

SIEMENS
Ingenuity for life



Configuration of TLS-based PG/HMI Communication And The Protection of Confidential PLC Configuration Data

TIA Portal V17 / S7-1500 PLC / TP1200 Comfort Panel

<https://support.industry.siemens.com/cs/ww/en/view/109798583>

Siemens
Industry
Online
Support



Información legal

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 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.

Información 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 ciberneticas, 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 o 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

Tabla de contenido

Información legal	2
1 Introducción	5
1.1 Visión de conjunto.....	5
1.2 Modo de operación.....	5
1.3 Componentes utilizados.....	7
2 Nuevas funciones de seguridad para PLC y panel HMI en TIA Portal V17.....	8
2.1 Concepto de "Seguridad por defecto"	8
2.2 Comunicación segura PG/PC y HMI	9
2.2.1 Seguridad de la capa de transporte - TLS	9
2.2.2 Mecanismo de comunicación segura	10
2.3 Protección de los Datos Confidenciales de Configuración del PLC	13
2.4 Asistente de seguridad.....	15
2.5 Compatibilidad de comunicación	diecisésis
3 Ingeniería	17
3.1 Preparación del proyecto.....	17
3.2 Configuración del controlador SIMATIC	19
3.2.1 Ajustes de seguridad del PLC.....	19
3.2.2 Establecer la dirección IP	23
3.2.3 Activar la configuración de seguridad global para el administrador de certificados	24
3.3 Configuración del panel HMI.....	27
3.3.1 El PLC y el panel HMI están en el mismo proyecto del TIA Portal	28
3.3.2 El PLC y el panel HMI se encuentran en dos proyectos TIA Portal diferentes	30
3.3.3 El panel HMI no está configurado en el TIA Portal - Conexión con WinCC SCADA Sistemas V7	35
4 Instalación y puesta en marcha.....	36
4.1 Configuración de hardware.....	36
4.2 Instalación de componentes de hardware y software	36
4.3 Cargar componentes de hardware	37
4.3.1 Cargar el autómata S7-1500	37
4.3.2 Cargar el SIMATIC TP1200 Comfort Panel	40
4.4 Operación	42
5 Escenarios de intercambio de dispositivos	45
5.1 El PLC de reemplazo no tiene contraseña para los datos de configuración confidenciales	46
5.2 El PLC de reemplazo tiene la misma contraseña para los datos de configuración confidenciales	46
5.3 El PLC de reemplazo tiene otra contraseña para datos de configuración confidenciales	47
5.3.1 Configuración de la contraseña en TIA Portal	47
5.3.2 Configuración de la contraseña con una SIMATIC Memory Card adicional	49
6 Actualización de firmware y copia de seguridad del dispositivo	51
6.1 Actualización de firmware del autómata S7-1500	51
6.2 Copia de seguridad y restauración de un PLC (PLC S7-1200, PLC S7-1500)	52
6.3 Actualización de firmware y copia de seguridad del dispositivo del panel HMI	53
7 Información útil	54
7.1 Una lista de componentes que soportan comunicación segura PG/PC y HMI	54

Tabla de contenido

7.2	Cambio de la contraseña para proteger los datos confidenciales de configuración del PLC (PLC S7-1200, PLC S7-1500)	54
7.2.1	Cambiar contraseña: la configuración aún no está cargada	54
7.2.2	Cambiar contraseña - La configuración ya está cargada	57
7.3	Restablecimiento de la contraseña para proteger los datos confidenciales de configuración del PLC (PLC S7-1200, PLC S7-1500)	60
7.3.1	Restablecimiento de la contraseña: la configuración aún no está cargada.....	60
7.3.2	Restablecimiento de la contraseña - La configuración ya está cargada	61
7.3.3	Restablecimiento de la contraseña con SIMATIC Memory Card.....	62
7.4	Sugerencias para evitar y manejar errores	63
7.5	Uso de la comunicación PG/PC heredada en el TIA Portal	64
7.6	Descripción del proyecto TIA Portal V17.....	66
7.6.1	Resumen	66
7.6.2	El bloque de función "SimulatedDrive"	67
7.6.3	El bloque de datos global "SimulatedDriveData".....	68
8	Apéndice.....	69
8.1	Servicio y soporte.....	69
8.2	Centro comercial de la industria	70
8.3	Enlaces y literatura	70
8.4	Modificar la documentación	71

1. Introducción

1 Introducción

1.1 Visión de conjunto

Tarea

La digitalización y la creciente interconexión de máquinas y sistemas industriales también suponen un aumento del riesgo de ciberataques. Las medidas de protección adecuadas son imperativas, especialmente para las instalaciones de infraestructura crítica.

Enfoque

Como pionero en el mundo de la seguridad industrial, Siemens siempre ha tenido como objetivo proporcionar soluciones holísticas y de vanguardia para garantizar la máxima protección de máquinas y plantas. Por este motivo, Siemens ha introducido nuevas funciones de seguridad en TIA Portal V17. Estas características aseguran que los datos de comunicación no estén sujetos a manipulación mediante encriptación. También brindan protección contra el acceso no autorizado a máquinas y software.

Descripción de la solución

Este ejemplo de aplicación describe las nuevas funciones de seguridad que se han introducido con TIA Portal V17 y cómo aplicarlas en los PLC S7-1500 en conexión con los paneles HMI. El usuario aprenderá a utilizar el asistente de seguridad recientemente introducido que ayuda con la configuración de seguridad del PLC. La configuración de seguridad incluye los siguientes pasos de configuración:

- Proteger los datos de configuración confidenciales del PLC.
- Conecte los paneles HMI a la CPU a través de conexiones de comunicación seguras.
- Configurar la protección de acceso al PLC.

Además de eso, se describen los siguientes casos de uso:

- Reemplace un dispositivo antiguo por uno nuevo
- Compatibilidad con dispositivos más antiguos
- Configuraciones que se han implementado con TIA Portal < V17
- Actualización de la versión de firmware del PLC y del panel HMI

1.2 Modo de operación

En la producción se utiliza un PLC S7-1500 para monitorear y controlar un sistema transportador y cintas transportadoras. El PLC S7-1500 comprueba la velocidad real de la cinta transportadora, "actualSpeed", a intervalos regulares y la compara con un valor predefinido, "setPointSpeed".

- Si la velocidad real es mayor que el valor predefinido, la velocidad "actualSpeed" se reduce al valor "setPointSpeed".
- Si la velocidad real es menor que el valor predefinido, la velocidad "actualSpeed" aumenta al valor "setPointSpeed".

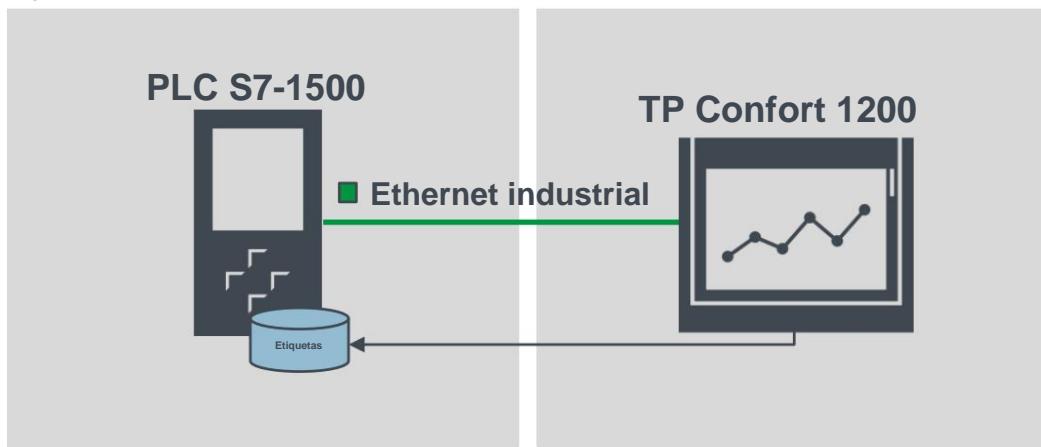
El S7-1500 está conectado a un panel HMI a través de Ethernet y se comunica con él a través de TCP/IP. La comunicación está asegurada mediante el protocolo de seguridad de la capa de transporte (TLS), que utiliza certificados digitales para el cifrado y la autenticación. El valor "setPointSpeed" se puede configurar en el panel HMI que también muestra el valor "actualSpeed" y el estado actual de la cinta transportadora "isActive".

1. Introducción

Diagrama

La siguiente figura muestra los componentes más importantes de la solución:

Figura 1-1



Funciones implementadas

Las siguientes funciones están implementadas en el ejemplo de aplicación:

Configuración de las siguientes funciones de seguridad del PLC S7-1500 utilizando el asistente de seguridad:

- La protección de los datos confidenciales de configuración del PLC.
- La conexión segura al panel HMI mediante certificados digitales.
- La protección de acceso al PLC.

• Configuración del panel HMI para conexión segura con el PLC S7-1500. Esto incluye las siguientes posibilidades: – El PLC y el panel HMI están en el mismo proyecto del TIA Portal.

- El PLC y el panel HMI están en diferentes proyectos del TIA Portal.
- El panel HMI no está configurado con TIA Portal – El PLC está conectado a WinCC SCADA V7.

• Los pasos necesarios para reemplazar una CPU antigua por una nueva se pueden realizar utilizando uno de los siguientes métodos: –

Descargue el proyecto TIA Portal directamente al nuevo PLC.

- Vaya online a la nueva CPU para establecer la contraseña y utilice la SIMATIC Memory Card de la vieja CPU.

– Utilice una SIMATIC Memory Card adicional y un archivo JOB especial.

Entonces es posible utilizar la SIMATIC Memory Card de la CPU antigua en la nueva CPU.

• Actualización de la versión de firmware del PLC y del panel HMI.

 1. Introducción

1.3 Componentes utilizados

Este ejemplo de aplicación se ha creado con los siguientes componentes de hardware y software:

Tabla 1-1

Componente	Número	Número de artículo	Nota
CPU 1515-2 PN a partir del firmware V2.9	1	6ES7 515-2AM01-0AB0	Un autómata S7-1500/S7-1200 diferente de la lista mencionada en el capítulo 7.1 también se puede utilizar como alternativa.
SIMATIC TP1200 Comfort Panel a partir del firmware V17.0.0.0	1	6AV2 124-0MC01-0AX0	También se puede utilizar como alternativa un panel HMI diferente de la lista mencionada en el capítulo 7.1 .
Fuente de alimentación PM1207	1	6EP1332-1SH71	Alternativamente, se puede utilizar una fuente de alimentación diferente.
TIA Portal V17	1	6ES7822-0AA07-0YA5	TIA Portal V17

Puede adquirir estos componentes en [Siemens Industry Mall](#)

NOTA Este ejemplo de aplicación también se puede utilizar como base para conectar de forma segura otros tipos de controladores SIMATIC y paneles HMI. Consulte el capítulo [7.1](#) para obtener una lista completa de los dispositivos que admiten la característica de comunicación segura PG/PC y HMI.

Este ejemplo de aplicación consta de los siguientes componentes:

Tabla 1-2

Componente	Nombre del archivo	Nota
Proyecto	"109798583_PLC_HMI_Security_PROJ_V17.zip"	Este archivo comprimido contiene el proyecto TIA Portal V17.
Documentación	"109798583_PLC_HMI_Security_DOCU_V10_en.pdf"	Este documento.

2 Nuevas características de seguridad para PLC y panel HMI en TIA Portal V17

2 Nuevas funciones de seguridad para panel PLC y HMI en TIA Portal V17

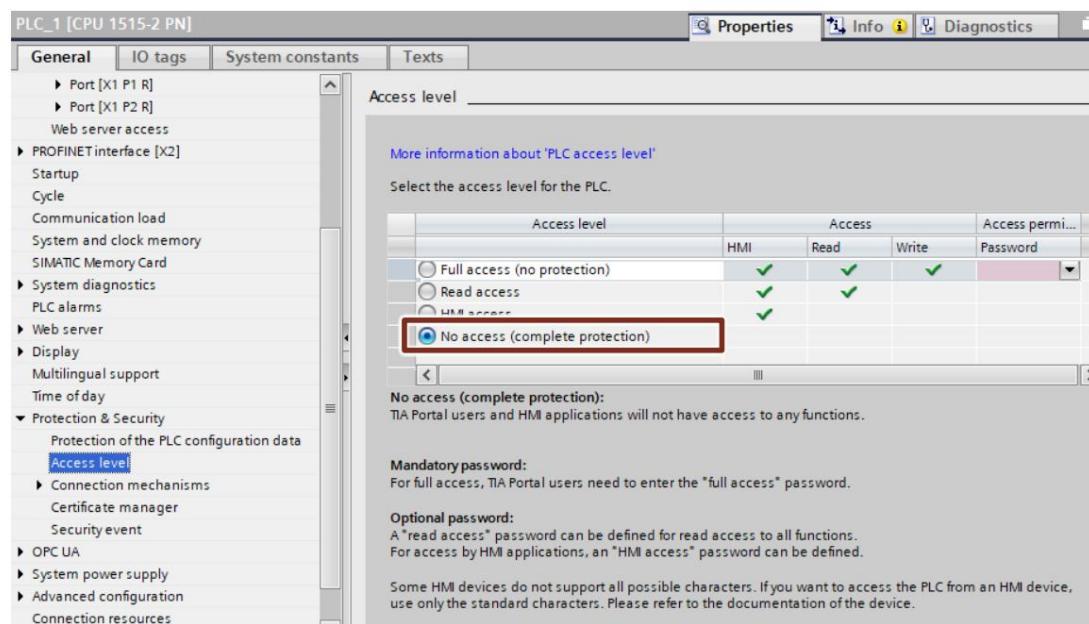
Este capítulo proporciona una descripción general de las últimas características de seguridad que se introdujeron en TIA Portal V17.

2.1 Concepto de "seguridad por defecto"

Con TIA Portal versión 17, se han preconfigurado varias opciones y se establecen de forma predeterminada para garantizar un mayor nivel de seguridad para máquinas e instalaciones.

Esto incluye:

- La protección de acceso al PLC preactivada, que impide cualquier tipo de acceso al controlador a menos que el cliente sea verificado con la contraseña correcta.

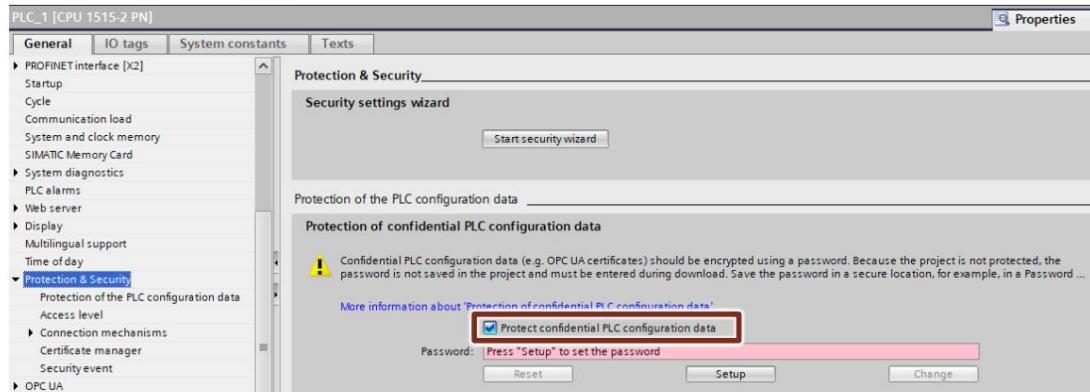


- La comunicación segura predefinida de PG/PC y HMI, que evita que PG/PC heredados comunicación con otros socios. Consulte el capítulo 2.2.



2 Nuevas características de seguridad para PLC y panel HMI en TIA Portal V17

- El requisito preactivado para configurar la contraseña para proteger el PLC confidencial datos de configuración, que garantiza que todos los datos confidenciales de configuración del PLC estén protegidos de forma predeterminada. Consulte el [capítulo 2.3](#).



2.2 Comunicación segura PG/PC y HMI

Una característica de la comunicación PG y la comunicación HMI sobre todo es su simplicidad.

Establecer una conexión en línea del TIA Portal desde un dispositivo de programación a un PLC, por ejemplo, para cargar un programa, requiere poco esfuerzo. Esta conexión en línea también cumple con ciertos criterios, como la confidencialidad y la integridad, basada en un estándar de comunicación SIMATIC probado.

Sin embargo, la integración de máquinas y sistemas en un entorno de TI abierto requiere que la comunicación entre el dispositivo de programación o el panel HMI y el PLC esté protegida en el sentido de mantener la integridad y confidencialidad de los datos confidenciales. También requiere que esta seguridad cumpla con los estándares generalmente aceptados y, por lo tanto, esté lista para los desafíos del futuro.

A partir de TIA Portal V17, se mejoró la comunicación PG/PC y HMI. Aquí, el protocolo de seguridad de la capa de transporte (TLS) se utiliza para asegurar la comunicación PG/PC y HMI utilizando mecanismos de seguridad estandarizados.

2.2.1 Seguridad de la capa de transporte - TLS

TLS está diseñado para proporcionar seguridad en las comunicaciones a través de una red informática. Esta seguridad se realiza mediante los siguientes elementos:

- Confidencialidad: los datos están encriptados o son ilegibles para los intrusos no autorizados.
- Integridad: el mensaje que sale del remitente llega al destinatario sin cambios. En otras palabras, el mensaje no ha sido manipulado en tránsito.
- Autenticación de punto final: el interlocutor de la comunicación como punto final es exactamente el persona que pretende ser. Se verifica la identidad del socio.

TLS utiliza un certificado digital para cifrar y autenticar a los socios y los datos. En TIA Portal V17, el usuario tiene la opción de utilizar un certificado individual y específico del usuario para los socios de comunicación que proporciona una capa adicional de seguridad al sistema. Si un dispositivo se ve comprometido, otros dispositivos permanecen seguros ya que usan certificados diferentes. Los certificados se pueden importar o crear en TIA Portal con el administrador de certificados. Para obtener más información sobre el uso de certificados en TIA Portal, consulte el siguiente enlace: [\31](#).

2 Nuevas características de seguridad para PLC y panel HMI en TIA Portal V17

2.2.2 Mecanismo de comunicación segura

La base de la comunicación segura PG/PC y HMI es que el panel PG y HMI puede verificar la autenticidad del PLC utilizando el certificado de comunicación PLC que el PLC envía al establecer la comunicación y considera que este PLC es "digno de confianza". La comunicación segura PG/HMI solo es posible cuando el panel PG y HMI confía en el PLC.

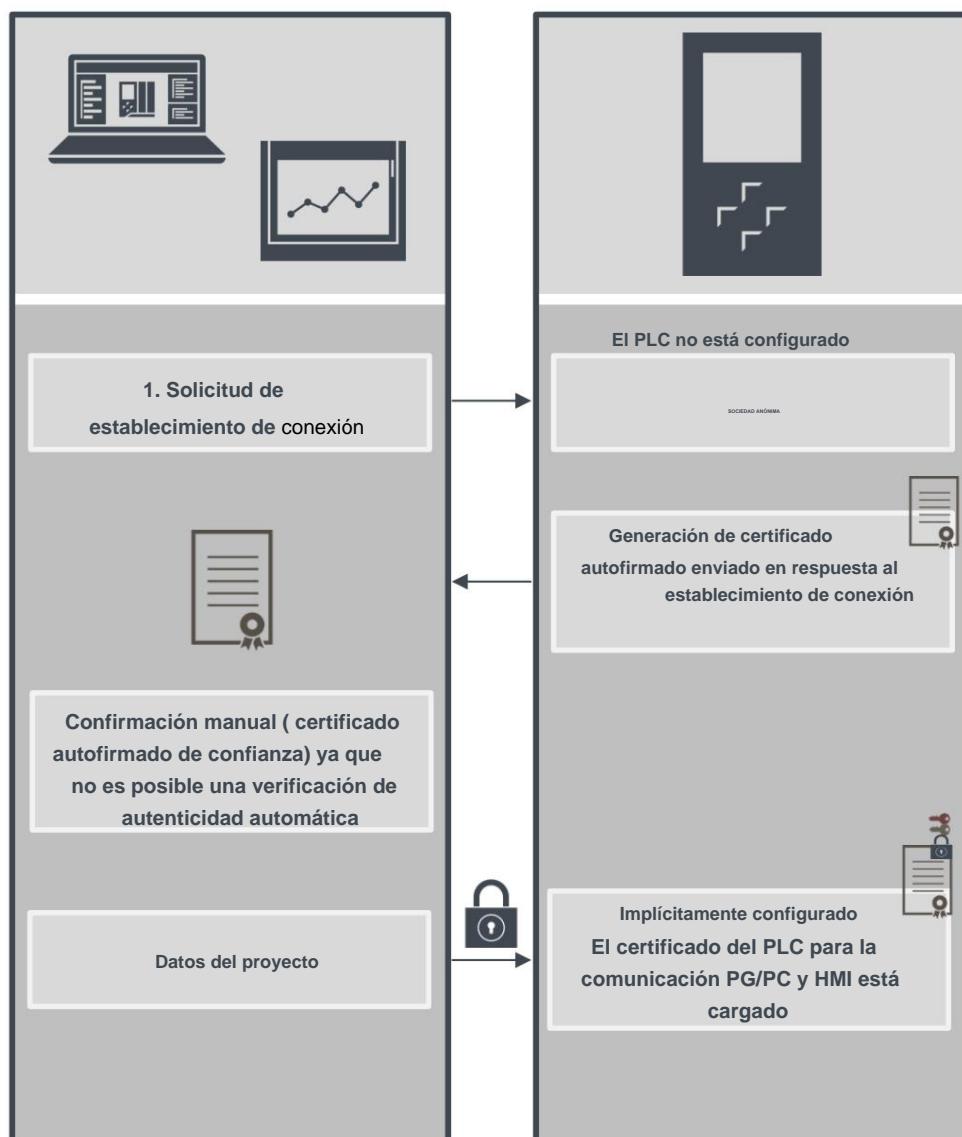
Durante el establecimiento de la conexión, el PLC transfiere el certificado de comunicación del PLC al interlocutor de la comunicación (PG o panel HMI).

Para garantizar que la comunicación entre el PLC y un dispositivo de programación o HMI sea segura, el PLC primero debe tener un certificado. Sin embargo, este certificado solo se emite cuando el proyecto se carga en el PLC. A continuación, se explica la comunicación segura entre el panel PG o HMI y el PLC.

Fase de aprovisionamiento

La siguiente figura explica el proceso de establecimiento de la conexión inicial desde el panel PG o HMI al PLC también conocidas como "fases de aprovisionamiento".

Figura 2-1



2 Nuevas características de seguridad para PLC y panel HMI en TIA Portal V17

El primer establecimiento de conexión para la carga inicial al PLC está asegurado por el procedimiento TLS en términos de comunicación segura PG/P y HMI. La PG envía una solicitud de establecimiento de conexión al PLC.

El PLC utiliza su certificado de dispositivo del fabricante (si está disponible) o un certificado autofirmado para establecer esta conexión. El PLC solo se puede utilizar de forma limitada en esta fase. En este punto, el PLC espera el suministro de la información clave basada en contraseña, es decir, el PLC está esperando la contraseña para los datos de configuración confidenciales del PLC (consulte el capítulo [2.3](#)). Esta fase también se denomina fase de aprovisionamiento. Un mensaje en el búfer de diagnóstico indica que el PLC se encuentra en fase de aprovisionamiento.

El PLC envía sus certificados al PG en el que el usuario debe confiar manualmente para que continúe el proceso de descarga inicial. Esto debe hacerse solo una vez durante la descarga inicial.

Cuando se carga un proyecto en el PLC, el PLC recibe los datos del proyecto:

- Configuración de hardware que incluye certificados configurados para comunicación segura (OPC UA, HTTPS, Secure OUC, Secure PG/P y comunicación HMI)
- Programa de usuario

Finalización de la Fase de Aprovisionamiento

TIA Portal no almacena la contraseña para los datos confidenciales de configuración del PLC ni la información clave generada a partir de la contraseña en el proyecto.

Por lo tanto, la contraseña se solicita en un diálogo cuando se carga el proyecto por primera vez o cuando se carga un nuevo proyecto y se transfiere al PLC como información clave. Solo después de este paso, el PLC puede utilizar los datos de configuración del PLC protegidos. Esto completa la fase de aprovisionamiento y la CPU puede comenzar a funcionar.

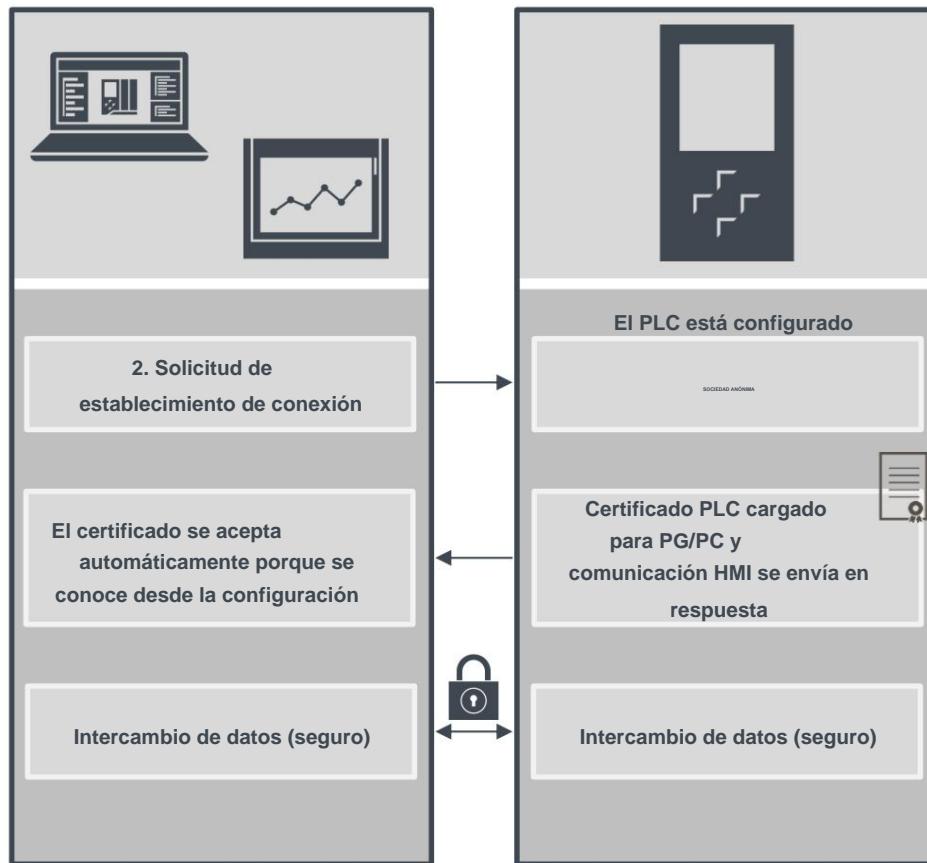
NOTA Si no protege los datos confidenciales de configuración del PLC con una contraseña, no hay necesidad de ingresar la contraseña al cargar la CPU por primera vez. Esto no influye en el flujo de la comunicación PG/PC y HMI. Si no se configura la contraseña de datos confidenciales de configuración del PLC, el PLC saldrá de la fase de aprovisionamiento y seguirá operativo. En este caso, los datos confidenciales de configuración del PLC (p. ej., claves privadas) no están protegidos contra el acceso no autorizado (consulte el capítulo [2.3](#)).

2 Nuevas características de seguridad para PLC y panel HMI en TIA Portal V17

Puesta en marcha de la comunicación PG/PC y HMI

Cuando el PLC está cargado y ha recibido el certificado de PLC para la comunicación segura PG/PC y HMI, el dispositivo de programación se conecta de nuevo. Esta vez basado en el certificado cargado.

Figura 2-2



2.3 Protección de los Datos Confidenciales de Configuración del PLC

El correcto funcionamiento de los mecanismos de comunicación basados en certificados que se utilizan para la comunicación segura, como la comunicación segura de PG/PC y HMI, la comunicación de usuario abierta segura, HTTPS, SMTP seguro sobre TLS u OPC UA, requiere que las claves privadas utilizadas por estos certificados estén protegidos lo mejor posible. A partir de TIA Portal V17, puede establecer una contraseña definida por el usuario para proteger estas claves y otros datos que vale la pena proteger: La contraseña para proteger los datos de configuración confidenciales del PLC.

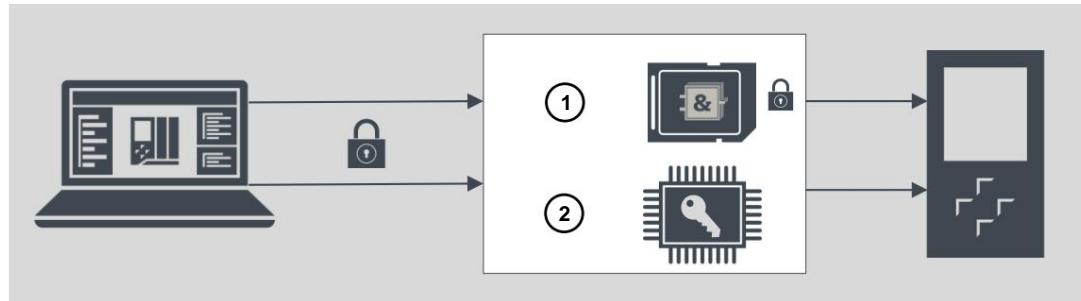
Para proteger los datos de configuración confidenciales del PLC, el usuario tiene la opción de ingresar una contraseña en el portal TIA. Los datos de configuración típicos que se consideran confidenciales son los certificados y las claves privadas.

La siguiente figura muestra de forma simplificada cómo se protegen los datos confidenciales de configuración del PLC, por ejemplo, de un PLC S7-1500 estándar: El proyecto y la información clave se colocan en diferentes áreas de memoria cuando se cargan por primera vez.

- El proyecto se coloca en la memoria de carga (SIMATIC Memory Card).
- La información clave se coloca en un área de memoria en el PLC. Esta tecla se utiliza para leer el datos de configuración confidenciales en la SIMATIC Memory Card.

Para otros sistemas de destino, como S7-1200 PLC y Software Controller), con otros conceptos de memoria, la implementación se adapta a los conceptos de memoria correspondientes. Sin embargo, el principio es el mismo.

Figura 2-3



1. Proyecto con datos de configuración confidenciales protegidos con contraseña (aquí: en carga memoria = tarjeta de memoria SIMATIC).
2. Información clave (generada a partir de la contraseña) para utilizar los datos de configuración confidenciales protegidos (aquí: en el área de memoria del PLC).

2 Nuevas características de seguridad para PLC y panel HMI en TIA Portal V17

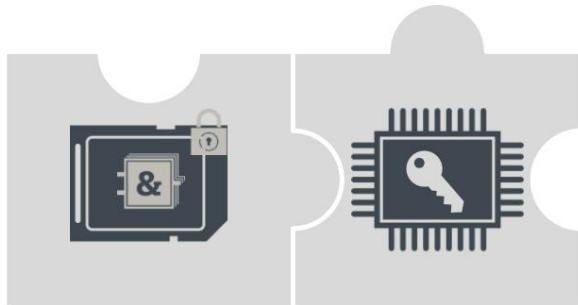
Dos áreas de memoria para mayor seguridad

El proyecto y la clave están relacionados entre sí como dos piezas de rompecabezas coincidentes: el proyecto está vinculado a la información de la clave cargada y la información de la clave cargada está vinculada a la contraseña que se asignó durante la configuración. La información clave y del proyecto debe coincidir; de lo contrario, el PLC no se iniciará.

El principio de dos áreas de memoria separadas también se aplica a las versiones de PLC S7-1200 y S7-1500 sin SIMATIC Memory Card, p. ej. para el controlador de software, PLCSIM y

PLCSIM Avanzado. En las versiones sin SIMATIC Memory Card, se utilizan dos particiones separadas para que los dos elementos de información se puedan gestionar de forma independiente.

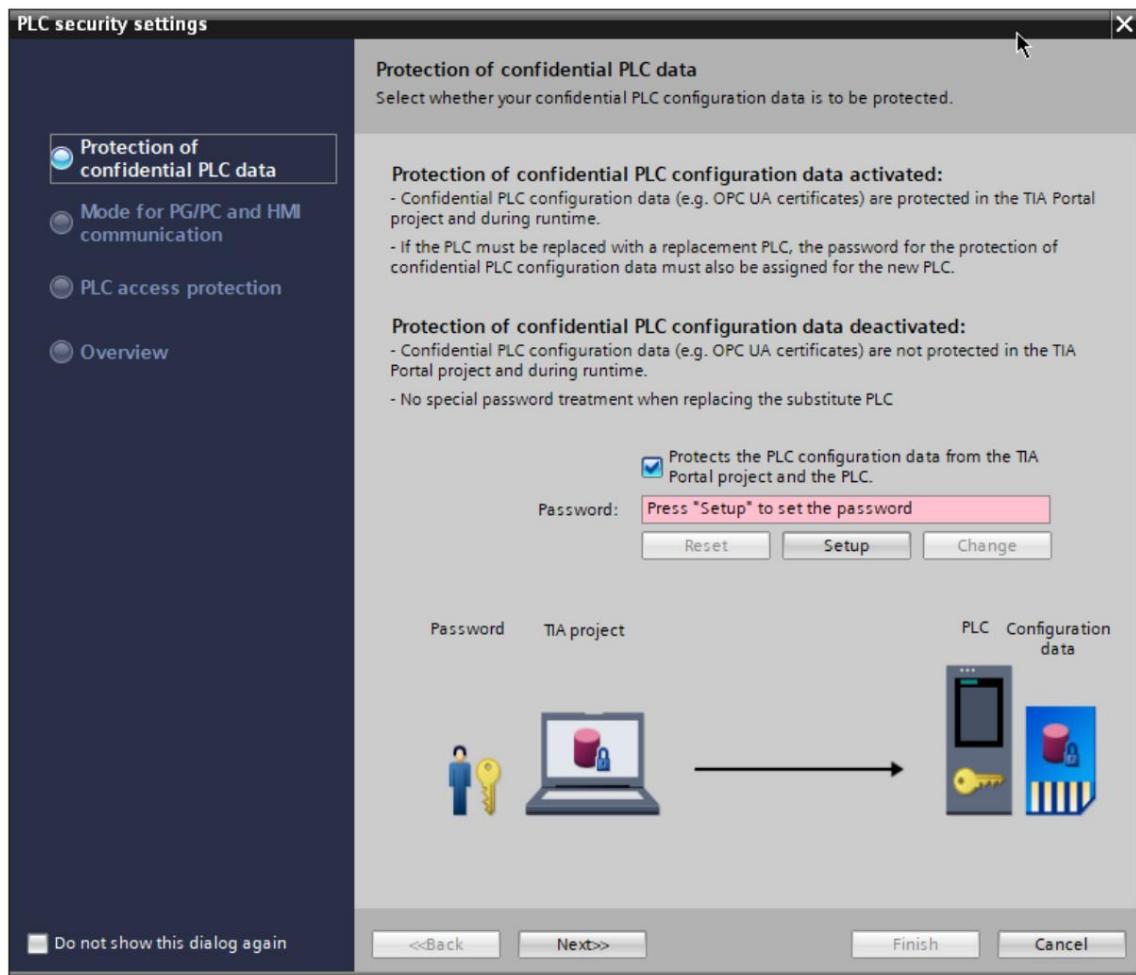
Figura 2-4



2 Nuevas características de seguridad para PLC y panel HMI en TIA Portal V17**2.4 Asistente de seguridad**

Para la configuración de seguridad en TIA Portal versión 17, se guía al usuario a través de un asistente que les ayuda con la configuración de seguridad. Esto incluye la protección de datos de configuración confidenciales, el nivel de acceso del controlador SIMATIC y la comunicación segura PG/PC y HMI.

Figura 2-5

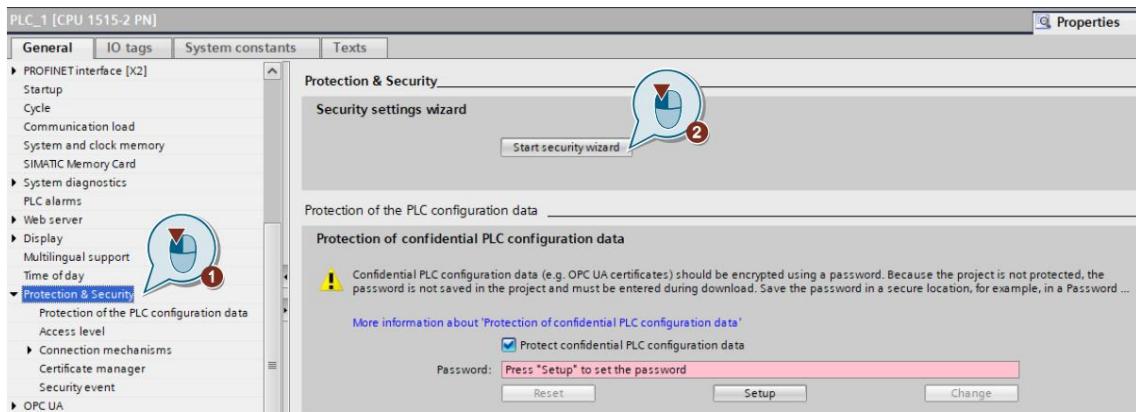


NOTA El asistente de seguridad se abre automáticamente cuando se agrega un nuevo PLC al proyecto del TIA Portal.

Alternativamente, es posible iniciar el asistente de seguridad manualmente en el menú de propiedades del PLC. En el menú de propiedades del PLC, vaya a "Protección y seguridad" y haga clic en el botón "Iniciar asistente de seguridad" para iniciar el asistente de seguridad.

2 Nuevas características de seguridad para PLC y panel HMI en TIA Portal V17

Figura 2-6



2.5 Compatibilidad de comunicación

La comunicación segura PG/PC y HMI está activada de forma predeterminada para los PLC configurados con TIA Portal V17. Este modo se llama "Modo seguro".

Sin embargo, para comunicarse con dispositivos que están configurados con versiones anteriores de TIA Portal, se ha introducido la compatibilidad de comunicación.

Tiene la opción de conectar un S7-1500 PLC V2.9 o S7-1200 PLC V4.5 a un dispositivo de programación actual con TIA Portal V17 o superior y además, por ejemplo, a un panel HMI con un tiempo de ejecución de la versión anterior .

Los dispositivos ajustan automáticamente sus mecanismos de conexión en consecuencia. Para poder diferenciar mejor entre los dos mecanismos de conexión, llamamos al procedimiento de conexión a versiones anteriores "modo heredado" que se basa en una variante de comunicación S7.

Hay dos modos de operación para los controladores SIMATIC en TIA Portal V17:

- Solo a través de una comunicación segura PG/PC basada en TLS y HMI ("Secure Mode").
- Tanto a través de la comunicación segura PG/PC y HMI como a través de la PG/PC utilizada anteriormente y Comunicación HMI ("Modo seguro" y "Modo heredado"). Este modo también se denomina "Modo mixto".

Teniendo en cuenta lo anterior, podemos resumir cómo se comporta la compatibilidad de comunicación en diferentes escenarios:

- El panel PG/HMI y el PLC están configurados en TIA Portal V17 o una versión superior: La comunicación segura PG/PC basada en TLS y HMI ("Secure Mode").
- El panel PG/HMI está configurado en una versión anterior (TIA Portal < V17): se utiliza "Legacy Mode" dado que ha desactivado la opción "Permitir solo comunicación segura PG/PC y HMI" en las propiedades del PLC.
- El PLC está configurado en TIA Portal V17 o versión superior y varios PG y paneles HMI están conectados que están configurados en TIA Portal V17 o superior como en versiones anteriores (TIA Portal < V17): "Mixed Mode" se utiliza si ha desactivado la opción "Permitir solo comunicación segura PG/PC y HMI" en las propiedades del PLC.

NOTA De forma predeterminada, en el TIA Portal solo se permite la comunicación segura de PG/PC basada en TLS y HMI. V17. Sin embargo, esta opción se puede desactivar si es necesario, en casos como cuando el rendimiento se ve afectado, debido a un estándar de seguridad más alto.

3 Ingeniería

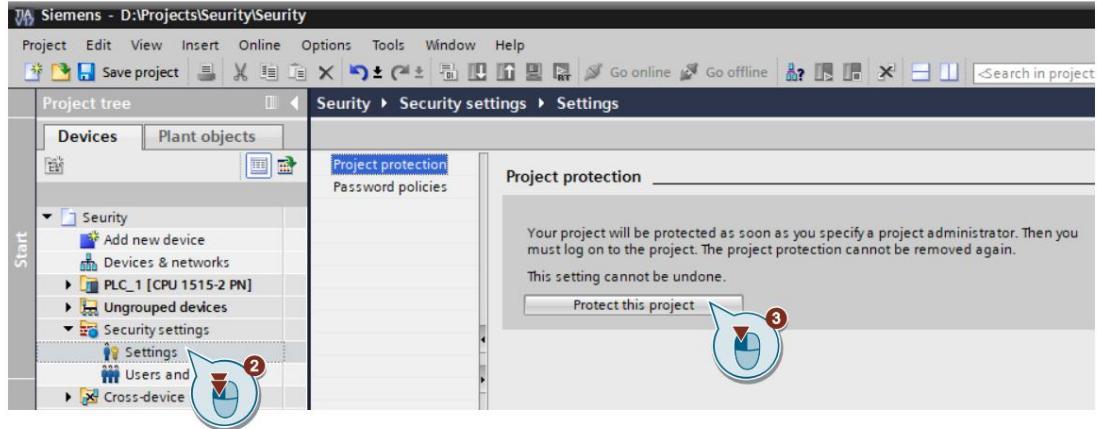
NOTA La ingeniería del PLC S7-1500 y el panel HMI están completamente implementadas en el proyecto.

Esta sección muestra cómo crear un proyecto con un PLC S7-1500 y un panel HMI.

3.1 Preparación del proyecto

1. Cree un proyecto de TIA Portal.
2. En el menú "Árbol del proyecto", vaya a "Configuración de seguridad > Configuración".
3. Haga clic en el botón "Proteger este proyecto" para definir las credenciales del administrador del proyecto.

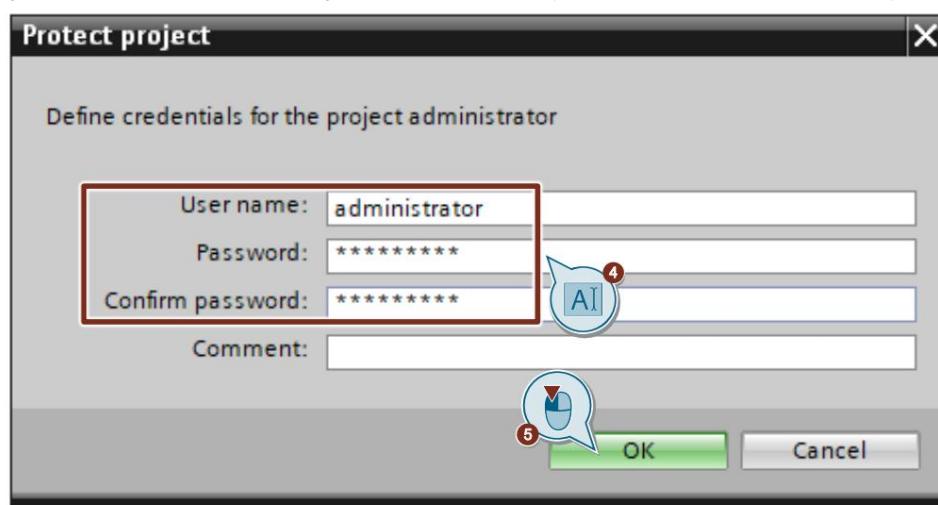
Se abre el cuadro de diálogo "Proteger proyecto".



4. Introduzca el nombre de usuario y la contraseña del administrador del proyecto.

La información de inicio de sesión para el administrador del proyecto se puede encontrar en [la Tabla 3-1](#).

5. Haga clic en el botón "Aceptar" para asignar el nombre de usuario y la contraseña al administrador del proyecto.



3 Ingeniería

Una lista de las contraseñas utilizadas se puede encontrar en la siguiente tabla:

Tabla 3-1

Descripción	Clave	Nota
Administrador del proyecto TIA Portal Siemens1!		Nombre de usuario: administrador
Contraseña para la protección de datos confidenciales de configuración del PLC	Siemens00 #	-
Contraseña para acceso completo	Siemens11 #	-
Contraseña para acceso de lectura	Siemens22#	-
Contraseña para acceso HMI	Siemens33#	-

3.2 Configuración del controlador SIMATIC

3.2.1 Configuración de seguridad del PLC

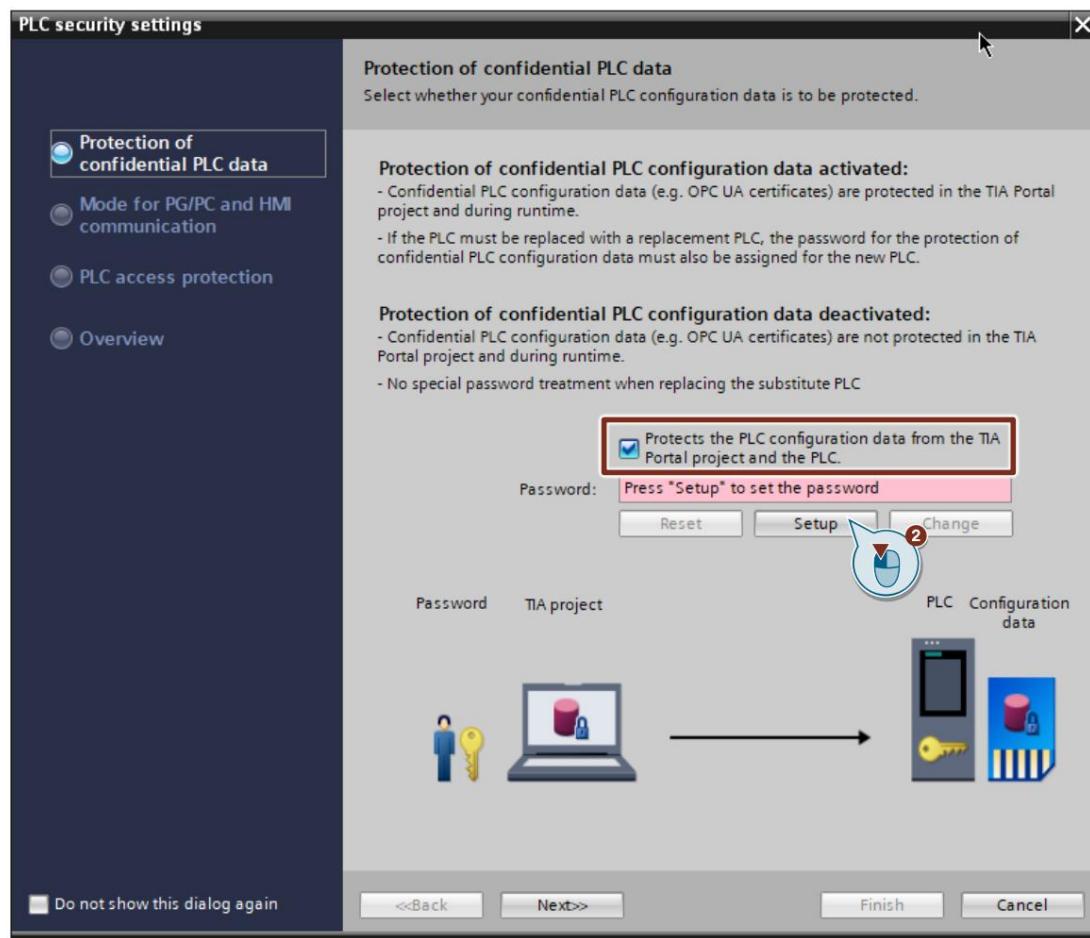
1. Agregue un nuevo S7-1500 PLC, p. ej. CPU 1515-2 PN V2.9.

El asistente de seguridad se abre automáticamente para admitir la configuración.

NOTA También se pueden utilizar otros modelos de controladores SIMATIC. Consulte el capítulo [7.1](#) para obtener una lista completa de los dispositivos que admiten la característica de comunicación segura PG/PC y HMI.

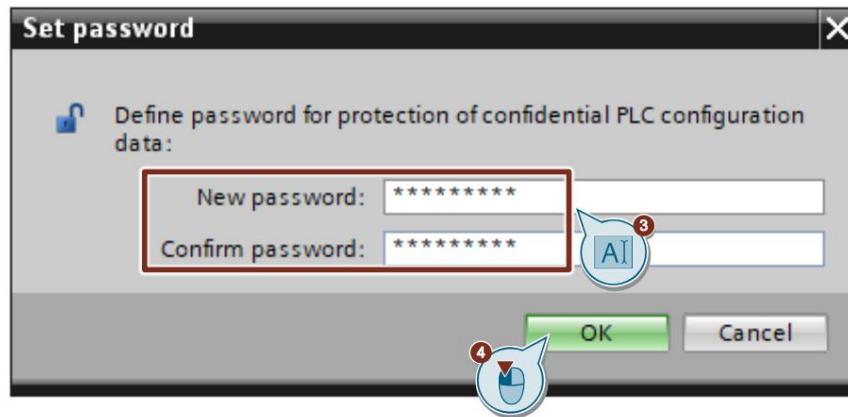
2. En la primera ventana, la casilla de verificación "Protege los datos de configuración del PLC del proyecto TIA Portal y del PLC" está activada de forma predeterminada según el concepto Security-By-Default.

Haga clic en el botón "Configurar" para configurar una contraseña para proteger los datos de configuración confidenciales del PLC.

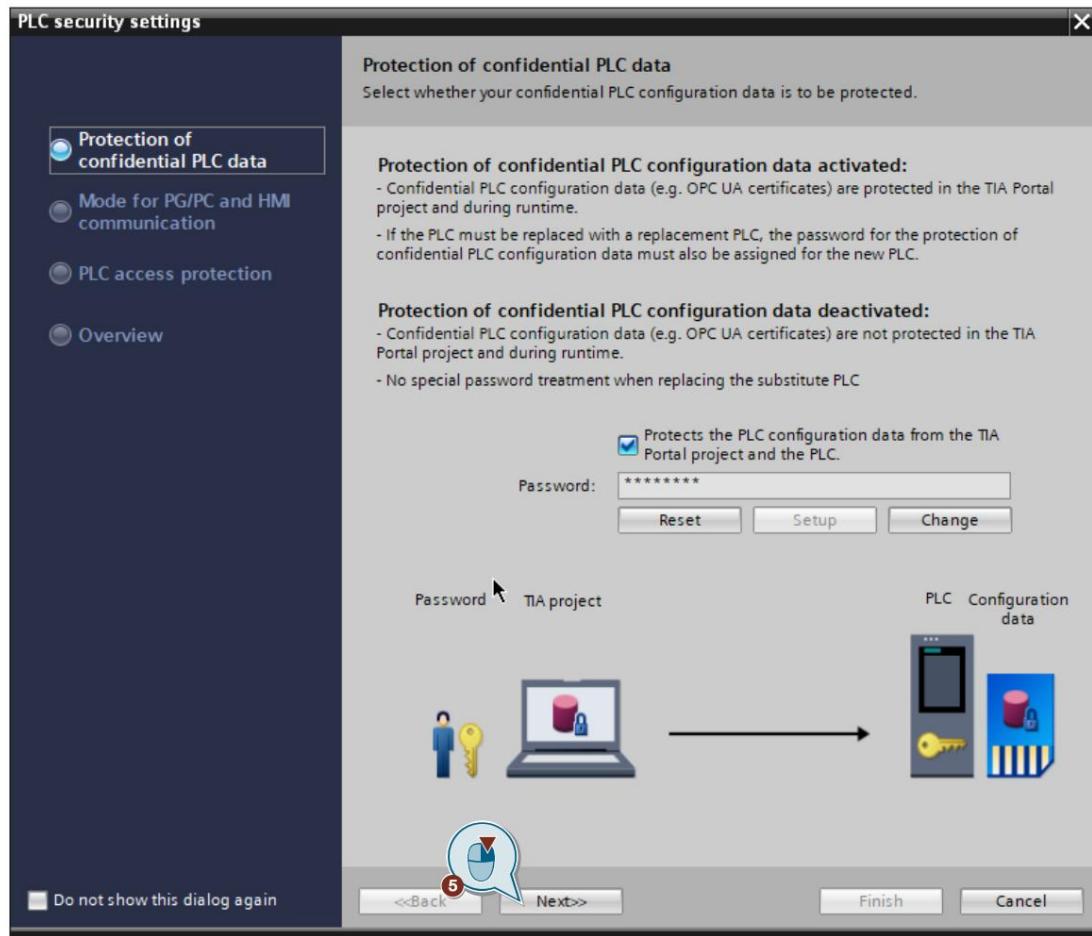


3. Ingrese la contraseña y la confirmación de la contraseña de acuerdo con la [Tabla 3-1](#).

4. Haga clic en el botón "Aceptar".

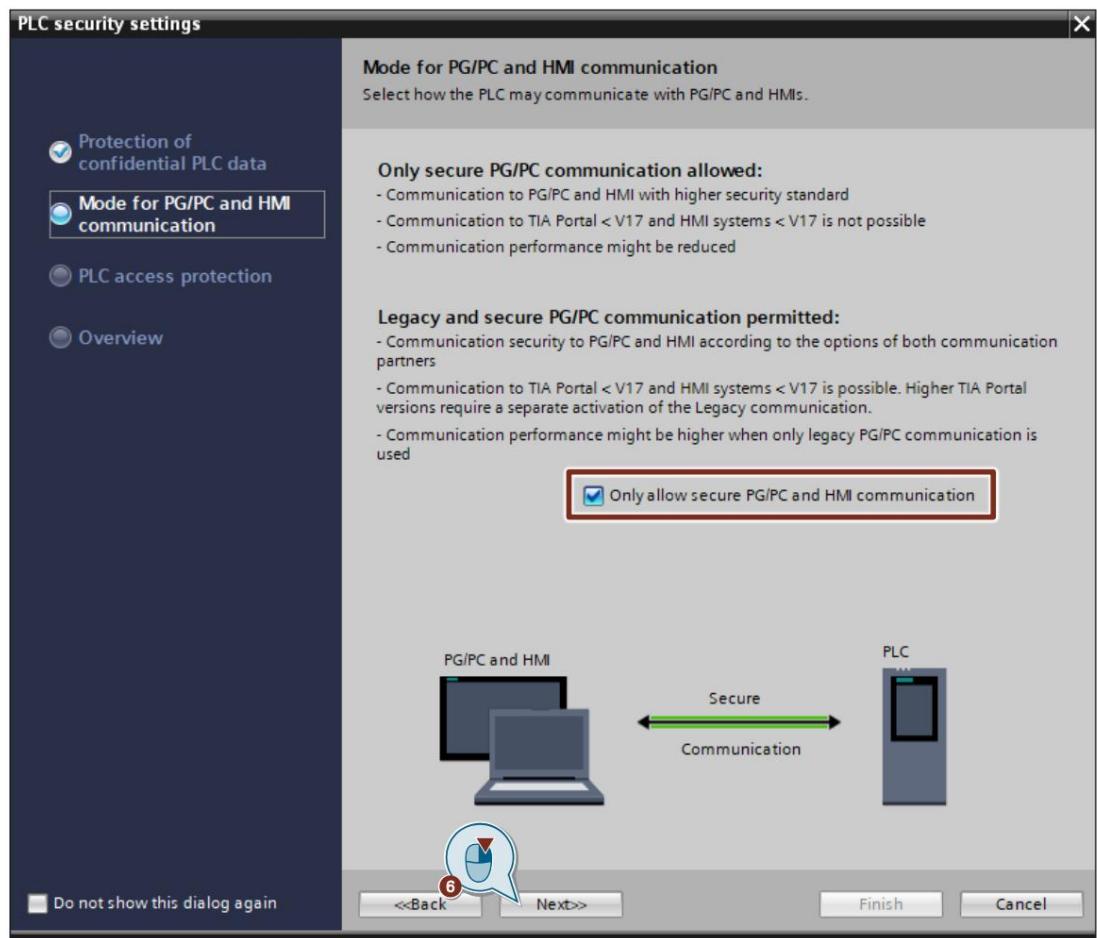
3 Ingeniería

5. Haga clic en el botón "Siguiente" para ir a la página siguiente.

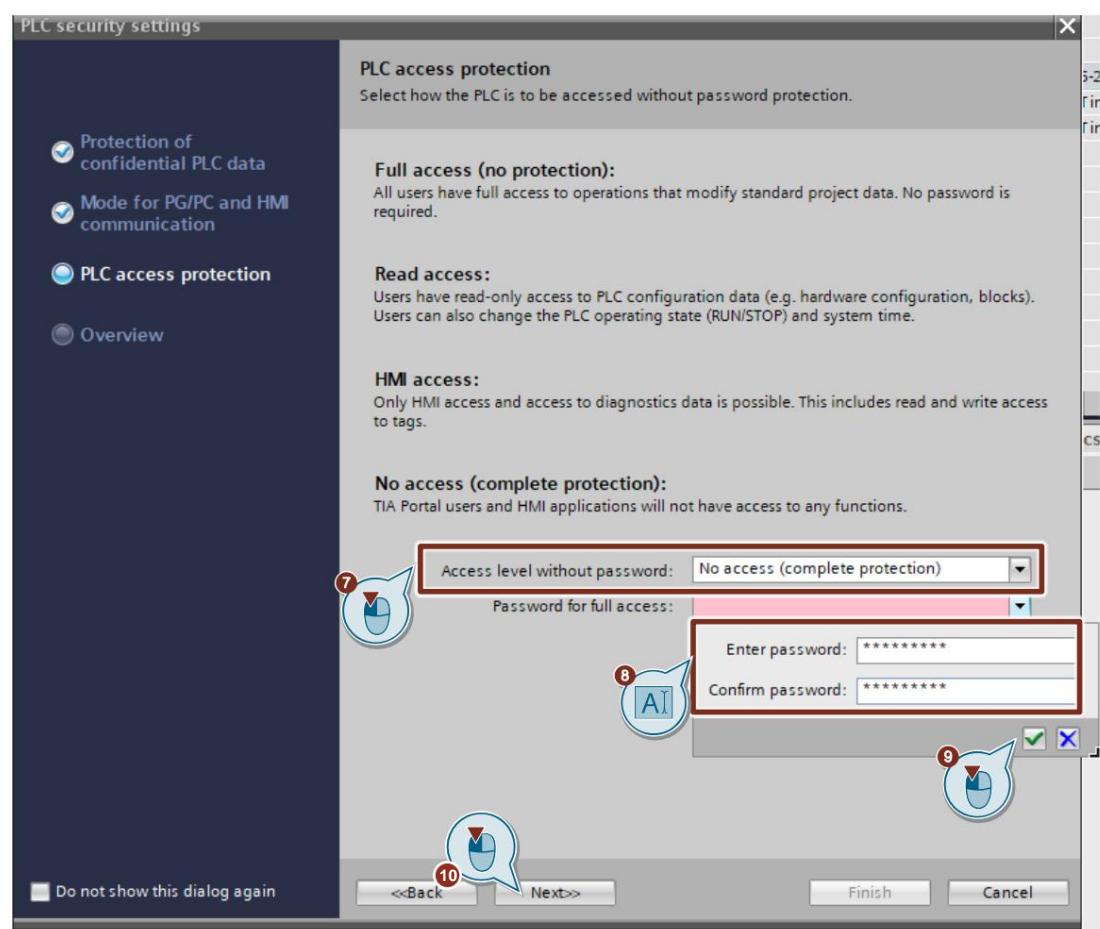


3 Ingeniería

6. En la segunda ventana se puede configurar el modo de comunicación PG/PC y HMI. Él La opción "Permitir solo comunicación segura PG/PC y HMI" está activada de forma predeterminada según el concepto Security-By-Default. Haga clic en el botón "Siguiente" para ir a la página siguiente.

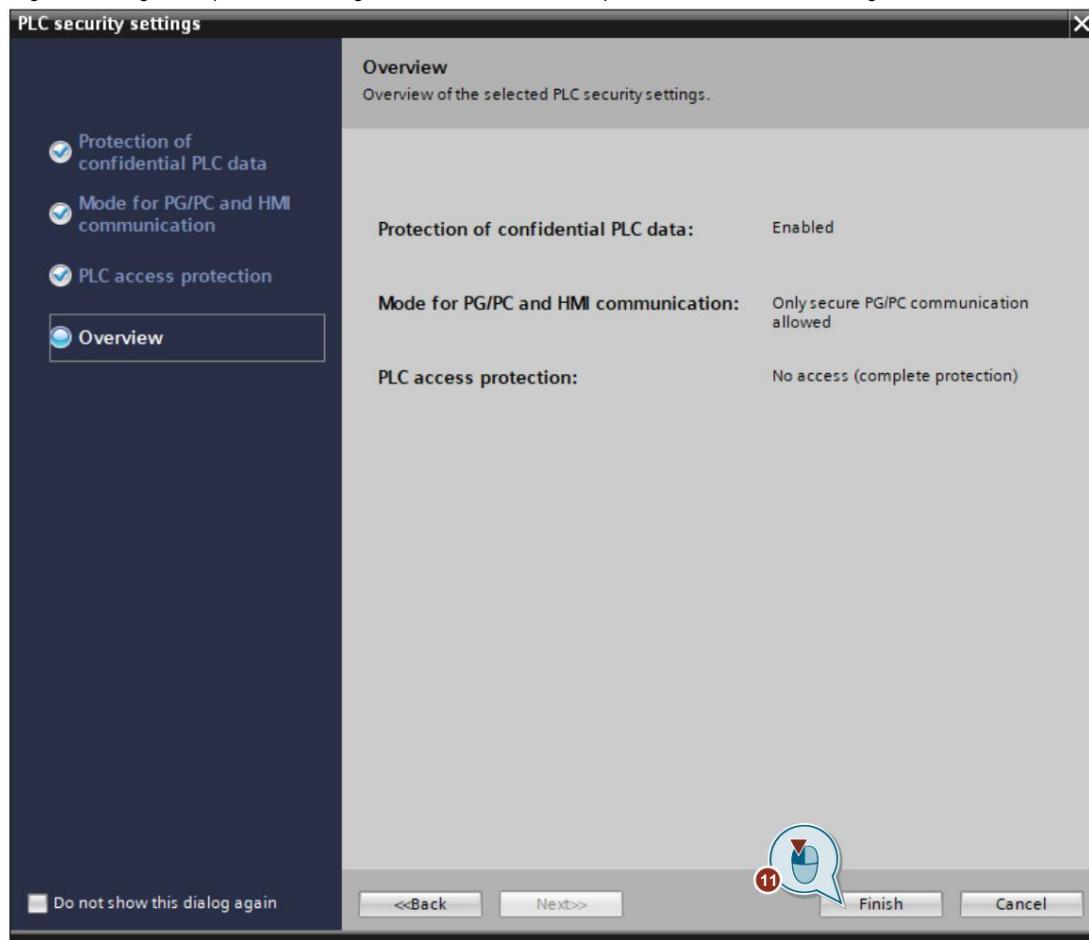


7. En la tercera ventana se puede configurar el nivel de acceso al PLC. De forma predeterminada, no se permite el acceso al PLC de acuerdo con el concepto de seguridad por defecto. Posteriormente, configurará la contraseña de acceso al PLC en el panel HMI para permitir la comunicación entre los dos dispositivos. Mantenga la opción predeterminada "Sin acceso (protección completa)".
8. Ingrese la contraseña de acceso completo en el campo de contraseña de acuerdo con la [Tabla 3-1](#) y confírmelo con una clave.
9. Haga clic en el siguiente símbolo.
10. Haga clic en el botón "Siguiente" para ir a la última página del asistente de seguridad.

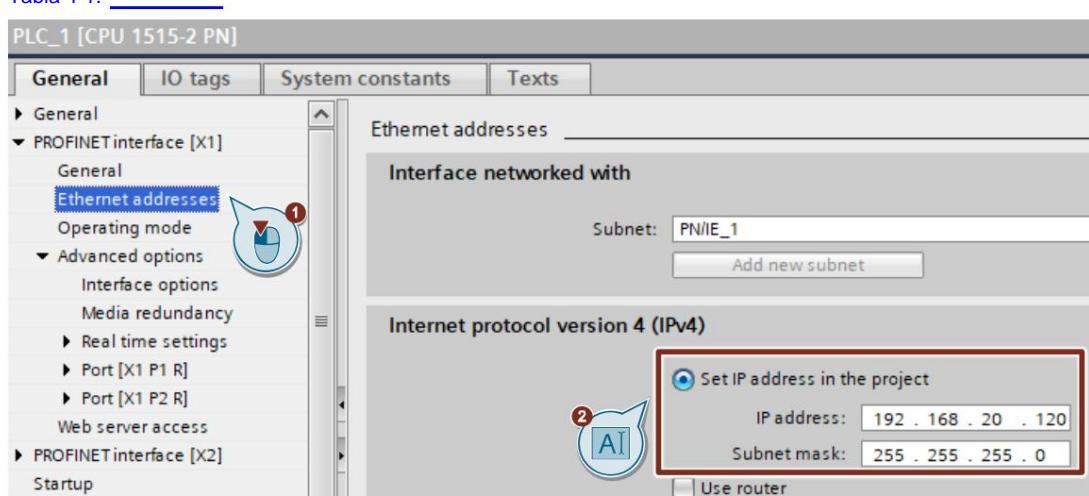
3 Ingeniería

3 Ingeniería

11. En la última ventana del asistente de seguridad, se puede encontrar una descripción general de las configuraciones de seguridad configuradas previamente. Haga clic en el botón "Finalizar" para finalizar el asistente de seguridad.

**3.2.2 Establecer la dirección IP**

- Navegue en el menú de propiedades del PLC hasta "Interfaz PROFINET [X1] > Direcciones Ethernet".
- Establezca la dirección IP y la máscara de subred del PLC. La dirección IP del PLC se puede encontrar en [la Tabla 4-1.](#)



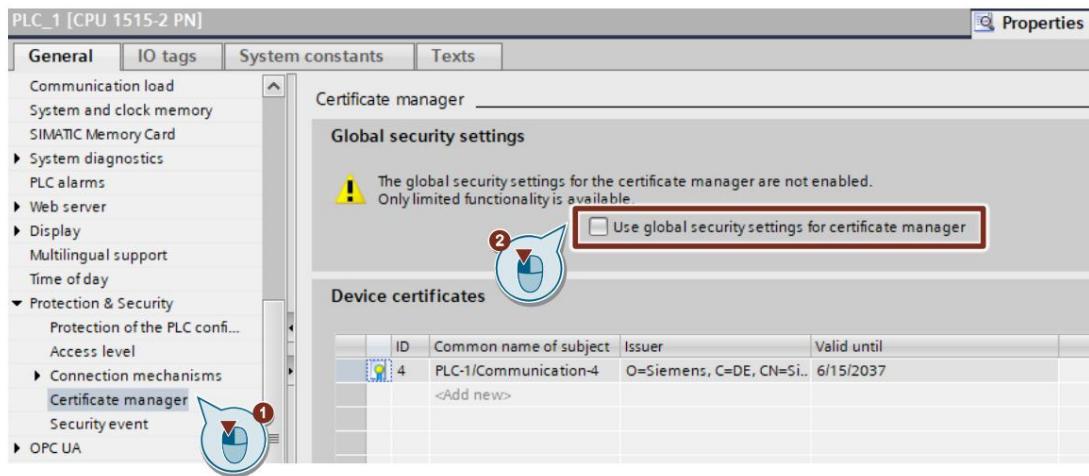
3.2.3 Activar la configuración de seguridad global para el administrador de certificados

1. En el menú de propiedades del PLC, vaya a "Protección y seguridad > Administrador de certificados".
2. Active la casilla de verificación "Usar configuración de seguridad global para el administrador de certificados".

En TIA Portal, existen dos métodos para administrar el certificado de PLC:

- localmente específico del dispositivo en el menú de propiedades del PLC
- globalmente para todo el proyecto TIA Portal en el árbol del proyecto en "Configuración de seguridad > Configuración".

La opción "Usar configuración de seguridad global para el administrador de certificados" activa el uso del administrador de certificados globales para asignar un certificado global al PLC.

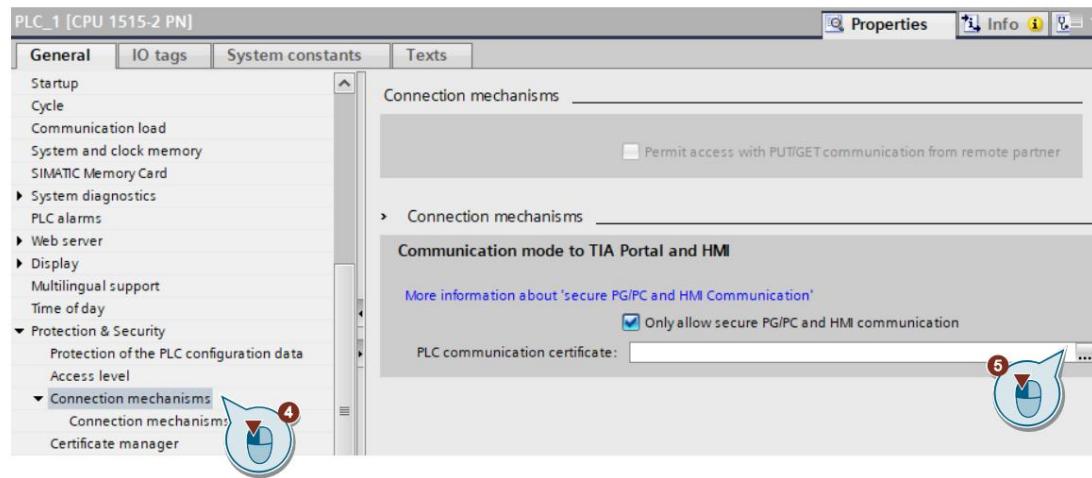


3. Al activar el administrador de certificados global, la configuración actual del certificado será perdida. Por lo tanto, aparece un mensaje de advertencia sobre la pérdida de claves y certificados actuales en el administrador de certificados local. Haga clic en el botón "Aceptar".



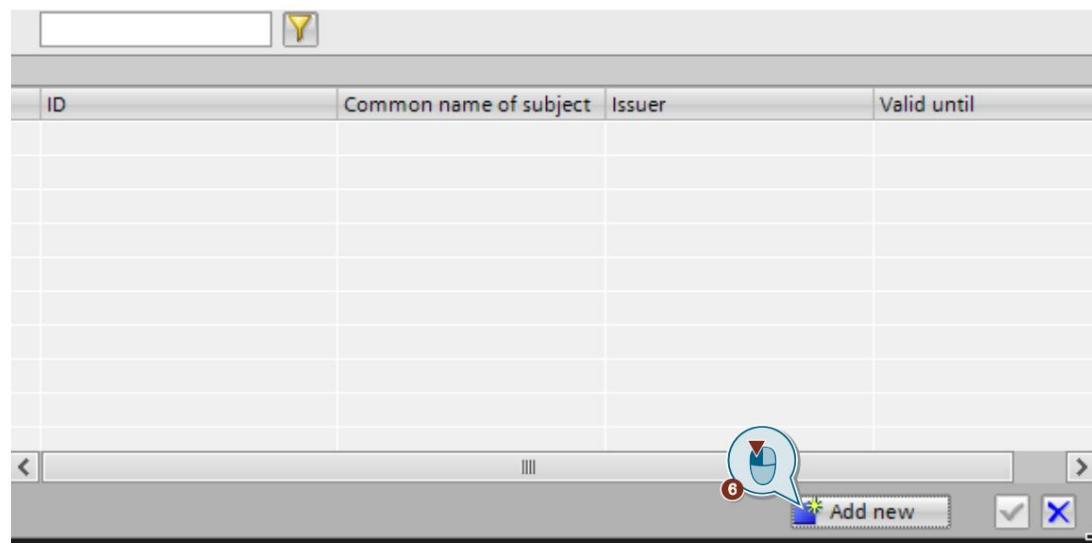
4. El certificado utilizado para la comunicación segura PG/PC y HMI debe crearse ya que el certificado creado localmente para el PLC se eliminó después de realizar el paso anterior.
Vaya a "Protección y seguridad > Mecanismo de conexión" en el menú de propiedades del PLC.
5. Haga clic en el siguiente botón para abrir el menú de creación de certificados.

3 Ingeniería



6. Haga clic en el botón "Agregar nuevo".

Se abre el cuadro de diálogo "Crear certificado".

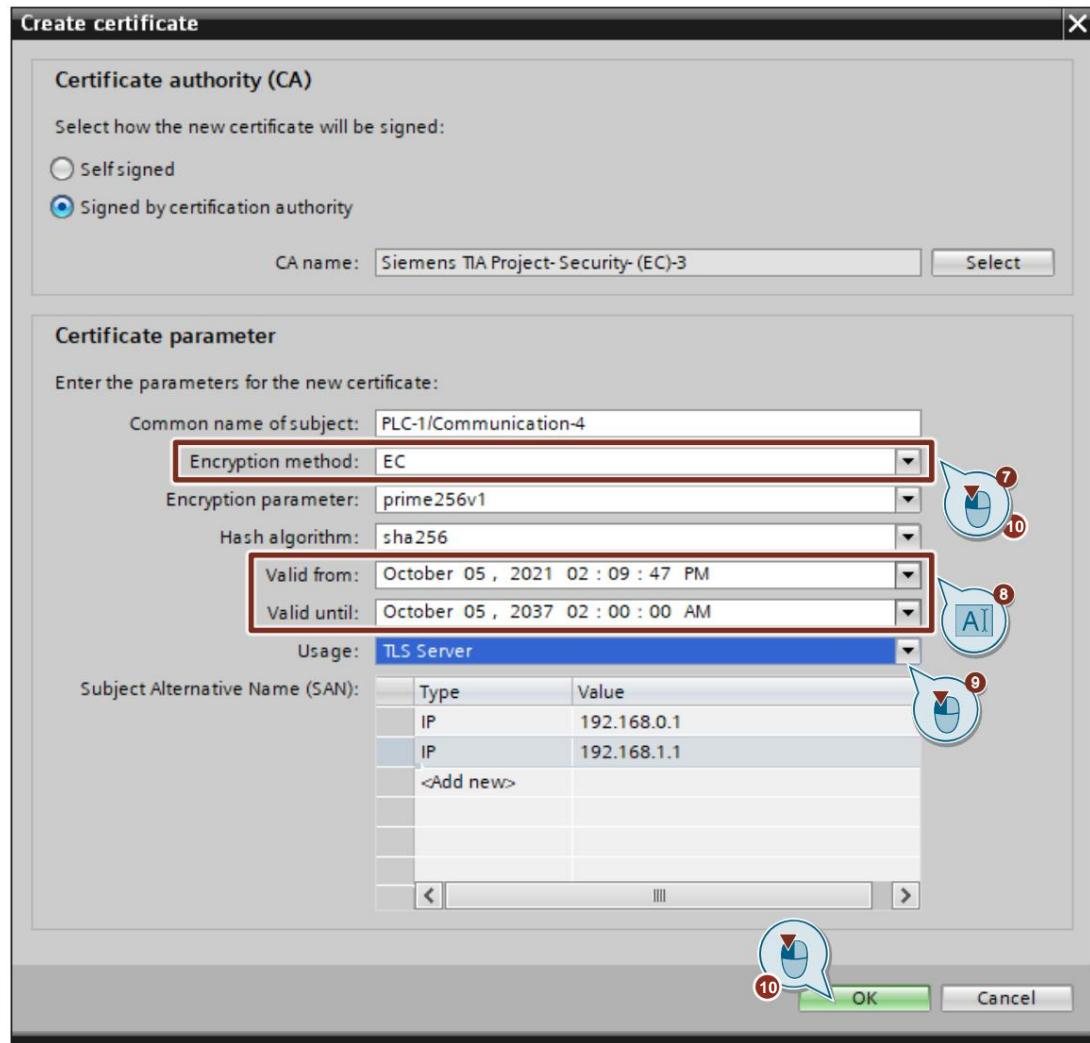


7. Configure los parámetros del certificado. Seleccione "EC" como método de cifrado.

8. Verifique la validez del certificado y ajústelo si es necesario.

9. Seleccione "Servidor TLS" para la opción "Uso".

10. Haga clic en el botón "Aceptar" para finalizar el proceso de creación del certificado.

3 Ingeniería

3.3 Configuración del panel HMI

NOTA La siguiente sección explica los pasos relevantes para configurar el panel HMI para comunicarse con la CPU S7-1500. Todos los pasos adicionales para configurar el panel HMI no se describen aquí, ya que son irrelevantes para el propósito de este ejemplo de aplicación. Puede encontrar más información sobre la configuración del panel HMI en el siguiente enlace \4\.

NOTA También se pueden utilizar otros modelos de paneles HMI. Consulte el capítulo [7.1](#) para obtener una lista completa de dispositivos compatibles con la función de comunicación segura PG/PC y HMI.

La comunicación HMI segura funciona de manera similar a como se describe en el capítulo [2.2.2](#). Sin embargo, hay dos escenarios a considerar:

- Cuando el certificado de comunicación del PLC ya está disponible en el panel HMI con el estado "confiable", se establece automáticamente una comunicación HMI segura entre el PLC y el panel HMI. Esto se aplica a los siguientes casos:
 - El PLC y el panel HMI están configurados con el mismo proyecto de TIA Portal
 - El PLC y el panel HMI están configurados en dos proyectos diferentes, pero se usa un proxy de dispositivo. Esto se explica en el capítulo [3.3.1](#) y el capítulo [3.3.2](#) respectivamente.
- Cuando el certificado de comunicación del PLC no está disponible en el estado "confiable" en el panel HMI, verá un mensaje en la vista de alarma del panel HMI que le informa que el PLC no es confiable junto con un código de error. En este caso, debe etiquetar el certificado de comunicación del PLC en el panel HMI como "confiable". Esto se explica en capítulo [3.3.3](#).

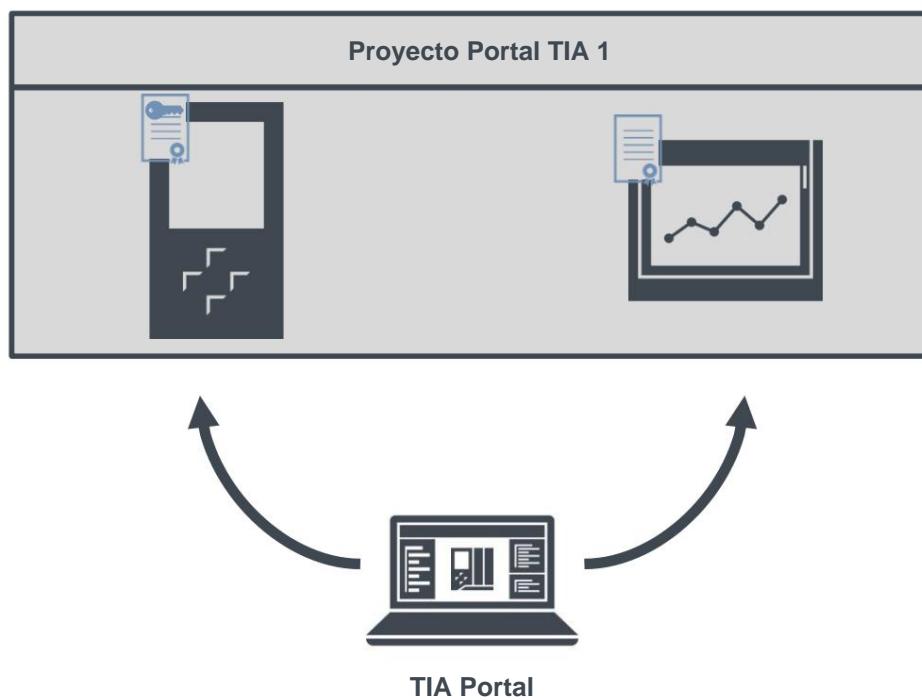
Para configurar un panel HMI para comunicarse con el PLC, distinguimos entre tres escenarios diferentes:

1. El PLC y el panel HMI están en el mismo proyecto de TIA Portal.
2. El PLC y el panel HMI están en diferentes proyectos del TIA Portal.
3. El panel HMI no está configurado con TIA Portal (conexión con WinCC SCADA V7 sistemas).

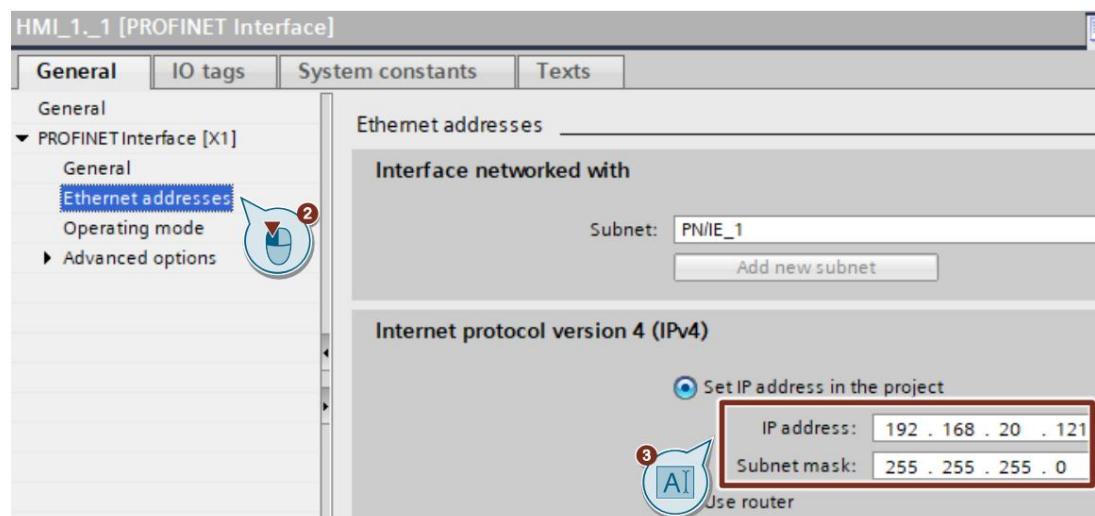
La configuración para cada uno de estos casos se muestra en esta sección.

3 Ingeniería**3.3.1 El PLC y el panel HMI están en el mismo proyecto de TIA Portal**

Figura 3-1

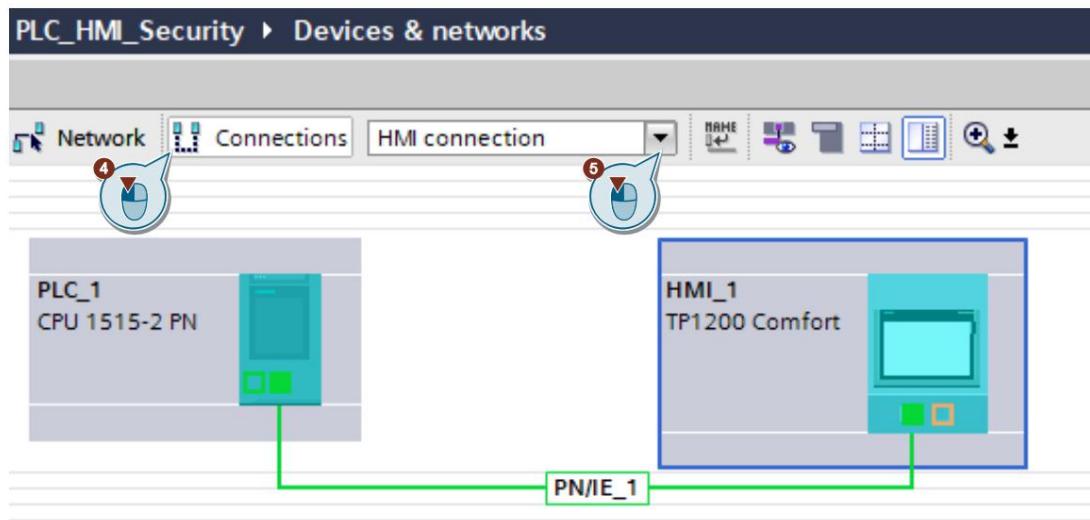


1. Agregue un nuevo panel HMI al proyecto, p. ej. SIMATIC TP1200 Comfort Panel, V17.0.
2. En el menú de propiedades del panel HMI, vaya a "Interfaz PROFINET [X1] > Ethernet direcciones".
3. Establezca la dirección IP y la máscara de subred del panel HMI. La dirección IP debe estar en la misma subred que la dirección IP del PLC.

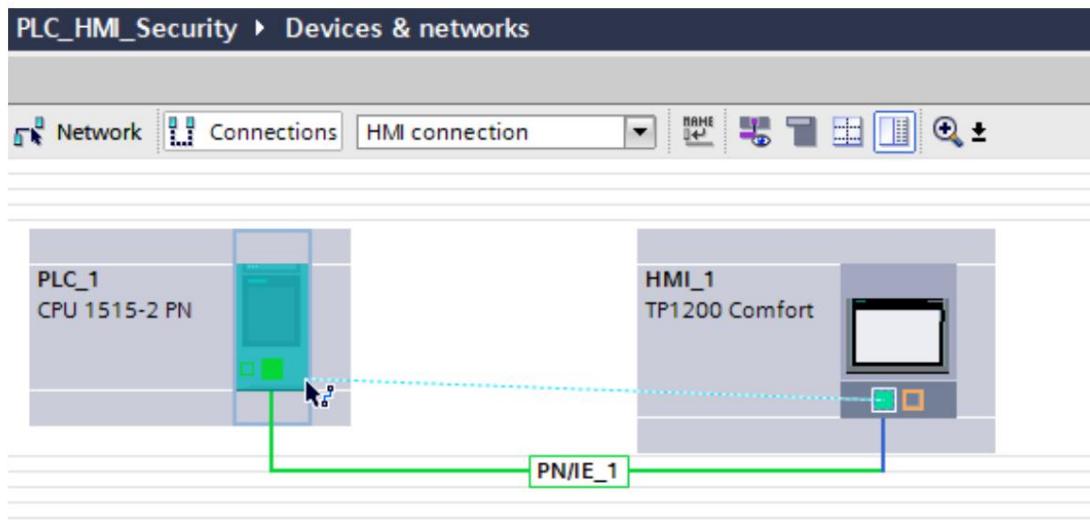


3 Ingeniería

4. En la "Vista de red" del proyecto, haga clic en "Conexiones".
5. Seleccione "Conexión HMI" en el menú desplegable.

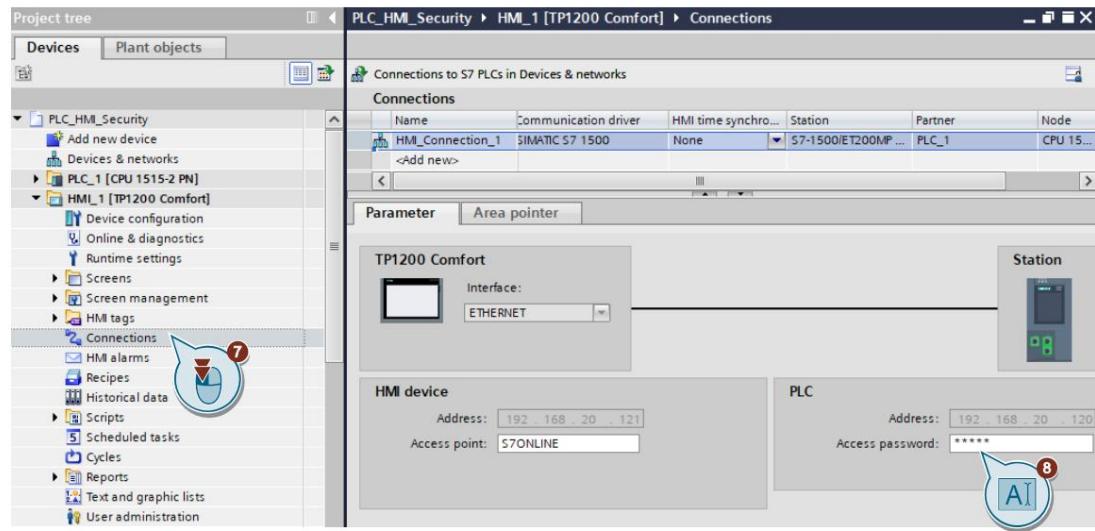


6. Arrastre y suelte una conexión desde el panel HMI al PLC para establecer una conexión HMI entre ambos dispositivos.



7. Haga doble clic en "Conexiones" en el árbol del proyecto en la carpeta de dispositivos del panel HMI.
8. Introduzca la contraseña para el acceso HMI de la CPU S7-1500, como se especifica en la Tabla 3-1.

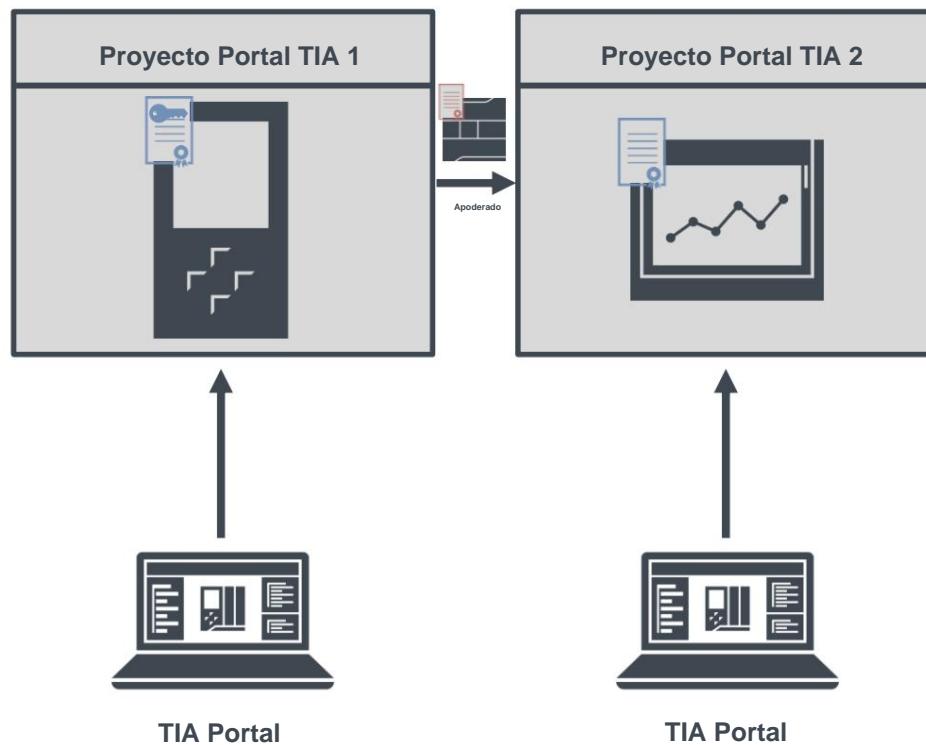
3 Ingeniería



La conexión segura entre el PLC y el panel HMI ya está configurada.

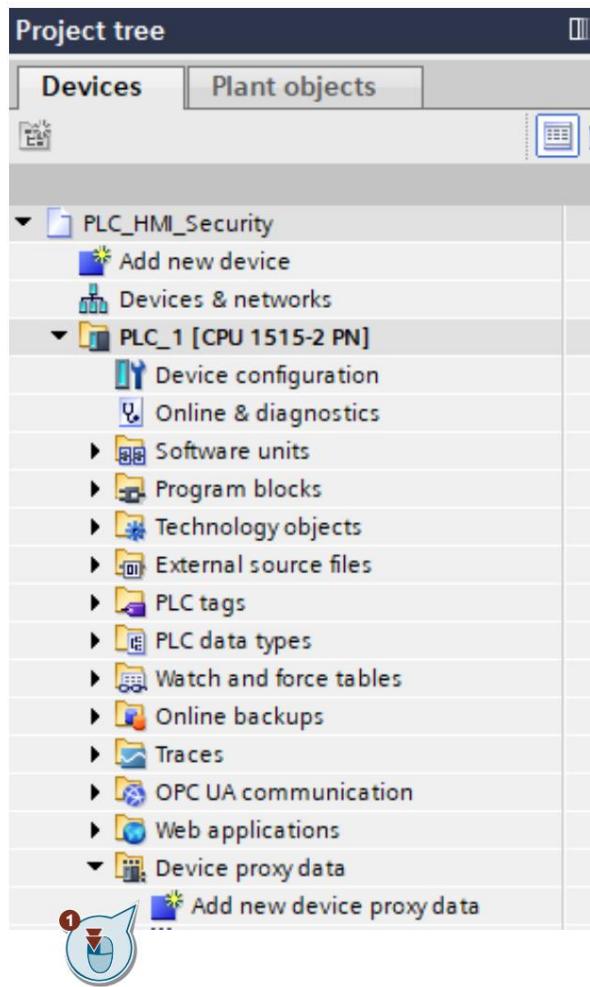
3.3.2 El PLC y el panel HMI están en dos proyectos diferentes de TIA Portal

Figura 3-2

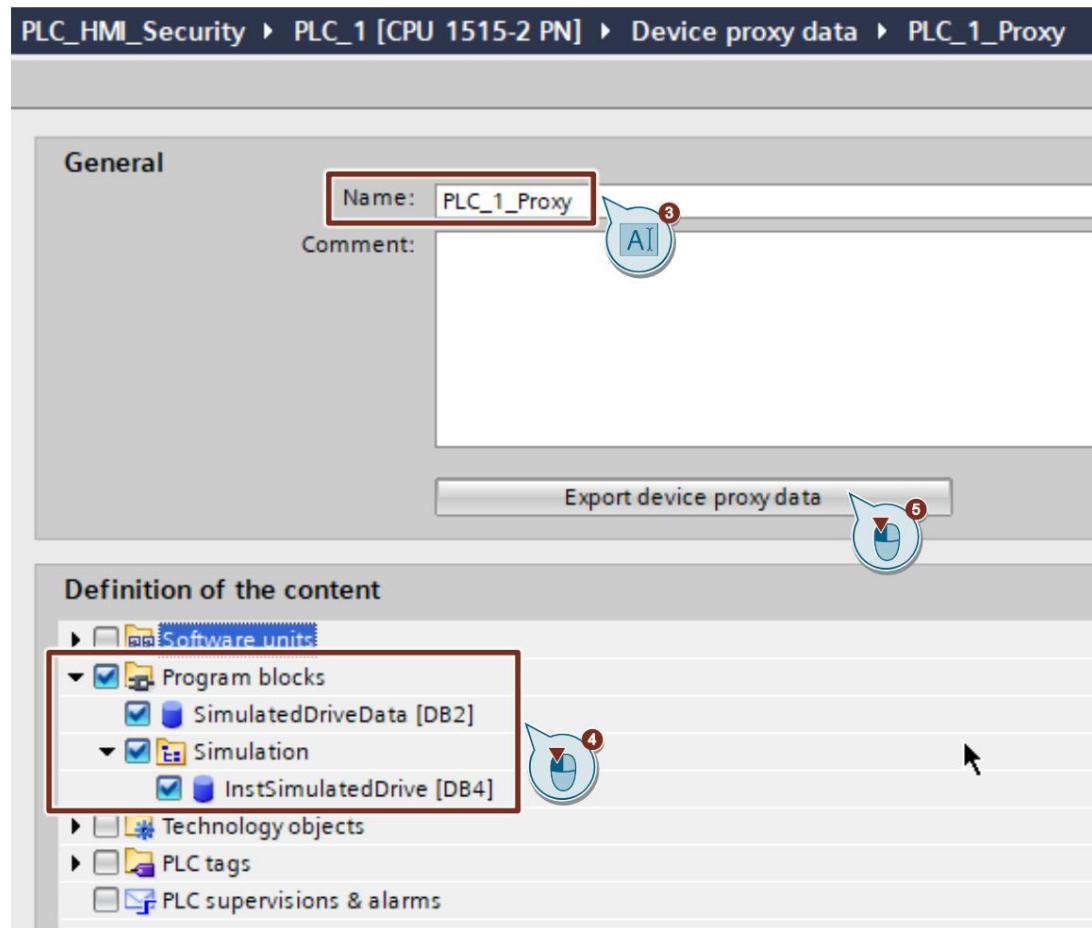


Si el PLC y el panel HMI están en dos proyectos diferentes, se debe exportar un proxy de dispositivo desde el proyecto del PLC e importarlo en el proyecto del panel HMI. Este dispositivo proxy contiene la configuración del PLC, así como el certificado necesario para la conexión segura. También puede incluir el bloques de programa, etiquetas y otras opciones del PLC.

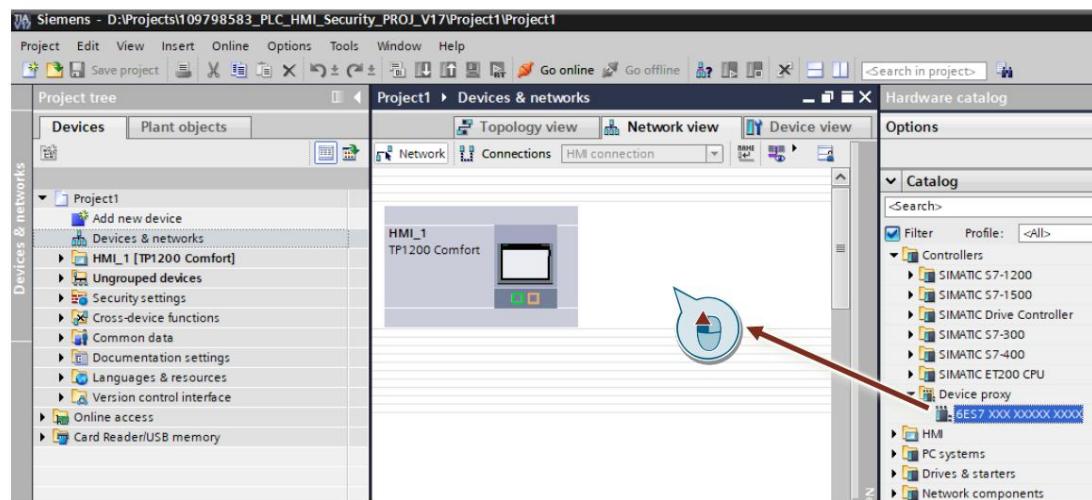
1. En el proyecto PLC, en el árbol del proyecto, navegue hasta "Datos proxy del dispositivo" y haga doble clic en "Aregar nuevos datos proxy del dispositivo". Se crea un nuevo proxy de dispositivo.



2. Haga doble clic en el proxy del dispositivo recién creado para abrir el menú de configuración.
3. En el menú de configuración, ingrese un nombre para el proxy del dispositivo.
4. Marque la casilla de verificación "Bloques de programa" para exportar los bloques de programa de PLC con el dispositivo apoderado. Si se necesitan otros parámetros de PLC en el proxy del dispositivo, también se pueden elegir aquí.
5. Haga clic en el botón "Exportar datos proxy del dispositivo" para guardar el archivo proxy del dispositivo en su PG.



6. En el proyecto del panel HMI, se debe importar el archivo proxy del dispositivo. Vaya a "Hardware catalog" y agregue un proxy de dispositivo al proyecto.

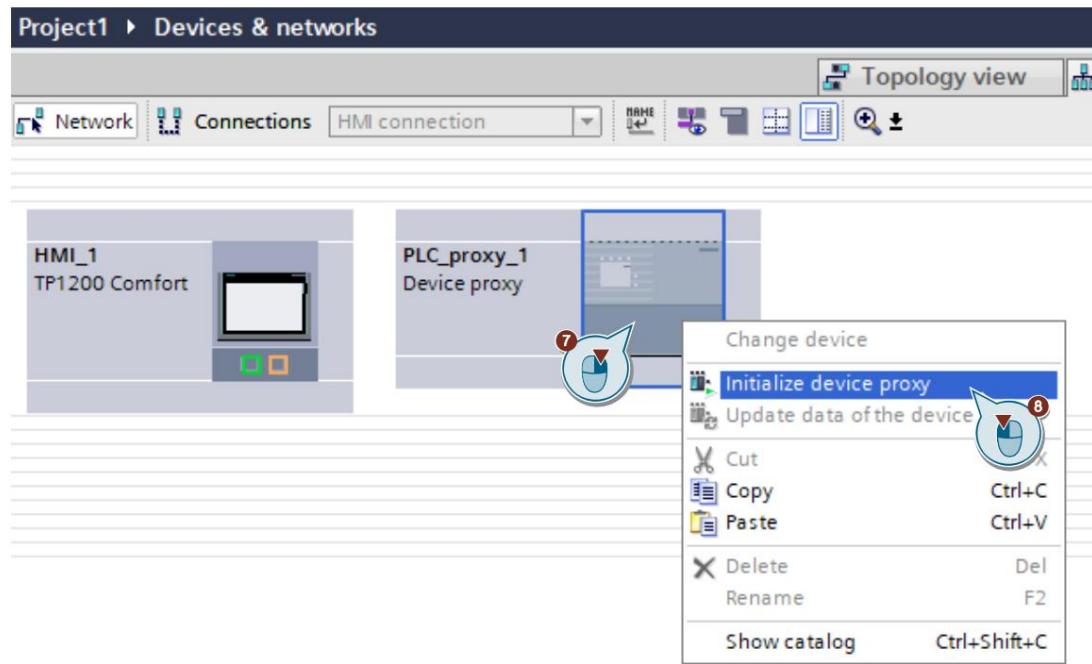


3 Ingeniería

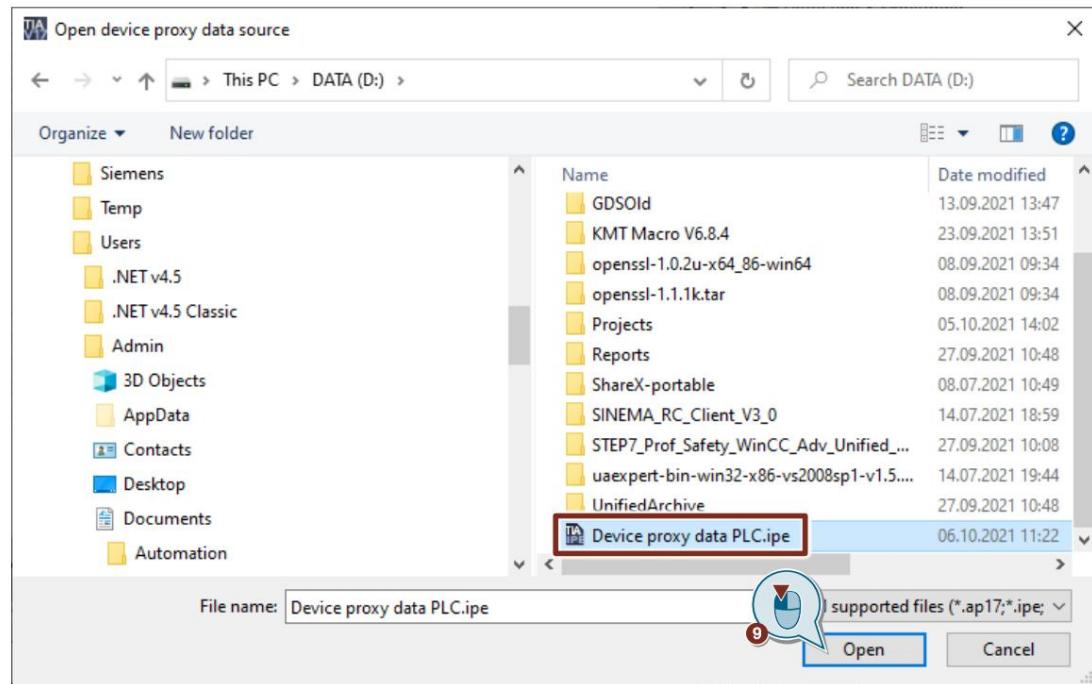
7. Haga clic derecho en el proxy del dispositivo.

Se abre el menú contextual.

8. Elija el menú "Inicializar proxy del dispositivo".

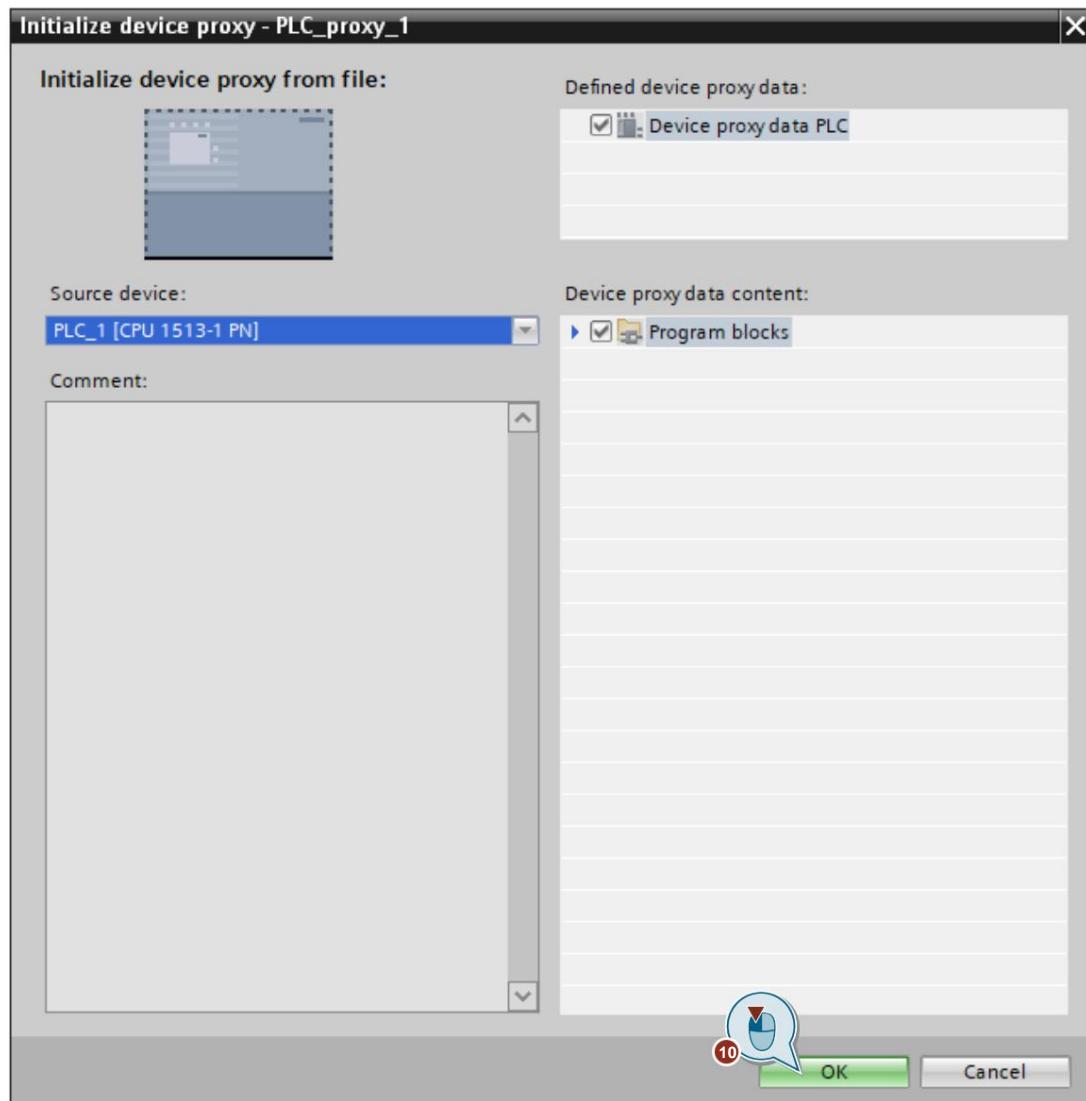


9. Elija el archivo proxy del dispositivo guardado en el paso 5.



3 Ingeniería

10. La información del PLC del Proyecto PLC TIA se puede ver aquí. Haga clic en el botón "Aceptar".



NOTA Los certificados de proyecto de PLC utilizados para asegurar la conexión se incluyen en el archivo proxy del dispositivo y estarán automáticamente disponibles para el panel HMI cuando este archivo se importe al proyecto HMI.

11. Repita los pasos 3 a 8 del capítulo [3.3.1](#) para establecer una conexión HMI entre el panel HMI y el proxy del dispositivo.

NOTA Dependiendo de su proyecto, es posible que se necesite otra configuración de HMI con respecto al acceso a las etiquetas de proxy del dispositivo. Esta configuración está detrás del alcance de este ejemplo de aplicación.

3.3.3 **El panel HMI no está configurado en el TIA Portal - Conexión con WinCC SCADA V7 Sistemas**

NOTA Las siguientes instrucciones son válidas a partir de WinCC SCADA V7.5 SP2 Update 4.

La conexión a WinCC SCADA V7 funciona de manera similar al método de proxy del dispositivo que se muestra arriba. Se debe exportar un archivo del proyecto PLC y luego importarlo en el proyecto WinCC SCADA. Para exportar el archivo desde el proyecto del PLC, se necesita una herramienta de exportación específica. Consulte este enlace para obtener más información [\5\](#).

Consulte el enlace [\6\](#) para obtener una explicación detallada de cómo conectarse de forma segura con WinCC SCADA V7.5.

4 Instalación y puesta en marcha

4.1 configuración de hardware

El Capítulo [1.3](#) enumera los componentes de hardware necesarios.



PRECAUCIÓN

Tenga en cuenta las directrices de instalación para el S7-1500 PLC y el SIMATIC TP1200 Comfort Panel. Lea el manual del dispositivo correspondiente [\71](#) y [\81](#).

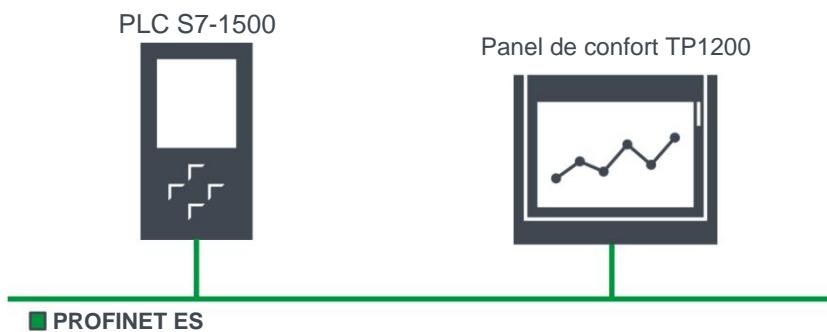


PRECAUCIÓN

¡Encienda la fuente de alimentación solo después de haber completado y comprobado el montaje!

La siguiente figura muestra la configuración del hardware del ejemplo de aplicación.

Figura 4-1



La siguiente tabla proporciona una descripción general de todas las direcciones IP utilizadas en este ejemplo. Se asume la asignación de direcciones IP estáticas.

Tabla 4-1

Componente	dirección IP
CPU 1515-2 PN	192.168.20.120
Panel de confort SIMATIC TP1200	192.168.20.121

La máscara de subred en todos los componentes de la red es 255.255.255.0.

4.2 Instalación de componentes de hardware y software

Para cargar los componentes de hardware y software, proceda de la siguiente manera:

1. Instale los componentes de hardware y software que se muestran en [la Tabla 1-1](#) y [la Tabla 1-2](#) de acuerdo con la descripción de los manuales de operación de los respectivos componentes.
2. Conecte los componentes de hardware como se muestra en [la Figura 4-1](#).
3. Descomprima el archivo "109798583_PLC_HMI_Security_PROJ_V17.zip".

4 Instalación y puesta en marcha

4.3 Cargar componentes de hardware

4.3.1 Cargue el autómata S7-1500

Requisito previo

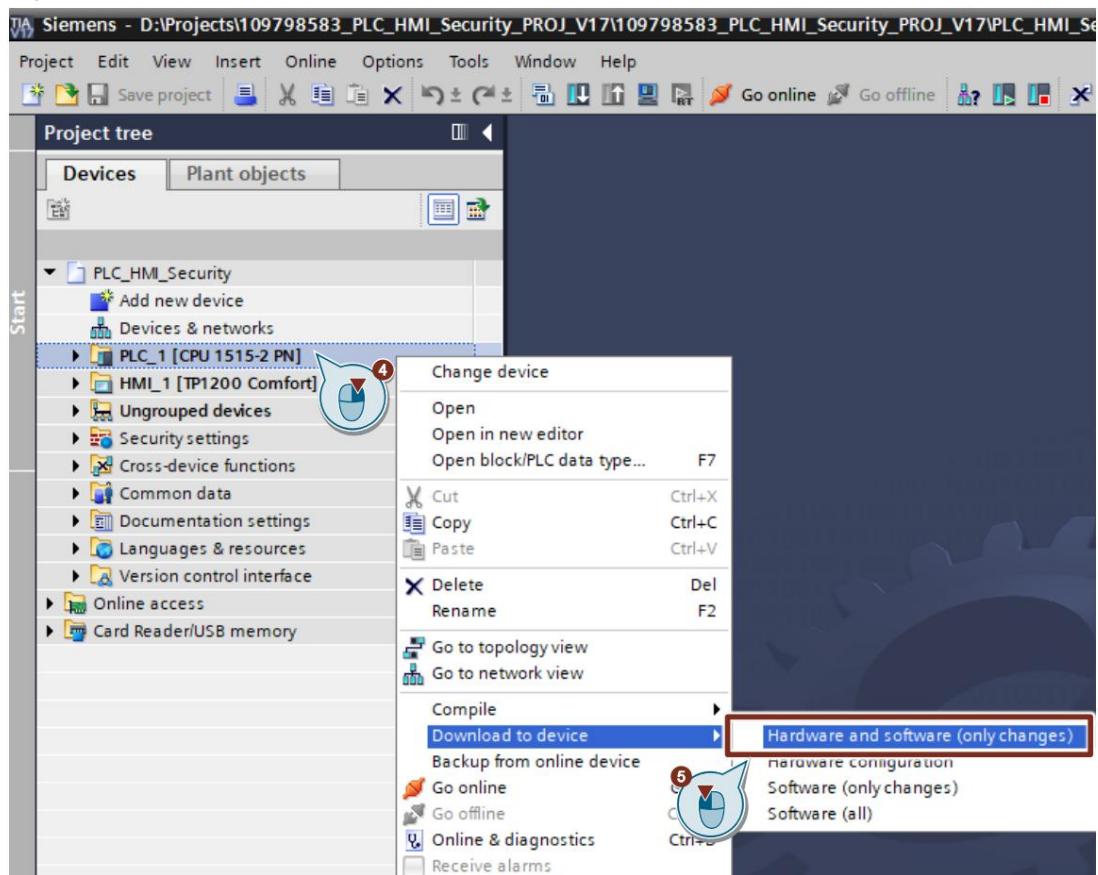
- Ha asignado a la CPU S7-1500 la dirección IP que ha configurado en el proyecto (ver [Tabla 4-1](#)).
- El PC de ingeniería y el PLC S7-1500 están en la misma subred IP.

Guía

Proceda de la siguiente manera para cargar la configuración en el PLC S7-1500:

1. Inicie TIA Portal V17.
2. Abra el proyecto "PLC_HMI_Security.ap17".
3. Conecte el cable Ethernet del PC de ingeniería con el PLC S7-1500.
4. Haga clic con el botón derecho en la carpeta de dispositivos del S7-1500 PLC en el árbol del proyecto. El menú contextual se abre
5. Seleccione el menú "Descargar en dispositivo > Hardware y software (solo cambios)".

Figura 4-2

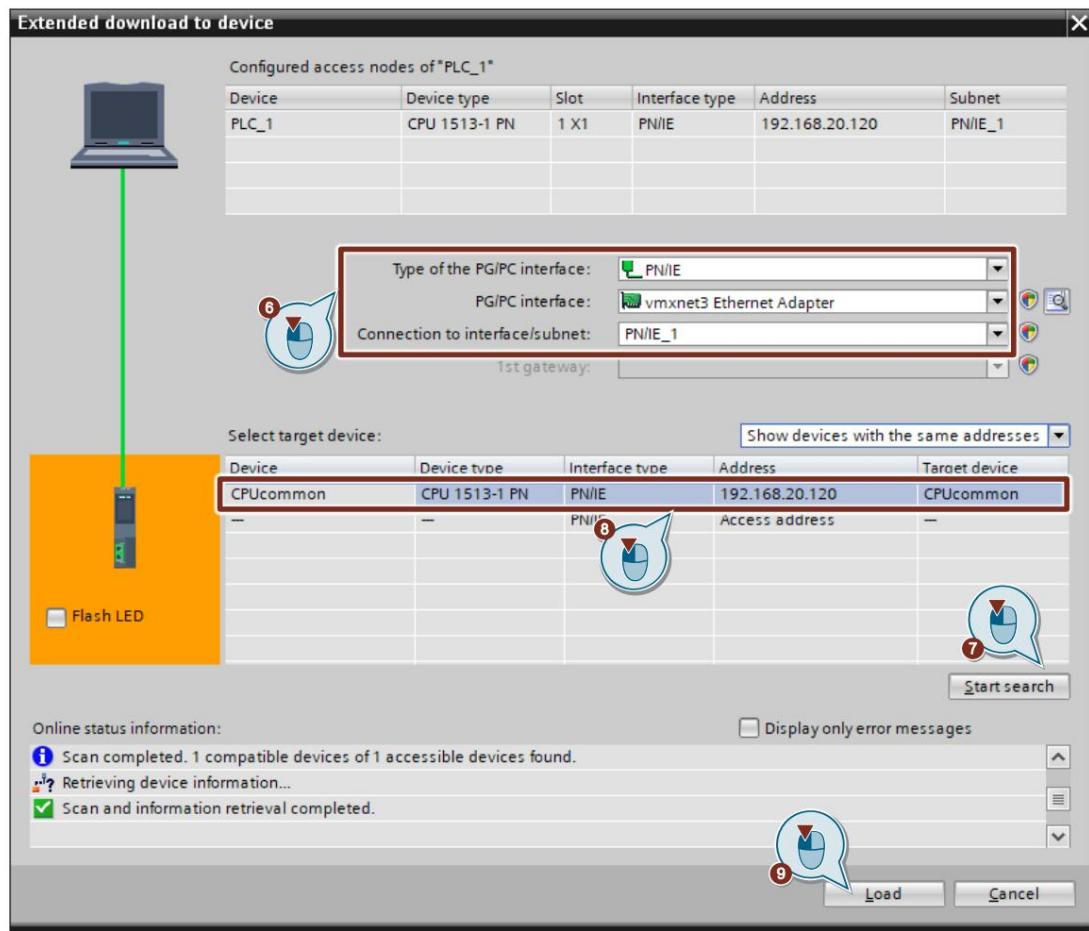


6. En el cuadro de diálogo "Descarga extendida al dispositivo", configure los parámetros de la interfaz.
7. Haga clic en el botón "Iniciar búsqueda".

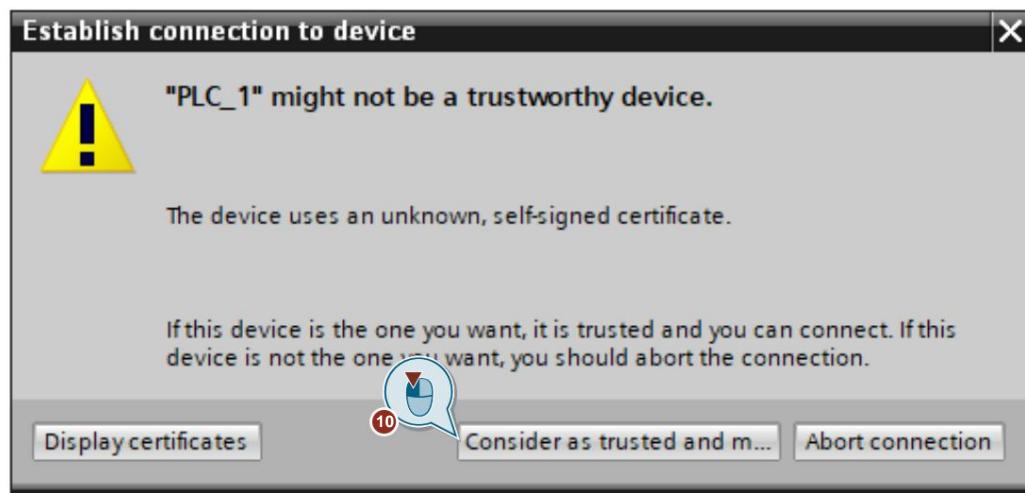
El S7-1500 PLC se muestra en la lista "Seleccionar dispositivo de destino".

8. Seleccione el PLC S7-1500 en la lista "Seleccionar dispositivo de destino".
9. Haga clic en el botón "Cargar".

4 Instalación y puesta en marcha



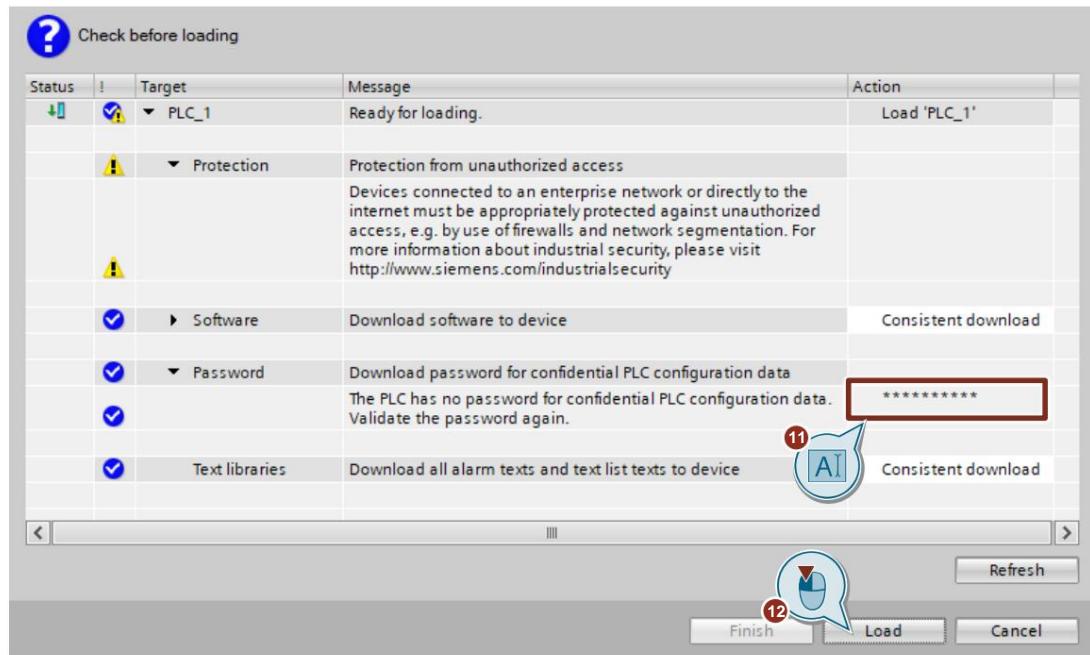
10. Aparece un mensaje de advertencia que indica que el certificado de la CPU no es confiable. Considera el Certificado de CPU para ser confiable para continuar cargando.



NOTA Este mensaje aparece durante la primera descarga al PLC para notificar al usuario que la PG aún no confía en el certificado autofirmado del PLC. Esto es importante ya que la base de la comunicación segura PG/PC y HMI es la verificación del certificado del PLC por parte del panel PG o HMI. Consulte el capítulo [2.2.2](#) para obtener más información sobre este mensaje de advertencia.

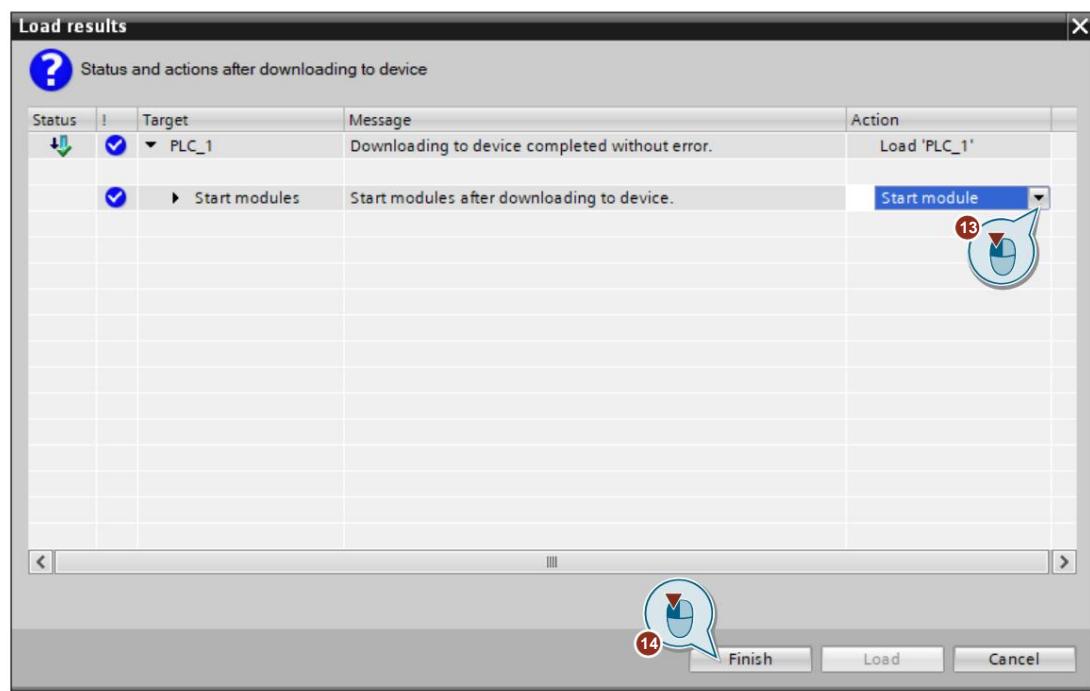
4 Instalación y puesta en marcha

11. Introduzca la contraseña confidencial de datos de configuración del PLC en el cuadro de diálogo "Cargar vista previa".
La contraseña se puede encontrar [en la Tabla 3-1](#).
12. Haga clic en el botón "Cargar".



NOTA Consulte el capítulo [2.3](#) para obtener más información sobre los datos de configuración confidenciales del PLC.

13. Seleccione la acción "Iniciar módulo" en el cuadro de diálogo "Cargar resultados".
14. Haga clic en el botón "Finalizar".



4 Instalación y puesta en servicio**4.3.2 Cargue el SIMATIC TP1200 Comfort Panel****Requisito previo**

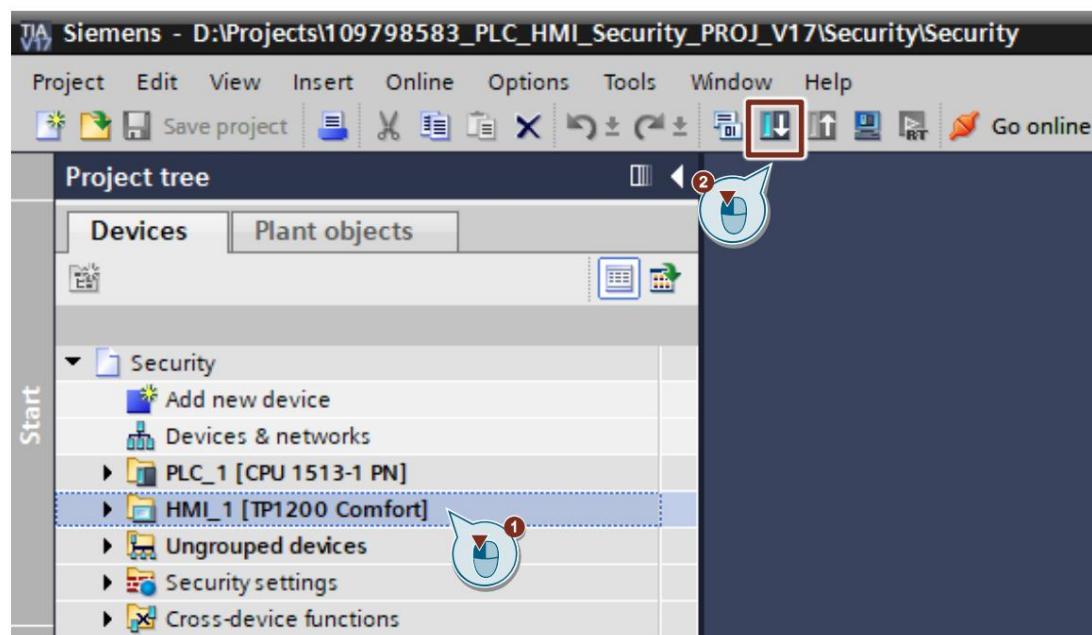
- Ha asignado al SIMATIC TP1200 Comfort Panel la dirección IP que ha configurado en el proyecto (ver [tabla 4-1](#)).
- El PC de ingeniería y el SIMATIC TP1200 Comfort Panel están en la misma subred IP.

Guía

Proceda de la siguiente manera para cargar la configuración en el SIMATIC TP1200 Comfort Panel: 1.

Seleccione la carpeta de dispositivos del SIMATIC TP1200 Comfort Panel en el árbol del proyecto.

2. Haga clic en el botón "Descargar en dispositivo".

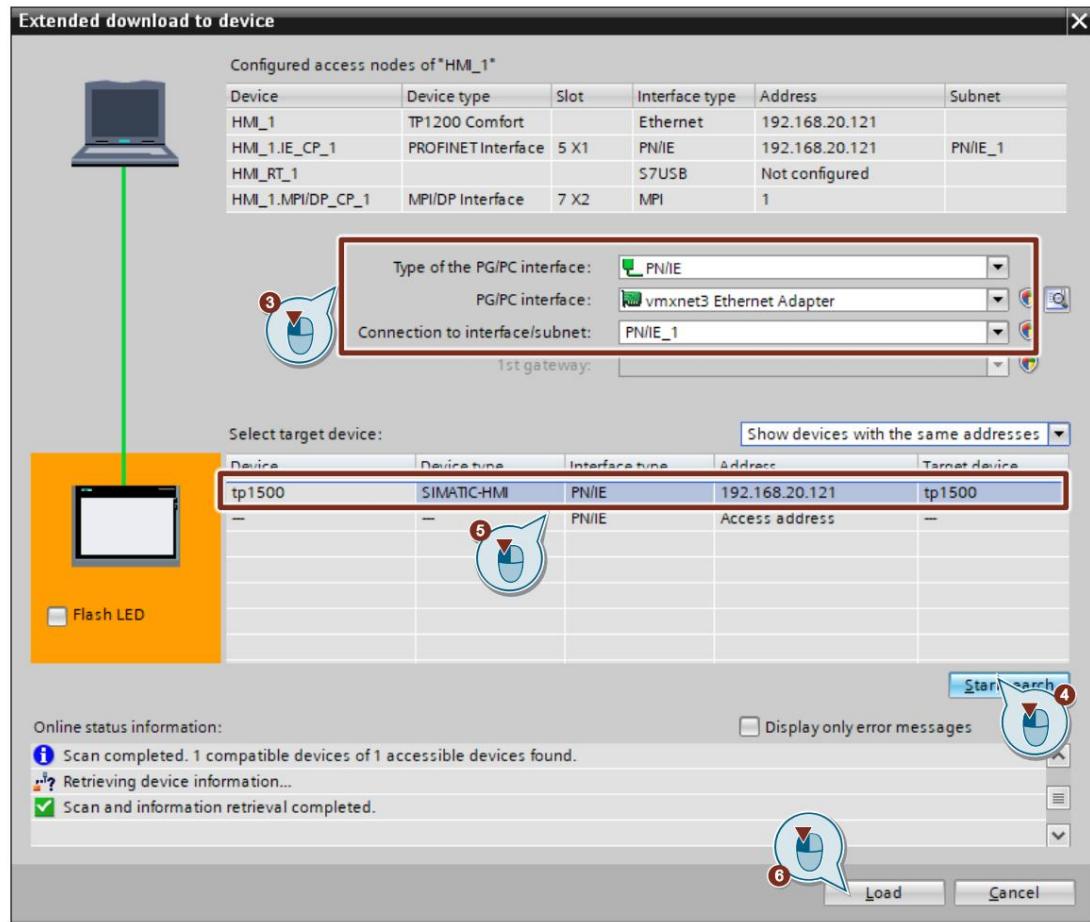


3. En el menú "Descarga extendida al dispositivo", configure los parámetros de la interfaz.
4. Haga clic en el botón "Iniciar búsqueda".

El panel HMI se muestra en la lista "Seleccionar dispositivo de destino".

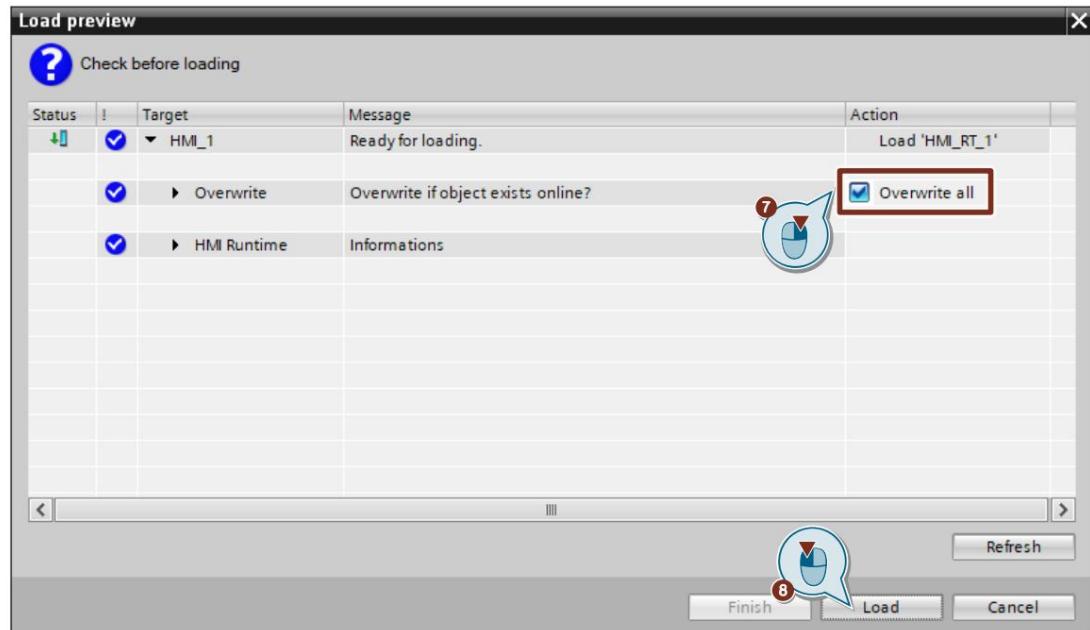
5. Seleccione el Panel HMI en la lista "Seleccionar dispositivo de destino".
6. Haga clic en el botón "Cargar".

4 Instalación y puesta en marcha



7. Active la casilla de verificación "Sobrescribir todo" en el cuadro de diálogo "Cargar vista previa".

8. Haga clic en el botón "Cargar".



4 Instalación y puesta en marcha

4.4 Operación

Introducción

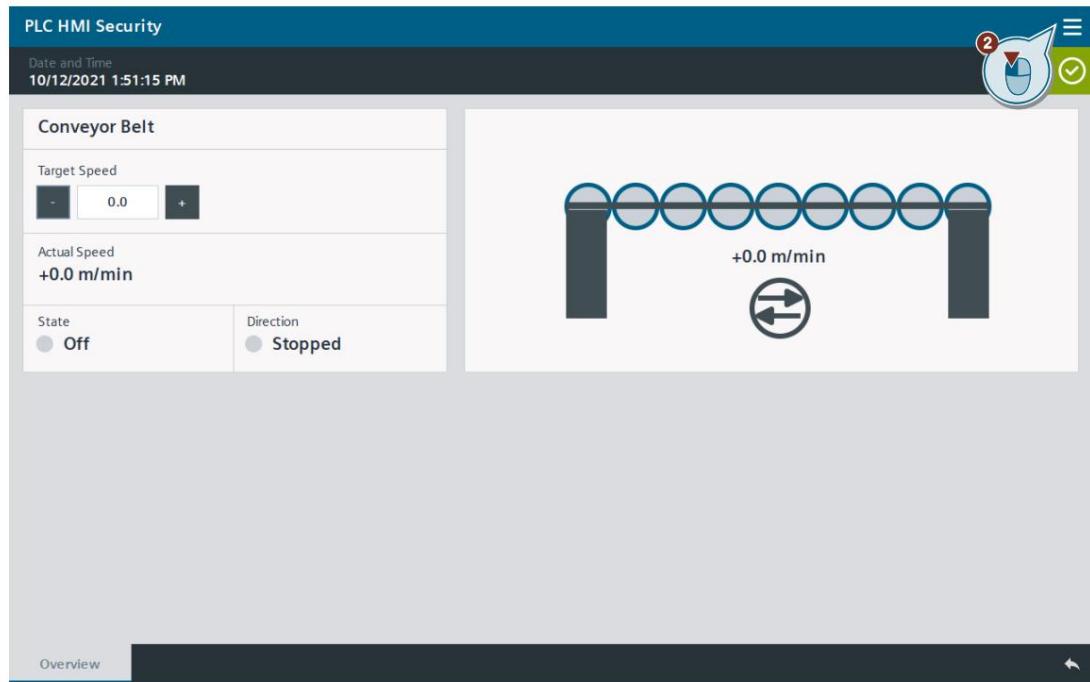
Esta sección le mostrará cómo utilizar las funciones del ejemplo de aplicación descrito anteriormente.

Procedimiento

1. En la página de inicio del panel HMI, haga clic en "Iniciar aplicación".

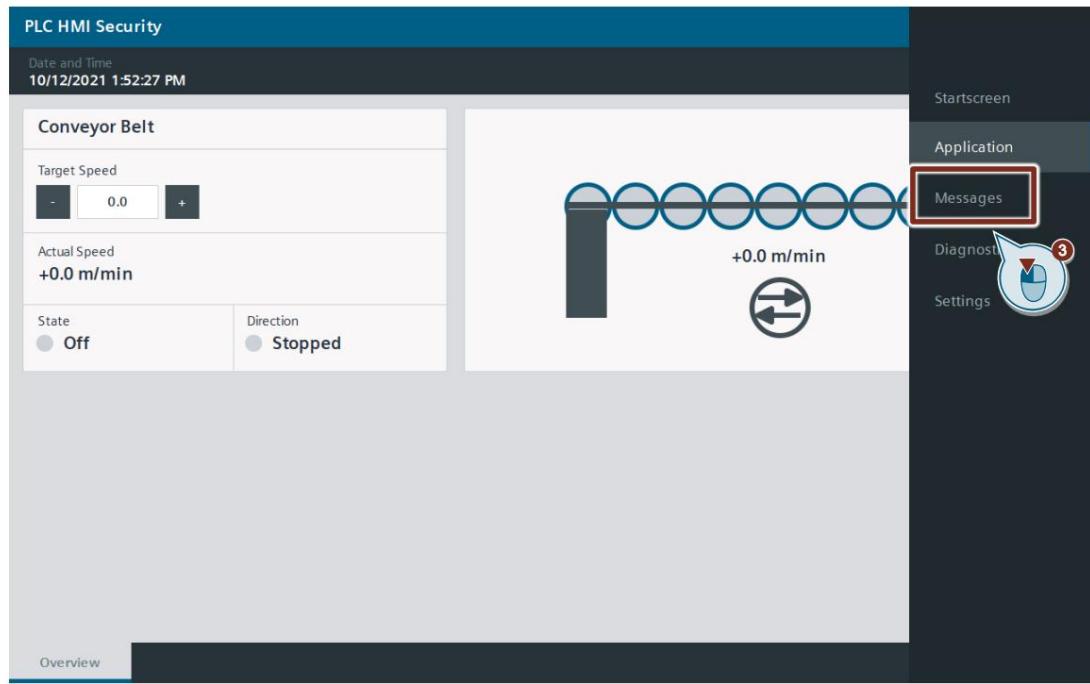


2. Haga clic en el botón "Navegación" en la esquina superior derecha para abrir el menú de navegación.



4 Instalación y puesta en marcha

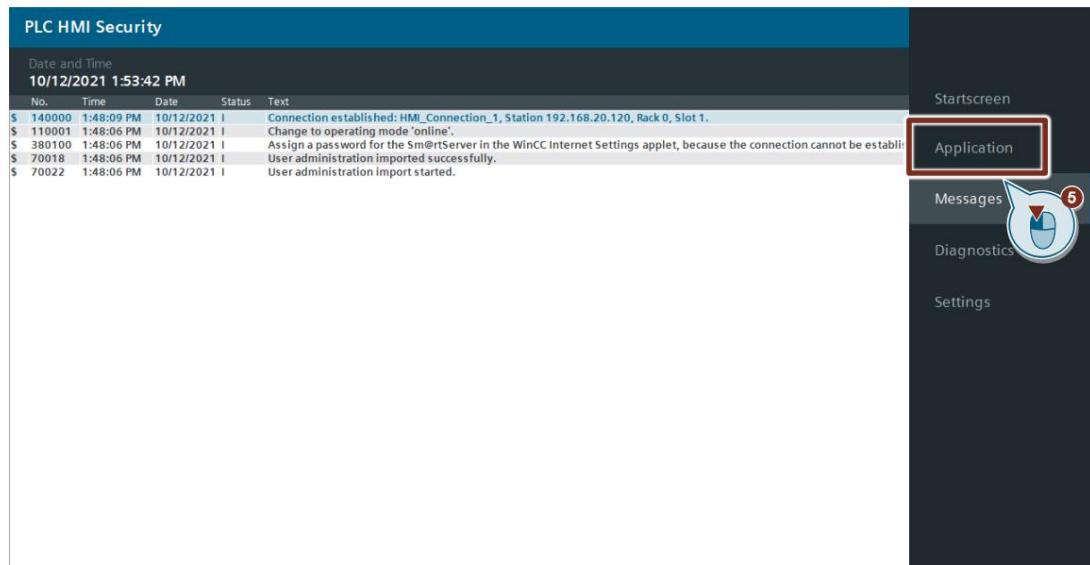
- Haga clic en "Mensajes".



- En la tabla, verá que la conexión entre el PLC y el panel HMI se ha establecido correctamente. Esta conexión está asegurada ya que solo se permitió la comunicación segura PG/P y HMI en la configuración del PLC (consulte el capítulo 3.2).

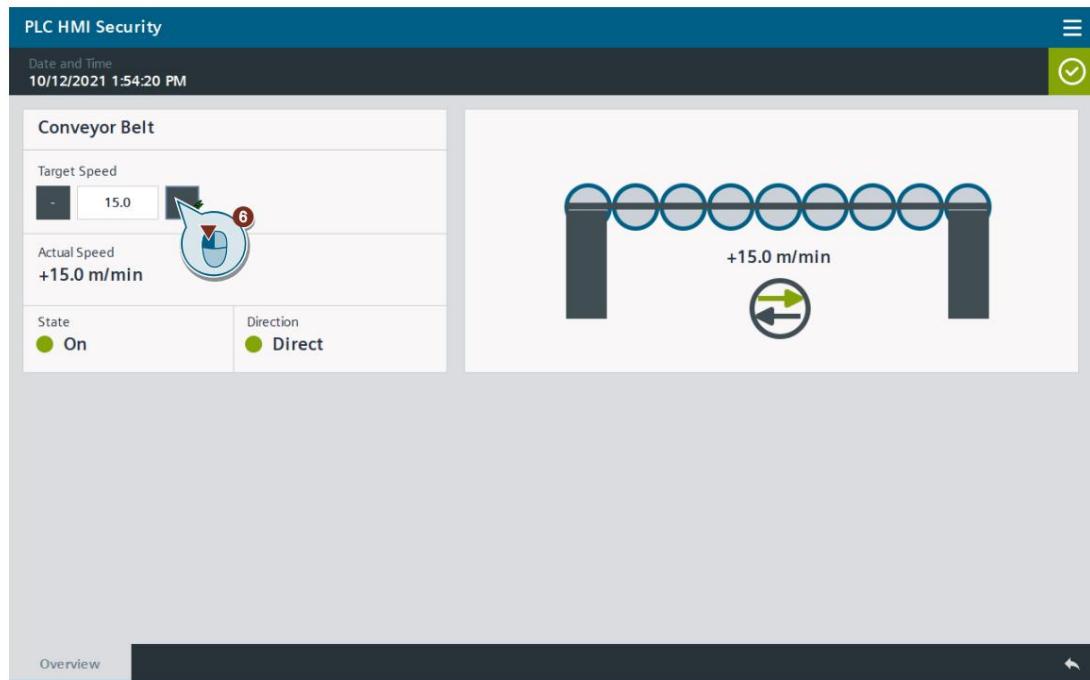
PLC HMI Security				
Date and Time 10/12/2021 1:52:49 PM				
\$ 140000	1:48:09 PM	10/12/2021	I	Connection established: HMI_Connection_1, Station 192.168.20.120, Rack 0, Slot 1.
\$ 110001	1:48:06 PM	10/12/2021	I	Change to operating mode 'online'.
\$ 380100	1:48:06 PM	10/12/2021	I	Assign a password for the Sm@rtServer in the WinCC Internet Settings applet, because the connection cannot be established o... 0
\$ 70018	1:48:06 PM	10/12/2021	I	User administration imported successfully.
\$ 70022	1:48:06 PM	10/12/2021	I	User administration import started.

- Vuelva a hacer clic en el botón de navegación y seleccione "Aplicación".



4 Instalación y puesta en marcha

6. En esta página, la cinta transportadora se puede controlar aumentando su velocidad o disminuyéndola. La "Velocidad real" cambiará para coincidir con la "Velocidad objetivo". También se muestra el estado actual de la cinta transportadora y su dirección.



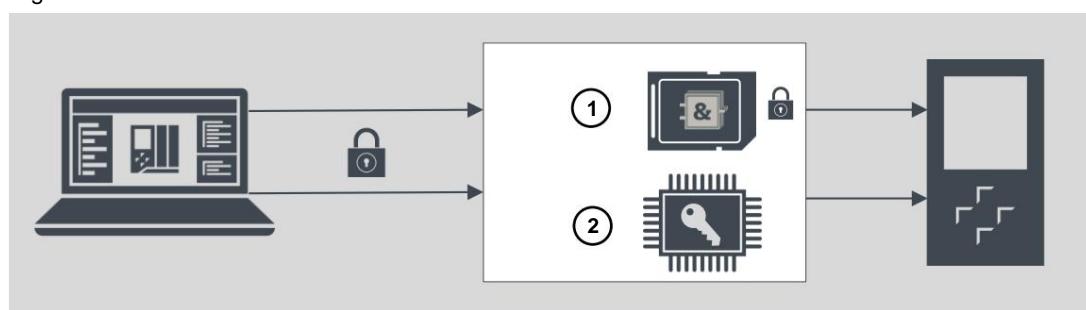
5**Escenarios de intercambio de dispositivos**

Como se describe en el capítulo [2.3](#), el proyecto TIA Portal y la clave generada a partir de la contraseña de datos de configuración confidencial del PLC están relacionados entre sí como dos piezas de un rompecabezas. El proyecto está vinculado a la información clave cargada. La información de la clave cargada está vinculada a la contraseña que se asignó durante la configuración. La información clave y del proyecto debe coincidir; de lo contrario, el PLC no se iniciará.

El proyecto y la información clave se colocan en diferentes áreas de memoria cuando se cargan por primera vez. El proyecto en la memoria de carga (SIMATIC Memory Card), la información clave en un área de memoria en el PLC. Esta clave se utiliza para leer los datos de configuración confidenciales en el SIMATIC

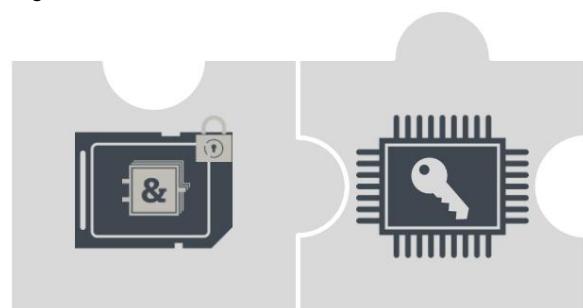
Tarjeta de memoria.

Figura 5-1



1. Proyecto con datos de configuración confidenciales protegidos por contraseña (aquí: en la memoria de carga = SIMATIC Memory Card).
2. Información clave (generada a partir de la contraseña) para utilizar los datos de configuración confidenciales protegidos (aquí: en el área de memoria del PLC).

Figura 5-2



Por lo tanto, la asignación de contraseña para proteger los datos de configuración confidenciales del PLC tiene un impacto en el escenario de las piezas de repuesto.

NOTA Si no ha asignado una contraseña al PLC en su proyecto para proteger la información confidencial del PLC datos de configuración, puede insertar la tarjeta de memoria SIMATIC del PLC que se va a reemplazar en un nuevo PLC sin necesidad de realizar ninguna otra acción.

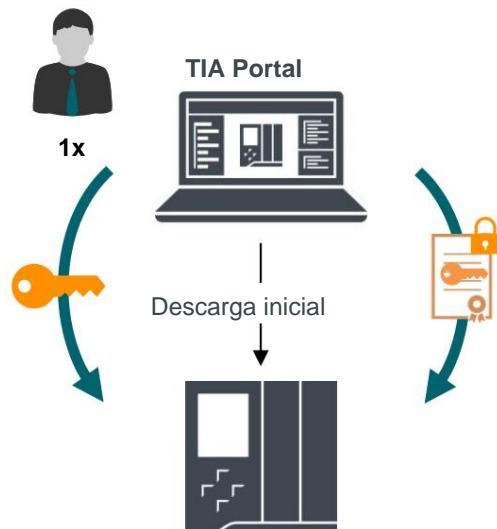
Si ha asignado una contraseña para proteger los datos confidenciales de configuración del PLC en su proyecto del TIA Portal, observe las siguientes reglas al reemplazar un PLC.

5 escenarios de intercambio de dispositivos

5.1 El PLC de reemplazo no tiene contraseña para información confidencial. Datos de configuración

Si el PLC de reemplazo no tiene una configuración o una contraseña configurada para proteger los datos confidenciales de configuración del PLC, puede cargar el proyecto en el PLC de reemplazo sin más preparación, independientemente de si se configura una contraseña o no en el proyecto del TIA Portal.

Figura 5-3

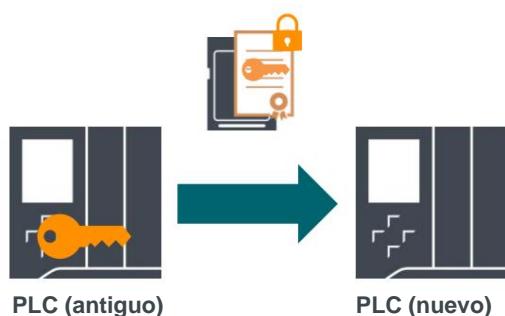


SOCIADAD ANONIMA

5.2 El PLC de reemplazo tiene la misma contraseña para información confidencial. Datos de configuración

Si el PLC de reemplazo tiene la misma contraseña que el PLC a reemplazar, la tarjeta de memoria SIMATIC del PLC a reemplazar se puede insertar directamente en el PLC de reemplazo sin configuración adicional.

Figura 5-4



5 escenarios de intercambio de dispositivos

5.3 El PLC de Reemplazo tiene otra contraseña para uso confidencial. Datos de configuración

Si el PLC de reemplazo ya se configuró con una contraseña diferente, debe restablecer el PLC a la configuración de fábrica con las siguientes opciones configuradas:

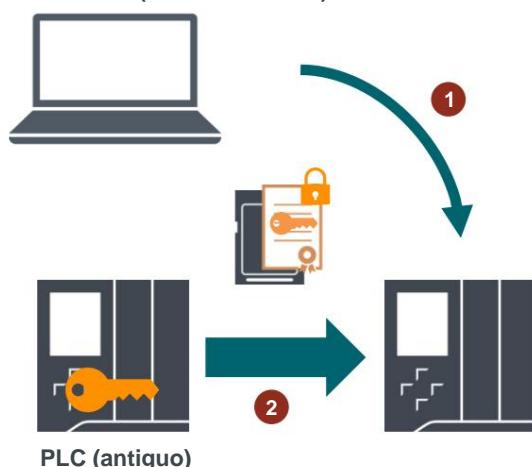
- "Eliminar contraseña para la protección de datos confidenciales de configuración del PLC".
- "Formatear tarjeta de memoria"

Luego se debe configurar la contraseña correcta en el PLC de reemplazo. Esto se puede lograr usando uno de los siguientes métodos.

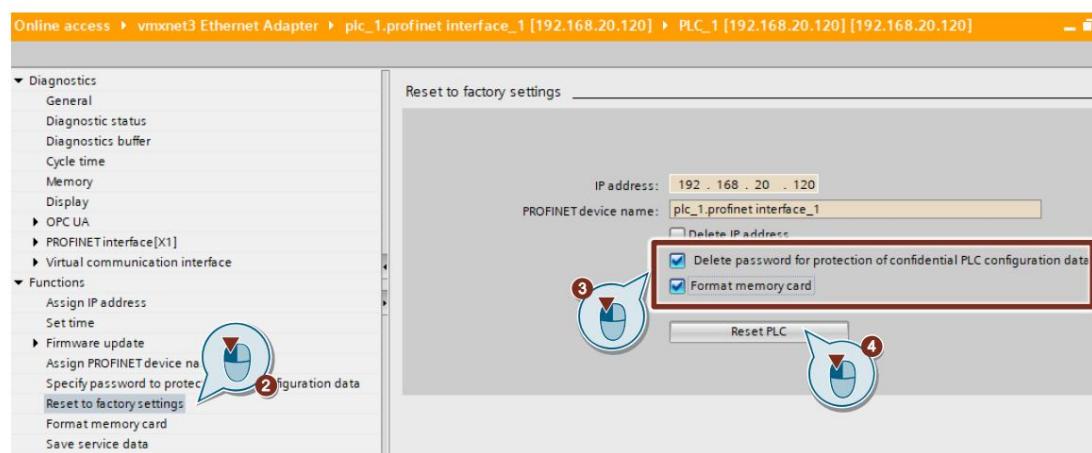
5.3.1 Configuración de la contraseña en el TIA Portal

Figura 5-5

Portal TIA (Acceso en línea)

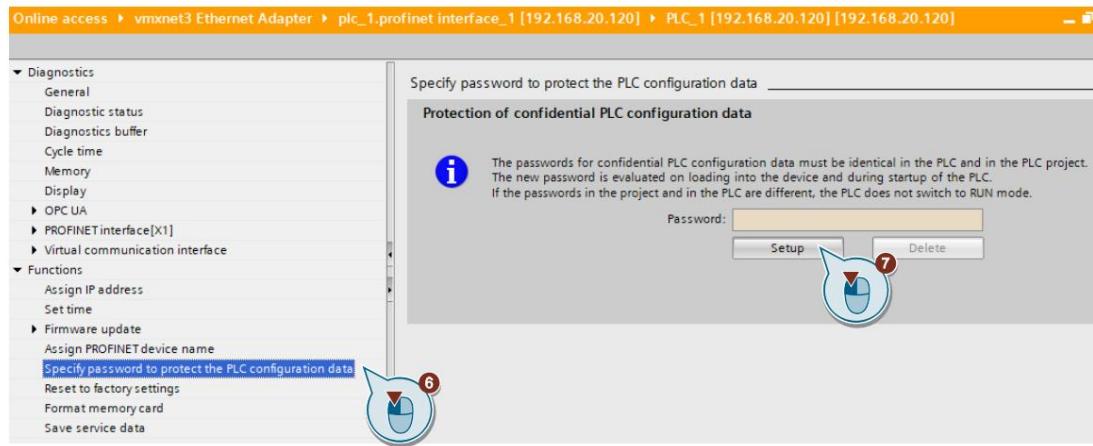


1. En TIA Portal, conéctese en línea en el PLC de reemplazo.
2. En la ventana en línea, vaya a "Funciones > Restablecer configuración de fábrica".
3. Active las siguientes funciones:
 - "Eliminar contraseña para la protección de datos de configuración confidenciales"
 - "Formatear tarjeta de memoria".
4. Haga clic en el botón "Reiniciar PLC".



5 escenarios de intercambio de dispositivos

5. Despues de que finalice el proceso de reinicio, vuelva a conectarse en linea al reemplazo.
6. Navegue hasta "Funciones > Especificar contraseña para proteger los datos de configuración del PLC".
7. Haga clic en el botón "Configuración".



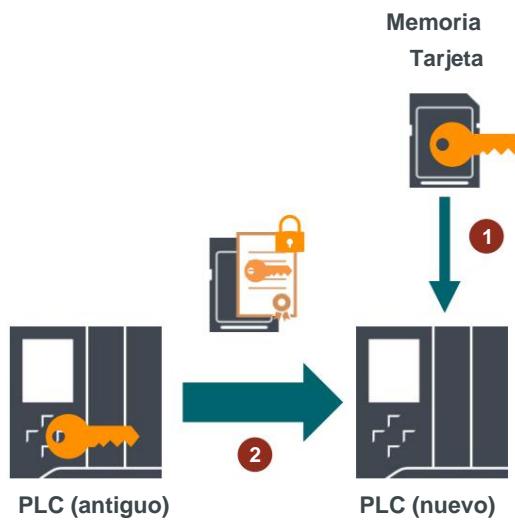
8. Configure la misma contraseña que en el PLC a reemplazar.
9. Haga clic en el botón "Aceptar".



10. Inserte la SIMATIC Memory Card del autómata a sustituir en el autómata de sustitución.

5.3.2 Configuración de la contraseña con una SIMATIC Memory Card adicional

Figura 5-6



Si TIA Portal no está disponible durante el reemplazo del dispositivo, se puede utilizar este método. Requiere una tarjeta de memoria SIMATIC adicional utilizada para configurar la contraseña para datos de configuración de PLC confidenciales en el PLC de reemplazo.

Procedimiento

- Configure una SIMATIC Memory Card con el archivo JOB "SET PASSWORD".

Con esta acción, se crea una estructura de carpetas y archivos siguiendo un patrón especial. Una contraseña para proteger los datos de configuración confidenciales del PLC se escribe como texto sin formato en un archivo especial en la tarjeta de memoria SIMATIC. Para ver la descripción de los pasos necesarios para crear el archivo JOB "FIJAR CONTRASEÑA", consulte estas [instrucciones](#).

- Inserte la SIMATIC Memory Card preparada en el PLC de repuesto y enciéndalo.

El PLC lee la contraseña, la procesa y almacena el resultado en la memoria interna. Se sobrescribe una entrada posiblemente existente.

- Extraiga la SIMATIC Memory Card y reinicie el PLC.

Resultado (autómata S7-1500)

Mientras el PLC lee la SIMATIC Memory Card, el LED muestra el mismo comportamiento que durante una actualización de firmware.

Mientras el PLC establece la contraseña, el LED "RUN/STOP" parpadea.

Una vez que el proceso se ha completado con éxito, el LED "RUN/STOP" es amarillo y el LED "MAINT" parpadea en amarillo.

El resultado de la operación se muestra en el búfer de diagnóstico como un mensaje de éxito o error.

Si no se pudo establecer la contraseña, el LED de error parpadea junto con los otros LED.

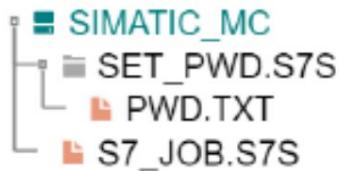
5 escenarios de intercambio de dispositivos

Creación de una SIMATIC Memory Card con el archivo JOB "SET PASSWORD"

1. Cree una carpeta en el directorio raíz y asignele el nombre "SET_PWD.S7S".
 2. Cree un archivo de texto con el nombre "PWD.TXT" con la contraseña como texto sin formato en la carpeta que acaba de crear en la SIMATIC Memory Card.
 3. Cree un archivo de texto con el nombre "S7_JOB.S7S" con el contenido "**SET_PWD**" en el directorio raíz de la SIMATIC Memory Card.
- Este archivo es el "archivo TRABAJO". Se utiliza para asignar una contraseña al PLC para proteger los datos de configuración confidenciales.

La figura siguiente muestra la estructura de archivos en la SIMATIC Memory Card.

Figura 5-7



PRECAUCIÓN

Almacenamiento seguro de la SIMATIC Memory Card

Guarde la SIMATIC Memory Card en un lugar seguro al que solo puedan acceder las personas autorizadas.

Reglas y Recomendaciones

- La contraseña debe establecerse en un entorno seguro.
- El contenido del archivo de texto "PWD.TXT" define la contraseña para proteger los datos de configuración confidenciales del PLC. Debe corresponder a la contraseña que también ha establecido en el PLC configuración.
- Para restablecer una contraseña existente de un PLC, el archivo de texto "PWD.TXT" debe estar vacío. Eso significa que el tamaño del archivo debe ser de 0 bytes.
- Use cualquier editor de texto para crear el archivo de texto. El formato de texto recomendado es "UTF-8".
- Los nombres de carpetas y archivos no distinguen entre mayúsculas y minúsculas. Sin embargo, la contraseña distingue entre mayúsculas y minúsculas.
- No agregue el carácter "CR" o "LF" al final de los archivos de texto ("PWD.TXT" o "S7_JOB.S7S").

6 Actualización de firmware y copia de seguridad del dispositivo

6.1 Actualización de firmware del PLC S7-1500

Al actualizar el firmware del PLC, actualice siempre a la última versión disponible para el número de artículo respectivo.

Aquí encontrará un resumen de los números de artículo y las versiones de firmware de los PLC S7-1500 incluidos, las pantallas y los PLC ET 200: [\9\](#).

La última versión respectiva de un firmware es válida para todas las versiones de ese número de artículo.

Al actualizar el firmware del PLC, no es obligatorio actualizar la pantalla, pero se recomienda.

Puede encontrar una descripción general de cómo actualizar el PLC aquí: [\10\](#).

Los PLC ya configurados que se han actualizado a la última versión de firmware en TIA Portal V17 no tendrán las capacidades de seguridad más recientes de forma predeterminada. El usuario debe configurar explícitamente el PLC para tener las nuevas funciones de seguridad. El PLC recién actualizado funcionará en el llamado "Modo heredado" de acuerdo con los datos de configuración en el PLC.

El "Modo mixto" permite que el PLC se comunique de forma segura con otros dispositivos, por ejemplo, PG o panel HMI que están configurados con TIA portal V17 y tienen las funciones de seguridad más recientes ("Modo seguro"). Además de eso, el PLC también puede comunicarse con dispositivos que han sido configurados con versiones anteriores de TIA Portal y no tienen las últimas funciones de seguridad de forma no segura ("Legacy Mode"). Puede encontrar más información sobre la compatibilidad de comunicación en el capítulo [2.5](#).

NOTA Los PLC en TIA Portal V17 pueden funcionar en dos modos:

- Modo seguro

En el modo seguro, solo se permite la comunicación segura basada en TLS entre el PLC y el panel PG o HMI.
- Modo mixto

En el modo Mixto, el PLC puede comunicarse de forma segura mediante TLS con el panel PG o HMI que utiliza TIA Portal V17, así como con el panel PG o HMI que utiliza una versión anterior de TIA Portal.

Proyectos creados con TIA Portal < V17

Si ha creado un proyecto con TIA Portal versión V16 para un S7-1500 PLC (p. ej., versión V2.8), la configuración correspondiente con TIA Portal V17 también se puede cargar en un S7-1500 PLC V2.9. El comportamiento del S7-1500 PLC V2.9 será el mismo que el de la V2.8, es decir, el PLC no es compatible con las nuevas funciones de seguridad de TIA Portal versión 17.

Esto también se aplica a los proyectos creados con TIA Portal < V17 y transferidos a una SIMATIC Memory Card. Funcionan sin problemas en un S7-1500 PLC V2.9.

Sin embargo, el concepto de proteger los datos de configuración confidenciales del PLC se aplica tan pronto como abre el proyecto con TIA Portal > V17, actualiza la versión de firmware del PLC mediante un cambio de dispositivo y lo guarda como un PLC con una versión de firmware > V2.9. El proyecto ya no se puede editar con versiones anteriores de TIA Portal V17.

6.2 Copia de seguridad y restauración de un PLC (PLC S7-1200, PLC S7-1500)

Puede hacer una copia de seguridad de una configuración funcional de un PLC en el TIA Portal y acceder a ella más tarde. Esto hace posible restaurar la configuración original respaldada. De esta manera puede cargar una configuración modificada para realizar las siguientes acciones, por ejemplo:

- probar las mejoras del producto
- cambiar los programas para solucionar problemas en el sistema
- reemplazar componentes en base a pruebas

A continuación, puede restaurar la copia de seguridad original de la configuración del PLC.

Copia de seguridad de la configuración

Si se realiza una copia de seguridad de una CPU en el TIA Portal mediante el menú "Online> Backup from online device", también se guarda la contraseña para proteger los datos confidenciales de configuración del PLC.

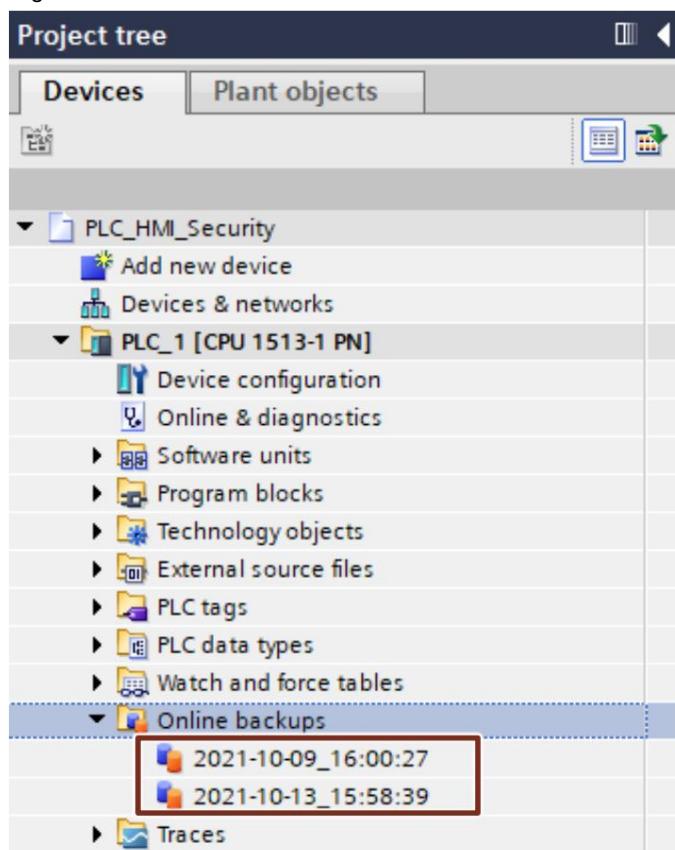
Restaurar la copia de seguridad

Al restaurar la copia de seguridad de un PLC utilizando el menú "Online > Descargar en dispositivo" con la copia de seguridad marcada en el TIA Portal, el PLC solo puede comunicarse con una PG/PC o un panel HMI si se cumple la siguiente condición:

- Despues de la restauración de una configuración protegida con una contraseña para proteger PLC confidencial datos de configuración, exactamente esta contraseña debe estar presente en el PLC.

De lo contrario, el PLC no puede acceder a los datos de configuración y no se inicia.

Figura 6-1



Recurso

Si ocurre el error anterior, es decir, la contraseña para proteger los datos confidenciales de configuración del PLC no coincide con la copia de seguridad, debe eliminar la contraseña y luego establecer la contraseña correcta. Consulte el capítulo [7.2](#). Después de reiniciar el PLC, la copia de seguridad es funcional.

6.3 Actualización de firmware y copia de seguridad del dispositivo del panel HMI

Puede encontrar una descripción general de los pasos necesarios para realizar las siguientes acciones en los paneles del operador aquí: [\11](#) y [\12](#).

- Actualizar
- Respaldo
- Restaurar

NOTA Al realizar una copia de seguridad del sistema en el panel HMI, los certificados se copian automáticamente también. Esto significa que, si hay una conexión segura en funcionamiento con el PLC antes de la copia de seguridad, la conexión con ese PLC se establecerá correctamente después de restaurar la copia de seguridad.

7 Información útil

7.1 Lista de componentes compatibles con la comunicación segura PG/PC y HMI

Servidores

- S7-1500 PLC V2.9
- S7-1200 PLC V4.5
- S7-PLCSIM Avanzado
- Controlador de accionamiento V2.9

Clientela

- STEP 7 V17 (TIA Portal V17) • Paneles básicos HMI de 2.^a generación, V17
- Paneles Móviles HMI 2da Generación, V17
- Paneles HMI Comfort, V17
- WinCC Runtime Avanzado V17
- WinCC Runtime Professional V17
- PC unificado WinCC V17
- Paneles de confort unificados HMI V17
- SIMATIC NET V17 (servidor OPC UA) • WinCC V7 a partir de V7.5 SP2 Update 4
- WinCC OA desde 3.18-P003

7.2 Cambiar la contraseña para proteger el PLC confidencial Datos de configuración (PLC S7-1200, PLC S7-1500)

Debe distinguirse entre los siguientes estados:

- El autómata está cargado con una configuración.
- El PLC se encuentra en el estado de entrega (ajuste de fábrica), es decir, el PLC aún no está cargado con una configuración.

Si el PLC está cargado con una configuración, tiene la información clave con la que se pueden utilizar los datos de configuración del PLC protegidos por contraseña.

7.2.1 Cambiar contraseña: la configuración aún no está cargada

Si la CPU aún no se ha cargado con una configuración, es posible cambiar una contraseña ingresada o revocar la activación de la protección por contraseña.

Condición previa

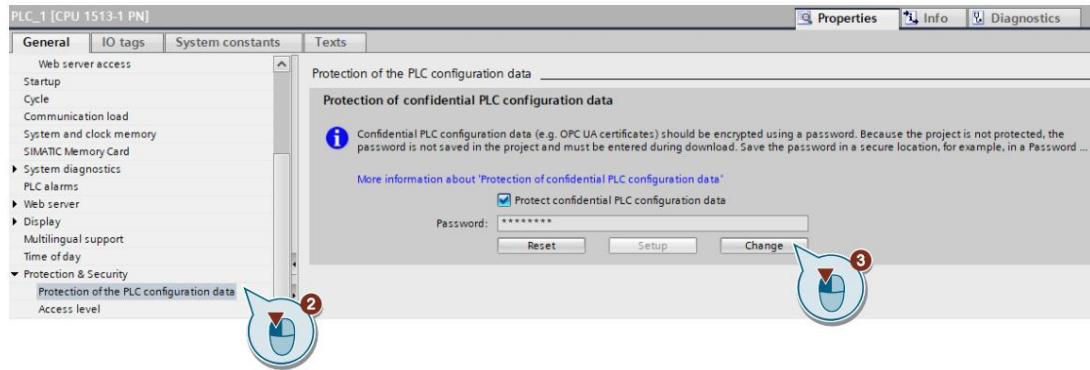
- El PLC aún no está cargado con una configuración.

7 Información útil

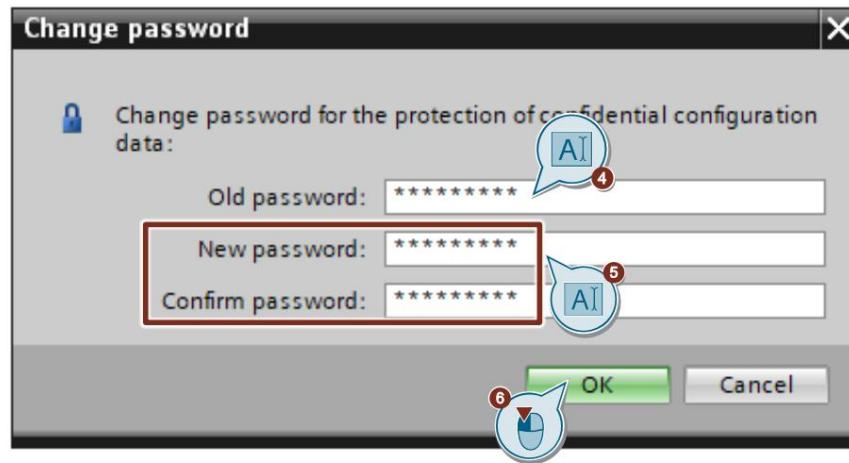
cambiar la contraseña

1. En el proyecto TIA Portal, abra el menú de propiedades del PLC.
2. Vaya a "Protección y seguridad > Protección de datos de configuración de PLC".
3. Haga clic en el botón "Cambiar".

Se abre el cuadro de diálogo "Cambiar contraseña".



4. Introduzca la contraseña válida anteriormente.
5. Introduzca la nueva contraseña y confirme la nueva contraseña.
6. Haga clic en el botón "Aceptar" para aplicar los cambios.

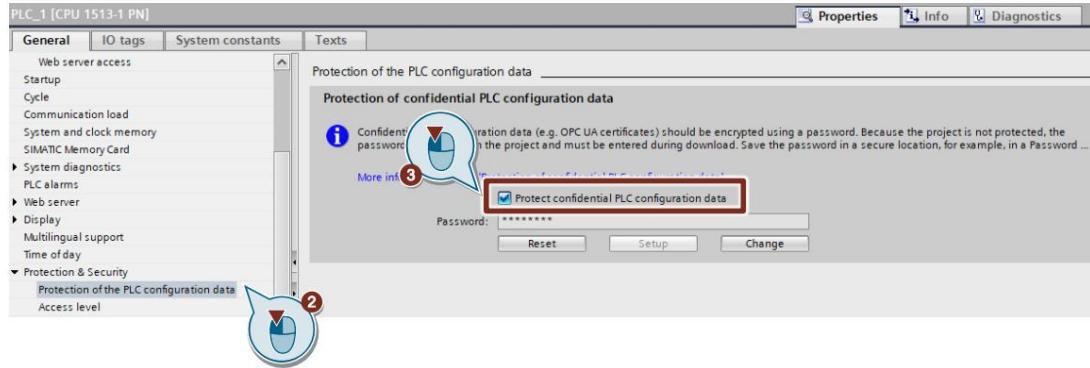


7 Información útil

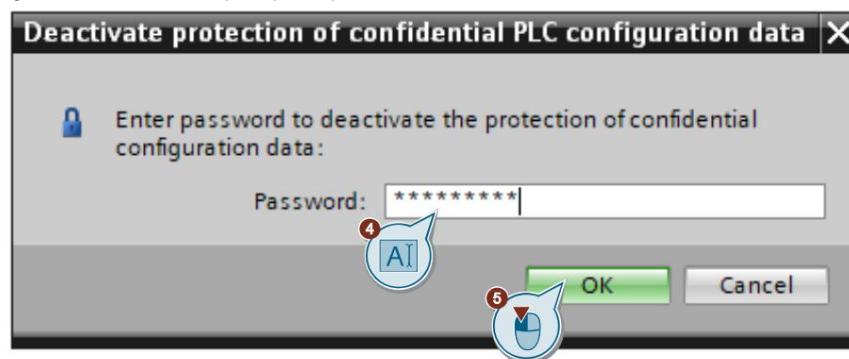
Desactivar la función "Proteger datos confidenciales de configuración del PLC"

1. En el proyecto TIA Portal, abra el menú de propiedades del PLC.
2. Vaya a "Protección y seguridad > Protección de datos de configuración de PLC".
3. Desactive la casilla de verificación "Proteger datos confidenciales de configuración del PLC".

Se abre el cuadro de diálogo "Desactivar protección de datos confidenciales de configuración del PLC".



4. Introduzca la contraseña válida anteriormente.
5. Haga clic en el botón "Aceptar" para aplicar los cambios.



Si aún no ha cargado ninguna configuración en el PLC, el PLC se encuentra en la fase de aprovisionamiento y puede cargar cualquier configuración válida con su contraseña configurada. Puede encontrar más información sobre la fase de aprovisionamiento y su significado en el capítulo [2.2.2](#).

7.2.2 Cambiar contraseña: la configuración ya está cargada

Si el PLC ya se ha cargado con una configuración y la configuración está protegida con una contraseña para datos confidenciales de configuración del PLC, esta contraseña debe eliminarse. Existen los siguientes métodos para eliminar la contraseña.

- Restablecer el PLC a la configuración de fábrica
- Vaya en línea al PLC para eliminar la contraseña para proteger la configuración confidencial del PLC datos directamente y volver a definirlos.

Condición previa

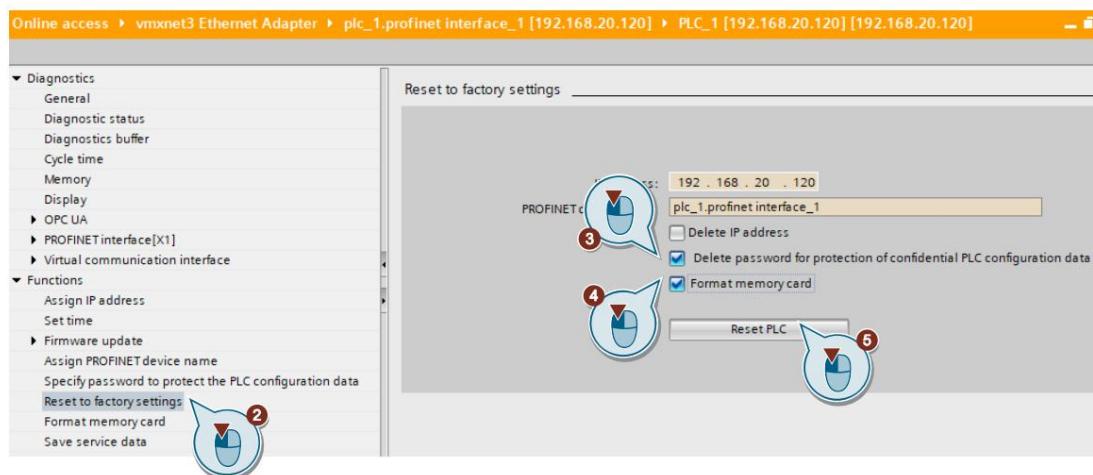
- Tiene acceso de escritura al PLC.
- El PLC está en modo "STOP".

Procedimiento

Dependiendo de la tarea a realizar, se debe realizar cualquiera de los siguientes pasos:

Si también desea cambiar el proyecto en la SIMATIC Memory Card, es decir, desea volver a cargar la configuración, debe realizar las siguientes acciones:

1. En el proyecto TIA Portal, vaya online al PLC.
2. En la ventana en línea, vaya a "Funciones > Restablecer configuración de fábrica".
3. Active la casilla de verificación "Eliminar contraseña para proteger datos confidenciales de configuración del PLC".
4. Seleccione la casilla de verificación "Formatear tarjeta de memoria" para evitar una puesta en marcha repetida del PLC.
5. Haga clic en el botón "Reiniciar PLC".

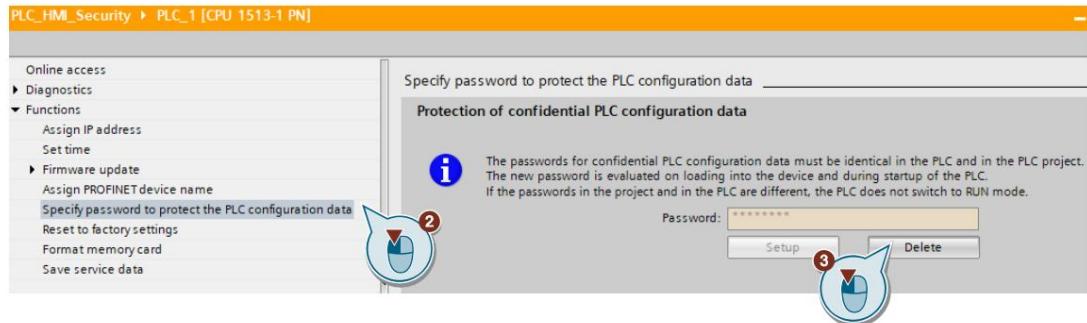


6. Cargue el proyecto con la configuración modificada y la contraseña deseada.

7 Información útil

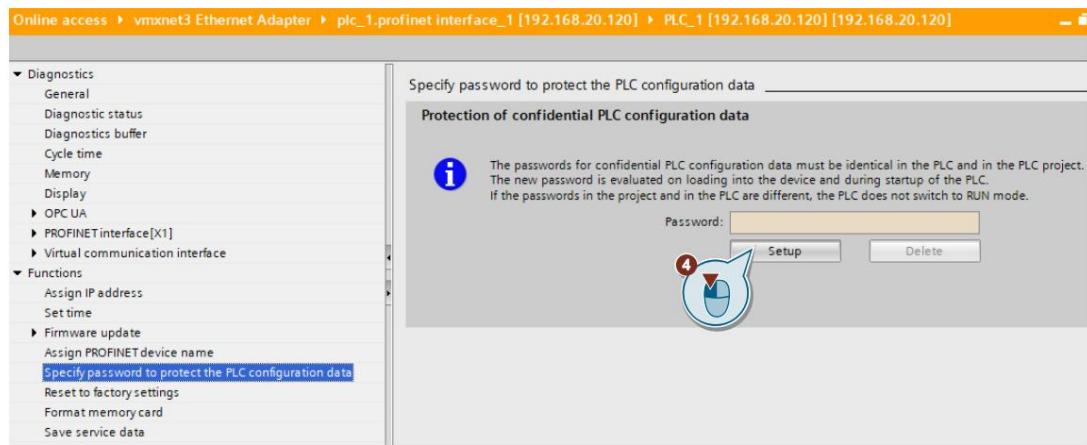
Si no tiene que cambiar el proyecto en la SIMATIC Memory Card, es decir, solo se ha configurado una contraseña incorrecta:

1. En el proyecto TIA Portal, vaya online al PLC.
2. En la ventana en línea, navegue hasta "Especificar contraseña para proteger los datos de configuración del PLC".
3. Haga clic en el botón "Eliminar". Si el botón "Eliminar" no está disponible, no se ha establecido ninguna contraseña en el PLC todavía.



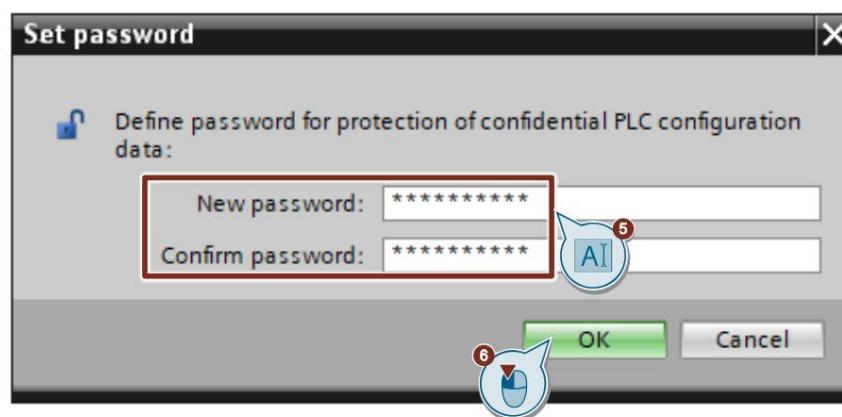
4. Haga clic en el botón "Configuración".

Se abre el cuadro de diálogo "Establecer contraseña".



5. Ingrese la contraseña requerida y confírmela.

6. Haga clic en el botón "Aceptar".



Si se ha introducido la contraseña correcta, el PLC puede utilizar los datos de configuración del PLC protegidos.

7 Información útil

Sin acceso de escritura al PLC

Si no tiene acceso de escritura a la memoria de carga sino solo acceso de lectura, realice una de las siguientes acciones:

- Retire la tarjeta de memoria SIMATIC del PLC antes de restablecer el PLC a la fábrica configuración con la opción "Eliminar contraseña para proteger datos confidenciales de configuración del PLC".
- Elimine la SIMATIC Memory Card externamente, p. ej. en su PC, antes de restablecer la configuración de fábrica del PLC con la opción "Eliminar contraseña para proteger datos de configuración confidenciales del PLC".

NOTA La restauración de la configuración de fábrica del PLC a través del selector de modo también elimina la dirección IP del PLC, pero no la contraseña para proteger los datos confidenciales de configuración del PLC.

7.3 Restablecimiento de la contraseña para proteger el PLC confidencial Datos de configuración (PLC S7-1200, PLC S7-1500)

La contraseña para proteger los datos confidenciales de configuración del PLC se puede restablecer. Esto es necesario, por ejemplo, si se va a cambiar la contraseña, pero ya no se conoce la contraseña actual.

7.3.1 Restablecimiento de la contraseña: la configuración aún no se ha cargado

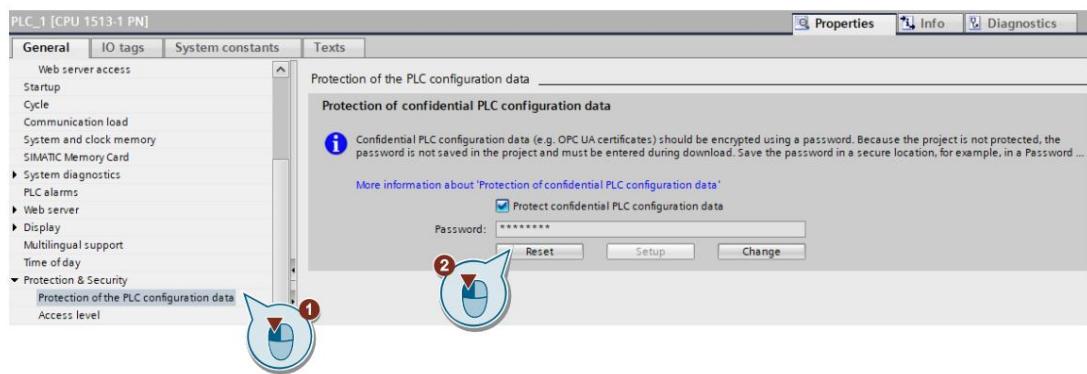
Dado que debe introducir la contraseña al cargar el PLC a través del TIA Portal por primera vez, la configuración del PLC para este PLC ya no se puede utilizar. Para cambiar la contraseña en el PLC properties, también debe ingresar la contraseña previamente válida. Si olvida su contraseña, haga lo siguiente.

Condición previa

- El PLC aún no está cargado.

Procedimiento

1. En el menú de propiedades del PLC en el TIA Portal, vaya a "Protección y seguridad > Protección de los datos de configuración del PLC".
2. Haga clic en el botón "Reiniciar".

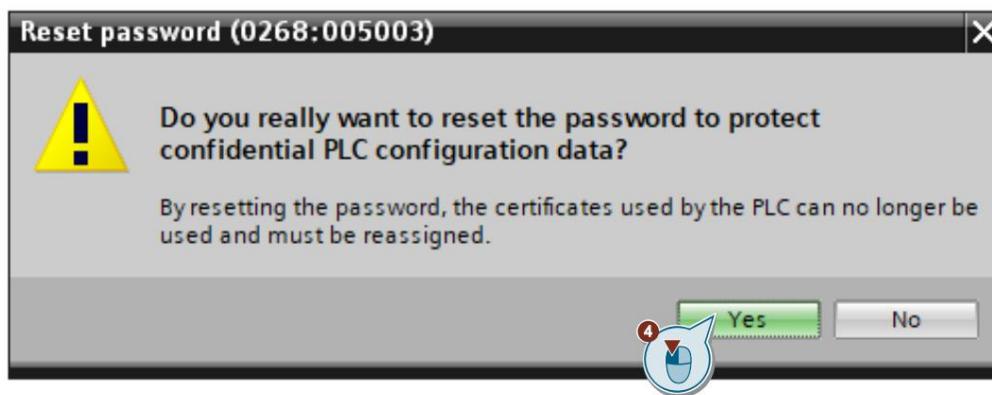


NOTA Los certificados de la CPU (p. ej., certificados para servidor web, para servidor OPC UA, para comunicación PG/PC y HMI) ya no se pueden utilizar después del reinicio. Es necesario recrear y reasignar los certificados de la UCP.

- Si utiliza la configuración de seguridad global para el administrador de certificados, debe reasignar los certificados desde el administrador de certificados.
- Si no utiliza la configuración de seguridad global para el administrador de certificados, debe volver a crear y reasignar los certificados.

7 Información útil

3. Confirme el restablecimiento de la contraseña con "Sí".



La opción para la protección de datos confidenciales de configuración del PLC aún está activada.

7.3.2 Restablecimiento de la contraseña: la configuración ya está cargada

Si el PLC ya se ha cargado con una configuración y la configuración está protegida con una contraseña para datos de configuración de PLC confidenciales, puede, para cargar un nuevo proyecto, borrar la contraseña para datos de configuración de PLC confidenciales en línea y luego especificar una nueva contraseña.

Condición previa

- Tiene acceso de escritura al PLC.
- El PLC debe estar en modo STOP.

Procedimiento

1. En TIA Portal, vaya online al PLC.
2. En la ventana en línea, vaya a "Funciones > Especificar contraseña para proteger el PLC datos de configuración".
3. Haga clic en el botón "Eliminar".

Si el botón "Eliminar" no está disponible, todavía no se ha establecido una contraseña en el PLC.

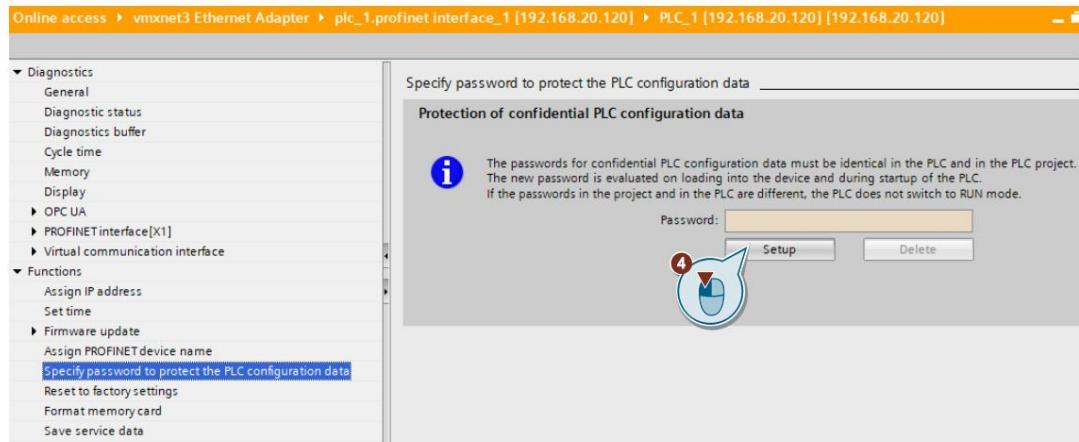


NOTA Si se elimina la contraseña y un proyecto cargado requiere una contraseña correspondiente, es posible que este proyecto ya no funcione sin ingresar la contraseña.

7 Información útil

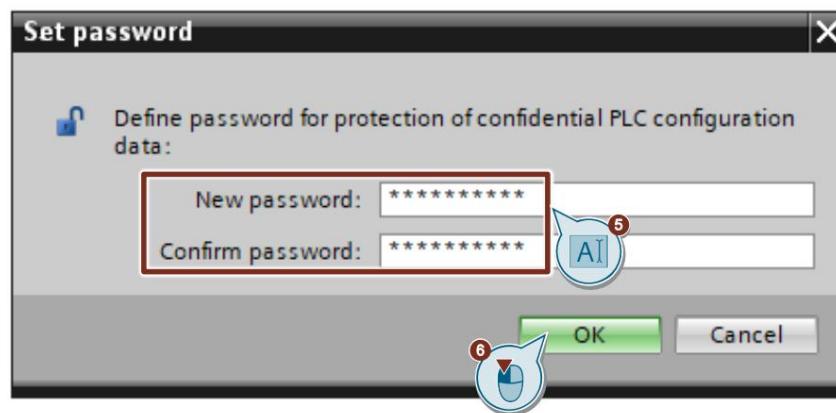
4. Si es necesario, haga clic en el botón "Configurar" para establecer una nueva contraseña.

Se abre el cuadro de diálogo "Establecer contraseña".



5. Introduzca la nueva contraseña.

6. Haga clic en el botón "Aceptar".



7.3.3 Restablecimiento de la contraseña con SIMATIC Memory Card

También es posible restablecer la contraseña utilizando una SIMATIC Memory Card adicional. Este método se puede utilizar para escenarios en los que TIA Portal no está disponible. Para obtener más información sobre cómo realizar este procedimiento, consulte el capítulo [5.1](#).

NOTA Para restablecer la contraseña, el archivo "PWD.TXT" debe estar vacío. Eso significa que el tamaño del archivo debe ser 0 bytes

7.4 Sugerencias para evitar y manejar errores

La siguiente descripción enumera algunos casos de uso que pueden generar mensajes de error del PLC.

El búfer de diagnóstico proporciona información

El PLC detecta cuando la contraseña para proteger los datos confidenciales de configuración del PLC y la configuración cargada no coinciden. Un mensaje en el búfer de diagnóstico indica posibles causas y remedios y, por lo general, lleva a la solución del problema.

"Trampas" típicas

Debe prestar atención a las siguientes circunstancias para evitar o corregir errores: ¿Configuración cargada?

Independientemente de si protege sus datos confidenciales de configuración de PLC con una contraseña o no, se debe observar la siguiente circunstancia:

Sin una configuración cargada, el PLC no sale de la fase de provisión (ver capítulo [2.2.2](#)).

-
- Está intentando cargar una contraseña configurada en una CPU que ya ha recibido otra contraseña, por ejemplo:

Se cambia PLC por otro PLC del stock. El PLC de reemplazo no se restableció por completo (restablecimiento a la configuración de fábrica con la opción "Eliminar contraseña para la protección de datos de configuración confidenciales del PLC").

Recurso:

- Para que se cargue la configuración, use la misma contraseña que ya usó para la configuración ya está cargada.
- También es posible que se haya cargado un proyecto o una configuración de PLC incorrectos. Compruebe si está disponible la configuración de PLC correcta.
- Utilice la función en línea "Especificar contraseña para proteger la configuración confidencial del PLC data" para borrar la contraseña o establecer la misma contraseña que en la configuración del PLC.

- El mismo error ocurre si la configuración de su PLC no usa una contraseña y la ya la configuración cargada requiere una contraseña definida por el usuario.

Recurso:

- Utilice la función en línea "Establecer contraseña para proteger datos confidenciales de configuración del PLC" para borrar la contraseña o establecer la misma contraseña que en la configuración del PLC.

7.5 Uso de la comunicación PG/PC heredada en el TIA Portal

A partir de la versión V17 del TIA Portal, el TIA Portal y los autómatas S7-1200 a partir del firmware V4.5, así como los autómatas S7-1500 a partir del firmware V2.9 se comunican automáticamente de forma "segura", es decir, los socios de conexión ajustan automáticamente sus mecanismos de conexión al máximo posible método de seguridad.

Solo circunstancias especiales provocan un retorno a la comunicación PG/PC heredada. Consulte la [Sección 2.5](#).

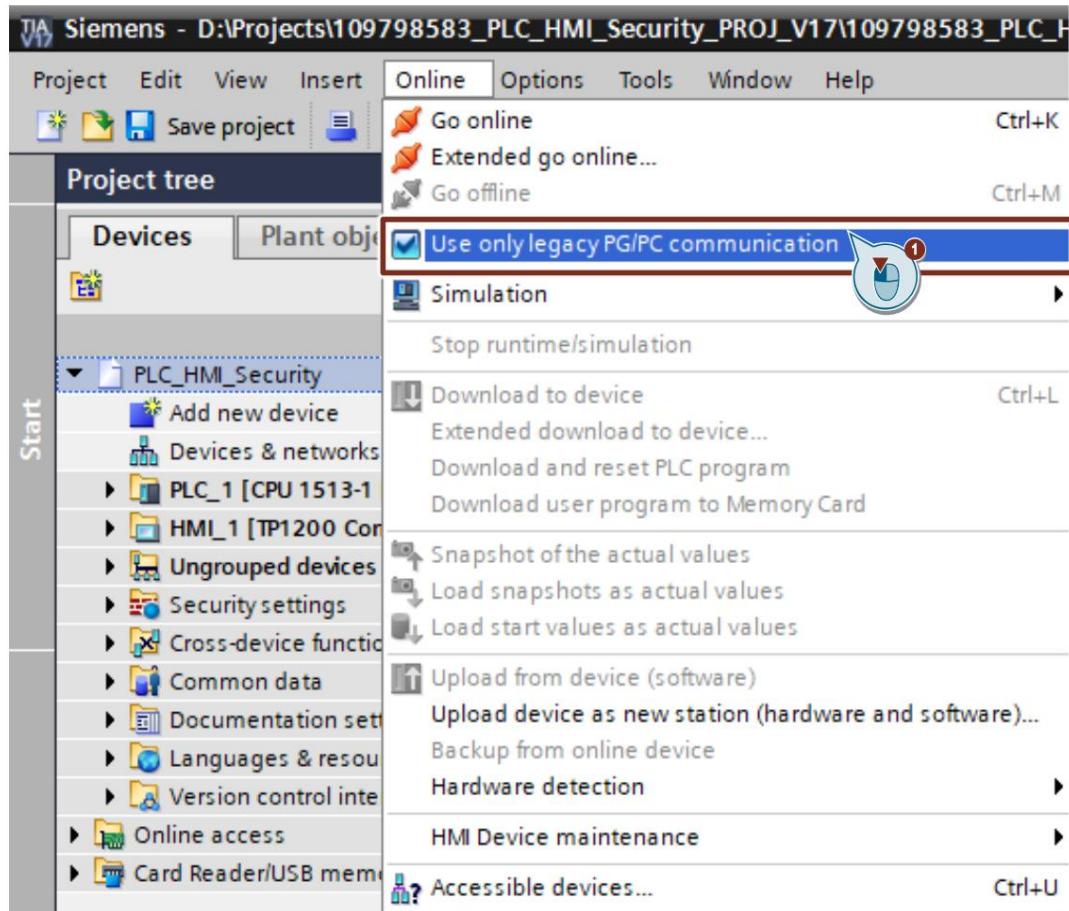
Puede haber algunos casos en los que la mayor seguridad no sea deseable porque puede afectar la velocidad de transmisión de los PLC con un rendimiento de comunicación débil. En los casos en que esto sea cierto, se puede activar la comunicación PG/PC heredada.

Requisito

- No se deben establecer conexiones online con las CPU.
- Para autómatas a los que se debe acceder online, la opción "Permitir solo PG/PC seguro y HMI comunicación" debe estar deshabilitado.
- Los interlocutores de la comunicación se encuentran en un entorno protegido, por ejemplo, durante la fase de puesta en marcha.

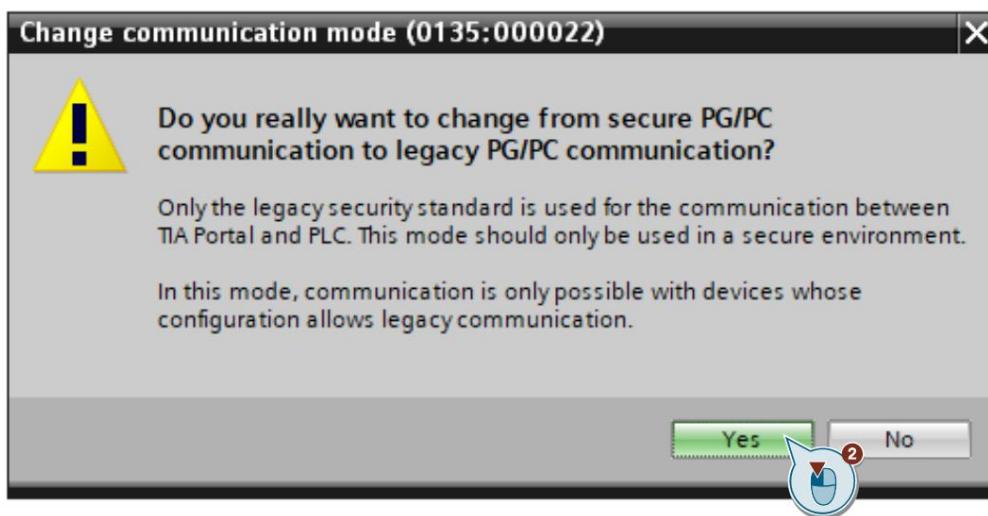
Configurar la comunicación Legacy PG/PC

1. En el menú "Online", active la casilla de verificación "Utilizar solo comunicación PG/PC heredada".



7 Información útil

2. Haga clic en el botón "Sí" cuando aparezca el mensaje de advertencia.



Todas las conexiones en línea están configuradas como para las versiones de TIA Portal < V17.

La configuración permanece activa durante la duración de la sesión. Al abrir un proyecto, la opción "Usar solo comunicación PG/PC heredada" no está activada.

Comportamiento con la opción habilitada "Utilizar solo comunicación PG/PC heredada"

- En el TIA Portal, no se puede especificar, modificar o eliminar online una contraseña para proteger los datos confidenciales de configuración del PLC para los PLC. Estas funciones requieren la desactivación de la función "Usar solo comunicación PG/PC heredada".
- Un PLC que está configurado para permitir solo la comunicación segura PG/PC y HMI ya no puede ser alcanzado en línea.

7 Información útil

7.6 Descripción del proyecto TIA Portal V17

7.6.1 Visión de conjunto

Introducción

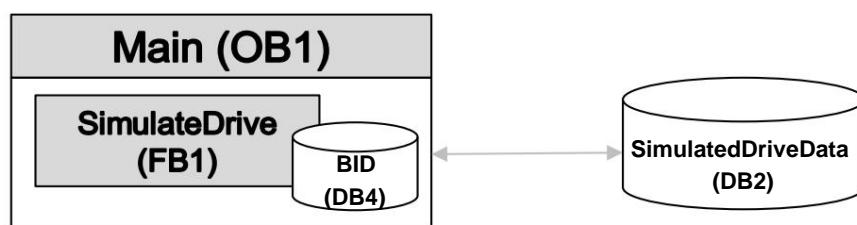
El proyecto TIA Portal V17 contiene:

- El programa de usuario para el PLC S7 con el bloque de función "SimulatedDrive". •
- La configuración de las nuevas funciones de seguridad del PLC S7-1500.
- La configuración del SIMATIC TP1200 Comfort Panel.

Diagrama

El siguiente gráfico muestra la estructura del programa de todo el proyecto TIA Portal V17.

Figura 7-1



Bloques de programa

El programa de usuario para el S7-1500 PLC consta de los siguientes elementos:

Tabla 7-1

Elemento	Nombre simbólico	Descripción
OB1	Principal	En el OB1 se llama cíclicamente al bloque de función "SimulatedDrive", incluido el correspondiente bloque de datos de instancia.
FB1	Unidad simulada	El bloque de funciones "SimulatedDrive" contiene las funciones implementadas en este ejemplo.
DB2	SimulatedDriveData	Bloque de datos global que almacena los datos.
DB4	InstSimulatedDrive	Bloque de datos de instancia del bloque de función "SimulatedDrive".

7 Información útil

7.6.2 El bloque de función "SimulatedDrive"

Función

El bloque de función "SimulatedDrive" comprueba la velocidad actual de la cinta transportadora "actualSpeed" a intervalos regulares y la compara con un valor predefinido "setpointSpeed". • Si la velocidad real es mayor que el valor predefinido, la velocidad "actualSpeed" se reduce al valor "setpointSpeed".

- Si la velocidad real es menor que el valor predefinido, la velocidad "actualSpeed" aumenta al valor "setpointSpeed".

Parámetro

La figura y la tabla siguientes muestran la interfaz de llamada del bloque de función "SimulatedDrive".

Figura 7-2

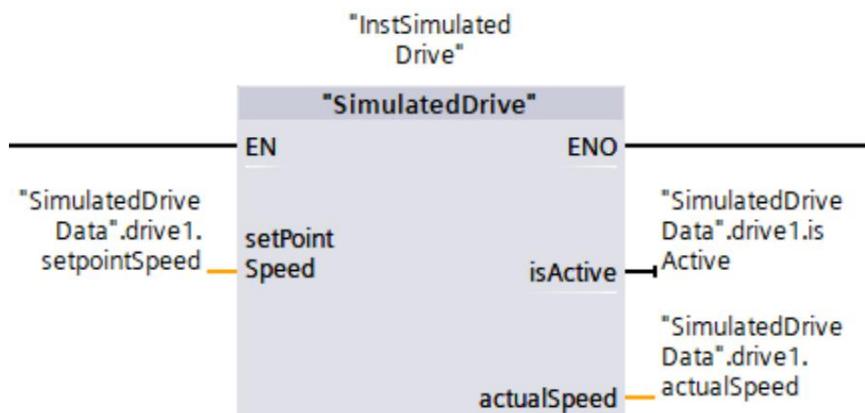


Tabla 7-2

Parámetro		Tipo de datos	Descripción
APORTE	EN	BOOL	Habilitar entrada. Sólo en FDP y LAD.
	consignaVelocidad	LREAL	Valor predefinido con el que se compara la velocidad de la cinta transportadora a intervalos regulares.
PRODUCCIÓN	ENO	BOOL	Habilitar salida. Sólo en FDP y LAD.
	está activo	BOOL	Estado de la cinta transportadora.
	velocidadreal	LREAL	Indica la velocidad actual de la cinta transportadora: <ul style="list-style-type: none"> Si la velocidad real es mayor que el valor predefinido, la velocidad "actualSpeed" se reduce al valor "setpointSpeed". Si la velocidad real es menor que el valor predefinido, la velocidad "actualSpeed" aumenta al valor "setpointSpeed".

7 Información útil

7.6.3 El bloque de datos global "SimulatedDriveData"

El bloque de datos "SimulatedDriveData" contiene los datos para la comunicación entre el S7-1500 PLC y el panel HMI:

- está activo.
- velocidadreal
- velocidad de consigna

Figura 7-3

SimulatedDriveData										
	Name	Data type	Start value	Retain	Accessible f...	Writa...	Visible in ...	Setpoint	Supervision	Comment
└ ▼ Static										
└ □ drive1	"typeDriveInterface"				<input checked="" type="checkbox"/>					
└ □ isActive	Bool	false			<input checked="" type="checkbox"/>	Drive state				
└ □ actualSpeed	LReal	0.0			<input checked="" type="checkbox"/>	Drive actual speed				
└ □ setpointSpeed	LReal	0.0			<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>		Drive target speed

NOTA Las variables de PLC utilizadas para la comunicación entre el PLC S7-1500 y el panel HMI deben declararse como accesibles para HMI ("Accesible desde HMI/OPC UA/Web API").

8 Apéndice

8.1 Servicio y soporte

Soporte en línea de la industria

¿Tiene alguna pregunta o necesita ayuda?

Siemens Industry Online Support ofrece acceso las 24 horas a todo nuestro servicio, soporte y conocimientos técnicos y cartera.

Industry Online Support es la dirección central para obtener información sobre nuestros productos, soluciones y servicios.

Información de productos, manuales, descargas, preguntas frecuentes, ejemplos de aplicación y videos: toda la información está accesible con unos pocos clics del ratón: support.industry.siemens.com

Soporte técnico

El Soporte técnico de Siemens Industry le brinda un soporte rápido y competente con respecto a todas las consultas técnicas con numerosas ofertas a medida, que van desde soporte básico hasta contratos de soporte individuales.

Envíe sus consultas al Soporte Técnico a través del formulario web:

siemens.com/SupportRequest

SITRAIN – Academia de la Industria Digital

Le apoyamos con nuestros cursos de formación disponibles en todo el mundo para la industria con experiencia práctica, métodos de aprendizaje innovadores y un concepto que se adapta a las necesidades específicas del cliente.

Para obtener más información sobre nuestras capacitaciones y cursos ofrecidos, así como sus ubicaciones y fechas, consulte nuestra página web:

siemens.com/sitrain

oferta de servicio

Nuestra gama de servicios incluye lo siguiente:

- Servicios de datos de planta
- Servicios de repuestos
- Servicios de reparación
- Servicios in situ y de mantenimiento
- Servicios de reacondicionamiento y modernización
- Programas y contratos de servicios

Puede encontrar información detallada sobre nuestra gama de servicios en la página web del catálogo de servicios:

support.industry.siemens.com/cs/sc

Aplicación de soporte en línea de la industria

Recibirá un soporte óptimo esté donde esté con la aplicación "Siemens Industry Online Support". La aplicación está disponible para iOS y Android: support.industry.siemens.com/cs/ww/en/sc/2067

8 Apéndice

8.2

Centro comercial de la industria



Siemens Industry Mall es la plataforma en la que se puede acceder a toda la cartera de productos de Siemens Industry. Desde la selección de productos hasta el pedido y el seguimiento de la entrega, Industry Mall permite el procesamiento completo de compras, directamente e independientemente de la hora y la ubicación:

mall.industry.siemens.com

8.3

Enlaces y literatura

Tabla 8-1

No.	Tema
\1\ Asistencia en línea de la industria de Siemens	https://support.industry.siemens.com
\2\ Enlace a esta página de entrada de este ejemplo de aplicación	https://support.industry.siemens.com/cs/ww/en/view/109798583
\3\ Uso de Certificado con TIA Portal	https://support.industry.siemens.com/cs/ww/en/view/109769068
\4\ Diseño HMI con HMI Template Suite	https://support.industry.siemens.com/cs/ww/en/view/91174767
\5\ Exportación SIMATIC SCADA para TIA Portal	https://support.industry.siemens.com/cs/ww/en/view/109748955
\6\ Preguntas frecuentes WinCC SCADA	https://support.industry.siemens.com/cs/ww/en/view/109798498
\7\ Colección de manuales SIMATIC S7-1500/ET 200MP	https://support.industry.siemens.com/cs/ww/en/view/86140384
\8\ SIMATIC HMI - Dispositivos HMI Comfort Panels	https://support.industry.siemens.com/cs/ww/en/view/49313233
\9\ Actualización de firmware CPU S7-1500 incl. Displays y CPU ET 200 (ET 200SP, ET 200pro)	https://support.industry.siemens.com/cs/ww/en/view/109478459
\10\ Descripción de la actualización de firmware para CPU S7-1500, pantallas, CPU ET 200SP y CPU ET 200pro	https://support.industry.siemens.com/cs/ww/en/view/77492231
\11\ ¿Cómo se actualiza el sistema operativo en los paneles del operador o se realiza un "Restablecimiento de la configuración de fábrica"?	https://support.industry.siemens.com/cs/ww/en/view/19701610
\12\ ¿Cómo se realiza una copia de seguridad/restauración con un Comfort Panel?	https://support.industry.siemens.com/cs/ww/en/view/58876345

8 Apéndice

8.4 Cambiar documentación

Tabla 8-2

Versión	Fecha	Modificaciones
V1.0	11/2021	Primera versión