

SIEMENS
Ingenuity for life

Seguridad en TIA Portal V17 - Preguntas y respuestas

STEP 7 V17 / S7-1500 / WinCC Runtime avanzado

<https://support.industry.siemens.com/cs/ww/en/view/109799540>

Siemens
Industria
En línea
Apoyo



Esta entrada es de Siemens Industry Online Support. Las condiciones generales de uso (http://www.siemens.com/terms_of_use) aplicar.

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 cibernéticas, es necesario implementar, y mantener continuamente, un concepto de seguridad industrial holístico y de última generación. Los productos y soluciones de Siemens solo forman un elemento de dicho concepto.

El cliente es responsable de evitar el acceso no autorizado a sus plantas, sistemas, máquinas y redes. Los sistemas, máquinas y componentes solo deben conectarse a la red empresarial o a Internet si es necesario y en la medida en que sea necesario y con las medidas de seguridad adecuadas (p. ej., uso de cortafuegos y segmentación de la red) implementadas.

Además, se debe tener en cuenta la orientación de Siemens sobre las medidas de seguridad adecuadas. Para obtener más información sobre seguridad industrial, visite <http://www.siemens.com/industrialsecurity>.

Los productos y soluciones de Siemens se someten a un desarrollo continuo para hacerlos más seguros. Siemens recomienda encarecidamente aplicar actualizaciones de productos tan pronto como estén disponibles y utilizar siempre 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 <http://www.siemens.com/industrialsecurity>.

Tabla de contenidos

1	Introducción.....	4
2	Preguntas y respuestas	5
2.1	¿Cuáles son las nuevas características de seguridad introducidas en TIA Portal V17?	
2.2	.5 ¿A qué debo prestar atención cuando actualizo el firmware de mi PLC?.....	
2.3	5 ¿Cuándo y cómo mi PLC utiliza completamente las nuevas características de seguridad introducidas en TIA Portal V17?	
2.4	6 ¿Qué es el "Asistente de seguridad" y por qué lo necesito?	6
2.5	¿Qué se puede configurar con el "Asistente de seguridad"?	6
2.6	¿Por qué necesito definir una contraseña para los datos de configuración del PLC?.....	7
2.7	¿La comunicación entre el PG y el PLC es segura incluso si no asigno una contraseña de datos de configuración confidencial del PLC?	7
2.8	¿Qué debo hacer si quiero cambiar un PLC que está protegido con una contraseña de datos de configuración confidencial?	8
2.9	¿Puedo asignar una contraseña de datos de configuración confidencial a un PLC sin utilizar el TIA Portal?	8
2.10	¿Cómo puedo asignar una contraseña de datos de configuración confidencial a un PLC sin utilizar TIA Portal?	9
2.10.1	Procedimiento	9
2.10.2	Creación de una SIMATIC Memory Card con "SET PASSWORD" archivo TRABAJO.....	
2.11	9 ¿Cómo puedo conectar sistemas HMI antiguos (<TIA Portal V17) con un nuevo firmware de PLC (≥V2.9)?	10
2.12	¿Qué se debe tener en cuenta para una comunicación PG / HMI segura cuando se trabaja con certificados?	11
2.13	¿Qué debo hacer si caducan los certificados en el PLC/HMI?....	12
2.14	¿Cuáles son las mejoras de seguridad con respecto a la protección de proyectos y la gestión de usuarios en TIA Portal V17?	12

1 Introducción

General

El avance de la digitalización de la industria también aumenta el riesgo de ataques cibernéticos. La Seguridad Industrial es, por tanto, un componente esencial de la digitalización. Para proteger plantas, sistemas, máquinas y redes contra amenazas cibernéticas, es necesario implementar, y mantener continuamente, un concepto integral de seguridad industrial. Las medidas de protección adecuadas son imperativas, especialmente para las instalaciones de infraestructura crítica.

Solución

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 tanto en TIA Portal V17 como en la versión de firmware de los dispositivos más nuevos. Estas funciones garantizan que los datos de comunicación no estén sujetos a manipulación mediante autenticación segura y protección de comunicación basada en TLS. También brindan protección contra el acceso no autorizado a máquinas y software.

2 Preguntas y respuestas

2.1 ¿Cuáles son las nuevas características de seguridad introducidas en TIA Portal V17?

1. Con TIA portal V17, se han introducido varias mejoras de seguridad para la comunicación entre estaciones de ingeniería, PLC y paneles HMI.
Esto incluye:
 - a. La comunicación está asegurada mediante el protocolo Transport Layer Security o TLS ampliamente utilizado en Internet. Proporciona cifrado e integridad de datos entre los socios de comunicación.
 - b. La comunicación se cifra y autentica aplicando certificados individuales para cada PLC. 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: <https://support.industry.siemens.com/cs/us/en/view/109769068>
 - c. Para garantizar que la comunicación del PLC funcione con versiones anteriores de TIA Portal < V17 y sistemas HMI < V17, se debe activar la comunicación en modo seguro y heredado.
 - d. La comunicación encriptada protege contra la manipulación de datos y asegura la integridad de los datos.
 - mi. Los datos de configuración confidenciales de los PLC pueden ser protegidos por un usuario contraseña definida. Esta protección es opcional.
2. También se han introducido otras mejoras relacionadas con la protección de proyectos y la gestión de usuarios. Para más información ver el capítulo 2.14.
3. Con TIA Portal V17, el servidor S7-1500 OPC UA es compatible con Global Discovery Server - GDS a partir del firmware V2.9. Esto permite actualizar el certificado durante el tiempo de ejecución sin interrupción del PLC. El servidor OPC UA también admite Listas de revocación de certificados: CRL que aumentan la seguridad al declarar uno o más certificados previamente confiables como no confiables cuando sea necesario.

2.2 ¿A qué debo prestar atención cuando actualizo el firmware de mi PLC?

Los PLC ya configurados cargados con TIA Portal ≤ V16 que se han actualizado a la versión de firmware 2.9 no tendrán las funciones de seguridad más recientes activadas de forma predeterminada. Debe configurar explícitamente el PLC con TIA Portal V17 y activar las nuevas funciones de seguridad.

Si actualiza un PLC que se configuró originalmente con TIA Portal ≤ V16 al firmware V2.9, entonces el PLC funciona en el llamado "modo de compatibilidad" (heredado). Para beneficiarse de las nuevas funciones de seguridad en TIA Portal V17, puede: • Agregar un nuevo dispositivo en el proyecto TIA Portal (nueva configuración). • o configure las opciones de seguridad manualmente para los existentes y los recién actualizados PLC

NOTA

Los PLC en TIA Portal V17 pueden funcionar en dos modos: modo seguro y modo mixto.

- En el modo seguro, solo se permite la comunicación segura basada en TLS entre el PLC y las estaciones de ingeniería/paneles HMI.
- En el modo Mixto, el PLC puede comunicarse de forma segura mediante TLS con estaciones de ingeniería/paneles HMI reales, así como con estaciones de ingeniería/paneles HMI que utilizan una versión anterior de TIA Portal.

2.3 ¿Cuándo y cómo utiliza completamente mi PLC las nuevas características de seguridad introducidas en TIA Portal V17?

Cuando se agrega un nuevo PLC al proyecto TIA Portal V17, se han preconfigurado varias funciones de seguridad de forma predeterminada para garantizar un mayor nivel de seguridad para las máquinas y las plantas.

Esto incluye:

- La protección de acceso al PLC preactivada que impide cualquier tipo de acceso al PLC a menos que se configure explícitamente (Nivel de Acceso: Sin acceso).
- El requisito de contraseña de configuración preactivada que garantiza que todos los datos de configuración confidenciales del PLC estén protegidos de forma predeterminada.
- La opción preactivada "Permitir solo comunicación segura PG/PC y HMI" lo que evita la comunicación heredada con otros socios.

Solo cuando todas las opciones mencionadas anteriormente están configuradas, se beneficia al máximo de las nuevas funciones de seguridad introducidas en TIA portal V17.

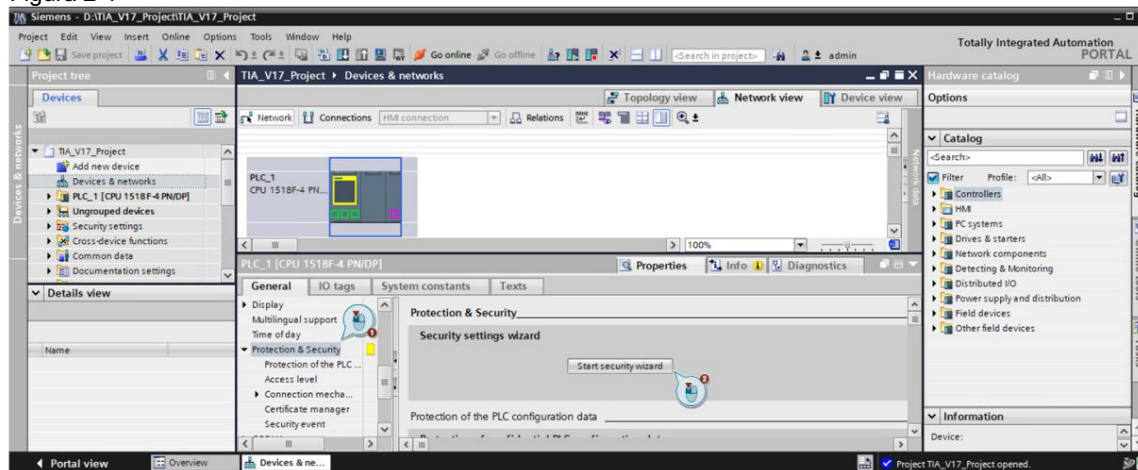
Esto instituye el concepto principal de "Seguridad por defecto" que garantiza que se introduce en consecuencia el máximo nivel de protección del dispositivo.

2.4 ¿Qué es el "Asistente de seguridad" y por qué lo necesito?

El concepto de "Seguridad por defecto" requiere que establezca más de una configuración en el menú de seguridad. Para simplificar este proceso, se presenta un asistente en TIA Portal V17 para ayudarlo con la configuración de seguridad.

El asistente se inicia automáticamente al agregar un nuevo PLC al proyecto TIA. Para iniciar el asistente manualmente, ingrese al menú de propiedades del PLC en: "Protección y seguridad" y luego "Iniciar asistente de seguridad".

Figura 2-1

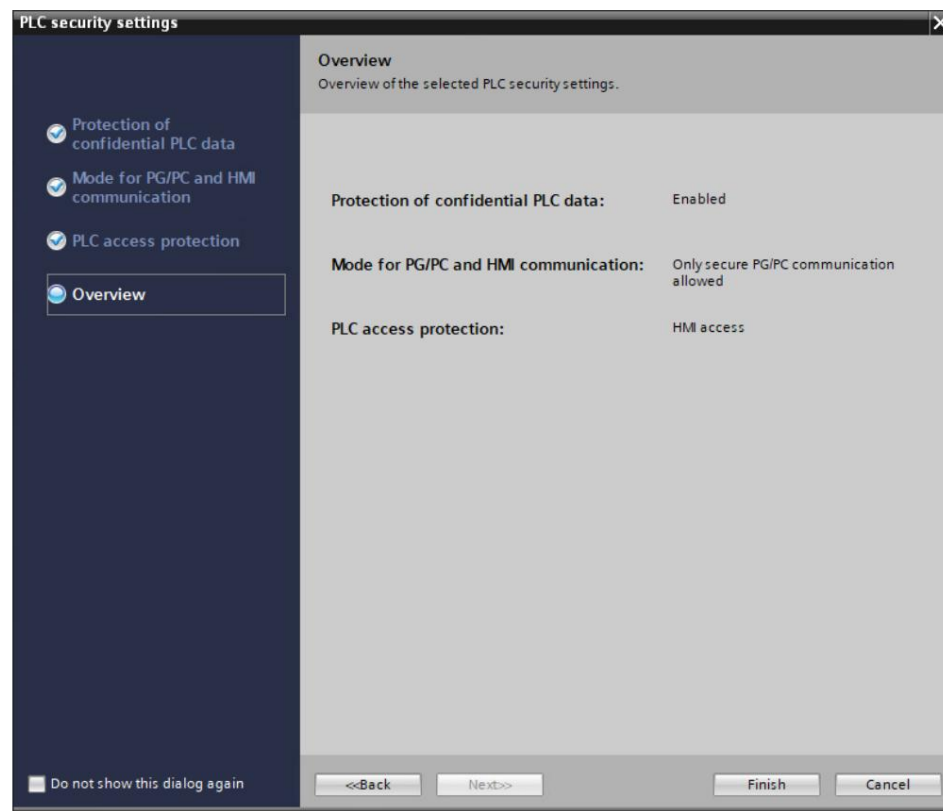


2.5 ¿Qué se puede configurar con el "Asistente de seguridad"?

Con el asistente de seguridad se pueden configurar las siguientes opciones de seguridad:

- La protección de los datos confidenciales de configuración del PLC.
- El modo de comunicación PG/HMI. (Modo Seguro – Modo Mixto).
- El nivel de acceso del PLC.

Figura 2-2



2.6 ¿Por qué necesito definir una contraseña para los datos de configuración del PLC?

Para proteger los datos de configuración confidenciales (p. ej., claves privadas para certificados, contraseñas) de los PLC, tiene la opción de introducir una contraseña en el TIA Portal.

La contraseña se descarga con la primera descarga, junto con los datos de configuración confidenciales y no confidenciales. La contraseña se guarda directamente en el PLC y se utiliza para leer los datos de configuración confidenciales en la SIMATIC Memory Card.

Los datos de configuración típicos que se consideran confidenciales son los certificados y las claves privadas. Los datos de configuración no confidenciales se almacenan en la SIMATIC Memory Card junto con los datos confidenciales.

Con este nuevo mecanismo, tiene la opción de proteger los datos de configuración confidenciales con una clave personalizada.

2.7 ¿La comunicación entre la PG y el PLC es segura incluso si no asigno una contraseña de datos de configuración confidencial del PLC?

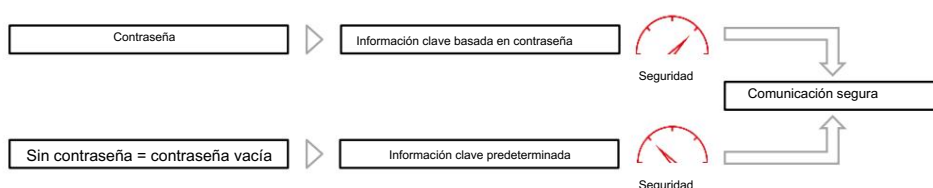
La comunicación segura entre PG, PLC y paneles HMI requiere protocolos basados en certificados que, a su vez, dependen de claves privadas que deben protegerse lo mejor posible. A partir de TIA Portal V17, puede usar una contraseña para proteger estas claves y otros datos que vale la pena proteger: La contraseña para proteger los datos confidenciales de configuración del PLC. Es posible prescindir de la contraseña si tiene

implementó medidas para evitar el acceso no autorizado al proyecto TIA Portal y la configuración del PLC.

Independientemente de si asigna una contraseña o no: el TIA Portal genera una información clave que proporciona la protección de los datos confidenciales de configuración del PLC. Esta contraseña no influye en el proceso de comunicación segura. Sin embargo, la complejidad de la contraseña para la protección de los datos confidenciales de configuración del PLC determina qué tan bien se protegen las claves privadas, por ejemplo.

La presencia de información clave es un requisito previo para una comunicación segura, como la comunicación PG/HMI segura basada en TLS: el PLC puede manejar certificados que se requieren para una comunicación segura solo si esta información clave está disponible. La siguiente figura muestra las relaciones descritas:

Figura 2-3



2.8

¿Qué debo hacer si quiero cambiar un PLC que está protegido con una contraseña de datos de configuración confidencial?

Cuando se requiere un cambio de dispositivo, los datos de configuración del PLC anterior, que están protegidos por una contraseña personalizada, deben transferirse al nuevo PLC. Para conseguirlo existen tres posibilidades diferentes: 1. Descargando el proyecto TIA al nuevo PLC.

La contraseña de configuración

se establecerá en el nuevo PLC durante la primera descarga.

2. Mediante acceso online directo al nuevo PLC mediante TIA Portal o SIMATIC

Herramienta de automatización - SAT y establecimiento de la contraseña de configuración en él. Después de eso, la SIMATIC Memory Card - SMC debe retirarse del antiguo PLC e insertarse en el nuevo PLC.

3. Mediante el uso de una SIMATIC Memory Card adicional. La contraseña de configuración del antiguo PLC, así como un archivo JOB especial, se almacenan en esta tarjeta de memoria que se puede insertar en el nuevo PLC para la configuración inicial. Después de eso, la tarjeta de memoria del antiguo PLC se puede insertar en el nuevo PLC. Para obtener más información sobre este método, consulte el capítulo [2.10](#)

2.9

¿Puedo asignar una contraseña de datos de configuración confidencial a un PLC sin utilizar el TIA Portal?

Es posible asignar una contraseña a un PLC para proteger los datos de configuración confidenciales del PLC sin utilizar el TIA Portal. Esto se puede hacer usando una tarjeta de memoria SIMATIC.

El uso de una tarjeta de memoria SIMATIC es adecuado para los siguientes propósitos: •

Preparación de un nuevo PLC: cuando se configura un PLC nuevo, debe configurarse con una contraseña para garantizar que se puedan utilizar los datos de configuración confidenciales.

Una vez completada esta configuración, es posible utilizar otra SIMATIC Memory Card con el proyecto deseado.
(PLC S7-1200: También es posible utilizar una tarjeta "Transfer" con trabajo de transferencia para instalar el programa en el PLC).

- El PLC ya tiene una contraseña para proteger los datos de configuración confidenciales, pero la contraseña no coincide con el proyecto. En caso de contraseñas diferentes, puede configurar la contraseña correcta con la tarjeta de memoria en el PLC.
(S7-1200 PLC: equipado con tarjeta SIMATIC "Transfer" o con tarjeta SIMATIC "Programa").
- Restablecimiento de la contraseña para proteger los datos de configuración confidenciales en el PLC.
Esto puede ser útil en casos como la preparación para la eliminación de PLC o en la preparación de un nuevo proyecto para el PLC.

2.10 ¿Cómo puedo asignar un dato de configuración confidencial? contraseña a un PLC sin utilizar el TIA Portal?

2.10.1 Procedimiento

1. 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 la descripción de los pasos necesarios para crear el archivo JOB "SET PASSWORD" vea el capítulo [2.10.2](#).
2. Inserte la SIMATIC Memory Card preparada en el PLC y enciéndala.
El PLC lee la contraseña, la procesa y almacena el resultado en la memoria interna. Se sobrescribe una entrada posiblemente existente.
3. Extraiga la SIMATIC Memory Card y reinicie el PLC.

Resultado (S7-1500)

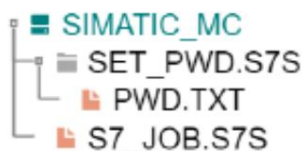
Mientras el PLC lee la SIMATIC Memory Card, el LED muestra el mismo comportamiento que durante una actualización de firmware. Mientras el PLC establece la contraseña, el LED RUN/STOP parpadea. Una vez que el proceso se ha completado con éxito, el LED RUN/STOP es amarillo y el LED MAINT parpadea en amarillo.


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.

2.10.2 Crear una tarjeta de memoria SIMATIC con el archivo JOB "SET PASSWORD"

1. Cree una carpeta en el directorio raíz y asígnele el nombre "SET_PWD.S7S".
2. Cree un archivo de texto llamado "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" en el directorio raíz de la SIMATIC Memory Card con el contenido "SET_PWD".
Este archivo es el "archivo TRABAJO". Se utiliza para asignar una contraseña al PLC para proteger los datos de configuración confidenciales.
4. La estructura de archivos en la SIMATIC Memory Card tendrá el siguiente aspecto:

Figura 2-4



 PRECAUCIÓN	<p>Almacenamiento seguro de la SIMATIC Memory Card</p> <p>Guarde la tarjeta de memoria SIMATIC en un lugar seguro al que solo tengan acceso las personas autorizadas.</p>
--------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------

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 asignado en la configuración del PLC.
- 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. La contraseña en sí es mayúscula sensible.
- No agregue caracteres CR/LF al final (PWD.TXT o S7_JOB.S7S).

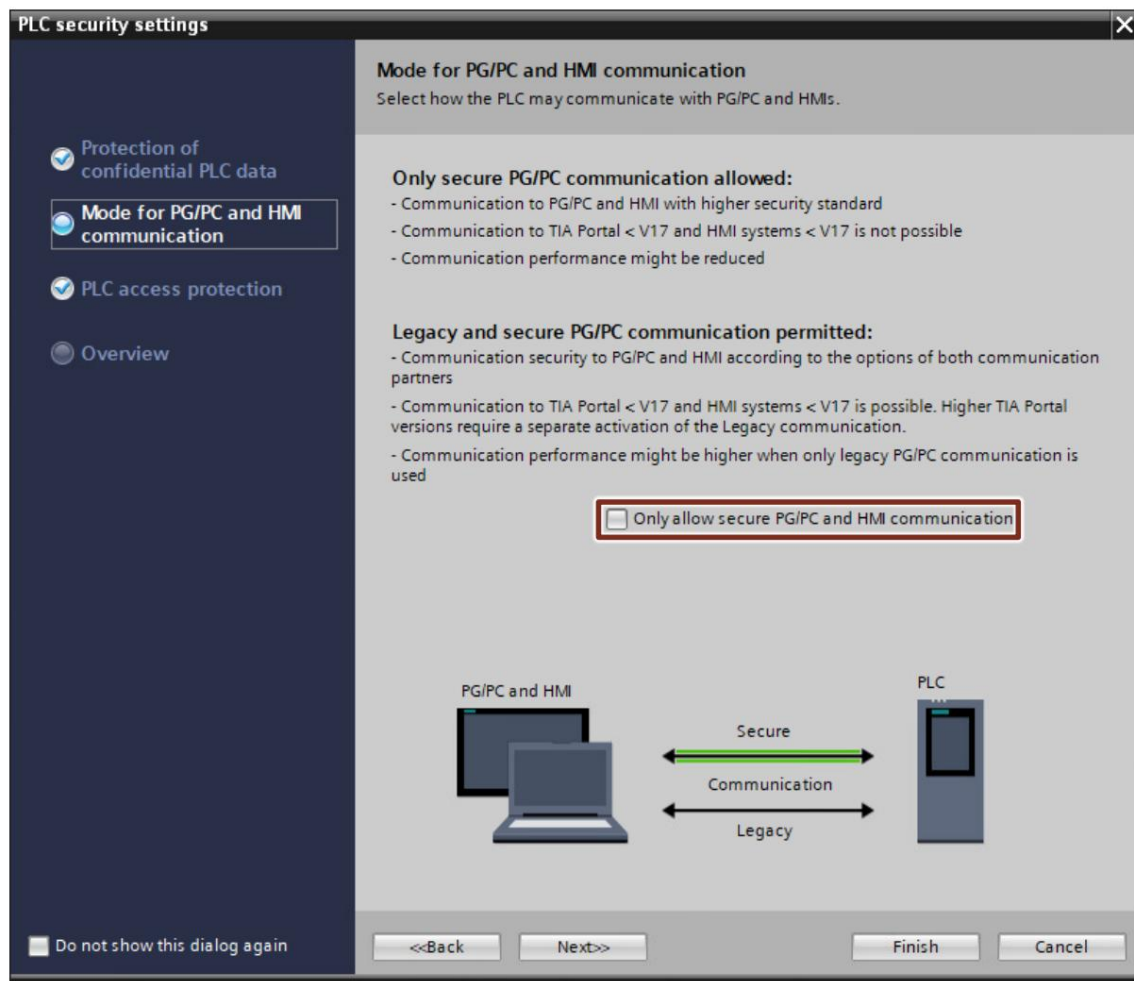
2.11 ¿Cómo puedo conectar sistemas HMI antiguos (<TIA Portal V17) con un nuevo firmware de PLC (≥V2.9)?

Siempre se recomienda actualizar los sistemas HMI a la última versión de firmware. De esta forma, puede tener lugar una comunicación segura entre el PLC y los sistemas HMI.

Sin embargo, para los casos en los que no es posible actualizar los sistemas HMI, el PLC con la última versión de firmware aún puede comunicarse con los sistemas HMI más antiguos al permitir que el PLC funcione en el modo mixto, es decir, en el modo seguro y en el modo heredado.

2 Preguntas y respuestas

Figura 2-5



2.12 Qué se debe tener en cuenta para un PG seguro

/ ¿Comunicación HMI cuando se trabaja con certificados?

Cada certificado tiene una vigencia o validez que comienza y finaliza en un momento determinado. Cuando crea un certificado en TIA Portal, es válido hasta el año 2037 de forma predeterminada. Esta configuración se puede cambiar. Cuando pasa la vida útil de los certificados, debe renovarse manualmente en el TIA Portal. Todavía no es posible una renovación automática para el certificado TLS.

Para garantizar la validez temporal de los certificados de la CPU, se recomienda utilizar un servidor NTP en los interlocutores de la comunicación para sincronizar su tiempo. Puede encontrar más información sobre la sincronización horaria aquí: <https://support.industry.siemens.com/cs/ww/en/view/69864408>

2.13 ¿Qué debo hacer si vencen los certificados en el PLC/HMI?

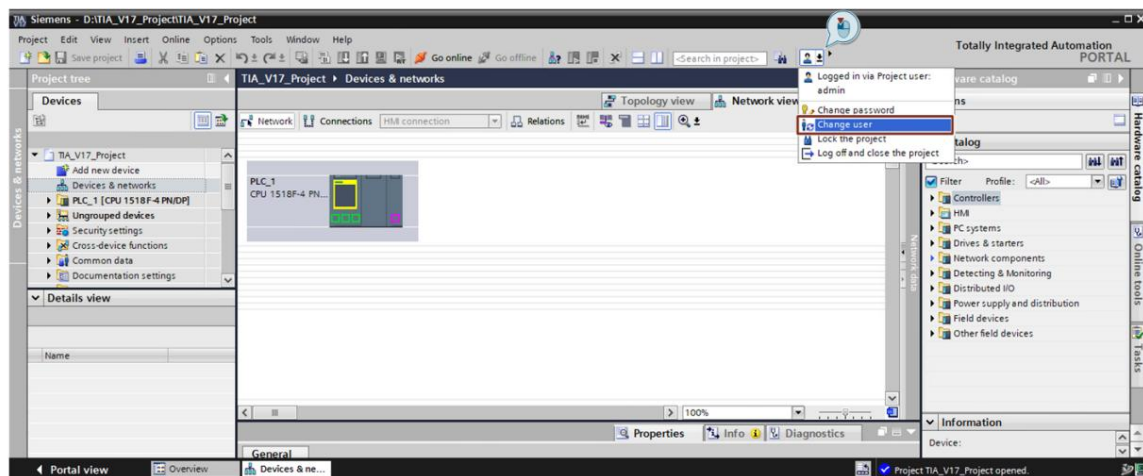
Cuando caduca el certificado, aparece una entrada en el búfer de diagnóstico del PLC para indicar este evento. Lo mismo sucede en los paneles HMI. Posteriormente, el certificado debe renovarse manualmente en el TIA Portal. Tenga en cuenta que aún no es posible una renovación automática de los certificados TLS.

NOTA Esto no se aplica a los certificados de comunicación OPC UA. Aquí, un nuevo
Se ha introducido en TIA Portal V17 un mecanismo que permite la renovación automática de los certificados OPC UA mediante un Global Discovery Server - GDS.

2.14 ¿Cuáles son las mejoras de seguridad con respecto a la protección de proyectos y la gestión de usuarios en TIA Portal V17?

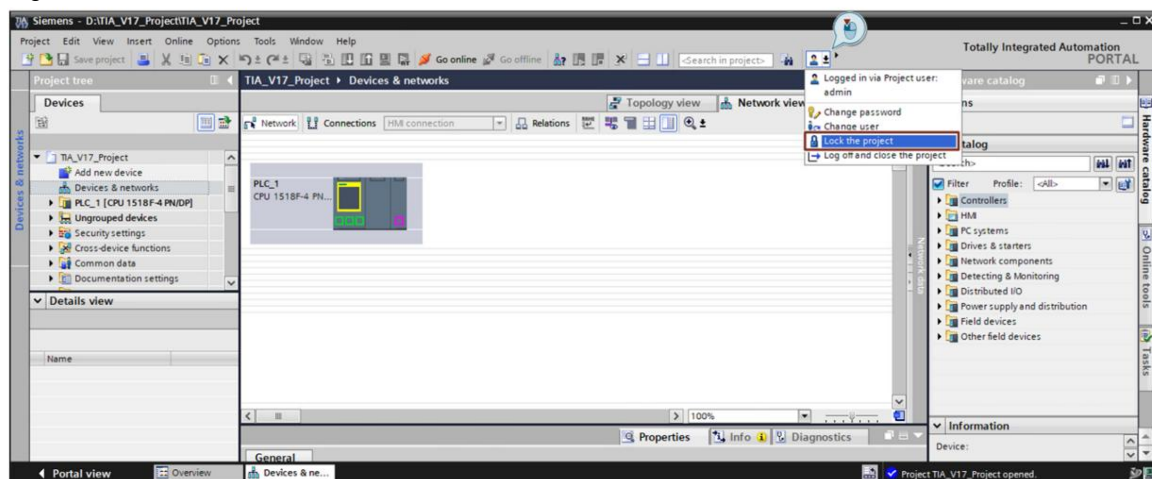
1. Cambiar usuario: entrada de menú para cambiar el usuario activo dentro de un proyecto abierto

Figura 2-6



2. Bloqueo de proyecto: un proyecto abierto se puede proteger contra la edición a través del bloqueo de proyecto. El bloqueo del proyecto se puede activar de forma manual o automática tras un tiempo configurable de inactividad

Figura 2-7



2 Preguntas y respuestas

3. Las acciones del usuario pueden ser restringidas por los nuevos derechos de usuario de la función:
 - Derechos de funciones generales: Modificar tipo de biblioteca, Cambiar configuración de hardware, Importar texto de proyecto, Actualizar proyecto
 - PLC: Descargar, Cambiar programa, Modificar programa de PLC de seguridad, Monitorear, Editar programa de PLC en línea
 - HMI: Descargar, Configurar, Mantenimiento
 - Unidades: modificar la configuración de la unidad
 - Runtime Rights: derechos para componentes de red
4. Inicio de sesión único (SSO): TIA Portal y HMI Runtimes admiten inicio de sesión único conexión (en la misma estación de ingeniería)
5. Compatibilidad con SIMATIC Logon Protocol en servidores UMC para WinCC Runtime Avanzado