos ya que estos pueden cortar el ataque o limitar el acceso de los atacantes a los demás niveles, por ello la importancia del seccionamiento del sistema por niveles como lo indica la ISA-95. Aunque los firewalls tradicionalmente son más del entorno TIC, cada vez son las empresas que están creando firewalls que soporten los distintos protocolos de comunicación industrial.

- IDS: o sistema de detección de intrusiones, es una aplicación que como su nombre lo dice se encarga de detectar accesos no autorizados a un ordenador o una red, es decir, es un sistema que se encarga de monitorizar el tráfico en la red y lo compara con una base de datos actualizada de firmas de ataques conocidos y ante cualquier actividad sospechosa, este emite una alarma para que se pueda tomar las medidas correspondientes.

- IPS: o sistema de prevención de instrucciones, es una aplicación que a diferencia del IDS este se encarga de prever las instrucciones al sistema realizando un análisis en tiempo real de las conexiones y protocolos para detectar si se va a producir algún incidente, analizando patrones, anomalías o comportamientos sospechosos y permitiendo el acceso o no a la red implementando políticas basadas en el contenido del tráfico monitorizado, es decir que el IPS a diferencia del IDS tiene la autoridad para descartar paquetes y/o desconectar conexiones. Cabe mencionar que hoy en día ya existen proveedores que ofrecen ambos servicios en uno IDS/IPS

- VPN: muy importante a la hora se asegurar las comunicaciones entre dispositivos si estos cuentan con una conexión remota, el VPN o Virtual Private Network como su nombre lo indica es una red privada donde solo se puede acceder con autenticación lo cual es muy importante para evitar

instrucciones, además de que encripta el tráfico de la red para mayor seguridad del mismo.

- Antivirus: esta solución se limita más a los sistemas de control que cuentan con sistema operativo o mejor dicho están instalados en un computador ya que la mayoría de los dispositivos de control no permiten la instalación de otros programas dentro de ellos como los PLC y DCS, sin embargo, es posible instalar dentro de un ordenador que también tiene instalado el SCADA, esto muy importante para evitar que el equipo quede expuesto y pueda comprometer el resto de los dispositivos.

Todo esto ayuda mucho a la hora de mitigar las amenazas a los ICS, sin embargo, si no son instalados correctamente o no se toman las medidas necesarias no hay mucho que puedan hacer por sí mismos, es por ellos que organizaciones en todo el mundo realizan estudio, investigaciones y pruebas para poder encontrar las mejores prestaciones de las mismas, de ahí salen los distintos Frameworks de distintas organizaciones dedicadas a la seguridad de los ICS.

### B. Normativas referentes a la ciberseguridad y a los ICS

#### 1) ISA 99/IEC 62443

El estándar ISA 99/IEC 62443 es la principal referencia en cuanto a Ciberseguridad de ICS se refiere, ya que en ella se reúnen una serie de documentos que ayudan al incremento de la protección de los ICS frente a ataques informáticos.

El comité de desarrollo de estándares ISA 99 reúne a expertos en ciberseguridad industrial de todo el mundo para desarrollar estándares ISA sobre seguridad de sistemas de control y automatización industrial. Este trabajo sirvió como base para la Comisión Electrotécnica Internacional para producir la serie IEC 62443 de múltiples estándares. [31]

Se lo llama serie al IEC 62443 ya que está compuesta por cuatro grupos principales (General, Políticas y procedimientos, Sistemas y Componentes) que luego se subdividen nuevamente, para tocar aspectos específicos que componen a cada grupo

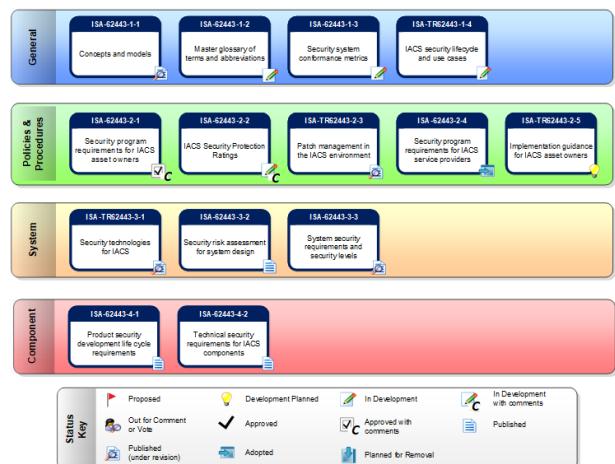


Fig. 4. Serie IEC 62443

2) *NIST SP 800-82 “Guía para la Seguridad de los Sistemas de Control Industrial (ICS)”.*

Este documento proporciona orientación sobre cómo proteger los sistemas de control industrial (ICS), incluidos los sistemas de control de supervisión y adquisición de datos (SCADA), los sistemas de control distribuido (DCS) y otras configuraciones del sistema de control, como los controladores lógicos programables (PLC), mientras se abordan sus requisitos únicos de rendimiento, confiabilidad y seguridad. El documento proporciona una descripción general de ICS y topologías de sistema típicas, identifica las amenazas y vulnerabilidades típicas de estos sistemas y proporciona contramedidas de seguridad recomendadas para mitigar los riesgos asociados. [10]

3) *La Familia de normas ISA 27000*

Las series 27000 están orientadas al establecimiento de buenas prácticas en relación con la implantación, mantenimiento y gestión del Sistema de Gestión de Seguridad de la Información (SGSI) o por su denominación en inglés Information Security Management System (ISMS). Estas guías tienen como objetivo establecer las mejores prácticas en relación con diferentes aspectos vinculados a la gestión de la seguridad de la información, con una fuerte orientación a la mejora continua y la mitigación de riesgos. [22]

*C. Estado de preparación de Paraguay con respecto a la Ciberseguridad*

Así como varios otros países Paraguay también se encuentra en un proceso de adaptación a las nuevas tendencias de la digitalización, prueba de ello es que en 2015 se desarrollaron mesas de discusión con los representantes todos los sectores de la sociedad paraguaya que son afectados directa e indirectamente por la nueva problemática de la ciberseguridad. Despues. varias reuniones y de varios borradores se publicó "el Plan Nacional de Ciberseguridad".

En este Plan Nacional de Ciberseguridad se abordan varios aspectos correspondientes al ciberespacio como los son el internet y su estructura, el fomento al uso de las TIC (Tecnología de la Información y la comunicación), la creación del CERT-PY para respuesta a los incidentes cibernéticos, la investigación de delitos informáticos de la cual estará encargada la Unidad Especializada de Delitos Informáticos, también nos hablan de la administración pública y del sector privado. [4]

La SENATIC es la institución que define, fiscaliza y apoya la implementación de políticas y estrategias transversales para garantizar el acceso y el uso de las TIC a la población paraguaya. En cuanto a la materia de ciberseguridad, el artículo 12, inciso h, de la ley N° 4.989/2013, atribuye expresamente a la SENATIC la tarea de " establecer y gestionar las políticas de protección de la información personal y gubernamental, y cultivar los conocimientos sobre la industria de seguridad de la información, para lo cual deberá establecer un sistema de organización de seguridad, proponer

una política de seguridad a nivel nacional, y establecer un plan de integración de protección de información" . Asimismo, el Artículo 14, inciso g) dispone la atribución de "establecer y gestionar políticas de protección de la información personal y gubernamental, y cultivar los conocimientos sobre la industria de seguridad de la información, para lo cual deberá establecer un sistema de organización de seguridad, proponer una política de seguridad a nivel nacional y establecer un plan de integración de protección de información", y el inciso h) "diseñar e implementar estándares, mecanismos y medidas tecnológicas de seguridad para el adecuado y correcto funcionamiento de los programas y servicios de acceso electrónico para el ciudadano". [4]

*D. Protección de Infraestructuras críticas*

En el Plan Nacional de Ciberseguridad también se anexa un plan de acción enfocado a las infraestructuras críticas en la cual divide la misma en dos aspectos fundamentales:

1) La resiliencia de las infraestructuras críticas ante las amenazas cibernéticas y garantizar la estabilidad de los servicios esenciales. Por ello se pretende:

- a) Crear una base de datos de todas las infraestructuras críticas tanto públicas como privadas con sistemas informáticos asociados.
- b) Impulsar la implementación de una normativa en ciberseguridad para la protección de infraestructuras críticas que abarque tanto el ámbito físico como el tecnológico.
- c) Realizar análisis de riesgo de las deficiencias sistemáticas, organizacionales y técnicas, de forma anual, en todas las infraestructuras críticas y activos críticos.
- d) Elaborar directrices técnicas para la gestión de sistemas de control industrial de las empresas.
- e) Llevar a cabo, en coordinación con los otros países que comparten con nosotros las infraestructuras críticas, proyectos específicos de control industrial

2) La responsabilidad por la ciberseguridad de las infraestructuras críticas es compartida tanto entre el estado y el sector privado, para fomentar la cooperación público-privada se pretende:

- a) Realizar reuniones periódicas con representantes del Ministerio Público y del CERT-PY para analizar la información de los incidentes y delitos informáticos para poder realizar procedimientos para la rápida acción contra los mismos.
- b) Desarrollar de forma conjunta procedimientos de cooperación entre los operadores de infraestructuras críticas, el Ministerio Público y el CERT-PY para reaccionar de manera más efectiva a los incidentes de ciberseguridad.
- c) Fomentar la participación del sector privado en ejercicios de simulación de incidentes cibernéticos, que permitan la compresión del rol que compete a cada sector, ante incidentes de ciberseguridad.

### E. Primera Prueba de Concepto (PoC)

La prueba de concepto consiste en simular las comunicaciones de dos dispositivos PLC uno maestro y otro esclavo comunicándose a través del protocolo Modbus, por ello para esta prueba se está usando la herramienta Modbus tools, que es un software de simulación de comunicación a través del protocolo modbus.

Para la prueba de concepto, se montó ha montado un laboratorio virtual con lo siguiente:

- 1 PC Master-Cliente: Servidor Windows Server 2012 virtualizado en VMWare.
- 1 PC Slave-Server: Servidor Windows Server 2012 virtualizado en VMWare.
- 1 PC Atacante: Sistema Operativo Kali-Linux virtualizado en VMWare.

#### Funcionamiento normal

En las siguientes imágenes se irá mostrando el funcionamiento normal de la prueba, una vez instalados los sistemas operativos en VMware y después de instalar también las herramientas Modbus Tools en sus respectivos sistemas operativos, se procede a realizar la configuración de los mismo, empezando por la IP de cada uno (es muy importante que ambos se encuentren en la misma red), como se trata de un entorno virtualizado no se puede simular la comunicación RS-485, por lo que se opta por la configuración Modbus TCP/IP. Se procede a hacer la configuración como se ven en la imagen.

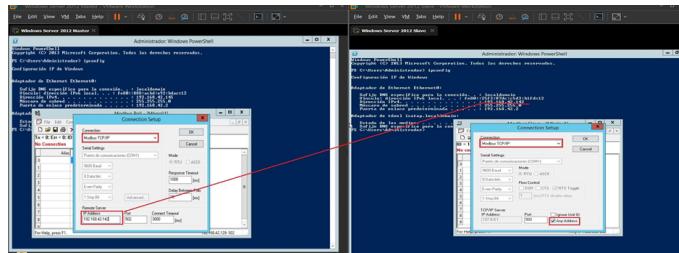


Fig 5. Configuración de IP

Donde el SCADA será el master que nos permitirá cambiar los valores en el PLC o Slave, como podemos ver en la siguiente imagen.

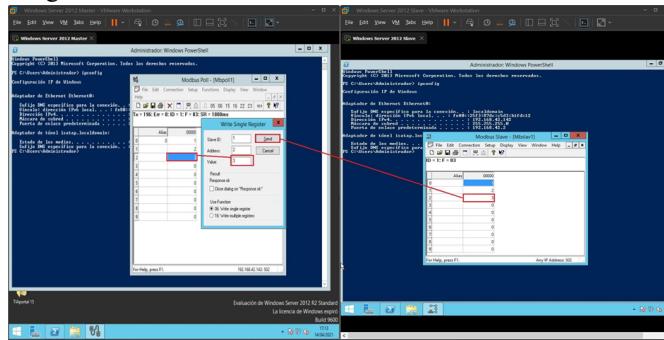


Fig 6. Envío de datos del Master al Slave

#### 1) Ataque a Modbus

Ya estuvimos viendo el funcionamiento normal del procedo de la prueba de concepto, ahora vamos a analizar la situación

desde el punto de vista del atacante para de esta forma poder entender mejor la naturaleza de un ciberataque, para ello ahora nos dirigiremos a nuestra máquina virtual con sistemas operativo Kali-Linux, que como mencionamos anteriormente ya cuenta con varias herramientas para el hacking.

#### 2) Primera parte: Sniffer

Una vez dentro lo primero que suponemos hará el cibodelinciente será un reconocimiento de la red o “sniffer” para ello existen varias aplicaciones, pero nosotros usaremos Wireshark, en el cual podremos filtrar el tráfico de forma a poder concentrarnos únicamente en las comunicaciones con protocolo Modbus. De ahí podemos sacar la IP del PLC y los datos que está transmitiendo ya que el protocolo modbus no cuenta con encriptación de datos.

#### 3) Segunda Parte: Ataque

Ahora que conocemos el IP del PLC nos disponemos a Kali y ejecutamos la aplicación Metasploit colocando el comando msfconsole en la terminal. Una vez que se despliegue la aplicación, colocamos search Modbus para buscar en la base de datos de Metasploit por los exploits que tiene disponible para el protocolo Modbus, y utilizamos el módulo que dice: auxiliary/scanner/scada/modbusclient que según la descripción nos permitirá comportarnos como el Cliente o en este caso Master para poder realizar modificaciones en los registros. Una vez desplegado el módulo colocamos “show options” para que nos muestre lo que podemos hacer con el módulo y pasamos a configurar

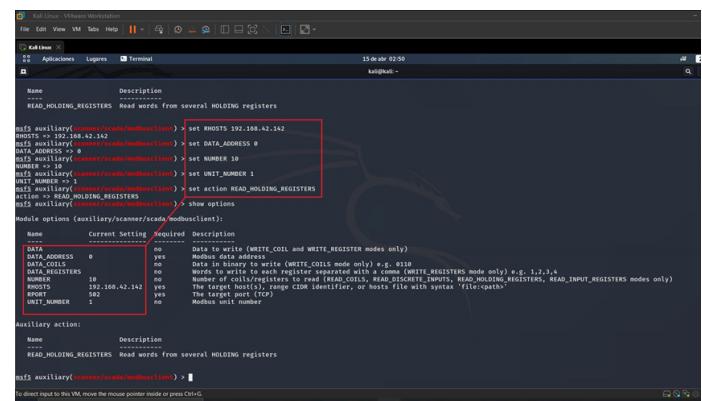


Fig 7. Configuración del ataque

Una vez que este todo configurado ejecutamos con el comando “run” para realizar el ataque. Como se puede comprobar en la siguiente imagen el ataque fue exitoso.

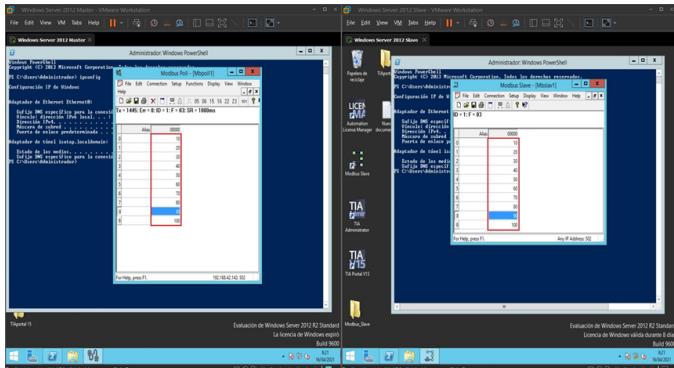


Fig 8. Confirmación del ataque

### F. Segundo PoC

Para esta prueba de concepto estaremos utilizando un escenario diseñado por la empresa Fortiphyd Logic en conjunto con el Instituto Tecnológico de Georgia para realizar pruebas de ciberseguridad a ICS de forma gratuita. La prueba de concepto se llama GRFICSV2 y se trata de la simulación de una Planta Química basada en la planta de la compañía Eastman Chemical, pero en la versión resumida ofrecida por la Universidad de Washington donde esta versión simplifica el proceso en un reactor separador químico de dos fases en la que se tiene un total de cuatro válvulas de control para monitorear medidas de salida.

Este escenario cuenta con 5 máquinas virtuales todas para desarrollarse en la aplicación llamada VirtualBox (también open source), todas las máquinas tienen sistema operativo Ubuntu y ya están programadas para ejercer su rol designado. Entre los roles designados se encuentran: La simulación de la planta química, el sistema SCADA, el PLC, el firewall, y la Workstation, también para se utiliza una máquina virtual con kali linux pero anteriormente mencionamos que eran solo 5 ya que es el número de máquinas virtuales que nos brinda GRFICSV2 en su página de GitHub: <https://github.com/Fortiphyd/GRFICSV2>.

La Máquinas Virtuales son:

ChemicalPlanta: la Simulación de la planta Química



Fig 9. ChemicalPlant

PLC: el VM (Virtual Machine) es una versión modificada de OpenPLC que usa una versión anterior de la biblioteca libmodbus con vulnerabilidades conocidas.

HMI: en esta maquinan se utilizar el sofware open source ScadaBR, con el cual estaremos monitoreando los procesos que realiza el PLC.



Fig 10. ScadaBR

Pfsense Firewall/Router: este firewall VM proporciona funciones de enruteamiento y valga la redundancia de firewall entre la red DMZ y la ICS.

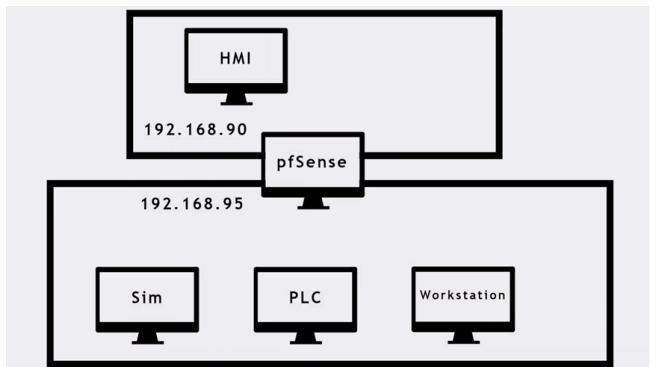


Fig 11. Estructura de las redes

Engineering Workstation: la Estación de trabajo o Workstation es una máquina virtual con Ubuntu 16.04 con el software OpenPLC instalado para realizar las programaciones del PLC.

Así como en el anterior PoC realizamos el ataque empezando por analizar el tráfico en la red y encontramos dos IP que se repiten Uno pertenece a la red 192.168.90.0/24 y el otro a la red 192.168.95.0/24, como la primera red pertenece al WAN sabemos que pertenece al HMI por lo tanto la segunda red debe pertenecer al PLC. También, analizando los datos del tráfico, se pudo constatar que hay un valor binario que se repite en varias ocasiones, esto es importante ya que, colocándonos en la situación del Cibercriminal, no entenderíamos mucho de los datos que se están transfiriendo, sin embargo, un dato binario solo varía entre 0 y 1 por lo que el cibercriminal sabría que para generar un perjuicio solo debería cambiar ese valor.

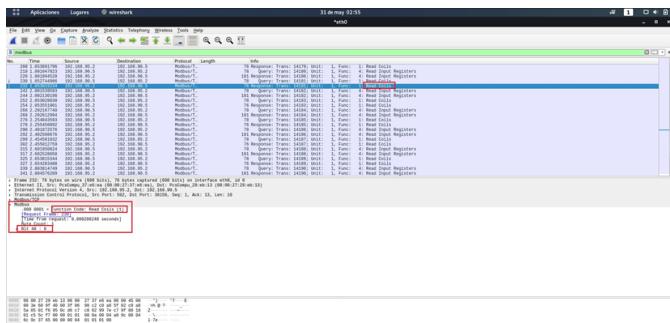


Fig 12. Escaneo de la red con wireshark

### 1) Primer Ataque

Ahora que tenemos un objetivo nos dirigimos nuevamente a nuestro Kali Linux y desplegamos Metasploit como en el PoC anterior. También utilizamos el mismo Modulo auxiliary/scanner/scada/modbusclient para este ejercicio, pero en vez de utilizar DATA\_REGISTER utilizamos DATA\_COILS que sería el correspondiente a binario y en vez de WRITE\_REGISTERS utilizamos WRITE\_COILS como acción.

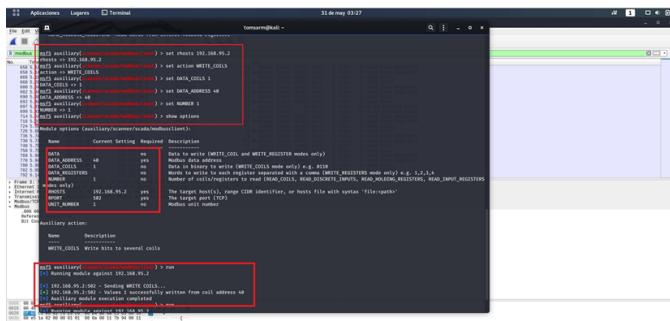


Fig 13. Configuración para el ataque a protocolo modbus

Y como se puede ver en la siguiente imagen el binario se trataba nada más y nada menos que del botón de apagado de emergencia.



Fig 14. Apagado remoto del atacante

### 2) Segundo Ataque

Para este ataque consideraremos que conseguimos acceso remoto al Workstation y cargaremos una nueva configuración con valores por encima de los niveles soportados por el tanque en el PLC. Entonces, nos dirigimos a la Workstation y abrimos el OpenPLC Editor y guardamos el archivo de forma que el OpenPLC pueda leerlo, en formato .st, luego nos dirigimos al navegador que ya nos despliega automáticamente

el Web Server y podemos ver que no cuenta con un factor de autenticación por lo que nos disponemos a cargar la nueva configuración sin problemas.



Fig 15. Web Server del OpenPLC

Una vez que la nueva configuración esté cargada nos dirigimos al SCADA y vemos que no salta ninguna alarma ya que este cree que se están cumpliendo los requisitos ya que lo está comparando con la nueva configuración, sin embargo, en la simulación podemos ver como está afectando realmente la nueva configuración.

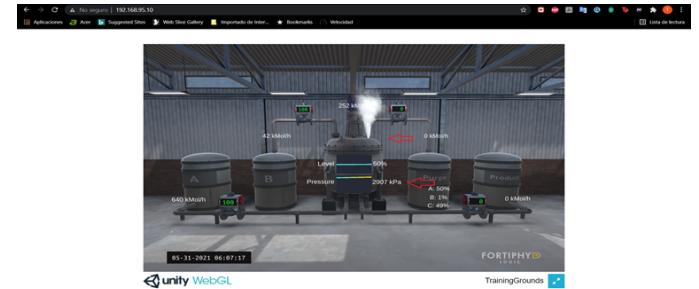


Fig 16. Primera fuga en el tanque

Terminando en un resultado catastrófico como se puede ver en la siguiente imagen.

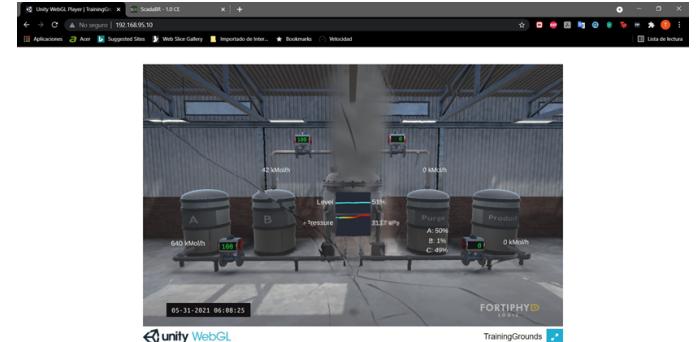


Fig 17. Explosión provocado por el ciberataque

### 3) Escenario Seguro

Primero que nada, cabe resaltar que no existe escenario completamente seguro, y más aun en las industrias ya que estas normalmente cuando elaboran su presupuesto lo estiman con una duración de al menos unos 20 años, por lo que no se encuentran constantemente actualizando sus dispositivos y esto los deja muy vulnerables, pero existen otras formas de proteger el dispositivo. En esta prueba se estuvo utilizando el programa Pfsense como router sin embargo también puede funcionar como Firewall, este programa cuenta con mas formas para mitigar los ataques como los son OpenVPN y Snort que es una aplicación que posee IDS/IPS, sin embargo,

por cuestiones de tiempo, no se pudieron configurar estas opciones también.

Con el Firewall optamos por seccionar la red y solo permitir el acceso a los dispositivos que son estrictamente necesarios como el SCADA. Cabe mencionar que en una situación real usaríamos la dirección MAC de los dispositivos ya que la misma es irrepetible y no se puede cambiar, si embargo, como estamos trabajando en un entorno virtual optaremos por hacerlo mediante la dirección IP.

Como se puede ver en la siguiente imagen, luego de aplicar la nueva regla ahora el atacante ya no puede acceder al PLC por lo que no puede cambiar sus valores.

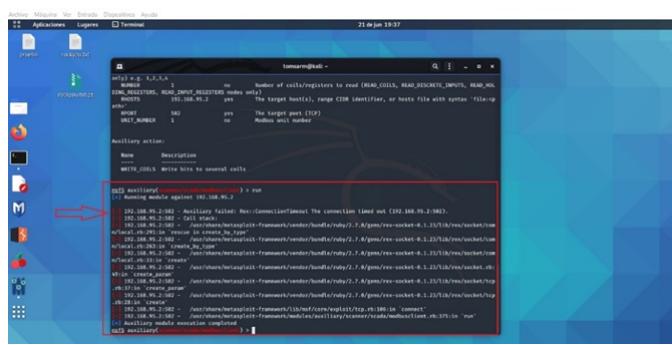


Fig 18. Fallo en el ataque

## RESULTADOS

Con estos experimentos pudimos ver como es sencillo para un hacker realizar estos ataques ya que los ICS no cuentan con muchas maneras para evitarlos, también pudimos ver lo expuesta que esta la información ya que la mayoría de los protocolos no cuentan con un cifrado, y lo importante de contar con un sistema de autenticación para evitar que cualquier persona pueda realizar cambios en el sistema, ya que como vimos en las segunda prueba de concepto, aunque consideramos que un hacker lo hizo pudo haber sido también un error de programación de un personal inexperto.

También cabe resaltar que, aunque en este escenario la limitación de comunicación entre redes gracias al Firewall pudo mitigar el ataque esto puede ser fácilmente evitado en la vida real, por lo que es de suma importancia contar con un sistema IDS/IPS con una buena base de datos de firmas que pueda detectar cada nuevo ataque.

## CONCLUSIÓN

Este Proyecto Final de Grado consistía en demostrar la importancia de la ciberseguridad en los sistemas de control industrial estableciendo la relación entre las TIC y los TO, utilizando un caso de interés y explicar desde el punto de vista técnico lo que sucedió mal. Y esto lo podemos ver claramente en el Capítulo II donde hablamos de que la convergencia de TIC con TO se da a través de esta cadena de mando que se genera durante la integración de los niveles de la ISA 95, que funciona como un camino desde la red de gestión empresarial a la red de TO.

También con la PoC se pudo demostrar la importancia de la ciberseguridad y que debe de aplicarse también a nivel de TO y no solo en los niveles de TIC.

Si bien el concepto de Ciberseguridad aún queda ambiguo podemos decir que la definición proporcionada por Kaspersky “la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, la redes y los datos de ataques maliciosos” es la más acertada en este contexto actual ya que agrega también sistemas electrónicos refiriéndose a los dispositivos de control y demás dispositivos electrónicos encontrado en las industrias.

Referente al marco normativo nacional se puede ver como el Paraguay está tomando cartas en el asunto. Desde el desarrollo de un Plan Nacional de Ciberseguridad donde nos habla de varios proyectos como la de aumentar la integración a las TIC, Plan de protección de a los Sistemas Críticos, la creación de un Centro de Respuestas a Incidentes Cibernéticos respaldado por la SENATIC y la OEA, entre otros.

En conclusión como Ingenieros Electromecánicos con Orientación en Electrónica no nos encontramos absentas ya que como lo fui mencionando a lo largo del trabajo es nuestro trabajo como futuros ingenieros proyectistas el tomar en cuenta estos nuevos desafíos y realizar un proyecto previendo estas situaciones que ya no son de un futuro cercano sino que ya son una realidad, y no solo como proyectistas sino también como ingenieros en automatismo, ingenieros encargados de mantenimiento, operadores, todos nosotros estaremos en contacto directo con estas situación y por ende es nuestro deber estar preparados para dichas situaciones.

## REFERENCIAS

- [1] L. Zhang, An Implementation of SCADA Network Security Testbed, 2015.
- [2] C. d. Wikipedia, «wikipedia,» 8 junio 2021. [En línea]. Available: <https://es.wikipedia.org/w/index.php?title=Metasploit&oldid=136189335>.
- [3] J. Weiss, Protecting Industrial Control Systems From Electronic Threats, New York: Momentum Press, 2010.
- [4] SENATIC, «Plan Nacional de Ciberseguridad,» 2017.
- [5] Secure&IT, «Secure&IT,» 2021. [En línea]. Available: <https://www.secureit.es/ciberseguridad-industrial/el-estandar-isa99-iec62443/>.
- [6] I. J. L. Salinas, «InTech Mexico Automatización,» 26 septiembre 2017. [En línea]. Available: <https://www.isamex.org/intechmx/index.php/2017/09/26/estandar-isa-95-integracion-de-los-sistemas-de-control-empresarial/>.
- [7] T. Safe, «O ESTADO DA SEGURANÇA CIBERNÉTICA NAS INFRAESTRUTURAS CRÍTICAS BRASILEIRAS,» Rio de Janeiro , 2018.
- [8] J. P. C. Quiñones y M. F. H. Quila, Analisis de riesgo y elaboracion de controles para un prototipo de control y automatizacion industrial en la empresa INTECNO SAS, Bogota, 2018.

- [9] I. Punzenberger, «COPADATA,» 2020. [En línea]. Available: <https://www.copadata.com/es/industrias/energia-infraestructura/energy-insights/dnp3-protocolo-de-red-distribuida/energy-infrastructure-2/>.
- [10] NIST 800-82, *NIST 800-82*, 2015.
- [11] S. Mukherjee, «Implementing Cybersecurity in the Energy Sector,» August 2019. [En línea]. Available: <https://www.researchgate.net/publication/335368810>.
- [12] C. ©. 2. S. Modbus, «Simply modbus,» 2020. [En línea]. Available: <http://www.simplymodbus.ca/FAQ.htm>.
- [13] M. Á. Mendoza, «welivesecurity,» 9 abril 2018. [En línea]. Available: <https://www.welivesecurity.com/las-2018/04/09/nueva-acepcion-de-la-rae-define-a-un-hacker-como-experto-en-computadoras/>.
- [14] T. B. B. L. C. d. M. J. S. J. d. A. J. Marcelo Ayres Branquinho, Segurança de Automação Industrial e SCADA, Rio de Janeiro: Elsevier Editora Ltda., 2014.
- [15] E. P. López, Los sistemas SCADA en la automatización industrial, 2015.
- [16] E. Knapp, Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems, Elsevier, 2011.
- [17] ©. 2. I. S. o. A. ISA, «International Society of Automation,» 2021. [En línea]. Available: <https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa99>.
- [18] INCIBE, «Incibe-Cert,» 24 enero 2019. [En línea]. Available: <https://www.incibe-cert.es/blog/estandar-iec-61850-todos-uno-y-uno-todos>.
- [19] INCIBE, «INCIBE,» 2017. [En línea]. Available: [https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia\\_glosario\\_ciberseguridad\\_metad.pdf](https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf).
- [20] D. Hadžiosmanović, The Process Matters: Cyber Security in Industrial Control Systems.
- [21] J. Gomar, «Profesional review,» 25 noviembre 2018. [En línea]. Available: <https://www.profesionalreview.com/2018/11/25/que-es-el-procesamiento-batch/>.
- [22] S. GlobalSUITE, «Solutions GlobalSUITE,» 2021. [En línea]. Available: <https://www.globalsuitesolutions.com/es/la-familia-de-normas-iso-27000/>.
- [23] I. G. Gallego, Estudio de la Ciberseguridad Industrial. Pentesting y Laboratorio De Pruebas De Concepto, 2018.
- [24] Electromecanic, «Automantenimiento.net,» 2013. [En línea]. Available: <https://automantenimiento.net/electricidad/tipos-de-plc/>.
- [25] K. O. D. G. a. J. S. David E. Whitehead, «Ukraine Cyber-Induced Power Outage: Analysis and Practical Mitigation Strategies,» 2017.
- [26] N. D. C. O. Cristian Carmona Cabrera, Pruebas de Penetración en la Infraestructura de la red de Comunicación del Centro Tecnológico de la Universidad del Cono Sur de las Américas, 2008.
- [27] V. Barrero y E. J. R. P. M. P. Oscar Bou, Estado de preparación en ciberseguridad del sector eléctrico en América Latina, PUNTOAPARTE, 2020.
- [28] J. A. G. Arias, Ciberseguridad aplicada a los Sistemas de Control Industrial con énfasis en el sector energético, Catalunya, 2017.
- [29] P. N. America, «PI North America,» [En línea]. Available: <https://us.profinet.com/tecnologia/profibus-es/>.
- [30] N. I. o. S. a. T. (NIST), «National Institute of Standards and Technology U.S. Department of Commerce,» 2021. [En línea]. Available: <https://www.nist.gov/>.
- [31] I. S. o. A. (ISA), «Internacional Society of Automation (ISA),» 2021. [En línea]. Available: <https://www.isa.org/>.
- [32] Wikipedia, «Wireshark,» 26 julio 2021. [En línea]. Available: <https://es.wikipedia.org/wiki/Wireshark>.
- [33] «Tutorial de Electrónica Básica,» 2020. [En línea]. Available: <http://tutorialesdeelectronicaabasica.blogspot.com/2020/04/que-es-el-sistema-de-control.html>.
- [34] Simply Modbus, «Simply Modbus,» 2020. [En línea]. Available: <https://www.simplymodbus.ca/FAQ.htm>.
- [35] Wikipedia, «Shodan,» 1 abril 2021. [En línea]. Available: <https://es.wikipedia.org/wiki/Shodan>.
- [36] Wikipedia, «RS-485,» 2021. [En línea]. Available: <https://es.wikipedia.org/wiki/RS-485>.
- [37] Rapid7, «Rapid7,» 2021. [En línea]. Available: <https://docs.rapid7.com/metasploit/metasploit-web-interface-overview/>.
- [38] Offensive Security, «Offensive Security,» 2021. [En línea]. Available: <https://www.offensive-security.com/metasploit-unleashed/armitage-post-exploitation/>.
- [39] NMAP.ORG, «NMAP.ORG,» sf. [En línea]. Available: <https://nmap.org/man/es/index.html>.
- [40] MICROSOFT, «MICROSOFT SECURITY INTELLIGENCE REPORT,» 2017.
- [41] LAPP España, «LAPP España,» 2021. [En línea]. Available: <https://lappespana.lappgroup.com/ethernet-industrial.html>.
- [42] INCIBE, «incibe-cert,» 02 enero 2018. [En línea]. Available: <https://www.incibe-cert.es/blog/convergencia-ti>.
- [43] IEC, IEC 61131-1, 2003.
- [44] MITIC, «Estado de la Ciberseguridad en el Paraguay,» 2019.
- [45] OVERTEL Tecnology System, «DOCPLAYER,» 2018. [En línea]. Available: <https://docplayer.es/87857256-Sistemas-mes-manufacturing-execution-system-sistema-de-ejecucion-de-manufactura.html>.
- [46] Digital Guide, «Digital Guide,» 06 noviembre 2020. [En línea]. Available: <https://www.ionos.es/digitalguide/servidores/seuridad/que-es-el-ethical-hacking/>.
- [47] Automación Micromecánica s.a.i.c, Curso 061, 2017.
- [48] Campus Internacional Ciberseguridad, «Campus Internacional Ciberseguridad,» 19 abril 2021. [En línea]. Available: <https://www.campusciberseguridad.com/blog/item/139-que-es-el-pentesting>.
- [49] BBC NEWS, «BBC NEWS,» 11 octubre 2015. [En línea]. Available: [https://www.bbc.com/mundo/noticias/2015/10/151007\\_iwonder\\_find\\_tecnologia\\_virus\\_stuxnet](https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_find_tecnologia_virus_stuxnet).