eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea

BILBOKO
INGENIARITZA ESKOLA

ESCUELA
DE INGENIERÍA DE BILBAO

TRABAJO DE FIN DE GRADO

Grado en Ingeniería en Tecnología de Telecomunicación

LA CIBERSEGURIDAD COMO NORMA

ESTUDIO DEL ESTADO DEL ARTE EN ESTÁNDARES Y CERTIFICACIÓN EN MATERIA DE SEGURIDAD CIBERNÉTICA APLICADA A INDUSTRIA 4.0 E IOT

Estudiante *Zabalo Arteche Eñaut*
Fecha *10, 2018*
Director/a *Pérez Gonzalez Federico*
Curso académico *2018-2019*

- *Estudiante:* Zabalo Arteche Eñaut.
- *Director/a:* Pérez Gonzalez Federico
- *Departamento*: Ingeniería de Sistemas y Automática.
- *Título del Trabajo:* La Ciberseguridad Como Norma. Estudio del Estado del Arte en Estándares y Certificación en Materia de Ciberseguridad Aplicada a Industria 4.0 e IoT.
- *Resumen*: En este Trabajo Fin de Grado se realiza, mediante una revisión sistemática de la literatura científica disponible actualmente, el estado del arte de los actuales estándares en ciberseguridad relacionados con la iniciativa de industria 4.0, así como de las tecnologías denominadas IoT (Internet of Things) y su posible aplicación en marcos de certificación.
- *Palabras clave*: Ciberseguridad, Industria 4.0, IoT, estándar, certificación.

- *Izenburua:* Zibersegurtasuna Arau. Zibersegurtasuneko Esparruaren Estandar eta Zertifikazioen Artearen Egoeraren Behaketa Industria 4.0 eta IoT-ri Aplikaturik.
- *Laburpena:* Gradu Amaierako Lan honetan, gaur egunean eskuragarri dagoen literatura zientofikioaren behaketa sistematikoa gauzatuz, zibersegurtasunaren esparruko estándarren artearen egoera aztertzen da, betiere Industria 4.0 eta IoT teknologiak irizpide harturik. Estandar hauek zertifikazio berriak sortzeko orduan izan dezaketen garrantzia aztertuz.
- *Hitzgakoak*: Zibersegurtasuna, Industria 4.0, IoT, estandar, zertifikazioa.

- *Title*: Cybersecurity as a Norm. State of the Art Study on Cybersecurity Standards and Certification Schemes Applied to Industry 4.0 and IoT.
- *Abstract*: In this paper, through a systematic analysis of the currently available scientific literature, a state-of-the-art study on cybersecurity standards is performed focusing on Industry 4.0 and IoT technologies and the possible application of these standards in certification frameworks.
- *Keywords*: Cybersecurity, Industry 4.0, IoT, standard, certification

TABLA DE CONTENIDOS

1 INTRODUCCIÓN

La tendencia actual en el sector tecnológico es la de fomentar la conectividad. Uno de los sectores que está experimentando un mayor crecimiento en este aspecto es el Industrial. Tanto es así, que se considera que el sector está sufriendo una revolución.

Esta revolución, ha sido bautizada como Industria 4.0 y su principal cometido es el de llevar las tecnologías de acceso remoto relacionadas tradicionalmente con el mundo IT (Information Technology) al mundo de OT (Operational Technology). Sin embargo, esta mejora en la conectividad no está exenta de riesgos. De hecho, los riesgos derivados de dotar de conectividad a servicios y sistemas que hasta ahora operaban en modo local es un factor muy importante a tener en cuenta, especialmente para las comunicaciones Industriales.

Tradicionalmente, las redes de comunicaciones industriales se encontraban confinadas en las propias plantas de producción. Este hecho y la necesidad de que las comunicaciones fueran en tiempo real han relegado a un segundo plano el aspecto de la ciberseguridad.

No obstante, la situación actual ha obligado al sector a buscar soluciones de ciberseguridad que protejan sus redes de las amenazas externas sin comprometer las características de tiempo real que exigen las comunicaciones industriales.

Es por este motivo que se detecta la necesidad de realizar un documento que recopile los tipos de amenazas y posibles soluciones que afectan hoy día a las comunicaciones industriales, primando las soluciones estandarizadas.

2 Contexto

Desde que Internet se creara en 1968-1969 como tecnología militar y su posterior migración al sector civil, la cuantía de dispositivos conectados ha experimentado un crecimiento exponencial hasta encontrarse hoy en día en el orden de miles de millones. Esta tendencia y la cobertura cada vez más global de Internet han impulsado la aparición de los dispositivos y tecnologías denominadas IoT cuyo objetivo es dotar de conectividad a todo tipo de dispositivos y servicios.

Dentro de esta tendencia a la conectividad, surge la iniciativa de Industria 4.0, la cual se define como la nueva revolución industrial y que tiene como objetivo dotar de conectividad a un sector, como es el de la industria, que ha operado tradicionalmente de manera local.

Dicha conectividad, como la mayoría de las innovaciones tecnológicas, plantea numerosos beneficios que no están exentos de sus riesgos derivados. Una mayor conectividad implica mayor visibilidad y disponibilidad de los recursos por parte de la empresa. Esto crea un nuevo reto para la seguridad de los recursos, puesto que cada vez es mayor la cantidad de ataques que sufren las plataformas conectadas.

Es por esta necesidad de *securizar* los bienes conectados a Internet que surge la ciberseguridad, la cual tiene por objetivo dotar de una capa de protección a todo recurso conectado. Sin embargo, se presenta frecuentemente como una solución ad-hoc, lo que crea una diversidad de opciones en el mercado que dificulta la aplicación sistemática de la misma en los distintos sectores conectados. Del mismo modo, la ciberseguridad está destinada tradicionalmente al sector de IT, siendo incompatible o de difícil implementación en el sector industrial.

Como ya hemos mencionado, existe una diferencia considerable entre las redes industriales y las redes convencionales. Desde las distintas pilas de protocolos que las forman hasta las prioridades en mente a la hora de optimizar su funcionamiento. Esto dificulta enormemente la aplicación de las medidas de ciberseguridad más comunes en el sector IT al mundo Industrial.

3 Alcance del proyecto

El presente documento tiene como objetivo obtener una visión general del estado de la ciberseguridad en el entorno industrial. Para ello, se buscará toda la documentación relevante en materia normativa y se realizará el estudio de estándares de ciberseguridad relacionados con el entorno industrial; más concretamente, las nuevas tecnologías que se pretenden incorporar al mismo dentro de la iniciativa de industria 4.0.

Del mismo modo, se pretende analizar cualquier tipo de documento que mencione medidas de seguridad aplicables a la industria que pueda formar parte de un marco de normalización y certificación en el sector.

De este estudio se espera obtener un documento de referencia de estándares, guías de buenas prácticas y artículos de investigación que aporten información relevante a la seguridad cibernética en el entorno industrial. Se espera que este documento sirva como base para la consulta de la documentación necesaria para la creación de un marco de certificación para la industria y sus componentes.

4 Conceptos de Ciberseguridad

Para conocer mejor los factores de riesgo a los que están expuestos los dispositivos conectados y las medidas que se implementan como contrapartida, a continuación, se describen los vectores de ataque más comunes y las medidas de seguridad que se aplican a las comunicaciones para evitar o mitigar estos y otros ataques posibles.

4.1 Ciberataques más comunes

Por la naturaleza local de las redes industriales, las medidas de ciberseguridad siempre han quedado en segundo plano frente a otras necesidades como la velocidad de transmisión de datos o el asegurar un comportamiento determinista de las comunicaciones. Es por este motivo, que la apertura a Internet que supone la iniciativa de Industria 4.0 ha generado gran interés entre distintos grupos de atacantes.

Los ataques más comunes registrados en los últimos años son:

- **Ingeniería Social y Phishing**: puesto que estos ataques se dan de forma combinada la mayoría de las veces, se cubrirán en el mismo apartado. La ingeniería social consiste en utilizar la psicología y el conocimiento del comportamiento humano para obtener datos confidenciales de integrantes de la empresa (nombres de usuario, contraseñas, credenciales, etc.). Este método de ataque se utiliza en conjunto con la técnica llamada phishing, que consiste en falsificar e-mails, mensajes de texto u otros tipos de comunicación con el objeto de obtener los datos confidenciales arriba mencionados. Una vez obtenidos los datos necesarios de su objetivo, el atacante utilizará dicha información para acceder a la red corporativa o a otros objetivos haciéndose pasar por la persona cuyos datos ha obtenido. Este tipo de ataque se utiliza para ganar acceso a los distintos recursos de la empresa y, posteriormente, infectarla con distintos tipos de software malicioso.
- **Malware**: el malware es todo aquel software destinado a infectar sistemas informáticos o cualquier tipo de dispositivo electrónico dotado de un sistema operativo o firmware. Existen distintos tipos de malware, como son troyanos, rootkits, worms o gusanos… pero el fin de todos es el mismo: sortear los sistemas de seguridad de los que dispone el sistema informático objetivo (si es que dispone de alguna medida de seguridad) y establecerse dentro del sistema operativo o firmware sin ser detectado. Una vez un equipo ha sido infectado, el malware concede cierto tipo de control o acceso al atacante.
- **Ransomware**: es un tipo específico de ataque utilizando software del tipo malware arriba mencionado. Una vez infecta los equipos objetivo, encripta sus unidades de almacenamiento de modo que son inaccesibles para los usuarios. Una vez los equipos han sido infectados, los atacantes exigen una suma de dinero por “liberar” los equipos de dicha encriptación. Si bien es un tipo de malware y este apartado ya ha sido cubierto, dada la gran escala y frecuencia de los ataques de ransomware se ha considerado importante su mención específica.
- **Vulnerabilidades de software**: uno de los vectores de ataque más comunes en el mundo IT y que afecta especialmente al mundo OT por lo anticuado de los sistemas operativos utilizados en los equipos embebidos. Este ataque consiste

en explotar las vulnerabilidades de software conocidas de distintos sistemas operativos o firmwares de equipos. Las vulnerabilidades de software son consecuencia de errores de programación y pueden tener una gran variedad de usos maliciosos, desde ejecución de código hasta escalada de privilegios. Sin embargo, los programadores de los distintos softwares hacen frente a dichas vulnerabilidades actualizando o aplicando parches. Es por este motivo que el uso de software no continuado es un gran peligro, puesto que las posibles vulnerabilidades que poseía su última versión siguen siendo explotables, lo que sucede con frecuencia en el entorno industrial, ya que los sistemas embebidos utilizados para el control o supervisión de los procesos de fabricación suelen contar con software anticuado.

- **Ataques Dos**: los ataques Dos (Denia lof Service), son en general maniobras de distracción que se utilizan en conjunto con otro tipo de ataques arriba mencionados. Consisten en saturar con un número de peticiones por encima de su capacidad de procesado a los servidores objetivo. Esto resulta en una caída del servicio ofrecido por dichos servidores que obliga en muchas ocasiones a reiniciar los sistemas o desconectarlos temporalmente, lo que hace que el centro de atención de los supervisores de dichos sistemas sea el restablecimiento del servicio. Los atacantes utilizan esta distracción para intentar penetrar los sistemas por otros medios que pueden pasar desapercibidos.

4.2 Medidas de Ciberseguridad

Dado que el mayor factor de riesgo en cualquier entorno informatizado son las comunicaciones, las medidas de seguridad a adoptar por el entorno industrial son aquellas que se llevan implementando y utilizando en el entorno IT durante cierto tiempo y que han demostrado su eficacia. Los cuatro pilares fundamentales en cuanto a la seguridad de las comunicaciones son:

- **Disponibilidad**: la disponibilidad de los equipos dentro de una red debe estar garantizada. Este aspecto es incluso más importante en entornos industriales por las grandes exigencias de continuidad de las líneas de producción. Un paro en dichas líneas supone unas pérdidas significativas para la empresa, por lo cual es imprescindible que todos los dispositivos que componen la cadena de producción estén activos y accesibles en todo momento.
- **Autenticación**: dentro de una red formada por varios dispositivos, es necesario implementar un sistema de identificación que permita verificar la fuente de los mensajes. De este modo, se podrá asegurar que solamente los equipos autorizados tienen acceso a la red y que los mensajes que circulan por ella son seguros, evitando así que agentes externos no deseados se comuniquen con los distintos equipos que conforman la red.
- **Integridad**: la integridad de los datos enviados dentro de la red es un factor primordial para garantizar la seguridad de la misma. Deben existir medidas en vigor que hagan posible la verificación de que un mensaje transmitido por un equipo legítimo de la red llegue a su destino sin sufrir ningún tipo de alteración. Esto evita que los mensajes transmitidos en la red sean interceptados y/o modificados por terceros.

- **Confidencialidad**: es la propiedad que asegura que los datos transmitidos por la red no sean accesibles a aquellos que no forman parte de la misma o que aun formando parte de la red no sean destinatarios de dicha información. Esta medida evita que en caso de que un mensaje sea interceptado por un equipo que no pertenezca a la red o que no sea el equipo de destino del mensaje, no sea capaz de extraer el contenido del mismo.

4.3 Protocolos de Ciberseguridad

Para poder implementar las medidas de ciberseguridad descritas en el apartado anterior, existen varios protocolos. La mayoría se encargan de la confidencialidad y la integridad de las comunicaciones, siendo estos últimos adaptables para proporcionar medidas de autenticación.

4.3.1 Protocolos de Cifrado y Firma

En la actualidad, el método más utilizado para garantizar la confidencialidad de los datos, tanto en comunicaciones como en almacenamiento, es el cifrado.

El cifrado es la técnica empleada para codificar los datos de un mensaje o archivo de modo que la información no sea accesible a todo aquel que no conozca la clave de cifrado.

Para garantizar la integridad y la autenticación de los mensajes, se utilizan protocolos de firma digital.

Una firma digital es un mecanismo criptográfico que permite al receptor de un mensaje firmado digitalmente identificar a la entidad originadora de dicho mensaje (autenticación), y confirmar que el mensaje no ha sido alterado desde que fue firmado por el originador (integridad).

4.3.1.1 Advanced Encryption Standard (AES)

El cifrado AES es un tipo de cifrado simétrico (se utiliza la misma llave para encriptar/desencriptar los datos) utilizado mundialmente para asegurar todo tipo de datos y comunicaciones. Se recoge en el estándar ISO/IEC 18033-3 (Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers) y es el cifrado aprobado por la NSA para la protección de documentos secretos.

Funcionamiento

AES procesa bloques de 128 bits mediante el uso de una llave secreta de 128,192 o 256 bits. Procesa estos bloques por bytes (un total de 16) tratándolos como una matriz de 4X4 y aplica operaciones algebraicas para transformar los datos de entrada en un mensaje cifrado. Las fases del cifrado son las siguientes:

1. **Añadir Llave de Fase (AddRoundKey):** mediante la expansión de llave se generan las necesarias subllaves para cada fase dependiendo del número de fases necesarias para el proceso. En este paso, se realiza una operación XOR entre la matriz de estado (los 128 bits a codificar) y la subllave de cada fase.

2. **Reemplazar Bytes (SubBytes):** se reemplazan los bytes de la matriz de estado con bytes de la “Caja-S” o caja de sustitución.
3. **Desplazar Filas (ShiftRows):** se desplazan los bytes de las filas hacia la derecha, de modo que los bytes que salen por la derecha de la matriz vuelven a entrar por la izquierda. Cada fila desplaza un diferente número de bytes. Este proceso se ilustra en la siguiente figura:

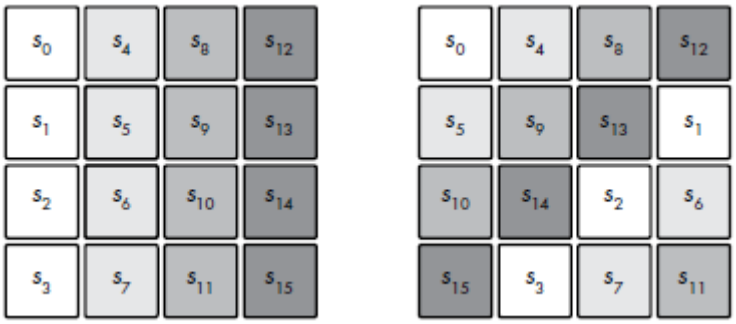

Ilustración 1. Proceso de desplazar filas

4. **Mezclar Columnas (MixColumns):** como paso final se multiplica cada columna por el mismo polinomio, de esta manera se añade mayor difusión criptográfica.

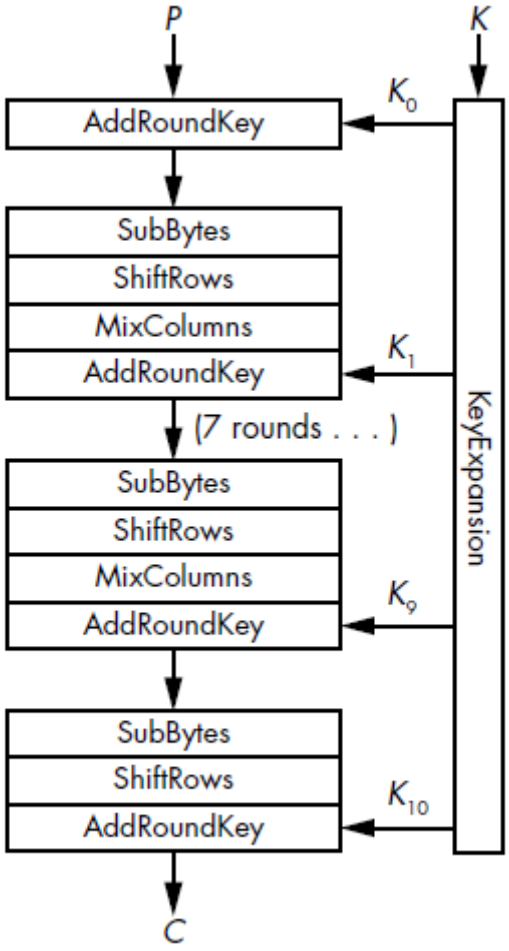

Ilustración 2. Pasos principales del algoritmo AES

CBC (Cipher-block chaining)

En el modo CBC (cipher-block chaining), antes de ser cifrado, a cada bloque de texto (P_i) se le aplica una operación XOR con el bloque previo ya cifrado (C_i). De este modo, cada bloque cifrado depende de todos los bloques usados hasta ese punto. Además, para hacer cada mensaje único se debe usar un vector de inicialización (IV) en el primer bloque, puesto que este bloque no tiene bloques previos con los que se pueda aplicar la operación XOR necesaria.

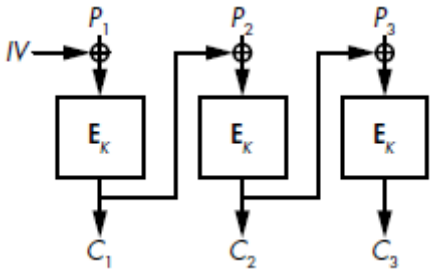

Ilustración 3. Diagrama de bloques del modo CBC

The Counter Mode (CTR)

En el modo CTR o modo de conteo, en vez de encriptar los bloques de datos, se utilizan bloques compuestos de un nonce (N) y un contador (Ctr). El contador es un número entero que incrementa para cada bloque y debe ser distinto para cada bloque dentro del mismo mensaje, siendo posible su reutilización para distintos mensajes. El nonce es un numero único que se emplea para encriptar todos los bloques de un mensaje, pero no puede reutilizarse para distintos mensajes. Una vez creados los bloques, se aplica la operación XOR entre los bloques encriptados y la entrada de datos (P_i) para crear el mensaje encriptado (C_i).

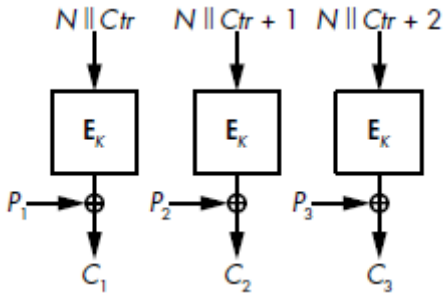

Ilustración 4. Diagrama de bloques del modo CTR

4.3.1.2 Encriptado Rivest–Shamir–Adleman (RSA)

El cifrado RSA es un método de cifrado asimétrico que está recogido en el estándar de internet RFC8017. Un sistema asimétrico de cifrado (también llamado sistema de llave publica o PKI por sus siglas en inglés) consta de dos llaves, una pública y una privada, con las cuales se encriptan y desencriptan los mensajes. La llave pública es utilizada para cifrar los datos de modo que son imposibles de desencriptar sin el conocimiento de la llave privada. Por esta característica, el cifrado RSA es capaz de producir firmas además de encriptar los datos.

Sin embargo, encriptar los mensajes con la llave pública es determinista: dados los mismos datos de entrada, la salida siempre será la misma, por lo tanto, la encriptación simple de RSA no es segura y no se utiliza como tal. Para solucionar este problema, se utiliza el método OAEP.

Optimal Asymmetric Encryption Padding (OAEP)

Para evitar que el proceso de encriptación de RSA sea determinista, el método OAEP añade bits de relleno (padding) aleatorios al mensaje original (K) antes de ser encriptado (P), de modo que dos mensajes de entrada idénticos resulten en mensajes cifrados (C) diferentes.

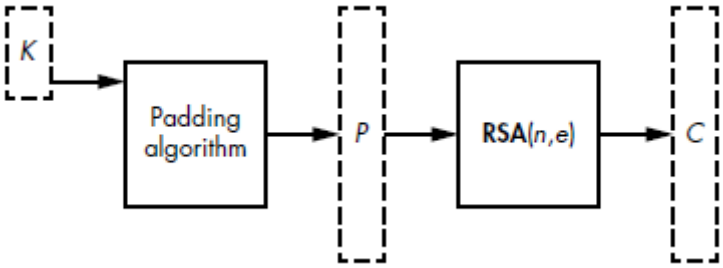

Ilustración 5. Diagrama de bloques de OAEP

Funcionamiento

En el proceso de encriptado del mensaje se divide en las siguientes fases:

1. El mensaje (K) se mezcla con una constante (H) definida por el protocolo OAEP y se rellena con tantos bytes como sea necesario, dando como resultado un mensaje codificado.
2. Se computa el hash de una cadena aleatoria (R), cuyo resultado (Hash 1) tiene la misma longitud que el mensaje codificado.
3. Se aplica la operación XOR entre el Hash 1 y el mensaje codificado, dando como resultado un segundo mensaje (M) que es de igual longitud que el mensaje codificado.
4. Se computa el hash de M (Hash 2) y se aplica la operación XOR con la cadena aleatoria (R) para conseguir R'.
5. Por último, se crea el mensaje a codificar (P) como se indica en la imagen y se aplica la codificación RSA a este mensaje P.

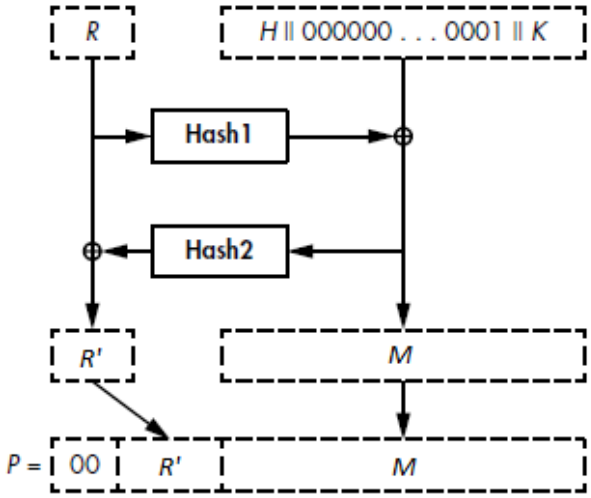

Ilustración 6. Funcionamiento interno de OAEP

Cabe destacar que el cifrado RSA es un proceso lento y no se utiliza para encriptar los mensajes de una comunicación. En su lugar, se utiliza en los procesos de inicio de comunicaciones seguras para intercambiar las llaves simétricas en esquemas de este tipo, que son mucho más eficientes a la hora de encriptar grandes cantidades de datos.

4.3.1.3 SHA-256 (Secure Hash Algorithm)

El acrónimo SHA engloba una familia de estándares hash creados por el NIST (National Institute of Standards and Technology) para las agencias federales no militares de Estados Unidos, actualmente utilizadas en todo el mundo dada su fiabilidad.

Las funciones hash tienen la particularidad de poder crear valores de salida de longitud fija, independientemente de la longitud de los valores de entrada. Esta particularidad hace que las funciones hash tengan infinidad de aplicaciones, principalmente en las áreas de indexación de información, compresión o verificación de datos.

Puesto que los valores hash son únicos para cada valor de entrada, no se puede determinar la entrada desde el valor hash y su cálculo es rápido, son de gran interés en el área de la criptografía para garantizar la integridad de los datos.

Creado para reemplazar el estándar SHA-1 debido a sus vulnerabilidades, el SHA-2 fue desarrollado por la NSA y estandarizado por el NIST dentro de la FIPS PUB 180-2, (actualmente recogido en la FIPS PUB 180-4). SHA-2 agrupa cuatro diferentes modos de operación: SHA-224, SHA-256, SHA-384 y SHA-512. Los dígitos representan la longitud de salida de la función hash en bits y actualmente los más utilizados son el SHA-256 y el SHA-512. Dado que su funcionamiento es muy similar es suficiente analizar uno de ellos para comprender los mecanismos utilizados a la hora de crear un hash del tipo SHA-2. Al ser SHA-256 el más utilizado, será el que se describa a continuación.

Funcionamiento

Para calcular el hash, el mensaje de entrada se divide en bloques de 512 bits (M_N) sobre los que se iteran 64 ciclos. El proceso del cálculo del hash se describe al final de este

apartado (Calculo Hash), pero para poder comprenderlo mejor se describen dos procesos que lo complementan.

1. **Rellenado (Padding)**

   Con el fin de asegurar que la longitud mensaje de entrada (L) es múltiplo de 512 y poder generar una salida fija de 256 bits, se rellena el mensaje original del siguiente modo:

1.1. Se añade un bit con el valor de 1 (L+1).

1.2. Se añaden tantos bits (K) con el valor 0 como sea necesario para que la longitud del mensaje original (L), más el relleno añadido (K+1+64) sea múltiplo de 512, teniendo en cuenta que al final del relleno se añadirá la longitud original del mensaje (L) como un entero de 64 bits de longitud. La operación para calcular los K bits se resume en (L+1+K+64) mod 512=0.

1.3. Finalmente se añade la longitud original del mensaje (L) codificada en un entero de 64 bits.

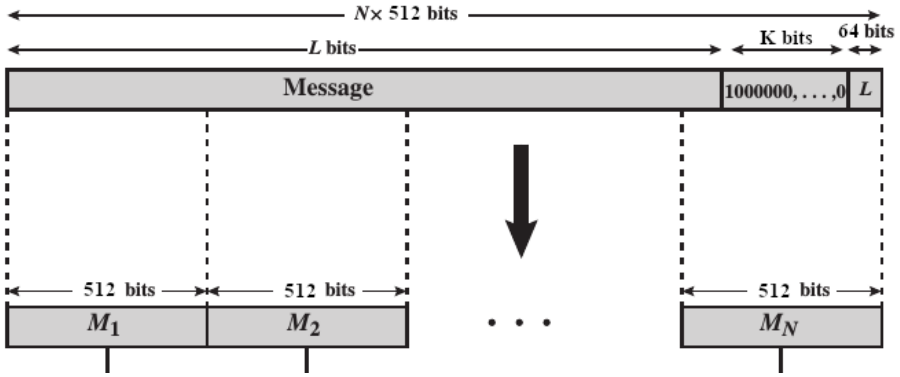

Ilustración 7. Proceso de segmentación y rellenado

El proceso de rellenado siempre se lleva a cabo, aunque la longitud del mensaje original sea múltiplo de 512 desde el principio.

2. **Descomposición de bloques**

Cada bloque de 512 (M_N) bits se utiliza para crear 64 palabras (W_n) de 32 bits de modo que:

2.1. Las primeras 16 palabras (w_0-w_{15}) se obtienen directamente del bloque de entrada, dividiéndolo en palabras de 32 bits.

2.2. Para las 48 siguientes (w_{16}-w_{63}) se aplica la siguiente operación sobre las 16 primeras:

para n entre 16 y 63

s0: = ($w_{[n-15]}$ rotdcha 7) xor ($w_{[n-15]}$ rotdcha 18) xor ($w_{[n-15]}$ despldcha 3)

s1: = ($w_{[n-2]}$ rotdcha 17) xor ($w_{[n-2]}$ rotdcha 19) xor ($w_{[n-2]}$ despldcha 10)

$w_{[n]}$: = $w_{[n-16]}$ + s0 + $w_{[n-7]}$ + s1

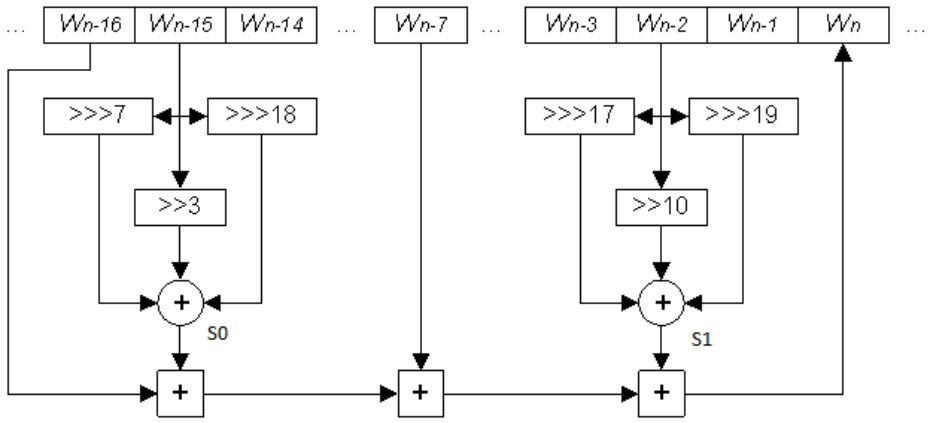

Ilustración 8. Algoritmo para la creación de palabras

3. Calculo Hash

Para calcular el hash final del mensaje se ejecutan 64 rondas por cada bloque de 512 bits (M_N) hasta haber procesado la totalidad del mensaje de modo que:

3.1. Se inicializan 8 sub-bloques de 32 bits a tratar (a-h) con valores iniciales derivados de los primeros 64 números primos (K_n).
3.2. Se ejecuta la descomposición del bloque de 512 bits (M_N), descrito anteriormente, para lograr las 64 palabras necesarias (W_n) para el proceso.
3.3. Se aplican las operaciones descritas en la siguiente imagen para cada palabra generada en la fase de descomposición de bloques (un total de 64):

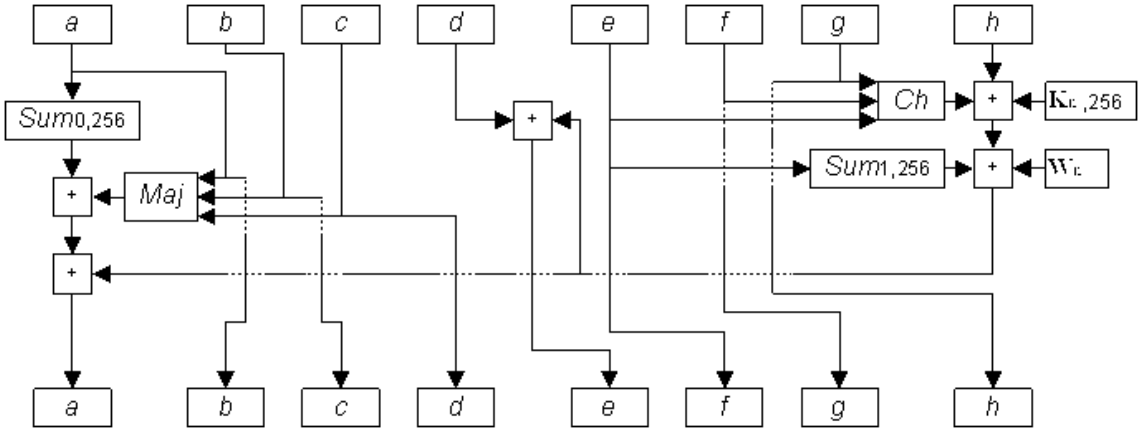

Ilustración 9. Esquema del calculo hash

**Maj(a,b,c)= (a AND b) XOR (a AND c) XOR (b AND c)*

***Ch(e,f,g)= (e AND f) XOR (ē AND g)*

3.4. Se mezclan los bloques de salida con los bloques iniciales.

Finalmente, tras procesarse el último bloque del mensaje se juntan los 8 bloques de salida (a-h) de modo que se crea un hash de 256 bits de longitud (8x32).

4.3.1.4 HMAC (Hash-based MAC)

Un MAC (Message Authentication Code), es un mecanismo que permite crear valores de autenticación de mensajes, llamados etiquetas de autenticación. Estos valores se utilizan para dotar a los mensajes de integridad y autenticación.

La función HMAC, recogida en los estándares FIPS 198-1 y RFC 2104, permite crear etiquetas de autenticación a partir de valores hash y aportará la misma seguridad que la función hash utilizada a la hora de crear la etiqueta y la robustez de llave. Dado que HMAC permite utilizar distintos algoritmos hash, se añade el algoritmo usado al nombre para facilitar su identificación. Como ejemplo el HMAC-SHA-256 utiliza SHA-256 como función hash subyacente.

Funcionamiento

De la llave original (key) se generan dos llaves secundarias:

1. La llave interna (i_key_pad): utilizando la operación XOR entre la llave (key) y el relleno interno (i_pad).
2. La llave externa (o_key_pad): utilizando la operación XOR entre la llave (key) y el relleno externo (o_pad).

A continuación, aplica la operación hash del mensaje junto con la llave interna (i_key_pad) que da como resultado un valor hash intermedio (hash sum 1).

Como paso final, se aplica la operación hash a la combinación de la llave externa (o_key_pad) y el hash intermedio (hash sum 1), dando como resultado la etiqueta de autenticación (hash sum 2).

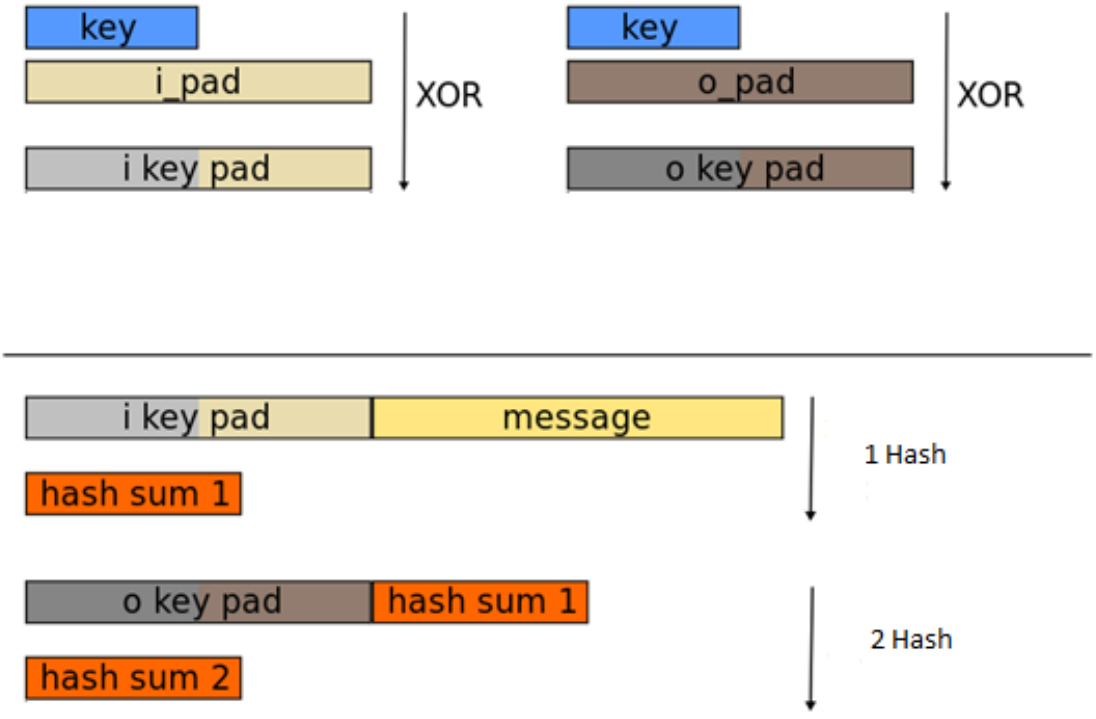

Ilustración 10. Llaves HMAC

4.3.1.5 RSA-PKCS

Como se ha descrito en el apartado de cifrado RSA, este protocolo de cifrado permite su uso para firmas digitales. El proceso de firmado para RSA es tan simple como efectivo:

1. Se calcula el hash del mensaje enviado.
2. Se cifra el mensaje enviado con la llave privada creando la firma del mensaje.
3. Se envía el mensaje junto a la firma.
4. Se desencripta la firma con la llave pública y se calcula el hash del mensaje
5. Si los valores hash coinciden se da por auténtico el contenido.

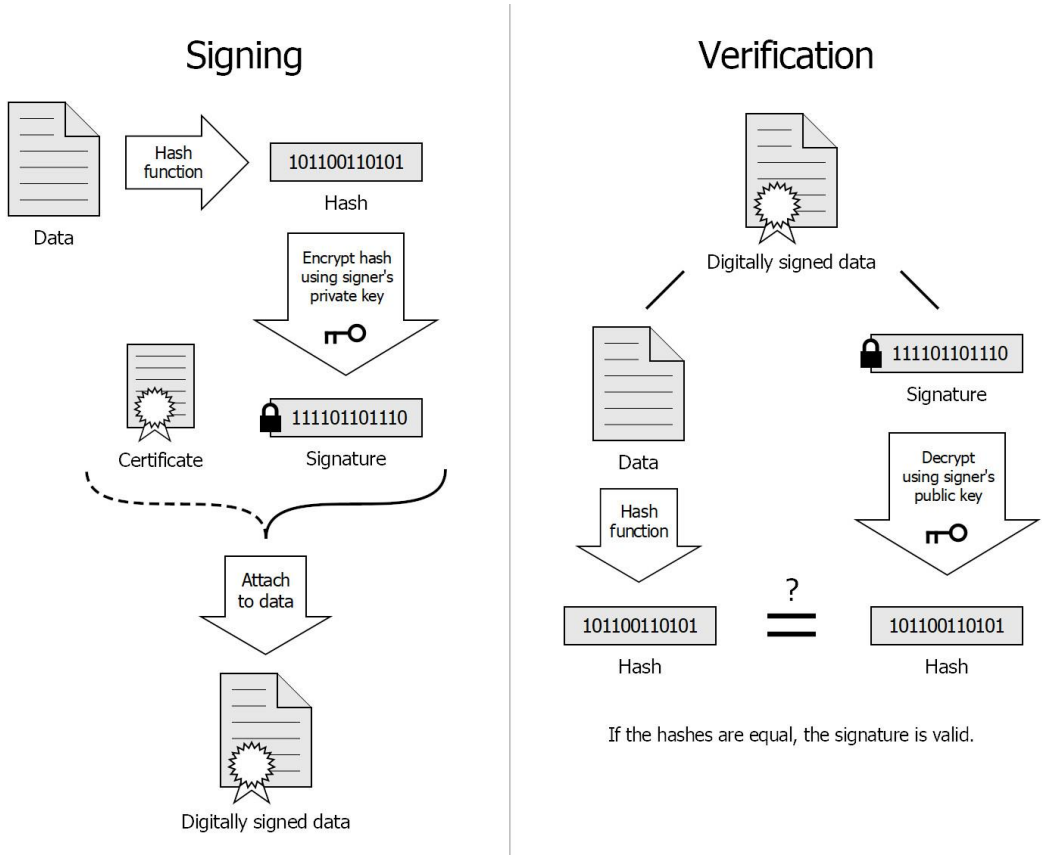

Ilustración 11. Proceso de autenticación RSA-PKCS

Aunque no se han encontrado vulnerabilidades respecto al firmado RSA-PKCS, no existe una prueba para determinar su nivel de seguridad, por lo que se decidió crear el esquema RSA-PSS como alternativa más segura.

4.3.1.6 RSA-PSS

Del mismo modo que para el modo de cifrado RSA-OAEP, el método de firma RSA-PSS busca añadir seguridad al firmado RSA-PKCS mediante el uso de rellenado (padding).

El proceso de firma PSS consta de las siguientes fases:

1. Se calcula el hash del mensaje original (hash(M)) utilizando la función hash correspondiente (SHA-256 comunmente), este hash tendrá un tamaño h-bytes.

2. Se crea una cadena de r-bytes utilizando una función PRNG (Pseudo Random Number Generator) denominado salt.
3. Se crea mensaje intermedio (M'), que consta de un rellenado de 8 bytes de valor 00, el hash del mensaje original (hash(M)) y la cadena de r-bytes generada en el paso anterior (salt).

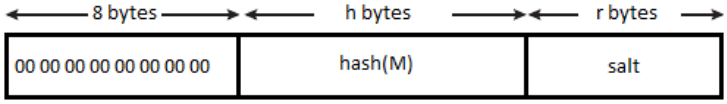

Ilustración 12. Estructura de M'

4. Se calcula el hash del mensaje intermedio (hash (M')) de longitud h'-bytes.
5. Se crea un segundo mensaje (L) compuesto por un rellenado que consta de una serie de bytes de valor 00 terminados en un byte de valor 01 y el salt creado en el paso 2. El tamaño de este mensaje (l) estará limitado por el tamaño de la llave pública (m-bytes), requisito de RSA, de modo que el tamaño del mensaje será: l= m-h'-1byte (BC).

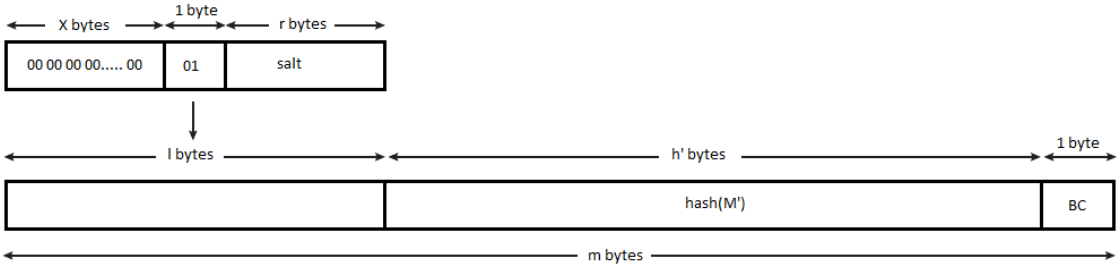

Ilustración 13. Estructura de L y L'

6. Se aplica la función XOR a L y hash (M') creando L'.
7. Se compone el contenido final de la firma con L', hash(M') y el byte de cola (BC).

Ilustración 14. Estructura final

8. Finalmente, se encripta el contenido con la llave privada y se genera la firma.

Para poder verificar la firma, es necesario comunicar al receptor la función hash utilizada y la longitud del salt, dado que el resto está definido en el estándar o puede deducirse. Finalmente, una vez obtenido el hash de la firma, se computa el hash del mensaje recibido y se compara para verificar la integridad y autenticidad del mensaje.

Al añadir un factor de aleatoriedad como es el salt, y puesto que existe una prueba para verificar que es una firma segura, se recomienda utilizar RSA-PSS sobre RSA-PCKS.

4.4 Ciberseguridad en la Industria

Como se ha mencionado con anterioridad, el estado de la ciberseguridad en la Industria se encuentra en sus etapas iniciales. Sin embargo, existen varias iniciativas enfocadas a impulsar la adopción de la ciberseguridad por parte de la industria a nivel internacional.

ENISA (European Union Agency for Network and Information Security) es el ente europeo encargado de promover la ciberseguridad en todos los sectores a nivel europeo. A pesar de no tener su foco central en la industria, dada la importancia de la misma, ENISA ha publicado un documento de referencia para la ciberseguridad industrial.

4.4.1.1 Communication network dependencies for ICS/SCADA Systems

Este documento redactado por ENISA hace referencia a sistemas ICS y SCADA y analiza los distintos factores de ataque, las vulnerabilidades más comunes y cómo combatirlas. También se recomienda el uso de ciertas tecnologías de comunicación por sus características de seguridad.

Ilustración 15. Amenazas cubiertas en el documento

Finalmente, se incluye un listado de buenas prácticas en cuanto a ciberseguridad para entornos industriales. Aunque no sea un estándar, guías de buenas prácticas como la mencionada son documentos que responden a las necesidades de ciberseguridad presentes en la actualidad y proponen maneras de mitigar las causas más comunes de ataques y vulnerabilidades presentes en el sector.

5 Comunicaciones Industriales

Por sus necesidades de tiempo real, las comunicaciones industriales se han diferenciado de las comunicaciones convencionales desde la automatización de la industria. El siguiente apartado cubre las arquitecturas de comunicaciones industriales y su evolución y analiza el protocolo de comunicación OPC UA, protocolo de referencia para el futuro de las comunicaciones industriales.

5.1 Modelos de Arquitecturas para las Comunicaciones Industriales

Las comunicaciones industriales están ligadas a las arquitecturas implementadas en cada planta. La arquitectura principal para las comunicaciones desde hace décadas ha sido el modelo CIM, sin embargo, recientemente se han creado nuevos modelos de arquitecturas para adaptar la industria a las nuevas tecnologías.

5.1.1 Modelo CIM

La estructura actual de las comunicaciones industriales se basa en el modelo CIM (Computer Integrated Manufacturing), mencionada por primera vez en el libro del mismo nombre del Dr. Joseph Harrington a principios de los años 70.

El modelo CIM es una estructura de capas que se representa en forma de pirámide y agrupa en distintos niveles dispositivos con funcionalidades similares que tienen el mismo nivel de exigencia en cuanto a la transmisión de información.

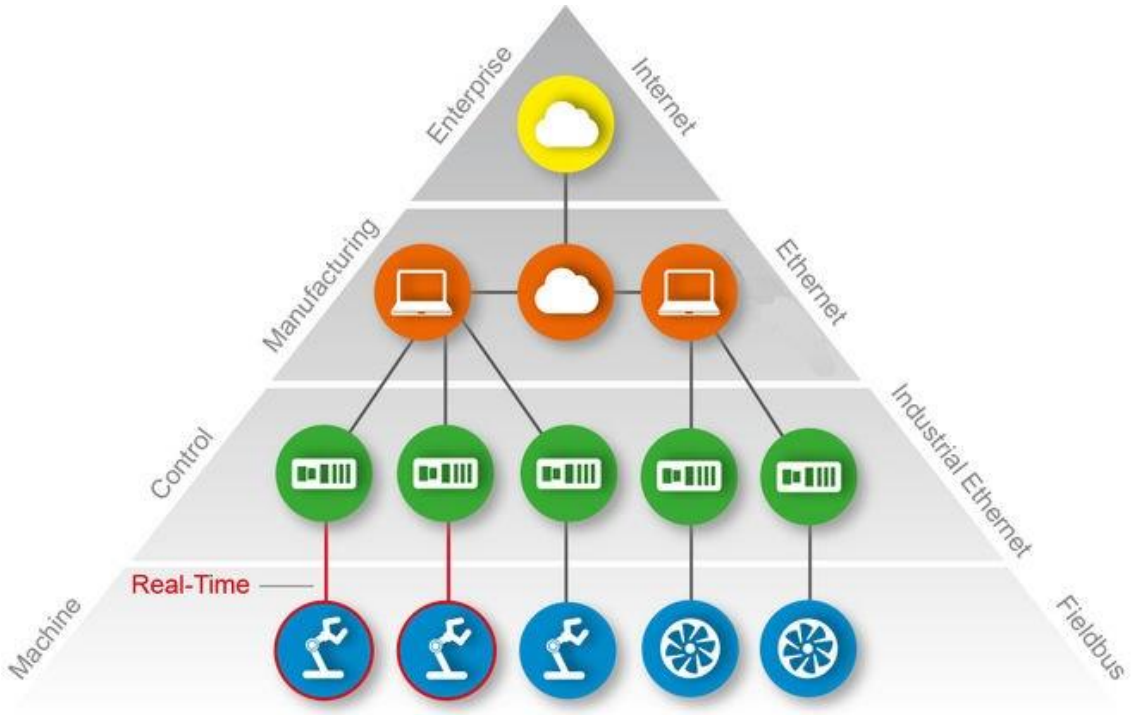

Ilustración 16 - Pirámide CIM y sus protocolos más significativos

5.1.1.1 Nivel de dispositivo (Machine)

Es el nivel más cercano a la producción. En él, se encuentran todos los sensores y actuadores que forman parte del proceso de fabricación. La información transmitida en este nivel es la que está relacionada directamente con el proceso de fabricación, como temperaturas, recorrido de la cinta, etc. Además de la información mencionada, también se incluye información relevante para la seguridad y calidad del proceso.

En este nivel se utilizan buses de campo. Los buses de campo son redes locales industriales que conectan los elementos que componen el nivel de dispositivo con el nivel superior. Por la naturaleza de los datos transmitidos en este nivel, las comunicaciones en los buses de campo deben cumplir requisitos de tiempo real y contar con sistemas de control de error. Los protocolos correspondientes a este nivel son robustos, manejan pocos datos con rapidez y fiabilidad, tienen definidos mensajes especiales de alarmas y eventos para adaptarse a posibles errores en la red y priman la transmisión de datos en tiempo real.

5.1.1.2 Nivel de célula (Control)

El nivel de control está constituido mayormente por PLCs (Programmable Logic Controller), que se encargan de recolectar la información transmitida por los sensores y actuadores del nivel inferior para su procesado. Es el nivel responsable de la automatización de los procesos dependiendo de la información obtenida del nivel inferior. Este nivel se compone de distintas islas, siendo cada isla responsable de una parte del proceso de fabricación. Las islas se componen de un controlador ligado a varios elementos de campo (actuadores, sensores, etc.). En ocasiones dependiendo de la complejidad de la tarea o el tamaño de la cadena de producción pueden agruparse varios controladores secundarios o esclavos al mando de un controlador principal o maestro.

En este nivel encontramos un paradigma de comunicación similar al anterior, en cuanto a que la mayor parte del tráfico va dirigido al nivel inferior. Existe también cierto flujo de información horizontal para posibilitar la coordinación entre distintas etapas del proceso, pero suele estar coordinada por los controladores maestros haciendo uso de los distintos eventos que proveen los protocolos de campo.

5.1.1.3 Nivel de planta (Manufacturing)

En este nivel se supervisan las distintas células de producción mediante el uso de sistemas SCADA (Supervisory Control And Data Acquisition) en combinación con computadoras con adaptadores especiales de comunicaciones. La función principal del nivel de planta es la supervisión del proceso en tiempo real utilizando los datos recopilados por los PLCs del nivel inferior. Es el primer nivel que permite la interacción humana. Consta principalmente de interfaces adaptados para el visionado de temperaturas, niveles de tanques, número de operaciones efectuadas, etc. También permite realizar modificaciones del proceso o cambiar parámetros de producción dependiendo de las necesidades del momento.

Este nivel es el punto de unión entre las comunicaciones industriales y las comunicaciones IT, puesto que es posible acceder a los sistemas SCADA remotamente o incluso conectar computadoras en este nivel mediante el uso de tarjetas adaptadas.

Por lo tanto, en este nivel se enlazan las redes IT tradicionales (LAN/WAN) con los buses de campo.

5.1.1.4 Nivel de Fábrica (Enterprise)

En la cúspide de la pirámide se encuentra la red más compleja. Está compuesta en su mayoría por computadoras y se encarga de gestionar el proceso global de fabricación y los controles de logística. No interviene en el proceso ya que su cometido es meramente de recopilación de datos para su visionado y evaluación. Puesto que esta red se compone de computadoras en su mayoría, se utiliza una estructura y componentes tradicionalmente IT, aunque puede incluirse algún elemento para la compatibilización con redes inferiores.

5.1.2 RAMI 4.0

Con la necesidad de integrar las nuevas tecnologías de comunicación y dispositivos conectados dentro del entorno industrial, se ha creado un nuevo modelo de comunicaciones industriales que se aleja del tradicional. Este da paso a una estructura más descentralizada y menos rígida, capaz de hacer frente a las necesidades de integración con el mundo IT que muchas de las nuevas tecnologías presentan e integrar así un nuevo modelo de industria.

El modelo RAMI 4.0, (Reference Architectural Model Industrie 4.0) diseñado por Platform Industrie 4.0 como modelo de referencia para el nuevo modelo de industria conectada, desecha el modelo tradicional de pirámide donde las funcionalidades o el tipo de hardware definían el nivel en el que se encontraban los distintos componentes de la red. Esta nueva arquitectura opta por un modelo sin jerarquías definidas, en el que todos los dispositivos forman parte de la red y las comunicaciones se dan libremente dentro de la misma.

5.1.2.1 Enfoque Tridimensional

Dejando atrás la tradicional pirámide CIM, el nuevo modelo de referencia para la industria 4.0 busca abordar la organización de la empresa desde tres puntos de vista principales que engloban varios aspectos del proceso de fabricación.

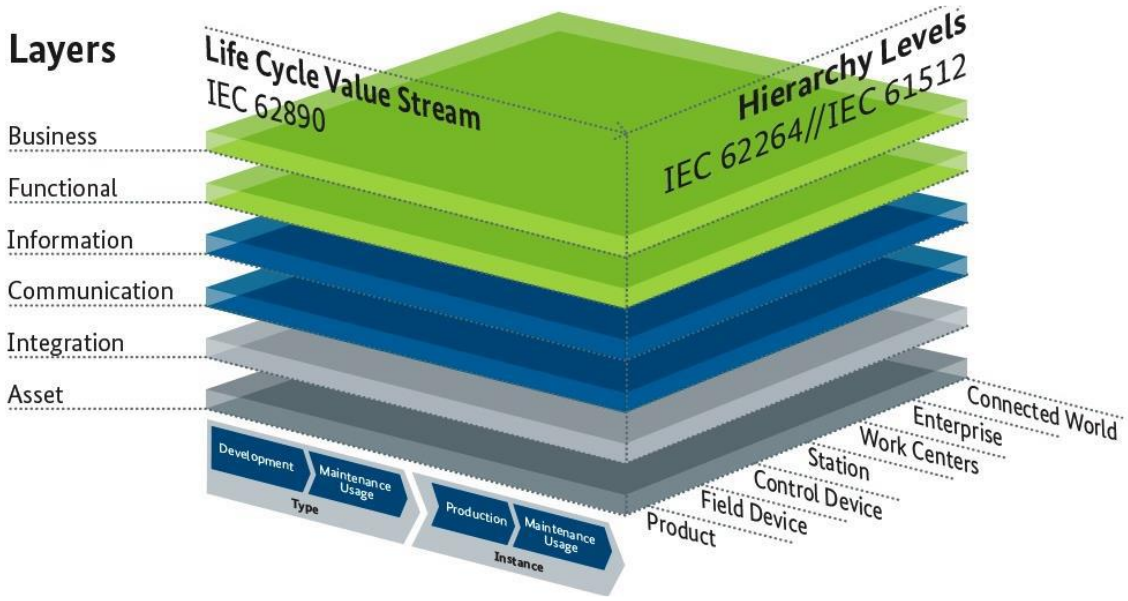

Ilustración 17. Arquitectura RAMI 4.0

- **Jerarquía:** el nuevo modelo propone un sistema distribuido de los elementos que forman parte de la empresa, en el que existen tres grandes grupos, El mundo conectado, El Producto Inteligente y La Planta Inteligente. Se define que tanto los sistemas como los componentes sean flexibles, capaces de adaptarse a cambios en la red y el proceso. Las distintas funciones se llevan a cabo de modo distribuido y las conexiones entre los componentes no se reducen a un nivel concreto, sino que todos los elementos forman parte de la red, incluido el propio producto.
- **Ciclo de Vida del Producto:** se tienen en cuenta todas las fases implicadas en la creación del producto final, así como el servicio postventa. Se hace referencia a la fase del producto: si está en fase de desarrollo, se le considera un tipo y si está en fase de producción, una instancia. De este modo, cada vez que un producto es renovado o se actualiza, pasa de la fase de instancia, a la de tipo y de nuevo a la fase de instancia, implementando la ideología de desarrollo y mejora continua.
- **Capas:** se definen en capas los distintos aspectos a tener en cuenta a la hora de manufacturar un producto. Las capas de Activos, Integración y Comunicación hacen referencia a los componentes físicos de la planta, su digitalización y los estándares de comunicación utilizados. La capa de Información, como su nombre indica, engloba todos los datos relativos al producto y su manufacturación, materiales, números de serie, pedidos, proveedores, etc. Esta información alimenta las demás capas del modelo. Por último, las capas de Funcional y de Negocios, se encargan de gestionar el proceso de manufactura y sus aspectos técnicos y de supervisión y la parte de logística y marketing.

5.1.2.2 Internet de las cosas y servicios

RAMI 4.0 se centra en el aspecto digital de la empresa, incluyendo a todos los dispositivos que forman la red en una capa denominada la capa física o la capa de las “cosas”, haciendo referencia al IoT (Internet of Things) o Internet de las cosas.

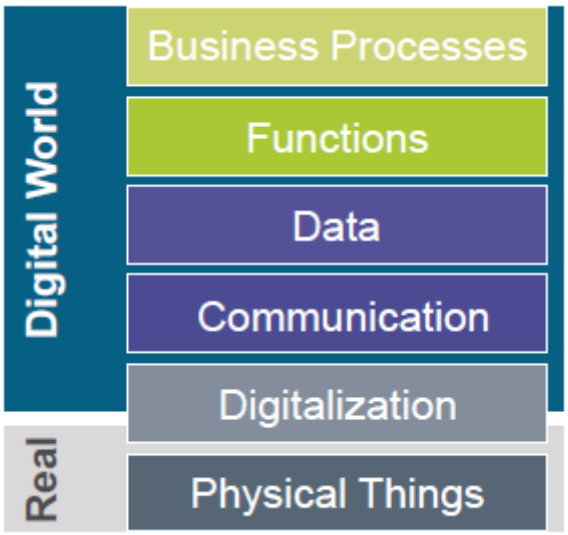

Ilustración 18. Distintas capas y su soporte

Se prioriza de este modo la digitalización de los procesos creando objetos virtuales de cada dispositivo físico para poder gestionar su información correspondiente en diversos apartados dependiendo del estado en el que se encuentra del proceso de fabricación. Dado que el aspecto digital tiene gran importancia en el papel de la Industria 4.0, en este modelo se incluye el concepto de la seguridad y la privacidad de los datos como un aspecto más a la hora de diseñar la red y los componentes que formarán la empresa.

5.1.2.3 La capa de administración

La capa de administración es la capa que se encarga de gestionar los dispositivos físicos en el entorno digital. Es el interfaz estándar de comunicación dentro de la red industrial y permite crear un objeto que representa al dispositivo físico, reflejando sus funcionalidades, variables, medidas, etc.

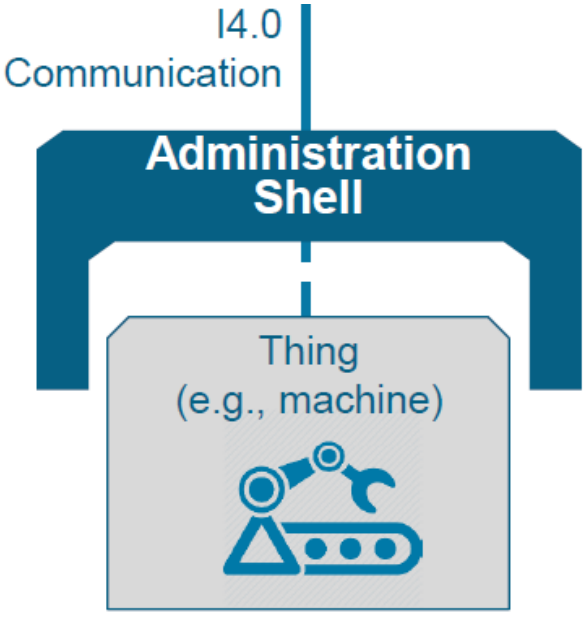

Ilustración 19. Esquema de la Administration Shell

La capa de administración permite agrupar distintos dispositivos dentro de grupos de trabajo o unidades que dispondrán a su vez de su propia capa de administración. De este modo, se consigue una red modular que facilita la interconexión de los distintos componentes de la cadena de producción.

5.1.3 IIRA

Industrial Internet Reference Architecture (IIRA) es una arquitectura de referencia creada por Industrial Internet Consortium que busca ser el modelo de referencia para la fabricación inteligente. Al igual que la arquitectura RAMI 4.0, aborda los desafíos que plantean la conectividad y las tecnologías IoT en el entorno industrial. Esta arquitectura se basa en el estándar ISO/IEC/IEEE 42010:2011 y se centra en las necesidades de lo que define como “actores” (stakeholders), “intereses” (concerns) y “puntos de vista” (viewpoints).

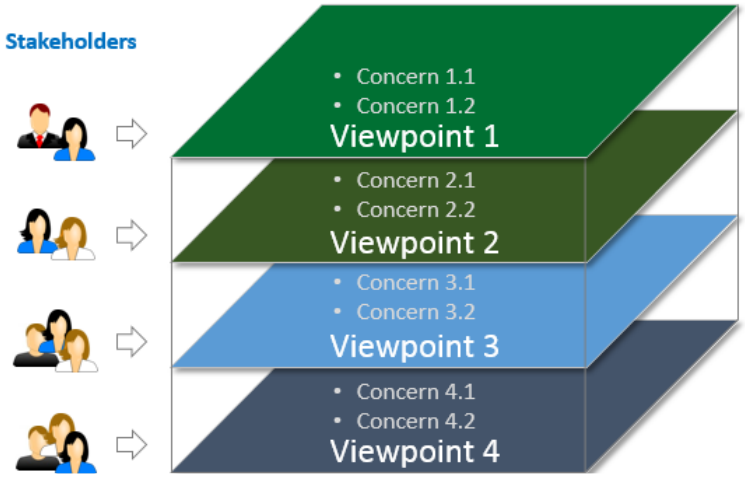

Ilustración 20. Modelo completo IIRA

5.1.3.1 Modelo General

Al igual que en la arquitectura RAMI 4.0, el modelo del Industrial Internet Consortium consta de una arquitectura definida por un modelo compuesto de distintas capas. Dichas capas engloban los puntos de vista de los diferentes factores que conforman la empresa. Dentro del modelo se diferencian 4 capas principales: La capa de negocio, la capa de utilización, la capa funcional y la capa de implementación.

Como se puede observar por el nombre de las capas, el alcance del modelo IIRA dista del de RAMI 4.0 en que no solo se centra en cómo diseñar e implementar un ecosistema de fabricación inteligente dentro de la planta, sino que tiene en cuenta los diferentes departamentos de los que consta la planta de producción como empresa y establece una hoja de ruta para cada departamento basado en sus diferentes puntos de vista.

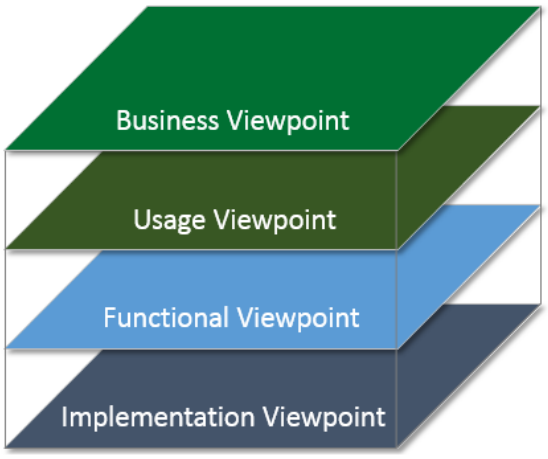

Ilustración 21. Capas IIRA

5.1.3.2 Capa de Negocio

En esta capa, el modelo IIRA se centra en el aspecto económico de un sistema de fabricación inteligente y ayuda a evaluar aspectos clave como la propuesta de valor, la rentabilidad o el coste de mantenimiento. De este modo se asegura que la directiva de la empresa está involucrada en la implementación del sistema de fabricación inteligente desde el principio.

En esta capa se introduce la necesidad de justificar la ciberseguridad como un riesgo más, dado que una brecha de seguridad en el sistema puede incurrir en una parada de la producción, en una filtración de información confidencial o en otros ataques que supondrían una pérdida económica considerable.

5.1.3.3 Capa de Utilización

En esta capa se describe como traducir los objetivos identificados en la capa de negocio al diseño de una red industrial bajo el marco de la IIRA. Para la creación del diseño es necesario identificar y definir los requisitos del sistema, que utilizarán las actividades descritas en este apartado para facilitar dicha definición.

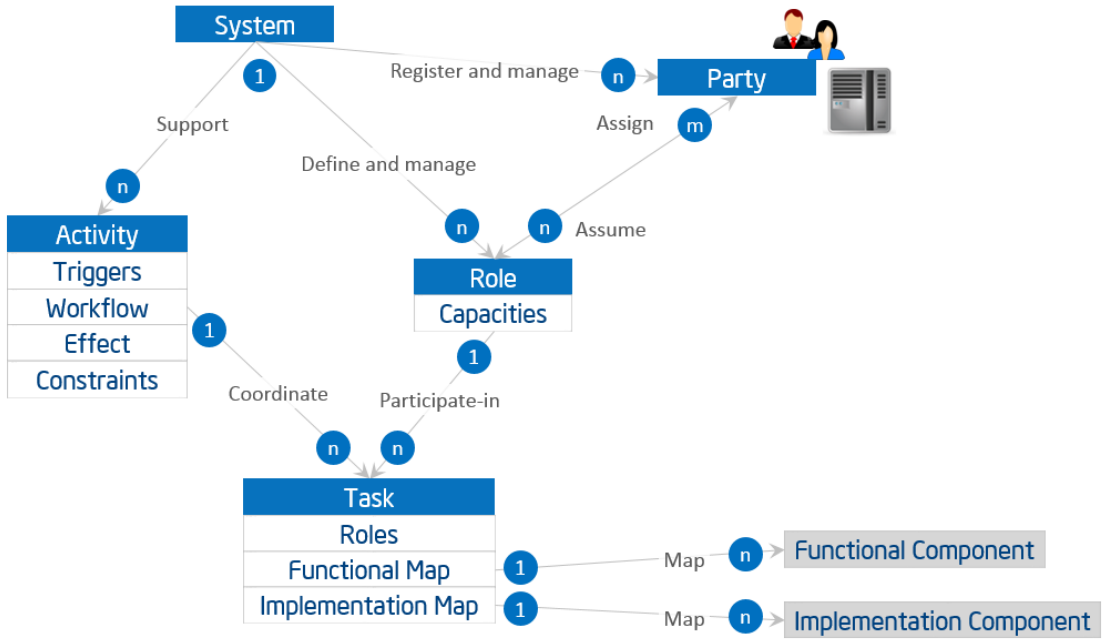

Ilustración 22. Detalle de la capa utilización

La tarea (Task) es la unidad básica de trabajo, la llamada a una operación, una transmisión de datos o una acción ejecutada por un agente (Party). Las tareas son ejecutadas por agentes asumiendo un puesto (Role).

Un puesto es un conjunto de capacidades asumido por una entidad para iniciar o participar en la ejecución de una tarea o consumir el resultado de la misma, como parte de una actividad (Activity).

Un agente es una entidad, humana o automatizada, que tiene autonomía, interés y responsabilidad en la ejecución de una tarea.

En este apartado se habla de cuatro medidas de seguridad: La monitorización, la auditoría, la administración de políticas de seguridad y la administración de soporte criptográfico.

La monitorización y la auditoría se encargan de recolectar, analizar y guardar eventos relacionados con la seguridad de las actividades y el sistema. La administración de políticas de seguridad se encarga del aspecto de la seguridad relacionada con los agentes, tanto automatizados como humanos, finalmente, el soporte criptográfico administra las llaves globales y el almacenamiento y revocación de las credenciales.

5.1.3.4 Capa Funcional

La capa funcional es donde se encuentran la mayoría de las equivalencias con el modelo RAMI 4.0, ya que es la capa en la que se definen las secciones funcionales de una planta y cómo implementarlas.

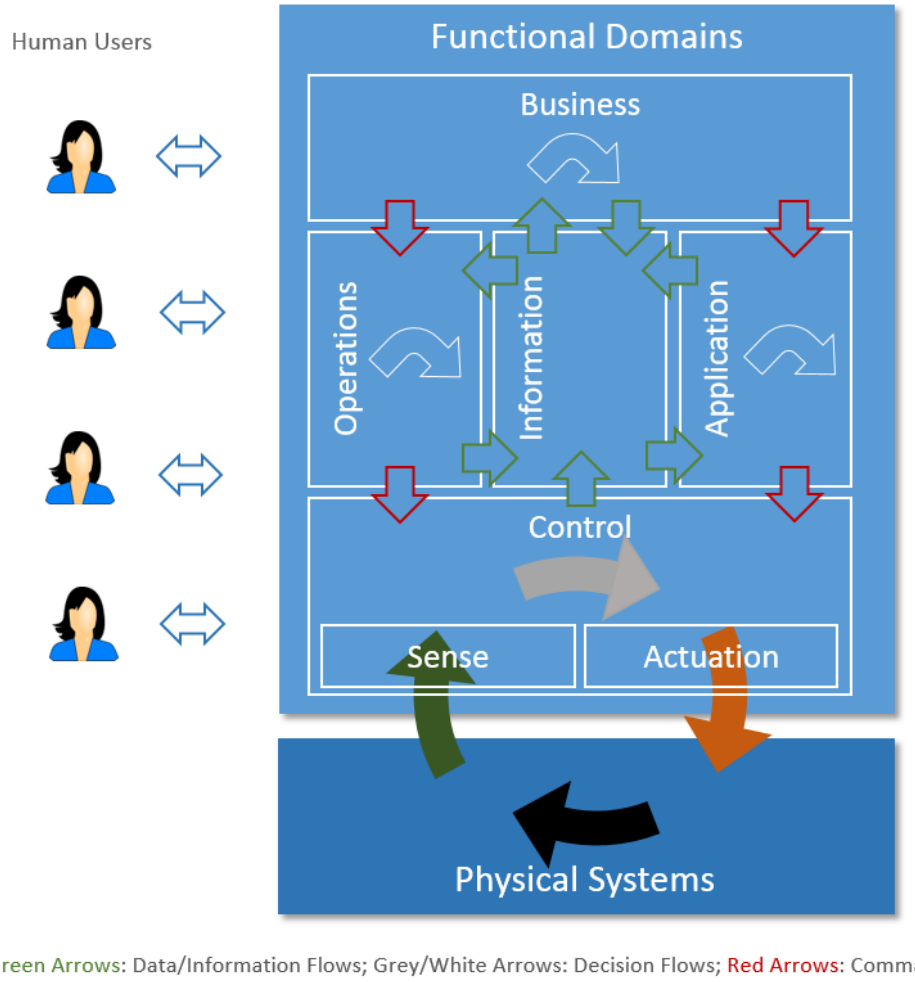

Ilustración 23. Detalle de la capa funcional

Como se puede observar en la imagen, se definen varios campos entre los que habrá flujos de información, ya sean órdenes, peticiones o datos, y al igual que en el modelo RAMI 4.0 se agrupan los sistemas físicos en una capa y se capitaliza en procesar la información que esta capa genera.

- **Campo de Control:** el campo de control es el responsable de procesar toda la información que se genera en los sensores de la capa física y gestionar los actuadores en consecuencia. Del mismo modo, es el campo de control el que creara entidades abstractas basadas en los distintos sensores y actuadores de la capa física que reflejarán en un modelo digital todas sus características. Estas entidades abstractas son las equivalentes a la capa de administración del modelo RAMI 4.0.
- **Campo de Operación:** el campo de operación se encarga de la administración, suministro, monitorización y optimización de los sistemas en el campo de control. Teniendo en cuenta el aspecto global de la empresa no solo una planta en concreto. Se utilizará la información generada en el campo de control para optimizar los recursos de la empresa en general.
- **Campo de Información:** el campo de información es donde se analizarán los datos obtenidos en el campo de control para modelar las diferentes plantas y

ayudar en el proceso de toma de decisiones y mejora y optimización de las plantas.

- **Campo de Aplicación:** el campo de aplicación será el encargado de recoger todas las reglas, lógica de control, modelos e interfaces utilizados en el campo de control.
- **Campo de Negocio:** en el campo de negocio se utilizarán los datos generados durante el proceso de fabricación para mejorar los aspectos de gestión de la empresa, relación con los clientes, facturación, servicio postventa y planificación.

5.1.3.5 Capa de Implementación

La capa de implementación es la que aúna las demás capas en un esquema integral. Recoge las representaciones técnicas del sistema y sus tecnologías y componentes necesarios para implementar las actividades y funciones descritas en la capa de Utilización y en la capa Funcional.

La capa de negocio será la que ayude a decidir la arquitectura y las tecnologías elegidas para la implementación. Será la que marque objetivos de mercado, estrategias de negocio, cumplimiento de regulaciones y la planificación de los objetivos globales.

5.2 OPC UA

OPC UA (Open Platform Communications Unified Architecture) es una tecnología de comunicación creada para facilitar la interconexión de los nuevos modelos de industria y ha sido propuesta por VDE y ZVEI como capa interoperable de comunicaciones para el modelo de RAMI 4.0. Orientada a comunicaciones Machine to Machine (M2M), concede gran importancia a la seguridad de las comunicaciones.

OPC UA es un estándar abierto (IEC 62541) creado por la OPC Foundation para ser compatible con diferentes plataformas y crear una arquitectura de red industrial más simple y compatible con el mundo IT/IoT, sin descuidar las necesidades de tiempo real de los procesos de fabricación.

5.2.1 Flexibilidad de diseño

El estándar OPC-UA ofrece gran flexibilidad en su implementación dada la distinta naturaleza de los dispositivos que componen el tejido industrial. Define funcionalidades necesarias y opcionales a la hora de aplicar el estándar y ofrece varias opciones de tecnologías existentes para su realización.

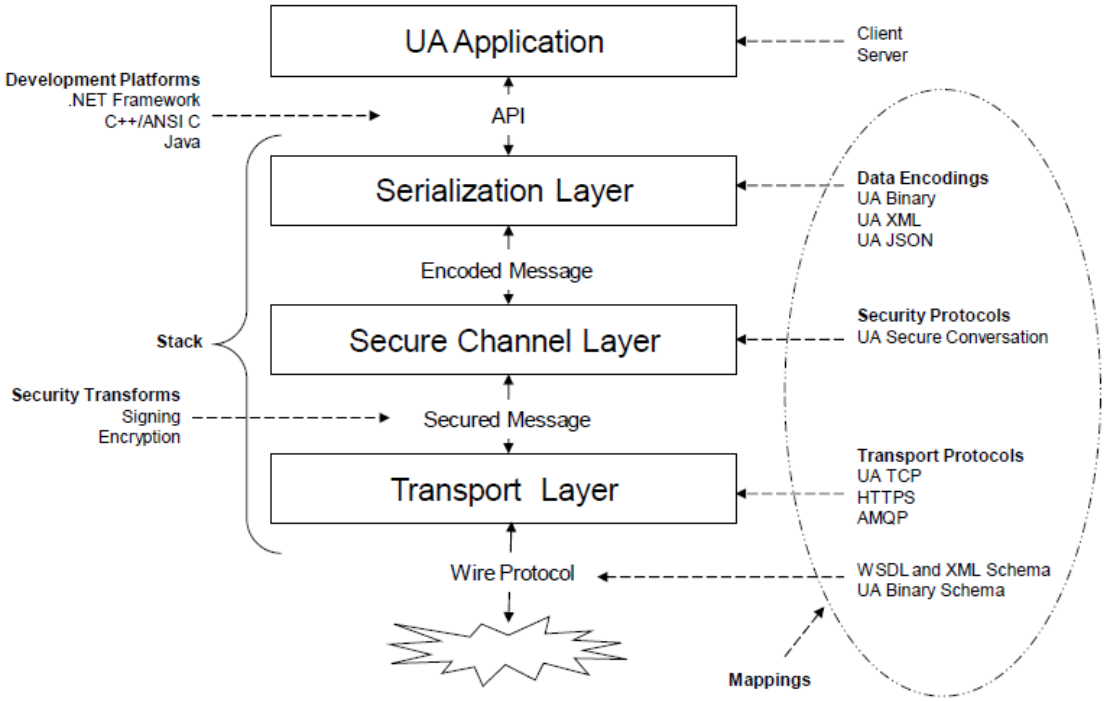

Ilustración 24. Estructura OPC UA

En la figura se puede apreciar un esquema completo de lo que sería una implementación de OPC-UA y sus distintos componentes. Cabe destacar que para cada sección se proporcionan varias opciones de tecnologías existentes con sus debidos mapeos a las funcionalidades exigidas por OPC-UA. En su documentación OPC-UA ofrece varios "Stacks", que consisten en grupos predefinidos de protocolos para cada sección de OPC-UA con el objetivo de facilitar su implementación.

Con respecto al modelo de referencia OSI (Open Systems Interconnection) OPC UA se sitúa en la capa de aplicación (7) pudiendo ser encapsulada en otro protocolo de nivel de aplicación (HTTPS) o en uno de transporte directamente (TCP+TLS/SSL).

5.2.2 Capa de transporte

Para su capa de transporte, OPC-UA define la necesidad de ofrecer conexiones full dúplex entre cliente y servidor, dejando a elección del desarrollador las tecnologías empleadas para ello.

Estructura del mensaje

Todos los mensajes de OPC UA estarán adaptados a la capacidad de transporte de sus capas inferiores, lo que crea la posibilidad de dividir el mensaje en segmentos denominados "trozos" (chunks).

Cada trozo dispondrá de al menos tres cabeceras -la cabecera de mensaje, la cabecera de seguridad y la cabecera de secuencia-, contando el primer trozo con una cabecera adicional denominada prefijo de extensión de objeto.

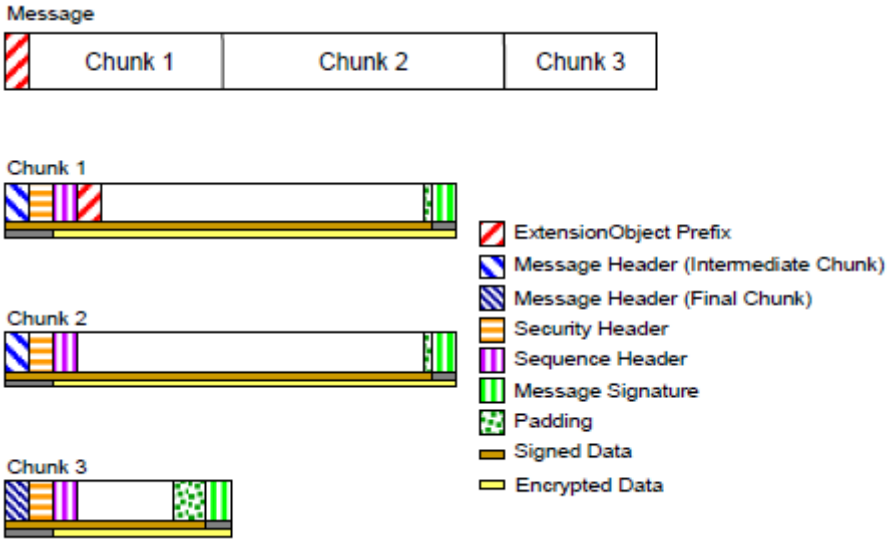

Ilustración 25. Ejemplo de mensaje

Prefijo de extensión de objeto

Campo que define el tipo de estructura de datos que contiene el mensaje. Existe una lista de estructuras de datos preestablecidos en el protocolo que recoge las estructuras de datos más comunes, dando la posibilidad de combinar varios de ellos o insertar estructuras de datos propias.

Cabecera de mensaje

Tipo de Mensaje	FF	Longitud del mensaje en Bytes

Ilustración 26. Contenido de la cabecera

La cabecera del mensaje consta de tres apartados como se observa en la imagen. Los primeros 3 bytes corresponderán al tipo de mensaje que puede ser:

- HEL (Hello, utilizado para iniciar la conexión por parte del cliente o para aceptarla si la conexión es iniciada por el servidor).
- ACK (Acknowledge, mensaje de aceptación de la conexión por parte del servidor).
- ERR (Error, mensaje de error).
- RHE (ReverseHello, utilizado para iniciar la conexión por parte del servidor).

El cuarto byte será ignorado y tendrá el valor hexadecimal del FF.

Los últimos 4 bytes informarán de la longitud del mensaje en bytes incluyendo los 8 bytes de la cabecera de mensaje.

Establecimiento de la conexión

La conexión puede ser iniciada tanto por el cliente como por el servidor.

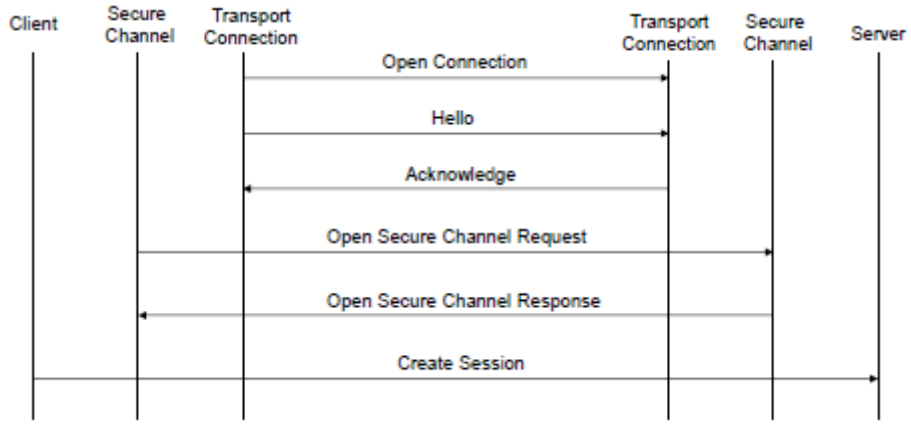

Ilustración 27. Conexión iniciada por el servidor

Si la conexión es iniciada por el cliente, este enviará un mensaje del tipo Hello con la que iniciará la negociación del buffer, que determinará el tamaño máximo de cada trozo (chunk). Si el servidor acepta el tamaño de buffer, confirmará la conexión con un mensaje del tipo Acknowledge. El tamaño del buffer será transmitido a la capa de canal seguro que analizaremos más adelante.

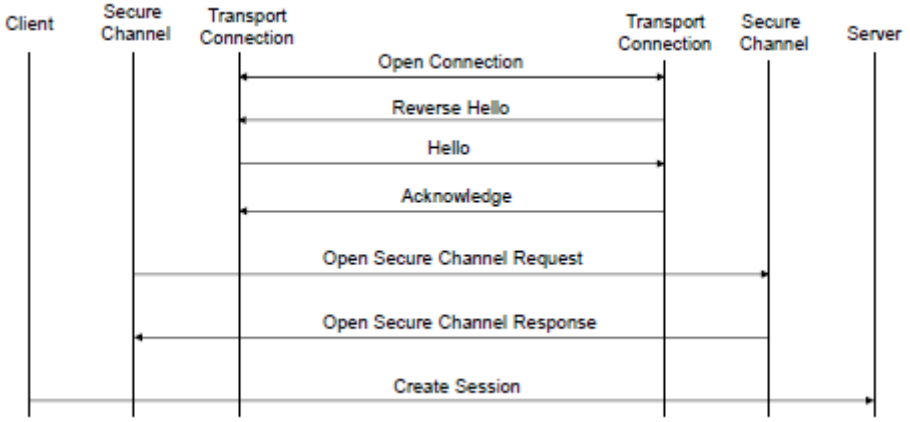

Ilustración 28. Conexión iniciada por el cliente

Si la conexión la inicia el servidor, este enviará un mensaje del tipo Reverse Hello, iniciando así la transacción descrita en el apartado anterior.

Una vez establecida la conexión, se negocian las medidas de seguridad que se aplicarán a la conexión en la capa de canal seguro.

5.2.3 Capa de canal seguro

Esta capa es la responsable de garantizar la seguridad en las comunicaciones entre cliente y servidor. La capa de canal seguro es responsable de la **integridad** de los mensajes, la **confidencialidad** y la **autenticación de las aplicaciones**.

Existen 3 niveles de seguridad para crear un canal seguro.

- **Sin seguridad:** el canal se crea sin ningún método de autenticación, integridad ni confidencialidad. Este modo solamente se implementa para poder garantizar la compatibilidad con sistemas antiguos y no se recomienda, puesto que, como su nombre indica, no aporta ninguna seguridad a la comunicación
- **Firmado:** el método de firmado solo garantiza la integridad y la autenticación de los mensajes, obligando tanto al cliente como al servidor a firmar los mensajes con sus llaves privadas, que deberán estar en los listados de confianza del receptor para ser validados.
- **Firmado y Cifrado:** el método más seguro que ofrece OPC UA, garantiza tanto la integridad y autenticación como la confidencialidad obligando a encriptar el mensaje además de firmarlo.

Establecimiento de comunicaciones seguras

El proceso de crear un canal seguro (para los modos de firmado y firmado y encriptado) es un proceso de conexión asimétrica. Este se inicia con un mensaje de OpenSecureChannel que el cliente encriptará con la llave pública del servidor y firmará con su llave privada.

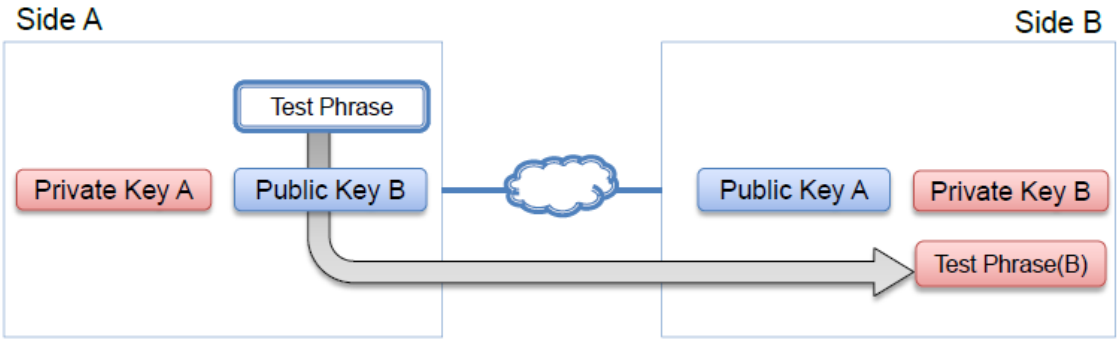

Ilustración 29. Inicio del canal seguro

En el segundo paso el servidor desencriptará el mensaje con su llave privada (un mensaje encriptado con la llave pública solo puede ser desencriptado con la correspondiente llave privada) y verificará la firma del cliente. Acto seguido, encriptará un mensaje de respuesta con la llave pública del cliente y lo firmará con su llave privada.

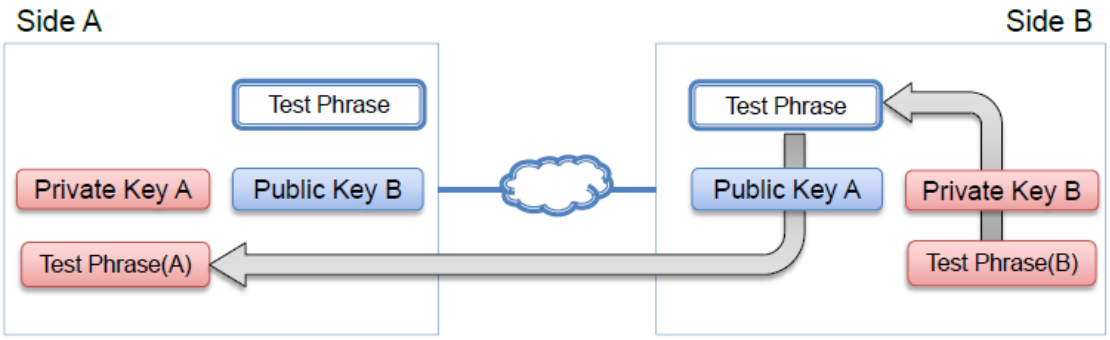

Ilustración 30. Respuesta del servidor

Finalmente, el cliente desencriptará el mensaje de respuesta con su llave privada y confirmará la identidad del servidor.

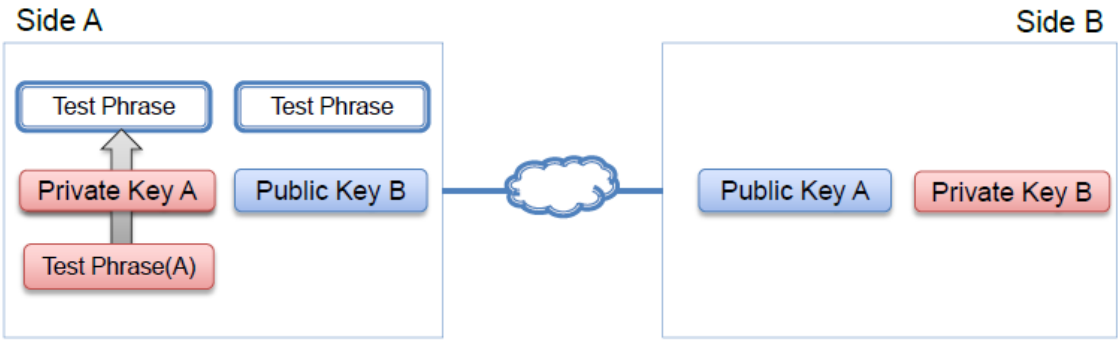

Ilustración 31. Confirmación de la identidad del servidor por parte del cliente

Una vez establecido el canal seguro y dado que el proceso de encriptación asimétrico consume mucho tiempo y recursos, tanto el cliente como el servidor compartirán una llave de cifrado (método simétrico) que al ser más vulnerable a ataques renovarán periódicamente. Cabe destacar que en el método de solo firma, el establecimiento del canal seguro procede del mismo modo, solo que una vez establecido el canal dejan de encriptarse los mensajes transmitidos.

Políticas de seguridad

En la actualidad se aplican las siguientes políticas de seguridad:

Política de seguridad	Protocolo de Cifrado		Protocolo de Firma	
	Simétrica	Asimétrica	Simétrica	Asimétrica
Aes128-Sha256-RsaOaep	AES128-CBC	RSAES-OAEP	HMAC-SHA2-256	RSASSA-PKCS1-v1.5
Basic256Sha256	AES256-CBC	RSAES-OAEP	HMAC-SHA2-256	RSASSA-PKCS1-v1.5
Aes256-Sha256-RsaPss	AES256-CBC	RSAES-OAEP	HMAC-SHA2-256	RSASSA-PSS
PubSub-Aes128-CTR	AES128-CTR	X	HMAC-SHA2-256	X
PubSub-Aes256-CTR	AES256-CTR	X	HMAC-SHA2-256	X

Ilustración 32. Políticas de seguridad OPC UA

5.3 Estándares para la Securización de las Comunicaciones Industriales

Los estándares de protocolos de comunicación industrial y las medidas de seguridad a adoptar por dichos protocolos son limitados. No obstante, las nuevas tecnologías introducidas en el sector y la creciente amenaza que suponen los ataques cibernéticos están impulsando un cambio en este aspecto. A continuación, se introducen los estándares mas importantes en cuanto a ciberseguridad en las comunicaciones industriales.

5.3.1 ISO/IEC 27033

Dispone de una serie de guías técnicas para el diseño y la implementación de redes seguras para industria 4.0. Dentro de este documento se incluyen soluciones actualmente utilizadas en escenarios IT adaptadas al mundo OT.

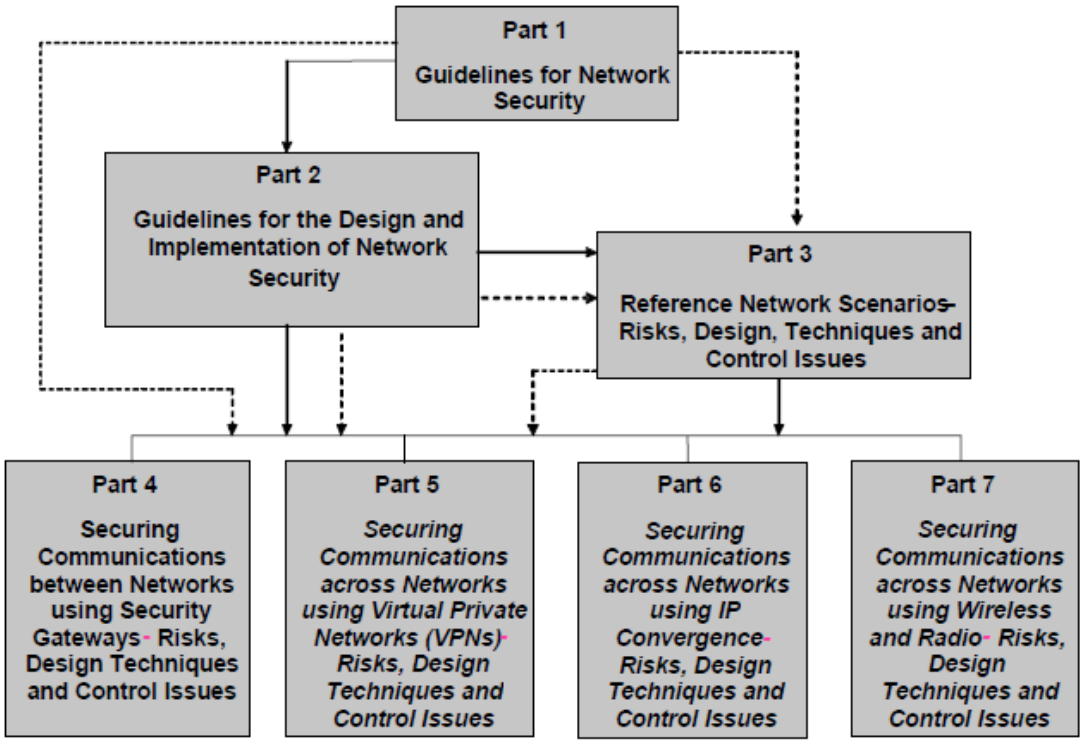

Ilustración 33. Resumen de apartados ISO/IEC 27033

- Define y describe conceptos relacionados con la seguridad en las redes.
- Incluye guías de detección y análisis de riesgos de seguridad en redes y define requisitos de seguridad basados en los análisis realizados.
- Contiene una descripción general de los controles técnicos para arquitecturas de redes seguras, así como los controles no técnicos y los controles técnicos que se aplican no solo a las redes.
- Dispone de una introducción a los riesgos, diseño y métodos de control asociados con estructuras de red tradicionales. Incluye también un sumario de posibles problemas derivados de implementar los mecanismos de seguridad más comunes.

5.3.2 IEC 62443

El estándar IEC 62443 toma un enfoque global de la seguridad para entornos industriales abarcando varios aspectos dentro de este sector. En el documento IEC 62443-3-2 se establecen los mínimos requeridos para considerar una red industrial segura y en el documento 62443-3-3 se establecen los mecanismos necesarios para hacer frente a distintos perfiles de atacante.

El modo en el que este estándar afronta los retos de seguridad de un sistema industrial es mediante el uso de 4 niveles de seguridad distintos. Primero ayuda a identificar el

perfil de atacante y tipos de ataques más probables contra las estructuras de red que se disponen en la empresa. En base al nivel de seguridad que se quiere adquirir, se describen los métodos de seguridad que son necesarios y describe los requisitos que se deben cumplir a la hora de aplicar los mismos.

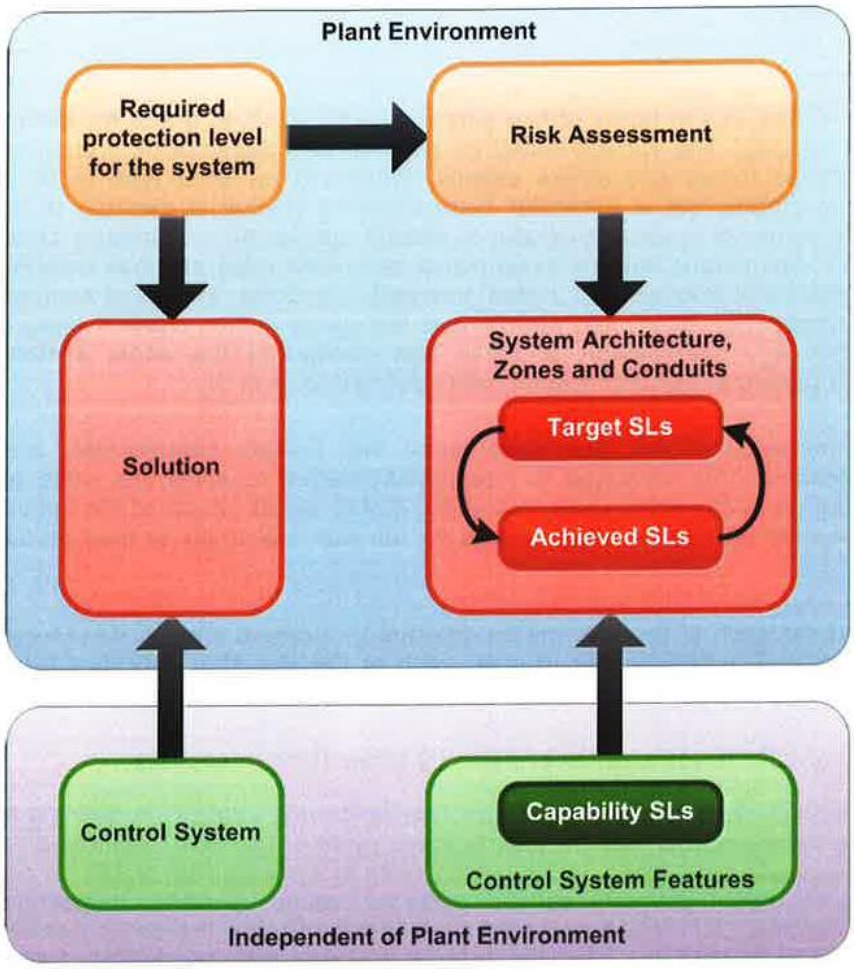

Ilustración 34. Esquema de implementación de un nivel de seguridad

5.3.3 IEC 62351

Esta familia de estándares está enfocada a las denominadas “Smart Grids” y la securización de sus comunicaciones. En sus distintos apartados define medidas de seguridad específicas dependiendo de los protocolos utilizados.

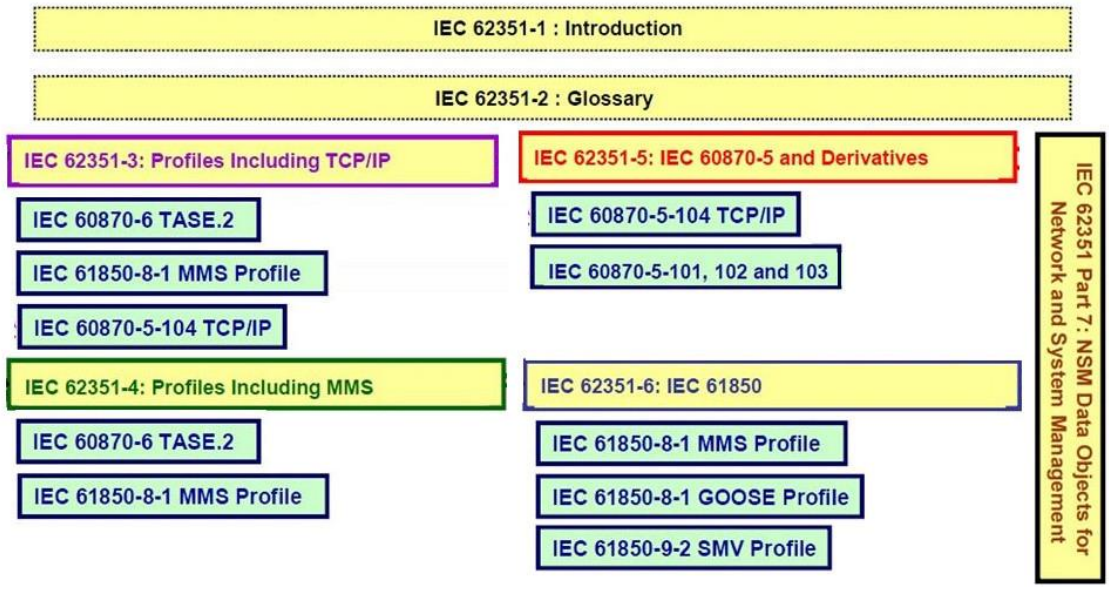

Ilustración 35. Apartados de la familia IEC 62351

Los distintos protocolos de comunicaciones cubiertos son:

- IEC 61850, utilizado en la automatización de subestaciones.
- IEC 61400-25, para las comunicaciones y monitorización en plantas eólicas.
- IEC 60870-5, protocolo para el control remoto de equipos.
- IEC 60870-6, utilizado para telemetría.
- IEC 61970, empleado en sistemas de gestión de la energía.
- IEC 61968, estándar en desarrollo que se encargará de las comunicaciones entre sistemas de distribución eléctrica.

La sección IEC 62351-1 da una visión global de los requisitos de seguridad necesarios para las comunicaciones en Smart Grids y posibles amenazas.

Esta familia de estándares pretende dotar a los distintos protocolos de comunicaciones cubiertos en sus apartados con las herramientas necesarias para hacer frente a los ataques cibernéticos, cada vez más frecuentes, contra este tipo de infraestructuras.

5.3.4 NIST 800-82v2

Parte de la iniciativa impulsada por el NIST (National Institute of Standards and Technology) conocida como NIST Risk Management Framework, que tiene como objetivo proporcionar una guía de gestión de riesgos para entornos industriales.

Este documento es una guía para securizar los entornos SCADA e ICS (Industrial Control Systems) entre otros, así como sistemas consolidados por PLCs. Dentro del mismo se analizan diferentes tipos de topologías para dichos sistemas, posibles amenazas y se dan recomendaciones de cómo combatirlas.

Se utiliza en conjunto con el estándar NIST 800-53 que define:

- Controles de acceso.

- Identificación y autenticación.
- Protección de sistemas y comunicaciones.
- Integridad de los sistemas y la información.

Entre varios aspectos más relacionados con la seguridad de los sistemas industriales.

6 Conclusiones

Tras la realización del estudio del estado del arte se han obtenido las siguientes conclusiones:

1. Existen varias tecnologías y protocolos de seguridad cibernética robustos y asentados en el entorno IT de mostrada eficiencia que están siendo adaptados o podrían adaptarse al entorno OT.
2. Los entornos OT en la actualidad no pueden implementar la mayoría de las medidas de seguridad utilizadas en entornos IT debido a varios factores técnicos, que se esperan superar mediante la iniciativa de Industria 4.0.
3. La iniciativa Industria 4.0 es un marco de implementación maduro y con grandes avances en conectividad y ciberseguridad para el entorno industrial, pero supone una gran inversión en infraestructura que la mayoría de las empresas no efectuarán a corto plazo.
4. Existe gran variedad de estándares que recogen medidas de ciberseguridad y marcos de aplicación sobre tecnologías ya implementadas. Sin embargo, la práctica totalidad están orientadas al mundo IT.
5. Pese a la novedad de las tecnologías implicadas en la Industria 4.0, ya existe un marco de certificación disponible que cubre el aspecto de ciberseguridad de la misma.

Considerando los puntos descritos se considera que el trabajo normativo en torno a la ciberseguridad para la industria se encuentra en un estadio inicial y, por lo tanto, los estándares específicos dirigidos a la Industria 4.0 en esta materia son limitados. Sin embargo, se ha detectado desde las entidades reguladoras y de estandarización una gran voluntad de trabajo e iniciativas dirigidas a cubrir este vacío.

Por lo tanto, se considera que en un corto plazo existirán diversas tecnologías adaptadas para dotar de seguridad a los entornos industriales, así como estándares y certificados aplicables a las mismas, lo que se considera esencial para poder hacer frente a la cada vez mayor amenaza que implican los ataques cibernéticos.

Finalmente, cabe destacar que el entorno industrial es un sector con gran reticencia a los cambios en su modo de operar por las grandes inversiones que suelen suponer dichos cambios y la inercia del propio sector. Sin embargo, existen precedentes de aceptación e integración de nuevos modelos de negocio por parte de la industria que hoy en día se consideran parte intrínseca de la misma, como pueden ser los procesos de calidad. Teniendo en cuenta esta última anotación, se prevé que la adopción de la ciberseguridad por la industria será una cuestión de tiempo, para la que ya se están sentando las bases desde los principales actores a nivel mundial.

7 Bibliografía

ENISA, «Communication network dependencies for ICS/SCADA Systems». 2016.

Y. Lu, K. C. Morris, y S. Frechette, «Current standards landscape for smart manufacturing systems», *National Institute of Standards and Technology, NISTIR*, vol. 8107, p. 39, 2016.

A. C. K. Gary y U. N. Prananto, «Cyber Security in the Energy World», en *2017 Asian Conference on Energy, Power and Transportation Electrification (ACEPT)*, 2017, pp. 1-5.

L. Thames y D. Schaefer, *Cybersecurity for Industry 4.0*. Springer, 2017.

S.-W. Lin *et al.*, «Industrial internet reference architecture», *Industrial Internet Consortium (IIC), Tech. Rep*, 2015.

H. Bedenbender *et al.*, «Industrie 4.0 plug-and-produce for adaptable factories: Example use case definition models and implementation», *Federal Ministry for Economic Affairs and Energy (BMWi), Tech. Rep.*, 2017.

W. A. Conklin, «IT vs. OT security: A time to consider a change in CIA to include resilienc», en *System Sciences (HICSS), 2016 49th Hawaii International Conference on*, 2016, pp. 2642–2647.

L. Rauchhaupt, G. Kadel, y others, «Network-based Communication for Industrie 4.0-Proposal for an Administration Shell», *Federal Ministry for Economic Affairs and Energy (BMWi)*, 2013.

OPC Foundation, «OPC Unified Architecture Interoperability for Industrie 4.0 and the Internet of Things». 2016.

OPC Foundation, «OPC Unified Architecture Specification». 22-nov-2017.

N. O. Alonso y others, *Redes de comunicaciones industriales*. Editorial UNED, 2013.

Dr. Tobias Heer, Markus Heintel, Stefan Hiensch, Dr. Lutz Jänicke, y Others, «Secure Communication for Industrie 4.0», *Federal Ministry for Economic Affairs and Energy (BMWi), Tech. Rep.*

T. Bartman y K. Carson, «Securing communications for SCADA and critical industrial systems», en *Protective Relay Engineers (CPRE), 2016 69th Annual Conference for*, 2016, pp. 1–10.

J.-P. Aumasson, *Serious Cryptography: A Practical Introduction to Modern Encryption*. No Starch Press, 2017.

The European Cyber Security Organisation, «STATE OF THE ART SYLLABUS Overview of existing Cybersecurity standards and certification schemes v2». 2017.

S. McLaughlin *et al.*, «The cybersecurity landscape in industrial control systems», *Proceedings of the IEEE*, vol. 104, n.º 5, pp. 1039–1057, 2016.

O. Post, J. Seppälä, y H. Koivisto, «The Performance of OPC-UA Security Model at Field Device Level.», en *ICINCO-RA*, 2009, pp. 337–341.