UNIVERSITAT POLITÈCNICA DE VALÈNCIA

_ TELECOM ESCUELA TÉCNICA VLC SUPERIOR DE INGENIERÍA DE TELECOMUNICACIÓN

APLICACIÓN DE SIEMS A LA PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

Vázquez Puig, Arturo

Tutor: Esteve Domingo, Manuel

Trabajo Fin de Grado presentado en la Escuela Técnica Superior de Ingenieros de Telecomunicación de la Universitat Politècnica de València, para la obtención del Título de Graduado en Ingeniería de Tecnologías y Servicios de Telecomunicación

Curso 2019-20

Valencia, 29 de octubre de 2020

Escuela Técnica Superior de Ingeniería de Telecomunicación
Universitat Politècnica de València
Edificio 4D. Camino de Vera, s/n, 46022 Valencia
Tel. +34 96 387 71 90, ext. 77190
www.etsit.upv.es

VLC/ CAMPUS VALENCIA, INTERNATIONAL CAMPUS OF EXCELLENCE

EMAS Gestión ambiental verificada REG.NO. ES-CV- 000030

Resumen

El documento que se presenta a continuación, se centra en la utilización de una categoría de software conocida como SIEMs (Gestión de Eventos e Información de Seguridad) para la defensa de Infraestructuras Críticas, en cuanto a monitorización y detección de ataques a las mismas, haciendo hincapié en los ICS (Sistemas de Control Industrial) y los sistemas SCADA (Control de Supervisión y Adquisición de Datos); los cuales se caracterizan por tener una parte que interactúa con el mundo físico, y otra más enfocada al mundo cibernético.

Primeramente, se definirá qué es lo que se conoce como una Infraestructura Crítica, repasando tanto los sistemas ICS y SCADA para así poder caracterizar los componentes ciber-físicos de estas; particularmente los CPS (Sistemas Ciber-Físicos) frente a los sistemas IT (Tecnología de la Información).

Seguidamente, se pasará a definir qué son los SIEMs, así como su funcionamiento; con el objetivo final de conocer cómo se emplearían dichos SIEMs a la hora de proteger los CPS de una Infraestructura Crítica.

Resum

El document que es presenta a continuació, es centra en la utilització d'una categoria de software conegut com a SIEMs (Gestió d'Esdeveniments i Informació de Seguretat) per a la defensa d'Infraestructures Crítiques, en quant a monitorització i detecció d'atacs a estes, fent èmfasi en els ICS (Sistemes de Control Industrial) i els sistemes SCADA (Control de Supervisió i Adquisició de Dades); els quals es caracteritzen per tindre una part que interactua amb el món físic, i una altra més enfocada a el món cibernètic.

Primerament, es defineix que és el que es coneix com una Infraestructura Crítica, repassant tant els sistemes ICS i SCADA per així poder caracteritzar els components ciber-físics d'aquestes; particularment els CPS (Sistemes Ciber-Físics) enfront dels sistemes IT (Tecnologia de la Informació).

Seguidament, es passarà a definir què són els SIEMs, així com el seu funcionament; amb l'objectiu final de conèixer com s'emprarien aquests SIEMs a l'hora de protegir els CPS d'una Infraestructura Crítica.

Abstract

The document presented below focuses on the use of a software category known as SIEMs (Security Information and Event Management) for the defense of Critical Infrastructures, in terms of monitoring and detecting attacks on them, making emphasis on ICS (Industrial Control Systems) and SCADA (Supervisory Control and Data Acquisition) systems; which are characterized by having a part that interacts with the physical world, and another more focused on the cybernetic world.

Firstly, it is defined what is known as a Critical Infrastructure, focusing on ICS and SCADA systems in order to characterize their cyber-physical components; particularly CPS (Cyber-Physical Systems) on IT systems (Information Technology).

In addition, we will define what SIEMs are, as well as how they work; And the final objective of knowing how SIEMs would be used when protecting CPS from a Critical Infrastructure.

Índice

Capítulo 1. Objetivos de este TFG 2
Capítulo 2. Introducción 3
2.1 Infraestructura Crítica 3
2.2 SIEM 3
2.3 Amenazas y ataques 3
2.3.1 Man-in-the-Middle 3
2.3.2 Usurpación de credenciales 3
2.3.3 Inyección SQL 3
2.3.4 Ransomware 4
2.3.5 DoS (Denegación de Servicio) 4
2.3.6 Gusano informático 4
2.3.7 Ataque a componentes físicos 4
Capítulo 3. Caracterización de Infraestructuras Críticas 5
3.1 ICS (del inglés, Industrial Control System) 5
3.2 Smart Grid o Redes Inteligentes 7
3.3 Dispositivos médicos 9
3.4 Vehículos inteligentes 10
Capítulo 4. SIEMs, soluciones de detección y mitigación de ataques 13
4.1 ICS (del inglés, Sistemas de Control Industrial) 13
4.2 Smart Grids o Redes Inteligentes 14
4.3 Dispositivos médicos 15
4.4 Vehículos inteligentes 15
Capítulo 5. Conclusiones 17
Capítulo 6. Anexo 18
Capítulo 7. Bibliografía 19
Capítulo 8. Figuras 20

Capítulo 1. Objetivos de este TFG

Los objetivos de este Trabajo de Fin de Grado son los que se presentan a continuación:

- Definir qué es una Infraestructura Crítica.
- Identificar los diferentes tipos de Infraestructuras Críticas, así como sus componentes ciber-físicos y las diferentes vulnerabilidades de los mismos.
- Definir qué es un SIEM y cuál es su funcionamiento.
- Aplicar los conocimientos obtenidos sobre IC y SIEMs para establecer unas defensas frente a posibles ataques.
- Establecer futuros desafíos para la ciberseguridad.

Capítulo 2. Introducción

A continuación, se pasará a realizar un primer esbozo de todo lo mencionado previamente, en referencia a los SIEM, Infraestructuras Críticas, así como los componentes y sistemas ciber-físicos.

2.1 Infraestructura Crítica

El concepto de Infraestructura Crítica es muy amplio, pero en pocas palabras, son infraestructuras que nos ofrecen servicios esenciales e indispensables, y que en la mayoría de los casos no existe una solución alternativa, por lo que la manipulación maligna o accidental de su comportamiento 'normal' o incluso su destrucción generaría un gran impacto en los servicios ofrecidos.

Para ponernos más en contexto, algunos ejemplos de Infraestructuras Críticas podrían ser desde redes de información, instalaciones industriales, Centrales Eléctricas, hasta producción, almacenamiento o transporte de mercancías peligrosas, o también algunos dispositivos médicos como los marcapasos.

2.2 SIEM

En grandes rasgos, podríamos definir el concepto de SIEM como un tipo de software que permite a la infraestructura que monitoriza obtener información que puede ser relevante a la hora de detectar posibles amenazas o intrusiones de seguridad. Esto es posible gracias a que recaba información de los diversos sistemas que componen nuestra infraestructura o nuestra organización. Para ello es necesario conocer bien nuestro sistema, o lo que es lo mismo, caracterizarlo; descubriendo todos los activos y posibles puntos de intrusión para un ataque. Algunos ejemplos de SIEM del mercado son *Shodan* o *Alien Vault*.

2.3 Amenazas y ataques

Un intruso puede entrar de diversas maneras en nuestro sistema, incluso combinando distintos métodos simultáneamente con el fin de lograr un ataque de mayor impacto. Algunos de los que se tratan en siguientes puntos son los siguientes:

2.3.1 Man-in-the-Middle

En este tipo de ataques, el intruso adquiere la capacidad de situarse 'en medio' de las comunicaciones, pudiendo leer las comunicaciones, modificar los mismos o incluso generar su propio tráfico haciéndose pasar por uno de los dos interlocutores. El siguiente esquema nos presenta un esquema sencillo de qué es a lo que nos referimos.

2.3.2 Usurpación de credenciales

Este tipo de amenaza compromete las claves de acceso de uno o varios entes dentro de nuestro sistema, la cual otorgaría al intruso poder dentro de nuestra organización. Dicha amenaza puede ser generada mediante ingeniaría social, con correos cuyo remitente no es quien dice ser; *Eavesdropping* también conocido como 'escuchas', *Skimming* o clonación de tarjetas, fuerza bruta o diccionarios que se utilizan para probar palabras clave, o *keylogger* que recogen todas las entradas del teclado, incluso mediante *Phising*. Estos son algunos de los métodos más utilizados para la usurpación de credenciales.

2.3.3 Inyección SQL

Este tipo de ataques se centran en aprovechar una vulnerabilidad de un sistema que ejecuta SQL, y el cual opera con las variables de forma incorrecta. De esta forma se pueden llegar a obtener los

nombres de usuario, información confidencial, o incluso contraseñas; realizando una serie de consultas. Es por esto que se recomienda la parametrización de sentencias SQL con la sentencia del tipo *PreparedStatement* para evitar este tipo de amenazas.

2.3.4 Ransomware

Software que "secuestra" uno o varios equipos a base de cifrar los archivos de datos con claves de gran tamaño.

2.3.5 DoS (Denegación de Servicio)

Los ataques por Denegación de Servicio se fundamentan en que fuerzan a una red o sistema a dejar de dar el servicio, o parte de este, al resto de usuarios legítimos. En su mayoría son provocados por colapsos debido a la congestión y consumo de recursos, pero también puede verse provocado por el ataque a componentes físicos de dicho sistema o la obstrucción de la comunicación entre un usuario y un servicio.

En un nivel superior, encontramos los DDoS (del inglés, *Distributed Denial of Service*), en el cual un grupo de máquinas distribuidas apuntan a un mismo servidos, inhabilitando este inmediatamente.

2.3.6 Gusano informático

Este tipo de *malware* es utilizado por los atacantes para que se reproduzca por el resto de equipos de la red de nuestro sistema, una vez ha conseguido llegar a uno de ellos puede simplemente reproducirse en los demás equipos, sin causar daño real, para más tarde ser utilizado como *backdoor* para otro tipo de virus o *malware*. Pero hay otros casos en los que este tipo de *malware* también puede ser usado para causar daños a los equipos, ralentizando los mismos, o incluso ralentizando el tráfico de la red, puesto que su finalidad principal es la propagación.

Existen diversas formas por las que puede propagarse el gusano, lo más común es que se utilicen conexiones P2P o mediante correo electrónico.

Uno de los gusanos informáticos más conocidos es **STUXNET**, el cual podría considerarse una de las primeras armas cibernéticas, y cuyo objetivo son los sistemas de control industrial (ICS/SCADA) que veremos detenidamente en capítulos posteriores.

2.3.7 Ataque a componentes físicos

En otros casos, se puede llegar a atacar a componentes físicos, ya sea con su inutilización porque son estaciones alejadas de nuestra organización y por lo tanto más difíciles de proteger y vigilar; o porque se consigue inyectar tráfico malicioso haciendo creer al sistema que esos datos se están obteniendo de un componente físico legítimo.

Capítulo 3. Caracterización de Infraestructuras Críticas

Se entiende por 'Caracterización' de un sistema, el conocimiento de todos los activos y posibles focos de ataque, así como de sus vulnerabilidades o posibles fallas del Sistema.

Seguidamente, pasaremos a la caracterización de los distintos tipos de Infraestructura Crítica, ya definida en la introducción, así como de sus distintos tipos de Sistema.

Dentro de las infraestructuras críticas podemos encontrar diferentes sistemas, los cuales pueden ser el foco de ataques para modificar el correcto funcionamiento de nuestra infraestructura, o incluso dejar sin servicio la misma.

3.1 ICS (del inglés, Industrial Control System)

El término ICS se refiere a sistemas de control, monitorización y producción de en diferentes industrias como centrales nucleares, sistemas de aguas residuales…

Los **sistemas de control industrial** muestran un conjunto de procesos, el más común es:

SCADA: concepto que se emplea para realizar un software para ordenadores que permite controlar y supervisar procesos industriales a distancia. Dentro de estos sistemas encontramos diversas redes, destinadas al control o almacenamiento de información, en las cuales encontramos y diferenciamos diversos activos:

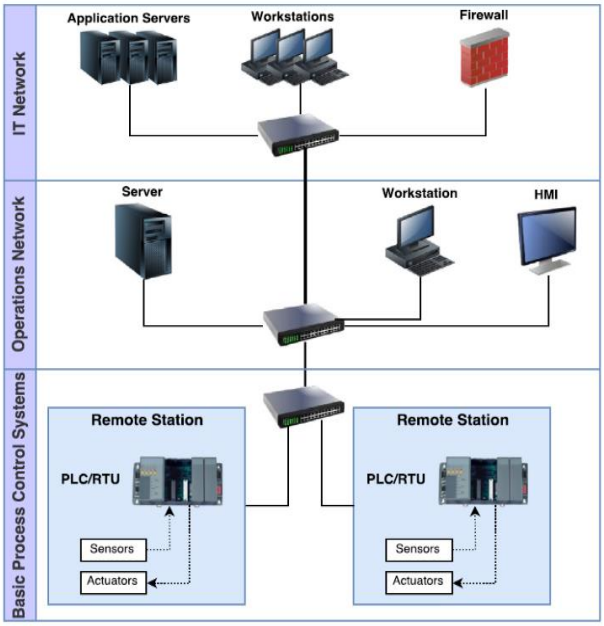

Figura 1. Sistema SCADA.[i]

- **Red IT (en la figura 2. *IT Network*)**: Hace referencia a la red de tecnologías de la información, en la cual podemos encontrar: Los servidores de aplicación, estaciones de trabajo y el firewall.
- **Red de Operaciones (*Operations Network*)**: Es la red de operaciones, la cual consta típicamente de los servidores internos, estaciones de trabajo y HMI (del inglés, *Human-Machine Interface*).
- **Systemas de control de procesos básicos (*Basic Process Control Systems*)**: Donde se encuentran las estaciones remotas como PLCs (del inglés, *Programmable Logic Controllers*), en las cuales encontramos sensores y transmisores, que permitirán manipular nuestro sistema de forma remota.

Algunas de las vulnerabilidades son debidas a que la fiabilidad del sistema a menudo puede ser prioritaria a las amenazas de seguridad, ya que la operatividad de SCADA debe ser continua, por lo que resulta más complicado **aplicar actualizaciones** o modificar componentes de dicho sistema.

Por otro lado, la **ausencia de cifrado** en protocolos de comunicación entre las distintas redes vistas anteriormente y entre componentes internos; sumado a que los protocolos están bien documentados y las soluciones de hardware disponibles. Si bien esto último no es un mecanismo de seguridad per se, la obtención de estos datos por parte de un atacante agilizaría un intento de ataque hacia nuestro sistema.

La seguridad de las redes SCADA se está volviendo cada vez más complicada, debido a que están conectadas con las redes IT, con la finalidad de permitir una comunicación más rápida; este hecho provoca nuevos riesgos y amenazas en las comunicaciones relacionadas con SCADA.

Uno de los grandes problemas es que un gran porcentaje de los **ataques se producen desde el interior**, donde la **defensa perimetral** únicamente, **no puede proteger al sistema**. Se ha comprobado que, a pesar de la gran variedad de ataques a la dinámica del sistema, gran parte de estos surgen a raíz de un error humano. Para fortalecer este tipo de vulnerabilidades internas en los sistemas SCADA, se propone una solución de defensa en profundidad, por capas de seguridad, es decir, se introducen barreras y múltiples controles para proteger los activos con la intención de la amenaza tenga más dificultades para acceder al sistema.

Uno de los ataques más conocidos a este tipo de sistemas es el del virus **STUXNET**, el cual fue diseñado para atacar y controlar las PLCs mencionadas anteriormente. Este virus ha propiciado la necesidad de aumentar la inteligencia y control de los equipos y dispositivos, como RTUs (del inglés, *Remote Terminal Units*), sensores, válvulas, etc, los cuales se utilizan para influir en el comportamiento del sistema.

Por otro lado, encontramos comunicaciones **CPS** (del inglés, *Cyber-Physical Systems*), en concreto en un ICS encontramos 2 categorías distintas:

- Una dedicada a la automatización y control, como Modbus o DNP3 (del inglés, *Distributed Network Protocol*).
- Otra dedicada a la interconexión de centros de control ICS, como ICCP (del inglés, *Inter-Control Center Protocol*).

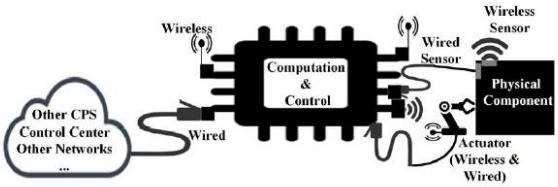

Figura 2. Modelo esquemático de un CPS[ii]

Centrándonos en las **ciber-vulnerabilidades** en relación a la dependencia de los ICS de los protocolos estándares como TCP/IP e ICCP es cada vez mayor. Esto genera una vulnerabilidad ya que, pese a que han sido estudiados e investigados durante años, estos protocolos no fueron diseñados en sus inicios como protocolos seguros. Por ejemplo, el ICCP carece de medidas de seguridad como el cifrado o la autenticación. Otro protocolo conocido es el RPC (del inglés, *Remote Procedure Call*), el cual presenta una serie de vulnerabilidades, las cuales propiciaron el mencionado ataque STUXNET.

Las **comunicaciones por cable** pueden ser tanto de fibra óptica, como Ethernet. Este último generalmente usado en redes de área local en subestaciones, debido al medio de las comunicaciones Ethernet, este es vulnerable al ataque conocido como *Man-In-The-Middle*, por el cual un atacante interno en nuestra red podría hacerse pasar por componentes legítimos de nuestro sistema, inyectar datos falsos o divulgar información confidencial o vulnerable. En cuanto a las **comunicaciones inalámbricas** de corto alcance, se utilizan normalmente dentro de la planta de ICS, suponiendo que un atacante no puede acercarse lo suficiente como para poder capturar el tráfico inalámbrico. Pese a esto, dicho tráfico aun es vulnerable a ser capturado, analizado o manipulado por algún agente malicioso. Asimismo, debemos tener en cuenta los dispositivos de los empleados que se conectan a la red inalámbrica, los cuales podrían ser un vector de ataque. Como resumen sobre las comunicaciones en ICS, podemos afirmar que las comunicaciones inalámbricas son más vulnerables a ciberataques, escuchas activas y pasivas, ataques de repetición, entre otros.

Adicionalmente, nos encontramos con otra ciber-vulnerabilidad conocida como inyección SQL, por medio de la cual, un atacante podría tener acceso a la base de datos sin necesidad de autorización.
Por otro lado, nos encontramos también con **vulnerabilidades ciber-físicas**, en relación a las comunicaciones entre los distintos componentes ICS, mediante protocolos como Modbus y DNP3 para controlar y monitorizar, desde el centro de control a los distintos sensores y demás componentes físicos. La carencia de encriptado en el tráfico expone al mismo a ataques de espionaje. Igualmente, debido a que no existe un proceso de autenticación, existe la posibilidad de que la integridad de los datos pueda verse comprometida. A pesar de esto, sí existe un código de **verificación de errores por redundancia** (CRC) que, pese a ser un mecanismo muy simple, es preferible a no verificar nada en absoluto. Dentro de este tipo de vulnerabilidades ciber-físicas, encontramos otra relacionada con dispositivos como PLCs y RTUs, pero más que una vulnerabilidad física como la mencionada antes, en este caso tiene relación con que estos no aplican ninguna medida de control de acceso, otorgando el máximo nivel de privilegios a cualquiera que logre acceder; esto convierte a cualquier ordenador o portátil que se conecte a dichos dispositivos, en potenciales vectores de ataque, pudiendo llegar a afectar a los componentes físicos. Este tipo de vulnerabilidades son explotadas, por el ataque STUXNET entre otros.

En cuanto a **vulnerabilidades físicas** debemos tener en cuenta que gran parte de los componentes están expuestos y dispersos en un área de gran superficie, como PLC, RTU y demás sensores. Por lo que una seguridad física insuficiente de los mismos, los vuelve vulnerables a manipulaciones o incluso sabotaje.

3.2 Smart Grid o Redes Inteligentes

Una *Smart Grid* es un sistema que podemos considerar el siguiente escalón de los sistemas de red eléctrica; el cual permite una comunicación bidireccional entre consumidor final y compañía eléctrica.

La seguridad es estos sistemas se basa en su mayoría en los posibles ataques remotos que podrían provocar apagones a gran escala, los cuales pueden implicar desde fallos en el funcionamiento de equipos médicos, hasta pérdida de datos en centros de datos. Además de esta amenaza, también existe la posibilidad de que la información personal de los clientes se vea comprometida.

Podemos diferenciar 2 grandes componentes en este tipo de sistemas:

- Uno que es el encargado de abastecer de energía a nuestra red inteligente; generando electricidad, transmitiéndola y distribuyendo la misma.

- Mientras que otro se encargará de ofrecer soporte a nuestra infraestructura, permitiendo el control y monitorización de nuestro centro de operaciones, gracias a un conjunto de software, hardware y redes de comunicación.

Respecto a las comunicaciones CPS, se pueden diferenciar entre: las destinadas a los dispositivos sobre el terreno, las cuales son comunicaciones inalámbricas para enviar medidas y recibir nuevos comandos desde el centro de control utilizando señales de frecuencia de corto alcance; y las comunicaciones del centro de control ICCP similar a lo visto anteriormente en ICS.

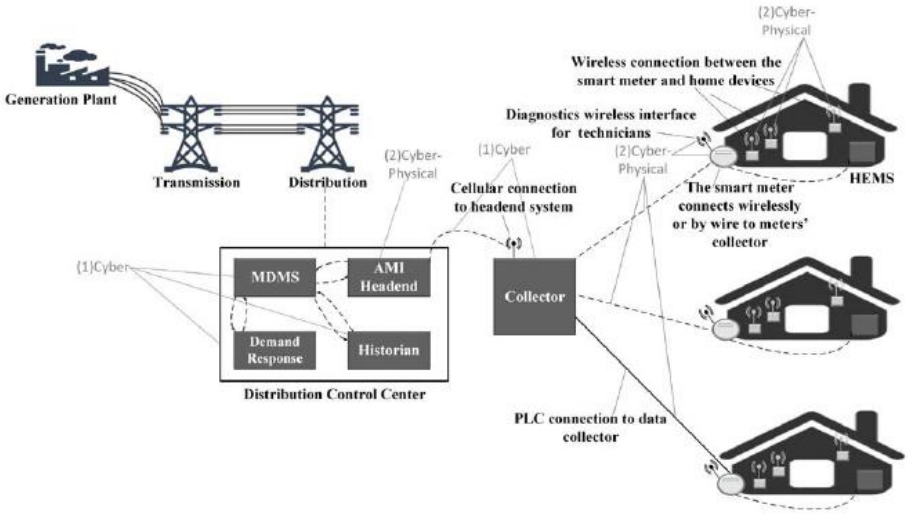

Figura 3. Componentes CPS en una Smart Grid.[iii]

En cuanto a las **ciber-vulnerabilidades**, cabe destacar que la infraestructura de la información de la red inteligente depende de un protocolo estandarizado de internet como es TCP/IP, cuyas vulnerabilidades son más que conocidas. Además de dicho protocolo, ICCP, protocolo encargado del intercambio de datos entre centros de control, presenta una crítica vulnerabilidad de desbordamiento de buffer. En relación a las vulnerabilidades software, son las mismas que en ICS en su mayoría, aunque hay algunas específicas de estos sistemas, por ejemplo, la existencia de medidores inteligentes que se pueden actualizar de forma remota. Un atacante puede hacer uso de dicha vulnerabilidad para provocar apagones tomando el control de dichos medidores. Pudiendo atacar al propio centro de control, o a los medidores individualmente, asimismo, como este tipo de redes se han hecho cada vez más accesibles en cada hogar, estos se han convertido indirectamente en una potencial puerta de entrada para los atacantes. Ligado al hecho de que exista esta comunicación bidireccional entre los medidores y los hogares, las redes inteligentes presentan otro problema añadido, ya que puede verse comprometida información privada de los clientes.

En cuanto a las **vulnerabilidades ciber-físicas**, como las redes inteligentes dependen en su mayoría de los mismos protocolos que en una ICS, en cuanto a la infraestructura del sistema de energía, debemos mencionar de nuevo el inconveniente de protocolos como Modbus y DNP3. Adicionalmente, los recientes avances de estos protocolos han propiciado la aparición de comunicaciones entre subestaciones.

Entre este tipo de comunicaciones encontramos diferentes carencias en cuanto a las propiedades de seguridad; una de las cuales es la falta de encriptado en las comunicaciones, haciendo accesible todo el tráfico de datos para, por ejemplo, hacer ataques de inyección de datos falsos.

Cabe mencionar también, los ataques a los medidores inteligentes debido a la cualidad bidireccional de las comunicaciones, dando lugar a 3 posibles escenarios de ataques:

- **Interrupción de energía**, atacando directamente al suministro energético o bien, inyectando datos falsos para que se tomen decisiones erróneas en el sistema.
- **Utilizando medidores** infectados **como "bots"** para así lanzar ataques contra otros medidores.
- **Manipulando los datos** capturados por los medidores.

Por último, en cuanto a las **vulnerabilidades físicas**, se debe tener en cuenta que los dispositivos de campo, al igual que ocurría en un ICS, se encuentran altamente expuestos y sin seguridad física. Por ejemplo, las líneas eléctricas están expuestas a ataques maliciosos, pero también a accidentes o incluso problemas naturales.

3.3 Dispositivos médicos

Dos de los más comunes son la **"bomba" de insulina** y el **desfibrilador cardioversor implantable**. El primero se utiliza para detectar cuando un paciente diabético necesita insulina e inyectársela automáticamente, monitorizando los niveles de glucosa en sangre. El segundo detecta cuando los latidos del corazón son demasiado rápidos, y suelta una pequeña descarga eléctrica para mantener un ritmo cardiaco normal.

La seguridad en dispositivos portátiles los hace inmunes a ataques que puedan comprometer la seguridad y privacidad del paciente. Pero debido a las distintas circunstancias que rodean a los dispositivos, surge la necesidad de establecer unos objetivos de seguridad, incluyendo la necesidad de autorizar entidades que puedan acceder a datos precisos, de identidad y de configuración del dispositivo, actualizaciones y mantenimiento del mismo. Otro objetivo a remarcar es la protección de la información privada de los dispositivos existentes.

Debido a que los dispositivos necesitan configuración y actualizaciones, y para evitar la necesidad de una extracción quirúrgica cada vez, las comunicaciones de estos dispositivos son inalámbricas. La Comisión Federal de Comunicaciones especifica que las señales deben ser de baja frecuencia, para que programadores y dispositivos médicos puedan comunicarse. Además, también dependen de otro tipo de comunicaciones inalámbricas, la red de área corporal o BAN (del inglés, *Body Area Network*) que utiliza tecnologías como Bluetooth o ZigBee.

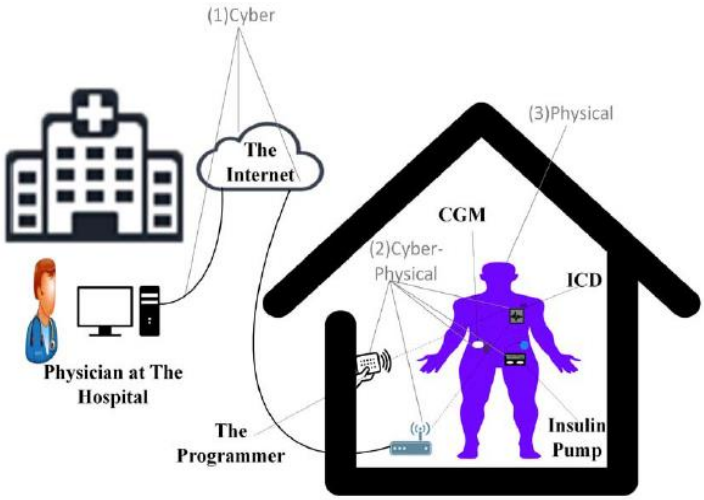

Figura 4. Componentes CPS en dispositivos médicos.[iv]

En primer lugar, respecto a las **ciber-vulnerabilidades** de los sistemas médicos, nos encontramos la ausencia de obligatoriedad a la hora de estandarizar las medidas de seguridad, diseñando sus propios protocolos y dejando que estos dependan del secretismo de los mismos como medida de seguridad, lo que en la mayoría de los casos suele ser una vulnerabilidad. Debido a que las comunicaciones son inalámbricas, encontramos las vulnerabilidades básicas que presentan este tipo de comunicaciones como son: interferencias, ruido, escuchas, ataques de repetición y ataques de inyección; en su mayoría, a causa de la falta de encriptación. Asimismo, los dispositivos con información única pueden utilizarse para ataques de rastreo. Por otra parte, el rol del software en los dispositivos médicos se ha visto incrementado en los últimos tiempos, por consiguiente, encontramos también un aumento en cuanto a los defectos relacionados con el software.

En segundo lugar, en relación con las **vulnerabilidades ciber-físicas**, como se ha mencionado anteriormente, la dependencia de los dispositivos de las comunicaciones inalámbricas, genera vulnerabilidades que pueden presentar una complicación física a los pacientes cuando alguna de las vulnerabilidades es explotada. Por ejemplo, un ataque de repetición no requeriría de conocimiento del protocolo, el atacante únicamente necesitaría capturar un mensaje legítimo y reenviarlo más tarde. Desde otro punto de vista, un atacante puede usar un programador comercial sin la necesidad de autorización debido a la confianza implícita con la que se predispone a los programadores; esto provoca una vulnerabilidad a ataques críticos para seguridad, incluso sin el conocimiento técnico necesario.

En tercer lugar, acerca de las **vulnerabilidades físicas**, el atacante necesitará lidiar físicamente con el dispositivo médico, por ejemplo, para fines de mantenimiento aprovechando la ausencia del propietario del mismo. Pudiendo poner en peligro la salud del paciente; pudiendo acceder también al número de serie del dispositivo. Otra vulnerabilidad física a considerar es el entorno del paciente, algo que los diseñadores no pueden controlar y que podría resultar potencialmente peligroso en una ubicación insegura. Esto es algo especialmente cierto en los ataques por motivos políticos.

3.4 Vehículos inteligentes

la red en los automóviles presenta distintas unidades de control electrónico (ECU), destinadas a distintas tareas, formando subredes. Estas ECU pueden estar conectadas entre sí.

En la actualidad, debido a la innovación en la industria automovilística, los vehículos requieres de comunicaciones inalámbricas y componentes físicos; estas dos necesidades han generado la mayor parte de las vulnerabilidades de seguridad y ataques a coches inteligentes.

En cuanto a las comunicaciones, podemos encontrarnos con diversos tipos de comunicaciones como, vehículo a vehículo (V2V), vehículo a infraestructura (V2I) y las comunicaciones internas de los componentes propios del vehículo. Estas últimas, conocidas como ECUs, las cuales se comunican mediante un bus.

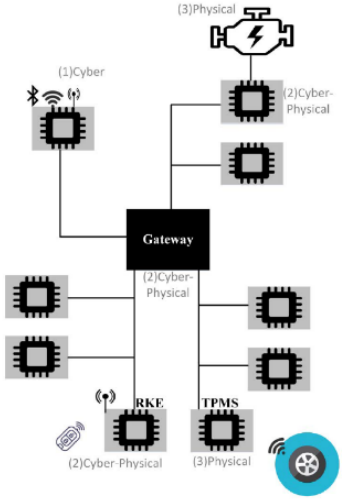

Figura 5. Componentes CPS en vehículos inteligentes.[v]

En relación con las **ciber-vulnerabilidades**, podemos diferenciar las relacionadas con las comunicaciones; y dentro de estas están las que permiten la función de manos libres, y las que permiten personalizar los servicios, actualizaciones de software, respuesta a choques o prevención ante robos. Debido a que los vehículos tienen herramientas de seguimiento como GPS y micrófonos, estas pueden dar la posibilidad de convertirse, además, en herramientas de espionaje. Por otra parte, nos encontramos con las comunicaciones a través de Bluetooth, uno de los vectores de ataque más vulnerables ya que la única medida de autenticación es un código PIN sugerido por el propio vehículo, por lo que, mediante fuerza bruta, un atacante puede acceder a este e iniciar un ataque, extrayendo el control de la información del dispositivo.

Por lo que concierne a las **vulnerabilidades ciber-físicas**, diferenciamos tres tipos de estas vulnerabilidades.

Primeramente, vulnerabilidades en la comunicación de componentes ciber-físicos, son las comunicaciones internas mencionadas anteriormente en las que están involucrados los componentes del vehículo mediante protocolos como CAN y LIN (del inglés, *Local Interconnect Network*); la falta de encriptación, autenticación y mecanismos de autorización generan un gran número de vulnerabilidades, por ejemplo, de espionaje o suplantación de identidad. Además, debido a la propia naturaleza *broadcast* de CAN, esto favorece los ataques por denegación de servicio.

Desde otro punto de vista, nos encontramos con la vulnerabilidad provocada por las ECUs (del inglés, *Electronic Control Units*) de confort, ya que en la actualidad hemos visto un gran avance en ECUs que se han ido añadiendo a los vehículos para satisfacer necesidades de seguridad y de confort. Varios ejemplos de estos añadidos son ACC (del inglés, *Adaptative Cruise Control*) el cual puede controlar la velocidad en carretera detectando el vehículo que tiene delante, asistencia en la dirección para controlar que el coche vaya todo el rato dentro del mismo carril o incluso prevención de colisiones. Como ACC utiliza sensores laser o radar para detectar la velocidad de los vehículos que se encuentran alrededor, un atacante bien equipado podría modificar inesperadamente la velocidad, aumentando o disminuyendo la misma.

Por último, las vulnerabilidades por *X-by-wire*, son las conocidas debido a que en la actualidad se han sustituido los componentes mecánicos de control como frenos o acelerador, por componentes electro-mecánicos por los cuales el conductor puede controlar su vehículo presionando un botón. Esto abre una nueva ventana de oportunidades a los atacantes. Aunque esta tecnología depende del protocolo de comunicación *FlexRay*, el cual es más avanzado que CAN visto anteriormente.

Finalmente, en cuanto a las **vulnerabilidades físicas**, no es necesario para este tipo de ataques tener conocimientos y ciber-capacidades especiales. Por ejemplo, un mecánico puede acceder a las partes internas del vehículo directamente. Además, nos encontramos con que hay componentes con acceso a la red interna que se encuentran expuestos, como los espejos interiores.

Capítulo 4. SIEMs, soluciones de detección y mitigación de ataques

Como se ha visto previamente en la introducción, la categoría de SIEM es un tipo de software que recoge datos que pueden ser originados por otro tipo de aplicaciones, tales como antivirus, firewalls o incluso dispositivos de seguridad física de temperatura o movimiento; con el fin de detectar amenazas o posibles intrusiones. Para que sea posible detectar estas evidencias, y así poder hacer frente a dichas amenazas, se convierte en requisito indispensable haber realizado una buena caracterización de nuestra infraestructura, como ya hemos aprendido en el Capítulo 3. *Caracterización de Infraestructuras Críticas*, para así poder conocer qué comportamientos del sistema se salen del funcionamiento "normal" del mismo; en algunos casos se generarán lo que se conoce como "falso positivo" como que un trabajador haya superado el límite de intentos a la hora de introducir su contraseña en su puesto de trabajo; mientras que otros sí serán amenazas reales, como que mediante algún software de "fuerza bruta" se esté intentando acceder al equipo de un puesto de trabajo.

¿Dónde reside **la ventaja de agregar a nuestro sistema de seguridad la solución de un SIEM** si ya se cuenta con antivirus, firewall y demás aplicaciones de securización? Con los sistemas de protección mencionados antes, se genera tal cantidad de información, que resulta **costoso** tener que interpretar toda esta información generada para poder observar un problema real y una vez hecho, actuar en consecuencia; lo decrementa considerablemente la velocidad de anticipación y respuesta frente a amenazas. Añadiendo un SIEM a nuestro sistema de detección de amenazas, estamos automatizando procesos, así como gestionando la seguridad de forma **centralizada**, lo cual simplifica y agiliza en gran medida la labor de los profesionales encargados de la protección.

Por lo tanto, podemos deducir que tener el control sobre lo que está sucediendo en nuestro sistema CPS será el primer paso dentro de nuestra solución de ciberseguridad. Llevando un control sobre el aumento de conectividad en un punto de acceso frente a accesos no autorizados ya que algunas veces se usan protocolos abiertos como TCP/IP, y en otros casos las comunicaciones se llevan a cabo mediante otro tipo de protocolos, como puede ser DNP3 o Modbus, mencionados previamente, estos dos últimos, presentan infinidad de vulnerabilidades ya que cuando fueron diseñados se consideraron supuestamente "aislados". Por otro lado, debemos hacer controles en las comunicaciones, por ejemplo, establecer un tiempo límite en el que las comunicaciones caduquen, puede ser un buen método para la detección de intrusos. Además, otro aspecto a tener en cuenta a la hora de establecer una serie de controles que minimicen los riesgos es la certificación de los dispositivos y componentes, pues todos los componentes de nuestro CPS deberán verificar la autenticidad del software que ejecutan.

Seguidamente, se pasará a comentar otras soluciones de control y seguridad, más enfocadas a un tipo de aplicación en concreto, en nuestro caso, los distintos IC vistos en el capítulo anterior, distinguiendo entre controles cibernéticos, ciber-físicos y físicos.

4.1 ICS (del inglés, Sistemas de Control Industrial)

Dentro de los controles de ICS, establecemos los tres tipos de controles que hemos mencionado en el apartado anterior:

En cuanto al apartado de controles cibernéticos, el primer punto que vamos a mencionar es el **cifrado y gestión de claves** ya que existe la necesidad de cifrar las redes ICS, el problema que esto genera es un retraso en un marco donde existe una baja tolerancia a retrasos. Debido a esto, una solución para la gestión de estas claves que se propone, es la enfocar la seguridad de nuestro sistema en capas, dividiendo las zonas en niveles de seguridad alto y bajo; y encadenando *Hash*, logrando de esta manera, que si un intruso logra el control total de un dispositivo situado en la zona de seguridad baja, dicho intruso no podrá acceder a niveles superiores. Por otro lado, se debe llevar a cabo un **control sobre el software**, actualizando el mismo regularmente frente a vulnerabilidades que vamos descubriendo sobre nuestro sistema operativo y aplicaciones. Un ejemplo de esto fueron los parches lanzados por Windows relacionados con STUXNET, de no

ser así, este "gusano" informático todavía seguiría presente; por su parte, los proveedores de aplicaciones ICS deben mantener sus versiones al día en cuanto a compatibilidad, para que no se tenga que recurrir a versiones anteriores del sistema operativo que sí sean compatibles. Desde otra perspectiva de la ciber-seguridad, la **estandarización** es otro aliado que puede contribuir enormemente a mitigar ataques y a proteger nuestra infraestructura. Un ejemplo de organismo de estandarización es el **NIST** (del inglés, *National Institute of Standards and Technology*), proporcionando una serie de pautas y recomendaciones que van desde los controles del firewall hasta la ciber-concienciación de los empleados de una entidad.

En cuanto a los controles **ciber-físicos** se añaden nuevas herramientas a la seguridad que consisten, más que en crear nuevas soluciones en el nivel de comunicación de los ICS, propuestas de mejora basadas en los protocolos actuales, tales como **Modbus**, **DNP** e **ICCP**. Un ejemplo de esto es el *framework* **Secure Modbus** que proporciona autenticación, no repudio y obstaculizar la reproducción de paquetes. Otro ejemplo a destacar es el *framework* **DNPSec**, que incorpora a la solución DNP confidencialidad, integridad y autenticidad. En cuanto al diseño de IDS que protejan nuestro ICS, podemos definir una serie de objetivos a controlar y detectar: el acceso a controladores y enlaces de comunicación, las modificaciones que se puedan realizar a la configuración de un sensor; y la manipulación física de los mismos. Como solución concreta, podemos mencionar **WildCAT**, que se centra en la exposición física de las comunicaciones inalámbricas. La idea es instalar este prototipo en los coches de los guardias de seguridad que vigilan la planta, los datos que recogen estos prototipos son recopilados en un centro de análisis que, analiza si se está realizando una actividad sospechosa y envía a los guardias donde se esté produciendo dicha actividad. Se debe limitar el acceso remoto a los dispositivos de campo únicamente al personal autorizado. Para prevenir ataques del tipo DoS, se han de cerrar de forma periódica las conexiones inactivas y no permitir diversas conexiones simultaneas.

Referente a los controles de seguridad **física**, el NIST ya mencionado previamente, aconseja en un listado algunos métodos de defensa como: protección de la ubicación física del sistema, control de acceso y seguimiento de personal y activos; así como tener en cuenta factores ambientales que también puedan considerarse desfavorables en cuanto al servicio que desea ofrecer.

4.2 Smart Grids o Redes Inteligentes

En cuanto a los controles de **cibervulnerabilidades** en las redes inteligentes, mencionamos primeramente los **controles DoS** para evitar o por lo menos detectar ataques por denegación de servicio; esto lo logramos mediante el filtrado de paquetes, la limitación de velocidad y la reconfiguración de la arquitectura de red, esto último puede llegar a resultar complicado, pues el sistema de esta red suele ser en su mayoría estático. Otro de los controles necesarios en la seguridad, es en lo relacionado a la **preservación de la privacidad**, pues conseguir protocolos que garanticen la confidencialidad e integridad de los datos es algo crucial en este tipo de infraestructuras, por tanto, se proponen técnicas que controlen el tráfico de datos entre medidores inteligentes y centros de control de las redes inteligentes, es más, también debemos tener en cuenta que no solo hay que controlar la confidencialidad de los datos, sino también su veracidad, realizando controles sobre una posible inyección de datos falsos desde algún punto de la red. Por último, algo que ya se ha remarcado en el sub-apartado anterior, y se mencionará también más adelante, es la **estandarización**, llevada a cabo por el mencionado antes **NIST** o el **IEC** (del inglés, Comisión Electrotécnica Internacional), los cuales han elaborado una serie de estándares que ayudan a afianzar las comunicaciones en las redes inteligentes.

En cuanto a los controles **ciber-físicos**, en sistemas grandes, como es el caso de una *Smart Grid*, es muy común que en dispositivos de campo que se encuentran en capas de bajo nivel, se comparta la misma contraseña para todos los empleados, esto provoca que sea imposible el repudio cuando se produce una intrusión o ataque desde estos dispositivos, lo que significa que no se puede rastrear quien lo hizo. Por lo que se propone implementar mecanismos que otorguen a cada empleado su propio mecanismo de autenticación y autorización. Igualmente, se están añadiendo extensiones de los propios protocolos, como en el caso de ICS, para así incorporar a los protocolos

ya existentes, una seguridad añadida; es lo que sucede por ejemplo en el protocolo **Secure DNP3**, extensión que aporta autenticación, integridad y confidencialidad al protocolo DNP3. Desde otra perspectiva, se debe evitar que un atacante pueda hacer uso de la función que adquieren los medidores inteligentes en las *Smart Grids* que nos permite desactivarlos remotamente, por ejemplo, podemos mitigar el ataque notificando previamente al cliente que dicho dispositivo va a ser desactivado, con antelación para poder reaccionar.

Aparte de lo mencionado en el aparatado 4.1 sobre ICS, en cuanto al NIST en los controles de seguridad **física**, se debe de tener en cuenta y, por tanto, hacer hincapié en que los sensores y medidores inteligentes de la red suelen estar expuestos, por lo que es imprescindible que estos estén sellados en unidades que aseguren que no pueden ser manipulados físicamente.

4.3 Dispositivos médicos

A la hora de prevenir **ciber**-ataques a IMD (del inglés, *Implantable Medical Device*), se nos presenta una complicación añadida, pues para la actualización de dichos IMDs es necesaria una intervención quirúrgica para la extracción y actualización de los mismos, por otro más seguro; algo que, dejando a un lado las complicaciones que se pueden originar debido a la propia intervención, resulta un proceso **costoso**, por ello, una solución que se propone es la de utilizar dispositivos portátiles externos que protejan al IMD. Un ejemplo de esto sería un IMDGuard, que sirve para defender nuestro dispositivo frente a ataques de interferencias, o incluso de suplantación de, por ejemplo, dispositivos de resincronización cardíaca. En el aspecto de la **estandarización**, en este caso es la FDA (del inglés, *Food and Drug Administration*) una de las organizaciones punteras en la estandarización de dispositivos médicos.

En otro orden de cosas, por parte de los controles **ciber-físicos**, una de las propuestas que se realizan para establecer estos controles, es relativa a la **autenticación**, mediante un intercambio de claves que no requiera un consumo de energía de la batería adicional, sino que depende de la frecuencia a la que modula, utilizando canales adicionales que sean diferentes a los convencionales de audio o video. Además, se propone adicionalmente el uso de IDS (Sistema de Detección de Intrusos) para alertar al paciente de que algún intruso está intentando establecer una comunicación con el IMD. Una de las propuestas podría ser la del uso de ***Shield***, que pese a no ser una solución concebida como un IDS, sí puede servir como tal, centrandose en detectar sensores que puedan verse comprometidos y, que por tanto, puedan representar una amenaza para la salud del paciente. Igualmente, existen otros controles que se basan en la ubicación del dispositivo, de este modo, un atacante no podrá lanzar un ataque de forma remota; o incluso utilizando soluciones adhesivas, como BCC, de modo que el atacante necesite estar en contacto corporal con el propio paciente para realizar su sabotaje, lo cual dificulta considerablemente los ataques.

En cuanto a la seguridad **física**, simplemente se deberá asegurar que ningún atacante tenga acceso al IMD en cuestión, ya que, por lo general no suelen estar expuestos.

4.4 Vehículos inteligentes

En el caso del control de las **cibervulnerabilidades** en vehículos inteligentes, se proponen diversos IDS (del inglés, *Intrusion Detection System*) para detectar anomalías en el bus CAN (del inglés, *Controller Area Network*), como por ejemplo un reloj que calcula los intervalos de mensajes periódicos de las ECU, para identificar las mismas e identificarlas frente a señales intrusas.

Por parte de los controles **ciber-físicos**, los fabricantes deberán hacer hincapié en las conexiones **Bluetooth**, pues pueden ser la puerta de entrada de los atacantes para así comprometer a las distintas ECU del vehículo, por lo tanto, se deberá de autenticar en los vehículos inteligentes los smartphones que se conecten a nuestro vehículo. Por otro lado, el uso de la **criptografía** podría ser de gran utilidad, pues aportaría a nuestro vehículo algunos beneficios como confidencialidad, integridad o autenticación, ahora bien, los mecanismos criptográficos requieren de una potencia

computacional de la cual un vehículo carece, es por esto que se diseñan otros mecanismos, basados en hardware, dedicado íntegramente a la seguridad del vehículo. Y desde el punto de vista de la "confianza" de los dispositivos, se debe denegar la misma en ECUs de forma arbitraria, permitiendo únicamente a las ECU que lo requieran la realización de tareas tanto de actualización como de diagnóstico.

Por lo que concierne a los controles de seguridad **físicos** del vehículo, se propone un esquema de autenticación que prevenga al mismo de la suplantación de sensores como, por ejemplo, el de frenado asistido en caso de una posible colisión con el vehículo de delante. Un ejemplo de este ataque es que si un intruso logra acceder al puesto OBD-II (del inglés, *On Board Diagnostics*) del vehículo, mediante ingeniería inversa podría llegar a tener el control de una función crítica como es el acelerador o los frenos.

Capítulo 5. Conclusiones

Para concluir, se ha de remarcar los objetivos que se han conseguida en este documento, tales como, dar sentido al término de **Infraestructura Crítica**, identificando sus componentes ciber-físicos así como sus vulnerabilidades o puertas de entrada para los atacantes de dichas infraesttrucuras. De igual forma, se ha comprendido la utilidad y necesidad de incorporar a nuestro sistema de vigilancia y seguridad activa, un **SIEM**, mencionando también cuales son los diversos controles y soluciones tanto **cibernéticas**, **ciber-físicas**, como **físicas,** que se establecen para preservar la seguridad, o por lo menos mitigar el daño que pueda originar un ataque en nuestros sistemas.

En definitiva, la responsabilidad de seguridad de un sistema debe estar cimentada sobre una buena **gestión de la seguridad**, clasificando todos los activos vulnerables, y mediante reglas y estándares de los organismos competentes; además de una buena operación para la seguridad, administrando correctamente las herramientas y datos que recibimos desde el sistema.

De este modo, podemos generalizar como se debería afrontar un proyecto de protección de sistemas, de forma cíclica y de autoaprendizaje, pues el proyecto deberá actualizarse constantemente para estar siempre preparado de forma activa y pasiva a futuras amenazas. A grandes rasgos, los pasos que deberían seguir y retroalimentar unos de otros serían:

- **Paso 0:** planificación del proyecto.
- **Paso 1:** análisis de activos y vulnerabilidades detectadas.
- **Paso 2:** clasificar por niveles de peligrosidad todos los activos y vulnerabilidades encontradas.
- **Paso 3:** definir las estrategias para proteger y controlar tanto el tráfico de datos, como el control de personal en áreas vulnerables de nuestra IC.
- **Paso 4:** implantar herramientas que faciliten la labor de los responsables de seguridad de nuestra IC en base a los criterios y estrategias definidos en pasos anteriores.

Como **paso extra**, siempre es aconsejable invertir esfuerzos en la ciber-concienciación y formación del personal que trabaja en la IC debido a la propia naturaleza de las comunicaciones y la peligrosidad que tiene el “estar todos conectados”.

Evidentemente, es necesario un SIEM potente para hacer frente a toda la información que va a recibir de todas las partes del sistema, de distinta procedencia y variedad en el tipo de datos. Pero lo que también resulta algo esencial para un buen blindaje frente a ataques y además poder ofrecer una respuesta a ellos, es una buena caracterización; pues si no es así, de nada servirá disponer del SIEM más completo y potente del mercado.

Por ejemplo, si en todo nuestro sistema, al responsable de seguridad ha pasado por alto incluir en la caracterización una simple impresora que disponga de conexión a la red, los atacantes podrían utilizarla como puerta de entrada para desplegar un ataque más potente y perjudicial, y en un análisis forense posterior resultaría más complicado reconocer que parte del sistema se utilizó para acceder al mismo, por lo que se podría incluso dar el caso de que este ataque se volviera a producir.

Actualmente, algunos desarrolladores software del tipo SIEM están trabajando en algo que se conoce como **descubrimiento de activos**, para conocer todos los posibles ordenadores, impresoras, sensores, cámaras y cualquier cosa que pueda ser objeto de un ataque. De esta forma solo faltaría categorizar todos los activos descubiertos, para poder distinguir los diferentes niveles de amenaza, facilitando así la labor de los analistas de seguridad.

Capítulo 6. Anexo

- **STUXNET:** es una de las amenazas mencionadas en la introducción de este documento, un *malware* del tipo gusano informático que afecta a equipos Windows, en concreto a sistemas industriales SCADA, siendo capaz de reprogramar PLCs, sin que el administrador de la seguridad del sistema se percate.
- **Instituto Nacional de Estándares y Tecnología (NIST):** agencia que se encarga de, como su propio nombre indica, establecer normas y estándares que promueven el progreso e innovación de la tecnología en el mercado estadounidense, lo cual deriva en el mercado internacional.
- **International Electotechnical Commission (IEC):** organización de estándares que promueve la cooperación internacional y la normalización electrotécnica.
- **Modbus:** protocolo arquitectónicamente basado en maestro-esclavo, diseñado para aplicaciones industriales con la finalidad de controlar PLCs. TCP.
- **Distributed Network Protocol versión 3 (DNP3):** protocolo industrial utilizado para las comunicaciones de los componentes que conforman un sistema SCADA.
- **Inter-Control Center Protocol (ICCP):** protocolo de transferencia de datos entre centros de control en tiempo real. Basado en el típico protocolo cliente-servidor.
- **Controller Area Network (CAN):** protocolo de comunicación basado en la trasferencia de datos mediante bus.
- **Local Interconnect Network (LIN):** protocolo que permite al ordenador de a bordo de un vehículo comunicarse con los diferentes subsistemas. (ISO-17987).
- **FlexRay:** protocolo superior a CAN en cuanto a prestaciones, aporta una alta tasa de transmisión de datos y redundancia en el sistema, lo cual aporta indirectamente seguridad y mayor tolerancia a errores.
- **Food and Drug Administration (FDA):** agencia estadounidense que se encarga de regular, entre otros, os dispositivos médicos.

Capítulo 7. Bibliografía

[1] James M. Taylor, Jr and Hamid R. Sharif "Security Challenges and Methods for Protecting Critical Infrastructure Cyber-Physical Systems," *2017 International Workshop on the Practical M2M Communications Issues and Solutions on 5G+ Networks*, 2017

[2] Awais Rashid, Wouter Joosen and Simon Foley "Security and Resilience of Cyber-Physical Infrastructures," *Lancaster University Technical Report* No: SCC-2016-01, April 2016.

[3] Abdulmalik Humayed, Jingqiang Lin, Fengjun Li, and Bo Luo "Cyber-Physical Systems Security – A Survey," *IEEE Internet of things journal*, vol. 4, no. 6, pp. 1802–1831, December 2017.

[4] Leandros A. Maglaras, Ki-Hyung Kim, Helge Janicke, Mohamed Amine Ferrag, Stylianos Rallis, Pavlina Fragkou, Athanasios Maglaras, Tiago J. Cruz "Cyber-security of critical infrastructures," *ICT Express 4* pp. 42-45, February 2018.

[5] "Analysis of the Cyber Attack on the Ukrainian Power Grid" *Electricity Information Sharing and Analysis Center*, March 2016.

[6] Luigi Coppolino, Salvatore D'Antonio "Enhancing SIEM technology for protecting Critical Infrastructures" *ETSI Security Workshop Programme Committee*, January 2012.

[7] Yassine Maleh, Mohammad Shojafar, Ashraf Darwish, Abdelkrim Haqiq "Cybersecurity and Privacy in Cyber-Physical Systems" *Taylor & Francis Group*, May 2019.

[8] Gianfranco Cerullo, Valerio Formicola, Pietro Iamiglio, Luigi Sgaglione "Critical Infrastructure Protection: having SIEM technology cope with network heterogeneity" *Department of Engineering University of Naples "Parthenope" Naples, Italy.*

Capítulo 8. Figuras

[i] Figura 1. Sistema SCADA. [4]

[ii] Figura 2. Modelo esquemático de un CPS. [3]

[iii] Figura 3. Componentes CPS en una Smart Grid. [3]

[iv] Figura 4. Componentes CPS en dispositivos médicos. [3]

[v] Figura 5. Componentes CPS en vehículos inteligentes. [3]