# Integración de un laboratorio de ciberseguridad OT en un laboratorio de automatización industrial

Alejandro Manuel López Gómez
Universidad Pontificia Comillas
Comunidad de Madrid
amanuellopezgomez@alu.comillas.edu

José Antonio Rodríguez-Mondejar
Universidad Pontificia Comillas
Comunidad de Madrid
mondejar@comillas.edu

Gregorio López
Universidad Pontificia Comillas
Comunidad de Madrid
gllopez@comillas.edu

Jaime Mohedano
Universidad Pontificia Comillas
Comunidad de Madrid
jaime.mohedano@alu.comillas.edu

Agustín Valencia
Fortinet
Comunidad de Madrid
avalencia@comillas.edu

Javier Jarauta
Universidad Pontificia Comillas
Comunidad de Madrid
jarauta@comillas.edu

Atanasio Carrasco
Centrales Nucleares Almaraz-Trillo
Comunidad de Madrid
jacm@cnat.es

Rafael Palacios
Universidad Pontificia Comillas
Comunidad de Madrid
palacios@comillas.edu

Roberto Gesteira-Miñarro
Universidad Pontificia Comillas
Comunidad de Madrid
rgesteira@comillas.edu

***Resumen*—Si la ciberseguridad en las Tecnologías de la Información (IT, Information Technology) es una persona adulta, la ciberseguridad en las Tecnologías Operativas (OT, Operational Technology) está aún en su infancia. Los desafíos únicos en materia de seguridad que presentan los entornos industriales requieren una formación que combine conocimientos de automatización industrial y ciberseguridad. Fruto de esta necesidad, en la Universidad Pontificia Comillas se ha puesto en funcionamiento un laboratorio dedicado a la formación en ciberseguridad en entornos industriales. Este laboratorio tiene como principal objetivo la concienciación y formación en seguridad industrial lógica a partir de diferentes escenarios, así como la investigación de posibles ataques y sus mitigaciones. En este artículo se detalla el nacimiento de este laboratorio en colaboración con Fortinet a partir de un laboratorio de automatización industrial preexistente. Se explicarán en detalle los escenarios realizados, desde ataques a máquinas Windows desplegadas en un entorno virtualizado a la realización de ataques a hardware real de control industrial, además de abordarse posibles mitigaciones como la activación de reglas de cortafuegos ó segmentación de redes.**

***Index Terms*—JNIC, Ciberseguridad, OT, Siemens, Fortinet**

**Tipo de contribución:** *Formación e innovación educativa*

## I. Introducción

La tendencia de los fabricantes de equipos de control a usar equipos y aplicaciones preparados para el sector IT, hace que crezca la importancia de tener un planteamiento de ciberseguridad bien definido en el entorno OT. Si bien las tecnologías de la información ofrecen numerosos beneficios en materia de conectividad y supervisión, también exponen a los sistemas de control industriales a nuevas amenazas.

En muchos aspectos, la ciberseguridad en OT se ha quedado rezagada con respecto a su contraparte en IT. Afortunadamente, según apunta un informe realizado por Fortinet en el año 2023 [1], la ciberseguridad OT ha empezado a recibir la atención que merece de los cargos directivos y de responsabilidad. Sin embargo, la mayoría de las organizaciones aún tienen mucho trabajo por hacer.

De cara a reforzar la postura en ciberseguridad de entornos OT, existen retos propios de este ambiente que dificultan la equiparación en seguridad con despliegues IT.

- Muchos equipos OT fueron desplegados antes de que la ciberseguridad se convirtiese en una preocupación primordial, y su reemplazo por equipos más actualizados no es sencillo o eficiente.
- Mientras que los sistemas IT se centran principalmente en la confidencialidad y la integridad de los datos, en los sistemas OT priman la disponibilidad y la seguridad operativa.
- Falta de concienciación y capacitación en ciberseguridad dentro de la comunidad OT. Existe una notable diferencia en la cantidad de recursos de formación en ciberseguridad disponibles en entornos IT y OT.

Desafortunadamente, los dos primeros puntos se pueden considerar inherentes al entorno industrial. Respecto al tercer punto comentado, es innegable que en el entorno OT existe una diferencia considerable en formación en ciberseguridad con el mundo IT.

Con la finalidad de ayudar a lograr esta tan necesaria equiparación en talento, en la Universidad Pontificia Comillas se ha puesto en marcha un laboratorio de ciberseguridad OT en colaboración con Fortinet, que permitirá formar y concienciar a alumnos de diferentes perfiles en materia de ciberseguridad OT desde un punto de vista práctico y realista.

En España actualmente existen organizaciones dedicadas al desarrollo e investigación, a mencionar se encuentran el proyecto ARISTEO de la fundación CIDAUT [2] ó los laboratorios de Ziur situados en Guipúzcoa [3]. Destacar también la red nacional de laboratorios de ciberseguridad industrial del INCIBE (Instituto Nacional de Ciberseguridad) [4]. Frente a las instalaciones previamente mencionadas, el laboratorio propuesto tiene objetivos didácticos, reforzando lo visto en clases teóricas previas con ejemplos y equipos realistas.

El laboratorio presentando en este artículo ofrece ocho puestos de trabajo en los que se pueden evaluar tanto estrategias y configuraciones defensivas, como ataques a dispositivos de todos los niveles. Desde diferentes sensores y sistemas operativos, pasando por PLCs [5] (Programmable Logic Controllers) de diferentes generaciones y teniendo en cuenta las conexiones a Internet que resultan indispensables en los entornos productivos de hoy. Se detallan el proceso de integración de un laboratorio de automatización industrial y un laboratorio de ciberseguridad OT.

Las soluciones de un portfolio completo de aplicaciones ciberseguridad (antimalware, sondas IDS e IPS, NGFW, sandboxes, Honeypots, SIEM,... ) ya han sido probadas en formato virtualizado en el Trabajo de Fin de Máster de José Rafael Martín Torre, dirigido por Agustín Valencia [6].

## II. Laboratorio de automatización industrial

El laboratorio de Automatización Industrial está formado por ocho puestos de trabajo y una minifábrica (Fig. 1) que simula una planta industrial conectada entre sí mediante una red Ethernet y una red Wi-Fi. El conjunto forma la red OT del laboratorio. Cada puesto de trabajo (Fig. 2) tiene una estación de trabajo con pantalla de 24" que actúa como estación de ingeniería, un PLC S7-1516-3 PN/DP (Fig. 3) del fabricante Siemens y un HMI (*Human-Machine Interface*) TP700 del mismo fabricante. Cuatro de los puestos tienen montados en el propio puesto una cámara para control de cada calidad por visión artificial y un sistema de lectura de etiquetas RFID (*Radio Frequency Identification*) con dos antenas.

La minifábrica representa una línea de fabricación formada por cuatro estaciones (Fig. 1). Cada una está atendida por un robot. Dependiendo de la estación, el robot es de tipo colaborativo (ABB GoFA) o de tipo industrial (ABB Swifty). Hay una cinta transportadora que comunica todas las estaciones. Dos de las estaciones tienen su propia cinta transportadora para tareas de buffering. El material circula entre las estaciones sobre palés, guiados con cambios de aguja y elevadores.

Asociados a cada cambio de aguja hay retenedores que evitan conflictos en la circulación de los palés. En cada puesto de trabajo existe también una cámara y un sistema de lectura de etiquetas de RFID. Esta combinación de elementos permite que el alumno esté en un entorno semi-industrial: hay fabricación representada por los robots que montan y desmontan objetos formados por piezas de LEGO, hay transporte de material gracias a las cintas accionadas mediante variadores de velocidad, hay control de calidad a través de las cámaras y trazabilidad mediante la lectura de etiquetas RFID montadas en los palés.

Todos los elementos, tanto de la minifábrica como de los puestos están conectados según el esquema de red mostrado en la Fig. 4. Esta red está formada por múltiples switches que permite la comunicación entre cualquier elemento de la minifábrica y de los puestos de trabajo. Existe una configuración de red tanto en estrella como en cascada. Esta última se consigue gracias a que la mayoría de los dispositivos tienen un switch interno de dos puertos. Los protocolos de comunicación usados son S7Comm, PROFINET y OPC UA.

Alrededor de la minifábrica hay desplegada una red de seguridad formada por un PLC de seguridad, setas de emergencia en cascada, detectores de puerta abierta, barreras de luz, cierres magnéticos y láseres de proximidad que utiliza como protocolo principal PROFIsafe, utilizando la misma red Ethernet.

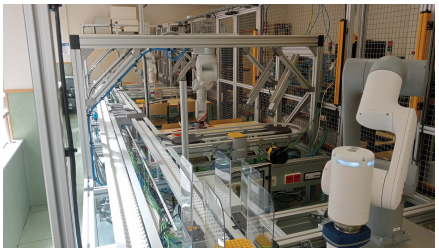

Figura 1. Minifábrica

Figura 2. Estaciones de ingeniería

Desde el punto de vista de la automatización, cada puesto está dotado de la herramienta TIA Portal para programar los PLC y resto de material del fabricante Siemens, y de la herramienta RobotStudio para programar los robots. Además, en cada puesto se pueden arrancar PLC virtuales, paneles virtuales y robots virtuales. Desde el punto de vista de conexión, sin entrar en los temas de ciberseguridad que se verán en el próximo apartado, cada puesto está conectado a la red corporativa de la universidad, a la red OT del laboratorio, y la red interna de dispositivos virtuales del puesto, que desde el punto de vista operación, siguen estando en la misma red OT. Todos los dispositivos del laboratorio están actualmente en el mismo dominio, aunque gracias a la red Wi-Fi, se pueden montar más dominios.

En este laboratorio los alumnos aprenden técnicas clásicas de automatización basadas en PLC y en robots y técnicas más avanzadas como integración (OPC UA) o de control de calidad por visión. El laboratorio es utilizado por alumnos de diferentes másteres: Ingeniería Industrial, Ingeniería de Telecomunicación, Ciberseguridad, Transformación Digital de la Industria, etc.

## III. Laboratorio de ciberseguridad OT

Este laboratorio tiene como objetivo ofrecer escenarios de aprendizaje sencillos para formar y concienciar al alumnado. En esta sección se describe a alto nivel el proceso de integración con el laboratorio de automatización industrial, así como los equipos desplegados. Además, se detalla a menor nivel el esquema de las conexiones realizadas.

Para reducir necesidades de espacio en el laboratorio, como es realizado en muchas industrias, el despliegue de herramientas de monitorización y detección de intrusiones se realiza de manera virtualizada en un servidor VMWARE ESXi, permitiendo además minimizar los cambios realizados


Figura 3. Equipo Siemens Simatic S7-1500

Figura 5. Equipo Siemens Simatic S7-300

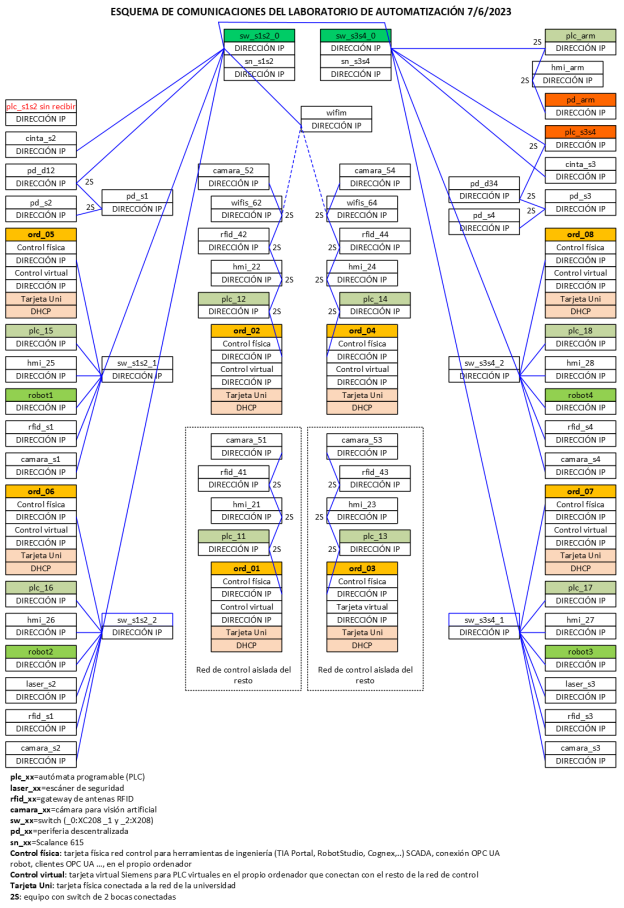


Figura 4. Esquema conectividad laboratorio A. Industrial

en las estaciones de trabajo. En este equipo se encuentran máquinas Kali Linux y Windows 11 para la realización de escenarios.

Aparte de los PLC S7-1500 usados en el laboratorio de automatización industrial, se han instalado también equipos Siemens Simatic S7-300 (Fig. 5). Los ataques realizados deben ser sencillos para que cumplan su finalidad formativa, por ello en ambos modelos de PLCs se emplean versiones de firmware vulnerables y comunicaciones no cifradas.

Una adecuada segmentación de los entornos IT y OT es fundamental. Es habitual realizarla acorde con el conocido modelo de Purdue [7] y las directrices de una red convergente extendida de planta, como la definida por Cisco y Rockwell [8]. Para el despliegue de los equipos se ha optado por seguir la pirámide de Purdue. Se emplea el cortafuegos avanzado NGFW FG-80F de Fortinet como zona desmilitarizada industrial (iDMZ), segmentando los equipos IT (nivel dos en el esquema mostrado en la Fig. 6, dedicado a la red de procesos) y OT (nivel uno en la misma figura, donde se encuentran los equipos de control). Gracias al acuerdo educativo con Fortinet se pueden dar formación en sus productos a los alumnos y usar herramientas virtuales que potencien las soluciones físicas.

Desde el punto de vista de la seguridad, idealmente todas las comunicaciones entre los distintos niveles de Purdue deberían realizarse a través de segmentación a nivel de aplicación y protocolo industrial (capa 7 en el modelo OSI [9]). Sin embargo, durante el proceso de integración de los laboratorios esto resultó imposible debido a la no exclusividad de uso del equipamiento, ya que se trata de un espacio compartido con otras titulaciones no relacionadas con la ciberseguridad industrial. Las conexiones que no siguen esta filosofía de segmentación se observan en el esquema simplificado de la Fig. 6 marcadas con un símbolo de peligro. Este resultado accidental se aprovecha para explicar a los alumnos como se debería realizar la segmentación de forma correcta y destacar el delicado balance entre la disponibilidad y la seguridad lógica en entornos OT.

El nuevo laboratorio requiere de una red aislada que permita la ejecución de diferentes pruebas sin posibilidad interferir con otros equipos ajenos al ejercicio. En la Fig. 7 se puede observar como se ha incorporado esta red (nuevos enlaces en rojo). En cada estación se obtiene una nueva conexión de red a través de adaptadores USB-Ethernet. Estos equipos se conectan a uno de los dos posibles switches conectados entre sí. Finalmente el switch de nivel superior es conectado al cortafuegos FG-80F. A este cortafuegos se conectan el resto de equipos, como es la red de automatización preexistente (red de la Fig. 4), los dos PLC S7-300 y la subred dedicada a las máquinas y herramientas virtualizadas. El resultado es la convivencia de ambos espacios de docencia e investigación donde los punto de interferencia son minimizados a lo estrictamente necesario.

## IV. Casos de uso realizados

Los escenarios realizados tienen la finalidad de mostrar a los estudiantes posibles ataques así como sus mitigaciones. En los casos de uso planteados, los estudiantes realizan ataques desde las máquinas Kali Linux situadas en el servidor VMWare a equipos PLC, actuando bajo la suposición de que el atacante (el alumno) ha conseguido previamente acceder a la red interna de la planta y, tras realizar un reconocimiento de red, ha logrado identificar la dirección IP de un PLC vulnerable. Estos escenarios han sido preparados para

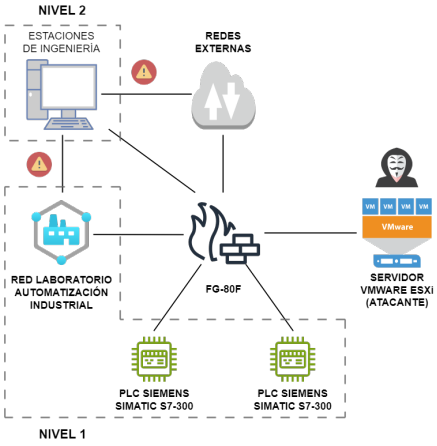


Figura 6. Esquema simplificado laboratorio ciberseguridad OT

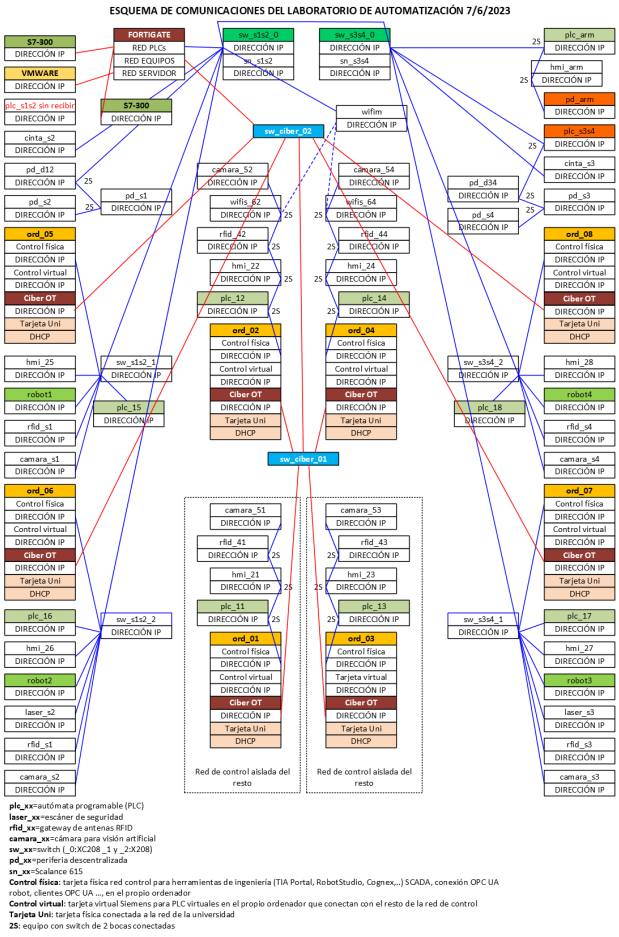


Figura 7. Esquema detallado conectividad laboratorio

reproducir situaciones reales de ataques a entornos industriales eliminando la complejidad de los mismos, ya que su propósito es formar a estudiantes sin experiencia en el campo de la ciberseguridad OT. En primer lugar el alumno realizará la acción ofensiva, para posteriormente aplicar las mitigaciones o salvaguardas necesarias.

### *IV-A. Ataque a maquinas Windows 11*

Este primer escenario pretende introducir a estudiantes sin experiencia a conceptos clave en ciberseguridad. Los alumnos aprenden acerca de la plataforma de tests de penetración *Metaesploit* [10] y la herramienta asociada para la generación *payloads msfvenom*. Los estudiantes preparan un archivo malicioso que permita abrir una sesión *meterpreter* en el objetivo.

Este fichero posteriormente es enviado mediante una conexión HTTP (*Hyper Text Transfer Protocol*) a la máquina víctima donde el fichero es ejecutado. En las máquinas Kali, se indica a los alumnos que deben arrancar la herramienta *multi handler*. El resultado debe ser la creación de una sesión *meterpreter* estable entre ordenador víctima y atacante.

Este ataque es fácilmente eludible mediante concienciación acerca de los peligros de ejecutar archivos desconocidos, mantener el equipo actualizado y emplear software antivirus. Este sencillo ejemplo es utilizado para concienciar a los alumnos sobre la necesidad de buenas prácticas en ciberseguridad, y como incluso los sistemas operativos más modernos y actualizados son vulnerables si no son utilizados de forma segura. A pesar de la simpleza del escenario en las prácticas de laboratorio realizadas este caso de uso demostró ser muy eficaz a la hora de captar la atención de los estudiantes y despertar su interés.

### *IV-B. Ataque START/STOP S7-300*

Los dispositivos PLC de Siemens utilizan un protocolo propio denominado S7Comm. Este protocolo sigue el enfoque tradicional de cliente-servidor. La comunicación se basa en peticiones y respuestas que emplean una serie de códigos de funciones conocidos por ambos extremos de la comunicación. Los códigos de funciones presentan un valor fijo, y en el resto del protocolo no existe ninguna variabilidad, por lo que los paquetes enviados siempre poseen la misma estructura y valores I.

Tabla I
CÓDIGOS DE FUNCIÓN S7COMM [11]

| Función | Código Hexadecimal |
|---|---|
| Setup Comunicación | 0xf0 |
| Lectura / Escritura | 0x04/0x05 |
| Descarga / Subida | 0x1a-1f |
| Control PLC | 0x28 |
| **Stop PLC** | **0x29** |

Un atacante podría capturar diferentes paquetes y retransmitirlos al equipo para provocar comportamientos indeseados, un ejemplo de esto es el script escrito por Dillon Beresford [12], que emplea paquetes preparados para arrancar o detener el PLC.

Este ataque es efectivo debido a que el protocolo S7Comm no incorpora seguridad por defecto, lo que permite realizar comandos de nivel administrativo sin necesidad de una autenticación previa [13].

Para solucionar este problema, Siemens ha incluido en versiones más recientes del protocolo mecanismos de autenticación por contraseña para acciones administrativas. Sin embargo, se ha demostrado que es viable obtener las claves secretas a partir de capturas de tráfico o de los propios ficheros de configuración del PLC.

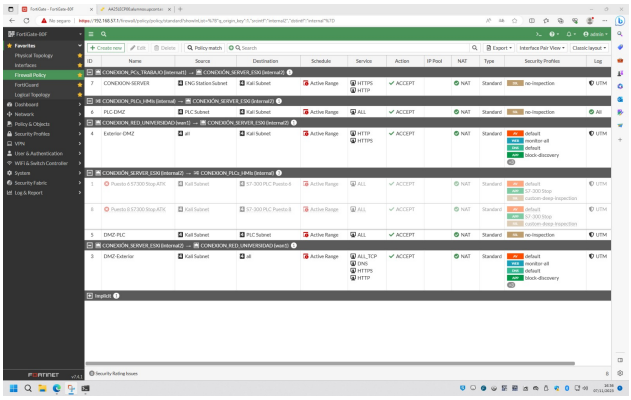

Figura 8. Politicas FG-80F

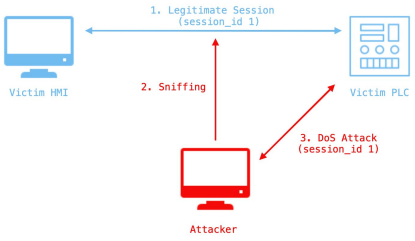


Figura 9. Esquema secuestro y suplantación (primer enfoque)

La mitigación que se enseña en el laboratorio para este ataque consiste en aplicar reglas de NGFW en un nivel superior al equipo industrial. El cortafuegos FG-80F cuenta con la licencia de Fortinet para la protección de protocolos industriales, que otorga las capacidades de análisis y disección de los mismos, así como aplicar reglas de detección o prevención logrando evitarse acciones maliciosas. Para evitar una orden STOP PLC maliciosa, se utilizan las reglas mostradas en la Fig. 8. De esta forma, se ofrece una protección granular sin afectar al entorno de producción.

### *IV-C. Manipulación de sesión S7-300*

Se trata de un ataque de denegación de servicio que afecta a la sesión de comunicación. Se puede realizar siguiendo dos enfoques diferentes.

- Secuestro y suplantación de la sesión de comunicación del PLC con un HMI legítimo.
- Establecimiento de una nueva sesión suplantando un supuesto HMI nuevo comunicándose con el PLC.

La comunicación se realiza a través del protocolo S7Comm, que a diferencia de su versión más reciente, S7CommPlus, no utiliza cifrado. Además de la ausencia de cifrado el ataque aprovecha el hecho de que en la comunicación no se verifique el *checksum*, ni a nivel de IP (*Internet Protocol*) ni a nivel de TCP (*Transmission Control Protocol*).

Para realizar el ataque siguiendo el primer enfoque (Fig. 9), se intercepta un paquete desde el HMI al PLC; ya sea de escritura, porque el operador busque modificar alguna variable del PLC o, de lectura, por el ciclo de lectura ya comentado. El paquete interceptado sirve para obtener el puerto TCP origen usado por el HMI y los números de secuencia y de ACK de la comunicación TCP. Cabe mencionar que en la comunicación

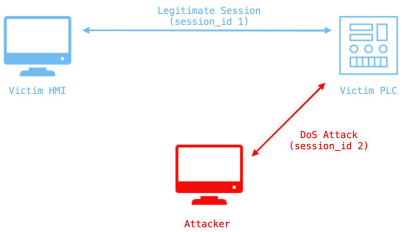


Figura 10. Esquema creación de nueva sesión (segundo enfoque)

entre el PLC y el HMI, existe una variable de ciclo de lectura que sirve al HMI para actualizar los valores que tiene de las variables del PLC.

Para el segundo enfoque (Fig. 10), no es necesario esperar a capturar un paquete legítimo ya que no se necesitan números de secuencia ni puerto del HMI, pues se trata de una nueva sesión y estos valores pueden ser aleatorios. Adicionalmente al primer enfoque, se requiere, en primer lugar, realizar el establecimiento tanto de TCP, mediante el TCP *handshake*, como de los protocolos de capas superiores, COTP y S7Comm.

Independientemente del enfoque, tras estos pasos, se envían paquetes de escritura en bucle para actualizar una variable del PLC continuamente, de tal forma que este sature y no responda cuando el HMI legítimo intente enviarle un paquete. Durante este envío continuo es necesario actualizar los números de secuencia y de ACK de nivel TCP de los paquetes, además de enviar los correspondientes paquetes de ACK a las respuestas provenientes del PLC.

La mitigación recomendada para este tipo de ataques consiste en aplicar reglas en el NGFW que bloqueen el tráfico procedente de fuera de la red del laboratorio con puerto destino el 102, puerto para el protocolo S7Comm, en conjunto con una lista blanca de los dispositivos presentes en el laboratorio. Aun así, como se ha demostrado en el ataque, es posible la suplantación de un dispositivo legítimo estando dentro de la red del laboratorio. Por ello, adicionalmente, se recomiendan medidas disponibles en el NGFW FG-80F como la limitación del ancho de banda para restringir el uso excesivo de recursos de red por dispositivos individuales y la propia protección contra ataques DoS que posee este dispositivo, la cual detecta y bloquea patrones de tráfico que indiquen este tipo de ataques.

### *IV-D. Extracción de listas SZL*

Las listas SZL (del alemán System-ZustandsListen) son listas que permiten conocer el estado actual del equipo de solo lectura. Estas listas y la información que contienen se pueden obtener sin necesidad de una autenticación previa, pudiendo ser utilizadas por un potencial adversario para labores de reconocimiento previas a un ataque. Un ejemplo sencillo sería obtener el número de equipo, como se muestra en la Fig. 11. Una rápida búsqueda en Internet devolverá el equipo PLC en cuestión. Se puede conseguir otra información de igual o incluso mayor criticidad. La contramedida enseñada para detener esta acción es muy similar a la descrita anteriormente, aplicar reglas en el NGFW bloqueando el tráfico S7Comm procedente de fuera del exterior de la red en junto con una lista blanca de los dispositivos permitidos.

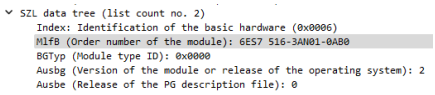


Figura 11. Extracción identificador del equipo

### *IV-E. Ataque DoS S7-1500*

Este ataque de denegación de servicio aprovecha una vulnerabilidad [14] en el monitor de recursos usado en los equipos PLCs de la familia S7-1500. A través del envío continuado de paquetes UDP maliciosos el atacante provoca el uso de un gran número de recursos que puede llevar al agotamiento de los mismos, provocando la ralentización e incluso la detención de actividades legítimas. Este ataque puede ser realizado sin necesidad de una autenticación previa.

De nuevo la mitigación para evitar este ataque consiste en el uso de reglas en el NGFW respecto a la cantidad y el tipo de tráfico generado. En un futuro con la instalación de herramientas como FortiSIEM se espera expandir este escenario, permitiendo al alumnado monitorizar y actuar en tiempo real.

### *IV-F. Acceso con OPC UA*

En esta práctica se familiariza al alumno con el uso de OPC UA a través de un ejemplo de automatización. La lógica de la automatización consiste en abrir y cerrar el cajón continuamente durante el tiempo programado, para comprobar que no hay fallo de las guías en las que se apoya el cajón. La automatización ha sido realizada programando el PLC del laboratorio utilizando el lenguaje GRAFCET (GRAPH en el argot de Siemens). Además, se ha configurado el panel del laboratorio para controlar y supervisar de manera simplificada la operación del test de guías de cajón. También es objetivo de la práctica familiarizar al alumno con el uso del lenguaje o metodología GRAFCET.

Desde el punto de vista de formación en ciberseguridad OT, la conexión descrita en el párrafo anterior es insegura. Como contramedida, se emplean certificados digitales para cifrar la comunicación y forzar la autenticación entre cliente y servidor. La práctica muestra la complejidad que puede suponer la instalación y el mantenimiento de la ciberseguridad en el mundo OT.

## V. Siguientes pasos

En un futuro cercano, se espera ampliar aun más los casos de uso y capacidades del laboratorio para ofrecer una experiencia de aprendizaje más enriquecida y diversa. Actualmente se está trabajando en lo siguiente.

- Instalación de más aplicaciones de ciberseguridad de Fortinet, prefiriéndose en formato virtualizado como el ya probado en [6], mejorando la implementación del modelo Purdue y aumentando la formación dada en el manejo de sistemas de monitorización, detección y prevención de intrusos.
- Investigación en otros posibles ataques y mitigaciones en equipos de la familia S7-1500. Utilizar equipos más actuales y con mejores medidas de seguridad aumentará el realismo de los escenarios realizados y mejorará la preparación dada a los alumnos.
- Diseño de un acceso remoto seguro a los recursos del laboratorio, simulando lo ya conseguido en muchos entornos industriales.
- Despliegue de soluciones de dominios virtuales (VDOM) [15] para accesos individualizados desde cada una de las estaciones de trabajo. En las prácticas realizadas con el alumnado, se generaba confusión al tener a varios estudiantes manipulando las mismas reglas dentro de un mismo equipo.
- Desarrollo de prácticas de ataque al nivel de sensores (nivel 0 del modelo de Purdue), tanto a nivel de Wi-Fi interna como a nivel de conexiones IoT externas.
- Llegar a formar parte de la red de laboratorios de ciberseguridad industrial del INCIBE (Instituto Nacional de Ciberseguridad).

## VI. Conclusiones

El laboratorio de ciberseguridad OT de la Universidad Pontificia Comillas, ha permitido a varias promociones de estudiantes de diferentes titulaciones un aprendizaje práctico más allá de los conceptos teóricos.

En este artículo se ha descrito el nacimiento de este laboratorio a partir de un laboratorio de automatización industrial preexistente. Se han explicado los retos de despliegue, destacando la necesidad de garantizar la coexistencia sin interferencias entre ambos y la segmentación de ambas redes minimizando los puntos de conexión (Fig. 4) y 7) teniendo en cuenta las limitaciones debido a la necesidad de mantener conexiones que desde un punto de vista de Purdue son inseguras (conexiones marcadas en la Fig. 6 con un símbolo de peligro).

Posterior al despliegue se han comentado los escenarios realizados. A destacar se encuentran los escenarios que tratan directamente con hardware, en concreto los equipos PLC S7-300 5, utilizado para los escenarios de START/STOP IV-B y manipulación de sesión IV-C, y S7-1500 3, empleado los escenarios de lectura de listas SZL IV-D y ataque de denegación de servicio IV-E.

Respecto al futuro de este laboratorio, aparte de las mejoras técnicas comentadas como el despliegue de soluciones VDOM o la instalación de más herramientas de Fortinet, uno de los objetivos más relevantes es lograr formar parte de la red de laboratorios de ciberseguridad industrial del INCIBE.

Con la creciente preocupación por la ciberseguridad en industriales es evidente que en un futuro no tan lejano serán necesarios más profesionales especializados en ciberseguridad OT y responsables familiarizados y concienciados con ella. Desde el equipo responsable del laboratorio, se tiene la convicción de que estas prácticas ayudan a los estudiantes a entender la necesidad de asegurar los sectores industriales y de infraestructuras críticas y permiten formar profesionales con experiencia en equipos y escenarios realistas. Mediante innovaciones educativas, como este laboratorio de ciberseguridad industrial, se espera contribuir a reducir la brecha entre los mundos de la ciberseguridad IT y OT y lograr entornos industriales donde la ciberseguridad se convierta en un pilar fundamental.

## Referencias


[1] Fortinet: ”2023 State of Operational Technology and Cybersecurity Report”. Accedido: Mayo 4, 2024.
[2] CIDAUT: ”Proyecto ARISTEO”. Accedido: Mayo 2, 2024.
[3] Ziur: ”Ziur”. Accedido: Mayo 2, 2024.
[4] INCIBE-CERT: ”Red Nacional de Laboratorios de Ciberseguridad Industrial”. Accedido: Marzo 22, 2024.
[5] Wikipedia: ”Programmable logic controller”. Accedido: Marzo 17, 2024.
[6] José Rafael Martín Torre, Agustín Valencia Gil-Ortega: ”Despliegue de arquitecturas e implementación de medidas de ciberseguridad.”Trabajo Fin de Master en Madrid, España:*Universidad Pontificia Comillas*, Junio 2023.
[7] Dean Parsons: ”2023’s Challenges and Tomorrow’s Defenses”, en *SANS ICS/OT Cybersecurity Survey*, Septiembre 2023.
[8] Cisco: ”Enabling a Converged Plantwide Ethernet (CPwE) network”. Accedido: Marzo 17, 2024.
[9] Cloudfare: ”Modelo OSI”. Accedido: Mayo 2, 2024.
[10] Metaesploit Framework. Accedido: Marzo 21, 2024.
[11] gmiru: ”The Siemens S7 Communication”. Accedido: Marzo 19, 2024.
[12] exploit-db: ”Siemens Simatic S7-300/400 - CPU START/STOP Module (Metasploit)”. Accedido: Marzo 18, 2024.
[13] P. Ackerman: Ïndustrial Cybersecurity: Efficiently Secure Critical Infrastructure Systems..[en] Birmingham, Reino Unido: Packt Publishing, 2017.
[14] NIST: ”CVE-2019-19281”. Accedido: Marzo 18, 2024.
[15] Fortinet: VDOM. Accedido: Mayo 2, 2024.