

STORMSHIELD

Mejore la protección de su sistema operativo

Todo acerca de la norma IEC 62443

Índice

CONTEXTO

Amenazas cibernéticas y retos industriales

Puesta en marcha de un sistema de gestión de riesgos

Mejora de la protección del sistema operativo

Estructura de la norma

IEC 62443 e ISO 27001

DATOS SOBRE LA NORMA

La defensa en profundidad

Zonas de seguridad

Conductos

Nivel de seguridad

Ejemplo de segmentación por zonas y conductos

VENTAJAS

Los 7 requisitos fundamentales

La certificación IEC 62443-4

Especificaciones IEC 62443-4-1

Beneficios esperados

STORMSHIELD LE ACOMPAÑA

Resumen de las indicaciones propuestas por cada capítulo de la norma

Resumen ejecutivo

La arquitectura de los sistemas de automatización y control industriales (IACS, por sus siglas en inglés) se ha vuelto más compleja, y ahora está ampliamente interconectada con sistemas externos. Estas interconexiones favorecen la explotación de las vulnerabilidades, por lo que el mundo de la tecnología operacional (conocida como OT, por sus siglas en inglés) se ha convertido en un objetivo preferente para los ciberdelincuentes.

Las consecuencias de un ataque cibernético para un sistema industrial pueden ser devastadoras: desde la pérdida de producción, económica y financiera, hasta daños medioambientales e incluso vidas humanas.

Por estos motivos, es importante establecer un plan de gestión de riesgos sólido y fiable para garantizar la protección de los sistemas industriales y operativos. En este contexto, **la norma IEC 62443 propone un marco completo de gestión de riesgos asociado a la implantación de un sistema de ciberseguridad industrial en estos sistemas.**

Este enfoque implica, *en la práctica*, la identificación exhaustiva de los activos, el análisis en profundidad de las diferentes amenazas y vulnerabilidades que estos sistemas pueden presentar. Este documento de referencia guía al lector industrial en la aplicación coherente de medidas de seguridad con cada uno de los sistemas industriales y operativos.

Este libro blanco le desentraña la norma IEC 62443, así como **las etapas necesarias para la implantación de una gobernanza cibernética coherente con las necesidades operativas**. Muestra, en particular, la importancia de la certificación IEC 62443 en la elección de las soluciones puestas en práctica para la puesta en conformidad. Esta certificación garantiza, en algunos casos, la confianza que puede depositar en estas soluciones a la hora de asegurar la infraestructura de los sistemas de automatización y control industriales.

En resumen, este libro blanco propone una lectura en profundidad de la norma IEC 62443 para una mejor comprensión de los retos y su aplicación en un marco operativo definido, a saber, la puesta en práctica de una política de seguridad global que proteja los activos sensibles de diversos sistemas de automatización industrial.

Además, esta publicación le proporcionará pistas de reflexión para integrar sus contenidos de referencia según el estado de la técnica en materia de ciberseguridad industrial.

ACERCA de este libro electrónico

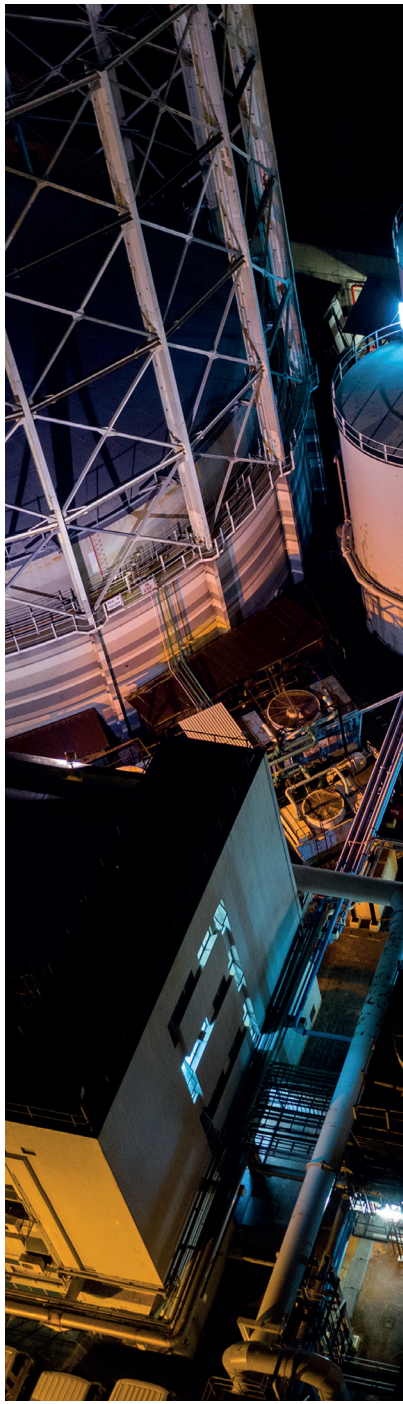
Esta publicación está dirigida a los responsables de operaciones, de mantenimiento, actividades y directores operativos a cargo de infraestructuras críticas, así como a los responsables de seguridad de los sistemas de información.

26,8 %:

porcentaje de ordenadores que forman parte de un sistema de control industrial (ICS) que han sufrido intentos de ciberataques[1]

70 %:

porcentaje de organizaciones industriales que han sido víctimas de ciberataques en 2023[2]



1: https://rendre-notre-monde-plus-sur.goron.fr/pourquoi-le-secteur-industriel-est-il-devenu-une-cible-privilegiee-des-cyberattaques/

2: https://itsocial.fr/enjeux-it/enjeux-securite/cybersecurite/pres-de-70-des-organisations-industrielles-ont-ete-victimes-dune-cyberattaque-en-2023/



70 %:

aumento potencial de ciberataques a las infraestructuras de producción, según diversos especialistas[1]

3,8 M €:

coste medio de un fallo informático para una empresa industrial[2]

1: https://www.linkedin.com/pulse/cybers%C3%A9curit%C3%A9-industrielle-les-attaques-en-hausse-holiseum-qcsme/

2: https://www.imsnetworks.com/ressources-et-actual/cout-cyberattaques-industrie/

El despliegue de la industria del futuro, iniciado desde hace años, ha complicado el entorno de los sistemas de automatización y control industriales. La interconexión entre la red industrial y la infraestructura informática de gestión tradicional, o los socios externos, aumenta la superficie de ataque y, por lo tanto, las posibles vulnerabilidades de seguridad que pueden explotarse.

Amenazas cibernéticas y retos industriales

El aumento del número de ataques contra sistemas industriales ilustra la explotación de estas deficiencias. Así, en 2023, cerca del 70 % de las organizaciones industriales fueron víctimas de un ciberataque[1]. En ese mismo año, el conjunto de los sistemas industriales de los ámbitos de la salud, la energía y las industrias farmacéutica y manufacturera experimentaron un coste global por fugas de datos por valor de más de 25 millones[2] de dólares.

Filtración de información

25

millones de dólares

Coste global en 2023

Los riesgos asociados a estos ciberataques van mucho más allá del ámbito financiero. En efecto, **la interacción entre los procesos y los equipos de los sistemas de automatización y control industriales puede provocar accidentes industriales** que pueden comportar consecuencias mucho más graves, como la pérdida de vidas humanas o los daños medioambientales.

1: https://itsocial.fr/enjeux-it/enjeux-securite/cybersecurite/pres-de-70-des-organisations-industrielles-ont-ete-victimes-dune-cyberattaque-en-2023/

2: https://www.ibm.com/resources/downloads/cost-data-breach-report

Implantación de la gestión de riesgos

La ejecución de un plan de gestión de riesgos se basa en un proceso de evaluación de amenazas y riesgos que tiene por objeto poner en práctica medidas para abordar las vulnerabilidades existentes y aumentar así el nivel de protección cibernética del sistema industrial en su conjunto. Este plan debe encuadrarse en un procedimiento de gobernanza global, a fin de garantizar un seguimiento periódico de las acciones puestas en marcha y de los nuevos riesgos futuros.

El principio, descrito en la norma IEC 62443, se basa en **la identificación y el inventario de activos** que pueden adoptar la forma de datos relacionados con la propiedad intelectual, de personas, de servidores o incluso de componentes o procesos del sistema industrial. El proceso de evaluación de riesgos consiste en determinar la probabilidad de que una amenaza cibernética explote una vulnerabilidad específica con consecuencias para los activos identificados.

Finalmente, a partir de este riesgo inicial, la organización pondrá en práctica medidas organizativas, técnicas y administrativas para reducir o evitar los riesgos identificados (y aceptar los que no se puedan suprimir). En esta fase, es importante señalar que los medios empleados deben ser adecuados en función de los riesgos que se corren. **El objetivo no es eliminar todos los riesgos, sino, más bien, alcanzar una cota de riesgo residual que resulte aceptable para la organización en relación con estos medios y estos retos**.

La norma IEC 62443 se basa en la instauración de una gobernanza global en torno a una política de seguridad que tenga como objetivo proteger los activos sensibles de un sistema de automatización y control industrial. Este enfoque facilita la consideración del sistema industrial en su conjunto, incluidas las interconexiones desde sistemas externos, como el sistema de información ofimática.

Mejora de la protección del sistema operativo

La puesta en práctica de la política de seguridad definida en torno a la evaluación de amenazas y riesgos consiste en aplicar medidas técnicas y organizativas en términos de ciberseguridad. Sin embargo, las medidas técnicas de seguridad enumeradas en la norma no son suficientes, incluso si se dirigen por completo a los sistemas de automatización y control industriales;

en efecto, una medida de seguridad técnica se entiende en función del riesgo incurrido y de las limitaciones operativas. Estas limitaciones son especialmente importantes cuando asume la gobernanza el equipo encargado de la seguridad del sistema de información de la empresa. Los equipos informáticos y de fabricación o producción deben trabajar juntos y reunir sus conocimientos y competencias para definir las medidas de seguridad que deben aplicarse.

Finalmente, **el despliegue de las medidas de seguridad, así como su seguimiento regular y su mejora de conformidad con las limitaciones propias de los sistemas de automatización y control industriales, tienen como objetivo mejorar el nivel de protección del sistema operativo.**

Gobernanza

Los equipos informáticos y de fabricación o producción deben trabajar conjuntamente.

ESTRUCTURA DE LA NORMA

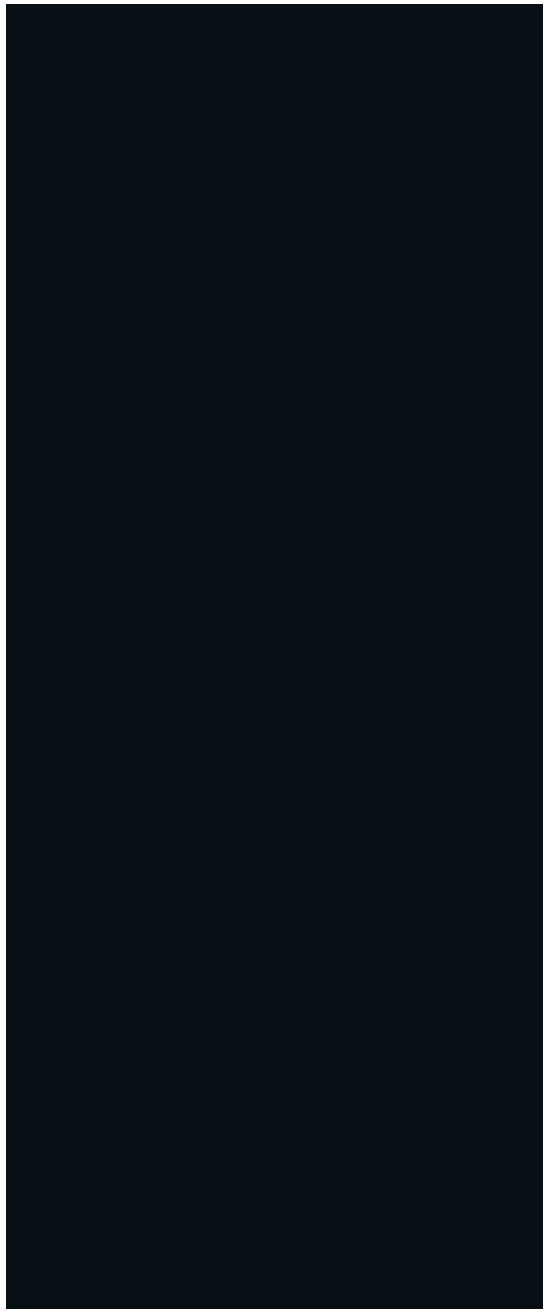
GENERAL	**IEC-62443-1-1** Terminología, concepto y modelos	**IEC-62443-1-2** Glosario principal de términos y abreviaturas	**IEC-62443-1-3** Medidas de conformidad del sistema de seguridad	**IEC-62443-1-4** Ciclo de vida y caso de uso de la seguridad IACS
POLÍTICAS Y PROCEDIMIENTO	**IEC-62443-2-1** Requisitos para un sistema de gestión de la seguridad IACS	**IEC-62443-2-2** Guía de implantación de un sistema de gestión de la seguridad IACS	**IEC-62443-2-3** Gestión de parches en un entorno IACS	**IEC-62443-2-4** Requisitos de instalación y mantenimiento para un proveedor de
SISTEMAS IACS	**IEC-62443-3-1** Tecnologías de seguridad de IACS	**IEC-62443-3-2** Niveles de seguridad para zonas y conductos	**IEC-62443-3-3** Requisitos del sistema de seguridad y niveles de seguridad	
A NIVEL DE COMPONENTE	**IEC-62443-4-1** Requisitos de desarrollo de los productos	**IEC-62443-4-2** Requisitos técnicos de seguridad para los componentes IACS		

La norma IEC-62443-1-x introduce los conceptos principales de la norma IEC 62443. Entre ellos figuran los principios relativos a la gobernanza y la gestión de riesgos.

La norma IEC-62443-2-x describe los elementos necesarios para una gobernanza de gestión de ciberseguridad para un sistema de automatización y control industrial.
En particular, ofrece orientaciones relativas a la manera de desarrollar estos elementos.

La norma IEC-62443-3-x presenta los conceptos básicos para entender la gestión de riesgos cibernéticos de sistemas de automatización y control industriales.

La norma IEC-62443-4-x describe las buenas prácticas de desarrollo de productos para sistemas de automatización y control industriales y, principalmente, el ciclo de vida del desarrollo de productos, así como las funciones de seguridad que deben implantarse.



IEC 62443
ISO 27001

Aunque estas dos normas tienen el mismo objetivo, que es la protección de un sistema de información, presentan diferencias en cuanto a las acciones que deben aplicarse, así como en el objetivo de los sistemas que reciben protección y los elementos que pueden certificarse.

Con el fin de asegurar los sistemas de automatización y control industriales, **la norma IEC 62443 define la política, los procedimientos y los medios de protección que deben aplicarse**. Aunque la norma recomienda tener en cuenta el sistema de información en su conjunto a través de un programa de seguridad, está principalmente centrada en los sistemas operativos. Además, favorece su despliegue con la propuesta de certificación de productos, sistemas, procesos de desarrollo o la organización.

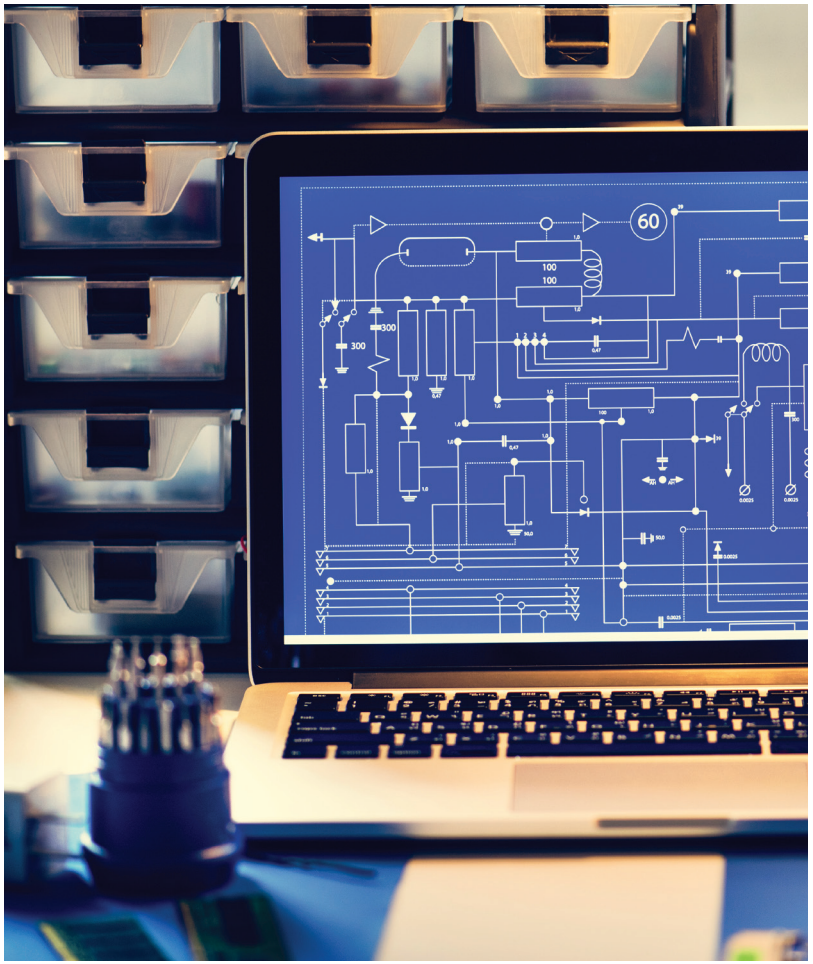
La norma ISO 27001 es un sistema de gestión que propone una certificación más global, ya que precisa más los procedimientos que deben aplicarse para definir y efectuar un seguimiento temporal de la política de seguridad del sistema de información de la organización.

Resumen

Las dos normas son complementarias en el sentido de que las buenas prácticas de gestión de la seguridad de un sistema de información de la norma ISO 27001 pueden servir para las acciones y procedimientos desplegados en el marco de la conformidad con la norma IEC 62443.









IEC 62443



La defensa en profundidad

Por lo general, no es posible alcanzar los objetivos de seguridad por medio de una única técnica o contramedida. El enfoque **de defensa en profundidad consiste en desplegar en cascada múltiples medios de protección o contramedidas**. El ejemplo siguiente presenta diferentes medios desplegados en varios niveles, desde la gobernanza hasta la seguridad de datos, sin olvidar la periferia o incluso los equipos del sistema industrial.

Política específica de los ICS, estándares, procedimiento, sensibilización	• PSS • Estándares • Procedimientos	• Formación • PCA (Plan de continuidad de actividad) • PRA (Plan de recuperación de la actividad)
Seguridad física	• Vigilancia • Control de acceso	
Seguridad perimetral	• Cortafuegos • DMZ • VPN • IDS/IPS	
Seguridad de la red	• Zonas y conductos • Segmentación de la red • DMZ interno	• Cortafuegos sobre el terreno
Seguridad de los equipos	• Gestión de parches • Refuerzo de los puestos • Control de puertos	• Control de accesos • Supervisión continua • Auditoría
Seguridad de aplicaciones	• Control de acceso • Autenticación • Gestión de contraseñas	• Gestión de actualizaciones
Seguridad de los datos	• Comunicaciones seguras (cifrado) • Autenticación • Seguridad de los terminales	

Zonas de seguridad

En infraestructuras complejas o de gran envergadura, no todos los componentes tienen necesariamente el mismo nivel de seguridad; lo que se impone es la necesidad de crear zonas que agrupen los equipos con el mismo nivel de seguridad.

Por lo tanto, una zona de seguridad es una agrupación lógica de activos que comparten los mismos requisitos de seguridad. Las zonas pueden jerarquizarse para incluir zonas en el seno de otras zonas, o subzonas, para brindar seguridad a varios niveles. Este concepto constituye uno de los fundamentos de la defensa en profundidad.

Una zona de seguridad tiene una frontera que requiere la definición de las comunicaciones y los accesos necesarios para permitir que la información y las personas se desplacen dentro de las zonas de seguridad y entre ellas.

La definición de una zona de seguridad **se basa en la evaluación de los requisitos de seguridad, por medio de la cual se determina si un activo particular debe considerarse dentro o fuera de la zona**. Esta elección se basa en el tipo de acceso al activo, que puede ser físico o en forma de comunicación.

Zonas de seguridad

Dos maneras de definir

1 Física:

para activos que se encuentran en un mismo lugar.

2 Lógica o virtual:

para activos que comparten la misma funcionalidad u otras características.

Conductos

El concepto de «conductos» permite abarcar las exigencias de seguridad de los accesos a los activos mediante comunicaciones. Regulan las conexiones de activos dentro de una zona o entre diferentes zonas. Se trata, en efecto, de un **tipo especial de zona de seguridad llamado «canal de comunicación»** que agrupa comunicaciones constituidas por flujos de información. Por lo tanto, los conductos pueden ser físicos, como un cable de red, o lógicos cuando diferentes flujos de información comparten el mismo nivel de seguridad.

Casos que deben tenerse en cuenta al definir de los requisitos de seguridad

El conducto no atraviesa los límites de la zona: generalmente, se aprueba por medio de los procesos de comunicación en la propia zona.

Un conducto de confianza cruza los límites de la zona: debe utilizar un proceso seguro de extremo a extremo.



Niveles de seguridad

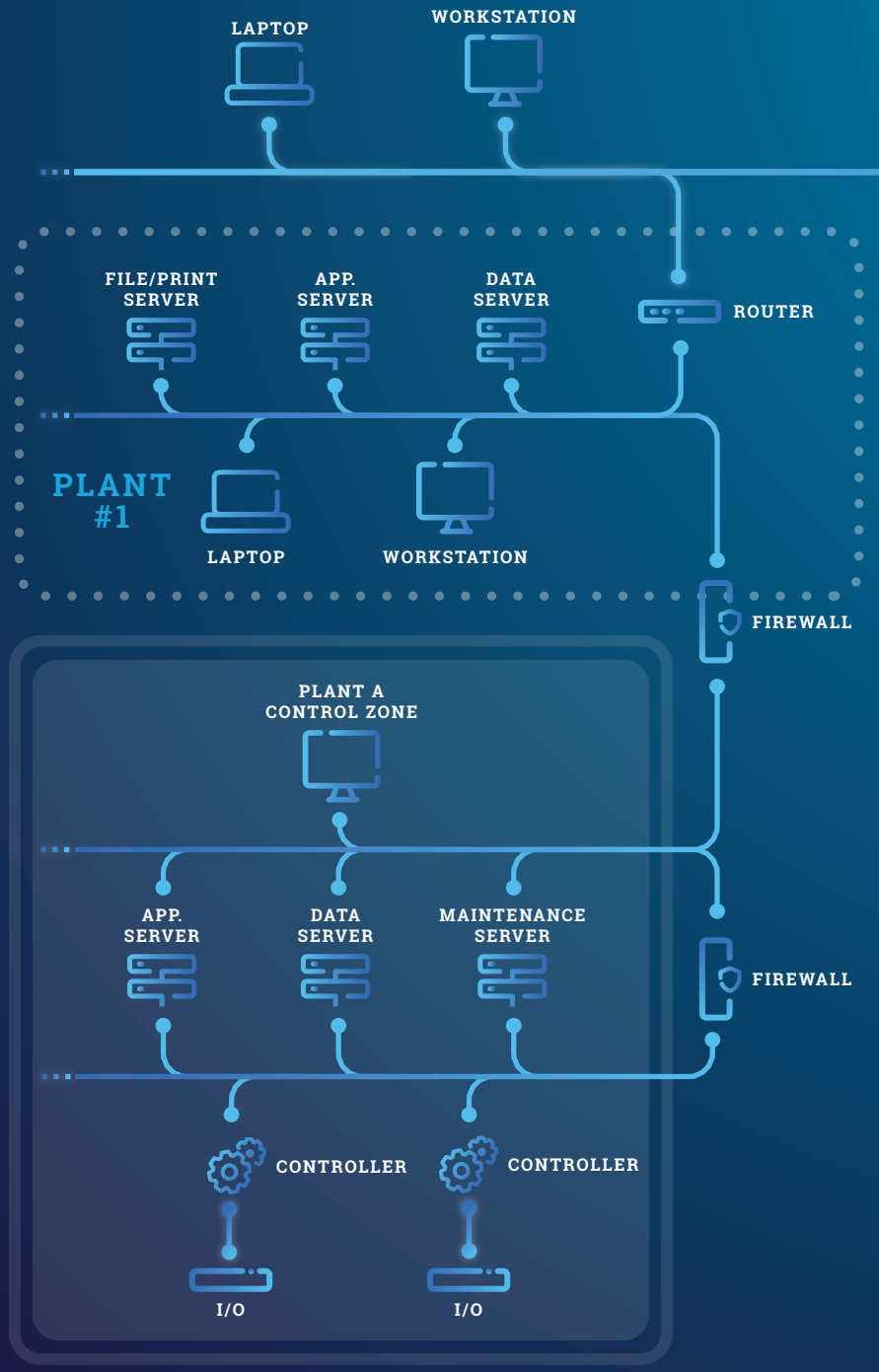
La implantación de una gobernanza de gestión de riesgos se basa en un proceso de evaluación de las amenazas sobre los activos distribuidos por zonas, en función del nivel de protección esperado. Para facilitar el despliegue de las contramedidas o incluso de los medios técnicos y organizativos, los objetivos de seguridad de la norma IEC 62443 proponen **diferentes niveles de seguridad que permiten disponer de un enfoque cualitativo**, con el fin de garantizar la seguridad esperada por cada zona.

Los niveles de seguridad se definen en función de los criterios específicos de cada tipo de amenaza, como las competencias, los medios o los recursos necesarios para llevar a cabo un ataque. La siguiente tabla describe los cuatro niveles de seguridad esperados en función de las amenazas que se puedan contrarrestar.

Nivel de seguridad	Objetivos	Competencias	Motivaciones	Medios	Recursos
1	Infracciones ocasionales o accidentales	Sin competencias en materia de ataques	Errores	Actos no intencionales	Limitados a un individuo
2	Ciberdelincuencia, piratería	Carácter genérico	Débiles	Simples	Débiles (individuo aislado)
3	Hacktivismo terrorista	Específicos para los sistemas de control industrial	Nivel moderado	Carácter sofisticado (ataque)	Nivel moderado (banda de piratas)
4	Nación/Estado	Específicos para los sistemas de control industrial	Nivel elevado	Carácter sofisticado (campaña)	Carácter amplio (equipo multidisciplinar)

EJEMPLO DE SEGMENTACIÓN POR ZONAS Y CONDUCTOS

La figura adjunta representa una organización compuesta por tres fábricas con sede independiente.
Las tres fábricas están conectadas a la red de la empresa para permitir las comunicaciones con la sede central y las demás fábricas.

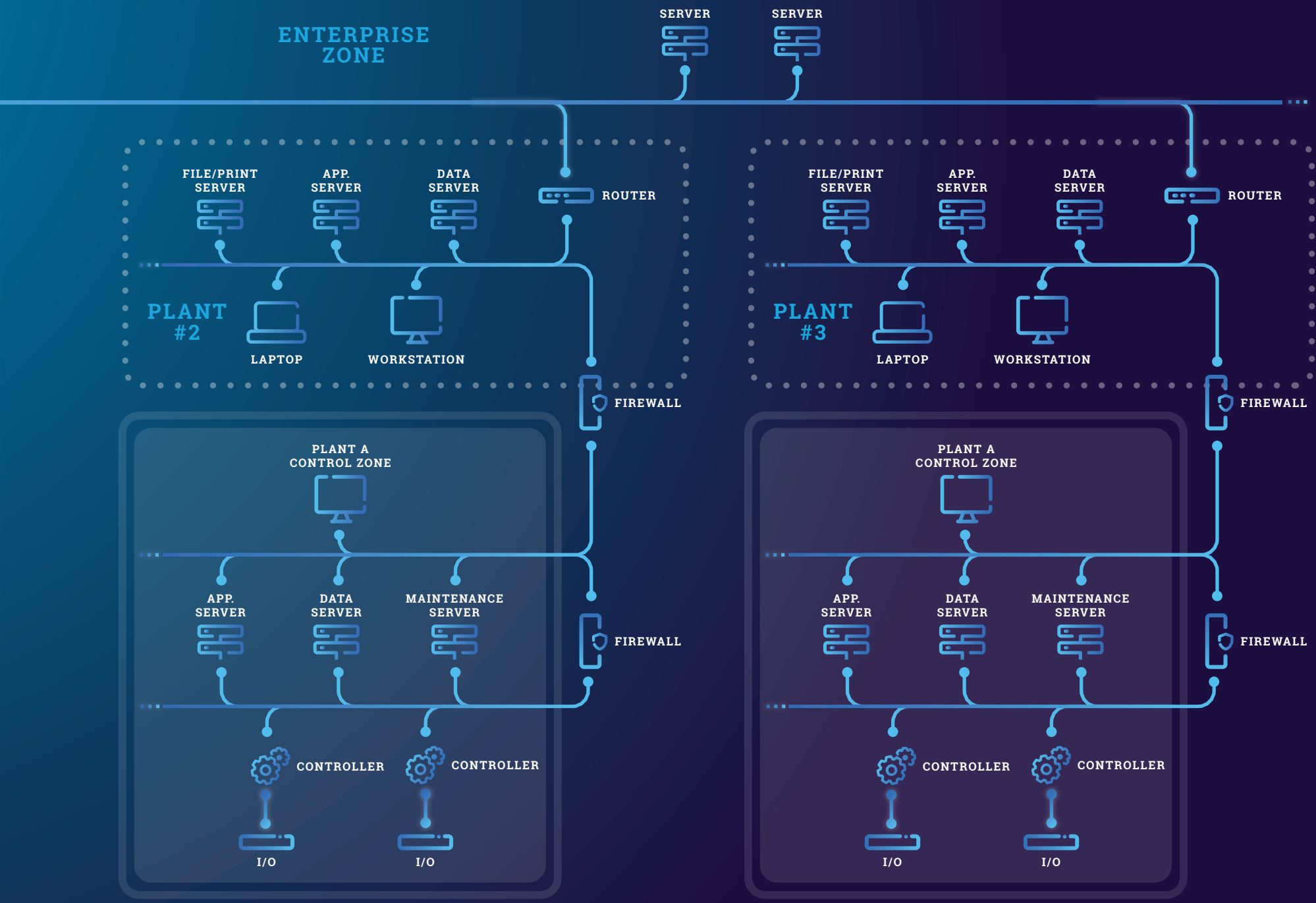


En el dibujo se definen cuatro posibles conductos (podrían definirse otros, pero se ignoran en aras de la concisión).

El primero es el conducto de empresa, que aparece ilustrado en la parte superior de la figura. Este conecta varias fábricas, ubicadas en diferentes lugares, con el centro de datos de la empresa. Si la red de área extendida (WAN) se construye utilizando comunicaciones arrendadas o privadas, puede considerarse un canal de confianza.

Si se utilizan redes públicas y privadas a la vez, el canal puede considerarse como no confiable. El conducto incluye todos los equipos de comunicación y los cortafuegos que constituyen las conexiones de la fábrica.

En cada fábrica, se muestran instancias de la segunda clase de conductos. En este caso, cada una de las fábricas dispone de su propio canal de confianza para permitir la comunicación de control.


ENTERPRISE ZONE
SERVER
SERVER
FILE/PRINT SERVER
APP. SERVER
DATA SERVER
ROUTER
PLANT #2
LAPTOP
WORKSTATION
FIREWALL
PLANT A CONTROL ZONE
APP. SERVER
DATA SERVER
MAINTENANCE SERVER
FIREWALL
CONTROLLER
CONTROLLER
I/O
I/O
FILE/PRINT SERVER
APP. SERVER
DATA SERVER
ROUTER
PLANT #3
LAPTOP
WORKSTATION
FIREWALL
PLANT A CONTROL ZONE
APP. SERVER
DATA SERVER
MAINTENANCE SERVER
FIREWALL
CONTROLLER
CONTROLLER
I/O
I/O

Los 7 requisitos fundamentales

Las diferentes medidas de seguridad que deben adoptarse en relación con la gobernanza de gestión de riesgos que propone por la norma IEC 62443 se distribuyen por familias.

1

Control de la identificación y de la autenticación

FR1

Identificación y autenticación de todos los usuarios (personas, procesos de software y dispositivos) antes de autorizar el acceso al sistema.

2

Control del uso

FR2

Cumplimiento de los privilegios asignados a un usuario autentificado (personas, proceso de software o dispositivo).

3

Integridad del sistema

FR3

Aseguramiento de la integridad de los datos, el software y los equipos.

4

Confidencialidad de los datos

FR4

Aseguramiento de la confidencialidad de la información sobre los flujos de comunicación, así como en los espacios de almacenamiento de datos.

5

Restricción de flujos de datos

FR5

Segmentación del sistema de control por zonas y conductos para limitar los flujos innecesarios de datos.

6

Respuesta a los eventos dentro de los plazos

FR6

Respuesta a los ataques con notificación a la autoridad competente, con la transmisión de las pruebas necesarias de la infracción y la adopción de medidas correctivas oportunas cuando se detectan incidentes.

7

Disponibilidad de recursos

FR7

Aseguramiento de la resistencia del sistema a distintos tipos de eventos DoS. Esto incluye la indisponibilidad parcial o total de las funciones del sistema en varios niveles

La rama de certificación IEC 62443-4

La rama de certificación IEC 62443-4 certifica que un producto (material, componente o sistema) cumple con los requisitos descritos en la parte 62443-4 de la norma IEC 62443. Por lo tanto, esta parte de la norma se refiere a los productos que se implantan y se utilizan en los sistemas de automatización y control industriales.

Existen dos tipos distintos de certificación:

IEC 62443-4-1, que se centra en el proceso de desarrollo de productos de seguridad.

IEC 62443-4-2, que se relaciona con la conformidad con los siete requisitos fundamentales descritos en la parte IEC 62443-1-1 de la norma.



Especificaciones IEC 62443-4-1

Esta parte de la norma especifica los requisitos para garantizar un ciclo de vida de desarrollo seguro. El objetivo principal de estos requisitos es **brindar un marco que permita adoptar un enfoque de seguridad y defensa en profundidad** para el diseño, la construcción, el mantenimiento y la retirada de los productos utilizados en los sistemas de automatización y control industriales.

La certificación IEC 62443-4-1 abarca los siguientes aspectos principales:

Proceso de desarrollo seguro
para establecer y mantener el programa de desarrollo seguro durante todo el ciclo de vida del desarrollo del producto.

Gestión de riesgos
para facilitar directrices encaminadas a identificar, evaluar y gestionar los riesgos de seguridad asociados a los productos y sistemas.

Conformidad con las mejores prácticas
para fomentar la adopción de mejores prácticas de gestión de la seguridad del software y el hardware empleados en sistemas industriales.

Seguridad por diseño
para hacer hincapié en la integración de la seguridad en todas las fases de creación de los productos, desde el diseño hasta las pruebas y el mantenimiento.

Documentación y trazabilidad
para definir el nivel de exigencia de una documentación adecuada, así como la trazabilidad de los procesos de desarrollo y de las medidas de seguridad implantadas.

BENEFICIOS ESPERADOS

Los usuarios de productos certificados tienen la seguridad de disponer de un producto diseñado, producido y mantenido con un nivel óptimo de seguridad. De hecho, esta certificación abarca todos los procesos de desarrollo de software a través de ocho grandes ámbitos:

1

La gestión de la seguridad, que incluye, por ejemplo, el proceso de desarrollo, las responsabilidades o la gestión de las claves privadas.

2

La definición de las necesidades de seguridad, con un modelo de amenazas y un análisis de riesgo.

3

La seguridad By Design, que incluye los principios de arquitectura y diseño seguros.

4

Seguridad de la implementación a través de buenas prácticas de codificación.

5

Pruebas y verificación con el objetivo de asegurar que la implantación sea correcta, que incluyen tests de intrusión y de vulnerabilidades.

6

Gestión de incidentes de seguridad y vulnerabilidades detectadas.

7

Gestión de actualizaciones, salidas de versiones correctivas, documentación y procedimientos de información.

8

La documentación de las reglas de seguridad para garantizar un despliegue eficaz de la solución en el entorno objetivo, con guías de refuerzo, documentos de uso e incluso procedimientos de borrado seguros.

La certificación IEC 62443-4-1 permite alinear el proceso de desarrollo de productos con las elevadas necesidades de seguridad de los usuarios de productos de automatización industrial y sistemas de control. Estos usuarios pueden beneficiarse de las configuraciones de seguridad y los procedimientos de gestión de parches bien documentados con una comunicación clara y sucinta sobre las vulnerabilidades de seguridad detectadas en el producto.

Stormshield le acompaña

Stormshield acompaña a los sistemas de automatización y control industriales de cara a su conformidad con la norma IEC 62443 a través de tres gamas de productos que garantizan la protección periférica, de los puestos de trabajo y de los datos de extremo a extremo.

Con la certificación IEC 62443-4-1, la gama Stormshield Network Security garantiza la puesta a disposición de un producto diseñado, producido y mantenido con un nivel óptimo de seguridad. Por otro lado, las funciones de las diferentes soluciones Stormshield ofrecen una inestimable ayuda para responder a los siete requisitos fundamentales de la norma:

FR1: Identificación, control de autenticación (IAC)

La solución Stormshield Network Security permite identificar tanto las redes (incluida la de wifi) como las máquinas y los usuarios, al tiempo que integra los controles de acceso asociados en la política de seguridad.

Las funciones de gestión y autenticación de los usuarios ofrecen una gran flexibilidad que garantiza la recuperación de los datos del directorio de la empresa o la implantación de una infraestructura autónoma y completa, lo que permite la gestión de usuarios externos.

FR2: Control de utilización (UC)

La mayor parte de los controles de uso se basan en la política de seguridad definida en la protección periférica. La solución Stormshield Network Security va más allá de las operaciones de segregación o segmentación de red, de restricción de acceso (wifi o dispositivos móviles) o de control de sesiones. De hecho, la solución también permite limitar la duración de las sesiones, terminar las conexiones a distancia o incluso interceptar y bloquear los códigos móviles maliciosos.

Por otro lado, la solución de gestión de eventos del sistema de Stormshield garantiza la puesta en marcha de operaciones de auditoría seguras sobre las acciones realizadas en los sistemas de automatización y control industriales.

FR3: Integridad del sistema (SI)

Los controles de integridad del sistema, como la protección contra códigos maliciosos, están asegurados por las soluciones de protección de red y seguridad de los puestos de trabajo. Además, ambas soluciones son capaces de poner en marcha acciones de remediación predefinidas a través de su política de seguridad.

Por su parte, la solución Stormshield Network Security garantiza la integridad de las comunicaciones y sesiones, así como la verificación de los códigos de acción enviados a los autómatas, gracias a su análisis de paquetes en profundidad.

De la protección contra las modificaciones se encargan la solución Stormshield Endpoint Security en las aplicaciones del sistema y la solución Stormshield Data Security para la integridad de la información.

Finalmente, es posible proteger la información de auditoría mediante el envío simultáneo de registros a varios servidores.

FR4: Confidencialidad de los datos (DC)

El acceso a la información está garantizado tanto para los datos en tránsito, con las comunicaciones seguras de Stormshield Network Security, como para los datos almacenados, gracias a la solución de protección de datos Stormshield Data Security.

Los mecanismos de cifrado empleados por estas soluciones están cualificados al más alto nivel europeo y garantizan la gestión de los recursos que no tienen que acceder a la información después de su desactivación.

FR5: Restricción de flujos de datos (RDF)

La gestión de flujos de datos garantiza la conformidad de los sistemas de automatización y control industriales con los requisitos relativos a las zonas de seguridad y los conductos. Las funciones de enrutamiento y control de flujo de red hasta el nivel de aplicación de la solución Stormshield Network Security garantizan, por sí solas, una respuesta óptima a todos los requisitos de seguridad.

Son capaces de garantizar la segmentación de la red, la protección de las fronteras de las zonas de seguridad y el control de los mensajes salientes a través de un mecanismo de bloqueo por defecto de los flujos para autorizar únicamente las comunicaciones autorizadas.

FR6: Respuesta oportuna a los eventos (TRE)

Cada producto de Stormshield ofrece registros de eventos que permiten llevar a cabo un seguimiento de las acciones realizadas en el sistema de automatización y control industrial, los datos de red que transitan por él y las alertas de seguridad generadas.

El acceso de solo lectura a estos registros garantiza una supervisión continua de los eventos únicamente por parte de las personas autorizadas. Además, la solución Stormshield Log Supervisor garantiza una gestión eficaz de los incidentes de seguridad.

FR7: Disponibilidad de recursos (RA)

La disponibilidad de recursos se refiere a los requisitos relativos a la gestión de las denegaciones o de las degradaciones de servicio. Dichos requisitos están cubiertos por las soluciones Stormshield Network Security y Stormshield Endpoint Security para la gestión de copias de seguridad y restauración, para la configuración de las funciones de seguridad y para la gestión de los límites de uso de recursos.

Además, la solución Stormshield Network Security ofrece protección de red contra ataques de denegación de servicio y redundancia de fuente de alimentación, lo que permite cambiar a una red de energía secundaria si es necesario.



Los aspectos clave del acompañamiento de Stormshield

Stormshield, uno de los principales actores de la ciberseguridad industrial a nivel europeo desde hace 10 años, ofrece soluciones completas y adaptadas a los sistemas de automatización y control industriales. Sus equipos de expertos en ciberseguridad industrial están a su disposición para acompañarle en todas las fases de su proyecto industrial. Gracias a su formación experta, están en condiciones de ayudar a sus equipos operativos a desarrollar competencias en relación con las buenas prácticas que deben adoptarse en materia de ciberseguridad.

Las tres gamas de productos Stormshield cumplen todas las reglas de seguridad de los siete requisitos fundamentales de la norma. Así, acompañan a los sistemas de automatización y control industriales de cara a su conformidad con la norma IEC 62443 con la garantía de protección periférica, protección de los puestos de trabajo y protección de extremo a extremo de los datos.

Tres aspectos principales

La gama Stormshield Network Security, única solución puramente cibernética con certificación IEC 62443-4-1, garantiza el despliegue de productos diseñados, producidos y mantenidos con un nivel de seguridad óptimo.

Además de garantizar el cumplimiento de un proceso de desarrollo conforme a los requisitos de la norma, los productos Stormshield Network Security se desmarcan de sus principales competidores por tres aspectos principales.

Integración transparente en la infraestructura existente

La segmentación en subred combinada con el modo híbrido (enrutamiento + modo transparente) garantiza una interconexión segura entre los equipos, capaz de aislar los activos más críticos para controlar mejor los flujos dentro del sistema de automatización y control industrial.

El modo híbrido permite la implantación de funciones de enrutamiento y segmentación de red, lo que limita los cambios en la infraestructura operativa existente.

La riqueza de las configuraciones posibles ofrece compatibilidad con una gran variedad de arquitecturas, lo que garantiza una integración transparente de los cortafuegos en la infraestructura existente.

Inspección en profundidad de flujos de pedido

El motor de prevención de intrusiones ofrece un análisis profundo (DPI, del inglés ***Deep Packet Inspection***) de las comunicaciones dentro del sistema industrial.
Este análisis garantiza un control de conformidad protocolar, una protección contra códigos maliciosos y un análisis preciso de los mensajes intercambiados entre los autómatas y las capas superiores de gestión (supervisión/SCADA).
El enfoque innovador de este análisis garantiza un control preciso de los mensajes enviados a los autómatas de control para garantizar una gestión granular de las acciones autorizadas. Además, es posible aumentar el nivel de protección mediante la limitación de comandos y valores transmitidos (velocidad, presión, cantidad), a fin de restringir los comportamientos anormales o las desviaciones del proceso industrial.

Certificación al más alto nivel europeo

La certificación IEC 62443-4-1 demuestra el compromiso de Stormshield con su cometido de ofrecer productos de confianza para sistemas industriales. La confianza que brinda este sello también se refleja en la certificación de criterios comunes de los productos Stormshield, reconocida por varios agentes europeos. Este reconocimiento de productos calificados (OTAN o restringido de la UE) demuestra que los productos Stormshield están certificados al más alto nivel europeo.

Es así como la oferta de Stormshield, sustentada sobre productos certificados, garantiza la confianza mutua en los mensajes que se intercambian entre los distintos componentes del sistema. Las soluciones 100 % europeas de Stormshield contribuyen a la seguridad y soberanía de sus activos sensibles para mantener el control en todo momento.


STORMSHIELD
Stormshield response to IEC 62443 standard

To facilitate the implementation of countermeasures or technical and organisational solutions, the security objectives of standard IEC 62443 offer **different levels of security for a quality-driven approach** to deliver the expected security for each zone.

The security levels are defined according to the criteria specific to each type of threat, such as the skills, means or resources required to conduct an attack. The table below describes the 4 expected security levels according to the threats that can be countered.

Level of security	Targets	Skills	Reasons	Means	Resources
1	Occasional or accidental breaches	No expertise with regard to attacks	Errors	Unintentional acts	Limited to one individual
2	Cybercrime, hacker	Generic	Low	Simple	Low (isolated individual)
3	Hacktivist, terrorist	Specific to industrial control systems	Moderate	Sophisticated (attack)	Moderate (group of hackers)
4	Nation/State	Specific to industrial control systems	High	Sophisticated (campaign)	Extended (multidisciplinary team)

FR1: Identification, authentication control, and Access Control (AC)

Foundational requirements		Reached Security level	Stormshield answer
1.1	**Human user identification and authentication**	SL1 SL2 SL3 SL4	Stormshield provide multiple method for user authentication even with MFA for traffic accessing the firewall itself and also for traffic traversing the firewall. If a device doesn't support authentication it is possible to directly plug it in the firewall and use the authentication features (portal or SSL VPN).
1.2	**Software process and device identification and authentication**	SL1 SL2 SL3 SL4	Stormshield is able to create policy based on MAC addresses.
1.3	**Account management**	SL1 SL2 SL3 SL4	Stormshield provide individual or group account based on Internal LDAP, External LDAP, Multiple AD or Radius. It is possible to assign different granularities to different users or group of users.
1.4	**Identifier management**	SL1 SL2 SL3 SL4	Stormshield can assign different role to each user.
1.5	**Authenticator management**	SL1 SL2 SL3 SL4	Stormshield is able to force users to be authenticated on an internal or external database. It is possible to set a password lifetime and force the modification of the password at connection.
1.6	**Wireless access management**	SL1 SL2 SL3 SL4	Stormshield does not support WIFI but thanks to his hybrid mode, it is possible to connect a WIFI network to a dedicated port. Even if the WIFI network is sharing the same address space, in order to pass from the WIFI to the physical network it is possible to force authentication and IPS analysis.
1.7	**Strength of password-based authentication**	SL1 SL2 SL3 SL4	It is possible to force the length; entropy and characters type of a password on both firewall administrator and end user accounts.
1.8	**Public Key Infrastructure (PKI) certificates**	SL1 SL2	Stormshield provide on each firewall a PKI but it can also be integrated with an external PKI.
1.9	**Strength of public key authentication**	SL1 SL2 SL3 SL4	Stormshield provide the check of the validity of a certificate as well as the CRL. It checks also the validity of the CA releasing the certificates.
1.10	**Authenticator feedback**	SL1 SL3 SL4	Password are obscured during the authentication process.
1.11	**Unsuccessful login attempts**	SL1 SL2 SL3 SL4	Unsuccessful login attempts are stored in a dedicated log called l_auth and visible in the GUI. Moreover, the network intrusion prevention capabilities detects them on SSH and LDAP systems.
1.12	**System use notification**	SL1 SL2 SL3 SL4	It is possible to display a custom disclaimer on accessing the firewall.
1.13	**Access via untrusted networks**	SL1 SL2 SL3 SL4	The access to the device or to the internal network from untrusted networks can be filtered based on several methods like users, networks, geolocation or ip-reputations.

FR2: Use Control (UC)

Foundational requirements		Reached Security level	Stormshield answer
2.1	**Authorization enforcement**	SL1 SL2 SL3 SL4	Stormshield is able to assign different authentication rules to different port in order to define different policies according to the origin of the incoming connection. For the traffic directed to the firewall it is possible to create permission READ/WRITE according to the role. For the traffic passing through the firewall it is possible to create template of authorized industrial protocols commands ad assign it to different users.
2.2	**Wireless use control**	SL1 SL2 SL3 SL4	Stormshield firewalls helps to connect a wireless access point to the device and to force the authentication to access the other segment of the network. Stormshield Endpoint Security agent is able to only accept access for predefined wifi networks.
2.3	**Use control for portable and mobile devices**	SL1 SL2 SL3 SL4	Thanks to the BYOD signatures it is possible to authorize or block particular devices. It is also possible to force the mobile devices to open a secure channel to access the internal network, in this way it is possible to create user defined policies.
2.4	**Mobile code**	SL1 SL2 SL3 SL4	Stormshield is able to intercept and analyze the mobile code usage and prevent malicious activity.
2.5	**Session lock**	SL1 SL2 SL3 SL4	For authenticated users it is possible to define the Authentication periods that are allowed.
2.6	**Remote session termination**	SL1 SL2 SL3 SL4	It is possible to terminate a remote session for timeout after inactivity, manually by the user or to force it by a superuser
2.7	**Concurrent session control**	SL1 SL2 SL3 SL4	It is possible to control the concurrent session blocking the simultaneous connections from multiple host.
2.8	**Auditable events**	SL1 SL2	All the system and user access events are configurable and for each one it is possible to send email; event logs; generate alerts
2.9	**Audit storage capacity**	SL1 SL2 SL3 SL4	When the storage reaches a certain threshold, the administrator is warned by SNMP, MAIL or Alert. In any case the logs are rotated. Disk usage is in any case managed via SNMP.
2.10	**Response to audit processing failures**	SL1 SL3 SL4	To prevent audit processing failures Stormshield is able to store logs locally and send them to 4 different Syslog servers at the same time.
2.11	**Timestamps**	SL1 SL2 SL3 SL4	All the logs and system events are timestamped. Timestamp can be synchronized with internal clock or external NTP server.
2.12	**Nonrepudiation**	SL1 SL2 SL3 SL4	On the firewall itself all the logs are nominatives and it is possible to know if a user has modified a rule and when.

FR3: System Integrity (SI)

Foundational requirements		Reached Security level	Stormshield answer
3.1	**Communication integrity**	SL1 SL2 SL3 SL4	Stormshield provide multiple techniques to provide communication integrity. On certain industrial protocols traversing the firewall the IPS engine will store the status of the communication and it will try to detect any malicious attempt to inject packets in the a MIDM attack. In case of a firewall managing multiple port on the same network the device is able to block traffic with an IP SPOOFING alert if it detects any attempt to substitute a legit IP. Stormshield can also provide the possibility to create transparent layer2 IPSEC VPN. In this way it is possible to cypher the layer2 communications with any device not natively supporting this feature.
3.2	**Malicious code protection**	SL1 SL2 SL3 SL4	Stormshield have an entire set of signatures to intercept and block malicious code.
3.3	**Security functionality verification**	SL1 SL2 SL3 SL4	It is possible to artificially trig an event thanks to the command SENDALARM. It is also possible to artificially inject logs in the system in order to test the connection with external SIEM and audit platform.
3.4	**Software and information integrity**	SL1 SL2 SL3 SL4	All the code running on the firewall is signed and an attempt to modify it, will lead to an error in boot phase.
3.5	**Input validation**	SL1 SL2 SL3 SL4	The industrial plugin system is analyzing each industrial command in order to validate his conformity with the RFC and with the user requirements. A packet that is not validated is automatically blocked.
3.6	**Deterministic output**	SL1 SL2 SL3 SL4	This point is more related about the development methodology, but referring to the operation on the firewall itself we can say that: It is possible to configure the reaction to each type of attack: IPS: Detect an attack and block it IDS: Detect an attack and logs it without to block it FW: ignore the attack and continue with normal operations This behavior can be defined for each security policy.
3.7	**Error handling**	SL1 SL2 SL3 SL4	This point is more related about the development methodology, but referring to the operation on the firewall itself we can say that: When an administrator adds a security policy the whole policy chain is checked and in case an anomaly is detected it is prompted to the administrator .
3.8	**Session integrity**	SL1 SL2	For the access to the firewall itself: only one user at a time has the power to modify the configuration if another user attempt to modify a configuration that is already edited by another administrator he has to request the administrative privileges to operate.
3.9	**Protection of audit information**	SL1 SL2 SL3 SL4	Logs are backed up thanks to the support of up to 4 external syslog. On certain models there are redundant disks.

FR4: Data Confidentiality (DC)

Foundational requirements		Reached Security level	Stormshield answer
4.1	**Information confidentiality**	SL1 SL2 SL3 SL4	Stormshield is able to provide the confidentiality of the information transiting in the network thanks to his VPN support (IPSEC or SSL). If a user has to access to the internal network he can open a secure channel with the Stormshield in order to protect all the information exchanged. The encryption algorithm that are used can vary from user to user and according to the desired security level.
4.2	**Information persistence**	SL1 SL2 SL3 SL4	Stormshield provide SSH commands to purge the logs, to reset the configuration and in generally to delete or sensitive information that could be stored on the appliance.
4.3	**Use of cryptography**	SL1 SL2 SL3 SL4	Stormshield can use Cryptography to provide a secure channel. Cryptography can be defined for each type of communications transiting in the firewall.

FR5: Restricted Data Flow (RDF)

Foundational requirements		Reached Security level	Stormshield answer
5.1	**Network segmentation**	SL1 SL2 SL3 SL4	Stormshield can segment network creating multiple VLAN or portion of network attached to different ports. Even when the network is flat if 2 devices are connected to different port of the firewall it is possible to force the analysis of the data transiting from one port to another, creating a kind of virtual segmentation.
5.2	**Zone boundary protection**	SL1 SL2 SL3 SL4	The objects of Stormshield firewall (network, host, ranges) helps to managed the assets of the differents security zones. By using them in the security policies you can define the communication rules between security zones.
5.3	**General-purpose person-to-person communication restrictions**	SL1 SL2 SL3 SL4	Stormshield is able to filter out social media, mail and instant messaging applications.
5.4	**Application partitioning**	SL1 SL2 SL3 SL4	It is possible to create a template of allowed applications and assign the template to a specific SOURCE zone in direction to a specific DESTINATION Zone.

FR6: Timely Response to Events (TRE)

Foundational requirements		Reached Security level	Stormshield answer
6.1	**Audit log accessibility**	SL1 SL2 SL3 SL4	Each firewall provides a clear and intuitive web interface to access the logs. It is possible to select a security policy to see all the log generated or to jump from a security policy to a log. Logs are also displayed in graphical format to be more intuitive.
6.2	**Continuous monitoring**	SL1 SL2 SL3 SL4	Stormshield provide a real-time monitoring interface where it is possible to keep under control the usage of the resources or the status of the connections and user authenticated as well as the status of the encrypted channels.

FR7: Resource Availability (RA)

Foundational requirements		Reached Security level	Stormshield answer
7.1	**DoS protection**	SL1 SL2 SL3 SL4	Stormshield provide a dedicated DOS detection and protection mechanism that is fully configurable.
7.2	**Resource management**	SL1 SL2 SL3 SL4	Stormshield firewalls are developed with an internal watchdogs and multiple core to prevent that an intensive usage of a resource is going to impact the overall performance of the device.
7.3	**Control system backup**	SL1 SL2 SL3 SL4	Stormshield provide multiple backup functionalities From Active to Backup partition to have always a fully working backup on the sale firewall (useful in case of update) Cloud backup: to have always a copy of the backup in Stormshield partner are Custom Backup: to create you own cloud backup service SMC: It is possible to manage multiple firewalls with a central console, in this case it is possible to centralize the backups on SMC Stormshield Management Center
7.4	**Control system recovery and reconstitution**	SL1 SL2 SL3 SL4	It is possible to recover and restore for a backup even on different platform. It is also possible to restore from the backup partition on the same device.
7.5	**Emergency power**	SL1 SL2 SL3 SL4	Stormshield SNi20 and SNi40 can work on pass-on-fail mode. If configured in transparent way it is possible to simulate the behavior of a wire in case of issue in this way the access to the OT device is always guarantee. Stormshield supports also HA, when something happens to the Master firewall a Slave can take his place and keep all the active sessions.
7.6	**Network and security configuration settings**	SL1 SL2 SL3 SL4	Stormshield provide the possibility to export configuration in CSV format for a detailed of-site analysis.
7.7	**Least functionality**	SL1 SL2 SL3 SL4	Stormshield allows the creation of security policy based on port, protocol, applicative protocols, web service; geolocation; ip-reputation; users By default, the working policy block all the traffic. In this way it is possible to block all and authorize only the essential traffic.
7.8	**Control system component inventory**	SL1 SL2 SL3 SL4	Stormshield firewall are able to analyze the traffic and identify the components involved in the communications and the industrial protocol they are speaking. It is possible to export / Import object in CSV format and to integrate Stormshield with Sensors like Nozomi.

THE **EUROPEAN CHOICE** FOR **CYBERSECURITY**

www.stormshield.com

All distribution, reproduction or representation, even in part, of this white paper, for any purposes other than private use, regardless of the medium, is prohibited, and may engage the civil and criminal liability of any person failing to comply with this prohibition.

Copyright © 2024 Stormshield