Protección en infraestructuras críticas.

Análisis de seguridad de los sistemas de control industrial

Alumno: Álvaro Roberto Rojas Castro

Plan de Estudios: Máster Interuniversitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)

Área del trabajo final: Ad hoc

Consultor: Jorge Chinea

Responsable Asignatura: Víctor García Font

Fecha Entrega: Enero de 2019

Esta obra está sujeta a una licencia de Reconocimiento 3.0 España de Creative Commons

Copyright © 2019 Álvaro Roberto Rojas Castro

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.3 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.

A copy of the license is included in the section entitled "GNU Free Documentation License".

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Protección en infraestructuras críticas. Análisis de seguridad de los sistemas de control industrial*
Nombre del autor:	*Álvaro Roberto Rojas Castro*
Nombre del consultor/a:	*Jorge Chinea López*
Nombre del PRA:	*Víctor García Font*
Fecha de entrega (mm/aaaa):	01/2019
Titulación::	*Máster Interuniversitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones (MISTIC)*
Área del Trabajo Final:	*TFM-Seguridad en la Internet de las cosas*
Idioma del trabajo:	*Castellano*
Palabras clave	*Sistemas de Control Industrial, Infraestructuras críticas, Ciberseguridad en sistemas de control industrial*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados i conclusiones del trabajo.*

En el contexto de los Sistemas de Control Industrial, como infraestructura crítica de una organización, se debe tener en cuenta su ciberseguridad, porque es habitual que, a pesar de que los sistemas críticos industriales estén totalmente integrados en las tecnologías de la información, no se tengan en cuenta las posibles vulnerabilidades de seguridad que pueda mostrar el sistema.

Cada vez es más corriente encontrar Sistemas de Control Industrial totalmente integrados en las redes de telecomunicaciones de las empresas; sin embargo, es aún muy común ver como la seguridad de éstos se deja en segundo plano en favor de la disponibilidad.

La Industria 4.0 permite esta integración de los Sistemas de Control Industrial en la IT de las empresas y no se debe olvidar que la ciberseguridad es uno de los pilares fundamentales de esta cuarta revolución industrial.

En este documento se pretende destacar la importancia de la seguridad en las infraestructuras críticas y, más concretamente, en los Sistemas de Control Industrial, definiendo los componentes de los sistemas industriales y sus vulnerabilidades más típicas.

Se destaca la necesidad de realizar un diseño correcto, centrado en la seguridad, de las redes de comunicaciones entre sistemas, definiendo la necesidad de separar las redes empresariales e industriales con una red intermedia desmilitarizada.

En definitiva, las infraestructuras críticas son un activo muy importante de las organizaciones industriales, por tanto, es recomendable poner énfasis en la seguridad, que aumenta su disponibilidad.

Abstract (in English, 250 words or less):

In the context of Industrial Control Systems, as critical infrastructure of an organization, its cybersecurity must be taken into account, because it is usual that, despite the fact that critical industrial systems are fully integrated into information technologies, possible security vulnerabilities that the system may show are not taken into account.

It is increasingly common to find Industrial Control Systems fully integrated into the telecommunications networks of companies; however, it is still quite usual to see how their security is left in the background in favor of availability.

Industry 4.0 allows this integration of Industrial Control Systems in the IT of companies and it must not be forgotten that cybersecurity is one of the fundamental pillars of this fourth industrial revolution.

This paper aims to highlight the importance of safety in critical infrastructures and, more specifically, in Industrial Control Systems, defining the components of industrial systems and their most typical vulnerabilities.

The need to carry out a correct design, focused on security, of communication networks between systems is highlighted, defining the need to separate business and industrial networks with a demilitarized intermediate network.

In short, critical infrastructure is a very important asset of industrial organizations, therefore, it is advisable to emphasize safety, which increases its availability.

ÍNDICE

1. Introducción 1

1.1. Contexto y justificación 1

1.2. Objetivos 1

1.3. Enfoque y metodología 2

1.4. Identificación de tareas y Planificación del Trabajo 3

1.5. Identificación y evaluación de riesgos 6

1.6. Breve sumario de productos obtenidos 8

2. Sistemas de Control Industrial y sus elementos 9

2.1. Introducción a Infraestructuras Críticas y Sistemas de Control Industrial 9

2.2. Jerarquía y Estructura de los Sistemas de Control Industrial 9

2.3. Elementos de los sistemas de control industrial 12

2.4. Protocolos de comunicaciones de los sistemas de control industrial 16

3. Tecnologías de la Información y las comunicaciones en los sistemas de control industrial 18

3.1. Protocolos de Comunicaciones de Tecnologías de la Información en Sistemas de Control Industrial 18

3.2. Industria 4.0 19

4. Vulnerabilidades de seguridad en los sistemas de control industrial 27

4.1. Amenazas y Vulnerabilidades en Sistemas de Control Industrial 27

4.2. Incidentes de Seguridad conocidos en Sistemas de Control Industrial 31

5. Posibles Soluciones a las Vulnerabilidades de seguridad en los sistemas de control industrial 35

5.1. Gestión de Riesgos en Sistemas de control Industrial 35

5.2. Estándar ISA-99/IEC-62443, Industrial Automation and Control Systems Security 38

5.3. Modelo de seguridad en Profundidad 46

6. Prueba de concepto de aplicación de medidas de seguridad en sistemas de Control Industrial 49

6.1. Vulnerabilidad en aplicación de protocolos industriales de comunicación 49

6.2. Vulnerabilidad ante contenidos maliciosos de dispositivos USB 50

6.3. Vulnerabilidad en la red corporativa 53

7. Conclusiones 61

8. Glosario 63

9. Bibliografía 69

10. Anexos ..... **¡Error! Marcador no definido.**

LISTA DE FIGURAS

Figura 1 - Diagrama de Planificación del trabajo 6

Figura 2 - Jerarquía funcional de ISA-95 (Fuente: [4]) 11

Figura 3 - Niveles funcionales de ISA-95 (Fuente: [4]) 12

Figura 4 - Contexto de los sistemas MES (Fuente: [5]) 14

Figura 5 – Software en el ciclo de vida del producto (Fuente: [13]) 20

Figura 6 - Niveles de automatización (FUENTE: [13]) 21

Figura 7 - Sistemas ERP y MES (FUENTE: [13]) 22

Figura 8- Distribución de vulnerabilidades por componentes de los Sistemas de Control Industrial (Fuente: [15]) 28

Figura 9 - Tipos de vulnerabilidades más comunes (Fuente: [15]) 29

Figura 10 - Estructura del Estándar ISA-99/IEC-62443 [35] 39

Figura 11- Marco de un sistema de Control Industrial según ISA-99/IEC-62443 (Fuente: [37]) 41

Figura 12 - Marco lógico de CPwE (Fuente: [37]) 45

Figura 13 - Capas del Modelo de seguridad en profundidad [3] 46

Figura 14 - USB Port Lock (FUENTE: Internet) 52

Figura 15 - Diagrama de red por Zonas 55

Figura 16 - Zona Industrial segmentada en celdas 57

Figura 17 - Diagrama de red de la Zona desmilitarizada Industrial 58

Figura 18 - Diagrama de red de la Arquitectura resultante 60

LISTA DE TABLAS

Tabla 1 - Riesgo 001 – Alcance inabarcable 7

Tabla 2 - Riesgo 002 – Complejidad de Prueba de Concepto 7

Tabla 3 - Riesgo 003 – Falta de información 7

1. INTRODUCCIÓN

1.1. CONTEXTO Y JUSTIFICACIÓN

Hoy en día, las infraestructuras críticas de las grandes industrias y de las empresas vinculadas a los sectores energéticos, de transportes, suministros, etc. se ven afectadas por nuevas vulnerabilidades relacionadas con los soportes informáticos en los que se apoyan, por lo que se considera la seguridad informática como un elemento clave para garantizar la disponibilidad de sus sistemas y que permita la continuidad del negocio.

Una infraestructura crítica consta de un conjunto de sistemas y activos (físicos o virtuales) tan esenciales para la actividad de la empresa que una interrupción de su servicio tendría un serio impacto, bien económico o bien en la seguridad de las personas y el medioambiente.

En lo que respecta a los entornos industriales, cada vez más se están basando sus infraestructuras críticas en la automatización mediante la informática debido a la cuarta revolución industrial o Industria 4.0 que supone la proliferación de ordenadores y la automatización de mantenimiento de registros. Esta tendencia de la Industria 4.0 supone la inserción en el mundo de la industria de las últimas tecnologías de la información como el Cloud Computing, el Big Data o IoT, lo cual implica la necesidad de tener en cuenta la ciberseguridad para protegerse de las nuevas amenazas que se presentan con estas tecnologías.

Tradicionalmente, los sistemas de control industrial se han basado en tecnologías propias de fabricantes con estándares cerrados que no eran fáciles de atacar por no disponer de información sobre sus posibles vulnerabilidades; sin embargo, en los últimos tiempos, debido a la mencionada Industria 4.0 los sistemas de control industrial se basan en estándares comunes presentes en las tecnologías de la información y las comunicaciones, por lo que se ven amenazadas por las mismas vulnerabilidades propias de la informática y, por tanto son más fáciles de atacar.

En este trabajo se pretende explicar los sistemas de control industrial, su relación con las tecnologías de la información y las comunicaciones y, seguidamente, se discutirán las opciones para proteger estos sistemas de las posibles vulnerabilidades de seguridad que se integran en la industria. Para finalizar, se mostrará una prueba de concepto de aplicación de las medidas de protección identificadas a un sistema de control industrial de una fábrica de producción de cerveza.

1.2. OBJETIVOS

Los objetivos del presente trabajo los podemos dividir entre objetivos generales o a más alto nivel y objetivos específicos, donde se detallan los objetivos de nivel más bajo necesarios para conseguir los objetivos generales.

1.2.1. OBJETIVOS GENERALES

- Identificar las amenazas y vulnerabilidades de seguridad que afectan a los sistemas de control industrial como parte de la infraestructura crítica de las organizaciones.

- Estudiar los estándares y propuestas para la protección de dichos sistemas ante las amenazas y vulnerabilidades identificadas y realizar una propuesta de implantación de dichas medidas como prueba de concepto.

1.2.2. Objetivos específicos

- Describir los elementos y el funcionamiento de los sistemas de control industrial.
- Identificar elementos de los sistemas de control industrial cuya implementación se basa en las tecnologías de la información.
- Identificar las vulnerabilidades de los elementos de los sistemas de control industrial y sus posibles amenazas.
- Investigar incidencias de seguridad ocurridas en infraestructuras críticas y sus causas y consecuencias en la continuidad del negocio y/o en la seguridad de las personas y medioambiental.
- Recopilar y estudiar los estándares de seguridad de las tecnologías de la información aplicadas a sistemas de control industrial.
- Presentar un caso típico de sistema de control industrial en una empresa con una planta de fabricación de cerveza a la que aplicar las medidas de seguridad necesarias para su protección ante las amenazas identificadas aplicando estándares y recomendaciones de seguridad.

1.3. Enfoque y metodología

Parece evidente que la mejor estrategia para llevar a cabo este trabajo y cumplir los objetivos marcados en el apartado anterior sería la siguiente división en fases que pretende cumplir un objetivo específico en cada una:

1) Planificación del trabajo.

En esta primera fase se determina el contexto y justificación de la necesidad de realizar un trabajo en esta área. Identificamos los objetivos que se desean cumplir con este trabajo, los riesgos que podrían impedirlo. También se definen los entregables y se planifican, en consecuencia, las tareas necesarias para realizar el trabajo.

2) Descripción de Sistemas de Control Industrial.

Esta fase pretende definir qué son los sistemas de control industrial y determinar su importancia como infraestructuras críticas para las organizaciones de este ámbito.

3) Relación de las Tecnologías de la Información y las comunicaciones (TIC) con los Sistemas de Control Industrial.

En esta fase se establece la relación existente entre los sistemas de control industrial y las tecnologías de la información y las comunicaciones explicando cómo, en los últimos tiempos, se está apoyando el diseño de estos sistemas de control en estándares propios de

la informática y comunicaciones. También se explicará brevemente los nuevos escenarios que se presentan con la denominada Industria 4.0.

4) **Identificación de vulnerabilidades de seguridad en los Sistema de Control Industrial.**

Esta fase permitirá identificar las vulnerabilidades y se definen las amenazas a las que los sistemas de control industrial tienen que enfrentarse hoy en día. También se presentarán algunos ejemplos en que dichas amenazas se han hecho efectivas describiendo las consecuencias que se pudieron comprobar.

5) **Análisis de Soluciones a las vulnerabilidades en el ámbito de los Sistemas de Control Industrial.**

En esta fase definiremos las medidas preventivas recomendadas para la mitigación de riesgos de seguridad en los sistemas de control industrial. Se describirán diferentes estándares de recomendaciones de seguridad aplicadas al dominio de control de procesos industriales.

6) **Construcción de una Prueba de Concepto de aplicación de medidas de Seguridad en un Sistema de Control Industrial.**

En esta fase se definirá un entorno industrial de una fábrica productora de cerveza donde se observen vulnerabilidades de seguridad y la aplicación de las medidas de seguridad posibles para la mitigación de los riesgos observables.

7) **Conclusiones y trabajo futuro.**

En esta última etapa se presentarán las conclusiones del trabajo y las lecciones aprendidas gracias a su ejecución. Se evaluará el grado de consecución de los objetivos planteados en un principio y del seguimiento de la planificación de tareas realizada. Finalmente se plantearán posibles líneas de trabajo futuro que no se han podido explorar en este trabajo y han quedado pendientes.

1.4. IDENTIFICACIÓN DE TAREAS Y PLANIFICACIÓN DEL TRABAJO

En este apartado se detallan las tareas a realizar en cada fase descrita para la ejecución del trabajo:

- **Documentación previa de la temática del trabajo**: estudio del contexto y estado del arte.
- **Establecimiento de objetivos y alcance del trabajo**: especificación del alcance y de los objetivos generales y específicos del trabajo.
- **Planificación del trabajo**:

- *Contexto y justificación*: Se explica qué son los sistemas de control industrial, cómo éstos se apoyan sobre tecnologías de la información y las comunicaciones y la necesidad existente de proteger estos sistemas.
- *Objetivos*: Se detallan los objetivos generales y específicos que se deben cumplir con el trabajo.

- *Enfoque y metodología*: Se describen las fases que se deben seguir para la ejecución del trabajo.

- *Identificación de tareas y Planificación del Trabajo*: Se detallan las tareas a realizar y su planificación temporal marcando lo hitos parciales de cada PEC.

- *Identificación y evaluación de riesgos*: Se identifican los riesgos que pueden provocar desviaciones respecto a la planificación establecida y se define su probabilidad, impacto y medidas de mitigación.

- *Breve sumario de productos obtenidos*: Se definen los productos parciales que se entregarán en cada fase y que se corresponderán con un hito temporal de cada PEC.

- **Sistemas de Control Industrial y sus elementos:**

- *Descripción de Sistemas de Control industrial*: Se definen los sistemas de control industrial y se explica su importancia como infraestructuras críticas para la organización.

- *Descripción de elementos de los Sistemas de Control Industrial*: Se detallan los posibles elementos que forman un sistema de control industrial y sus funciones dentro del sistema.

- **Tecnologías de la Información y las Comunicaciones en los Sistemas de Control Industrial:**

- *Descripción de tecnologías tradicionales de los sistemas de control industrial.*

- *Descripción de las tecnologías de la información actuales sobre las que se apoyan los Sistemas de Control Industrial.*

- *Industria 4.0*: Estudio de nuevas tendencias en Sistemas de Control Industrial.

- **Vulnerabilidades de Seguridad en los Sistemas de Control Industrial:**

- *Definiciones*: Definición de conceptos de Seguridad, Vulnerabilidad, Amenazas, Ataques, etc.

- *Identificación de Vulnerabilidades*: Identificación de vulnerabilidades más comunes en Sistemas de Control Industrial.

- *Casos en que la seguridad se ha visto comprometida en Sistemas de Control Industrial*: Exposición de casos en los que la seguridad de los sistemas se ha visto comprometida analizando sus causas y consecuencias.

- **Soluciones a las Vulnerabilidades de Seguridad de los Sistemas de Control Industrial:**

- *Identificación de soluciones*: Se detallan posibles soluciones a las vulnerabilidades de seguridad identificadas.

- *Descripción de estándares de seguridad en Sistemas Industriales*: Se describen los estándares existentes en materia de ciberseguridad en entornos industriales (ISA99, …).

- **Prueba de Concepto:**

- *Descripción del sistema objeto de estudio*: Se detallan los elementos presentes en el sistema a estudiar y sus posibles vulnerabilidades de seguridad.

- *Soluciones a implementar para la mejora de la seguridad*: Descripción de medidas de seguridad a adoptar para la mitigación de las amenazas detectadas.

- **Conclusiones y trabajo futuro:**

- *Conclusiones*: exposición de las conclusiones y lecciones aprendidas del trabajo y evaluación de consecución de los objetivos.

- *Trabajo futuro*: descripción de posibles líneas de trabajo futuro que han quedado pendientes.

A continuación, se muestra este mismo desglose de tareas en un cronograma con las fechas estimadas para su finalización:

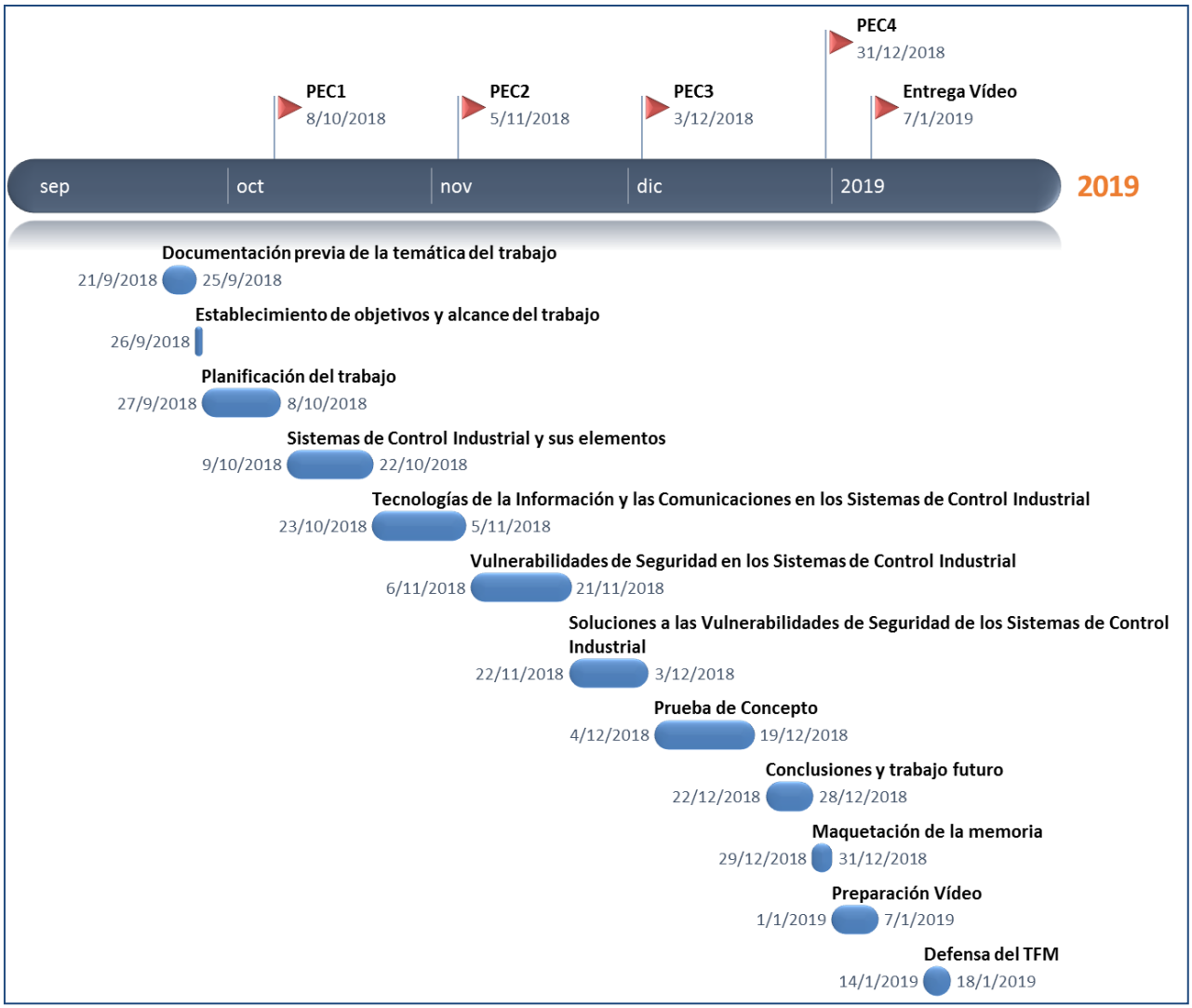

FIGURA 1 - DIAGRAMA DE PLANIFICACIÓN DEL TRABAJO

1.5. IDENTIFICACIÓN Y EVALUACIÓN DE RIESGOS

A continuación, se presenta una evaluación de los riesgos que se han identificado en la elaboración de este trabajo:

ID	001
Riesgo	Alcance del trabajo inabarcable
Descripción	La identificación inicial del alcance que se quería cubrir con el trabajo ha sido demasiado optimista para la dedicación del alumno en los calendarios previstos.
Probabilidad (0-100%)	30%
Impacto (1-5)	5
Acciones de Mitigación	• Eliminación de las tareas menos importantes para la consecución de los objetivos. • Simplificar objetivos. • Recortar el alcance del trabajo.

TABLA 1 - RIESGO 001 – ALCANCE INABARCABLE

ID	002
Riesgo	Prueba de concepto muy compleja
Descripción	Se selecciona una prueba de concepto excesivamente compleja que no permitirá la dedicación necesaria al resto de tareas ni mostrar las soluciones de mitigación de riesgos de forma clara y concisa.
Probabilidad (0-100%)	40%
Impacto (1-5)	3
Acciones de Mitigación	• Simplificar la prueba de concepto destacando la aplicación de soluciones de mitigación de riesgos.

TABLA 2 - RIESGO 002 – COMPLEJIDAD DE PRUEBA DE CONCEPTO

ID	003
Riesgo	Falta de información en alguna de las áreas a desarrollar
Descripción	No se tiene suficiente documentación de alguno de los temas a explicar en el trabajo
Probabilidad (0-100%)	20%
Impacto (1-5)	4
Acciones de Mitigación	• Ampliar el ámbito de búsqueda de información (otros idiomas, otras fuentes de documentación, etc.).

TABLA 3 - RIESGO 003 – FALTA DE INFORMACIÓN

1.6. BREVE SUMARIO DE PRODUCTOS OBTENIDOS

El presente trabajo se divide en los siguientes productos entregables parciales, que en conjunto forman el documento final del Trabajo Fin de Máster:

- **PEC1**: Definición del plan de trabajo. Se describe el problema que se pretende resolver, el trabajo concreto que se llevará a cabo y la descomposición en tareas y metas temporales. Este plan de trabajo contiene, además, los objetivos y metodología que se seguirá en este trabajo.

- **PEC2**: En esta entrega parcial se agregarán los capítulos necesarios para describir los Sistemas de Control Industrial y sus elementos y su importancia como infraestructuras críticas de las organizaciones en que se encuentran. También se identificarán las relaciones de estos sistemas con las tecnologías de la información y las comunicaciones.

- **PEC3**: Esta entrega parcial incorporará los capítulos que identifiquen vulnerabilidades, riesgos y amenazas de los sistemas de control industrial, se presentan casos en los que la seguridad de estos sistemas se ha visto comprometida y, finalmente, se presentarán diferentes soluciones y estándares de seguridad que pretenden mitigar los riesgos descritos.

- **PEC4**: Se realiza una presentación de un sistema de control industrial con la seguridad comprometida y se aplican algunas de las soluciones descritas anteriormente. Se finaliza la memoria del trabajo incorporando el capítulo de conclusiones.

- **PEC5**: Presentación de diapositivas en vídeo de una síntesis del trabajo realizado con la voz en off del autor del mismo.

2. Sistemas de Control Industrial y sus elementos

2.1. Introducción a Infraestructuras Críticas y Sistemas de Control Industrial

Según Nikolic y Drexler [1], una infraestructura crítica es aquella que los estados consideran indispensable para el funcionamiento de su sociedad y economía. Algunos de los componentes de la infraestructura crítica son: la producción y distribución de energía, la provisión de agua y de combustibles, comunicaciones y defensa entre otros.

Esta infraestructura crítica se mantiene operativa gracias, en parte, a los sistemas de control, por lo que es de vital importancia la protección de estos sistemas de control frente a posibles ataques.

A su vez, existen los sistemas de control industrial que son críticas para las organizaciones industriales, pues ofrecen control sobre sus sistemas de producción y, sin ellos, no pueden operar los procesos de negocio que otorgan valor a la organización.

Según L. A. Maglaras et al. [2] un Sistema de Control Industrial (ICS por sus siglas en Inglés, Industrial Control System) es un término que se refiere a un grupo de tecnologías de procesos de automatización, tales como sistemas SCADA (Supervisory Control And Data Acquisition) y DCS (Distributed Control Systems) que proporcionan servicios vitales a las infraestructuras críticas, tales como comunicaciones, fabricación y energía, entre otros.

Estos sistemas tienen unos requisitos de rendimiento y fiabilidad importantes y habitualmente utilizan sistemas operativos, aplicaciones y procedimientos que se pueden considerar poco convencionales por parte de profesionales de las Tecnologías de la Información actuales. Estos requisitos suelen priorizar la disponibilidad y la integridad en primer lugar, seguidos por detrás por la confidencialidad e incluyen la gestión de procesos que, de no ejecutarse correctamente, suponen un riesgo considerable a la salud y seguridad de las personas, daños al medioambiente, así como problemas financieros derivados de las pérdidas de producción.

En definitiva, la indisponibilidad de las infraestructuras críticas (energía eléctrica, transportes, etc.) puede tener un impacto económico más allá del daño físico en los sistemas. Por tanto, estos efectos pueden tener un impacto negativo en la economía local, regional, nacional o, incluso, global.

Resumiendo, los Sistemas de Control Industrial son una variedad de sistemas de control y su instrumentación asociada que se utilizan en las tecnologías de producción industrial para alcanzar un objetivo como la creación de un producto o la entrega de un servicio.

2.2. Jerarquía y Estructura de los Sistemas de Control Industrial

Ackerman [3] propone desde una perspectiva a alto nivel, categorizar los Sistemas de Control Industrial según su función:

- **La función de visualización**: Permite observar el estado actual del sistema de automatización en tiempo real. Esto permite al operador o supervisor la toma de decisiones en función de la información obtenida. Esta función es pasiva y tan solo ofrece la información mediante vistas para que el humano tome decisiones sobre ella. Desde el punto de vista de la seguridad, si un

atacante puede manipular la información que el operario visualiza, estaría tomando el control del proceso en sí mismo porque estaría manipulando la toma de decisiones en función de los valores observados.

- **La función de monitorización**: Esta función permite controlar el valor de algún parámetro crítico para que no exceda los umbrales predeterminados. La diferencia básica con la función de visualización está en que la reacción a un determinado valor en este caso es automática. Dicha reacción puede comprender desde la aparición de una señal de alerta hasta el procedimiento de apagado automático del sistema. Desde el punto de vista de la seguridad, si un atacante manipula los valores que el sistema de monitorización está observando, la reacción de esta función puede ser disparada o evitada de forma malintencionada.

- **La función de control**: En esta función es donde se modifica el comportamiento de los elementos del sistema. Estas acciones pueden ser iniciadas por el operador al pulsar un botón o al cambiar un punto de configuración en una pantalla HMI (Human-Machine Interface). Desde el punto de vista de la seguridad, si un atacante puede manipular los valores a los que el sistema de control reacciona o, incluso, llega a manipular el sistema de control en sí, puede conseguir que el sistema haga cosas para las que no había sido diseñado o que no se pretendía que las hiciera.

Para conocer mejor el funcionamiento de los sistemas de control industrial, podemos ayudarnos de la clasificación a nivel funcional definida en el estándar ISA-95. ISA-95 es un estándar internacional en desarrollo para la integración de la empresa con los sistemas de control que proporciona un modelo de referencia para la organización de sistemas, asignando el negocio a diferentes sistemas y el flujo de información entre sistemas. Originariamente es un estándar estadounidense de la Sociedad de Instrumentación, Sistemas y Automatización (ISA), pero se ha adoptado como un estándar internacional como IEC/ISO 62246.

El propósito del estándar es:

- Acentuar las buenas prácticas en la integración de sistemas de control con sistemas empresariales durante todo su ciclo de vida.
- Se puede utilizar para la mejora de las capacidades de integraciones existentes.
- Se puede aplicar sin importar el grado de automatización de los sistemas.

Dicho estándar define un modelo de jerarquía funcional en 5 niveles.

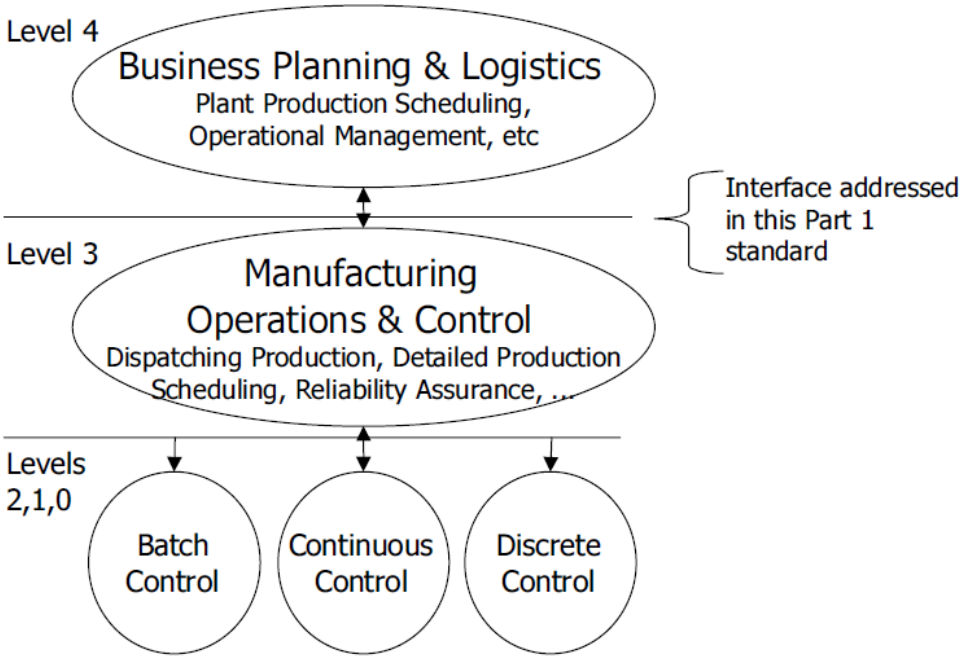

FIGURA 2 - JERARQUÍA FUNCIONAL DE ISA-95 (FUENTE: [4])

En el estándar, estos niveles funcionales se definen así:

1. **Nivel 0**: Define los procesos físicos reales.
2. **Nivel 1**: Define las actividades involucradas en la detección y manipulación de los procesos físicos.
3. **Nivel 2**: Define las actividades de monitorización y control de los procesos físicos.
4. **Nivel 3**: Define las actividades del flujo de trabajo para la producción del producto final deseado.
5. **Nivel 4**: Define las actividades relacionadas con el negocio que necesita gestionar una empresa industrial.

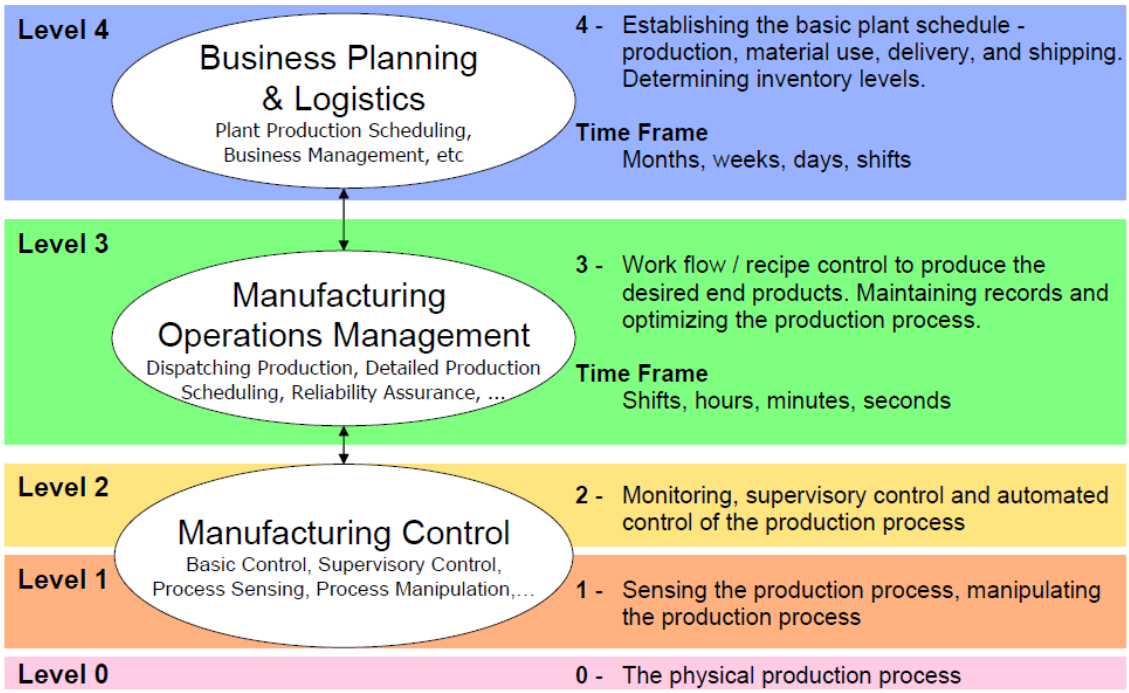

FIGURA 3 - NIVELES FUNCIONALES DE ISA-95 (FUENTE: [4])

Respecto a las correspondencias de estos niveles funcionales definidos por el estándar, queda claro que:

6. El nivel 0 incluye los dispositivos físicos propios del proceso de producción.
7. El nivel 1 se corresponde con dispositivos inteligentes como, por ejemplo, los Controladores Lógicos Programables (o PLC por sus siglas en inglés, Programmable Logic Controller).
8. El nivel 2 se corresponde con los sistemas de control que agregan los datos de los PLCs como pueden ser los HMI o sistemas SCADA.
9. El nivel 3 se corresponde con los sistemas de Operaciones de Fabricación (MES, Batch, Sistemas de Gestión de Información de Laboratorio o LIMS por sus siglas en inglés, Laboratory Information Management System).
10. El nivel 4 se corresponde con los sistemas logísticos del negocio (ERP).

2.3. ELEMENTOS DE LOS SISTEMAS DE CONTROL INDUSTRIAL

Para realizar una descripción de los elementos que pueden componer un sistema de control industrial, nos ayudaremos de la división por niveles de la infraestructura propuesta por la asociación ISA descrita en el apartado anterior.

11. **Nivel 0: Proceso físico de producción**: En este nivel nos encontramos con los sistemas físicos del proceso industrial. Aquí nos encontramos con el equipamiento que deseamos controlar y monitorizar desde los niveles superiores. Nos encontramos con sensores que miden velocidades, temperatura o presión, válvulas o motores. En este nivel es donde se ejecuta la producción del producto, por lo que es obligatoria que su ejecución nunca se interrumpa, el más mínimo desvío en su ejecución puede causar problemas al resto de operaciones.

11.1. *Sensores*: Son dispositivos que detectan señales físicas dentro del proceso de producción y almacenan sus valores para que sean analizados por otros dispositivos de niveles superiores.

11.2. *Actuadores*: Son dispositivos que pueden cambiar el comportamiento del sistema de producción mediante la modificación física de la temperatura, velocidad o presión del proceso.

11.3. *Robots*: Dispositivos más o menos autónomos que ejecutan parte del proceso productivo y de los que se puede modificar su comportamiento mediante la modificación de ciertas variables.

12. **Nivel 1: Control básico de la producción:** En este nivel se engloban todos los dispositivos de control. El propósito principal de los dispositivos de este nivel es el de abrir o cerrar válvulas, mover actuadores o iniciar motores.

12.1. *PLC (Controladores Lógicos Programables)*: Son el corazón de casi todo el sistema de control industrial. Estos dispositivos toman datos de los sensores mediante sus canales de entrada y controla los actuadores mediante sus canales de salida. Dichos canales de entrada y salida pueden ser valores analógicos, digitales o expuestos mediante red de comunicaciones. La programación de un PLC se puede realizar mediante una conexión USB, serial o mediante la red de comunicaciones. Los tipos comunes de estas redes son Modbus, Ethernet, ControlNet, PROFINET, y otros. Los PLCs pueden desplegarse como dispositivos autónomos controlando un proceso determinado de la producción o como parte de un sistema distribuido.

12.2. *IPC (Industrial Personal Computer)*: se tratan de computadoras diseñadas para ejecutar procesos industriales que hace que su formato de fábrica sea muy distinto a los PC convencionales, así como la electrónica utilizada para su fabricación, que los hace más resistentes y más caros.

13. **Nivel 2: Control y supervisión de la producción**: En este nivel se monitorizan y gestionan zonas específicas del proceso de producción con sistemas HMI, SCADA o Sistemas de Control Distribuidos. En este nivel también podemos encontrar estaciones de trabajo de ingeniería. Los sistemas de este nivel se sirven de los datos proporcionados por los PLC para sus funciones de visualización, monitorización y control.

13.1. *HMI (Human Machine Interface)*: Se trata de pantallas de visualización del sistema de control industrial que permite la visualización, inspección y manipulación del proceso que muestra alertas y tendencias de los valores de control. Básicamente se trata de dispositivos táctiles con comunicaciones serial o mediante Ethernet. Sistemas HMI más complejos pueden utilizar servidores distribuidos para proporcionar pantallas y datos redundantes.

13.2. *SCADA (Supervisory Control and Data Acquisition)*: Los sistemas de supervisión, control y adquisición de datos es el término utilizado para describir el uso combinado de distintos tipos y dispositivos de sistemas de control industrial, en el que todos trabajan de forma coordinada en una tarea común. Los sistemas SCADA suelen estar distribuidos en zonas geográficas extensas para su aplicación en redes eléctricas, suministros de agua, redes de tuberías y otros sistemas de control que utilizan estaciones remotas de operación.

13.3. *DCS (Distributed Control System)*: Un sistema de Control Distribuido está muy relacionado con los sistemas SCADA y sus diferencias son prácticamente indistinguibles. Tradicionalmente, los sistemas SCADA se aplicaban para la monitorización de procesos que abarcaban varias plantas

o edificios, mientras que los DCS se limitan a sistemas de control industrial de procesos centrados en una única planta. Este tipo de sistemas es habitual en sistemas de gestión de aguas, papel y refinerías de azúcar.

14. **Nivel 3: Gestión de Operaciones industriales**: En este nivel se ubican los sistemas que ofrecen un control y monitorización completas de los sistemas de producción de la planta industrial. Los sistemas que residen en niveles inferiores envían datos de la producción a los servidores de agregación de datos de este nivel; a su vez, desde este nivel, se pueden enviar datos al nivel superior bajo demanda o de forma automática. En este nivel nos encontramos los sistemas MES, servidores de bases de datos, servidores de aplicaciones (web y de informes), servidores de ficheros, etc.

14.1. *MES (Manufacturing Execution System)*: los Sistemas de Ejecución de la Fabricación. aparecen a mediados de la década de los 90 como una evolución de los conocidos como CIM (Computer Integrated Manufacturing). Los objetivos de los sistemas MES se pueden englobar en los siguientes:

14.1.1. Entrega y control de órdenes de producción en tiempo real desde su lanzamiento hasta la obtención del producto terminado.

14.1.2. Optimización de actividades de producción y mejora de la productividad global.

Los sistemas MES no suelen trabajar de forma autónoma y están enfocados a interactuar con otros sistemas de información que cubren la gestión de la empresa, como muestra, la siguiente figura de MESA:

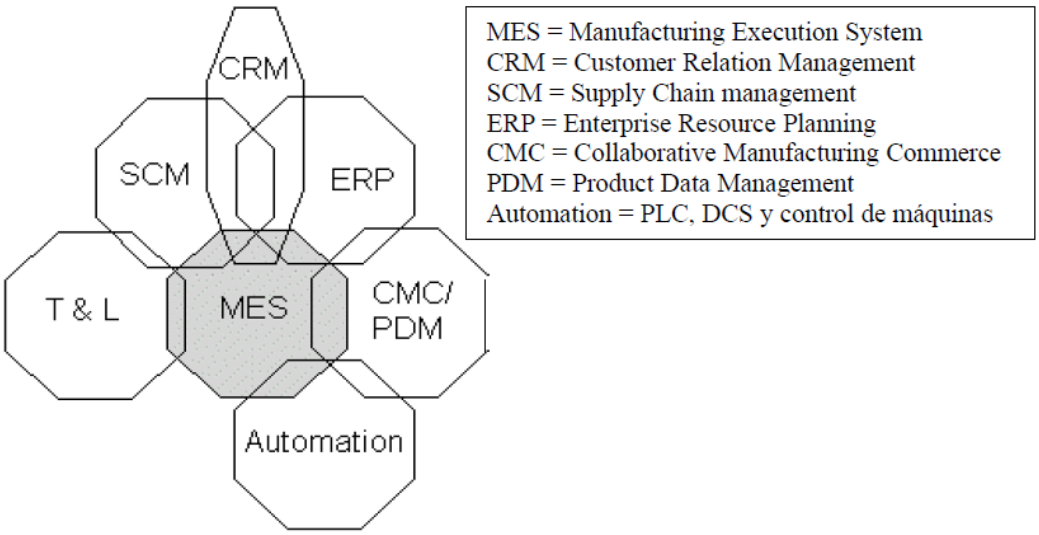

FIGURA 4 - CONTEXTO DE LOS SISTEMAS MES (FUENTE: [5])

Las necesidades de comunicación más frecuentes de los MES se producen con los sistemas ERP para la planificación de la producción y con los sistemas de control de la producción a pie de planta.

15. **Nivel 4: Planificación y Gestión logística del negocio**: En este nivel se engloban todos los sistemas IT (Information Technology) que dan soporte al proceso de producción industrial. Los sistemas de este nivel ofrecen informes estadísticos de la producción y efectúan órdenes de producción según la planificación de la producción del negocio. Los sistemas que se ubican en este nivel y, que nos interesan en los entornos industriales, suelen englobar los sistemas ERP, MRP, SCM, CRM.

    15.1. *ERP y MRP (Enterprise Resources Planning and Material Requirement Planning)*: Los sistemas de información conocidos como ERP (Enterprise Resources Planning) por sus siglas en inglés, se consideran por muchos autores la evolución de los sistemas MRP (Material Requirement Planning), y más concretamente de los sistemas MRP II (Manufacturing Resources Planning) al extender sus funcionalidades a otras áreas de la empresa. La utilización de sistemas MRP establece una forma de planificar la producción mediante la anticipación: se determina qué se quiere hacer en el futuro y, a partir de ahí, surge la secuencia de acciones a emprender para poder realizarlo.

    Los sistemas MRP originales presentaban un inconveniente claro en lo referente a la planificación de la producción, ya que no se tiene en cuenta la disponibilidad de recursos para llevar a cabo las órdenes de producción sugeridas; por lo tanto, pueden aparecer órdenes de producción irrealizables y que finalmente cuestionan la verosimilitud del resto de resultados de la planificación.

    En los años 80 aparecen los sistemas MRP II para solucionar el problema de gestión de la capacidad productiva disponible en los centros de producción para realizar los planes de producción que sugerían los MRP. También se les denomina "MRP con capacidad finita" porque contrasta la disponibilidad de los recursos necesarios para la ejecución de las órdenes de producción planificadas.

    Los sistemas MRP II incluyen la planificación de necesidades de capacidad en la planificación de órdenes de producción. Para poder contrastar la capacidad existente con el plan de producción, se incluye el módulo de centros de trabajo que define la disponibilidad de recursos del sistema. También se incluye información sobre rutas que determinan qué centros de trabajo y qué intensidad de uso requiere cada artículo de fabricación.

    Gracias a la planificación de necesidades de capacidad se calcula la capacidad disponible por cada centro de trabajo frente a la carga resultante de la ejecución de las órdenes de producción planificadas en un horizonte de tiempo determinado. Esta planificación de las necesidades de capacidad permite tomar decisiones respecto a la capacidad de los centros de trabajo como la modificación de dicha capacidad, la subcontratación de ciertos procesos o la modificación de rutas o fechas de las órdenes de producción.

    En la década de los 90, surge la necesidad de integrar diferentes áreas de la empresa (ingeniería, ventas, fabricación o compras) bajo un mismo sistema de información. Así aparecen los sistemas ERP que abordan la planificación de recursos humanos o financieros junto con la planificación de necesidades de materiales y de recursos de producción. Estos sistemas dotan a las empresas de un sistema de información sin

duplicidades respecto a la información utilizada por diferentes componentes de la empresa [6].

15.2. *SCM (Supply Chain Management)*: Son aquellos sistemas que permiten la gestión del flujo de bienes y servicios y comprende el movimiento y almacenaje de materias primas y productos terminados desde el punto de origen al destino final. La gestión de la cadena de suministro se puede definir como la planificación, ejecución, control y monitorización de las actividades de la cadena de suministro para la sincronización del suministro con la demanda, gestionar las relaciones con los proveedores y optimizar los canales de distribución.

En otras especificaciones estándar como la ISA-99, que trataremos en capítulos posteriores, agregan a estos niveles el nivel 5 que contiene la red corporativa de la organización e integra los sistemas de control industrial dentro del entorno de las tecnologías de la información.

2.4. PROTOCOLOS DE COMUNICACIONES DE LOS SISTEMAS DE CONTROL INDUSTRIAL

Tradicionalmente, los elementos de los sistemas de control industrial se han basado en protocolos de comunicaciones propietarios llamados Fieldbus (o buses de campo). A pesar de que la tendencia de los últimos años ha sido encapsular estos protocolos dentro de los protocolos de comunicaciones de las tecnologías de la información (Ethernet y TCP/IP), esto lo veremos en el siguiente capítulo. En este apartado intentamos explicar algunos de estos protocolos industriales dando unas nociones de su funcionamiento:

- **PROFIBUS (Process Field Bus)**: Estándar de comunicaciones definido por grandes empresas alemanas como Bosch y Siemens. Utiliza conexiones físicas seriales como RS-485, MBP (Manchester Coding and Bus Powered) o fibra óptica. [7]

- **Modbus**: Este protocolo de comunicaciones se ubica en la capa 7 del modelo OSI (capa de Aplicación). Es el estándar de facto de las comunicaciones industriales porque se diseñó teniendo en cuenta su uso para aplicaciones industriales, es público y gratuito, fácil de implementar y maneja bloques de datos sin suponer restricciones. Está basado en una arquitectura cliente/esclavo que permite el control de una red de dispositivos mediante una computadora. Se utiliza en conexiones con unidades de terminal remota (RTU) o en sistemas SCADA. Suele utilizar medios de comunicaciones serie RS-232. [8]

- **CAN (Controller Area Network)**: Protocolo desarrollado por la firma alemana Robert Bosch GmbH y está basado en una topología bus para la transmisión de mensajes distribuidos. Este protocolo está orientado a mensajes y se basa en un modelo productor/consumidor que describe una relación entre un productor y uno o más consumidores. Este protocolo fue desarrollado inicialmente para aplicaciones en automóviles y está estandarizado por ISO (ISO 11898-2 e ISO 11898-3, en función de la velocidad de transmisión utilizada). [9]

- **AS-interface**: se trata de un bus de sensores y actuadores, estándar internacional IEC62026-2 que surgió como alternativa económica al cableado tradicional creando una red simple de sensores y actuadores que permita transmitir datos y alimentación por el mismo bus y que permita gran variedad de topologías para poder instalar sensores y actuadores en cualquier punto del proceso con el menor esfuerzo posible. [10]

- **DeviceNet**: Este protocolo utiliza un Bus CAN al que le añade una capa de aplicación para cubrir un rango de perfiles de dispositivos. [11]

- **ControlNet**: Este protocolo abierto de red para aplicaciones de automatismos industriales define una capa física basada en cable coaxial RG-6 con conectores BNC. ControlNet se distingue de otros buses de campo porque incluye el soporte incorporado para cables totalmente redundantes y el hecho de que toda comunicación es estrictamente planificada y altamente determinista. [12]

Estos protocolos suelen tener muy en cuenta la disponibilidad, pero se olvidan muy a menudo de la integridad de los datos y, sobre todo de su confidencialidad. Esto supone un problema de seguridad que se extiende cuando incorporamos las tecnologías de la información, pues se está dando acceso a mayor número de usuarios al incluir los Sistemas de Control Industrial en la red corporativa de la organización.

3. TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES EN LOS SISTEMAS DE CONTROL INDUSTRIAL

La tendencia de los últimos años ha sido la de incorporar protocolos y tecnologías propias de las Tecnologías de la Información en los procesos industriales para abaratar y simplificar las instalaciones de sistemas de control industrial. Por lo tanto, se han dejado de lado o adaptado a nuevas tecnologías los protocolos tipo Fieldbus comentados en el capítulo anterior. En este capítulo detallaremos el uso de protocolos de las Tecnologías de la Información para permitir las comunicaciones dentro de los Sistemas de Control Industrial.

Otra de las tendencias recientes en el entorno industrial es la adopción de las últimas tecnologías en el movimiento llamado Industria 4.0, donde destaca el uso de dispositivos IoT (Internet of Things) como parte de los procesos industriales. En este capítulo también ahondaremos en este nuevo concepto de industria y sus implicaciones en los procesos de producción.

3.1. PROTOCOLOS DE COMUNICACIONES DE TECNOLOGÍAS DE LA INFORMACIÓN EN SISTEMAS DE CONTROL INDUSTRIAL

Cada vez es más habitual, e incluso fundamental, encontrar Sistemas de Control Industrial que se basan en protocolos propios de las Tecnologías de la Información y las Comunicaciones como por ejemplo Ethernet, TCP/IP, HTTP, HTTPS, SMTP, FTP, TFTP, SMB y SNMP; es decir, estos protocolos no son exclusivos de los niveles donde residen las tecnologías de la información (niveles 4 y 5), sino que también nos los podemos encontrar en los niveles inferiores más propiamente industriales para, por ejemplo, ofrecer una pantalla HMI mediante interfaz web con el protocolo HTTP.

Estos protocolos de las Tecnologías de la Información tienen sus propias vulnerabilidades y retos de seguridad, por lo que no es recomendable utilizar la misma red física en el Sistema de Control Industrial que en la zona de oficinas porque dichas vulnerabilidades estarían afectando directamente al sistema de producción.

Algunos protocolos propiamente industriales han evolucionado para adaptarse a los medios de las redes de comunicaciones de las TI, a continuación explicaremos esas adaptaciones en Modbus y PROFIBUS que modifican su nombre a Modbus TCP/IP y PROFINET tal y como los expone Ackerman [3].

- **Modbus TCP/IP**: En este caso, en lugar de utilizar la comunicación serial RS-232, se pasa a encapsular los paquetes de Modbus a través de los protocolos Ethernet y TCP/IP. No se modifica su funcionalidad, solo el medio por el que se transmiten los datos, por lo tanto, se mantiene simple la implementación de este protocolo importando también sus problemas de seguridad que no era el principal requisito del protocolo original.

- **PROFINET**: Es la adaptación del estándar PROFIBUS sobre Ethernet, HART, ISA100 o Wi-Fi como medio de comunicación. Este protocolo utiliza servicios TCP/IP para la configuración o diagnósticos, pero los evita para el intercambio de mensajes deterministas, en favor del protocolo RT (Real-Time) o IRT (Isochronous Real-Time). Al igual que Modbus, este estándar es un protocolo abierto, sin cifrado y sin protección, por lo que, con el acceso a la red local,

pueden ser atacados con métodos y vectores de ataque convencionales en las Tecnologías de la Información.

A continuación, se indican algunos protocolos de las TI comúnmente utilizados en los entornos industriales:

- **HTTP (Hypertext Transfer Protocol)**: Para la publicación de webs de diagnóstico o configuración mediante la publicación de un servidor web.
- **FTP (File Transfer Protocol)**: Se trata de un protocolo de transferencia de ficheros en texto claro.
- **Telnet**: Protocolo para la conexión remota y ejecución de comandos en texto claro. Es común encontrar servidores Telnet en elementos del Sistema de Control Industrial.
- **ARP (Address Resolution Protocol)**: El protocolo de resolución de direcciones permite a una computadora de la red enlazar las direcciones IP y MAC de otro elemento de la red almacenando dicha correspondencia en sus tablas ARP tras la consulta por broadcast a toda la red.
- **ICMP (Internet Control Message Protocol)**: Protocolo que se utiliza para comprobar si un elemento de la red es alcanzable mediante el comando ping.

3.2. INDUSTRIA 4.0

La Industria 4.0 o cuarta revolución industrial se basa en la potenciación y ampliación de la tercera revolución industrial, también conocida como Revolución Digital, que supuso la proliferación de los ordenadores y la automatización de mantenimiento de registros; pero la nueva ola de transformación se diferencia de sus predecesores con las siguientes singularidades:

- Las innovaciones se pueden desarrollar y difundir más rápido que nunca (informatización).
- La caída de los costos marginales de producción y el aumento de las plataformas que se agregan y concentran la actividad en múltiples sectores aumentan los rendimientos a escala (interconexión).
- Esta revolución global afecta a todos los países, y tiene un alto impacto en muchas áreas (globalización).

Lo digital y el mundo real están conectados en la Industria 4.0. Se tiende a un modelo donde la fabricación se efectúa con máquinas que se comunican entre ellas, y forman parte de un ecosistema de fabricación donde cada máquina estará informada inmediatamente cuando la pieza esté modificándose o fabricándose en otra máquina. Incluso conocerá el estado de esa pieza en los almacenes, en la cadena de suministro, y en el mercado final.

Las máquinas se adaptarán automáticamente a la secuencia de la producción de cada una de las piezas para ajustar automáticamente la unidad de producción a la serie a fabricar. Incluso el producto puede comunicar cuando esté terminado y, por lo tanto, solicitar vehículo autoguiado para ser enviado al almacén y listo para ser entregado.

Esta integración no solo se hace entre pieza-máquina y cadena de producción, sino que se puede hacer entre plantas ajustando los programas de producción y de entrega de materiales y componentes de la forma más adecuada.

3.2.1. De la gestión de datos del producto a la gestión del ciclo de vida

La Industria 4.0 engloba una serie de tecnologías que nos permitirá controlar de forma más completa e integrada el ciclo de vida de los productos.

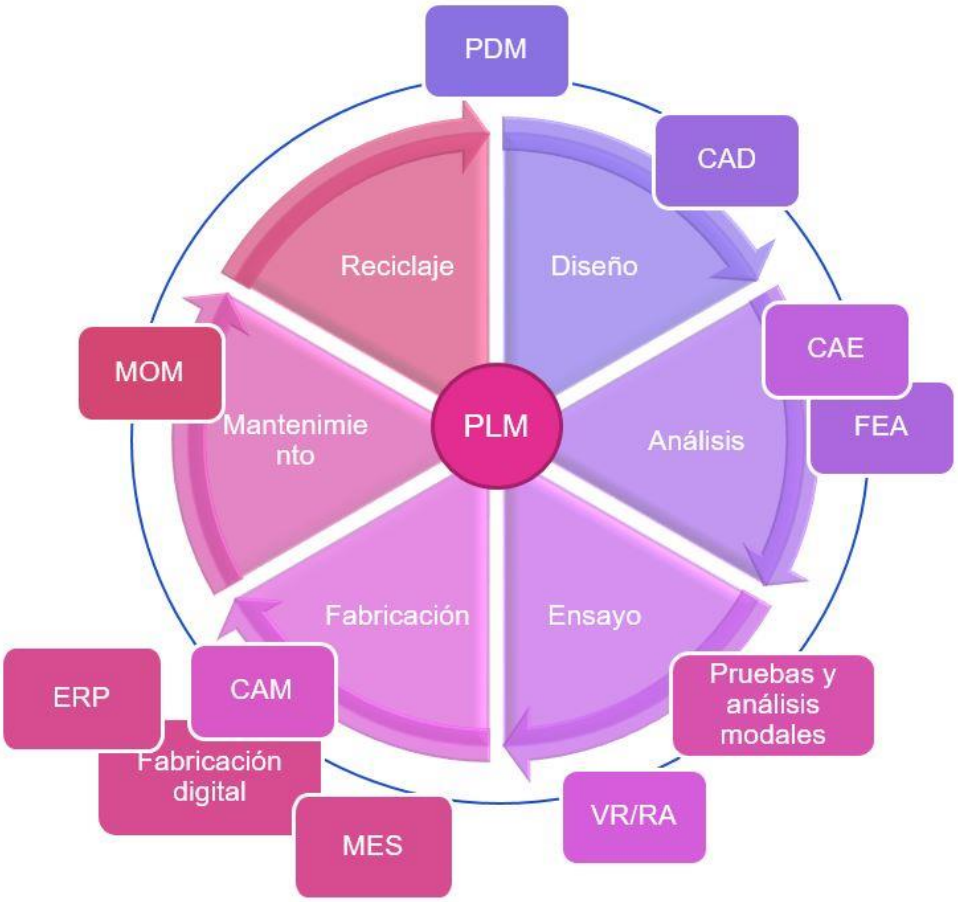

FIGURA 5 – SOFTWARE EN EL CICLO DE VIDA DEL PRODUCTO (FUENTE: [13])

Desde el diseño conceptual (CAD) al análisis y simulación de lo diseñado con su consiguiente optimización (CAE y FEA). La realidad virtual (RV), y la realidad aumentada (RA) nos permitirán incorporar al producto todavía no fabricado a la realidad física que nos rodea viendo su posible integración.

La fabricación digital (CAM, MOM) permite la construcción de la pieza de forma virtual y la gestión de los medios productivos necesarios para la mejor optimización de los mismos.

En la figura superior se ha intentado reflejar una relación de programas informáticos genéricos que están situados en cada una de las etapas de ciclo de vida del producto. Todos ellos pueden quedar englobados dentro de programas en una capa superior como son los ERP y CRM.

A continuación, se ofrece el significado de las siglas empleadas.

- Gestión de datos del producto (PDM)
- Diseño asistido por ordenador (CAD)
- Fabricación asistida por ordenador (CAM)
- Ingeniería asistida por ordenador (CAE) y simulación en 3D
- Análisis de elementos finitos (FEA o FEM)
- Gestión de operaciones de producción (MOM)
- Manufacturing Execution System (MES)
- Sistemas de planificación de recursos empresariales (ERP)
- Customer Relationship Management (CRM)

3.2.2. Fabricación integrada por ordenador

Desarrollado entre los años 80 y 90, la Computer Integrated Manufacturing establece una serie de niveles de automatización de la fábrica. Estos niveles ya comentados en el capítulo anterior, se recogen muy resumidamente en la figura siguiente:

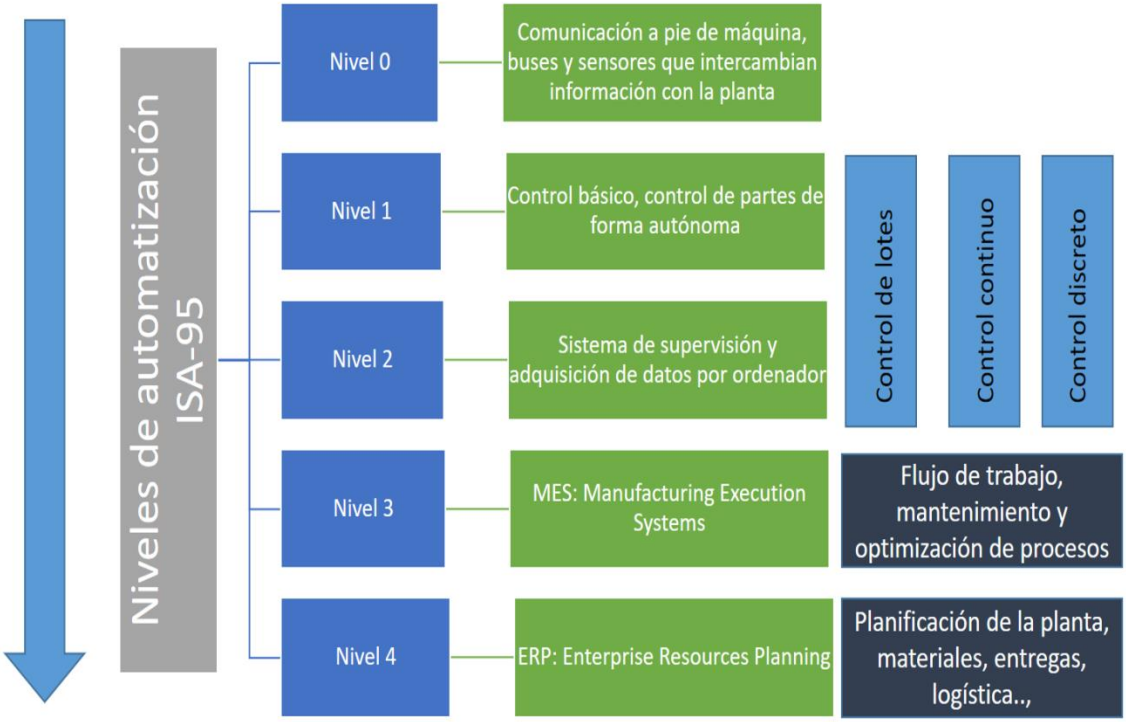

FIGURA 6 - NIVELES DE AUTOMATIZACIÓN (FUENTE: [13])

3.2.3. Sistemas ERP y MES

La tendencia actual es la integración superior por medio de los ERP (Enterprise Resources Planning) y los sistemas MES (Manufacturing Execution Systems). Los ERPs trabajan con bases de datos que pueden ser compartidas por todos los departamentos de la empresa y se utilizan para la planificación a largo plazo fundamentalmente.

Los sistemas MES convierten esta planificación en órdenes de fabricación para cumplir los objetivos en el medio plazo.

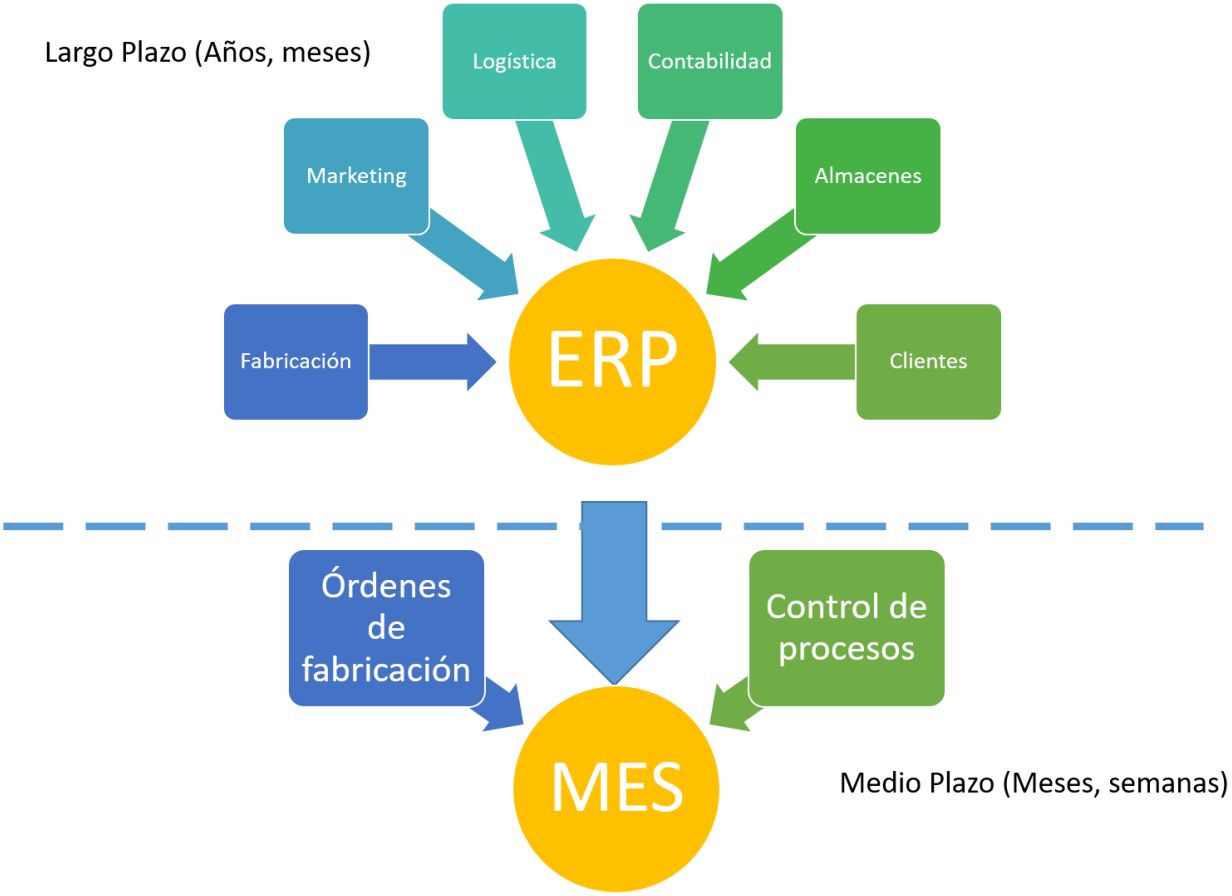

FIGURA 7 - SISTEMAS ERP Y MES (FUENTE: [13])

3.2.4. Integración vertical y horizontal de los sistemas productivos

Los sistemas productivos en la actualidad producen una gran cantidad de datos, los estándares de comunicación deben adaptarse para permitir el acceso a esta información, la gran variedad y heterogeneidad de fuentes de información, impondrán el desarrollo de nuevos estándares, o la utilización de estándares abiertos que permitan la posterior clasificación y explotación de la información. La explotación de estos datos de producción, en las capas superiores del modelo va a permitir generar un incremento muy significativo de la efectividad y por tanto un aumento de la productividad.

En el modelo productivo de la industria 4.0, se establecen diferentes niveles o capas que engloban funciones relativas al producto, producción, gestión y dirección. Ha quedado patente que la integración vertical entre diferentes capas es necesaria para el aumento de la productividad. Sin embargo, la integración horizontal dentro de los sistemas de información que participan en cada capa es básica para poder sustentar con garantías de éxito la integración vertical. La integración horizontal, resulta imprescindible si queremos evitar la descompensación en la carga de los recursos que forman cada capa.

Los datos procedentes de los productos y los sistemas de producción físicos, van a permitir llevar a cabo mejoras sustanciales en la gestión de todo el modelo productivo. La explotación selectiva de este gran volumen de datos obtenido, permitirá no sólo establecer ayudas para la intervención y corrección de disfunciones, sino incluso, automatizar en gran medida el diseño de la estrategia del negocio, tanto a medio como a largo plazo.

3.2.5. Tecnologías propias de la Industria 4.0

- **Realidad Virtual**: Permite la visualización informática por medio de dispositivos (cascos, gafas, pantallas 3d, etc.) de una planta industrial de acuerdo a una simulación que sigue una serie de parámetros que evoca su funcionamiento en unas determinadas condiciones.

- **Realidad Aumentada**: Añade una capa adicional a la visión que tenemos de la realidad aportando información extra. Al permitir superponer datos o imágenes físicas con datos del modelo de su gemelo digital, ya se empieza a utilizar esta tecnología para la gestión del mantenimiento preventivo y permite sentar las bases en actuaciones de resolución de problemas, o incluso automatizar la toma de decisiones sobre medidas para mejorar la eficiencia en los procesos de mantenimiento.

- **Redes de comunicación M2M**: La integración horizontal al nivel más bajo del modelo de Industria 4.0, va a depender fuertemente del desarrollo y la implantación de estándares de comunicación de Máquina a Máquina (M2M), la implantación de estándares abiertos como OPC UA, así como el desarrollo de nuevos, pensados específicamente para soportar la Internet Industrial de las Cosas (IIoT), van a contribuir de manera decisiva a recoger y compartir los datos de la planta de manera ordenada y eficaz, permitiendo su posterior integración vertical, para análisis y procesamiento.

- **Buses industriales e interconexión**: En la actualidad existen diferentes tipos de buses industriales, según sus aplicaciones se emplean para facilitar por ejemplo el despliegue e interconexión de sensores (CAN, ASI), la comunicación de controles y máquinas (PROFIBUS), o comunicación entre sistemas informáticos (PROFINET), el desarrollo para la industria 4.0 pasa por crear pasarelas que permitan la interconexión y traslado de datos, lo que facilitará la integración horizontal.

- **Cloud Computing**: La computación en la nube es una tecnología que deberá desarrollarse y adaptarse para poder completar el modelo de Industria 4.0, hay dos motivos fundamentales por los que se tendrán que descentralizar los recursos informáticos, por un lado por la capacidad de almacenamiento, ningún sistema en local podría competir con el volumen necesario para almacenar el torrente de datos de la IIoT, de otro lado la capacidad de procesamiento, la tendencia actual es emplear virtualización para resolver los problemas de

cálculo intensivo o análisis de grandes cantidades de datos. Es por esto que "la nube" jugará un rol decisivo en la implantación de las fases de gestión e inteligencia artificial de los sistemas Industria 4.0.

- **Internet Industrial de las Cosas (IIoT)**: la Internet Industrial de las Cosas (IIoT) va a desarrollar un papel fundamental en las aplicaciones de la Industria 4.0, al igual que sucede en nuestra vida cotidiana con la IoT, el desarrollo de nuevos sensores para máquinas y sistemas industriales, va a permitir recoger grandes cantidades de datos durante las fases de puesta en marcha y explotación de la planta. El desarrollo de las tecnologías y buses para redes de sensores, unido al desarrollo de los estándares de comunicación, va a permitir integrar esa información de forma vertical en la empresa.

- **Big Data**: En este escenario, se dispone de gran cantidad de datos, que para que sean útiles para la gestión de la fábrica, deberán ser procesados con herramientas avanzadas (algoritmos y analítica) que genere una información repleta de contenido. Tomando en consideración la presencia de problemas visibles e invisibles en una planta industrial, el algoritmo de generación de información tiene que ser capaz de detectar e identificar problemas invisibles como la degradación de máquinas o desgaste de componentes en el proceso industrial. La evaluación de la información obtenida de distintas fuentes (desde los dispositivos y sistemas industriales hasta los sistemas de gestión empresarial y de clientes) permite la toma de decisiones en tiempo real.

- **Inteligencia Artificial**: El Machine learning permite la realización de predicciones basadas en grandes cantidades de datos. Esta rama de la Inteligencia Artificial se basa en el reconocimiento de patrones y tiene la capacidad de generar conocimiento desde la experiencia. Por esta razón, esta tecnología ha encontrado su lugar en los procesos industriales. Dos de las ramas de la Inteligencia Artificial como el aprendizaje de máquinas (machine learning) y el aprendizaje profundo (deep learning) utilizan, ya hoy en día, las posibilidades del Big Data para la optimización de procesos, encontrar nuevas soluciones y obtener nuevos conocimientos. [14]

- **Ciberseguridad Industrial**: El gran problema de la interconexión masiva que propone el modelo de la Industria 4.0, es la necesidad de abrir puertos de comunicación en todos los sistemas informáticos conectados participantes, de la interconexión surge o puede surgir la vulnerabilidad, si no se tienen en cuenta los planteamientos de diseño de un sistema ciberseguro. Por lo tanto, los conceptos claves de ciberseguridad industrial, no pueden quedar al margen de ninguna implantación, y todo lo que es válido para sistemas de seguridad informática en el mundo IT (Tecnologías de la información y las Comunicaciones) va a resultar imprescindible también en el mundo OT (Tecnologías de operación), o sistemas informáticos de planta.

Estas tecnologías permiten, mediante su aplicación a la industria la definición de nuevos conceptos propios de la Industria 4.0:

- **Fabricación Digital**: Gracias a las tecnologías de realidad virtual y realidad aumentada, se puede reducir el ciclo de puesta en marcha de una fábrica elaborando un gemelo digital de la planta que permita su explotación en los sistemas de gestión, y la integración de los datos de producto o de planta con los sistemas de gestión de la empresa. El desarrollo de un modelo

tridimensional de la planta nos servirá para diseñar y planificar la integración de todas las máquinas y utillajes para la fabricación.

- **Sistemas Ciberfísicos**: Requiere de dos partes diferenciables la virtual y la real, que deben diseñarse en concordancia, de manera integrada, y con la posibilidad de intercambiar datos tanto en las fases de pruebas como en las fases de explotación. El concepto puede aplicarse tanto al ámbito del producto, como al del sistema de producción completo. Los sistemas ciberfísicos van a permitir la optimización del diseño y puesta en marcha a todos los niveles, permitirán refinar los modelos de comportamiento empleados en los procesos de diseño, y permitirán optimizar los productos y sistemas productivos en explotación. Representan un nuevo paradigma de diseño con capacidad de producir iteraciones de mejora de forma más rápida y eficiente.

- **Puesta en marcha virtual**: La tecnología actual permite crear un gemelo digital de toda la planta de producción. Este gemelo no es meramente un modelo geométrico, contiene restricciones de movimiento y leyes de funcionamiento. Por lo tanto, puede emplearse de forma muy similar a como se haría en un sistema real, para desarrollar toda la ingeniería de sistemas necesaria. Programación y sistemas de control pueden ser añadidos en el gemelo y pueden ser simulados para predecir el funcionamiento del sistema real, sin la existencia del mismo (puesta en marcha virtual). Esto repercutirá en la reducción de los tiempos de desarrollo de la ingeniería de planta de manera drástica, permitiendo adelantar las fases de puesta en marcha y acortando los procesos en la realidad.

- **Desarrollo simultáneo de la Ingeniería de Sistemas**: En el desarrollo de un proyecto de una nueva planta hasta ahora, la ingeniería de sistemas ha llegado siempre de manera secuencial, con posterioridad a la construcción física de la misma, por lo tanto, se trataba de una fase que debía esperar a que el proyecto avanzase hasta ese punto para iniciarse. Los sistemas de información que se emplean en la actualidad están dotados de la posibilidad de interactuar con los modelos digitales, la existencia de un gemelo digital de la planta, va a permitir iniciar la ingeniería de sistemas en la fase de diseño de la planta y por tanto simultanear su desarrollo, adelantando esta fase, por otro lado los modelos ciberfísicos van a permitir incluso la puesta a punto de las tareas de control más complejas en el sistema ciberfísico, de forma previa a la construcción del sistema real.

- **Gestión de la operación y mantenimiento**: El impacto de la fabricación digital puede incidir a dos niveles, en la fase de diseño, como ya se ha mencionado va a ser un factor clave en la puesta en marcha, pero también va a tener gran impacto en la fase de explotación, el sistema ciberfísico creado permitirá intercambiar datos en todo momento con el sistema real, lo que permitirá obtener información clave, que permitirá refinar los modelos empleados en sucesivos desarrollos, pero sobre todo mejorar tareas propias de la explotación como la gestión automatizada del mantenimiento, y el aumento de eficiencia a todos los niveles del sistema real en operación. La computación en la nube, pero sobre todo el empleo de nuevas herramientas software virtualizables que permitan trabajar de forma deslocalizada en la gestión de las operaciones y el mantenimiento de las empresas, van a permitir el desarrollo de aplicaciones de soporte, de asistencia en la toma de decisiones y de inteligencia artificial, que permitirán implantar sistemas de gestión mucho más avanzados, sin la necesidad de tener que asociarlos geográficamente a los medios productivos, y con la capacidad de aprovechar recursos humanos que participen en otras tareas similares de otros ámbitos.

- **Diseño del producto y gestión del proyecto deslocalizados**: En el nuevo paradigma de la Industria 4.0, y con la irrupción de las nuevas tecnologías de computación en la nube, se va a modificar por completo la forma de trabajar en los proyectos, el diseño del producto por ejemplo puede acometerse de forma deslocalizada geográficamente, la gestión de los proyectos, también se podrá llevar a cabo de la misma forma, la herramientas software en gran medida virtualizadas y residentes en la nube, van a permitir esta nueva forma de organización en el trabajo, si bien es cierto que hará falta un periodo de adaptación en las organizaciones, y un cambio por parte de las personas para adaptarse al nuevo paradigma.

- **Fabricación flexible y deslocalizada**: En la Industria 3.0 la localización geográfica de los medios y los sistemas de fabricación, así como de las OT (Tecnologías de la información para la operación), ha sido fundamental y necesaria en un ámbito local. La irrupción de nuevos procesos de fabricación, fácilmente deslocalizables como la Fabricación Aditiva, aún en fase emergente, unido a la automatización masiva (sobre todo robotización), de procesos que hasta ahora no estaban automatizados, va a contribuir a que no haya dependencia local de ciertos territorios en los sistemas de fabricación, y que las plantas puedan ubicarse con libertad geográfica independientemente de los costes laborales. Por otro lado, como los sistemas de información para la operación, van a estar virtualizados y en la nube, interconectados, en definitiva, tampoco estos sistemas van a quedar sujetos, por tanto, a una determinada localización geográfica próxima a los medios productivos. El conjunto de los medios de producción de una compañía será por tanto más flexible y reconfigurable, deslocalizado geográficamente y por tanto con mayor capacidad productiva, pero sobre todo adaptable a los cambios de la demanda.

- **Planificación estratégica integrada**: Por último, tareas hasta ahora reservadas a personas como las de planificación estratégica de la empresa, podrán plantearse de manera simultánea con sistemas basados en algoritmos de inteligencia artificial, algoritmos que ya están empezando a dar frutos en otros campos de la ciencia y la tecnología, podrán aprender de nuestros procesos industriales en un plazo razonablemente corto y dar soluciones innovadoras y hasta ahora impensables para la mente humana. Es quizá la parte de la Industria 4.0 más interesante y que más inquietud puede llegar a provocar, pero el futuro es sin duda diferente e inimaginable, y la tecnología ha conseguido ir a la misma velocidad que nuestros pensamientos.

4. VULNERABILIDADES DE SEGURIDAD EN LOS SISTEMAS DE CONTROL INDUSTRIAL

La incorporación de las Tecnologías de la Información y Comunicaciones a los procesos industriales ha propiciado la aparición de las mismas vulnerabilidades, propias los sistemas informáticos, dentro de las infraestructuras críticas de los entornos industriales. En este capítulo, analizaremos dichas vulnerabilidades, centrándonos en las que más afectan a los Sistemas de Control Industrial y; a continuación, se expondrán varios casos en los que se han producido ataques a los entornos industriales críticos con diversas consecuencias reseñables.

4.1. AMENAZAS Y VULNERABILIDADES EN SISTEMAS DE CONTROL INDUSTRIAL

En este apartado se exponen las vulnerabilidades de seguridad más frecuentes en los Sistemas de Control Industrial según el informe de la organización Kaspersky Labs correspondiente al año 2017 [15].

Las posibles consecuencias de los incidentes de seguridad en Sistemas de Control Industrial incluyen daños en la calidad del producto y del servicio, pérdida de patentes o información confidencial y reducción o pérdida de la producción, por lo tanto, al tratarse de sistemas críticos para las organizaciones, la seguridad de estos sistemas debe asegurarse.

Los componentes de los Sistemas de Control Industrial que mayor número de vulnerabilidades presentan son: [15]

- Los componentes de los sistemas SCADA y HMI.
- PLCs.
- Dispositivos de red diseñados para entornos industriales (Switches industriales).
- Software de Ingeniería.
- Relés de protección.
- Sistemas de apagado de emergencia.
- Sistemas de Supervisión Ambiental.
- Sistemas de Video-Vigilancia Industrial.

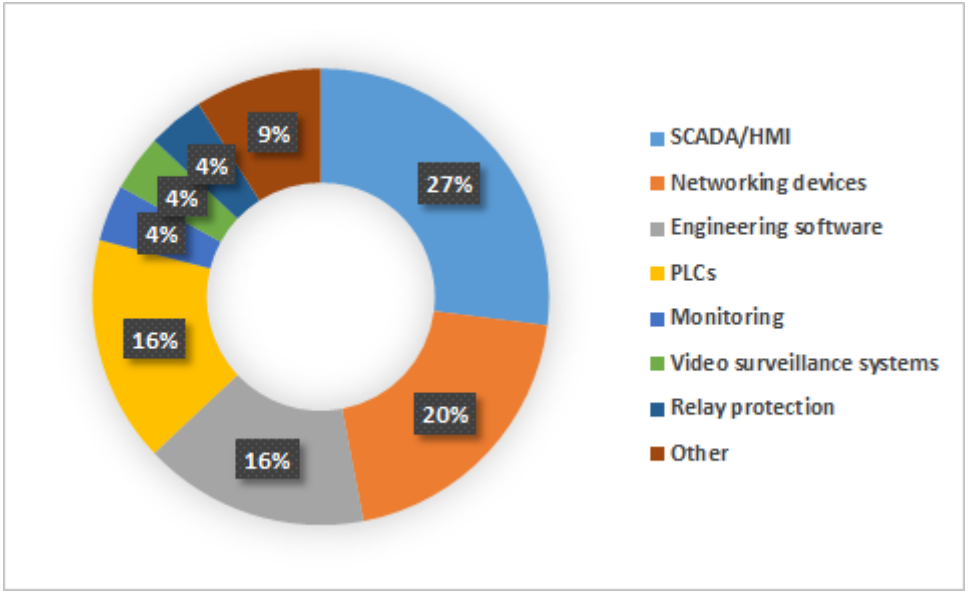

FIGURA 8- DISTRIBUCIÓN DE VULNERABILIDADES POR COMPONENTES DE LOS SISTEMAS DE CONTROL INDUSTRIAL (FUENTE: [15])

En cuanto al tipo de vulnerabilidades que afectan a los sistemas industriales, los más comunes son los desbordamientos de buffers (Buffer Overflow) y autenticaciones incorrectas (Improper Authentication). También son destacables las vulnerabilidades relacionadas con sistemas web (Injection, Path Traversal, Cross-Site Request Forgery – CSRF – y Cross-Site Scripting), aquellas relacionadas con problemas de autenticación (Improper Authentication, Authentication Bypass y ausencia de autenticación para funciones críticas) y las vulnerabilidades de problemas en el control de acceso (control de acceso, permisos por defecto incorrectos, gestión incorrecta de privilegios y gestión de credenciales).

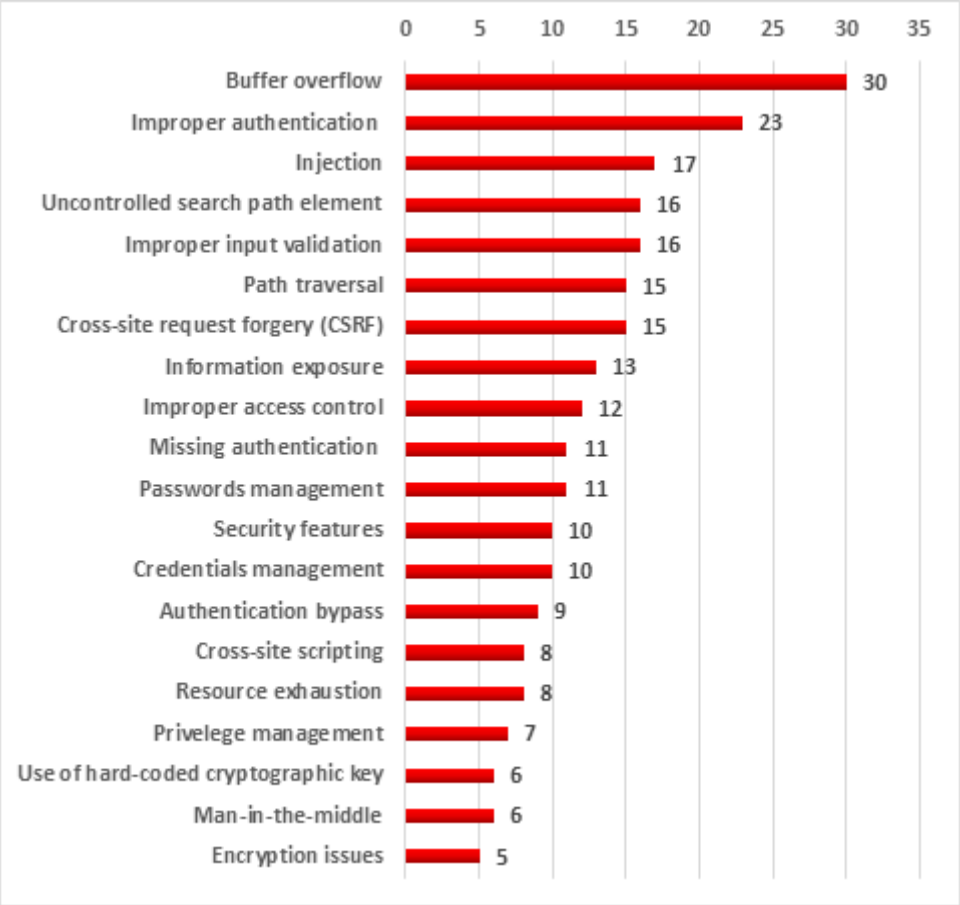

FIGURA 9 - TIPOS DE VULNERABILIDADES MÁS COMUNES (FUENTE: [15])

A continuación, detallaremos algunas vulnerabilidades de seguridad en ciertos elementos de los Sistemas de Control Industrial.

4.1.1. Vulnerabilidades en protocolos industriales.

Según el estudio de Kaspersky Lab [15] existen vulnerabilidades graves en la implementación de protocolos industriales. Específicamente, se identificaron vulnerabilidades en la implementación del Protocolo Modbus en los controladores de la serie Modicon [16], así como en implementaciones de la pila de protocolos OPC UA [17] y en una implementación del Protocolo de descubrimiento y configuración de PROFINET [18]. Estos problemas de seguridad identificados afectan a familias enteras de productos.

4.1.2. Impacto de Vulnerabilidades de tecnologías tradicionales en sistemas industriales.

Además de las vulnerabilidades específicas de los Sistemas de Control Industrial, existe una serie de debilidades graves en plataformas de software y protocolos de red que pueden ser explotados para atacar sistemas industriales.

Las vulnerabilidades en el protocolo WPA2 resultan relevantes para las soluciones industriales. Afectan a los equipos de varios proveedores, entre ellos Cisco, Rockwell Automation, Sierra Wireless, ABB y Siemens. Los sistemas de control industrial también se ven afectados por múltiples vulnerabilidades en

el servidor DNS de Dnsmasq [19], Java Runtime Environment [20], Oracle Java SE [21] y Cisco IOS e IOS XE [22].

Las vulnerabilidades en los productos Intel también pueden afectar la seguridad de los equipos industriales. En la segunda mitad de 2017, se publicó información sobre varias vulnerabilidades en los productos Intel [23] (ME, SPS y TXE). Estas vulnerabilidades afectan principalmente al hardware de servidores SCADA y las computadoras industriales que utilizan CPU vulnerables. Como norma, los proveedores no consideran necesario publicar avisos públicos sobre vulnerabilidades de este tipo (derivadas del uso de tecnologías de terceros). Por supuesto, hay algunas excepciones positivas; por ejemplo, Siemens AG ha publicado un aviso que indica que estas vulnerabilidades afectan a una variedad de productos de la compañía.

4.1.3. Vulnerabilidades en componentes del ICS.

El estudio de Kaspersky Labs [15] identificó unas 30 vulnerabilidades en productos de Sistemas de Control Industrial de diferentes fabricantes, tales como Schneider Electric, Siemens, Rockwell Automation, Emerson y otros.

4.1.4. Vulnerabilidades en soluciones basadas en hardware y software de terceras partes.

Los expertos de Kaspersky Lab ICS CERT [15] también analizaron soluciones de terceros basadas en hardware que se utilizan ampliamente en sistemas de automatización industrial.

Específicamente, los expertos analizaron la solución basada en el hardware SafeNet Sentinel de Gemalto. Como resultado de la investigación, se identificaron 15 vulnerabilidades en el software de la solución que afectan a una gran cantidad de productos que utilizan este software vulnerable, incluidas soluciones de ABB, General Electric, HP, Cadac Group, Zemax y otros desarrolladores de software, cuyo número puede llegar a 40 mil, según algunas estimaciones.

4.1.5. Vulnerabilidades en componentes IoT.

En los últimos tiempos se ha detectado un creciente número de vulnerabilidades en los dispositivos de Internet de las cosas (IoT). Como consecuencia, tales vulnerabilidades son cada vez más explotadas para crear botnets. Por ejemplo, nos encontramos la botnet Reaper [24] y las nuevas variantes de Mirai, incluida la botnet Satori [25].

Se han identificado múltiples vulnerabilidades en routers, cámaras IP inalámbricas, grabadores de video en red y otros dispositivos.

Además de las nuevas debilidades en los dispositivos de IoT, algunas vulnerabilidades antiguas aún no están corregidas, y hay ciertas amenazas que pueden aprovecharse para obtener la configuración de los conversores de serie a Ethernet. Esta vulnerabilidad en los conversores de serie a Ethernet afecta directamente la Internet industrial de las cosas (IIoT), ya que muchos sistemas que permiten a los operadores de equipos industriales controlar de forma remota su estado, modificar su configuración y controlar su funcionamiento se basan en conversores de interfaz serie.

La seguridad de los dispositivos de IoT también se ve afectada por problemas relacionados con la seguridad de la tecnología de información tradicional. Por ejemplo, las vulnerabilidades en las implementaciones del protocolo Bluetooth llevaron a la aparición del nuevo vector de ataque BlueBorne [26], que representa una amenaza para los sistemas operativos móviles, de escritorio y de IoT.

4.1.6. VULNERABILIDADES EN ROUTERS INDUSTRIALES.

En el informe de Kaspersky Labs [15] se identifican numerosas vulnerabilidades en dispositivos de redes industriales de diferentes proveedores. Las vulnerabilidades típicas que estos presentan son: divulgación de información, escalada de privilegios, ejecución de código arbitrario, denegación de servicio.

4.1.7. MALWARE EN SISTEMAS DE AUTOMATIZACIÓN.

Muchas empresas industriales utilizan modernas tecnologías de redes que mejoran la transparencia y la eficiencia de los procesos de gestión empresarial, además de proporcionar flexibilidad y tolerancia a fallos para todos los niveles de automatización industrial. Como resultado, las redes industriales son cada vez más similares a las redes corporativas, tanto en términos de escenarios de uso como en términos de tecnologías utilizadas. La desventaja de esto es que las amenazas de Internet, así como otras amenazas tradicionales de TI, afectan cada vez más a las redes industriales de las organizaciones modernas. Esto incluye el software malintencionado o Malware que amenaza cada vez más a los Sistemas de Control Industrial y obliga a mantener los sistemas antivirus actualizados también en entornos industriales.

4.2. INCIDENTES DE SEGURIDAD CONOCIDOS EN SISTEMAS DE CONTROL INDUSTRIAL

4.2.1. STUXNET

Stuxnet es el nombre con el que se ha bautizado a un gusano que, en enero de 2010 atacó las computadoras de una planta nuclear iraní ubicada en la localidad de Natanz [27]. Stuxnet no era como ningún otro virus o gusano conocidos anteriormente, en lugar de secuestrar los equipos objetivo o robar la información contenida en los mismos, pretendía provocar daño físico de los equipos controlados por las computadoras infectadas.

Se piensa que Stuxnet es la primera arma digital de la historia [28] porque su ataque se centró en dejar inutilizables las centrifugadoras que se usaban para enriquecer uranio en la planta nuclear iraní. Se sospecha que el gusano fue diseñado y propagado por parte de Estados Unidos para sabotear el programa nuclear de Irán.

Según las investigaciones posteriores, parece que, al no ser accesibles desde Internet las computadoras de la planta de Natanz, la infección se realizó a través de cinco empresas externas que se creía que estaban conectadas de alguna manera con el programa nuclear. El objetivo era convertir a cada "paciente cero" en un portador involuntario que ayude a extender y transportar el arma en memorias flash a las instalaciones protegidas y las computadoras de Siemens.

Se conoce que el ataque se llevó a cabo en dos fases, una primera en enero de 2010 y la segunda cinco meses después. Para llevar su arma a la planta, los atacantes utilizaron la misma estrategia que en la anterior infectado las computadoras de otras compañías que estaban involucradas en el control industrial y el procesamiento de algún tipo, ya sea fabricando productos y ensamblando componentes o instalando sistemas de control industrial. Probablemente todos fueron elegidos porque tenían alguna conexión con Natanz como contratistas y proporcionaron una puerta de entrada a través de la cual pasar Stuxnet a Natanz a través de empleados infectados.

Para asegurar un mayor éxito en la obtención del código donde debía llegar, esta versión de Stuxnet tenía dos formas más de propagarse que la anterior. Stuxnet 0.5 podría propagarse solo al infectar los

archivos del proyecto de Siemens Step 7, los archivos utilizados para programar los PLC de Siemens. Sin embargo, esta versión podría propagarse a través de unidades flash USB usando la función de ejecución automática de Windows o a través de la red local de la víctima usando la vulnerabilidad de día cero de la cola de impresión que se encontraron posteriormente en el código.

Este ataque se hizo famoso por el contexto de geopolítica que le rodea y por la magnitud de la operación, además de ser el primer ataque conocido en haber tenido éxito en menoscabar las operaciones de una infraestructura industrial y en dañar las instalaciones de una planta.

4.2.2. BLACKENERGY

A finales de 2015, la mitad de los hogares en la región ucraniana Ivano-Frankivsk se quedaron sin electricidad durante unas horas. Tras las investigaciones realizadas, se concluyó que los cortes de electricidad se debieron a un ciberataque que, utilizando el malware de puerta trasera BlackEnergy, instaló el componente KillDisk en los equipos objetivo, cuya función es impedir que arranquen.

El vector de infección utilizado en estos ataques son archivos de Microsoft Office que contienen macros maliciosas que, al ejecutarse hacen que el equipo quede infectado. El escenario de ataque es como sigue: el equipo de destino recibe un correo electrónico que contiene un archivo adjunto con un documento malicioso. Los atacantes suplantan la dirección del remitente para que parezca que pertenece a Rada (el Parlamento ucraniano).

El documento en sí contiene un texto que trata de persuadir a la víctima para que ejecute la macro del documento. Este es un ejemplo donde se emplea la Ingeniería Social en lugar de aprovechar las vulnerabilidades del software. Si se logra engañar a las víctimas, terminan infectadas con BlackEnergy Lite.

El troyano BlackEnergy es modular y emplea diversos componentes descargables para llevar a cabo tareas específicas. En el caso del ataque en Ucrania, se descubrió que el malware KillDisk estaba presente en los sistemas infectados. Además de borrar archivos del sistema para que el equipo no arranque, la variante KillDisk detectada en las compañías eléctricas también parece contener algunas funciones adicionales destinadas específicamente a sabotear los sistemas industriales.

En primer lugar, establece un tiempo de retardo específico después del cual se activa la carga destructiva. A continuación, además de su funcionalidad habitual, KillDisk intenta poner fin a dos procesos que no son estándar: komut.exe y sec_service.exe. El segundo proceso, sec_service.exe, puede pertenecer a un software llamado ELTIMA Serial to Ethernet Connector o ASEM Ubiquity, una plataforma muy utilizada en los Sistemas de Control Industrial (ICS). Si el troyano encuentra este proceso en el sistema de destino, no sólo lo cerrará, sino que también sobrescribirá el archivo ejecutable y lo reemplazará por datos aleatorios para dificultar la restauración del sistema. [29]

De nuevo este caso se produce en una zona con una alta tensión geopolítica como Ucrania y se piensa que el ataque fue lanzado por los servicios de seguridad rusos.

Se conoce de la existencia de un nuevo malware llamado GreyEnergy que podría estar relacionado con BlackEnergy. La estructura de GreyEnergy presenta muchas similitudes con BlackEnergy. Presenta una construcción modular similar, con lo cual su funcionalidad depende de la particular combinación de módulos que su operador cargue para cada uno de los sistemas de sus víctimas. Se ha observado que los operadores de GreyEnergy han estado dirigiéndose estratégicamente a estaciones de trabajo de

Sistemas de Control Industrial que corren software SCADA, los cuales tienden a ser sistemas esenciales que jamás se desconectan, salvo para tareas de mantenimiento.

A diferencia de BlackEnergy, GreyEnergy es un conjunto de herramientas más moderna que incluso presenta un mejor enfoque en cuanto a discreción; una técnica básica para evitar ser detectado es la de empujar solamente los módulos seleccionados hacia blancos elegidos y únicamente cuando es necesario. Encima de eso, algunos de los módulos de GreyEnergy están parciamente cifrados y algunos permanecen sin archivos (corriendo solo en memoria) con la intención de dificultar el análisis y la detección. Para evitar ser rastreado, los operadores de GreyEnergy generalmente limpian de manera segura los componentes del malware del disco rígido de la víctima [30].

4.2.3. Operation Ghoul

En agosto de 2016, se hizo evidente la vulnerabilidad de la industria manufacturera a las amenazas cibernéticas. Los investigadores de Kaspersky Lab descubrieron una sofisticada operación de ciberdelincuencia dirigida a más de 130 empresas de manufactura, industria e ingeniería en más de 30 países. Usando técnicas de phishing por correo electrónico que usaban correos electrónicos falsos de los bancos, la Operación Ghoul intentó que los destinatarios dieran información corporativa confidencial [31].

El phishing iba dirigido a miembros de alto nivel y ejecutivos de las organizaciones, probablemente porque los atacantes esperaban obtener inteligencia estratégica, cuentas de control y otra información interesante.

El objetivo de la Operation Ghoul era financiero, ya que la información hackeada se ha rastreado hasta las ventas en el mercado negro. Los ataques en sí mismos son ataques muy básicos de phishing, pero los humanos somos bastante crédulos. Los correos electrónicos que forman parte de estos ataques parecían provenir de un banco en los Emiratos Árabes Unidos: parecían consejos de pago del banco con un documento SWIFT adjunto, pero en realidad el archivo adjunto contenía malware.

El malware en cuestión se compra fácilmente en la Dark Web. Denominado HawkEye, este malware puede registrar pulsaciones de teclado, credenciales del servidor FTP, datos de cuentas de varias fuentes (correo electrónico, clientes de mensajería y navegadores) y programas o aplicaciones instaladas en la computadora infectada. Una vez que se recopilan los datos, se envían a la dirección IP 192.169.82.86, que Kaspersky Lab considera es un dispositivo comprometido que ejecuta varias campañas de malware.

Para evitar este tipo de ataques, las empresas deberían comenzar a tomarse en serio la capacitación en seguridad, equipando a cada empleado con los protocolos adecuados de seguridad cibernética, estos tipos de ataques continuarán ocurriendo. Puede tener la mejor IDS del mundo, pero eso significa que se pondrá en cuclillas si su CEO está abriendo correos electrónicos que infectan toda la red [32].

4.2.4. WannaCry

El ransomware WannaCry no se diseñó específicamente para infectar sistemas de control industrial, pero consiguió infiltrarse en varias redes de Sistemas de Control Industrial, lo que causó una inactividad en los procesos industriales.

Como ya se ha mencionado en apartados anteriores, es importante tener en cuenta que algunas amenazas de las Tecnologías de la Información pueden causar un daño mucho más significativo en una red industrial que en una red de oficina.

En el segundo semestre de 2017, varias empresas detectaron infecciones masivas de redes industriales con el malware de cifrado WannaCry. Más tarde, se determinó que las infecciones iniciales de las redes de oficinas en las compañías víctimas habían tenido lugar en todos los casos ocurridos en la primera mitad de 2017, en el momento más alto del brote de WannaCry. Sin embargo, las infecciones no se notaron hasta que el malware se propagó a las redes industriales de las empresas. Como se vio durante la investigación, la funcionalidad de cifrado en las muestras de malware se dañó y los sistemas infectados en las redes corporativas continuaron operando normalmente, sin fallas. Sin embargo, la infección de las redes industriales en estos casos tuvo consecuencias negativas inesperadas.

En una de las empresas infectadas por WannaCry, las estaciones de trabajo utilizadas por los operadores comenzaron a mostrar la "Pantalla Azul de la Muerte" todo el tiempo, lo que llevó a reinicios de emergencia. El motivo de esta inesperada consecuencia de la infección fue que las máquinas ejecutaban Windows XP. Es un hecho bien conocido que el exploit DoublePulsar utilizado por WannaCry para propagarse causa que Windows XP se bloquee, lo que resulta en una pantalla azul de la muerte y un reinicio. En los casos en que muchas máquinas en el segmento industrial de la red de una organización estén infectadas, las máquinas con Windows XP son a menudo atacadas y se reinician en casos de emergencia. Como resultado, los operadores se vuelven incapaces de monitorear y controlar el proceso industrial. Esto convierte a WannaCry en una herramienta de ataque de denegación de servicio.

En otro incidente, la propagación de WannaCry hizo que algunos de los dispositivos en la red industrial de una empresa dejaran de estar disponibles temporalmente durante los períodos en que la actividad de la red del malware coincidía con ciertas etapas del proceso industrial. Esto dio lugar a interrupciones de emergencia de un proceso industrial que fue crítico para la empresa durante un promedio de 15 minutos [15].

5. Posibles Soluciones a las Vulnerabilidades de seguridad en los sistemas de control industrial

Como ya se ha adelantado en capítulos anteriores, debido a la criticidad de los sistemas industriales para sus organizaciones, se hace necesario proteger estos sistemas de forma especialmente rigurosa. En este capítulo se discutirán las formas más habituales de proteger los sistemas en entornos industriales. En primer lugar, se pondrá en valor la necesidad de realizar una buena gestión de riesgos para los sistemas críticos, a continuación, se mostrarán ciertos estándares y buenas prácticas para la protección de los sistemas de control industrial y finalmente se mostrarán los distintos niveles del modelo de seguridad en profundidad.

5.1. Gestión de Riesgos en Sistemas de control Industrial

Como hemos visto en los incidentes de seguridad expuestos en el capítulo anterior, la mayoría de los ataques a sistemas de control industrial se pueden dividir en dos fases [3]:

- **Fase 1**: implica obtener acceso a la red de los Sistemas de Control Industrial por todos los medios posibles, con el objetivo de iniciar la fase 2 del ataque. Las actividades de la fase 1 incluyen establecer una posición en la red empresarial de una organización y desde allí encontrar un punto donde pivotar para saltar a la red de los Sistemas de Control Industrial. El objetivo de la etapa 1 en un ciberataque de entornos industriales casi siempre será ingresar a la red de los Sistemas de Control Industrial.

- **Fase 2**: comienza la parte de la explotación de los Sistemas de Control Industrial del ataque, donde se realizan las actividades necesarias para alcanzar los objetivos de la fase 2. Las actividades típicas de la fase 2 incluyen asegurar el acceso a la red de los Sistemas de Control Industrial, el sondeo y el mapeo de la red industrial, la creación de puertas traseras en dispositivos y aplicaciones industriales y la extracción de datos. El objetivo de la fase 2 de un ciberataque a Sistemas de Control Industrial puede ser el sabotaje del proceso de producción, el robo de propiedad intelectual, el espionaje corporativo y otros.

En definitiva, el objetivo final de un ataque a Sistemas de Control Industrial es el objetivo de la fase 2, ya sea sabotaje, robo de información o espionaje industrial.

5.1.1. Evaluación de Riesgos

La evaluación de riesgos según la norma ISO 27001, obliga a las organizaciones a [33]:

- Establecer y mantener ciertos criterios de riesgo de seguridad de la información.

- Asegurarse de que las evaluaciones de riesgo repetidas "produzcan resultados consistentes, válidos y comparables".

- Identificar los “riesgos asociados con la pérdida de confidencialidad, integridad y disponibilidad de la información dentro del alcance del sistema de gestión de seguridad de la información”, e identificar a los propietarios de esos riesgos.

- Analizar y evaluar los riesgos de seguridad de la información, de acuerdo con los criterios establecidos anteriormente.

Por su parte, en el Business Dictionary se define la evaluación de riesgos (risk assessment) como "La identificación, evaluación y estimación de los niveles de riesgos involucrados en una situación, su comparación con puntos de referencia o estándares, y la determinación de un nivel de riesgo aceptable."

En resumen, la evaluación de riesgos pretende descubrir todo lo que podría ir mal en una determinada situación. Al detectar las debilidades y vulnerabilidades de un sistema, las posibilidades de que algo vaya mal y el impacto potencial de dicha amenaza pueden ser determinados.

Según Clint Bodungen es al. "el riesgo es la probabilidad de que una fuente de amenaza cause un evento de amenaza, mediante un vector de amenaza, debido a una vulnerabilidad potencial en un objetivo, y cuál será la consecuencia y el impacto resultantes" [34].

- Una fuente de amenaza es el iniciador del exploit.
- Un evento de amenaza es el acto de explotar una vulnerabilidad o ataque al sistema en consideración.
- Un vector de amenaza es la vía de ataque o el método de entrega del exploit.
- Una vulnerabilidad es una debilidad del sistema en consideración.
- Probabilidad es la posibilidad de que la vulnerabilidad encontrada se convierta en un evento de amenaza.
- Un objetivo es el sistema en consideración.
- Una consecuencia es el resultado directo de un evento de amenaza exitoso.
- El impacto es el resultado del buen estado de las operaciones, la imagen o el estado financiero de la empresa.

En definitiva, una evaluación de riesgos consiste en evaluar qué vulnerabilidades acechan en el sistema en consideración, qué posibilidades hay de que estas vulnerabilidades sean explotadas y cuáles son las consecuencias de una explotación exitosa para el sistema, la empresa propietaria del sistema y el impacto ambiental. El resultado de una evaluación de riesgo es la puntuación de riesgo para una vulnerabilidad descubierta. El puntaje toma en consideración todos los factores que definen el riesgo al aplicar la siguiente ecuación:

$$riesgo = \frac{gravedad + (criticidad * 2) + (probabilidad * 2) + (impacto * 2)}{4}$$

En esta ecuación de puntuación:

- La *gravedad* es un número entre 0 y 10, dado a la vulnerabilidad por parte de un servicio como la Base de datos de vulnerabilidad nacional mediante la aplicación de un algoritmo como el Common Vulnerability Scoring System (CVSS).

- La *criticidad* es un número entre 1 y 5 que refleja la importancia del sistema en consideración para el proceso general.
- La *probabilidad* es un número entre 1 y 5 que refleja la posibilidad de que la vulnerabilidad se convierta en un evento de amenaza exitoso o, la posibilidad de que la vulnerabilidad se aproveche exitosamente.
- El *impacto* es un número entre 1 y 5 que refleja el impacto financiero en la empresa, el daño asociado a la imagen de la empresa, el impacto potencial en el medio ambiente y el riesgo asociado p ara los empleados y la seguridad de la salud pública en caso de un fallo de este sistema.

Debido a las limitaciones presupuestarias en TI y OT, los esfuerzos de mitigación deben concentrarse en las áreas que mitigan el mayor riesgo para los esfuerzos y dinero gastado. Para ese momento, la asignación de valores a estos cuatro factores debe hacerse de manera comparativa. El proceso completo debe tenerse en cuenta al evaluar los sistemas individuales y las vulnerabilidades dentro de esos sistemas. Cuanto mejor sea la puntuación correlativa, más accionable será la puntuación para que los esfuerzos de mitigación puedan ser mejor dirigidos y se logre un mejor retorno de la inversión. Los primeros tres valores de puntuación de riesgo son relativamente sencillos de evaluar:

- La *gravedad* es un número establecido, asignado por un algoritmo de puntuación utilizado por sistemas como CVSS.
- La *criticidad* es la puntuación resultante de evaluar la importancia del sistema dentro del proceso general.
- El *impacto* es una combinación del coste de recuperación del sistema, el coste asociado con el impacto ambiental, el coste relacionado con el impacto de la seguridad y la salud pública de los empleados y el coste relacionado con los esfuerzos de relaciones públicas en caso de que se materialice la amenaza. Combinando estos costes, se calcula un coste total de que se cumpla la amenaza, lo que crea una puntuación de acción cuando se correlaciona con todos los otros sistemas dentro del proceso.

La calidad de una evaluación de riesgos se basa, en gran medida, en el cálculo de la puntuación de probabilidad. La puntuación de la probabilidad agrega información sobre la probabilidad de que la vulnerabilidad descubierta se aproveche y genere un evento de amenaza.

A continuación, se detallan las tres actividades que se deben realizar para una correcta gestión de riesgos:

La primera etapa es la **identificación de activos** y la **caracterización del sistema**:

- Esta etapa implica encontrar todos los activos del sistema en consideración y evaluar su criticidad y el valor de los activos, utilizados para el cálculo de la puntuación del impacto.
- El resultado de este paso es una lista de objetivos potenciales

La segunda etapa es la **identificación de vulnerabilidades** y el **modelado de amenazas**:

- Esta etapa implica descubrir cualquier vulnerabilidad potencial dentro de los activos descubiertos y su puntuación CVSS asociada para el cálculo de gravedad.
- Esta etapa implica el uso de técnicas de modelado de hilos para agregar información sobre vectores de amenazas, eventos de amenazas y fuentes de amenazas.

- Esta etapa evalúa la probabilidad y consecuencia de un compromiso.
- El resultado de esta etapa será una lista de matrices con posibles escenarios de riesgo, que serán relevantes y procesables para el sistema en cuestión.

La tercera etapa es el cálculo y mitigación de riesgos:

- Esta etapa implica evaluar el impacto total de un evento de amenaza para la vulnerabilidad de cada objetivo descubierto.
- Combinando toda la información descubierta, esta etapa calcula la puntuación del riesgo.
- El resultado de esta etapa será una puntuación del riesgo accionable por vulnerabilidad que ayuda a diseñar estrategias de mitigación.

En resumen, para protegerse de los ataques que pueden sufrir los Sistemas de Control Industrial se debe realizar una completa evaluación de riesgos que permita, dentro del presupuesto de la organización, mitigar los riesgos que tengan mayor impacto y gravedad. Más aún, cuando dichos sistemas son críticos para las operaciones de la organización o la seguridad de las personas y el medioambiente.

5.2. Estándar ISA-99/IEC-62443, Industrial Automation and Control Systems Security

El estándar IEC-62443, anteriormente conocido como ISA-99, es el estándar global para la seguridad de las redes de los Sistemas de Control Industrial y ayuda a las organizaciones a reducir el riesgo de fallos y la exposición de las redes de los Sistemas de Control Industrial a las ciberamenazas. Este estándar fue desarrollado por la Sociedad Internacional de Automatización (ISA) y asumido por la Comisión Electrotécnica Internacional (IEC) para su desarrollo posterior. El marco de esta norma guía a los operadores de redes de Sistemas de Control Industrial a través de los requisitos, controles y mejores prácticas necesarias para una red industrial segura.

Como se ha adelantado en el capítulo anterior, la fase 1 de un ataque a un Sistema de Control Industrial implicaba obtener acceso a la red de esto sistemas, por lo tanto, al securizar la red estamos evitando esta primera fase del ataque.

Este estándar IEC-62443 consta de trece documentos organizados en cuatro grupos: General, Políticas y procedimientos, Sistema y Componentes. Los primeros dos grupos describen conceptos, casos de uso, políticas y procedimientos asociados con la seguridad de Sistemas de Control Industrial, mientras que los dos últimos grupos, Sistema y Componentes, definen los requisitos técnicos para las redes y los componentes del sistema.

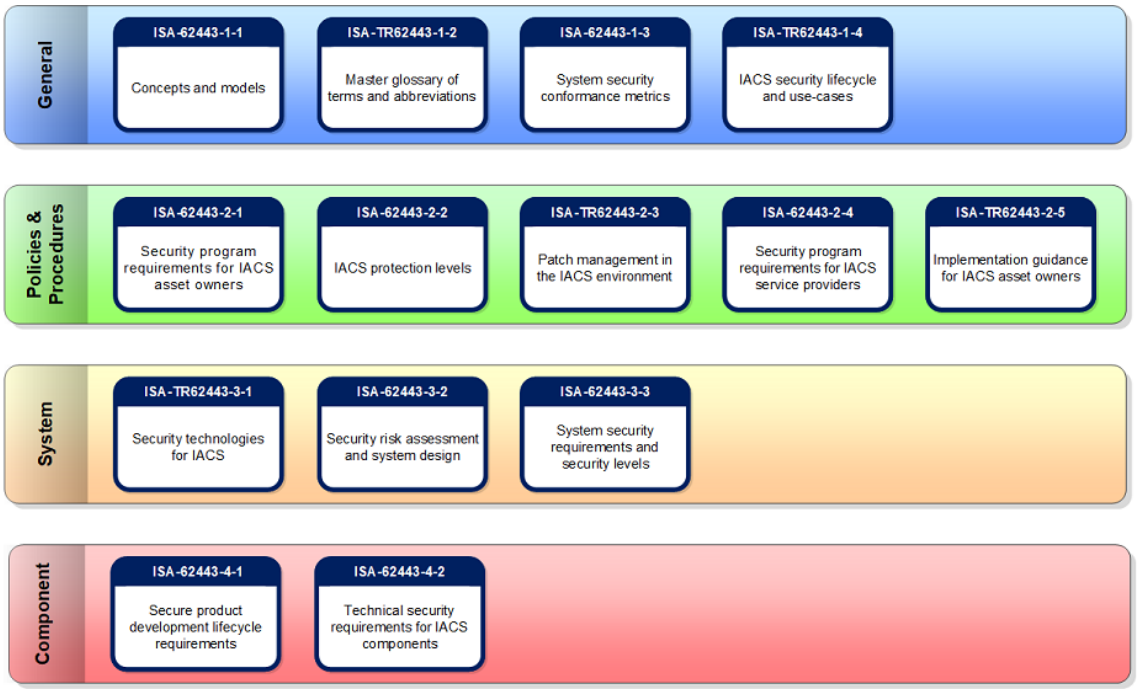

FIGURA 10 - ESTRUCTURA DEL ESTÁNDAR ISA-99/IEC-62443 [35]

Nos centraremos a continuación en los grupos de Sistemas y Componentes de la norma ISA-99/IEC-62443:

Requisitos del sistema:

Los tres documentos dentro del grupo Sistema se refieren a las opciones de diseño, modificaciones o ajustes necesarios para mejorar la seguridad de una red de Sistemas de Control Industrial.

- El primer documento (IEC 62443-3-1) proporciona una descripción general de las tecnologías de seguridad de red existentes, sus ventajas y limitaciones.
- El segundo (IEC 622443-3-2) aborda la evaluación de riesgos de seguridad y el diseño de la red. Sugiere cómo las organizaciones deben segmentar su red en zonas y conductos, agrupando sistemas que tienen una funcionalidad similar y restringen el acceso para limitar la exposición y propagación de amenazas.
- Finalmente, el tercer documento (IEC 62443-3-3) describe los requisitos generales de seguridad del sistema, como la autenticación, la confidencialidad de los datos y la integridad del sistema, haciendo hincapié en que el rendimiento y la disponibilidad no deben verse comprometidos durante el proceso de abordar estos requisitos.

Requisitos de los componentes:

El grupo de componentes consta de dos documentos. El primero (IEC 62443-4-1) trata con un proceso de desarrollo para productos de Sistemas de Control Industrial, destinado a reducir el número de vulnerabilidades de seguridad en las soluciones de sistemas de control. El segundo documento (IEC 62443-4-2) especifica los requisitos técnicos para asegurar los componentes individuales de una red de Sistemas de Control Industrial.

Basándonos en los requisitos de los grupos de Sistemas y Componentes, podemos identificar cuatro pasos que los operadores industriales deben seguir para mejorar la seguridad de su red de Sistemas de Control Industrial e implementar con éxito la norma IEC 62443 [36]:

1) Recopilación de datos: No puede proteger adecuadamente una red si no sabe qué es lo que necesita ser asegurado. La recopilación de información precisa de activos, que incluye detalles sobre cómo se comunican y cómo funciona la red, es un primer paso fundamental para mejorar la seguridad.
2) Evaluación de seguridad de red: Este paso implica analizar los resultados del primer paso y evaluar el estado actual de seguridad de la red. Esto nos permitirá determinar la mejor estrategia para aplicar las modificaciones o ajustes necesarios.
3) Construir la solución: El paso tres aprovecha los puntos críticos y las prioridades identificadas en el paso 2 y prepara la red para la implementación de las contramedidas necesarias. Esto incluye la definición de procedimientos, la identificación y separación de la red en zonas y la definición de conductos (es decir, flujos de comunicación).
4) Despliegue de soluciones: El último paso para asegurar la red es implementar las contramedidas elegidas, que podrían, por ejemplo, estar representadas por la tecnología de monitorización y segmentación. Estas medidas deben integrarse en la operación diaria para mantener la seguridad de la red y sus procesos.

Para garantizar el éxito de la implantación del estándar IEC 62443, es importante trabajar sistemáticamente a través de los cuatro pasos anteriores. Sin datos y evaluaciones completas y precisas, y sin implementar soluciones basadas en procedimientos bien definidos, no se puede garantizar un resultado exitoso y la red puede permanecer insuficientemente protegida contra amenazas.

El estándar ISA-99/IEC-62443 establece un marco que se utiliza para describir las funciones básicas y la composición de un sistema de fabricación. El marco, como se muestra en la siguiente figura, identifica los niveles y las zonas que se pueden encontrar en un Sistema de Control Industrial moderno:

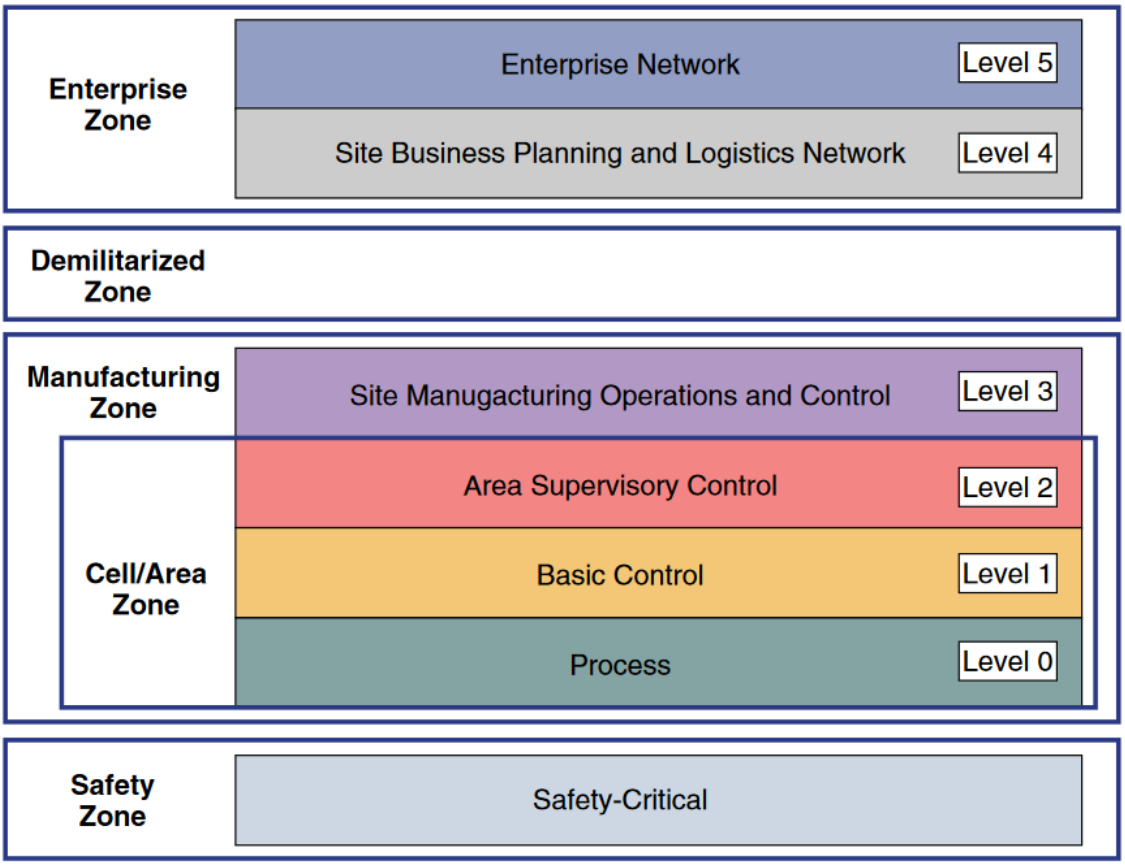

FIGURA 11- MARCO DE UN SISTEMA DE CONTROL INDUSTRIAL SEGÚN ISA-99/IEC-62443 (FUENTE: [37])

A continuación explicaremos brevemente cada uno de los niveles y zonas definidos por el estándar ISA-99/IEC-62443 [37]:

- **Zona de Seguridad (Safety Zone)**: Los sistemas de seguridad son a menudo la medida preventiva final para una catástrofe de todo el sistema. Tener estos sistemas en la misma red que el resto del Sistema de Control Industrial no tiene mucho sentido desde una perspectiva de seguridad, ya que son un objetivo para atacar, pero desde un punto de vista práctico, poder monitorizar, cambiar e interactuar con el sistema de seguridad tiene sentido; por lo tanto, los sistemas de seguridad aparecen cada vez más en las redes de Sistemas de Control Industrial. La creación de una zona de seguridad dedicada para estos sistemas de seguridad permite un control estricto e inspección del tráfico hacia y desde ellos.
- **Zonas de Áreas o celdas (Cell/Area Zone)**: Una zona de área es un área funcional dentro de una planta o instalación. Puede ser una línea de producción individual o parte de una línea de producción. En general, la mayoría de las plantas tienen múltiples zonas de área que se definen como una agrupación de dispositivos de Sistema de Control Industrial, todos trabajando hacia un objetivo común como producir un producto o ensamblar una parte del producto. Los dispositivos en una zona de área pueden comunicarse sin obstáculos y en tiempo real, pero el tráfico que sale o ingresa a la zona de área está sujeto a inspección. Una zona de área típica incluye tres niveles de actividad entre dispositivos relacionados de los Sistemas de Control Industrial, como PLC, HMI, sensores, actuadores y el equipo de red utilizado para comunicarse.

- *Nivel 0 - El proceso*: consta de una amplia variedad de sensores y actuadores involucrados en el proceso de fabricación básico. Estos dispositivos realizan las funciones principales del Sistema de Control Industrial, como arrancar un motor, medir variables, establecer una salida y realizar funciones clave, como pintar, soldar, doblar, etc. Estas funciones pueden ser muy simples (indicador de temperatura) o muy complejas (un robot en movimiento). Históricamente, esta era el área de dispositivos de campo y sus correspondientes protocolos (propietarios). En la actualidad, la omnipresencia de las tecnologías de red convergentes ha llevado a Ethernet e IP a estas áreas como un protocolo de comunicación. Tener estos dispositivos en la misma red permite acceder a ellos desde cualquier lugar de la red del Sistema de Control Industrial, lo cual agrega funcionalidad y permite una fácil administración de estos dispositivos; pero, a menos que esté debidamente protegido en el perímetro de la red o en los límites de seguridad, los expone a ataques.
- *Nivel 1 - Control básico*: consiste en controladores ICS que dirigen y manipulan el proceso de fabricación. Su función clave es interactuar con dispositivos de nivel 0 (por ejemplo, sensores y actuadores). En el proceso de fabricación, el controlador ICS se conoce como un sistema de control distribuido (DCS). Los controladores ICS ejecutan sistemas operativos en tiempo real, específicos de la industria, que están programados y configurados desde estaciones de trabajo de ingeniería. Por lo general, los controladores se mantienen mediante una aplicación en una estación de trabajo, ubicada en un nivel más alto de la red ICS (operaciones de sitio de nivel tres). Como el controlador del ICS tiene una función tan crítica en una operación del ICS, el acceso al mismo debe estar estrechamente controlado. El acceso directo a un controlador ICS podría dar a un atacante la capacidad de interrumpir el correcto funcionamiento del controlador o del proceso bajo control. La defensa de un ICS contra este tipo de ataques solo se puede lograr con una estrategia de defensa en profundidad, ya que ninguna solución única cubrirá todas las posibles vías de ataque. La estrategia de defensa en profundidad se discutirá ampliamente en un próximo apartado.
- *Nivel 2 - Área de control de supervisión*: representa las aplicaciones y funciones asociadas con la supervisión y operación del tiempo de ejecución de la zona del área. Algunos ejemplos de aplicaciones y sistemas de nivel 2 incluyen:
    - Interfaces de operador o HMIs
    - Alarmas o sistemas de alerta.
    - Estaciones de trabajo en sala de control.

  Las aplicaciones y los sistemas en el nivel 2 se comunican con los controladores en el nivel 1 y conectan o comparten datos con los sistemas y aplicaciones a nivel de sitio (nivel 3) o empresarial (nivel 4/5) a través del IDMZ. Por lo general, están conectadas internamente y directamente a la red de área para la que realizan las funciones de supervisión. A menudo tienden a ser sistemas informáticos basados en Microsoft Windows, atornillados al lado de una máquina o almacenados en una sala de control, cerca del proceso, que se espera estén disponibles para controlar o detener el sistema en caso de una emergencia. Por estas razones, a menudo no es práctico asegurar el tráfico hacia y desde estos dispositivos pasándolo a través de un mecanismo de defensa perimetral como un firewall o un dispositivo de inspección profunda de paquetes (DPI). Además, en este nivel en el ICS, a menudo es imposible desactivar las actualizaciones del sistema operativo y las aplicaciones, o instalar y mantener una solución antivirus.

- **Zona de Fabricación**: La zona de fabricación, o zona industrial, comprende todas las zonas de área y las actividades de operaciones de sitio de nivel 3 de una planta. La zona de fabricación alberga todas las aplicaciones, dispositivos y controladores del Sistema de Control Industrial, cruciales para monitorizar y controlar las operaciones de la planta. Requiere una clara segmentación lógica y protección de los niveles superiores 4 y 5 de la empresa para preservar las operaciones de la planta sin problemas y el funcionamiento de las aplicaciones de ICS y la red de ICS, mientras que tiene comunicaciones casi en tiempo real y una conectividad confiable con los niveles más bajos. Esta separación es provista por la Zona industrial desmilitarizada o IDMZ.
    - *Nivel 3: Operaciones de fabricación y control de la planta*: representa el nivel más alto de la zona de fabricación de un ICS. Los sistemas y aplicaciones que existen en este nivel admiten y administran las funciones de ICS en toda la planta. En el nivel 3 podemos encontrar: Funciones de red (enrutamiento entre VLAN e inspección de tráfico), Informes de proceso, Histórico de datos de la planta, Programación de la producción, Infraestructura virtual para el acceso a estaciones de trabajo (remotas), Servidores de aplicación, Servidores de Antivirus, Servidores de archivos, Servicios de red y dominio (AD), DHCP, DNS, WINS, NTP, etc.

        Los sistemas y aplicaciones de nivel 3 pueden comunicarse con dispositivos en los niveles 0 y 1 y pueden funcionar como un área de entrada para el acceso a la zona de fabricación desde los niveles más altos. Las aplicaciones en el nivel 3 pueden compartir datos con los sistemas de la zona empresarial y las aplicaciones en los niveles 4 y 5. Los sistemas y aplicaciones en el nivel 3 utilizan principalmente equipos informáticos y sistemas operativos estándar (sistemas informáticos basados en Unix o Windows) y lo más probable es que se comuniquen a través de Ethernet estándar y Protocolos de redes IP. Los ingenieros y el personal de mantenimiento usan sistemas en este nivel para hacer su trabajo. Los archivos y las aplicaciones se comparten, transfieren, visualizan y ejecutan como parte de las actividades diarias. Es altamente recomendable tener un programa de seguridad estricto que incluya un programa de respaldo y recuperación, involucre el fortalecimiento y la actualización de los sistemas informáticos, los parches detallados del Sistema de Control Industrial y el equipo de red, e incorpore monitorización e inspección del tráfico de la red.
- **Zona empresarial**: Es donde se hallan todas las aplicaciones comerciales que soportan la producción. Comprende los siguientes dos niveles:
    - *Nivel 4: Planificación del negocio y logística de la planta*: En este nivel es donde residen las funciones y los sistemas que necesitan acceso estándar a los servicios proporcionados por la red de la empresa. Las tareas básicas de administración de negocios se realizan aquí y dependen de los servicios estándar de las Tecnologías de la Información. Estas funciones y sistemas incluyen acceso a servicios de red empresarial como los siguientes: Acceso a Internet, Acceso al correo electrónico (alojado en centros de datos) Sistemas de planta no críticos, como sistemas de ejecución de manufactura y reportes generales de planta, como inventario, desempeño, etc., Acceso a aplicaciones empresariales, como SAP y Oracle (alojadas en centros de datos), Punto de entrada para soluciones de Remote Desktop Gateway en los niveles inferiores.

Debido a la naturaleza más abierta y expuesta de los sistemas y aplicaciones dentro de la red empresarial, este nivel a menudo se ve como una fuente de amenazas e interrupciones en la red de los Sistemas de Control Industrial. Al tener acceso a Internet disponible en el nivel 4 se pueden mantener los sistemas operativos y las aplicaciones actualizadas, pero también crea oportunidades potenciales donde un atacante puede entrar en la zona de fabricación. La protección de la interacción entre el nivel 4 y los niveles inferiores se realiza mediante la implementación de una zona industrial desmilitarizada o IDMZ.

- *Nivel 5: Empresa*: Es donde residen los sistemas y funciones de Tecnologías de la Información centralizados. Los servicios de gestión de recursos empresariales, de empresa a empresa y de empresa a cliente suelen residir en este nivel. A menudo, los socios externos o los sistemas de acceso de invitados existen aquí, aunque no es raro encontrarlos en niveles más bajos (por ejemplo, el nivel 3) del marco para obtener una flexibilidad que puede ser difícil de lograr a nivel empresarial. Sin embargo, este enfoque puede llevar a riesgos de seguridad significativos si no se implementa correctamente. El Sistema de Control Industrial debe comunicarse con las aplicaciones empresariales para intercambiar datos de recursos y fabricación. Por lo general, no se requiere acceso directo al ICS. Una excepción a esto sería el acceso remoto para la gestión del ICS por parte de los empleados o socios, como los integradores de sistemas y los fabricantes de máquinas. El acceso a los datos y los sistemas en la red Industrial debe ser administrado y controlado a través del IDMZ para mantener la seguridad, disponibilidad y estabilidad general del Sistema de Control Industrial.

5.2.1. Converged Plantwide Ethernet (CPwE)

Converged Plantwide Ethernet o CPwE describe una arquitectura que permite al implementador vincular o converger redes ICS con redes empresariales de una manera eficiente, conveniente y segura. La seguridad se diseña con una arquitectura segmentada. Al segmentar un Sistema de Control Industrial en zonas funcionales, los perímetros de seguridad se establecen con la capacidad de controlar, restringir e inspeccionar el tráfico entre zonas.

Para lograr la segmentación, Cisco y Rockwell Automation colaboran en la elaboración de las buenas prácticas de CPwE que adopta el marco desarrollado por el comité ISA-99 para la Seguridad de los Sistemas de Control y Fabricación de la International Society of Automation.

El Modelo de ISA-99 identifica niveles de operaciones y zonas clave para el marco lógico de los Sistemas de Control Industrial. Además de los niveles y las zonas, Cisco y Rockwell Automation incluyen una zona desmilitarizada (DMZ) entre las zonas Enterprise y Manufacturing como parte de la arquitectura CPwE. Los estándares de seguridad emergentes de IACS, como ISA-99, NIST 800-82 y el Departamento de Seguridad Nacional INL / EXT-06-11478 también incluyen una DMZ como parte de una estrategia de defensa en profundidad [37].

El propósito de la DMZ es proporcionar una zona de amortiguamiento donde los datos y los servicios se puedan compartir entre las zonas de la empresa y de fabricación. La DMZ es fundamental para mantener la disponibilidad, abordar las vulnerabilidades de seguridad y cumplir con los mandatos de cumplimiento normativo (por ejemplo, Sarbanes-Oxley). Además, la DMZ permite la segmentación del control organizacional; por ejemplo, entre la organización de TI y la fabricación. Esta segmentación permite aplicar y contener diferentes políticas. Por ejemplo, la organización de fabricación puede aplicar

políticas de seguridad y calidad de servicio (QoS) que son diferentes de la organización de TI. La DMZ es donde se pueden dividir las políticas y el control organizativo.

Estos niveles y zonas forman el marco lógico base alrededor del cual se diseñan los servicios y la infraestructura de red de Sistema de Control Industrial para la solución CPwE.

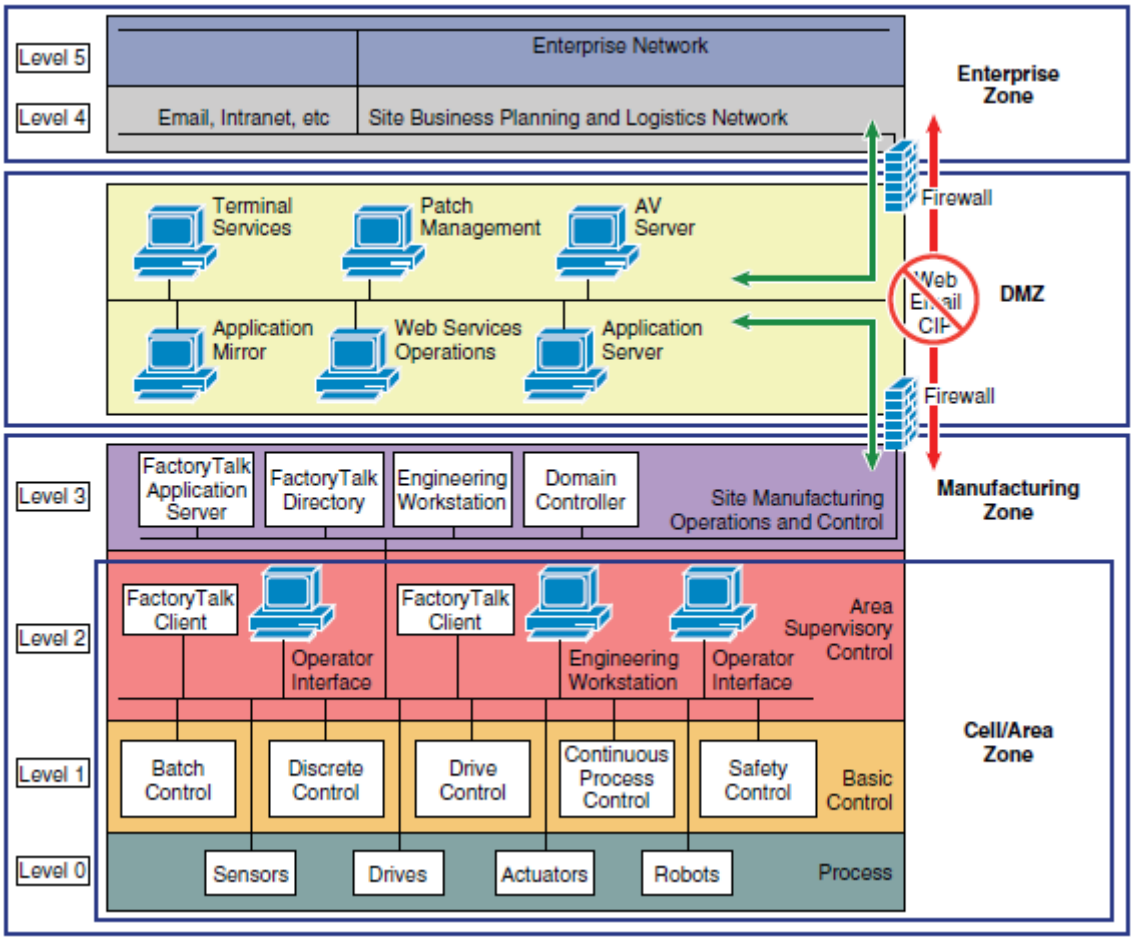

FIGURA 12 - MARCO LÓGICO DE CPWE (FUENTE: [37])

A continuación se dan más detalles de la IDMZ según la guía CPwE:

- *Nivel 3.5: La zona desmilitarizada Industrial* (IDMZ): también conocida como red perimetral, es un búfer que impone políticas de seguridad de datos entre una red confiable (zona industrial) y una red no confiable (zona empresarial). La IDMZ es una capa adicional de defensa para compartir de forma segura los datos de ICS y los servicios de red entre las zonas industriales y empresariales. El concepto de zona desmilitarizada es común en las redes de TI tradicionales, pero aún se encuentra en adopción temprana para aplicaciones ICS. Para permitir las interacciones seguras y el intercambio de datos con el Sistema de Control Industrial, la IDMZ contiene activos que actúan como servicios de intermediario entre la zona industrial y la zona empresarial. Existen múltiples métodos para intercambiar datos de ICS a través del IDMZ: utilizando una aplicación espejo, como la replicación de SQL para los historiadores de datos, utilizando los servicios de puerta de enlace de Escritorio

remoto (RD) de Microsoft para sesiones interactivas remotas o utilizando un servidor proxy inverso para el tráfico web.

Los servicios de intermediarios ayudarán a ocultar y proteger la existencia y las características de los servidores y aplicaciones de la zona industrial de los clientes y servidores de la zona empresarial. Se puede lograr un límite de seguridad efectivo teniendo en cuenta la supervivencia y la capacidad de uso de ICS si se implementan soluciones de intermediarios bien diseñadas que cumplan con los siguientes objetivos de diseño de la IDMZ:

- Todo el tráfico de la red desde cualquier lado de la IDMZ termina en la IDMZ; No hay tráfico que atraviese directamente la IDMZ.
- El tráfico de red ICS sensible, como los paquetes Ethernet/IP, no ingresa a la IDMZ; permanece dentro de la zona industrial.
- Los servicios primarios no se almacenan permanentemente en la IDMZ
- Todos los datos son transitorios, la IDMZ no almacena datos permanentemente.
- Las subzonas funcionales dentro de la IDMZ están configuradas para segmentar el acceso a los datos de ICS y los servicios de red.

Una IDMZ adecuadamente diseñada soportará la capacidad de ser desenchufada si se encuentra comprometida, mientras que se permite a la zona industrial funcionar sin interrupciones.

5.3. MODELO DE SEGURIDAD EN PROFUNDIDAD

No existe ninguna solución única que pueda proteger fiablemente contra todos los vectores de ataque y tapar cada agujero de seguridad de un sistema. Al aplicar un modelo de defensa en profundidad y aplicar medidas de protección por capas, las brechas de seguridad de una capa se pueden cerrar con controles en otra capa, creando una postura de seguridad holística [3].

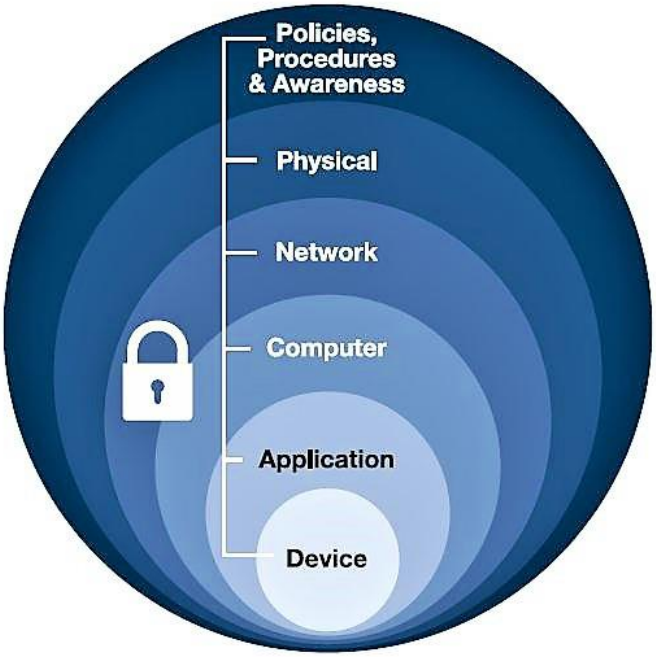

FIGURA 13 - CAPAS DEL MODELO DE SEGURIDAD EN PROFUNDIDAD [3]

A continuación, detallamos cada una de estas capas:

5.3.1. Capa física

Se limita el acceso físico a personal autorizado a la zona de área, a paneles de control, dispositivos, cableado y salas de control mediante el uso de cerraduras, puertas, tarjetas llave y datos biométricos. Puede que implique también el uso de políticas, procedimientos y tecnologías que permitan el acompañamiento y rastreo de visitantes.

El objetivo de la seguridad física es mantener a las personas fuera de las áreas donde no están autorizadas a estar. Esto incluye áreas restringidas, salas de control, áreas de alta seguridad, paneles eléctricos y de red, salas de servidores y otras áreas restringidas o sensibles. Si un atacante tiene acceso físico a una red o equipo informático, es solo cuestión de tiempo hasta que obtenga acceso a la red o al sistema informático. La capa de defensa física incluye recomendaciones como la construcción de muros de tamaño suficiente, la instalación de cerraduras en puertas, la instalación de cámaras de CCTV y la definición de políticas y controles para atender a los visitantes e invitados.

5.3.2. Capa de red

Al igual que la seguridad física se trata de restringir el acceso autorizado a áreas físicas y activos del Sistema de Control Industrial, la seguridad de la red trata de restringir el acceso a áreas lógicas de la red del Sistema de Control Industrial. La idea es dividir la red en zonas de seguridad, utilizando un IDMZ, aplicando reglas de firewall, configurando listas de control de acceso e implementando Sistemas de Detección de Intrusos (IDS) para cercar partes más sensibles (zonas más seguras) de la red de zonas menos seguras. Al controlar y monitorizar estrechamente el tráfico que atraviesa las zonas de seguridad, las anomalías se pueden detectar y manejar de manera efectiva.

5.3.3. Capa de computadora

La seguridad informática consiste en evitar la infiltración de los sistemas informáticos (estaciones de trabajo, servidores, equipos portátiles, etc.). Esto se logra aplicando estrategias de parches, realizando ejercicios de fortalecimiento para los sistemas informáticos e instalando aplicaciones y soluciones de seguridad como antivirus, protección de puntos finales y software de detección/prevención de intrusos en el host (HIDS / HIPS).

Los controles de seguridad de la computadora también incluyen la restricción o la prevención del acceso a los puertos de comunicación no utilizados de los dispositivos informáticos, como bloquear el acceso a los puertos USB y FireWire por medio de bloqueadores físicos de puertos (o pegamento caliente), así como a la aplicación de una política de dispositivos con una solución de protección de punto final como Symantec Endpoint Protection (SEP). Mantener los sistemas informáticos libres de vulnerabilidades mediante la actualización y la aplicación de parches también es una forma de seguridad informática.

5.3.4. Capa de aplicación

Cuando la seguridad informática se trata de mantener a un intruso fuera de un sistema informático, la seguridad de la aplicación consiste en evitar que un usuario realice interacciones no autorizadas con programas y servicios que se ejecutan en el sistema informático.

Esto se logra mediante la implementación de autenticación, autorización y auditoría. De esta manera, la autenticación verifica que el usuario es quien dice ser, la autorización restringe las acciones del usuario y la auditoría registra todas las interacciones que el usuario tiene con el sistema. Mantener las

aplicaciones libres de vulnerabilidades mediante detección y gestión de parches también es una forma de seguridad de la aplicación.

5.3.5. Capa de dispositivo

La seguridad del dispositivo implica las acciones y los controles de seguridad relacionados con los tres factores de disponibilidad, integridad y confidencialidad. En el contexto de un ICS, la disponibilidad es el más importante de los tres factores de criticidad, ya que el tiempo de disponibilidad es el objetivo número uno en producción y tiene el mayor impacto en la rentabilidad.

La seguridad del dispositivo incluye la aplicación de parches, el fortalecimiento del dispositivo, las restricciones de acceso lógico y físico y la configuración de un programa de ciclo de vida del dispositivo que implica la definición de procedimientos para la adquisición, implementación, mantenimiento, configuración y gestión de cambios y la eliminación de dispositivos.

5.3.6. Políticas, procedimientos y concienciación.

Finalmente, haciendo una unión de todos los controles de seguridad encontramos las políticas, los procedimientos y la concienciación. Las políticas son una guía de alto nivel sobre la postura de seguridad esperada para los sistemas y dispositivos de control industrial; por ejemplo, cifrar todas las bases de datos. Los procedimientos son instrucciones paso a paso sobre cómo lograr los objetivos de la política, como la forma de implementar el cifrado AES en las bases de datos de recetas de producción. La concienciación ayuda a captar y mantener la atención en aspectos relacionados con la seguridad del ICS y su funcionamiento. La formación en concienciación a menudo viene en forma de formación anual en seguridad que suele cubrir temas como el spam, las amenazas internas y las prácticas de seguimiento (un intruso que sigue de cerca a un empleado en una instalación que está protegida por controles de acceso físico).

6. PRUEBA DE CONCEPTO DE APLICACIÓN DE MEDIDAS DE SEGURIDAD EN SISTEMAS DE CONTROL INDUSTRIAL

En este capítulo vamos a presentar una serie vulnerabilidades de seguridad en un escenario que podría ser real, y la manera en que podemos mitigar o eliminar los riesgos asociados a dichas vulnerabilidades en función de su impacto y probabilidad. En cada uno de los casos que se presentan se explicarán las vulnerabilidades del sistema, estimaremos su riesgo e impacto para la infraestructura crítica y aplicaremos las soluciones que se estimen oportunas para evitar estas vulnerabilidades.

Todas estas vulnerabilidades de seguridad se plantearán en un escenario común correspondiente a una planta de producción de la industria cervecera. En dicha planta de producción se dispone de ciertos sistemas críticos en cada una de las áreas que la componen: Cervecería (o cocimiento), Envasado, Servicios adicionales (o utilities) y Calidad.

6.1. VULNERABILIDAD EN APLICACIÓN DE PROTOCOLOS INDUSTRIALES DE COMUNICACIÓN

En la planta de producción cervecera, en el área de cocimientos, se tienen desplegados una serie de PLCs Siemens Simatic S7 para el control de temperaturas y presión de las calderas de cocimiento. Estos PLCs se comunican con las estaciones de ingeniería y los sistemas SCADA que los controlan mediante el protocolo industrial de comunicaciones S7 Communication, del que es propietario Siemens. Como se ha comentado en el capítulo anterior sobre el ataque Stuxnet, este tipo de PLCs tiene varias vulnerabilidades conocidas fruto de la ausencia de autenticación en el protocolo de comunicaciones utilizado.

Más concretamente, las vulnerabilidades que vamos a analizar pueden permitir a un atacante la parada de los PLCs, con el consecuente riesgo para la seguridad de las personas. Dichas vulnerabilidades se encuentran en los PLCs de los modelos S7 300, S7 400 [38] y S7 1200 [39].

Las mitigaciones y soluciones recomendadas por el fabricante Siemens pasan por la segmentación de la red y establecer medidas de seguridad en profundidad como las que se explicaron en el capítulo anterior [40].

6.1.1. ESTIMACIÓN DEL RIESGO DE LA VULNERABILIDAD

Siguiendo los pasos descritos en el capítulo de Gestión de riesgos, podemos calcular el impacto que esta vulnerabilidad puede tener para la organización y su entorno.

En primer lugar, debemos definir la puntuación base de esta vulnerabilidad; esta suele tomarse de la que se defina en la base de datos de vulnerabilidades CVE (Common Vulnerabilities and Exposures); en nuestro caso, como no existe CVE publicada para estas vulnerabilidades, tendremos que calcularlo utilizando el sistema CVSS versión 3.0 (Common Vulnerability Scoring System) que no es más que la asignación de respuestas a una serie de aspectos cualitativos. En nuestro caso, obtenemos las siguientes valoraciones:

- **Attack Vector (AV)**: Network (N). Se trata de una vulnerabilidad explotable mediante red.
- **Attack Complexity (AC)**: Low (L). Es una vulnerabilidad fácilmente atacable, de hecho, como hemos visto, existen exploits disponibles en Internet.

- **Privileges Required (PR)**: None (N). No requiere de la obtención de privilegios previos por parte del atacante.
- **User Interaction (UI)**: None (N). No requiere de la interacción del usuario con el Sistema para que pueda efectuarse el ataque.
- **Scope (S)**: Unchanged (U). El sistema vulnerable y el que sufre el impacto son el mismo.
- **Confidentiality (C)**: High (H). Al acceder a los PLCs, el atacante puede obtener el proyecto que estos tienen cargados junto con la receta de cocción de cervezas de distintas marcas.
- **Integrity (I)**: None (N). No se aprecia impacto en la integridad de datos de los PLCs ante esta vulnerabilidad.
- **Availability (A)**: High (H). Un atacante sería capaz de parar los PLCs afectados y; por tanto, su disponibilidad se podría ver interrumpida.

Es nos ofrece la siguiente cadena del vector del riesgo: **CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H** que resulta en una puntuación de gravedad de **9.1** sobre 10; es decir, la vulnerabilidad es crítica.

A continuación, asignamos las siguientes evaluaciones:

- **Criticidad de los activos (0-5)**: Los PLCs, que son los activos afectados por la vulnerabilidad son críticos para la producción, por lo que le asignamos un valor de 4.
- **Probabilidad de ocurrencia (0-5)**: Le asignamos un 3 debido a que no es simple obtener acceso al segmento de red donde se encuentran los PLCs afectados.
- **Impacto (0-5)**: La parada de los PLCs provocaría la pérdida del control del proceso de cocción por parte de los operarios con el consecuente riesgo para el proceso de producción e incluso la seguridad de las personas, por lo que le asignamos un 5.

Utilizando la fórmula ya comentada:

$$riesgo = \frac{gravedad + (criticidad * 2) + (probabilidad * 2) + (impacto * 2)}{4}$$

Concluimos que la vulnerabilidad tiene una puntuación de riesgo de 8.275 que se puede tomar como un riesgo alto.

6.1.2. Mitigación del riesgo

Como se ha comentado anteriormente la recomendación del fabricante Siemens para evitar estas vulnerabilidades de seguridad en sus dispositivos es la aplicación de una política de seguridad en profundidad (Defense-in-Depth) y la segmentación de la red.

Para evitar estas vulnerabilidades en los PLCs, se procede a aislar la LAN virtual donde se encuentran los PLCs afectados de tal manera que sólo se permita el acceso a los mismos desde los puestos de ingeniería necesarios y los servidores SCADA por los puertos de comunicaciones que se identifican. Esto se consigue mediante la aplicación de listas de control de acceso a dicha VLAN. Veremos más detenidamente esta protección de la red en próximos apartados.

6.2. Vulnerabilidad ante contenidos maliciosos de dispositivos USB

Como ya se explicó en el incidente de seguridad Stuxnet, el vector de ataque utilizado fue el uso de software malicioso en dispositivos USB de proveedores que accedían a la planta industrial.

En nuestro caso, en la fábrica de cerveza se detecta el mismo escenario y, de forma más o menos periódica, técnicos de los distintos proveedores acceden a la planta de producción para realizar el mantenimiento de PLCs y sistemas SCADA. Para realizar dicho mantenimiento es habitual que los técnicos introduzcan dispositivos USB en los componentes del sistema de control lo cual se ve como un riesgo a eliminar en la fábrica.

Los componentes que se desean proteger son los PLCs del área de cocimientos, los PLCs del área de envasado, distribuidos por la zona donde se encuentran los trenes de envasado, y los servidores SCADA de ambos entornos que se encuentran ubicados dentro del Centro de Procesado de Datos (CPD) de la propia planta. Además, también se desea proteger los equipos de ingeniería ante el uso de USB descontrolado que pueden realizar los usuarios.

6.2.1. Estimación del riesgo de la vulnerabilidad

En este apartado calcularemos el impacto que esta vulnerabilidad puede tener para la organización y su entorno.

La puntuación base de esta vulnerabilidad vamos a calcularla utilizando también el sistema CVSS versión 3.0 (Common Vulnerability Scoring System):

- **Attack Vector (AV)**: Local (L). Se trata de una vulnerabilidad que sólo puede explotarse a nivel local; es decir, con acceso directo o indirecto a los componentes del sistema de control industrial.
- **Attack Complexity (AC)**: Low (L). Es una vulnerabilidad fácilmente atacable, pues prácticamente todos los componentes disponen de puertos USB y niveles de parches del sistema operativo y antivirus desactualizados.
- **Privileges Required (PR)**: None (N). No requiere de la obtención de privilegios previos por parte del atacante.
- **User Interaction (UI)**: Required (R). Se requiere, al menos una mínima interacción con el usuario o el proveedor con acceso al sistema.
- **Scope (S)**: Changed (C). El sistema vulnerable puede servir como acceso puente a otros sistemas de la fábrica.
- **Confidentiality (C)**: High (H). Al acceder a los PLCs, servidores SCADA y/o estaciones de ingeniería, el atacante puede obtener información confidencial da organización.
- **Integrity (I)**: High (H). Se pierde totalmente la protección de los datos y el atacante pasaría a tener control absoluto de los mismos.
- **Availability (A)**: High (H). Un atacante sería capaz de parar los equipos afectados y; por tanto, la disponibilidad del sistema podría interrumpirse.

Es nos ofrece la siguiente cadena del vector del riesgo: **CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H** que resulta en una puntuación de gravedad de **8.6** sobre 10; es decir, la vulnerabilidad es crítica porque tiene una gravedad alta.

A continuación, asignamos las siguientes evaluaciones:

- **Criticidad de los activos (0-5)**: Los PLCs, sistemas SCADA y estaciones de ingeniería, que son los activos afectados por la vulnerabilidad son todos críticos para la producción, por lo que le asignamos un valor de **4**.

- **Probabilidad de ocurrencia (0-5)**: Le asignamos un **4** debido a que puede resultar relativamente sencillo hacer llegar un software malicioso a proveedores y usuarios que lo terminen almacenando en un dispositivo USB que introduzcan en la planta.
- **Impacto (0-5)**: La parada de los sistemas de producción y envasado provocaría la pérdida del control de los procesos por parte de los operarios y su parada inmediata de emergencia, por lo que le asignamos un **5**.

Utilizando la fórmula ya comentada:

$$riesgo = \frac{gravedad + (criticidad * 2) + (probabilidad * 2) + (impacto * 2)}{4}$$

Concluimos que la vulnerabilidad tiene una puntuación de riesgo de 8.65 que se puede tomar como un riesgo alto.

6.2.2. Mitigación del riesgo

Para evitar o mitigar esta vulnerabilidad de seguridad utilizaremos una aproximación de seguridad en profundidad (Defense-in-Depth) mediante la aplicación de medidas de seguridad en la capa física y en la capa de computadora.

En primer lugar, para evitar el uso físico de los puertos USB se decide la adquisición de unos bloqueadores de puertos USB que protege su uso a no ser que se utilice una llave para desbloquearlo como el que aparece en la siguiente imagen.

FIGURA 14 - USB PORT LOCK (FUENTE: INTERNET)

Estos bloqueadores de puertos USB se instalan en todos los PLCs que se encuentran desplegados por la fábrica y en los servidores SCADA ubicados en el CPD; es decir, en todos aquellos componentes cuya ubicación sea fija.

Por otro lado, además de esta protección física de puertos USB, se decide también realizar el bloqueo del uso de estos puertos mediante configuración, ya sea a través de políticas del dominio (Active Directory), o bien, a nivel local en cada equipo que no esté incluido en el dominio.

De esta manera, se protegen los componentes del sistema de control industrial de posibles infecciones de software malicioso mediante el bloque de uso de puertos USB tanto a nivel físico como a nivel de computadora.

Sin embargo, para permitir la operativa de proveedores que utilizan dispositivos USB para el mantenimiento de estos componentes, se le ofrece una solución alternativa consistente en la provisión de una computadora totalmente actualizada de parches de sistema operativo y antivirus en el que se introducen los USB de los proveedores que visiten la fábrica. Esta computadora, una vez que analiza los contenidos del dispositivo USB, si estos son seguros, los copia en una ubicación de red accesible por los componentes del sistema; en caso contrario, no permite pasar el contenido al sistema.

6.3. VULNERABILIDAD EN LA RED CORPORATIVA

Como ya se ha indicado en apartados anteriores, la red de computadoras de la fábrica que nos ocupa se encuentra segmentada en VLANs, pero la visibilidad entre todas las redes virtuales es total, por lo que no existe protección del tráfico que se intercambia entre ellas.

Realmente, la protección de la red debería ser el primer paso para la eliminación de vulnerabilidades; sin embargo, debido a la rápida incorporación de los sistemas industriales a las redes corporativas ha impedido que dicha incorporación se realizara de manera segura protegiendo los sistemas críticos.

Una red vulnerable puede ser el origen de múltiples vulnerabilidades porque supone el vector de ataque más comúnmente utilizado por los atacantes. Por lo tanto, es indispensable la protección de los sistemas de control industrial conectados a la red mediante el diseño de una arquitectura de red segura.

6.3.1. ESTIMACIÓN DEL RIESGO DE LA VULNERABILIDAD

La puntuación base de esta vulnerabilidad vamos a calcularla utilizando también el sistema CVSS versión 3.0 (Common Vulnerability Scoring System):

- **Attack Vector (AV)**: Network (N). La vulnerabilidad es básicamente la inseguridad de la propia red.
- **Attack Complexity (AC)**: Low (L). Es una vulnerabilidad fácilmente atacable.
- **Privileges Required (PR)**: None (N). No requiere de la obtención de privilegios previos por parte del atacante.
- **User Interaction (UI)**: None (N). No se requiere interacción con el usuario para atacar la red.
- **Scope (S)**: Changed (C). La red vulnerable es simplemente un medio para alcanzar los sistemas críticos industriales.
- **Confidentiality (C)**: High (H). El acceso malintencionado a la red puede ocasionar pérdidas graves de confidencialidad.
- **Integrity (I)**: High (H). Se pierde totalmente la protección de los datos y el atacante pasaría a tener control absoluto de los mismos.
- **Availability (A)**: High (H). Un atacante sería capaz de interrumpir el sistema.

Esto nos ofrece la siguiente cadena del vector del riesgo: **CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H** que resulta en una puntuación de gravedad de **10** sobre 10; es decir, la vulnerabilidad es crítica porque tiene una gravedad muy alta.

A continuación, asignamos las siguientes evaluaciones:

- **Criticidad de los activos (0-5)**: La red es un activo crítico que permite el acceso a todos los demás activos que se conectan a ella, por lo que le damos una puntuación de criticidad de **5**.
- **Probabilidad de ocurrencia (0-5)**: Conociendo los incidentes de seguridad que ocurren en los últimos tiempos y que casi todos ellos se producen por ataques a través de la red, le asignamos un **5**.
- **Impacto (0-5)**: La puntuación máxima de **5** pues una caída de la red supone la caída de todo el sistema en manos del atacante.

Utilizando la fórmula del riesgo:

$$riesgo = \frac{gravedad + (criticidad * 2) + (probabilidad * 2) + (impacto * 2)}{4}$$

Concluimos que la vulnerabilidad tiene una puntuación de riesgo de **10**; es decir, el riesgo más alto que se puede obtener con este modelo.

6.3.2. Mitigación del riesgo

Dado el nivel de riesgo obtenido, es evidente que la protección de la red debe ser una prioridad en el proceso de mejora de la seguridad de la planta industrial. Para ello nos vamos a basar en las recomendaciones de Cisco y Rockwell contenidas en la Guía de diseño e implementación de Ethernet convergente en toda la planta (Converged Plantwide Ethernet (CPwE) Design and Implementation Guide) [37].

La implementación de la seguridad de la red, literalmente, comienza estableciendo una base sólida a la red del Sistema de Control Industrial, con esta base sólida se permite una implementación más ágil del proyecto de seguridad de la red. Una base sólida se presenta en forma de decisiones de diseño de arquitectura de red centradas en la seguridad. Un ejemplo de una decisión de diseño centrada en la seguridad diseñar una segmentación de red que admita el confinamiento y la detección de incidentes de seguridad y que mantenga las interrupciones, como las tormentas de difusión de paquetes (broadcast storm) locales a la zona, protegiendo la red en general. Si establecemos unos buenos cimientos en la seguridad de la red, el trabajo de mantener la seguridad de la misma se vuelve más sencillo.

El primer paso para diseñar una arquitectura de red industrial centrada en la seguridad es definir la segmentación de la red. Un segmento de red es una agrupación lógica de sistemas de información y automatización en una red de Sistemas de Control Industrial. La red debe dividirse en segmentos de red manejables para limitar el dominio de difusión, restringir el uso del ancho de banda y reducir la superficie de ataque. Una zona de seguridad de red tiene un perímetro bien definido y una estricta protección de límites. Las zonas de seguridad tienen un nivel de confianza de seguridad (alto, bajo o medio) según la utilidad que se le asigne. Dentro del contexto de una red de Sistemas de Control Industrial, la Zona Industrial se considera la zona de alta seguridad y la Zona de empresa (u oficina) la zona de baja seguridad. Esto permite que los sistemas con requisitos de seguridad similares se coloquen dentro de la misma zona. Por ejemplo, una estación de trabajo suministrada por el proveedor que se crea a la medida de ese proveedor y se utiliza para controlar una parte crítica del proceso de

producción, puede estar prohibido contractualmente para obtener actualizaciones de parches sin la aprobación estricta del proveedor, en este caso, se puede alojar en la Zona Industrial donde se puede proteger del acceso directo desde zonas menos seguras mediante la IDMZ. Por otro lado, una computadora de escritorio que simplemente se utiliza para ejecutar informes de producción y no tiene restricciones de actualización ni un gran valor para el proceso de producción se ubicará en la Zona Empresarial, donde se puede restringir el acceso directo a los sistemas y dispositivos de producción críticos mediante la IDMZ.

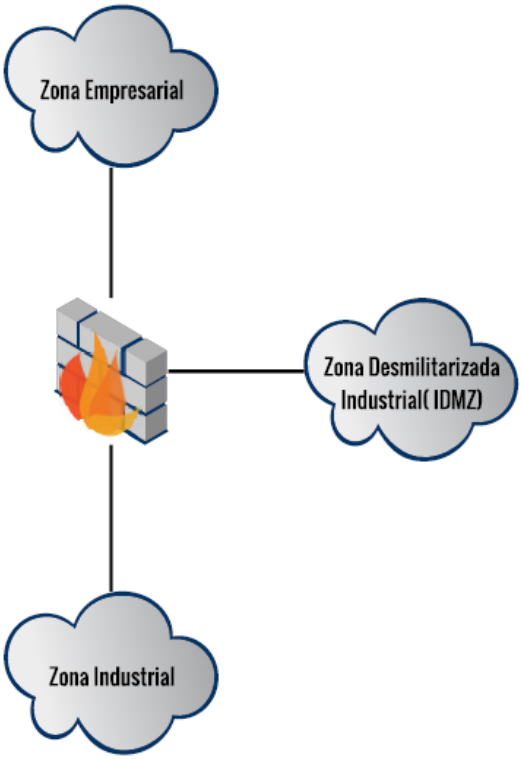

FIGURA 15 - DIAGRAMA DE RED POR ZONAS

Al establecer una pequeña cantidad de zonas de seguridad de red con requisitos de seguridad claramente definidos, se limita la complejidad y se elimina la ambigüedad cuando se selecciona una zona para nuevos sistemas y dispositivos. Una red ICS típica incorpora las siguientes zonas de seguridad de red con los niveles de confianza correspondientes:

- Zona Empresarial: Baja confianza
- DMZ industrial: confianza media
- Zona industrial: Alta confianza.
- Zonas de Área Celular: Subzonas de la Zona Industrial - Alta confianza

A continuación, veamos un poco más de cerca los requisitos de seguridad de cada una de estas zonas.

La Zona Empresarial

La Zona Empresarial es donde normalmente residen los sistemas de usuarios del negocio, incluidas las estaciones de trabajo, las impresoras y los teléfonos VoIP. Los usuarios y los sistemas en la Zona Empresarial a menudo requieren conectividad a Internet y acceso a recursos de toda la empresa, como

correo electrónico, chat y almacenamiento corporativo. Los controles de seguridad aplicables en esta zona incluyen protección de punto final, actualizaciones (automáticas) del sistema operativo y aplicaciones, y esfuerzos regulares de escaneos de vulnerabilidades. Los sistemas y dispositivos que viven en esta zona suelen incluir los siguientes:

- Sistemas ERP
- Estaciones de usuario final con conectividad a internet.
- Sistemas de bases de datos en toda la empresa.
- Soluciones de acceso remoto (Citrix, VPN y RDP).

La Zona Industrial

La Zona Industrial alberga sistemas y dispositivos críticos para la producción, que incluyen estaciones de trabajo, servidores, bases de datos y dispositivos de control de automatización e instrumentación. Un incumplimiento de la disponibilidad, integridad o confidencialidad de cualquier sistema en esta zona podría impactar negativamente en la productividad y rentabilidad, reputación o seguridad de una empresa. Esta zona debe tener el nivel más alto de protección para garantizar que se prevengan y detecten aquellos ataques que tienen más probabilidades de tener éxito contra los sistemas internos. Los sistemas y dispositivos que viven en esta zona suelen incluir los siguientes:

- Sistemas MES.
- Servidores de etiquetas.
- Servidores de recopilación de datos e históricos.
- Estaciones de trabajo del sistema de producción, estaciones de operador y servidores.
- Dispositivos de automatización y control (PLC y HMI).
- Cualquier sistema relacionado con la producción que sea demasiado restrictivo para asegurar por medios convencionales, como computadoras con sistemas operativos obsoletos.

Celdas de la zona industrial

La zona industrial debe subdividirse en celdas donde cada una contendrá los sistemas y dispositivos que tienen una tarea común o un interés mutuo en el proceso de producción. En el caso que nos ocupa de la planta de producción de cerveza, podríamos segmentar la zona industrial en las celdas de Cervecería, Envasado, Utilities y Calidad:

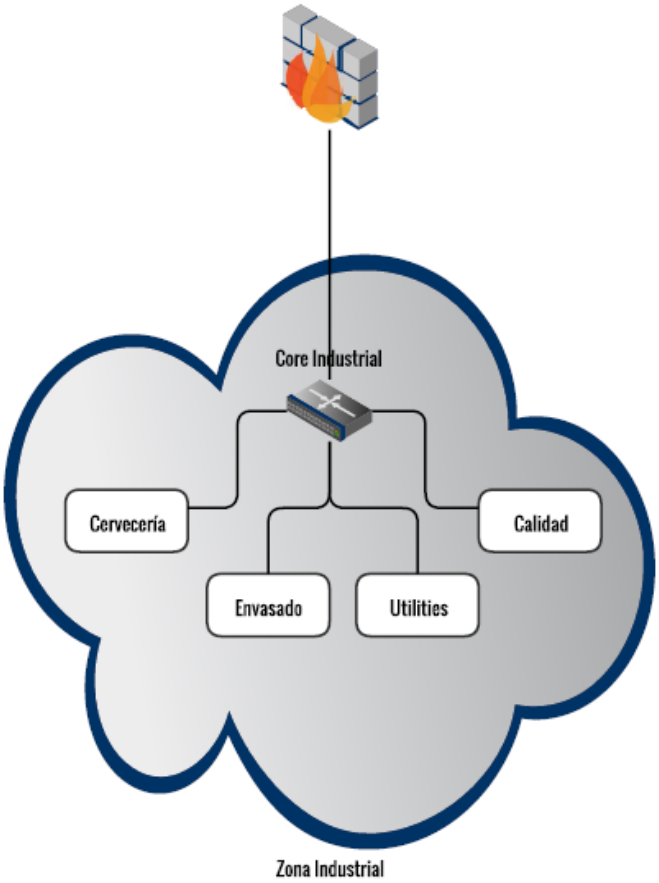

FIGURA 16 - ZONA INDUSTRIAL SEGMENTADA EN CELDAS

Las celdas de la zona industrial permiten esquemas de control de seguridad más granulares y confinan aún más el tráfico de red relacionado. La definición de lo que entra en una zona de área de celda a menudo depende del objetivo de los esfuerzos de seguridad para toda la red de ICS. A veces, las celdas están definidas por las áreas funcionales de un proceso de producción. Como en nuestro ejemplo, separamos las redes por celdas funcionales: Cervecería, Envasado, Utilities y Calidad. Otro criterio para la segmentación de celdas podría ser la agrupación de sistemas por su vinculación con servicios comunes como gas, electricidad, etc. Un tercer método para definir celdas es la ubicación. Por ejemplo, si un proceso de producción se extiende entre edificios separados, que incluso podrían estar en ciudades distintas; entonces, podría tener sentido asignar celdas a cada ubicación. Los sistemas y dispositivos que se encuentran típicamente en las celdas de la zona industrial incluyen los siguientes:

- Dispositivos de automatización como PLC y HMI.
- Actuadores inteligentes como motores, servos y bancos de válvulas neumáticas.
- Dispositivos de instrumentación habilitados para Ethernet, como sondas de temperatura, sensores de presión y velocímetros.
- Sistemas informáticos suministrados por el fabricante que interactúan directamente con el equipo de producción.

La Zona Desmilitarizada Industrial (IDMZ)

La segmentación de la red debe incluir decisiones sobre dónde colocar los sistemas relacionados con el Control Industrial. Los sistemas utilizados principalmente por personal de oficina se ubicarán en la Zona Empresarial. Los sistemas que utilizan ampliamente los usuarios de producción o que necesitan comunicarse con el equipo de producción se moverán a la Zona Industrial. Esta separación conducirá a sistemas o procesos de producción que terminarán teniendo partes tanto en la Zona Empresarial como en la Zona Industrial. Para facilitar de manera segura la comunicación entre esas partes separadas y permitir interacciones administrativas seguras en la Zona Industrial, la Zona Desmilitarizada Industrial intermediará estas interacciones entre la Zona Empresarial y la Zona Industrial. Los servicios de intermediación comunes que se encuentran en el IDMZ incluyen lo siguiente:

- Servidor de puerta de enlace de escritorio remoto de Microsoft.
- Servidor de transferencia de ficheros gestionada.
- Servidor proxy web inverso.
- Servidor de actualizaciones de Microsoft (SCCM o WSUS).
- Servidor de puerta de enlace del antivirus.

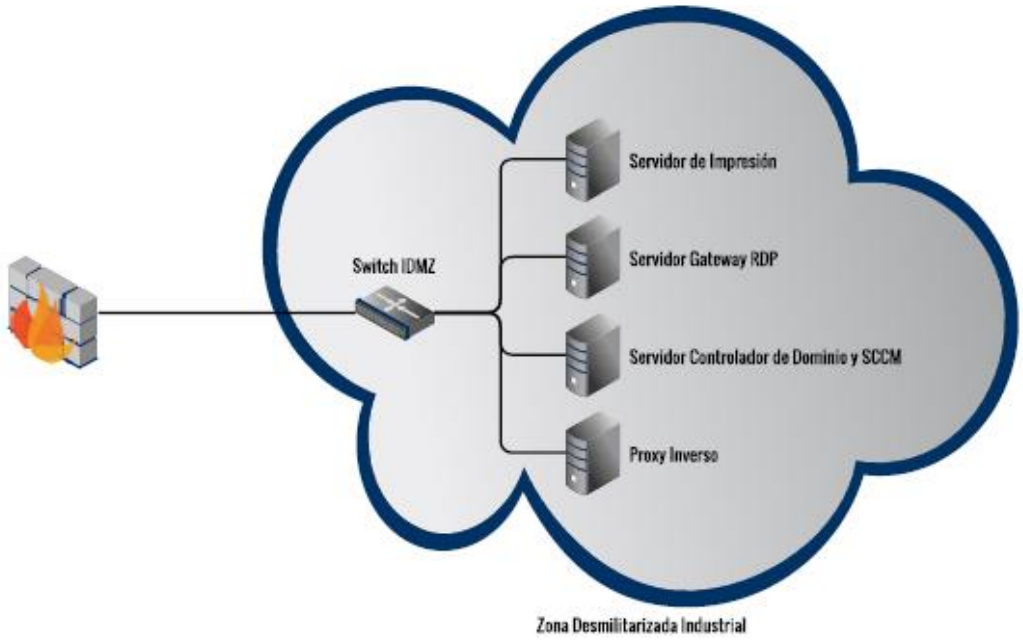

FIGURA 17 - DIAGRAMA DE RED DE LA ZONA DESMILITARIZADA INDUSTRIAL

Caminos de Comunicaciones

Este modelo de separación en zonas de seguridad de red utiliza el concepto de confianza de base. A cada zona se le asigna un nivel de confianza. La confianza aumenta desde la zona exterior (zona empresarial) hasta la interior (zona industrial), que alberga los activos y datos de producción más críticos de la empresa. La comunicación solo está permitida entre sistemas en zonas adyacentes, no se permite omitir o desviar zonas. Los controles de seguridad se colocan entre cada zona (firewalls de inspección de estado y sistemas de detección y prevención de intrusos). Los controles de seguridad implementados dentro de una zona permiten la detección de actividad maliciosa entre sistemas dentro de una zona.

La Zona Desmilitarizada Industrial sirve como nexo de unión entre la Zona Empresarial y la Zona Industrial y sólo permitirá el intercambio de tráfico que se considere seguro entre zonas (por protocolo, puerto o IPs origen y destino).

RECUPERACIÓN Y REDUNDANCIA.

Como ya se ha indicado anteriormente, en el contexto de la seguridad de los Sistemas de Control Industrial, la disponibilidad adquiere mucha más importancia que la confidencialidad y la integridad. Para garantizar la disponibilidad en una red es la capacidad de recuperación y la redundancia. Los términos "resiliencia" y "redundancia" se confunden a menudo. El hecho simple es que no puede tener uno sin el otro y ambos son fundamentales para diseñar e implementar una solución de red de alta disponibilidad. Redundancia significa tener más de uno, como tener un servidor de seguridad de respaldo o un enlace alternativo entre dos switches. La resiliencia se basa en la redundancia, dictando que los cortafuegos deben instalarse en los extremos opuestos de las instalaciones para que un solo evento no elimine ambos. Las prácticas de redundancia proporcionan las capacidades de recuperación, convergencia y autorreparación de la red. Algunas prácticas recomendadas de resistencia y redundancia incluyen las siguientes:

- Zona Industrial:
  - Switch de Core (Central):
    - Pareja de switches apilados/combinados
    - Pila de switches virtuales
  - Switch de distribución/agregación:
    - Pareja de switches apilados/combinados
    - Pila de switches virtuales
  - Controladores de LAN inalámbrica (WLC – Wireless LAN Controller) activo/pasivo.
  - Infraestructura física robusta.
- Celda industrial:
  - Topología redundante con protocolo de resiliencia:
    - Topología en estrella
    - Topología en anillo:
      - REP
      - MSTP
    - Conmutación Ethernet industrial.
    - Servidores virtuales
    - Servicios de seguridad y de red.
    - Infraestructura física robusta.
- Zona industrial desmilitarizada:
  - Cortafuegos activos/pasivos
  - Infraestructura física robusta.
  - Servidores virtuales
  - Centros de datos redundantes

ARQUITECTURA DE RED RESULTANTE

Teniendo en cuenta todo lo descrito en este apartado, para disponer de una red más segura en nuestra prueba de concepto, deberemos desplegar una red similar al siguiente diagrama:

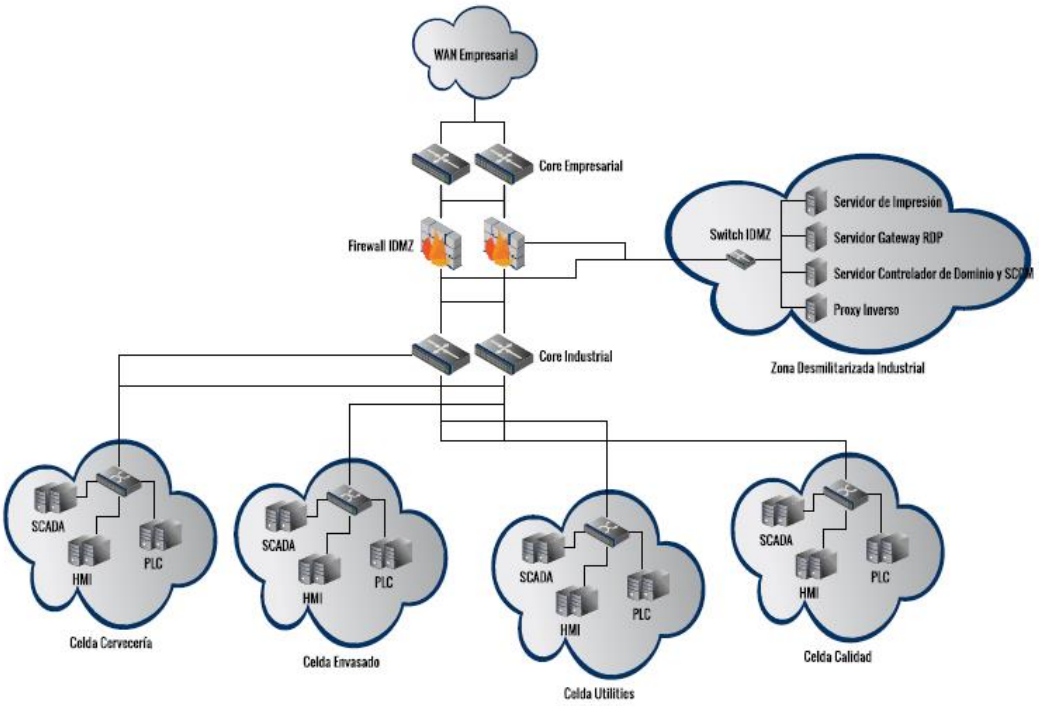

FIGURA 18 - DIAGRAMA DE RED DE LA ARQUITECTURA RESULTANTE

7. CONCLUSIONES

Como ya se ha comentado a lo largo del presente documento, es habitual que los proveedores de sistemas de control industrial soliciten la no actualización de parches del sistema operativo y de firmas del antivirus con la condición de que, en caso contrario, no se garantiza el correcto funcionamiento de los sistemas, con la posibilidad de perder el soporte por parte de sus técnicos. En estos casos, es evidente la necesidad de que dichos proveedores de sistemas industriales se acerquen más a la llamada Industria 4.0 que tiene como uno de sus pilares fundamentales la ciberseguridad y permitir, por tanto, la utilización de sistemas operativos actuales (no obsoletos) con su respectiva actualización de parches y de firmas del sistema antivirus.

Mientras tanto, se hace necesaria la presencia de un equipo responsable de la ciberseguridad de las infraestructuras críticas en empresas industriales que se encarguen del aseguramiento de los sistemas industriales críticos y del análisis continuo de las vulnerabilidades presentes con las herramientas adecuadas. Es también habitual encontrar organizaciones que no ofrecen la importancia que se merece a la seguridad IT en lo que respecta a sus entornos industriales, lo cual también debería de corregirse con una mayor concienciación por parte de la dirección de las organizaciones.

En lo que respecta al logro de los objetivos planteados en este trabajo, podemos concluir que todos los objetivos se han conseguido, a continuación, se resume el logro de cada uno de ellos:

7.1.1. OBJETIVOS GENERALES

- Se han identificado una serie de amenazas y vulnerabilidades de seguridad que afectan a los sistemas de control industrial como parte de la infraestructura crítica de las organizaciones.
- Se han estudiado los estándares y propuestas para la protección de dichos sistemas ante las amenazas y vulnerabilidades identificadas y se ha realizado una prueba de concepto de implantación de algunas de esas medidas.

7.1.2. OBJETIVOS ESPECÍFICOS

- Se han descrito los elementos y el funcionamiento de los sistemas de control industrial.
- Se han identificado los elementos de los sistemas de control industrial y su relación con las tecnologías de la información.
- Se han identificado algunas vulnerabilidades de los elementos de los sistemas de control industrial y sus posibles amenazas.
- Se han expuesto incidencias de seguridad ocurridas en infraestructuras críticas y sus causas y consecuencias en la continuidad del negocio y/o en la seguridad de las personas y medioambiental.
- Se han recopilado y estudiado algunos estándares de seguridad de las tecnologías de la información aplicadas a sistemas de control industrial.
- Se ha presentado un caso de sistema de control industrial en una empresa con una planta de fabricación de cerveza a la que se han aplicado algunas medidas de seguridad

necesarias para su protección ante las amenazas identificadas, aplicando estándares y recomendaciones de seguridad.

Sobre la metodología y la planificación planteada al inicio del documento, se ha seguido la planificación lo más fielmente posible con ciertos repuntes de trabajo necesarios por circunstancias personales que, en ocasiones, ha limitado el seguimiento de la planificación establecida. Sin embargo, estas circunstancias no han tenido impacto en la planificación realizada.

Para completar el trabajo iniciado en este documento, se podría realizar un caso de aplicación de medidas de seguridad en un Sistema de Control Industrial del mundo real y menos abstracto que el escenario que se ha planteado a lo largo de este trabajo. En dicha aplicación se podrían observar amenazas reales y aplicar las medidas propuestas de forma ajustada a presupuesto para aumentar el nivel de seguridad de la planta en estudio.

8. Glosario

- **Amenaza**: Violación de la seguridad en potencia, que existe en función de unas circunstancias, capacidad, acción o evento que pueda llegar a causar una infracción de la seguridad y/o causar algún daño en el sistema.

- **ARP**: Address Resolution Protocol. El protocolo de resolución de direcciones permite a una computadora de la red enlazar las direcciones IP y MAC de otro elemento de la red almacenando dicha correspondencia en sus tablas ARP tras la consulta por broadcast a toda la red. Se trata de un protocolo de la capa 2 (enlace de datos) del modelo OSI.

- **AS-interface**: bus de sensores y actuadores, estándar internacional IEC62026-2 que surgió como alternativa económica al cableado tradicional creando una red simple de sensores y actuadores que permita transmitir datos y alimentación por el mismo bus y que permita gran variedad de topologías para poder instalar sensores y actuadores en cualquier punto del proceso con el menor esfuerzo posible. [10]

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

- **Big data:** Es un término que describe el gran volumen de datos, tanto estructurados como no estructurados que inundan los negocios y que son analizados para obtener ideas que conduzcan a mejores decisiones y movimientos de negocios estratégicos. [41]

- **BlueBorne**: Vector de ataque de ciertas vulnerabilidades del protocolo Bluetooth que permite a un atacante tomar el control de dispositivos, penetrarse en redes corporativas y distribuir malware mediante Bluetooth. [26]

- **Botnet**: Red de equipos informáticos infectados por un atacante remoto, que los controla de manera distribuida con fines tanto malintencionados como lucrativos. Dichos equipos infectados componen una red de robots (agentes software) al servicio del atacante. El atacante se convierte, así pues, en operador de una compleja y potente red cuyos servicios serán finalmente vendidos a organizaciones de todo tipo.

- **Buffer Overflow:** Desbordamiento de buffer. Se trata de un tipo de vulnerabilidad que consiste en que una anomalía de un programa que escribe datos en un buffer de memoria y excede los límites del mismo sobrescribiendo partes de memoria adyacentes. Esta vulnerabilidad hace posible la ejecución de código malicioso en esas partes adyacentes de memoria.

- **CAD**: Computer-Aided Design. Diseño asistido por ordenador que permite la generación de dibujos y modelos con muchas características de un determinado producto y pueden almacenarse como dibujos en dos o tres dimensiones. [42]

- **CAE**: Computer-Aided Engineering. Ingeniería asistida por ordenador. Describe el proceso completo de ingeniería de un producto, desde el diseño y pruebas virtuales hasta la planificación de la producción. [43]

- **CAM**: Computer-Aided Manufacturing. Fabricación asistida por ordenador. Permite la automatización del proceso de fabricación.

- **CAN (Controller Area Network)**: Protocolo desarrollado por la firma alemana Robert Bosch GmbH y está basado en una topología bus para la transmisión de mensajes distribuidos. Este protocolo está orientado a mensajes y se basa en un modelo productor/consumidor que describe una relación entre un productor y uno o más consumidores. Está estandarizado por ISO (ISO 11898-2 e ISO 11898-3, en función de la velocidad de transmisión utilizada). [9]

- **Ciberfísico**: Término acuñado en Industria 4.0. Se trata de sistemas compuestos por componentes u objetos físicos a los que se les ha dotado de capacidades de computación y de comunicación para convertirlos en objetos inteligentes.

- **Cloud computing:** Computación en la nube, tecnología que permite acceso remoto a software, almacenamiento de archivos y procesamiento de datos por medio de Internet. [44]

- **ControlNet**: Es un protocolo abierto de red para aplicaciones de automatismos industriales que define una capa física basada en cable coaxial RG-6 con conectores BNC. [12]

- **CRM**: Customer Relationship Management. Sistema de información para la gestión de las relaciones con los clientes.

- **Cross-Site Request Forgery – CSRF**: Falsificación de petición de sitio cruzado. Vulnerabilidad de seguridad que aparece en sistemas basados en tecnología web que permiten a un atacante lograr que el usuario realice acciones no deseadas en dominios remotos. Se basa en la idea de aprovechar la persistencia de sesiones entre pestañas de un navegador. Se basa en las técnicas de Cross-Site Scripting.

- **Cross-Site Scripting**: Ejecución remota de código. Vulnerabilidad de seguridad que aparece en sistemas basados en tecnología web que se basa en la posibilidad de insertar código en un campo de entrada de datos de la web que después vaya a mostrarse al usuario, si el sitio web es vulnerable, se ejecutará el código insertado.

- **DCS**: Distributed Control System. Se trata de un tipo de Sistema de control industrial ubicado en el nivel 2 de la jerarquía funcional de los procesos industrial.

- **DeviceNet**: Este protocolo utiliza un Bus CAN al que le añade una capa de aplicación para cubrir un rango de perfiles de dispositivos. [11]

- **ERP**: Enterprise Resources Planning. Planificación de recursos empresariales. Se trata de un sistema de información que aborda la planificación de recursos humanos o financieros junto con la planificación de necesidades de materiales y de recursos de producción de una empresa.

- **Ethernet**: Estándar IEEE 802.3 de redes de computadoras de área local. Define las características de cableado y señalización de nivel físico y los formatos de tramas de datos de nivel enlace de datos del modelo OSI.

- **FEA**: Finite Element Analysis. Técnica de simulación por ordenador utilizada en ingeniería.
- **Fieldbus**: Bus de campo. Familia de protocolos de comunicaciones industriales utilizados en redes de control industrial. Está estandarizado como norma IEC 61158. [45]
- **FTP**: File Transfer Protocol. Protocolo de la capa de aplicación del modelo OSI para la transmisión de ficheros por la red de computadoras.
- **HMI**: Human Machine Interface. Es el interfaz Hombre Máquina que ofrece las herramientas necesarias para que los operarios coordinen y controlen los procesos industriales y de fabricación [46]. Se trata de un elemento de sistema de control industrial ubicado en el nivel 2 de la jerarquía funcional de los procesos industriales.
- **HTTP**: Hypertext Transfer Protocol. Protocolo de la capa de aplicación del modelo OSI para la transmisión de documentos de hipertexto como los HTML.
- **ICMP**: Internet Control Message Protocol. Protocolo que se utiliza para comprobar si un elemento de la red es alcanzable mediante el comando ping. Se trata de un protocolo de la capa 3 (red) del modelo OSI.
- **ICS**: Infrastructure Control System: Sistema de Control Industrial.
- **IDMZ**: (Industrial DeMilitarized Zone) Zona desmilitarizada Industrial.
- **IIoT**: Industrial Internet of Things. Internet de las cosas en el entorno industrial.
- **Improper Authentication**: Autenticación incorrecta. Vulnerabilidad de seguridad que consiste en la validación incorrecta de un atacante en el sistema mediante la presentación de parámetros de autenticación modificados maliciosamente. Se deben a una débil verificación de credenciales de usuario.
- **Industria 4.0**: Consiste en la introducción de las tecnologías digitales en la industria mediante la digitalización de los procesos productivos en las fábricas. [47]
- **Injection**: Inyección. Vulnerabilidad de seguridad que permite a un atacante transmitir código malicioso a través de una aplicación a otro sistema. Estos ataques incluyen llamadas al sistema operativo, el uso de programas externos a través de comandos de shell, así como llamadas a bases de datos de back-end a través de SQL (es decir, inyección de SQL). Suele deberse a aplicaciones mal diseñadas y ejecutadas.
- **Inteligencia Artificial**: Programa de computación diseñado para realizar determinadas operaciones que se consideran propias de la inteligencia humana, como el autoaprendizaje.
- **IoT:** Internet de las cosas (**I**nternet **o**f **T**hings), sistema de dispositivos de computación interrelacionados, máquinas mecánicas o digitales, objetos, animales o personas con la habilidad de enviar datos por una red sin necesidad de requerir interacción humana. [48]
- **IPC**: Industrial Personal Computer. Computadoras diseñadas para ejecutar procesos industriales que hace que su formato de fábrica sea muy distinto a los PC convencionales,

así como la electrónica utilizada para su fabricación, que los hace más resistentes y más caros.

- **IRT**: Isochronous Real-Time. Protocolo incluido dentro de PROFINET para la comunicación síncrona en tiempo real.

- **ISA-95**: estándar internacional para la integración de la empresa con los sistemas de control. Se ha adoptado como un estándar internacional como IEC/ISO 62246.

- **IT**: Information Technology. Tecnología de la Información.

- **LIMS**: Laboratory Information Management System. Sistema de gestión de información de Laboratorio que permite la administración de datos de laboratorio para mejorar su eficiencia. Permite automatizar flujos de trabajo, integrar instrumentos y gestionar información relacionada. [49]

- **M2M**: Machine To Machine. Se refiere al intercambio de información entre dos o más máquinas sin intervención humana.

- **Malware**: Software malicioso que ha sido diseñado para infiltrarse en una computadora y provocarle algún daño u obtención de información.

- **MES**: Manufacturing Execution System. Sistema de información Industrial que se encarga de la entrega y control de órdenes de producción en tiempo real desde su lanzamiento hasta la obtención del producto terminado y de la optimización de actividades de producción y mejora de la productividad global. Son elementos de un sistema de control industrial ubicados en el nivel 3 de la jerarquía funcional de los procesos industriales

- **MESA**: Manufacturing Enterprise Solutions Association. Comunidad global de fabricantes de soluciones MES. [50]

- **Modbus**: Protocolo de comunicaciones industrial situado en la capa 7 del modelo OSI y basado en una arquitectura maestro/esclavo. [8]

- **MOM**: Manufacturing Operations Management. Gestión de las operaciones de fabricación. Se puede entender como un sistema equivalente al MES.

- **MRP**: Material Requirement Planning. Sistema de información que establece una forma de planificar la producción mediante la anticipación. Los sistemas MRP originales presentaban un inconveniente claro en lo referente a la planificación de la producción, ya que no se tiene en cuenta la disponibilidad de recursos ni las capacidades de las plantas. para llevar a cabo las órdenes de producción sugeridas

- **MRP II**: Manufacturing Resources Planning. Sistema de información que surge como evolución de los MRP tradicionales donde se tiene en cuenta la disponibilidad de materiales y la capacidad de las plantas para la planificación de la producción.

- **OPC**: Estándar de interoperabilidad para el intercambio fiable de datos en el entorno de la automatización industrial. [51]

- **OPC UA**: Arquitectura Unificada de OPC es una arquitectura orientada al servicio que integra todas las funcionalidades de las especificaciones OPC en un marco extensible. [52]

- **OT**: Operation Technology. Tecnología de la Operación, normalmente referido al entorno de las operaciones industriales.

- **Path Traversal**: Recorrido de ruta de directorios. Vulnerabilidad de seguridad que consiste en que el sistema no realiza una validación adecuada de la información introducida por el usuario de tal manera que no se detectan los caracteres de subida al directorio superior y permite a un atacante acceder sin permisos al sistema de archivos.

- **PLC**: Programable Logic Controller. Controladores Lógicos Programables. Dispositivos que toman datos de los sensores mediante sus canales de entrada y controlan los actuadores mediante sus canales de salida. Son elementos de un sistema de control industrial ubicados en el nivel 1 de la jerarquía funcional de los procesos industriales.

- **PROFIBUS**: Process Field Bus. Estándar de comunicaciones definido por grandes empresas alemanas como Bosch y Siemens. Utiliza conexiones físicas seriales como RS-485, MBP (Manchester Coding and Bus Powered) o fibra óptica. [7]

- **PROFINET**: Es la adaptación del estándar PROFIBUS sobre Ethernet, HART, ISA100 o Wi-Fi como medio de comunicación. Este protocolo utiliza servicios TCP/IP para la configuración o diagnósticos, pero los evita para el intercambio de mensajes deterministas, en favor del protocolo RT (Real-Time) o IRT (Isochronous Real-Time).

- **RA**: Realidad Aumentada. Añade una capa adicional a la visión que tenemos de la realidad aportando información extra proveniente de un modelo digital de la realidad.

- **Ransomware**: Programa de software malicioso que infecta una computadora y muestra mensajes que exigen el pago de dinero para restablecer el funcionamiento del sistema.

- **RT**: Real-Time Protocol o RTP Real-Time Transport Protocol. Se trata de un protocolo de comunicaciones en la capa de Transporte que permite comunicaciones entre extremos. Se suele utilizar para el envío de audio, vídeo e información crítica que es necesario obtenerla en tiempo real.

- **RV**: Realidad Virtual. Permite la visualización informática por medio de dispositivos (cascos, gafas, pantallas 3d, etc.) de un modelo informático que sustituye a la realidad que nos rodea.

- **SCADA**: Supervisory Control And Data Acquisition. Se trata de un elemento de Sistema de control industrial ubicado en el nivel 2 de la jerarquía funcional de los procesos industriales.

- **SCM**: Supply Chain Management. Sistema de información para la gestión de la cadena de suministro. Incluye Planificación, Distribución y logística, Compras y Producción.

- **TCP/IP**: Conjunción de los protocolos TCP (Transmission Control Protocol) de la capa de Transporte e IP (Internet Protocol) de la capa de red del modelo OSI.

- **Telnet**: Telecommunication Network. Protocolo de la capa 7 del modelo OSI que proporciona un terminal virtual bidireccional basado en texto entre computadoras.

- **TIC:** Tecnologías de la Información y las Comunicaciones.

- **VLANs:** Virtual Local Area Network. Redes lógicas independientes creadas dentro de una única red física.

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

9. BIBLIOGRAFÍA

[1] A. D. J. Nikolic, «Seguridad Informática para Sistemas de Control Industrial en Instalaciones Nucleares».

[2] K.-H. K. H. J. M. A. F. S. R. P. F. A. M. T. J. C. Leandros A. Maglaras, «Cyber security of critical infrastructures,» *ScienceDirect,* 2018.

[3] P. Ackerman, Industrial Cybersecurity - Efficiently secure critical infrastructure systems, Birmingham - Mumbai: Packt Publishing, 2017.

[4] I. (. I. S. a. A. Society), «Estándar ANSI/ISA-95, Part 3: Activity Models of Manufacturing Operations Management,» American National Standard, 2005.

[5] MESA International, «MES explained: A high level vision. White Paper 6,» 1997.

[6] F. M. J. Delgado, «Evolución en los sistemas de gestión empresarial. Del MRP al ERP,» 2000.

[7] «Wikipedia,» [En línea]. Available: https://es.wikipedia.org/wiki/Profibus. [Último acceso: 01 Noviembre 2018].

[8] «Wikipedia,» [En línea]. Available: https://es.wikipedia.org/wiki/Modbus. [Último acceso: 01 Noviembre 2018].

[9] «Wikipedia,» [En línea]. Available: https://es.wikipedia.org/wiki/Bus_CAN. [Último acceso: 01 Noviembre 2018].

[10] «Wikipedia,» [En línea]. Available: https://es.wikipedia.org/wiki/AS-interface. [Último acceso: 01 Noviembre 2018].

[11] «Wikipedia,» [En línea]. Available: https://es.wikipedia.org/wiki/DeviceNet. [Último acceso: 01 Noviembre 2018].

[12] «Wikipedia,» [En línea]. Available: https://es.wikipedia.org/wiki/Controlnet. [Último acceso: 01 Noviembre 2018].

[13] U. P. d. Madrid, *Materiales del MOOC (Massive Online Open Course) Industria 4.0,* 2018.

[14] «Hannover Messe,» [En línea]. Available: http://www.hannovermesse.de/en/news/key-topics/artificial-intelligence/. [Último acceso: 02 Noviembre 2018].

[15] «Kaspersky Lab "La ciberseguridad en los sistemas de control industrial",» 07 Junio 2017. [En línea]. Available: https://securelist.com/threat-landscape-for-industrial-automation-systems-in-h2-2017/85053/. [Último acceso: 15 11 2018].

[16] «Schneider Electric Modicon Modbus Protocol - ICS-CERT,» 11 Abril 2017. [En línea]. Available: https://ics-cert.us-cert.gov/advisories/ICSA-17-101-01. [Último acceso: 16 Noviembre 2018].

[17] «Siemens industrial products using the Discovery Service of the OPC UA protocol stack by the OPC foundation (Update B) - ICS-CERT,» 03 Octubre 2017. [En línea]. Available: https://ics-cert.us-cert.gov/advisories/ICSA-17-243-01B. [Último acceso: 16 Noviembre 2018].

[18] «Siemens devices using the PROFINET Discovery and Configuration Protocol (Update J) - ICS-CERT,» 09 Mayo 2017. [En línea]. Available: https://ics-cert.us-cert.gov/advisories/ICSA-17-129-01. [Último acceso: 16 Noviembre 2018].

[19] «Dnsmasq Vulnerabilities Affect Siemens SCALANCE Solutions - Kaspersky Lab ICS CERT,» 05 Diciembre 2017. [En línea]. Available: https://ics-cert.kaspersky.com/news/2017/12/05/dnsmasq/. [Último acceso: 16 Noviembre 2018].

[20] «Schneider Electric Trio TView - ICS-CERT,» 01 Agosto 2017. [En línea]. Available: https://ics-cert.us-cert.gov/advisories/ICSA-17-213-02. [Último acceso: 16 Noviembre 2018].

[21] «PHOENIX CONTACT mGuard Device Manager - ICS-CERT,» 19 Septiembre 2017. [En línea]. Available: https://ics-cert.us-cert.gov/advisories/ICSA-17-262-01. [Último acceso: 16 Noviembre 2018].

[22] «Rockwell Automation Stratix 5900 - ICS-CERT,» 09 Mayo 2017. [En línea]. Available: https://ics-cert.us-cert.gov/advisories/ICSA-17-094-04. [Último acceso: 16 Noviembre 2018].

[23] «Intel Releases Updates to Close ME, SPS and TXE Vulnerabilities - Kaspersky Lab ICS CERT,» 24 Noviembre 2017. [En línea]. Available: https://ics-cert.kaspersky.com/news/2017/11/24/intel-updates/. [Último acceso: 16 Noviembre 2018].

[24] «New Botnet Recruits IoT Devices Across the Globe - Kaspersky Lab ICS CERT,» 09 Noviembre 2017. [En línea]. Available: https://ics-cert.kaspersky.com/news/2017/11/09/reaper/. [Último acceso: 18 Noviembre 2018].

[25] «The brief awakening of the Satori botnet - Kaspersky Lab ICS CERT,» 14 Diciembre 2017. [En línea]. Available: https://ics-cert.kaspersky.com/news/2017/12/14/satori/. [Último acceso: 18 Noviembre 2018].

[26] «New Attack Vector Affecting Bluetooth Devices - Kaspersky Lab ICS CERT,» 15 Septiembre 2017. [En línea]. Available: https://ics-cert.kaspersky.com/news/2017/09/15/blueborne/. [Último acceso: 18 Noviembre 2018].

[27] «El virus que tomó control de mil máquinas y les ordenó autodestruirse - BBC News Mundo,» 11 octubre 2015. [En línea]. Available: https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet. [Último acceso: 20 Noviembre 2018].

[28] K. Zetter, «An Unprecedented Look at Stuxnet, the World's First Digital Weapon - WIRED,» 11 Marzo 2014. [En línea]. Available: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/. [Último acceso: 20 Noviembre 2018].

[29] R. L. y. A. Cherepanov, «El troyano BlackEnergy ataca a una planta de energía eléctrica en Ucrania,» 5 Enero 2016. [En línea]. Available: https://www.welivesecurity.com/la-es/2016/01/05/troyano-blackenergy-ataca-planta-energia-electrica-ucrania/. [Último acceso: 20 Noviembre 2018].

[30] A. C. y. R. Lipovsky, «GreyEnergy: uno de los actores maliciosos más peligrosos cuenta con un arsenal actualizado,» 17 Octubre 2018. [En línea]. Available: https://www.welivesecurity.com/la-es/2018/10/17/greyenergy-actores-maliciosos-peligrosos-arsenal-actualizado/. [Último acceso: 23 Noviembre 2018].

[31] «Cyber Security in the Manufacturing Industry - MAMTC,» 23 Junio 2017. [En línea]. Available: https://www.mamtc.com/blog/2017/06/23/cyber-security-in-the-manufacturing-industry. [Último acceso: 23 Noviembre 2018].

[32] D. Kortepeter, «Operation Ghoul cyber attack hits industrial, engineering sectors - TechGenix,» 02 Septiembre 2016. [En línea]. Available: http://techgenix.com/operation-ghoul-cyber-attack/. [Último acceso: 24 Noviembre 2018].

[33] «Cyber Security Risk Assessments - IT Governance UK,» [En línea]. Available: https://www.itgovernance.co.uk/cyber-security-risk-assessments-10-steps-to-cyber-security. [Último acceso: 27 Noviembre 2018].

[34] B. S. A. S. K. W. S. H. Clint Bodungen, Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions, McGraw-Hill Education, 2016.

[35] «ISA99, Industrial Automation and Control Systems Security,» [En línea]. Available: https://www.isa.org/isa99/. [Último acceso: 28 Noviembre 2018].

[36] E. Edbrooke, «A Four Step Guide to Secure Your ICS Network Using ISA 99/IEC 62443 - Security Matters,» 05 Septiembre 2017. [En línea]. Available: https://www.secmatters.com/blog/a-four-step-guide-to-secure-your-ics-network-using-isa-99iec-62443. [Último acceso: 29 Noviembre 2018].

[37] «Converged Plantwide Ethernet (CPwE) Design and Implementation Guide,» Cisco & Rockwell Automation, 2011.

[38] «Exploit Database - Siemens Simatic S7-300/400 - CPU START/STOP Module (Metasploit),» 14 Julio 2012. [En línea]. Available: https://www.exploit-db.com/exploits/19831. [Último acceso: 15 12 2018].

[39] «Exploit Database - Siemens Simatic S7 1200 - CPU Command Module (Metasploit),» 14 Diciembre 2015. [En línea]. Available: https://www.exploit-db.com/exploits/38964. [Último acceso: 15 Diciembre 2018].

[40] Siemens, «Operational Guidelines for Industrial Security,» Siemens AG, 2013.

[41] «PowerData - Big Data: ¿En qué consiste? Su importancia, desafíos y gobernabilidad,» [En línea]. Available: https://www.powerdata.es/big-data. [Último acceso: 4 Octubre 2018].

[42] «3D CAD Portal,» [En línea]. Available: http://www.3dcadportal.com/cad.html. [Último acceso: 04 Noviembre 2018].

[43] «SimWiki,» [En línea]. Available: https://www.simscale.com/docs/content/simwiki/general/whatiscae.html. [Último acceso: 04 Noviembre 2018].

[44] «Salesforce - ¿Qué es el Cloud Computing?,» [En línea]. Available: https://www.salesforce.com/mx/cloud-computing/. [Último acceso: 4 Octubre 2018].

[45] «Monografias.com,» [En línea]. Available: https://www.monografias.com/trabajos82/protocolo-fieldbus/protocolo-fieldbus.shtml. [Último acceso: 03 Noviembre 2018].

[46] «Wonderware,» [En línea]. Available: http://www.wonderware.es/hmi-scada/que-es-hmi/. [Último acceso: 01 Noviembre 2018].

[47] R. Archanco, «Papeles de inteligencia - ¿Qué es Industria 4.0 o la cuarta revolución indutrial?,» [En línea]. Available: https://papelesdeinteligencia.com/que-es-industria-4-0/. [Último acceso: 4 Octubre 2018].

[48] «TechTarget - What is internet of things (IoT)?,» [En línea]. Available: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT. [Último acceso: 4 Octubre 2018].

[49] «Hylasoft,» [En línea]. Available: https://www.hylasoft.com/es/solution/laboratory-information-management-system-lims. [Último acceso: 03 Noviembre 2018].

[50] «MESA.ORG,» [En línea]. Available: http://www.mesa.org/en/index.asp. [Último acceso: 03 Noviembre 2018].

[51] «OPC Foundation.ORG,» [En línea]. Available: https://opcfoundation.org/about/what-is-opc/. [Último acceso: 04 Noviembre 2018].

[52] «OPC Foundation.ORG,» [En línea]. Available: https://opcfoundation.org/about/opc-technologies/opc-ua/. [Último acceso: 04 Noviembre 2018].