Protocolos y seguridad de red en infraestructuras SCI

INSTITUTO NACIONAL DE CIBERSEGURIDAD

SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_

Autores

Miguel Herrero Collantes

Antonio López Padilla

Primera publicación en mayo 2015

Actualizado por CERTSI en febrero 2017

CERTSI_GUIA_SCI_001_ProtocolosRed_2017_v2

ÍNDICE

1 INTRODUCCIÓN

El crecimiento de Internet y la aparición de infinidad de dispositivos con conectividad y posibilidad de proceso han traído de la mano nuevos retos de seguridad que afectan también a infraestructuras críticas. Estas infraestructuras, normalmente regidas por sistemas de control industrial específicos para la monitorización y gestión de los procesos típicos de la industria, se ven cada día más expuestas a la interacción con otros sistemas del entorno de Internet. La tendencia observada en la detección de amenazas deja patente que las infraestructuras industriales han pasado a convertirse en un importante objetivo de ataques en los cuales se ven implicados actores relacionados con terrorismo, gobiernos, espionaje industrial, etc. Prueba de ello, son los cada vez más numerosos incidentes y eventos relacionados con este tipo de infraestructuras, como podemos observar en la siguiente línea temporal:

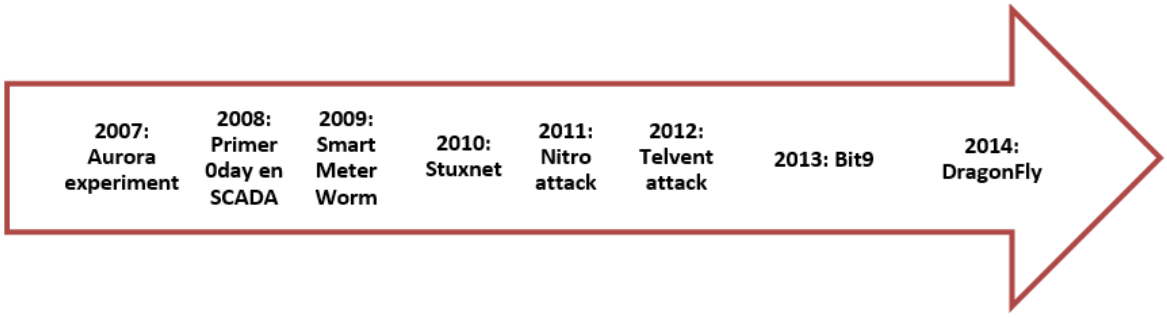

Ilustración 1. Linea de tiempo de amenazas en sistemas de control industrial

Como defiende la experta Marina Krotofil[1], es patente en la comunidad de seguridad de infraestructuras críticas que no es suficiente con incorporar medidas típicas de seguridad IT, como protección perimetral y segmentaciones seguras de red. También, al contrario que en sistemas IT estándar, en sistemas industriales es peligroso portar directamente una solución de un sistema a otro, ya que las características de éste último pueden incluir factores que hagan vulnerable esta integración «directa».

Todo ello hace que un conocimiento detallado de los protocolos implicados en procesos industriales sea clave para entender los posibles puntos débiles, vectores de ataque y posibles medidas de defensa deban ser barajadas a la hora de implementar o fortificar un sistema de control industrial.

[1] http://www.marinakrotofil.com/p/home.html

1.1. ORGANIZACIÓN DE ESTE DOCUMENTO

Este documento se compone de dos capítulos. En el primero, Arquitectura de red de los Sistemas de Control Industrial se pretende proporcionar unos conocimientos básicos al lector de cómo se debería realizar el despliegue de un Sistema de Control Industrial con la mayor seguridad posible.

El segundo capítulo, Protocolos de comunicación en SCI, pretende dar una visión de alto nivel sobre el diseño, funcionamiento y características de seguridad que presentan los protocolos. El estudio se centra en los protocolos más significativos utilizados en SCI de Europa y más concretamente España, sin realizar distinción del sector en el que se utilizan, con objeto de dotar al lector del conocimiento necesario para entender las propiedades, funcionalidades, fortalezas y debilidades en la implementación y seguimiento de sistema. También se describen una serie de recomendaciones específicas de seguridad para cada protocolo, si bien esas medidas de seguridad deben ser analizadas antes de ser puestas en marcha a fin de no afectar la operativa.

2 ARQUITECTURA DE RED DE LOS SISTEMAS DE CONTROL INDUSTRIAL

Cuando se diseña una arquitectura de red, desde el punto de vista de la seguridad, siempre se recomienda establecer un modelo con segmentos de red diferenciadas. Separando las redes en segmentos con distintas funciones y objetivos es posible aplicar una mayor granularidad en las medidas de seguridad y evitar flujos de información innecesaria.

Siguiendo esta recomendación el segmento de red de Sistemas de Control Industrial (SCI) debe separarse del segmento de red corporativa, puesto que la naturaleza del tráfico de las distintas áreas está perfectamente diferenciado. En la zona de red corporativa son necesarios servicios como acceso a Internet, correo electrónico, FTP, etc., que suponen un riesgo para la zona de red de SCI.

Así, un apropiado diseño con zonas diferenciadas y con mecanismos de control de tráfico entre los distintos segmentos debe ser siempre el primer paso en la implementación segura de la arquitectura de red.

Por lo tanto, es recomendable establecer distintos niveles en la arquitectura de red como primer paso para la planificación de una infraestructura SCI, identificando cada segmento según su cometido en la plataforma.

La arquitectura SCI propuesta por el estándar de la «*International Society of Automation*»(ISA) [1] en su norma ISA-95 sobre integración entre sistemas empresariales y de control, es un ejemplo de esta separación por niveles. En este estándar se propone un modelo denominado Purdue Enterprise Reference Architecture, que establece 5 niveles lógicos bajo los cuales se agruparán en segmentos de red elementos de la arquitectura con funciones diferenciadas, tal y como se puede ver en la Ilustración 2. Esta propuesta de segmentación facilita el diseño de estrategias de seguridad adoptando medidas específicas a cada nivel y estableciendo mecanismos seguros para el flujo de información entre ellos.

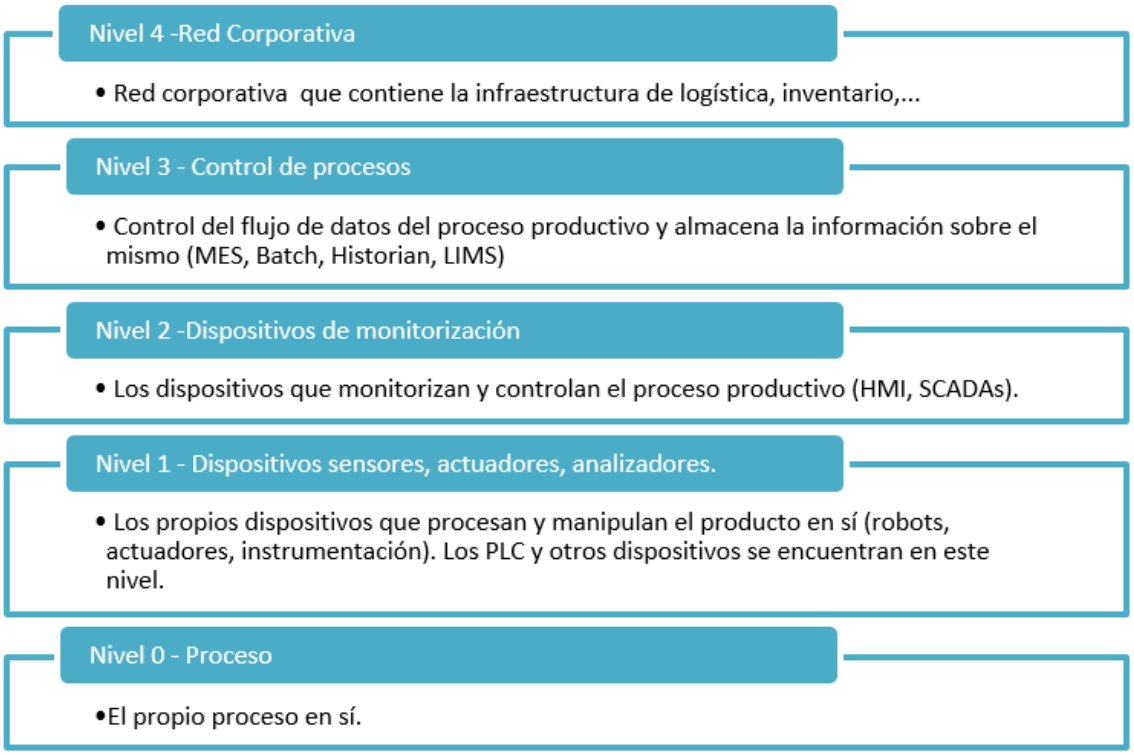

Ilustración 2. Niveles lógicos de arquitectura de red según norma ISA-95

2.1. SEGURIDAD BÁSICA EN EL DISEÑO DE UNA RED SCI

Partiendo pues de un modelo de arquitectura de red separada por zonas, se debe dividir la red en el número de segmentos de red necesarios para poder diferenciar y dotar de las medidas de seguridad y control de tráfico apropiados para cada uno de ellos. Esta separación es un concepto efectivo y esencial en la planificación de cualquier arquitectura de red e igualmente aplicable en Sistemas de Control Industrial. Este tipo de diseño, unido a controles de flujo de datos adecuados entre los dominios definidos, minimizará el daño producido por el posible compromiso de un dispositivo de un dominio determinado.

2.2. SEGURIDAD DE RED

Este objetivo puede lograrse incorporando soluciones habituales diseñadas para la división y protección de segmentos de red, donde se tendrán en cuenta:

- **Segmentación en zonas.** Dividir la arquitectura de red en zonas diferenciadas según su función para ajustarse lo más cercanamente posible a la propuesta de referencia ISA-95.Tal y como se muestra en la Ilustración 3, como mínimo se deben contar con **tres zonas** que separen Red Control, DMZ y LAN corporativa. Esta medida permite contener una infección dentro de una misma zona, dificultando el salto a otras zonas.

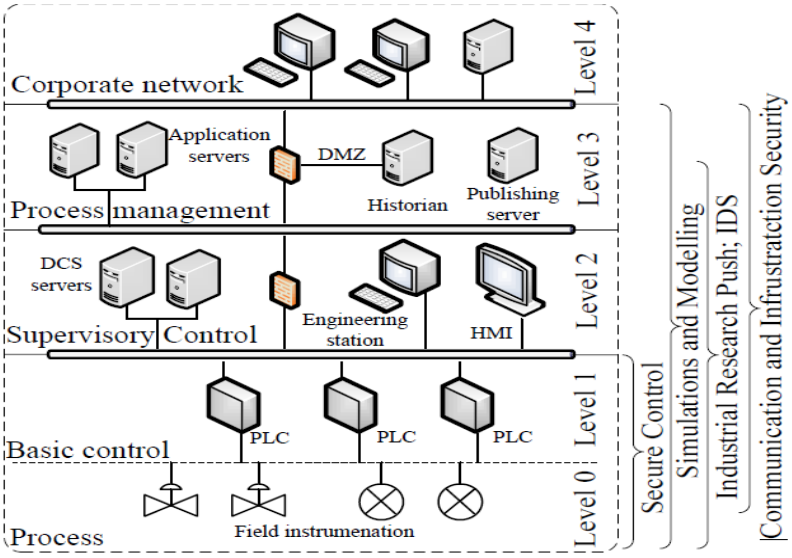

Ilustración 3. Arquitectura de referencia SCI [2] ajustada a modelo ISA-95.

- **Cifrado de la comunicación y separación lógica** entre segmentos de red, mediante el uso de tecnologías de VLAN y VPN. Esta medida también sirve para evitar el salto de una infección entre capas.

- **Control y filtrado de tráfico** a través de cortafuegos[2], *proxies*, y elementos destinados a identificar y separar tráfico y comunicaciones tanto a nivel de red (IP, encaminamiento) como por puerto/protocolo y nivel de aplicación. Esta medida ayudará a la detección de la infección cuando intente cambiar de zona. Si se añade a la red elementos como IDS o SIEM para el control de eventos, alertas de intrusión y *logs*, la red conformada será similar a la de la Ilustración 4.

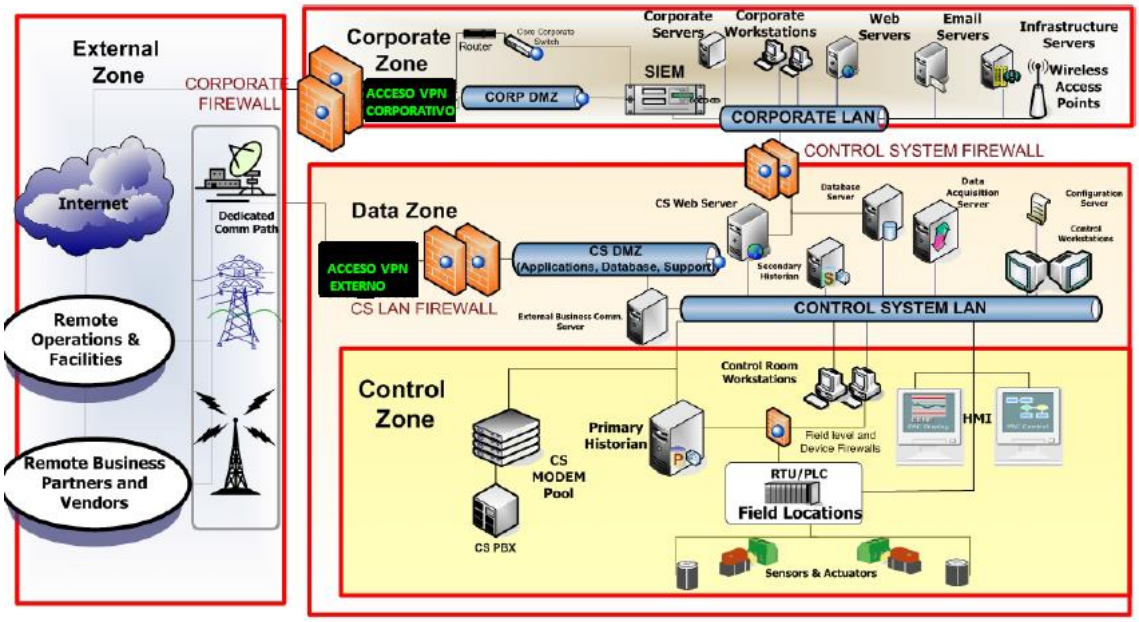

Ilustración 4. Segmentación de red y controles de comunicaciones [3]

- **Extensión de la seguridad a las capas de enlace y de aplicación.** Extender las medidas de seguridad a nivel de capa de enlace con controles de acceso como 802.1x y filtrado por dirección MAC, y a nivel de aplicación con uso de cortafuegos de aplicaciones (WAF).
- **Control de acceso.** Control de tráfico basado en listas blancas (*whitelisting*), implementando reglas de acceso basadas en elementos conocidos negando el acceso a todo lo demás.
- **Redes inalámbricas.** Las redes inalámbricas conllevan un riesgo adicional, por lo que deben implementarse únicamente bajo necesidad o decisión particular por la organización y siempre bajo condiciones justificadas. En su caso, se utilizarán mecanismos IEEE 802.1x para la autenticación haciendo uso de protocolos EAP-TLS que autentican clientes con certificados o haciendo uso de un servidor RADIUS. Los puntos de acceso se situarán en redes aisladas o con mínimos puntos de interconexión a la red de control SCI (evitándolo si es posible). Utilizar un protocolo robusto para las comunicaciones inalámbricas como WPA2, adicionalmente usar un SSID característico y único, desactivando su broadcast e igualmente habilitar filtrado por dirección MAC.

[2] Las recomendaciones generales para las reglas de cortafuegos y de otros servicios pueden consultarse en el Anexo I

2.3. CIFRADO DE LAS COMUNICACIONES

La mayoría de protocolos de control industrial, no incorporan cifrado en su implementación. Así, cualquier acceso no autorizado a la red permitiría a un atacante inspeccionar y manipular el tráfico. De esta forma el uso de HTTPS, SSH, SNMP v3 en la medida que sea posible es altamente recomendado para la autenticación y el acceso a servicios de la red o los dispositivos de la misma.

2.4. AUTENTICACIÓN Y CONTROL DE ACCESO

Una adecuada gestión de privilegios basados en roles (RBAC)[3] es una medida que aporta seguridad en el aspecto de las restricciones relativas a cada perfil. Por ello, crear distintos perfiles de usuario diferenciados y asignar un rol operativo a cada uno, dependiendo de sus funciones, resultará un complemento interesante. Añadir medidas adicionales como mensajes de advertencia que ayuden a identificar el servicio al que se accede en previsión de posibles errores no intencionados.

2.5. ACCESO REMOTO

En caso de ser necesario el acceso desde infraestructuras externas a la red de control, la utilización de soluciones VPN aportará el cifrado y autenticación necesarios para proteger la conexión. El uso de un software y/o hardware especializado para acceso remoto, así como una adecuada política de seguridad relativa al mantenimiento de actualizaciones, de gestión de acceso y usuarios.

2.6. DISPONIBILIDAD

En un sistema de control de procesos, la latencia y la velocidad de transmisión de mensajes son críticos, por eso son un factor determinante que el diseño de la red de control esté preparado para afrontar posibles problemas de congestión o pérdida de conectividad. Las recomendaciones para incrementar la resiliencia de red frente a estos problemas son:

- Uso de conmutadores que aporten funcionalidades de red para segmentar en VLAN y priorizar distintos tipos de tráfico mediante criterios de calidad de servicio[4].
- Utilizar topologías redundantes para reforzar la disponibilidad, así como implementar STP (*Spanning Tree Protocol)* para controlar la formación de bucles de red.
- Usar protocolo IGMP[5] junto con VLAN para proporcionar un mejor rendimiento y confinamiento de los mensajes de *multicast* dependiendo del tipo de tráfico y los dispositivos relacionados

[3] http://en.wikipedia.org/wiki/Role-based_access_control#RBAC_and_employees.27_responsibilities_alignment
[4] http://es.wikipedia.org/wiki/Calidad_de_servicio
[5] http://es.wikipedia.org/wiki/Internet_Group_Management_Protocol

2.7. POLÍTICA DE GESTIÓN DE LA SEGURIDAD

Todos los elementos que conforman la seguridad de la infraestructura han de tener una monitorización y seguimiento periódico para determinar necesidades de parcheado, actualizaciones y otros problemas derivados de la aparición de vulnerabilidades o defectos que puedan detectarse en el periodo de funcionamiento.

2.8. SEGURIDAD FÍSICA DE DISPOSITIVOS FINALES

Restringir el acceso físico a los dispositivos de control de procesos, así como elementos de red es un complemento necesario a las restricciones de acceso remoto y autenticación. Igualmente paneles de conexión, cableado, alimentación, etc. deben encontrarse debidamente protegidos contra accesos no autorizados.

3 PROTOCOLOS DE COMUNICACIÓN EN SCI

3.1. PROTOCOLOS A ANALIZAR

En este capítulo se va a analizar la seguridad de los protocolos de comunicación en sistemas de control industriales más utilizados en Europa y más concretamente en España, sin hacer distinción del sector en el que son más predominantes. Los protocolos analizados son los siguientes:

- Common Industrial Protocol (CIP).
- MODBUS
- DNP3
- Profibus
- Profinet
- Powerlink Ethernet
- OPC
- EtherCAT

3.2. CAPAS DE ACTUACIÓN DE LOS PROTOCOLOS

A pesar de que el modelo OSI de 7 capas de la ISO goza de gran popularidad, en este documento, a fin de simplificar el análisis y la comparativa, se va a utilizar el modelo TCP/IP de únicamente 4 capas.

Estas son:

- Capa aplicación: asimilable a las capas: 5, 6 y 7 del modelo OSI.
- Capa de transporte: similar a la capa 4 del modelo OSI.
- Capa de internet: equivalente a la capa 3 del modelo OSI.
- Capa de acceso a la red: asimilable a la capa 1 y 2 del modelo OSI.

La comparativa entre el modelo OSI y el modelo TCP/IP se muestra en la Ilustración 5.

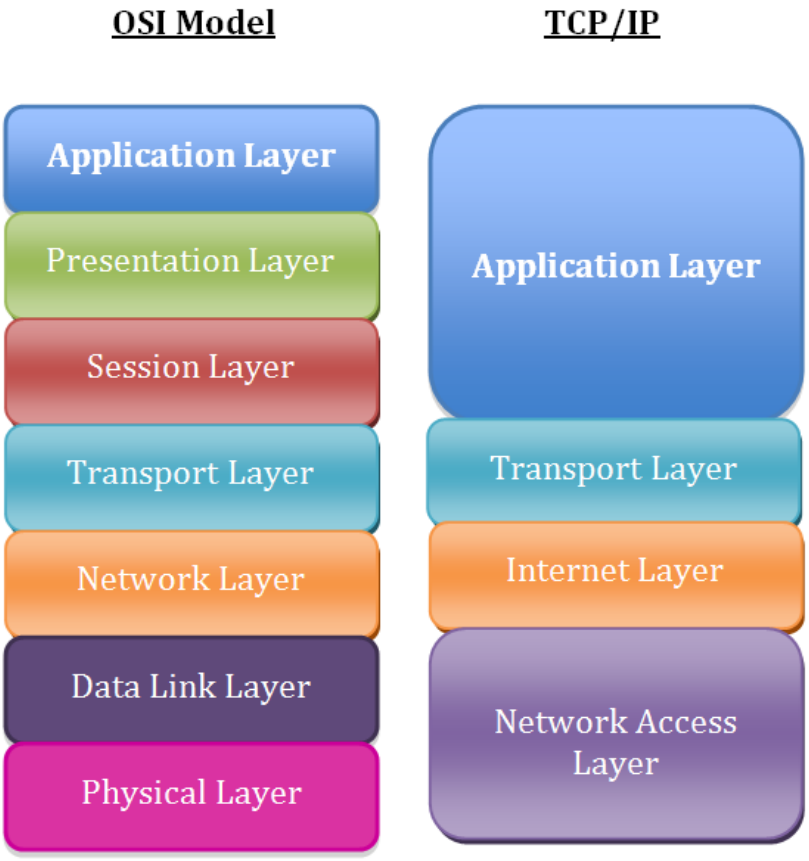

Ilustración 5: Relación entre el modelo OSI y el TCP/IP

La capa 1 de este modelo, la capa de acceso a la red, es la encargada de la transmisión de bits de forma individual entre estaciones, por lo que incluye medidas para comprobar la correcta transmisión del bit, pero no incluye medidas de seguridad propiamente dichas. También dispone de mecanismos de seguridad para comprobar que el acceso a la red es realizado únicamente por aquellos dispositivos autenticados, como podría ser 802.1x.

En el estudio individual de los protocolos analizaremos las medidas de seguridad específicas de las capas superiores, complementarias a aquellas medidas genéricas de la capa de acceso a la red.

3.3. COMMON INDUSTRIAL PROTOCOL (CIP)

3.3.1. Descripción

Common Industrial Protocol (CIP) es un protocolo creado por la compañía ODVA[6] para la automatización de procesos industriales. CIP engloba un conjunto de servicios y mensajes de control, seguridad, sincronización, configuración, información, etc., los cuales pueden integrarse en redes Ethernet y en Internet. CIP cuenta con varias adaptaciones, proporcionado intercomunicación e integración a distintos tipos de redes. Estas son:

- **Ethernet/IP**: adaptación de CIP a TCP/IP.
- **ControlNet:** integración de CIP con tecnologías CTDMA (Concurrent Time Domain, Multiple Access).
- **DeviceNet**: adaptación de CIP con CAN, Controller Area Network.
- **CompoNet:** adaptada a tecnologías TDMA, Time Division Multiple Access.

La integración del modelo OSI con las diferentes familias de este protocolo, así como sus niveles de equivalencia se puede ver en la Ilustración 6.

[6] https://www.odva.org/

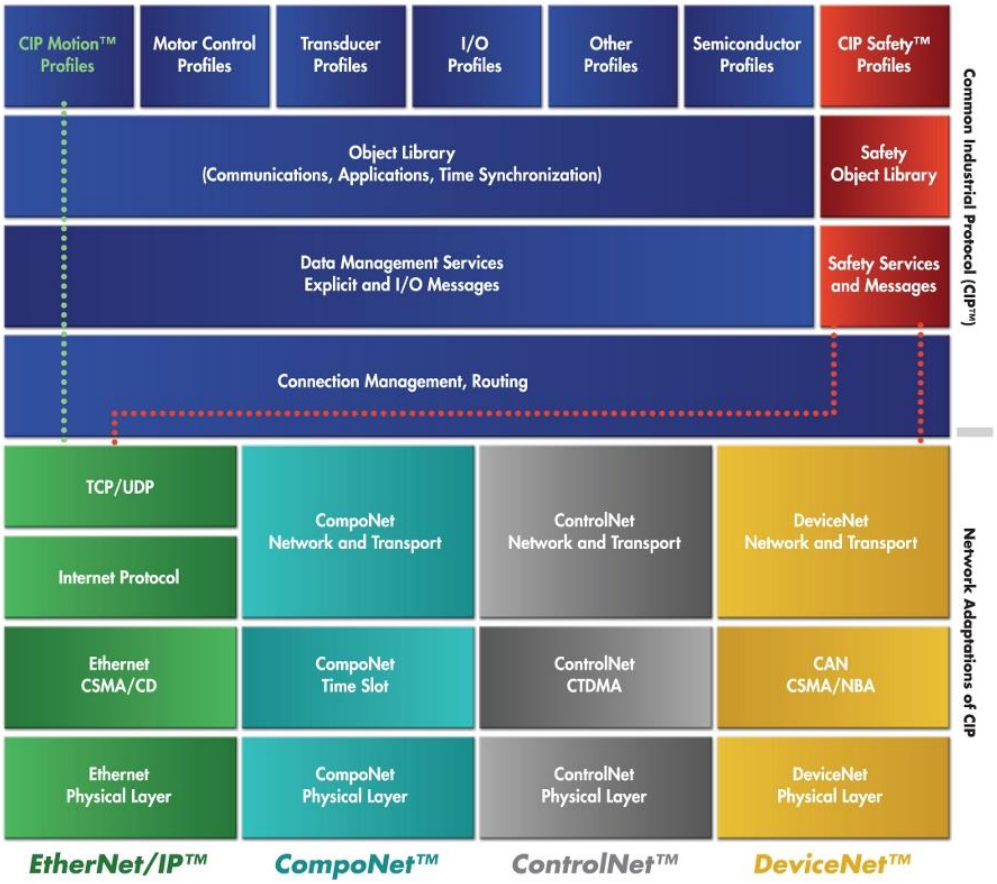

Ilustración 6. Integración de la arquitectura CIP en el modelo OSI de red. Fuente: odva.org

3.3.1.1. Modelo de objetos CIP

CIP es un protocolo que sigue un *modelo de objetos*. Cada objeto está formado por atributos (datos), servicios (comandos), conexiones y comportamiento (relación entre los datos y los servicios). CIP cuenta con un extenso número de objetos para cubrir las comunicaciones y funciones típicas con elementos comunes en procesos de automatización, como dispositivos entrada/salida analógicos y digitales, HMI, controles de movimiento, etc. Para asegurar la intercomunicación, un mismo objeto CIP implementado en distintos dispositivos se comporta de forma idéntica, constituyendo lo que se denomina un «perfil de dispositivo». Así, cualquier dispositivo que adopte un perfil, responderá de igual forma a los mismos comandos y mantendrá el mismo comportamiento de red que otro dispositivo con el mismo perfil.

3.3.1.2. Mensajes CIP

CIP sigue un modelo *productor/consumidor*. Este tipo de arquitectura, a diferencia de la tradicional origen/destino, es de *tipo multicast.* Es decir, los mensajes se ponen en circulación por un productor y son los distintos nodos consumidores de la red los que deciden si ese mensaje es para ellos o no en base a un campo identificador que acompaña a los mensajes.

De este modo, podemos discernir dos tipos de mensajes que se identifican con cada arquitectura:

- Mensajes implícitos (Ilustración 7), que únicamente llevan un identificador en lugar de direcciones de origen o destino y son los nodos consumidores, basándose en ese identificador, los que saben si el mensaje les concierne a ellos y qué acción tomar en ese caso.
- Mensajes explícitos (Ilustración 8), que contienen información de direcciones origen/destino de los dispositivos e información sobre una acción concreta como en un modelo IP.

Algunas implementaciones de CIP, como Ethernet/IP o ControlNet también hacen usos de mensajes explícitos.

Ilustración 7. Modelo de mensaje productor/consumidor (multicast)

Ilustración 8. Modelo de mensaje origen/destino

3.3.2. Implementaciones CIP: DeviceNET, ControlNET y CompoNET

3.3.2.1. Descripción

Estas familias de tecnologías de CIP utilizan diferentes medios para la transmisión. Respectivamente utilizan bus CAN[7], coaxial RG-6[8] y cables redondos (los sustitutos de los cables planos[9]).

3.3.2.2. Seguridad

La diferencia entre las tres implementaciones reside en el mecanismo físico para la transmisión de la información, el cual no tiene capacidad para aportar ninguna medida de seguridad.

[7] http://es.wikipedia.org/wiki/Bus_CAN
[8] http://es.wikipedia.org/wiki/RG-6
[9] http://es.wikipedia.org/wiki/Cable_cinta

3.3.2.3. Recomendaciones de seguridad

La mejor medida de seguridad para proteger estas implementaciones de CIP consiste en el aislamiento de forma lógica del resto de la red, siendo preciso un despliegue que los aísle de cualquier conexión exterior. Adicionalmente sistemas de inspección de tráfico y/o detección de intrusos[10] (IDS,IPS) son recomendables

3.3.3. Implementación CIP: Ethernet/IP

3.3.3.1. Descripción

Ethernet/IP fue introducido en 2001 y es uno de los protocolos que implementan CIP más extendidos, probados y completos en la automatización de industria manufacturera. Ethernet/IP es pues, la adaptación de CIP al modelo de red Ethernet el cual va unido inherentemente a TCP/IP. Por tanto, Ethernet/IP hace uso de la pila TCP/IP para todas las tareas de transporte y red, adaptando CIP para la capa de aplicación, como se puede ver en la Ilustración 9.

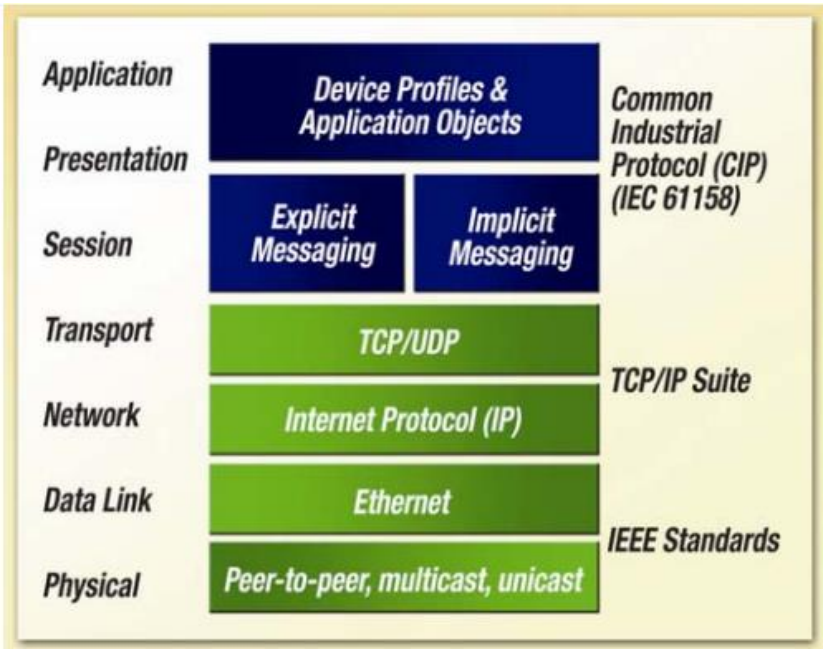

Ilustración 9. Integración de Ethernet/IP en modelo OSI. Encapsulación sobre trama TCP/UDP

Ethernet/IP como protocolo CIP, define dos métodos de conexión para su comunicación TCP/IP: Mensajes explícitos, usando TCP e implícito (de entrada/salida) usando UDP. Los mensajes explícitos siguen el patrón de conexión cliente-servidor o petición-respuesta. Entre

[10] http://es.wikipedia.org/wiki/Sistema_de_detecci%C3%B3n_de_intrusos

ellos están los mensajes entre los PLC y los HMI, mensajes de diagnóstico, y transferencia de ficheros. El puerto utilizado es el 44818 TCP.

Los mensajes implícitos son aquellos críticos y se usan para comunicaciones en tiempo real, como la transmisión de datos y generalmente operan con direcciones *multicast* por eficiencia. De este modo un mensaje cuyo destino son distintos dispositivos solo ha de mandarse una vez. Se transmiten usando el puerto UDP 2222. La Ilustración 10 muestra este tipo de comunicación.

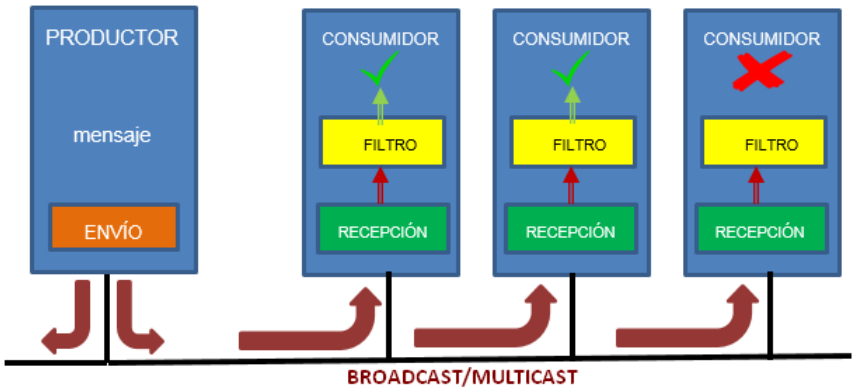

Ilustración 10. Modelo mensajes CIP productor/consumidor en comunicación implícita multicast

3.3.3.2. Seguridad

Ethernet/IP es susceptible de verse afectado por todas las vulnerabilidades de Ethernet, como puede ser la suplantación de identidad o la captura de tráfico. Además como utiliza UDP para sus mensajes implícitos y este carece de control de la transmisión, es posible la inyección de tráfico malicioso y la manipulación de la ruta de transmisión mediante el uso de IGMP.

3.3.3.3. Recomendaciones de seguridad

Al ser Ethernet/IP, un protocolo basado en Ethernet que utiliza UDP e IGMP, es necesario proporcionar al perímetro de la red Ethernet/IP de todos los mecanismos de seguridad basados en Ethernet e IP. También se recomienda la monitorización pasiva de la red a fin de asegurar que el tráfico Ethernet/IP sólo se utiliza en equipos explícitamente identificados y no proviene del exterior de la red.

3.3.4. Seguridad CIP

A pesar de que CIP utiliza un modelo de objetos bien definido, no define ningún mecanismo ni implícito ni explícito de seguridad. Además dispone de Objetos Obligatorios para la identificación de los dispositivos, lo que puede facilitar el descubrimiento de los equipos de la red, proporcionando objetivos a los atacantes. Como también dispone de Objetos de Aplicación comunes para el intercambio de información entre dispositivos, un intruso es capaz

de manipular gran variedad de dispositivos industriales manipulando y enviando ese tipo de objetos. Las características de algunos mensajes de CIP (tiempo real, mensajes multicast…) son además incompatibles con el cifrado de las comunicaciones, por lo que CIP no incorpora mecanismos que lo permitan.

3.4. MODBUS

3.4.1. Descripción

Modbus es uno de los protocolos de control industrial más veteranos. Fue introducido en 1979 utilizando comunicaciones serie para interaccionar con PLCs. En la década de los 90 tuvo un gran crecimiento y con objeto de lograr una mayor integración con sistemas modernos aparece en 1999 la versión para redes TCP/IP, Modbus/TCP. Este paso consolidó a Modbus como uno de los protocolos más utilizados en control industrial. Hoy en día es ampliamente utilizado en un amplio espectro de industrias, incluyendo infraestructuras críticas. Modbus es un protocolo de comunicaciones industriales que se sitúa en la capa de aplicación, permitiendo por ello utilizar diferentes soportes físicos para el transporte. Proporciona comunicación en modo cliente/servidor entre diferentes equipos conectados a través de diferentes tecnologías de capas inferiores entre las que se incluye, pero no se limita, la capa de protocolos de TCP/IP.

Se podría decir entonces que existen dos tipos de implementaciones de Modbus:

- Modbus serie: Como tecnología de transmisión utiliza el estándar HDLC[11], si se implementa Modbus, o RS232 (o RS485) si se implementa en modo maestro esclavo.
- Modbus/TCP: utiliza la pila de protocolos TCP/IP para transmitir la información.

Puesto que el protocolo Modbus es común para todas las implementaciones, las medidas de seguridad que se implementen en capa 7 serán independientes de las que se aseguren en capas inferiores.

3.4.2. Seguridad

Las implementaciones de Modbus serie, utilizan tanto RS232 y RS485, que son protocolos de comunicación de capa física. Estos protocolos, por definición, se encargan de transmitir bits de una estación a otra y definen las condiciones en las que un bit se entiende como un bit. No tiene sentido hablar de seguridad en esta capa, pues son funcionalidades que se desarrollan en capas superiores. Por encima del acceso físico al medio, se ubicarían los protocolos de nivel de enlace, HDLC y Ethernet según la implementación (serie o TCP respectivamente). Modbus no implementa ninguna característica de seguridad en este nivel.

Respecto a la seguridad ofrecida por la capa de aplicación Modbus fue diseñado para su uso en entornos muy controlados y no incluye ningún mecanismo de seguridad en esta capa.

[11] http://es.wikipedia.org/wiki/High-Level_Data_Link_Control

Carece por tanto de autenticación, siendo únicamente necesario para la sesión de Modbus una dirección y un código de función que sean válidos, información fácilmente conseguible a través de internet y un *sniffer* de red. Tampoco permite cifrado de la información. Estas funcionalidades no fueron añadidas con la posibilidad de usar la pila TCP/IP como protocolos de capas inferiores. Es posible aplicar medidas genéricas de la pila TCP/IP (IDS, cortafuegos…), pero únicamente a las implementaciones basadas en Ethernet y en ningún caso a aquellas basadas en Bus Serie.

Además, en las implementaciones serie los comandos se emiten mediante broadcast, lo que hace que todos los elementos conectados puedan ser afectados por un único ataque de Denegación de Servicio.

Todas estas carencias se ven magnificadas por el hecho de que Modbus sea un protocolo diseñado para la programación de los elementos de control como RTU o PLC, por lo que es posible la inyección de código malicioso a esos elementos.

3.4.3. Recomendaciones de seguridad

Debido a los problemas de seguridad anteriormente mencionados, la comunicación entre dispositivos utilizando Modbus debería estar controlada. En ese sentido, el despliegue de un analizador de tráfico que controle que únicamente permita el tráfico Modbus de determinados dispositivos y únicamente aquellas funciones permitidas podría ayudar a mitigar los problemas de comunicación si se utiliza este protocolo.

Además también se deberían de comprobar aquellos paquetes Modbus TCP con datos erróneos en su tamaño o el tráfico en el puerto TCP 502 con paquetes malformados. Como medida adicional aquellas funciones que fuercen a los esclavos a ponerse en modo «sólo escucha», las funciones que fuercen un reinicio de las comunicaciones, aquellas que borren o reseteen información diagnóstica como contadores o tráfico desde un servidor a múltiples esclavos deberían ser también monitorizados de forma activa para hacer la red más segura.

Existen soluciones genéricas IDS como Snort o especializadas en Modbus como el IPS Tofino TCP Enforcer LSM altamente recomendables para reforzar la seguridad de este protocolo.

3.5. DNP3

3.5.1. Descripción

DNP3 es un protocolo de comunicaciones desarrollado en 1993 y que se implementa ampliamente en el sector eléctrico principalmente en USA y Canadá. Su presencia en Europa es escasa por la presencia de alternativas como IEC-60870-5-101 o IEC-60870-5-104. Es un

protocolo de tres capas que actúa en las capas de nivel de enlace, de nivel de aplicación y de nivel de transporte[12].

3.5.2. Seguridad

DNP3 es un protocolo diseñado para maximizar la disponibilidad del sistema, dejando más descuidados los factores de confidencialidad e integridad de los datos.

A nivel de capa de enlace se incluyen las funciones típicas de esta capa, como la detección de errores de transmisión mediante el cálculo de CRC (lo que no es una medida de seguridad, ya que cualquiera que quiera modificar las tramas será capaz de modificar el CRC), pero no incluye ninguna medida de seguridad adicional que no ofrezca el protocolo Ethernet.

A nivel de aplicación se está haciendo un esfuerzo para proporcionar un estándar de autenticación segura en DNP3 [4], promovido por la Asociación de usuarios de DNP3. Esta autenticación se realiza a nivel de aplicación para garantizar las comunicaciones extremo a extremo, al ser DNP3 un protocolo que puede ser utilizado sobre diferentes tecnologías de capa 1 y 2.

Con el estándar de autenticación segura se resuelven los problemas de:

- Suplantación de identidad con usos generalmente maliciosos
- Modificación de mensajes de forma que se pueda alterar el funcionamiento del sistema
- Ataques de reinyección de tráfico consistentes en la transmisión maliciosa o fraudulenta de datos válidos
- *Eavesdropping* o escucha fraudulenta de la información que circula por la red, aunque únicamente para el intercambio de claves criptográficas y no para el resto de los datos que circulen por la red.

El estándar tiene un modelo de operación que se basa en Desafío-Respuesta, de forma que cuando se solicita una función que requiere de autenticación, no se procesa la petición a no ser que se resuelva un desafío de autenticación. Esta forma de comunicación se muestra en la Ilustración 11.

[12] Más bien pseudo-transporte porque no se corresponde con la capa de transporte de OSI.

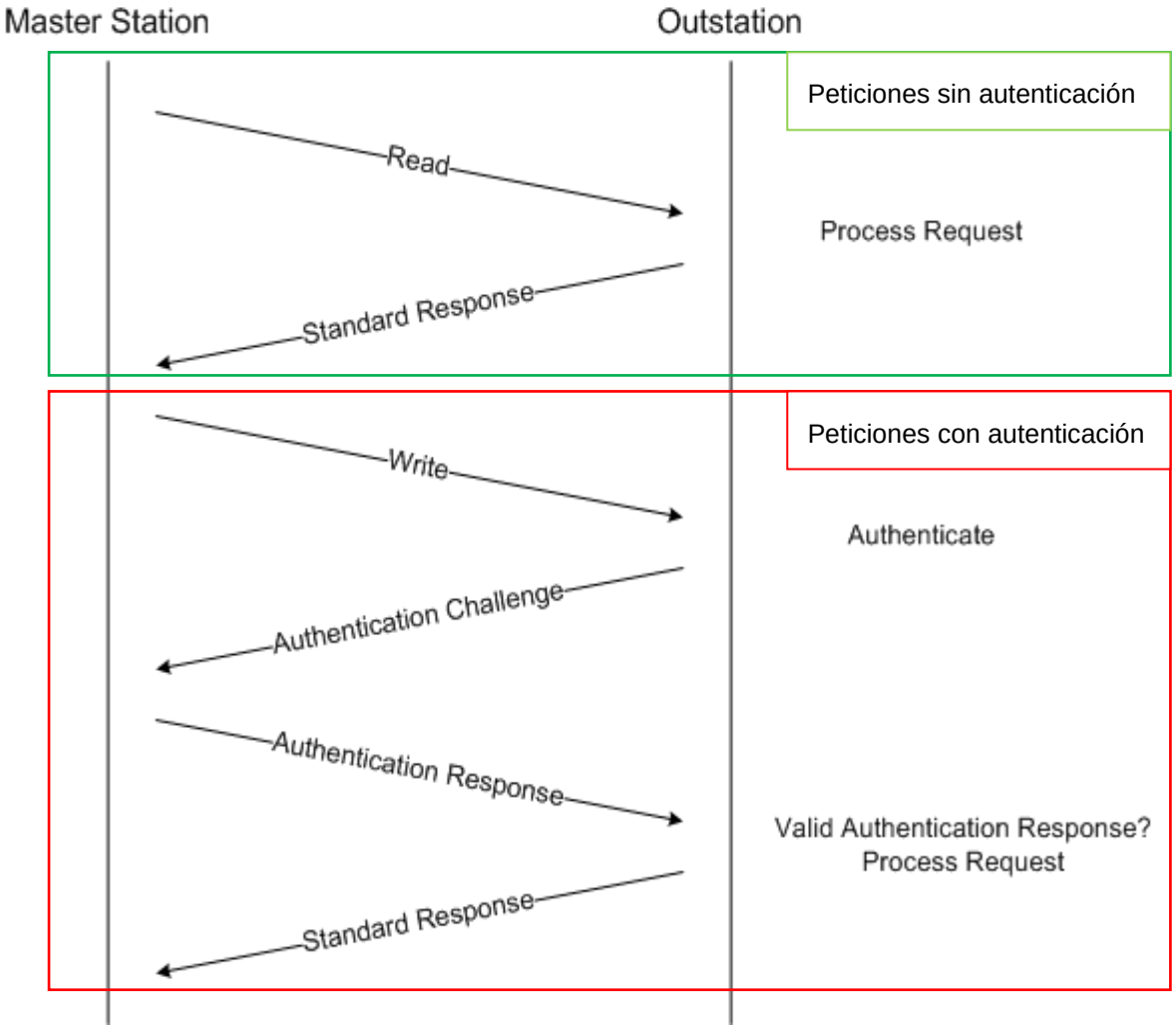

Ilustración 11: Diferentes tipos de peticiones DNP3.

Este modo de operación puede suponer retraso y sobrecarga de la red, por lo que se puede configurar la operación en modo «agresivo», con el cual la petición y la respuesta del desafío se envían de forma conjunta.

3.5.3. Recomendaciones de seguridad

Ya que DNP3 dispone de una implementación segura, la principal recomendación es desplegar únicamente DNP3 seguro. Puede ser que este despliegue no sea posible por diferentes factores como el soporte del fabricante, por lo que, en estos casos, se recomienda el uso de DNP3 encapsulado dentro de un protocolo de transporte seguro, como puede ser TLS. Actualmente hay fabricantes como PJM[13] que proponen este tipo de despliegues [5], como se puede ver en la Ilustración 12.

[13] http://www.pjm.com/

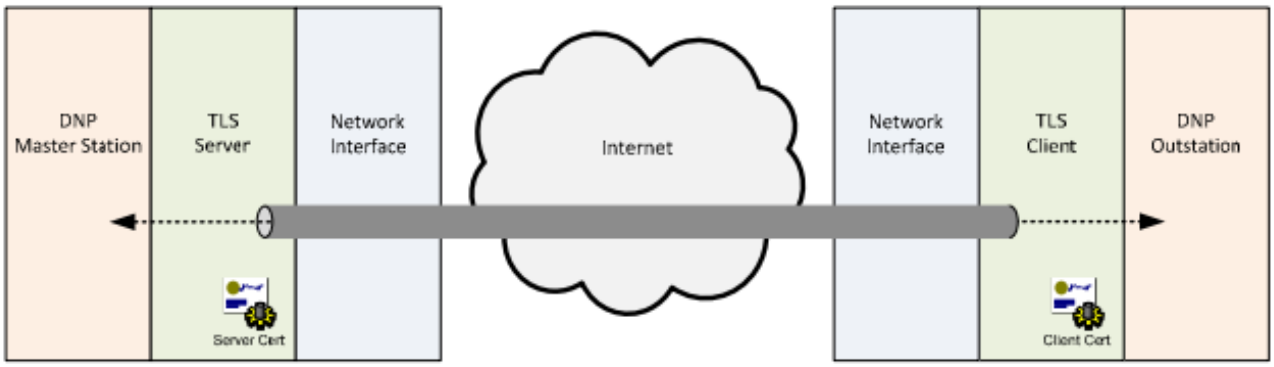

Ilustración 12: DNP3 encapsulado en TLS.

De forma adicional, es recomendable monitorizar cualquier comunicación no DNP3 en los puertos típicamente usados por DNP3 (TCP/UDP 20000), así como prestar especial atención a los códigos de función 4,5 y 6 (*Operate, Direct Operate* y *Direct Operate no ACK*), 18 (*Stop Application*), 21 (*Disable Unsolicited Messages*)[14].

3.6. PROFIBUS

3.6.1. Descripción

Profibus (del inglés PROcess FIeld BUS) es un estándar de comunicación a través de Fieldbus promovido en 1989 por el departamento alemán de educación e investigación y utilizado por Siemens. Se basa en comunicaciones serie con soporte sobre cable (RS-485, MBP) o sobre fibra óptica.

Actualmente tiene dos variantes, reflejadas en la Ilustración 13: **Profibus DP** (periféricos descentralizados) que se utiliza para la operación de sensores y actuadores a través de un controlador centralizado y **Profibus PA** (Automatización de Procesos) utilizado para la monitorización de equipos de medida a través de un sistema de control del proceso.

[14] La lista completa de las funciones de aplicación de DNP3 se puede consultar en [7]. Nótese que en la referencia la notación es hexadecimal mientras que en el texto se utiliza notación decimal.

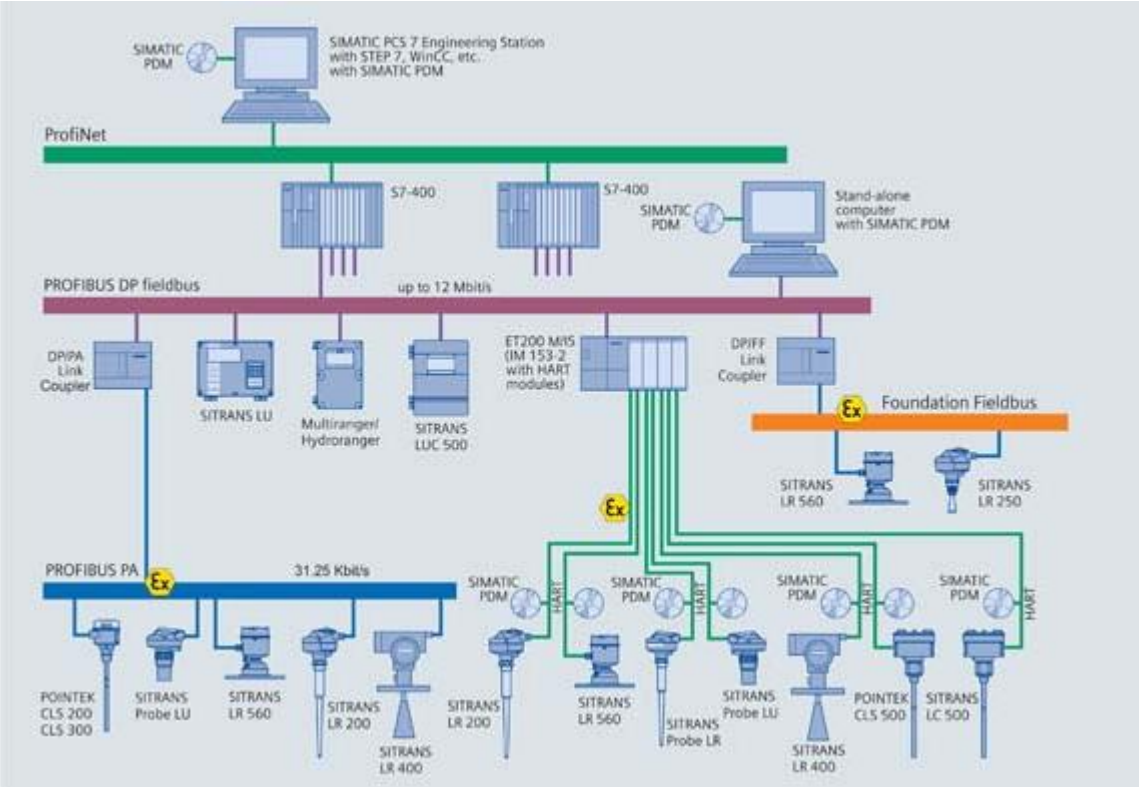

Ilustración 13: Arquitectura Profibus

3.6.2. Seguridad

Profibus es un protocolo que opera en las capas de aplicación, enlace y física. La capa de enlace de este protocolo utiliza FDL (Field bus Data Link) como mecanismo de gestión de acceso al medio. Funciona con un método de acceso híbrido que combina las tecnologías de maestro-esclavo con el paso de un testigo que es el que marca quien puede iniciar la comunicación y ocupar el bus. Estas medidas permiten que los dispositivos no se comuniquen a la vez, pero no constituyen ningún mecanismo de seguridad y podrían ser susceptibles a ataques de inyección de tráfico o denegación de servicio.

En capa de aplicación, existen tres niveles de utilización DP-V0, para intercambios de datos periódicos, DP-V1 para comunicaciones no periódicas y DP-V2 para comunicaciones asíncronas a través de mensajes de *broadcast*. De la documentación examinada no es posible inferir que Profibus añada ninguna capa de seguridad a las comunicaciones en esta capa.

Hay parte de los servicios ofrecidos por Profibus que pueden utilizar TCP/IP como protocolo de transporte, pero únicamente durante una fase inicial de asignación de dispositivos. En estos servicios sería posible añadir elementos de seguridad IT, siempre y cuando no perjudiquen la operativa del sistema.

3.6.3. Recomendaciones de seguridad

Al igual que con otros protocolos de la familia Fieldbus, la ausencia de autenticación y la falta de seguridad del protocolo exigen el aislamiento del bus del resto de componentes de la red. La seguridad perimetral debería ser muy severa para evitar cualquier tráfico no autorizado o sospechoso.

3.7. PROFINET

3.7.1. Descripción

Profinet es un estándar basado en Profibus que adopta como interfaz físico de conexión Ethernet en lugar de RS485, y un sistema de bis basado en pase de *token*. Ofrece para la transmisión de datos la funcionalidad completa de TCP/IP, lo que le proporciona aplicaciones inalámbricas y alta velocidad de transferencia. Los equipos que utilizan Profinet están orientados a la fiabilidad y a la comunicación en tiempo real, junto con la usabilidad. En la Ilustración 14 es posible ver la arquitectura de Profinet.

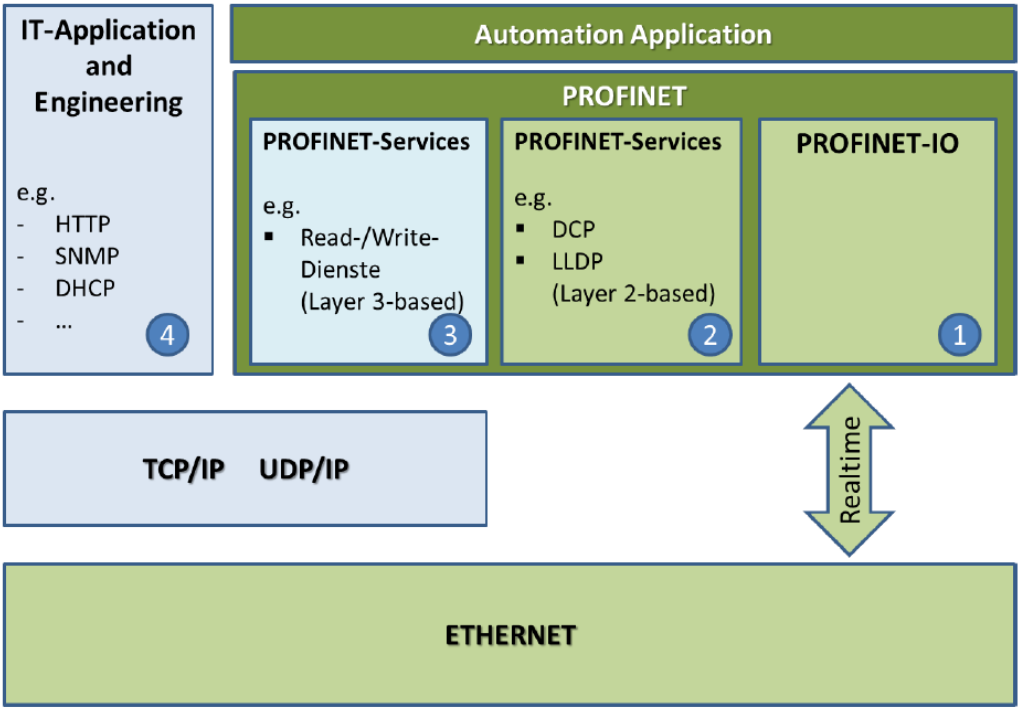

Ilustración 14: Arquitectura Profinet

3.7.2. Seguridad

Los equipos Profinet carecen de funciones de seguridad nativas, entendiéndolo como seguridad del punto final, por lo que la prevención de ataques a equipos Profinet es clave. Las medidas incorporadas por el protocolo se centran en mejorar la disponibilidad del sistema y la

fiabilidad operacional, así como la robustez de los equipos ante altos volúmenes de tráfico puntuales. En el documento «*PROFINET Security Guideline*» [6] se realizan recomendaciones para prevenir los posibles ataques a estos sistemas, donde se incluyen recomendaciones tradicionales del mundo IT, como la segmentación de las redes mediante VLAN o el establecimiento de DMZ, como se puede ver en la Ilustración 15siguie.

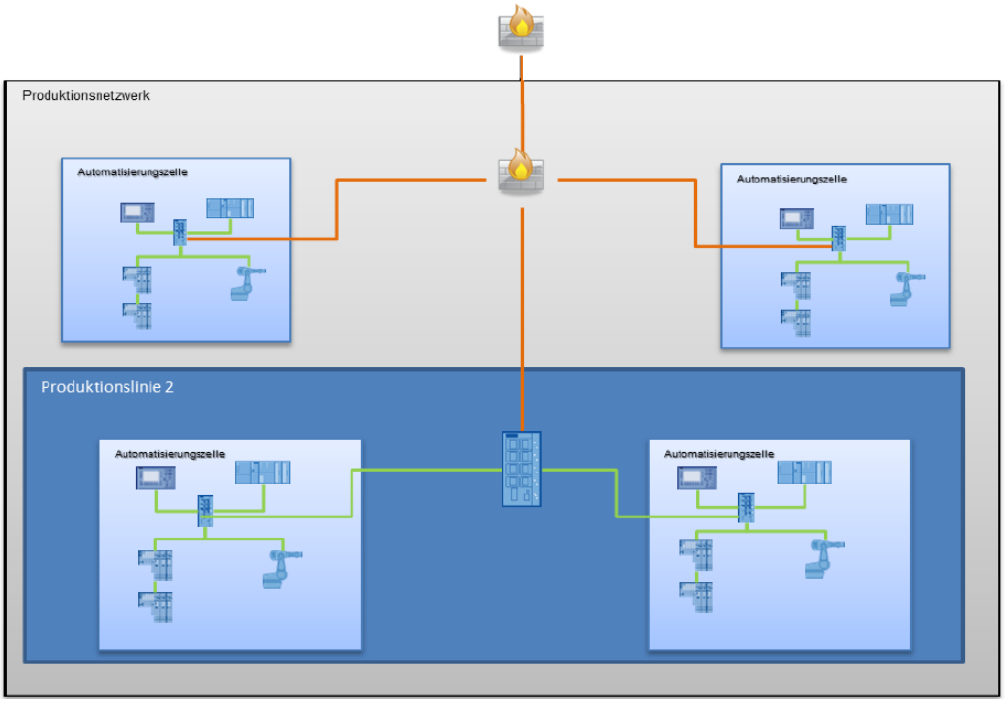

Ilustración 15: Una de las arquitecturas propuestas para ProfiNet.

3.7.3. Recomendaciones de seguridad

Al igual que con otros protocolos creados originalmente para comunicación a través de Fieldbus[15] la ausencia de autenticación y la falta de seguridad del protocolo exigen el aislamiento del resto de la red. Adicionalmente, el uso de métodos IT para autenticar los componentes de la red, junto con el cifrado de las comunicaciones de la misma es una buena práctica. Por último, la seguridad perimetral debería ser muy estricta para evitar cualquier tráfico no autorizado o sospechoso.

[15] Recordemos que Profinet es una adaptación de Profibus al protocolo Ethernet, por lo que la capa de aplicación se pensó originalmente para Fieldbus.

3.8. POWERLINK ETHERNET

3.8.1. Descripción

Powerlink sobre Ethernet [7] es un perfil de comunicación para Ethernet en Tiempo Real. Extiende Ethernet de acuerdo al estándar IEEE 802.3 con mecanismos para transmitir información con sincronización precisa e intervalos predecibles, con una arquitectura que se puede ver en la Ilustración 16. La especificación del protocolo [8] se puede descargar desde la página web del Grupo de Estandarización de Powerlink Ethernet[16].

Porwerlink proporciona mecanismos para conseguir:

1. Transmisión de aquella información para la que el tiempo es crítico en ciclos asíncronos. El intercambio de información se basa en el método de publicar/suscripción.
2. Sincronización de los nodos de la red con gran precisión
3. Transmitir la información para la que el tiempo no es tan crítico bajo demanda. La comunicación asíncrona puede utilizar protocolos de la pila TCP/IP o de capas superiores como HTTP, FTP…

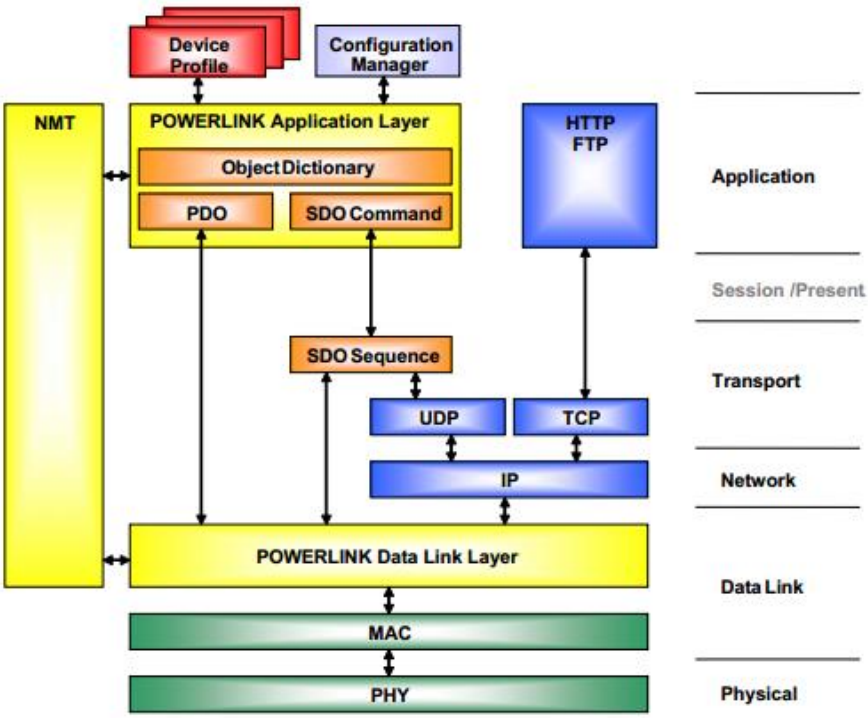

Ilustración 16: Modelo de referencia de Powerlink Ethernet.

[16] http://www.ethernet-powerlink.org/

Se maneja el tráfico de la red de forma que se dedican intervalos de tiempo para las transmisiones síncronas y las asíncronas, a la vez que se asegura que sólo los equipos de la red acceden al medio de transmisión. De esta forma se asegura que la información transmitida de forma asíncrona no interfiere con la síncrona y se mantienen los intervalos de comunicación. Este mecanismo, llamado *Slot Communication Network Management (SCNM)* es controlado por un equipo de la red, el Nodo Gestor (MN). El resto de nodos recibe el nombre de Nodos Controlados (CN). Los CN sólo pueden utilizar intervalos de transmisión asignados por el MN. Todos los nodos de la red se deben configurar en el MN y sólo se permite un MN dentro de la red. Además únicamente el MN puede mandar mensajes de forma independiente, mientras que los CN únicamente envían mensajes cuando el MN se los pide. Los CN envían la información solicitada por el MN en forma de *broadcast*, por lo que puede ser escuchada en toda la red. La siguiente ilustración muestra este proceso.

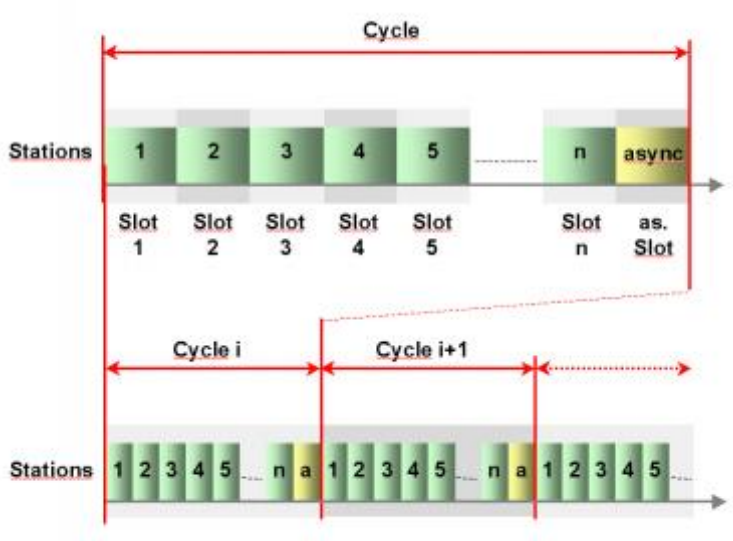

Ilustración 17: SCNM de Ethernet Powerlink

3.8.2. Seguridad

Como en otros casos de protocolos industriales se carece de mecanismos para comprobar la autenticidad del nodo o del mensaje. Si bien es cierto que un nodo sólo puede transmitir cuando el MN se lo solicita y le asigna un periodo de tiempo, no existe ningún mecanismo para comprobar que la información recibida proviene del nodo, por lo que es razonablemente sencillo alterar el tráfico de la red falsificando nodos legítimos o provocar DoS simplemente inundando la red de mensajes.

El uso de *broadcast* para las transmisiones también permite que un intruso obtenga toda la información que emiten los CN, no teniendo tampoco ningún tipo de cifrado que evite esta circunstancia.

3.8.3. Recomendaciones de seguridad

La sensibilidad al retraso del SCNM requiere que Powerlink Ethernet se despliegue aislado de cualquier otra red basada en Ethernet. La seguridad perimetral debe ser por tanto muy estricta para mantener aislado este protocolo del resto de la red y prevenir tráfico malicioso.

3.9. OPC

3.9.1. Descripción

OPC (OLE para control de procesos) no es un protocolo de comunicación industrial, sino más bien un marco operacional de comunicaciones de los sistemas de control de procesos basados en Windows que utilizan objetos enlazados y embebidos (OLE), que a su vez utilizan protocolos de comunicación como RPC. OPC es, por tanto, un conjunto de protocolos de conjuntamente permiten a los sistemas de control de procesos comunicarse utilizando algunas de las capacidades de comunicación de Windows.

OPC conecta sistemas Windows, normalmente a través de TCP/IP. Originalmente, OPC se basaba en DCOM y muchos sistemas OPC todavía utilizan DCOM, a pesar de que existe una actualización llamada OPC-*Unified Architecture* (OPC-UA), que permite la utilización de SOAP sobre HTTPS, mucho más segura.

3.9.2. Seguridad

El uso de DCOM y RCP hacen de OPC muy susceptible a ataques y además puede verse afectado por todas las vulnerabilidades utilizadas en OLE. Además OPC se ejecuta en sistemas Windows únicamente, por lo que también puede verse afectado por todas las vulnerabilidades que afectan a ese Sistema Operativo.

Debido a la dificultar inherente de aplicar parches en sistemas de control industrial, muchas de las vulnerabilidades ya descubiertas y para las que hay parches siguen siendo explotables en las redes de control industrial. OPC-UA si dispone de un modelo de seguridad, del que se puede encontrar un libro blanco [9], que aporta seguridad a la arquitectura, por lo que es recomendable el despliegue de OPC-UA en lugar de OPC clásico.

3.9.3. Recomendaciones de seguridad

En la medida de lo posible se debería desplegar OPC-UA. Además de esta recomendación, los servidores OPC deben ser convenientemente bastionados, cerrando todos los puertos y servicios innecesarios.

Adicionalmente se deben monitorizar aquellos puertos y servicios no OPC iniciados por el servidor OPC, así como la aparición de vulnerabilidades que afecten a Windows, OPC, OLE RPC o DCOM. Los servicios OPC que se inicien de servidores OPC desconocidos junto a fallos de autenticación en los servidores OPC también deben ser activamente monitorizados para mejorar la seguridad de los despliegues utilizando OPC.

3.10. ETHERCAT

3.10.1. Descripción

EtherCAT (*Ethernet for Control Automation Technology*) es un protocolo de comunicaciones de código abierto utilizado para incorporar Ethernet a los entornos industriales. Este protocolo se estandarizó en el IEC 61158[17], dentro de la estandarización de FieldBus. EtherCAT se utiliza en aplicaciones de automatización con ciclos de actualización pequeños (≤ 100µs) y con jitter[18] ≤ 1µs. Es, por tanto, el sistema más rápido disponible actualmente.

Con este sistema el paquete Ethernet no se recibe, interpreta y envía (como se hace tradicionalmente con el almacenamiento y reenvío) sino que se procesa sobre la marcha en cada nodo esclavo (actualizando la información correspondiente) mientras que se envía al siguiente dispositivo, obteniéndose un retraso de unos pocos nanosegundos. La trama de EtherCAT se muestra en la Ilustración 18.

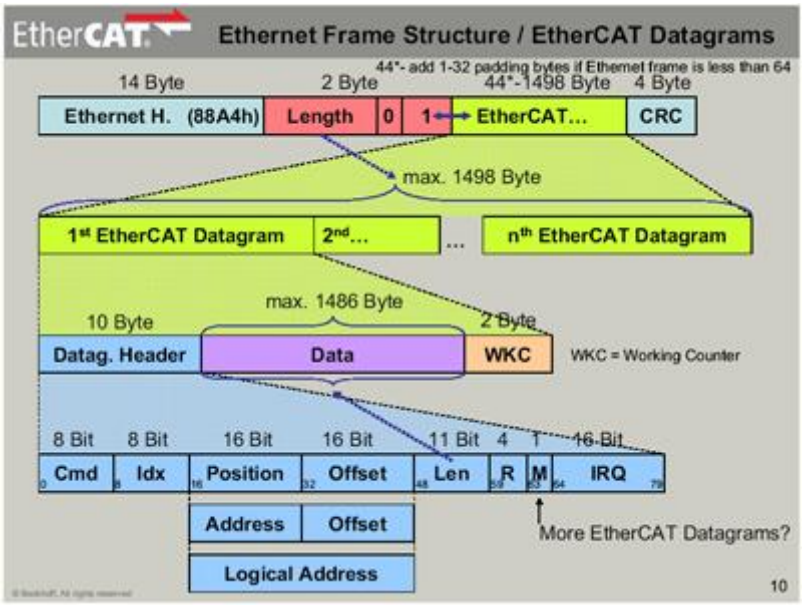

Ilustración 18: Estructura de tramas de EtherCAT.

3.10.2. Seguridad

Al ser EtherCAT un protocolo derivado de Ethernet, es susceptible a cualquiera de las vulnerabilidades de Ethernet, y por tanto vulnerable a cualquier ataque de Denegación de Servicio. El servicio de EtherCAT se puede alterar fácilmente mediante la inserción de

[17] http://es.wikipedia.org/wiki/Bus_de_campo
[18] http://es.wikipedia.org/wiki/Jitter

paquetes Ethernet a la red de forma que interfieran con la sincronización y es vulnerable a falsificaciones y MITM debido a la falta de autenticación, por lo que es recomendable separar la red EtherCAT del resto de sistemas Ethernet.

3.10.3. Recomendaciones de seguridad

Como ya se ha comentado, EtherCAT debe desplegarse aislado del resto de redes Ethernet. También es recomendable realizar una monitorización pasiva de la red a fin de asegurar la integridad de la misma, comprobando que el tráfico EtherCAT se origina únicamente de aquellos dispositivos explícitamente autorizados

ANEXO I: CUADRO COMPARATIVO DE PROTOCOLOS SCI

Protocolo		Características	Seguridad		Capas implementadas por el protocolo				Recomendaciones de seguridad
	Variante		Cifrado	Autenticación	Acceso al medio	IP	Transporte	Aplicación	
Common Industrial Protocol (CIP)	DeviceNET	Adaptación CIP con CAN	No	No	X	X	X	X	CIP cuenta con la tecnología a nivel de aplicación CIP SafetyTM. Complementar con medidas generales de segmentación y aislamiento de las redes de control
	ControlNET	Adaptación CIP con CTDMA	No	No	X	X	X	X	
	CompoNET	Adaptación CIP con TDMA	No	No	X	X	X	X	
	Ethernet/IP	Adaptación CIP con TCP/IP	No	No				X	
Modbus	Serie	Estándar abierto Usado ampliamente en la industria	No	No	X			X	Adoptar, si es posible, cifrado (SSL,VPN) o medidas de inspección de tráfico como IDS (Snort), IPS (Tofino), etc.
	TCP		No	No				X	
DNP3		Sector Eléctrico Escasa presencia en Europa	No	Si (DNP3 secure)		X	X	X	Implementar DNP3 Secure
ProfiBus		Estándar abierto Variantes Profibus DP y Profibus PA	No	No	X	X		X	Segmentar la red, cifrar la información y realizar inspección de tráfico
ProfiNET		Evolución de Profibus para Ethernet	No	No				X	Seguir la "Profinet Security Guide"
Powerlink Ethernet		Estándar abierto	No	No				X	Segmentar la red y aplicar medidas de seguridad habituales en la parte Ethernet
OPC		Marco operación de comunicaciones Originalmente basado en Windows	No	Si (OPC UA)				X	Implementar OPC UA
EtherCAT		Estándar abierto Para ciclos de actualización muy cortos	No	No				X	Segmentar la red y aplicar seguridad perimetral

ANEXO II: RECOMENDACIONES GENÉRICAS DE SEGURIDAD

I. RECOMENDACIONES GENÉRICAS PARA CORTAFUEGOS.

Complementando las recomendaciones propuestas para la arquitectura de red que se describen en el apartado 2.2, las siguientes reglas de carácter general pueden aplicarse:

- El conjunto de reglas de base debe ser denegar todo e ir permitiendo comunicaciones o servicios según necesidades (listas blancas).
- Los puertos y servicios entre el entorno de red de control y la red de la corporativa deben ser habilitados y permitidos de manera específica, según las necesidades de cada caso. Debe haber una justificación documentada con el análisis de riesgos y una persona responsable de cada flujo de datos entrante o saliente permitido.
- Todas las reglas de «acceso permitido» deben fijarse con una dirección IP y puerto TCP/UDP específico con control de estado.
- Todas las reglas deben definirse para restringir el tráfico solo a una dirección IP específica o a un rango de direcciones.
- Denegar tráfico directamente desde la red de control a la red corporativa. Todo el tráfico de control debe terminar en la zona DMZ.
- Todo protocolo permitido entre la red de control y DMZ **no** debe permitirse explícitamente entre la DMZ y las redes corporativas (y viceversa).
- Todo el tráfico saliente de la red de control de la red corporativa debe estar estrictamente restringido por fuente y destino así como el servicio y el puerto.
- Los paquetes salientes desde la red de control o DMZ **solo** deben ser autorizados si los paquetes tienen una dirección IP de origen correcta asignada a la red de control o dispositivos de la red DMZ.
- NO se debe permitir el acceso a Internet dispositivos de la red de control.
- Las redes de control **no** deben conectarse directamente a Internet, aunque estén protegidas por un firewall.
- Todo el tráfico de administración de firewall debe realizarse en cualquiera de una red separada, asegurado gestión (por ejemplo, fuera de banda) o en una red cifrada con autenticación de múltiples factores. El tráfico también debe ser restringido por dirección IP a las estaciones de gestión específicos.
- Todas las políticas de firewall deben probarse periódicamente.
- Todos los cortafuegos deben ser respaldados inmediatamente antes de la puesta en marcha.

II. RECOMENDACIONES GENÈRICAS SOBRE SERVICIOS

Como añadido a las reglas generales descritas en el apartado anterior, se proponen las siguientes reglas de cortafuegos genéricas según el servicio o protocolo:

SERVICIO	RECOMENDACIÓN
DNS	Hacer un uso de un servidor DNS local interno restringido para la red de control. En casos de elementos limitados puede hacerse uso de ficheros locales de hosts.
HTTP	El protocolo utilizado para acceso web con navegadores es muy útil y cómodo. No obstante si no se usa HTTPS cuyas transmisiones son cifradas debe ser denegado desde la red corporativa o pública a la red de control. Adicionalmente: ▪ Hacer uso de listas blancas (filtrado IP) para los accesos web a servicios en la red de control o física. ▪ Control de acceso tanto a orígenes como destinos ▪ Implementación de autorización a nivel aplicación ▪ Restringir el número de tecnologías soportadas para disminuir la superficie de vulnerabilidades ▪ Registrar y monitorizar tanto el uso como los intentos o accesos al servicio
FTP Y TFTP	Estos dos protocolos de transmisión de ficheros son de uso común en sistemas SCI. Sin embargo la ausencia de cifrado los hace vulnerables a robo de credenciales e información. Debe evitarse en la medida de lo posible y sustituir de versiones cifradas como SCP o SFTP. En caso estrictamente necesario utilizar únicamente bajo un túnel cifrado o restringir su uso a transmisiones no críticas.
TELNET	Este protocolo de acceso y comunicación no cuenta con cifrado lo que desaconseja su uso. En caso de necesidad utilizar una red privada o VPN para proteger la transmisión.
DHCP	Este protocolo diseñado para la configuración automática de red de dispositivos es de gran utilidad pero entraña riesgos de seguridad al poderse utilizar para ataques MITM e interceptar tráfico. En la medida de lo posible evitar su utilización o, en caso necesario implementar reglas de inspección de tráfico para evitar falsos servidores DHCP (*rogue servers*) así como medidas anti *spoofing* de ARP e IP.

SSH	Una correcta utilización de SSH debe considerarse como una medida eficaz para establecer comunicación segura entre segmentos o elementos de red con tráfico sensible. Debe permitirse y sustituir a FTP, TELNET, RCP y otros protocolos inseguros.
SOAP	SOAP (Simple Object Acess Protocol) utiliza una sintaxis XML para intercambiar mensajes. Es un mecanismo sin control de estado y por ello bastante vulnerable a falsificación e interceptación. En este sentido reglas de inspección de tráfico a nivel de aplicación son aconsejables para controlar el contenido de los mensajes.
SMTP	Este protocolo utilizado en el correo electrónico debe ser denegado en la red de control. Tráfico SMTP saliente desde la red de control a la corporativa puede permitirse para envió de alertas por correo electrónico.
SNMP	SNMP es el protocolo utilizado para el control y monitorización entre elementos de red siendo de gran utilidad. No obstante en sus versiones 1 y 2 hace uso de comunicaciones no cifradas y contraseñas genéricas. SNMP versión 3 ya soluciona estos problemas pero no siempre es compatible con todos los dispositivos. En caso de contar con el uso de las versiones anteriores a v3 se recomienda separar el tráfico SNMP en una red de gestión.
DCOM	DCOM, del inglés Distributed Component Object Model es el protocolo sobre el que se apoya OPC (OLE for Process Control. Hace uso de RPC (Remote Procedure Call) servicio que debe ser convenientemente parcheado por contar con múltiples vulnerabilidades. Además OPC a través de DCOM, hace uso de puertos dinámicos (desde 1024-65535) lo que incrementa la dificultad de establecer una regla concreta de firewall. El tráfico de este protocolo debe permitirse únicamente entre las redes de control y DMZ. Adicionalmente se recomienda aplicar configuraciones de DCOM en los dispositivos para reducir el rango de puertos dinámicos disponibles.

REFERENCIAS

[1] ISA-95. [En línea]. Available: https://www.isa.org/standards-and-publication.

[2] D. G. Maryna Krotofil, Industrial Control Systems Security: What is happening?.

[3] Homeland Security US, «Improving Industrial Control with Defense in Depth Strategies,» 2009.

[4] IEEE, IEEE Standard for Electric Power Systems Communications -- Distributed Network Protocol (DNP3), 2010.

[5] PJM, Jetstream Guide DNP SCADA over Internet with TLS Security, 2013.

[6] P. -. Profinet, Profinet Security Guideline. Guideline for PROFINET, 2013.

[7] DNP3 Quick Reference Guide, 2002.

[8] E. P. S. Group, Ethernet POWERLINK Communication Profile Specification, 2008.

[9] P. H. Randy Amstrong, The OPC UA Security Model For Administrators, 2010.

[10] Rockwell Automation, «REFERENCE ARCHITECTURES FOR MANUFACTURING,» 2011.

[11] E. D. Knapp, Industrial Network Security, 2011.

[12] L. A. a. C. M. P. Hollman, Compromising Industrial Facilities from 40 Miles Away, 2013.

[13] U. o. L. Dept. of Computer Engineering and Computer Science, Security Considerations in SCADA Communication Protocols, 2004.

[14] S. C. C. Agency, Guide to Increased Security in Industrial Control Systems, 2010.

[15] ISA, ISA-99 Industrial Automation and Control Systems Security.