Security with SIMATIC controller

SIMATIC S7-300/400/WinAC/1200/1500

https://support.industry.siemens.com/cs/ww/EN/view/77431846

Siemens Industry Online Support

Información legal

Uso de ejemplos de aplicación.

Los ejemplos de aplicación ilustran la solución de tareas de automatización a través de una interacción de varios componentes en forma de módulos de texto, gráficos y/o software. Los ejemplos de aplicación son un servicio gratuito de Siemens AG y/o una filial de Siemens AG ("Siemens"). No son vinculantes y no pretenden ser completos o funcionales con respecto a la configuración y el equipamiento. Los ejemplos de aplicación simplemente ofrecen ayuda con tareas típicas; no constituyen soluciones específicas para el cliente. Usted mismo es responsable del funcionamiento correcto y seguro de los productos de acuerdo con las normas vigentes y también debe verificar la función del ejemplo de aplicación respectivo y personalizarlo para su sistema.

Siemens le otorga el derecho no exclusivo, no sublicenciable e intransferible de que los ejemplos de aplicación sean utilizados por personal técnicamente capacitado. Cualquier cambio en los ejemplos de aplicación es su responsabilidad. Solo se permite compartir los ejemplos de aplicación con terceros o copiar los ejemplos de aplicación o extractos de los mismos en combinación con sus propios productos.
Los ejemplos de aplicación no están obligados a someterse a las pruebas e inspecciones de calidad habituales de un producto facturable; pueden tener defectos funcionales y de rendimiento, así como errores. Es su responsabilidad usarlos de tal manera que cualquier mal funcionamiento que pueda ocurrir no resulte en daños a la propiedad o lesiones a las personas.

Descargo de responsabilidad

Siemens no asumirá ninguna responsabilidad, por ningún motivo legal, incluida, entre otras, la responsabilidad por la usabilidad, disponibilidad, integridad y ausencia de defectos de los ejemplos de aplicación, así como por la información relacionada, los datos de configuración y rendimiento y cualquier daño causado por ello. . Esto no se aplicará en casos de responsabilidad obligatoria, por ejemplo, en virtud de la Ley alemana de responsabilidad por productos defectuosos, o en casos de dolo, negligencia grave o muerte culposa, lesiones corporales o daños a la salud, incumplimiento de una garantía, incumplimiento fraudulento. -revelación de un defecto o incumplimiento culposo de obligaciones contractuales materiales. No obstante, las reclamaciones por daños derivados del incumplimiento de obligaciones contractuales materiales se limitarán a los daños previsibles típicos del tipo de acuerdo, a menos que la responsabilidad surja de dolo o negligencia grave o se base en la pérdida de la vida, lesiones corporales o daños a la salud. Las disposiciones anteriores no implican ningún cambio en la carga de la prueba en su perjuicio. Deberá indemnizar a Siemens frente a reclamaciones existentes o futuras de terceros a este respecto, excepto cuando Siemens sea responsable obligatorio.

Al utilizar los ejemplos de aplicación, reconoce que Siemens no se hace responsable de ningún daño más allá de las disposiciones de responsabilidad descritas.

Otra información

Siemens se reserva el derecho de realizar cambios en los ejemplos de aplicación en cualquier momento sin previo aviso. En caso de discrepancias entre las sugerencias de los ejemplos de aplicación y otras publicaciones de Siemens, como catálogos, prevalecerá el contenido de la otra documentación.

Los términos de uso de Siemens (https://support.industry.siemens.com) también se aplicará.

Informacion de seguridad

Siemens ofrece productos y soluciones con funciones de Seguridad Industrial que respaldan el funcionamiento seguro de plantas, sistemas, máquinas y redes.

Para proteger plantas, sistemas, máquinas y redes contra amenazas cibernéticas, es necesario implementar, y mantener continuamente, un concepto de seguridad industrial holístico y de última generación.
Los productos y soluciones de Siemens constituyen un elemento de dicho concepto.

Los clientes son responsables de evitar el acceso no autorizado a sus plantas, sistemas, máquinas y redes. Dichos sistemas, máquinas y componentes solo deben conectarse a una red empresarial oa Internet si y en la medida en que dicha conexión sea necesaria y solo cuando estén implementadas las medidas de seguridad adecuadas (por ejemplo, cortafuegos y/o segmentación de la red).

Para obtener información adicional sobre las medidas de seguridad industrial que pueden implementarse, visite https://www.siemens.com/industrialsecurity.

Los productos y soluciones de Siemens se someten a un desarrollo continuo para hacerlos más seguros.
Siemens recomienda enfáticamente que las actualizaciones del producto se apliquen tan pronto como estén disponibles y que se utilicen las últimas versiones del producto. El uso de versiones de productos que ya no son compatibles y la falta de aplicación de las últimas actualizaciones puede aumentar la exposición del cliente a las ciberamenazas.

Para mantenerse informado sobre las actualizaciones de productos, suscríbase a la fuente RSS de Siemens Industrial Security en: https://www.siemens.com/industrialsecurity

Tabla de contenido

Información legal..... 2

1 Minimizar el riesgo a través de la seguridad 4

1.1 Estrategias de seguridad..... 4
1.2 Implementación de estrategias en soluciones 5
1.2.1 Fortalecimiento del sentido de la responsabilidad 5
1.2.2 El concepto de protección de Siemens: “Defensa en profundidad” 6
1.3 Diferencias entre seguridad en oficinas y seguridad industrial 7
1.4 Diferencias entre seguridad funcional y seguridad industrial 7
1.5 Gestion de seguridad 8

2 Mecanismos de seguridad de la CPU S7 9

2.1 Bloqueo de protección 9
2.2 Restricciones de funciones y acceso en línea 12
2.3 Protección anticopia (S7-1200 (V4) / S7-1500) 13
2.4 Protección de acceso local (S7-1500) 14
2.5 Otras medidas para proteger la CPU 15

3 Mecanismos de seguridad de los S7-CPs 17

3.1 Cortafuegos de inspección con estado 17
3.2 Codificación de datos a través de VPN 18
3.3 NAT/NAPT (traducción de direcciones)..... 18
3.4 Funciones informáticas seguras 19
3.4.1 Protocolo de transferencia de archivos (FTP) 19
3.4.2 Protocolo de tiempo de red (NTP) 19
3.4.3 Protocolo de transferencia de hipertexto (HTTP) 20
3.4.4 Protocolo simple de administración de redes (SNMP) 20

4 El Programa de Certificación Achilles 21

5 Literatura 22

6 Historia..... 23

1 Minimizar el riesgo a través de la seguridad

El aumento de las redes y el uso de tecnologías probadas del mundo de la oficina en los sistemas de automatización conducen a mayores requisitos de seguridad. No es suficiente ofrecer solo una protección superficial y limitada, ya que los ataques desde el exterior pueden ocurrir en varios niveles. Se requiere una comprensión profunda de la seguridad y cómo aplicarla para una protección óptima.

1.1 Estrategias de seguridad

Motivación

La primera prioridad en la automatización es mantener el control sobre el proceso de producción. Las medidas destinadas a reducir las amenazas a la seguridad no deben interferir con este prioridad. El uso de un concepto de protección adecuado debe garantizar que solo los usuarios autenticados puedan realizar operaciones (autorizadas), restringiendo el acceso a aquellas opciones de operación aprobadas para su uso por el usuario autenticado. La operación debe llevarse a cabo exclusivamente en rutas de acceso claramente planificadas para garantizar que el proceso de producción continuará funcionando de forma segura durante un comando sin ningún riesgo para las personas, el medio ambiente, el producto, los bienes a coordinar y el negocio de la empresa. .

Estrategias

Con base en estas declaraciones, un concepto de protección comprende estrategias generales de defensa que están destinadas a resistir los siguientes ataques:

- disminución de la disponibilidad (por ejemplo, denegación de servicio)
- eludir los mecanismos de seguridad únicos (como el "hombre en el medio")
- operación incorrecta intencional por parte de usuarios autorizados (como robar contraseñas)
- operaciones incorrectas debido a privilegios de usuario mal configurados
- monitoreo no autorizado de datos (como recetas y secretos comerciales o el funcionamiento de las máquinas y sistemas y sus mecanismos de seguridad)
- modificar datos (por ejemplo, para alterar los niveles de alarma)
- eliminar datos (por ejemplo, archivos de inicio de sesión para cubrir ataques).

La estrategia de defensa de Siemens utiliza los mecanismos de “Defensa en Profundidad”.

Defensa en profundidad

El concepto de defensa en profundidad contiene estructuras en capas de seguridad y medidas de reconocimiento que son superiores al nivel de seguridad de los sistemas independientes. Tiene las siguientes características:

- Capacidad para detectar atacantes que intentan atravesar o eludir la Defensa en la estructura de profundidad.
- Un punto débil en una capa de esta arquitectura se puede compensar temporalmente por las estrategias defensivas en otras capas.
- La seguridad del sistema tiene su propia estructura de capas dentro de la estructura general de capas de la seguridad de las redes.

1.2 Implementación de estrategias en soluciones.

1.2.1 Fortalecer el sentido de la responsabilidad.

Una implementación exitosa de la estrategia de seguridad en soluciones en los sistemas de automatización solo se puede lograr si todas las partes involucradas cooperan de manera responsable. Esto incluye:

• fabricantes (desarrollo, prueba del sistema, prueba de seguridad)

• integrador de sistemas (planificación, estructura, prueba de aceptación en fábrica)

• propietarios/operadores (operación y administración).

Las estrategias y su implementación deben ser supervisadas y actualizadas durante toda la vida útil del sistema (desde el inicio de la presentación de la oferta, planificación y diseño hasta la migración y desinstalación de un sistema).

Las siguientes capacidades hacen posible que un concepto de protección en los sistemas de automatización sea efectivo:

• el uso de productos de alta disponibilidad y probados en el sistema, que han endurecido y configuraciones de seguridad predefinidas, y han sido especialmente diseñados para aplicaciones industriales,

• una configuración moderna, que utiliza tecnologías y estándares de última generación y permite un diseño del sistema adaptado a las necesidades de seguridad del cliente,

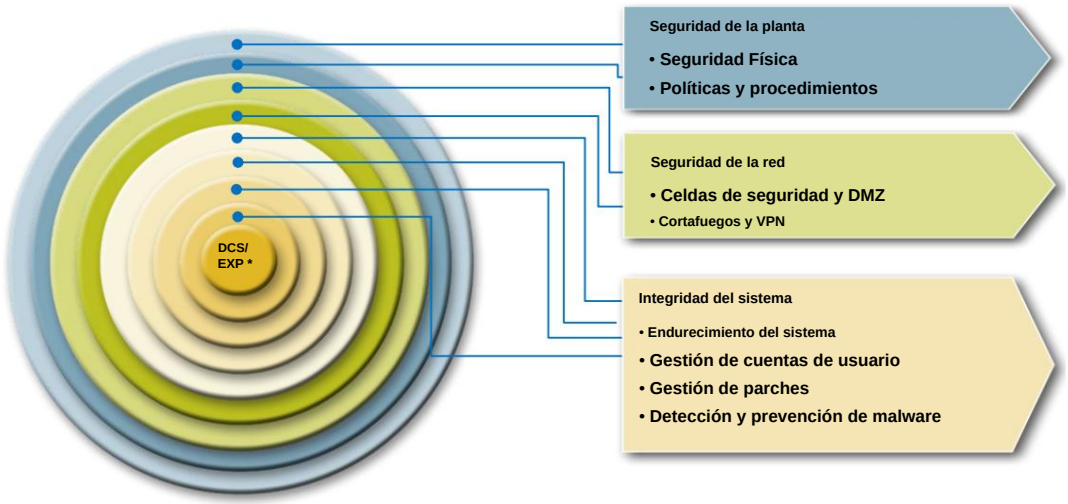
• la operación cuidadosa y responsable de los sistemas y componentes de acuerdo con los usos definidos por el fabricante.

1.2.2 El concepto de protección de Siemens: “Defensa en profundidad”

Siemens sigue la estrategia de "Defensa en profundidad" para lograr los objetivos de seguridad requeridos. El enfoque de esta estrategia es un modelo de seguridad multicapa que consta de los siguientes componentes:

- Seguridad de Planta
- Seguridad de la red
- Integridad del sistema

Figura 1-1



La ventaja de esta estrategia es el hecho de que un atacante primero tiene que atravesar varios mecanismos de seguridad para causar algún daño. Los requisitos de seguridad de cada capa se pueden tener en cuenta individualmente.

La solución de Siemens para la seguridad de la planta

La implementación de una gestión de seguridad completa y adecuada es la base para planificar y realizar una solución de seguridad industrial.

La gestión de la seguridad es un proceso que consta principalmente de cuatro pasos:

- Análisis de riesgos con definición de medidas de reducción de riesgos: Estas medidas deben ser definidas para la planta, en función de las amenazas y riesgos identificados.
- Determinación de lineamientos y coordinación de medidas organizativas.
- Coordinación de medidas técnicas.
- Un proceso de gestión de la seguridad consistente con controles regulares o dependientes de eventos. repetición del análisis de riesgos.

La solución de Siemens para la seguridad de la red

Si los controladores u otros dispositivos inteligentes con autoprotección mínima o nula están ubicados en un segmento de red, una buena opción a considerar es crear un entorno de red seguro para estos dispositivos. Un enfoque para lograr esto es mediante el uso de dispositivos de seguridad de red. . Se puede proporcionar seguridad adicional segmentando subredes individuales, por ejemplo, a través de un concepto de protección celular o una zona desmilitarizada (DMZ).

La solución de seguridad de Siemens se desarrolló especialmente para los requisitos de un entorno de automatización, con el fin de satisfacer la creciente demanda de redes

seguridad, para reducir la susceptibilidad a fallas de toda la planta de producción y así aumentar su disponibilidad.

Nota

Encontrará más información sobre este tema en Siemens Industry Online Support (entrada con ID: 27043887).
http://support.automation.siemens.com/WW/view/en/27043887

La solución de Siemens para la integridad del sistema

Para mantener la integridad del sistema, es importante minimizar las vulnerabilidades en los sistemas de PC y en el nivel de control. Siemens cumple este requisito con las siguientes soluciones:

- uso de software antivirus y de listas blancas,
- gestión de parches,
- autenticación de usuario para operadores de máquinas o plantas,
- mecanismos integrados de protección de acceso en componentes de automatización,
- protección del código del programa mediante protección de know-how, protección contra copia y asignación de contraseñas.

1.3 Diferencias entre la seguridad de la oficina y la seguridad industrial

Los mecanismos de seguridad integrados en las PC y los sistemas operativos Windows generalmente brindan un alto nivel de seguridad. Sin embargo, estas medidas suelen estar diseñadas para los requisitos de los entornos de oficina. En seguridad industrial, los objetos a proteger son bastante similares, pero, en cierta medida, sus prioridades difieren significativamente. Si bien las principales prioridades en la TI de la oficina suelen ser la confidencialidad y la integridad de la información, la disponibilidad o la operatividad de la planta son lo primero en la seguridad industrial. Al seleccionar las medidas de seguridad adecuadas, siempre se debe garantizar que brinden el nivel necesario de protección sin tener un impacto inaceptable en la operación real.

1.4 Diferencias entre seguridad funcional y seguridad industrial

La seguridad funcional aborda la protección del entorno controlado contra el funcionamiento anormal del sistema. Por otro lado, la seguridad aborda la protección del funcionamiento normal de un sistema contra violaciones intencionales o no intencionales.
Sin embargo, los sistemas de seguridad también deben estar particularmente protegidos contra tales violaciones.

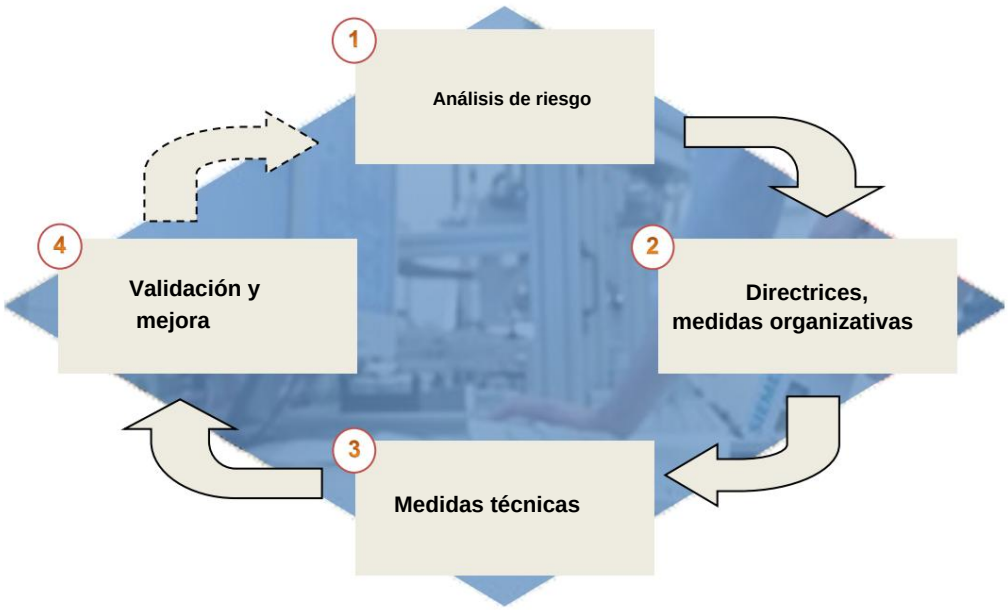
Es tarea del proveedor de máquinas establecer los mecanismos de seguridad apropiados. Estos mecanismos no deben incluirse principalmente en el concepto de defensa en profundidad, incluso si pueden contribuir.

Mientras que las amenazas a la seguridad son básicamente estáticas, las amenazas a la seguridad son dinámicas durante la vida útil de una máquina/planta. Por lo tanto, la protección de seguridad debe revisarse continuamente.

1.5 Gestion de seguridad

La gestión de la seguridad es una parte integral de un concepto de seguridad industrial para abordar todos los aspectos relevantes para la seguridad de una solución de automatización, ya sea una sola máquina, una sección de la planta o una planta completa. A medida que las amenazas potenciales a una solución de automatización cambian a lo largo de su ciclo de vida, se debe considerar un proceso para monitorear y detectar estas amenazas, conocido como gestión de seguridad. El objetivo de este proceso es alcanzar el nivel de seguridad necesario de una solución de automatización y mantenerla de forma permanente. El componente de análisis de riesgos contenido en un proceso de gestión de la seguridad garantiza que solo se implementarán las contramedidas adecuadas para reducir los riesgos. Un ejemplo de un proceso de gestión de la seguridad es el siguiente:

Figura 1-2



2 Mecanismos de seguridad de la CPU S7

Los siguientes capítulos muestran qué mecanismos integrados de protección de acceso
Oferta de controladores SIMATIC S7

2.1 Bloquear protección

Visión de conjunto

En STEP 7 V5.x y en STEP 7 (TIA Portal), existen diferentes funciones de protección:
para proteger el know-how de los programas en los bloques contra personas no autorizadas.

- Protección del know-how
- Privacidad del bloque S7

Si se abre un bloque protegido por esta función, solo se pueden leer la interfaz del bloque (parámetros IN, OUT e IN/OUT) y el comentario del bloque. El código del programa,
las variables temporales/estáticas y los comentarios de la red no se muestran.
No es posible modificar un bloque protegido.

La siguiente tabla ofrece una descripción general de las instalaciones de protección de know-how individuales:

Tabla 2-1

Entorno de desarrollo:	Idioma	Protección del módulo	Validez
PASO 7 V5.x	• KOP / FUP / AWL • SCL • S7-GRAFICO • CFC	Protección del saber hacer (no protegido por contraseña)	S7-300/400/ WinAC
PASO 7 V5.5	• KOP / FUP / AWL • S7-SCL	Privacidad del bloque S7 (contraseña protegida)	S7-300/400
PASO 7 (Portal TIA)	• KOP / FUP / AWL • S7-SCL • S7-GRAFICO	Protección del saber hacer (contraseña protegida)	S7-300/400
	• KOP / FUP • S7-SCL		S7-1200 (V4)
	• KOP / FUP / AWL • S7-SCL		S7-1500

Resumen de los bloques

Privacidad del bloque S7

Con S7 Block Privacy solo se pueden proteger FB y FC.

Protección del saber hacer

Con el atributo KNOW_HOW_PROTECT se puede activar un mecanismo de protección de know-how para bloques de tipo OB, FB y FC.

Los bloques de datos de instancia no se pueden proteger manualmente, ya que dependen de la protección de know-how del FB asignado. Esto significa que el bloque de datos de instancia de un FB protegido por contraseña también contiene una protección de know-how. Esto no depende de si el bloque de datos de instancia ha sido creado explícitamente o generado por una llamada de bloque.

En TIA Portal también se permiten bloques de datos globales. Los bloques de datos ARRAY no se pudieron proteger con la protección de know-how.

Limitaciones

Los bloques con protección de bloque no se pueden seguir procesando en STEP 7 (sin la contraseña correcta). Tampoco son posibles funciones de prueba y puesta en marcha como "Bloques de supervisión" o "Paradas". Solo las interfaces del bloque permanecen visibles.

Con un bloque protegido se pueden realizar las siguientes acciones:

- copiar y borrar
- llamar al bloque protegido
- comparación en línea/fuera de línea
- cargar

Privacidad del bloque S7

S7 Block Privacy es un paquete de ampliación de STEP 7 a partir de V5.5 para proteger funciones y bloques de función.

Al utilizar S7 Block Privacy, se debe tener en cuenta lo siguiente:

- S7 Block Privacy se opera a través de los menús contextuales. • Los

bloques, una vez protegidos, solo se pueden desproteger con la contraseña correcta y de acuerdo con la información de recopilación adjunta. Por lo tanto, se recomienda guardar la contraseña en un lugar seguro y/o hacer copias de los bloques desprotegidos.

- Los bloques protegidos solo se pueden cargar en 400 CPU a partir de la versión 6.0 en adelante, en 300 CPU solo a partir de la versión 3.2.
- Si hay fuentes en el proyecto, los bloques protegidos se pueden restaurar mediante las fuentes por compilación. Las fuentes se pueden eliminar por completo del S7 Block Privacy.

Nota

Encontrará más información sobre cómo configurar la protección de bloques con S7 Block Privacy en la pregunta frecuente "¿Cómo se puede configurar la protección de bloques mejorada para FB y FC en STEP 7 V5.5?" (Número de entrada: 45632073).
http://support.automation.siemens.com/WW/view/en/45632073

Protección de know-how (STEP 7 V5.x)

Los bloques en STEP7 V5.x se pueden proteger agregando un atributo de bloque. La palabra de código KNOW_HOW_PROTECT se indica durante la programación del bloque en el fuente.

La protección de bloque solo se puede revocar con la fuente STL. Si las fuentes STL ya no están disponibles para el programa o el proyecto, la protección de los bloques no se puede eliminar.

Se recomienda utilizar S7-Block Privacy en su lugar como un mecanismo mejorado de protección de conocimientos.

Nota

Puede encontrar más información sobre la configuración de la protección de bloques en las preguntas frecuentes de KNOW_HOW_PROTECT "¿Cómo se puede instalar una protección de bloques para los bloques que he creado yo mismo?" (ID de entrada: 10025431).

http://support.automation.siemens.com/WW/view/en/10025431

Protección del know-how (TIA Portal)

En el TIA Portal, la protección de bloques se establece a través del menú contextual indicando una contraseña.

Debe observarse lo siguiente:

- En la comparación entre la versión fuera de línea y en línea de los bloques protegidos por know-how, solo se compararán los datos que no están protegidos.
- No se puede crear ningún tipo de bloque protegido por know-how en la biblioteca. Si se agrega un bloque de este tipo a una biblioteca, la nueva plantilla de copia también contiene la protección de know how. Allí, necesita la contraseña correcta del bloque protegido por know-how para usar las copias.

  Si se va a utilizar un bloque protegido por know-how en una biblioteca sin revelar la contraseña, se deben tener en cuenta los siguientes elementos para programar estos bloques:

  – Durante la compilación deben conocerse todos los bloques de código y de datos llamados. Entonces no es posible realizar llamadas indirectas.
  – Para la programación de los bloques, el uso de variables de PLC y datos globales se deben evitar los bloques.

Nota Encontrará más información en la ayuda en pantalla de STEP 7 (TIA Portal) en: • Configurar la protección de know-how para bloques • Abrir bloques protegidos por know-how • Eliminar la protección de know-how para bloques

Para S7-1200 (V4) y S7-1500-PLC se puede configurar una protección adicional contra copias que vincula la ejecución del bloque al PLC a la tarjeta de memoria con el número de serie definido.

2.2 Restricciones de funciones y acceso en línea

Niveles de protección de la CPU

La CPU S7 ofrece tres (S7-300/S7-400/WinAC) o cuatro (S7-1200(V4)/S7-1500) niveles de acceso para limitar el acceso a determinadas funciones.

La configuración del nivel de acceso y las contraseñas restringe las funciones y las áreas de memoria a las que se puede acceder sin contraseña.

Los niveles de acceso individuales y las respectivas contraseñas se definen en las propiedades del objeto de la CPU.

Tabla 2-2

Niveles de acceso	Restricción de acceso
Nivel 1 (sin protección)	Cualquiera puede leer y modificar la configuración del hardware y los bloques.
Nivel 2 (protección de escritura)	Con este nivel de acceso, solo se permite el acceso de lectura sin contraseña, lo que significa que se pueden realizar las siguientes funciones: • leer la configuración del hardware y los bloques • lectura de datos de diagnóstico • cargar la configuración de hardware y los bloques en el dispositivo de programación. • cambiar el estado operativo (RUN/STOP) (no para S7-300 / S7-400 / WinAC) Sin la contraseña no se pueden realizar las siguientes funciones: • cargar los bloques y la configuración de hardware en la CPU • funciones de prueba de escritura • actualización de firmware (en línea)
Nivel 3 (protección contra escritura/lectura)	En este nivel de acceso, solo • Acceso HMI y • lectura de datos de diagnóstico es posible sin una contraseña. Sin la contraseña no se pueden realizar las siguientes funciones: • cargar los bloques y la configuración de hardware en o desde la CPU, • escribir funciones de prueba • cambiar el estado operativo (RUN/STOP) (no para S7-300 / S7-400 / WinAC) • actualización de firmware (en línea).
Nivel 4 (protección completa) S7-1200 (v4) S7-1500	Con una protección completa, la CPU prohíbe: • acceso de lectura y escritura a la configuración del hardware y a los bloques, • Acceso HMI, • modificaciones en la función del servidor para la comunicación PUT/GET, • acceso de lectura y escritura en el área "Dispositivos accesibles" y en el proyecto para dispositivos que se conectan en línea.

Comportamiento operativo con nivel de protección activado

Una CPU protegida por contraseña tiene el siguiente comportamiento durante el funcionamiento:

- La protección de la CPU se hace efectiva cuando la configuración se ha cargado en la CPU y se establece una nueva conexión.
- Antes de que se pueda llevar a cabo una función en línea, primero se verifica si está admisible, y si hay una protección de contraseña, se le pide al usuario que ingrese la contraseña.
- Las funciones protegidas por una contraseña solo pueden ser realizadas por una sola PG/PC a la vez. Ninguna otra PG/PC puede iniciar sesión con la misma contraseña. • Los derechos de acceso a

los datos protegidos se aplican solo durante la duración de la conexión en línea o hasta que la autorización de acceso haya sido eliminada manualmente con "En línea > Eliminar derechos de acceso"

Nota

La configuración de un nivel de acceso no reemplaza la protección del know-how.
Esto evita modificaciones no autorizadas en la CPU al restringir los derechos de descarga. Sin embargo, los bloques de la SIMATIC Memory Card no están protegidos contra escritura o lectura. Para proteger el código del programa, se debe utilizar la protección de know-how.

2.3 Protección anticopia (S7-1200 (V4) / S7-1500)

La protección contra copia permite asociar el programa completo o el bloque individual con una SIMATIC Memory Card o CPU específica. Al asociar los elementos del programa con un número de serie de una SIMATIC Memory Card o una CPU, solo es posible utilizar este programa o este bloque en combinación con esta SIMATIC Memory Card o CPU definida.

Si se carga un bloque con protección anticopia en un dispositivo que no corresponde al número de serie definido, se rechaza el proceso de carga completo. Esto también significa que incluso los bloques sin protección contra copias no se pueden cargar.

La protección contra copia y las entradas de los respectivos números de serie se realizan en las propiedades del bloque.

Nota

Si se instala una protección de copia de este tipo para un bloque, es importante que este bloque también contenga protección de know-how de bloque. Sin protección de know-how, cualquiera podría eliminar la protección contra copias.

Sin embargo, la protección contra copia debe instalarse primero, ya que los ajustes para la protección contra copia están protegidos contra escritura si el bloque tiene protección de know-how.

2.4 Protección de acceso local (S7-1500)

Bloqueo de la CPU

El SIMATIC S7-1500 tiene una tapa frontal con pantalla y botones de manejo. Para insertar y extraer la SIMATIC Memory Card y para cambiar manualmente el estado operativo de la CPU, debe abrirse.

Para la protección de la CPU contra el acceso no autorizado, esta tapa frontal se puede asegurar con la escotilla de cierre. Hay dos opciones disponibles:

- asegurar la solapa frontal con un candado
- asegurar la solapa frontal con un sello

Figura 2-1

Bloqueo de la pantalla

En la pantalla puede bloquear el acceso a una CPU protegida por contraseña (bloqueo local). La protección de acceso solo es efectiva cuando el interruptor de modo de operación está en la posición RUN. La protección de acceso es efectiva independientemente de la protección de contraseña, es decir, incluso si alguien accede a la CPU a través de un dispositivo de programación conectado e ingresa la contraseña correcta, el acceso a la CPU seguirá siendo denegado. La protección de acceso se puede configurar por separado para cada nivel de acceso en la pantalla, lo que significa que, por ejemplo, el acceso de lectura está permitido localmente, pero el acceso de escritura no está permitido localmente. Puede configurar una contraseña para la pantalla en STEP 7 en las propiedades de la CPU de tal manera que la protección de acceso local esté garantizada por una contraseña local.

2.5 Otras medidas para proteger la CPU

Las siguientes medidas aumentan adicionalmente la protección contra el acceso no autorizado a las funciones y datos de la CPU S7 desde fuera y dentro de la red:

- desactivar o restringir el servidor web
- desactivar la sincronización horaria a través del servidor NTP
- desactivar la comunicación PUT/GET (S7-1200(V4)/ S7-1500)

Nota En la configuración por defecto de los módulos, estas funciones están desactivadas.

Funciones de seguridad para el servidor web

Con el servidor web puede controlar y monitorear remotamente la CPU a través de la Intranet de la empresa. Por lo tanto, las evaluaciones y los diagnósticos son posibles a grandes distancias.

Sin embargo, el riesgo de accesos no autorizados a la CPU puede aumentar al activar el servidor web.

Si desea activar el servidor web, le recomendamos las siguientes medidas:

- no conecte el servidor web de la CPU directamente a Internet
- proteger el acceso al servidor web mediante el uso de la red apropiada segmentación, DMZ y dispositivos de seguridad.
- acceder al servidor web a través del protocolo de transmisión segura “https”,
- configurar los derechos de usuario y funciones a través de la lista de usuarios
  - crear un usuario
  - definir los derechos de ejecución
  - asignar contraseñas.

Los usuarios solo pueden realizar las funciones que se han establecido como parte de la configuración de administración de usuarios. Una vez que se ha configurado un usuario, puede iniciar sesión con su contraseña y acceder a los sitios web de acuerdo con sus derechos de acceso. De forma predeterminada, se ha establecido un usuario con el nombre "Todos". Este usuario tiene derechos de acceso mínimos (acceso de lectura a la introducción y la página de inicio). El usuario “Todos” se ha configurado sin contraseña y no se puede modificar.

Desactivar la comunicación PUT/GET (S7-1200(V4)/ S7-1500)

La CPU puede ser el servidor de una serie de servicios de comunicación. En este modo, otros dispositivos de comunicación pueden acceder a los datos de la CPU sin haber sido configurados o programados explícitamente para la CPU. De igual forma la UCP local no tiene la posibilidad de controlar la comunicación a los clientes.
Si este tipo de comunicación es admisible o no para la CPU local, se define en las propiedades del objeto de la CPU.

En la configuración por defecto, la opción “Acceso a través de la comunicación PUT/GET…” está desactivada. En este caso, el acceso de lectura y escritura a los datos de la CPU solo es posible para aquellas conexiones de comunicación que requieren programación para la CPU local y para el interlocutor de comunicación (p. ej., el acceso a través de instrucciones BSEND / BRECV es posible incluso en la configuración predeterminada).

Las comunicaciones, para las cuales la CPU local es solo servidor (es decir, que no hay configuración/ programación de la comunicación con el interlocutor de la comunicación), no son posibles en el funcionamiento de la CPU.

Esto incluye:

- PUT/GET, FETCH/WRITE o acceso FTP a través de módulos de comunicación
- Acceso PUT/GET por parte de otras CPU S7
- Acceso HMI a través de comunicación PUT/GET

3 Mecanismos de seguridad de los S7-CP

Los siguientes capítulos muestran qué mecanismos de seguridad ofrecen los SIMATIC S7-CP (CP x43-1 Advanced V3 y CP 1x43-1).

Nota

Las funciones del CP 1543-1 se pueden configurar a partir del STEP 7 Professional V12, incluida la actualización 1.
El CP 1243-1 necesita STEP 7 Professional V13 Update 3 o superior.

Figura 3-1

CP 1543-1 PC 1243-1 CP 343-1 Avanzado CP 443-1 Avanzado

3.1 Cortafuegos de inspección con estado

Descripción

Los cortafuegos permiten filtrar el tráfico entrante y saliente que fluye a través de un sistema. Un cortafuegos puede usar uno o más conjuntos de "reglas" para inspeccionar los paquetes de red a medida que entran o salen de las conexiones de red y permite el paso del tráfico o lo bloquea. Las reglas de un firewall pueden inspeccionar una o más características de los paquetes, como el tipo de protocolo, la dirección del host de origen o destino y el puerto de origen o destino.

Las capacidades de filtrado de un filtro de paquetes se pueden mejorar considerablemente si los paquetes de IP se comprueban en su contexto adecuado. Por ejemplo, un paquete UDP que llega desde una computadora externa solo debe reenviarse internamente si otro paquete UDP se envió a esa computadora poco antes desde dentro de la red (por ejemplo, en el caso de una solicitud de DNS de un cliente en la red interna a una externa). Servidor DNS). Para habilitar esto, el filtro de paquetes debe mantener registros de todos los estados de todas las conexiones actuales. Por lo tanto, los filtros de paquetes que pueden hacer esto se denominan **Stateful.**

Propiedades

Los cortafuegos de inspección con estado tienen las siguientes propiedades:

- con conexiones TCP: Imitación de la monitorización de estado de un TCP/IP completo pila de protocolos
- con conexiones UDP: simulación de conexiones virtuales
- creación y eliminación de reglas de filtrado dinámico.

3.2 Codificación de datos a través de VPN

Descripción

Una VPN (red privada virtual) es una red privada que utiliza una red pública (como Internet) para la transmisión de datos privados a una red de destino privada. Las redes no necesitan ser compatibles entre sí.

Aunque VPN usa los mecanismos de direccionamiento de la red del operador, todavía usa sus propios paquetes de red para separar el transporte de paquetes de datos privados de los demás. Debido a este hecho, las redes privadas aparecen como una red lógica (virtual) compartida.

IPSec

Un aspecto importante para la comunicación de datos a través de los límites de la red es IPSec (seguridad IP). Es un conjunto de protocolos estandarizados y proporciona un intercambio de datos seguro, protegido e independiente del fabricante a través de redes IP.
El objetivo principal de IPSec es proteger y asegurar los datos durante una transmisión a través de una red insegura. Este estándar de seguridad puede evitar las debilidades conocidas, como la intercepción y el cambio de paquetes de datos, debido a los paquetes de datos cifrados y la autenticación de los dispositivos.

3.3 NAT/NAPT (traducción de direcciones)

Descripción

La traducción de direcciones de red (NAT) / la traducción de puertos de direcciones de red (NAPT) son métodos para convertir direcciones IP privadas en direcciones IP públicas.

Conversión de direcciones con NAT

NAT es un protocolo para la conversión de direcciones entre dos espacios de direcciones. La tarea principal es la conversión de direcciones públicas, es decir, direcciones IP utilizadas y enrutadas en Internet en direcciones IP privadas y viceversa.

Mediante el uso de esta tecnología las direcciones de la red interna no son visibles en la red externa. En la red externa, los nodos internos solo son visibles a través de direcciones IP externas definidas en la lista de conversión de direcciones (tabla NAT).

La NAT típica es una conversión 1:1, es decir, una dirección IP privada se convierte en una pública.

Por lo tanto, la dirección de destino de los nodos internos es una dirección IP externa.

La tabla NAT contiene la asignación de direcciones IP públicas y privadas y se configura y administra en la puerta de enlace o enrutador.

Conversión de direcciones con NAPT

NAPT es una variante de NAT y, a menudo, se considera que es idéntico. La diferencia con NAT es el hecho de que los puertos también se pueden convertir con este protocolo.

La dirección IP ya no se convierte 1:1. En cambio, solo hay una dirección IP pública que se convierte en varias direcciones IP privadas al agregar números de puerto.

La dirección de destino de los nodos internos es una dirección IP externa con un número de puerto.

La tabla NAPT contiene la asignación de puertos externos a direcciones IP privadas, incluidos los números de puerto, y se configura y administra en la puerta de enlace o el enrutador.

3.4 Funciones informáticas seguras

3.4.1 Protocolo de transferencia de archivos (FTP)

Descripción

El Protocolo de transferencia de archivos es un protocolo de red específico para la transmisión de datos entre un servidor FTP y un cliente FTP, o entre dos servidores FTP.

FTP permite intercambiar datos, crear y renombrar directorios y también eliminarlos. La comunicación entre el cliente FTP y el servidor FTP es un intercambio de comandos basados en texto. Cada comando enviado por el cliente FTP da como resultado una respuesta del servidor FTP en forma de un código de estado y un mensaje en texto sin formato.

Para ello, FTP crea dos conexiones lógicas: un canal de control a través del puerto 21 para la transmisión de comandos FTP y sus respuestas, así como un canal de datos a través del puerto 20 para la transmisión de datos.

Con un FTP pasivo, los dos canales son iniciados por el cliente FTP, mientras que con un FTP activo, el servidor inicia uno de los canales hacia el cliente.

La solución para un FTP seguro es FTPS

La transmisión segura de datos con FTP se logra con una combinación de FTP y el protocolo SSL y utiliza los mismos puertos que en el modo FTP normal (puerto 20/21).

Como clave para SSL se utiliza un certificado que se genera y entrega con la configuración del CP de seguridad.

La transferencia segura de datos FTP con CPx43-1 Advanced V3 solo es posible si la función de seguridad está habilitada y se permite explícitamente en la configuración del CP.

3.4.2 Protocolo de tiempo de red (NTP)

Descripción

El Network Time Protocol (NTP) es un protocolo estandarizado para sincronizar la hora en varias computadoras/componentes a través de la red. La precisión está dentro del rango de milisegundos.

Un servidor NTP pone la hora a disposición de los clientes NTP.

NTP (seguro)

NTP (seguro) permite una sincronización horaria segura y autenticada mediante métodos de autenticación y un código de cifrado conjunto. Tanto el servidor NTP como los clientes NTP deben admitir esta función.

Una sincronización horaria segura es compatible con CP x43-1 Advanced V3 y CP 1x43-1, si la función de seguridad está activada y la configuración NTP ampliada se ha activado explícitamente en la configuración.

3.4.3 Protocolo de transferencia de hipertexto (HTTP)

Descripción

El Protocolo de transferencia de hipertexto (HTTP) es parte de la familia de protocolos de Internet y es un procedimiento estandarizado para transferir datos dentro de una red. HTTP se utiliza principalmente para cargar sitios web desde un servidor web a un navegador web.

HTTPS

Los datos transportados a través de HTTP se pueden leer como texto sin formato y pueden ser interceptados por terceros.
Hoy en particular, en la era de la banca en línea, las compras en línea y las redes sociales redes: es importante que la transmisión de datos confidenciales y personales sea segura y esté protegida contra el acceso no autorizado.
El Protocolo de transferencia de hipertexto seguro (HTTPS) es la forma más fácil de transmitir datos de forma segura.
HTTPS tiene la misma estructura que el protocolo HTTP, pero además utiliza el protocolo de capa de conexión segura para el cifrado.
Muchos de los últimos modelos de CPU y CP SIMATIC son compatibles con HTTPS y se pueden configurar para usar HTTPS exclusivamente, lo que proporciona un mayor nivel de seguridad para la transmisión de datos.

3.4.4 Protocolo simple de administración de red (SNMP)

Descripción

SNMP (Simple Network Management Protocol) es un protocolo basado en UDP que se especificó especialmente para la administración de redes de datos y, mientras tanto, se ha establecido también como un estándar de facto para dispositivos TCP/IP.

Los nodos individuales de la red (componentes de red o terminales) cuentan con un agente SNMP que proporciona información de forma estructurada. Esta estructura se denomina MIB (Base de información de gestión). En el nodo de red, el agente generalmente se implementa como funcionalidad de firmware.

Base de información de gestión – MIB

Una MIB (Base de información de gestión) es una estructura de datos estandarizada que consta de diferentes variables SNMP, que se describen mediante un lenguaje independiente del sistema de destino. Debido a la estandarización entre proveedores de MIB y mecanismos de acceso, incluso una red heterogénea con componentes de diferentes fabricantes puede monitorearse y controlarse. Si se necesitan datos no estandarizados específicos de componentes para el monitoreo de la red, los fabricantes pueden describir estos datos en "MIB privados".

SNMP seguro (SNMPv3)

Hay varias versiones de SNMP: SNMPv1, SNMPv2 y SNMPv3. A veces todavía se utilizan las versiones originales SNMPv1 y SNMPv2. Sin embargo, es recomendable no utilizar SNMPv1 y SNMPv2 ya que en estas versiones no se han implementado mecanismos de seguridad, o solo de forma restringida.
A partir de la versión 3, SNMP ofrece además administración de usuarios con autenticación y cifrado opcional de paquetes de datos. Estos aspectos mejoraron sustancialmente la seguridad con SNMP.
El SNMP seguro es compatible con CP x43-1 Advanced V3 y CP 1x43-1, si la función de seguridad está activada y SNMPv3 se ha activado explícitamente en la configuración.

4 El Programa de Certificación Achilles

Motivación

La seguridad en la automatización industrial solo se puede lograr si los fabricantes, proveedores, usuarios y operadores cooperan. Una parte importante de la cooperación es la creación de estándares internacionales que se aplicarán universalmente como base para conceptos y soluciones de seguridad orientados al futuro.

Creación de estándares uniformes

Los estandares

• ISA 99 “Seguridad de Sistemas de Control y Fabricación”, • IEC

62443 “Seguridad para Medición y Control de Procesos Industriales – Seguridad de Redes y Sistemas”,

• la directriz alemana VDI/VDE 2182 “Seguridad de la información en el automatización industrial” (seguridad de la información en la automatización industrial),

son de particular importancia para la creación de normas uniformes que se van a utilizar universalmente.

Mientras que este último se ocupa de los procedimientos y mecanismos para asegurar los componentes y sistemas de automatización, el Instituto de Cumplimiento de Seguridad de ISA (ISCI) enfrenta el desafío de crear un marco de certificación uniforme.

El programa de certificación Achilles

El programa de certificación Achilles de Wurldtech se considera un estándar internacional para la seguridad cibernética.

El certificado confirma que los sistemas de automatización cuentan con la robustez de comunicaciones necesaria para mejorar la seguridad y estabilidad de las plantas industriales. La certificación Achilles sirve como un criterio importante para la selección de productos con sistemas de comunicación robustos. El programa de certificación Achilles confirma que los sistemas de control de Siemens son resistentes a los ataques a la red. El programa de certificación se divide en dos niveles:

• Certificación Achilles Communications Nivel 1: El primer nivel del programa de certificación confirma la solidez de Ethernet, IP, ARP, ACMO, TCP y UDP en los módulos con un programa de prueba especial. Si cumplen con todos los requisitos de la prueba, los módulos obtienen la certificación Achilles Level 1.

• Certificación Achilles Nivel 2: Este segundo nivel comprende los mismos protocolos que el Nivel 1. Sin embargo, cada protocolo se prueba más intensamente. Además, el nivel 2 contiene más pruebas, pruebas de denegación de servicio (DoS) con una tasa de enlace más alta y más requisitos.
Todos los módulos Siemens Industry probados tienen la certificación Achilles Level 2.

5 Literatura

Bibliografía

Esta lista no es completa y solo presenta una selección de referencias relacionadas.

Tabla 5-1

	Tema	Título
/1/	PASO7 SIMATIC S7-300/400	Automatización con STEP7 en AWL y SCL Autor: Hans Berger Publicis MCD Verlag ISBN: 978-3-89578-397-5
/2/	PASO7 SIMATIC S7-300/400	Automatización con STEP 7 en KOP y FUP Autor: Hans Berger Publicis MCD Verlag ISBN: 978-3-89578-296-1
/3/	PASO7 SIMATIC S7-300	Automatización con SIMATIC S7-300 dentro de TIA Portal Autor: Hans Berger Publicis MCD Verlag ISBN: 978-3-89578-357-9
/4/	PASO7 SIMATIC S7-400	Automatización con SIMATIC S7-400 dentro del TIA Portal Autor: Hans Berger Publicis MCD Verlag ISBN: 978-3-89578-372-2
/5/	PASO7 SIMATIC S7-1200	Automatización con SIMATIC S7-1200 Autor: Hans Berger Publicis MCD Verlag ISBN: 978-3-89578-355-5
/6/	PASO7 SIMATIC S7-1500	Automatización con SIMATIC S7-1200 Autor: Hans Berger Publicis MCD Verlag ISBN: 978-3895784033
/7/	Seguridad SIMATIC NET	SIMATIC NET Industrial Ethernet Security Principios básicos y manual de configuración de aplicaciones http://support.automation.siemens.com/WW/view/en/56577508
/8/	Manual S7-1500	Sistema de automatización SIMATIC S7-1500 http://support.automation.siemens.com/WW/view/en/59191792
/9/	Manual del S7-1200	Sistema de automatización SIMATIC S7-1200 http://support.automation.siemens.com/WW/view/en/36932465
/10/	Manual S7-400	SIMATIC S7-400 Sistema de automatización S7-400 CPU-Data http://support.automation.siemens.com/WW/view/en/53385241
/11/	Manual S7-300	SIMATIC S7-300, CPU 31xC y CPU 31x: Datos técnicos http://support.automation.siemens.com/WW/view/en/12996906
/12/	CP343-1 Avanzado	Manual del sistema Parte B CP343-1 Avanzado http://support.automation.siemens.com/WW/view/en/62046619
/13/	CP443-1 Avanzado	Manual del sistema Parte B CP443-1 Avanzado http://support.automation.siemens.com/WW/view/en/59187252
/14/	Manual CP1543-1	SIMATIC NET S7-1500 - Ethernet industrial CP 1543-1

Especificaciones del enlace de Internet

Esta lista no está completa y solo representa una selección de información relevante

Tabla 5-2

	Tema	Título
\1\	Referencia a la entrada	http://support.automation.siemens.com/WW/view/en/77431846
\2\	Industria de Siemens en línea Apoyo	http://support.automation.siemens.com
\3\	Seguridad Ethernet industrial	http://support.automation.siemens.com/WW/view/en/18701555/130000
\4\	Primeros pasos S7-1500	http://support.automation.siemens.com/WW/view/en/71704272
\5\	Páginas de resumen „Protección completa con Industrial Seguridad"	https://support.industry.siemens.com/cs/de/en/view/50203404
\6\	Resumen de páginas „Industrial Comunicación remota“	https://support.industry.siemens.com/cs/de/en/view/64721753
\7\	Descripción general de la posible constelación basada en IP Redes remotas	https://support.industry.siemens.com/cs/de/en/view/26662448
\8\	SIMATIC NET Industrial Ethernet Security, configurar la seguridad en STEP 7 Profesional	https://support.industry.siemens.com/cs/de/en/view/109477192
\9\	SIMATIC NET Industrial Seguridad de Ethernet: configuración Seguridad - Primeros pasos	https://support.industry.siemens.com/cs/de/en/view/109474411
\10\	SIMATIC NET - Industria Seguridad Ethernet - Fundamentos y aplicaciones de seguridad - Manual de configuración	https://support.industry.siemens.com/cs/de/en/view/109474417

6 Historia

Tabla 6-1

Versión	Fecha	Modificaciones
V1.0	09/2013	Primera versión
V2.0	03/2016	Añadir CP 1243-1, añadir más enlaces