SIEMENS

SIMATIC NET

ET 200SP - Industrial Ethernet CP 1542SP-1, CP 1542SP-1 IRC, CP 1543SP-1

Instrucciones de servicio

01/2017

C79000-G8978-C426-03

Notas jurídicas

Filosofía en la señalización de advertencias y peligros

Este manual contiene las informaciones necesarias para la seguridad personal así como para la prevención de daños materiales. Las informaciones para su seguridad personal están resaltadas con un triángulo de advertencia; las informaciones para evitar únicamente daños materiales no llevan dicho triángulo. De acuerdo al grado de peligro las consignas se representan, de mayor a menor peligro, como sigue.

⚠PELIGRO
Significa que, si no se adoptan las medidas preventivas adecuadas **se producirá** la muerte, o bien lesiones corporales graves.

⚠ADVERTENCIA
Significa que, si no se adoptan las medidas preventivas adecuadas **puede producirse** la muerte o bien lesiones corporales graves.

⚠PRECAUCIÓN
Significa que si no se adoptan las medidas preventivas adecuadas, pueden producirse lesiones corporales.

ATENCIÓN
Significa que si no se adoptan las medidas preventivas adecuadas, pueden producirse daños materiales.

Si se dan varios niveles de peligro se usa siempre la consigna de seguridad más estricta en cada caso. Si en una consigna de seguridad con triángulo de advertencia se alarma de posibles daños personales, la misma consigna puede contener también una advertencia sobre posibles daños materiales.

Personal cualificado

El producto/sistema tratado en esta documentación sólo deberá ser manejado o manipulado por **personal cualificado** para la tarea encomendada y observando lo indicado en la documentación correspondiente a la misma, particularmente las consignas de seguridad y advertencias en ella incluidas. Debido a su formación y experiencia, el personal cualificado está en condiciones de reconocer riesgos resultantes del manejo o manipulación de dichos productos/sistemas y de evitar posibles peligros.

Uso previsto de los productos de Siemens

Considere lo siguiente:

⚠ADVERTENCIA
Los productos de Siemens sólo deberán usarse para los casos de aplicación previstos en el catálogo y la documentación técnica asociada. De usarse productos y componentes de terceros, éstos deberán haber sido recomendados u homologados por Siemens. El funcionamiento correcto y seguro de los productos exige que su transporte, almacenamiento, instalación, montaje, manejo y mantenimiento hayan sido realizados de forma correcta. Es preciso respetar las condiciones ambientales permitidas. También deberán seguirse las indicaciones y advertencias que figuran en la documentación asociada.

Marcas registradas

Todos los nombres marcados con ® son marcas registradas de Siemens AG. Los restantes nombres y designaciones contenidos en el presente documento pueden ser marcas registradas cuya utilización por terceros para sus propios fines puede violar los derechos de sus titulares.

Exención de responsabilidad

Hemos comprobado la concordancia del contenido de esta publicación con el hardware y el software descritos. Sin embargo, como es imposible excluir desviaciones, no podemos hacernos responsable de la plena concordancia. El contenido de esta publicación se revisa periódicamente; si es necesario, las posibles las correcciones se incluyen en la siguiente edición.

Siemens AG
Division Process Industries and Drives
Postfach 48 48
90026 NÜRNBERG
ALEMANIA

C79000-G8978-C426-02
℗ 01/2017 Sujeto a cambios sin previo aviso

Prólogo

Ámbito de validez de este manual

En este documento encontrará información acerca de los módulos siguientes:

- **CP 1542SP-1**
  Referencia **6GK7542-6UX00-0XE0**
  Versión del hardware 1
  Versión del firmware V1.0
  Procesador de comunicaciones para la conexión de una CPU SIMATIC ET 200SP a Industrial Ethernet
- **CP 1542SP-1 IRC**
  Referencia **6GK7542-6VX00-0XE0**
  Versión del hardware 1
  Versión del firmware V1.0
  Procesador de comunicaciones para la conexión de una CPU SIMATIC ET 200SP a un puesto de mando (TCSB, DNP3, IEC 60870-5-104) a través de Industrial Ethernet
- **CP 1543SP-1**
  Referencia **6GK7543-6WX00-0XE0**
  Versión del hardware 1
  Versión del firmware V1.0
  Procesador de comunicaciones para la conexión de una CPU SIMATIC ET 200SP a Industrial Ethernet Security

Figura 1 CP 1542SP-1 con BusAdapter insertado (en este caso 2xRJ45)

En el margen derecho de la cara frontal del módulo está impresa la versión de hardware en forma de comodín "X". Si está impresa, por ejemplo, "X 2 3 4", X es el comodín de la versión de hardware 1.

Inmediatamente debajo se indica la versión de firmware del CP en el momento del suministro.

La dirección MAC está impresa en la parte inferior izquierda de la cara frontal, sobre las conexiones para el suministro de tensión.

Nombre del producto, términos y abreviaciones

A continuación se recogen los términos y las abreviaciones utilizados asiduamente en el presente manual.

- **CP**

  Si la propiedad descrita en el contexto en cuestión es aplicable a los tres tipos de CP o si el tipo de CP utilizado puede determinarse claramente a partir del contexto, la abreviación "CP" se utiliza en representación de los tres nombres de producto siguientes:

  – CP 1542SP-1

  – CP 1542SP-1 IRC

  – CP 1543SP-1

  Si alguna información solo es aplicable a una variante de producto determinada, se indica el nombre completo del módulo.

- **TCSB**

  Software para puestos de control "TeleControl Server Basic"

- **Servidor de Telecontrol**

  PC con software instalado "TeleControl Server Basic"

Finalidad de este manual

El presente manual describe las propiedades del módulo y presta apoyo en el montaje y la puesta en servicio.

Los pasos de configuración necesarios se describen como descripción general y se ofrecen explicaciones de la relación entre las funciones de firmware y la configuración.

Además, encontrará indicaciones sobre las posibilidades de diagnóstico del dispositivo.

Conocimientos presupuestos

Para el montaje, la puesta en marcha y el servicio del CP se requieren conocimientos en los ámbitos siguientes:

- Automatización
- Diseño del sistema SIMATIC ET 200SP
- SIMATIC STEP 7 Professional

Novedades de la presente edición

Revisión de contenido (Homologación MSIP)

Edición sustituida

Edición 11/2016

Última edición del manual en Internet

También puede consultar la última edición del presente manual en las páginas web de Siemens Industry Online Support, en las siguientes direcciones:

- CP 1542SP-1 / CP 1543SP-1
  Enlace: (https://support.industry.siemens.com/cs/ww/es/ps/22144/man)
- CP 1542SP-1 IRC
  Enlace: (https://support.industry.siemens.com/cs/ww/es/ps/22143/man)

Referencias cruzadas

En este manual se emplean con frecuencia referencias cruzadas a otros capítulos.

Para volver a la página de inicio después de haber saltado a una referencia cruzada, algunos lectores de archivos PDF utilizan el comando <Alt>+<Flecha izquierda>.

Documentación complementaria

En el anexo de este manual encontrará la bibliografía existente en torno al tema.

Condiciones de la licencia

Nota

Open Source Software

Lea detenidamente las condiciones de la licencia para Open Source Software antes de utilizar el producto.

Encontrará las condiciones de licencia en el siguiente documento incluido en los soportes de datos suministrados:

- OSS_CP-ET200SP_86.pdf

Información de seguridad

Siemens ofrece productos y soluciones con funciones de seguridad industrial con el objetivo de hacer más seguro el funcionamiento de instalaciones, sistemas, máquinas y redes.

Para proteger las instalaciones, los sistemas, las máquinas y las redes de amenazas cibernéticas, es necesario implementar (y mantener continuamente) un concepto de seguridad industrial integral que sea conforme a la tecnología más avanzada. Los productos y las soluciones de Siemens constituyen únicamente una parte de este concepto.

El cliente es responsable de impedir el acceso no autorizado a sus instalaciones, sistemas, máquinas y redes. Los sistemas, las máquinas y los componentes solo deben estar conectados a la red corporativa o a Internet cuando y en la medida que sea necesario y

siempre que se hayan tomado las medidas de protección adecuadas (p. ej. uso de cortafuegos y segmentación de la red).

Adicionalmente, deberán observarse las recomendaciones de Siemens en cuanto a las medidas de protección correspondientes. Encontrará más información sobre seguridad industrial en
Enlace: (http://www.siemens.com/industrialsecurity).

Los productos y las soluciones de Siemens están sometidos a un desarrollo constante con el fin de mejorar todavía más su seguridad. Siemens recomienda expresamente realizar actualizaciones en cuanto estén disponibles y utilizar únicamente las últimas versiones de los productos. El uso de versiones anteriores o que ya no se soportan puede aumentar el riesgo de amenazas cibernéticas.

Para mantenerse informado de las actualizaciones de productos, recomendamos que se suscriba al Siemens Industrial Security RSS Feed en
Enlace: (http://www.siemens.com/industrialsecurity).

Firmware

El firmware está firmado y codificado. Con esto se garantiza que solo se pueda cargar firmware creado por Siemens en el dispositivo.

Glosario de SIMATIC NET

Las explicaciones de muchos de los términos utilizados en esta documentación están recogidas en el glosario de SIMATIC NET.

Encontrará el glosario de SIMATIC NET aquí:

- SIMATIC NET Manual Collection o DVD del producto

  Este DVD se adjunta a algunos productos SIMATIC NET.

- En la siguiente dirección de Internet:

  Enlace: (https://support.industry.siemens.com/cs/ww/es/view/50305045)

Formación, Service & Support

Encontrará la información relativa a la formación, Service & Support en el documento multilingüe "DC_support_99.pdf", disponible en las páginas de Internet de Siemens Industry Online Support:

Enlace: (https://support.industry.siemens.com/cs/ww/es/view/38652101)

Índice

Aplicación y funciones

1

1.1 Volumen de suministro

El volumen de suministro del producto incluye los siguientes componentes:

- CP 154xSP-1
- conector para el conector hembra de la alimentación (24 V DC) del CP
- DVD con documentación y textos de licencia

El volumen de suministro no incluye un BusAdapter para la conexión Ethernet del CP.

1.2 Aplicación

Aplicación de las variantes del CP

El CP permite conectar el ET 200SP a Industrial Ethernet a través de cable de cobre o de fibra óptica. Puede emplearse como interfaz Ethernet adicional de la CPU para la comunicación S7.

Para la conexión Ethernet el CP necesita un BusAdapter, que no está incluido en el volumen de suministro del CP.

Las tres variantes de CP están previstas para las siguientes tareas de comunicación:

- **CP 1542SP-1**

  El CP 1542SP-1 permite al ET 200SP disponer de una conexión Ethernet adicional.

- **CP 1542SP-1 IRC**

  El CP 1542SP-1 IRC soporta la comunicación Telecontrol para la integración de la CPU ET 200SP en un puesto de control. Los siguientes protocolos de Telecontrol pueden utilizarse de forma alternativa:

  – TeleControl Basic

    Para la conexión del ET 200SP a una central con servidor de Telecontrol (TCSB V3 SP3)

  – DNP3

    Para la conexión del ET 200SP a una central con maestros DNP3

  – IEC 60870-5-104

    Para la conexión del ET 200SP a una central con maestros IEC

- **CP 1543SP-1**

  El CP 1543SP-1 dispone de funciones Security para la seguridad de red, como por ejemplo cortafuegos y VPN. Eso posibilita el acceso protegido al ET 200SP.

1.3 Servicios de comunicación

Servicios de comunicación

Se soportan los siguientes servicios de comunicación:

- **Comunicación S7 y comunicación PG/OP con las siguientes funciones:**
  - PUT/GET como cliente y servidor para el intercambio de datos con estaciones S7
  - Funciones de PG
  - Funciones de manejo y visualización (HMI)

  Para la comunicación S7 el CP requiere una dirección IP fija.
- **Routing S7**
  - Enrutamiento de conexiones S7 a través del bus de fondo y la CPU con otras estaciones S7
- **Open User Communication (OUC)**

  OUC a través de bloques de programa con los siguientes protocolos:
  - TCP/IP
  - ISO-on-TCP
  - UDP

  El CP 1543SP-1 soporta Secure OUC.

  Encontrará los bloques de programa que soportan los tres tipos de CP en el capítulo Programación (OUC) (Página 97).
- **Correo electrónico a través de bloques de programa**
- **HTTP / HTTPS**

  A través de HTTP / HTTPS se puede acceder al servidor web de la CPU.

Respecto a la comunicación Telecontrol del CP 1542SP-1 IRC consulte el capítulo Comunicación Telecontrol del CP 1542SP-1 IRC (Página 13).

Respecto a las funciones Security del CP 1543SP-1 consulte el capítulo Funciones Security (CP 1542SP-1 IRC, CP 1543SP-1) (Página 15).

1.4 Comunicación Telecontrol del CP 1542SP-1 IRC

Protocolos Telecontrol

Además de los servicios de comunicación arriba indicados, el CP 1542SP-1 IRC soporta los siguientes protocolos de telecontrol para la comunicación con una central:

- **TeleControl Basic**

  Se trata de un protocolo propio de Siemens para aplicaciones de telecontrol. Este protocolo basado en IP sirve para integrar el CP en la aplicación TCSB.

  TCSB está instalada en un PC en la central, el servidor de Telecontrol. Mediante el servidor OPC-DA o el servidor OPC-UA de TCSB, un cliente OPC puede acceder a los datos de proceso del CP.

  TCSB se soporta a partir de la siguiente versión: V3.0 + SP3

  Sobre el manual de TCSB, consulte /3/ (Página 124).

- **DNP3**

  El CP actúa como estación DNP3 (Outstation).

  La comunicación se basa en la DNP3 SPECIFICATION Version 2.11 (2007/2009).

  En el perfil de dispositivo DNP3 encontrará una lista detallada de los atributos y las propiedades especificadas en el protocolo DNP3 y soportadas por el CP, consulte Enlace: (https://support.industry.siemens.com/cs/ww/es/ps/22143/man).

  Puede consultar los grupos de objetos y variaciones soportados en el capítulo Tipos de puntos de datos (Página 60).

  Los interlocutores (maestros DNP3) del CP pueden ser:

  – SIMATIC PCS7 TeleControl
  – SIMATIC WinCC TeleControl
  – SIMATIC WinCC OA
  – un bloque TIM apto para DNP3 (TIM 3V IE DNP3 / TIM 4R IE DNP3).

    Consulte el manual del módulo TIM en /5/ (Página 124).
  – sistemas de otros fabricantes que soporten la especificación DNP3 indicada más arriba.

- **IEC 60870-5-104**

  El CP actúa como subestación (esclavo).

  La comunicación se basa en la especificación IEC 60870-5, parte 104 (2006).

  En el perfil de dispositivo IEC encontrará una lista detallada de los atributos y las propiedades especificadas en las especificaciones IEC y soportadas por el CP, consulte Enlace: (https://support.industry.siemens.com/cs/ww/es/ps/22143/man).

  Encontrará las identificaciones de tipo IEC que se soportan en el capítulo Tipos de puntos de datos (Página 60).

  Los interlocutores (maestros IEC) del CP pueden ser:

- SIMATIC PCS7 TeleControl
- SIMATIC WinCC TeleControl
- SIMATIC WinCC OA
- sistemas de otros fabricantes que soporten la especificación DNP3 indicada más arriba.

Propiedades del CP Telecontrol

- **Configuración de puntos de datos**

  Los valores de proceso se configuran para la comunicación como puntos de datos. Los puntos de datos acceden a las variables PLC de la CPU. Los puntos de datos pueden procesarse uno a uno en el sistema de control.

- **Mensajes/correo electrónico**

  Para eventos configurables en la memoria imagen del proceso de la CPU, el CP 1542SP-1 IRC puede enviar mensajes en forma de correo electrónico. Los datos que se envían por correo electrónico se configuran mediante variables PLC.

- **Almacenamiento de eventos**

  El CP 1542SP-1 IRC puede guardar eventos de diferentes clases y transferirlos agrupados al interlocutor.

- **Preprocesamiento de valores analógicos**

  Los valores analógicos pueden preprocesarse en el CP 1542SP-1 IRC siguiendo distintos métodos.

1.5 Otros servicios y propiedades

Otros servicios y propiedades del CP

- **Configuración IP**
  - Tipos de dirección

    El CP soporta direcciones IP según IPv4 e IPv6.
  - Direccionamiento

    La dirección IP, la máscara de subred y la dirección de una transición de red pueden ajustarse manualmente en la configuración. La dirección IP también se puede obtener a través de bloques de programa.
  - DHCP: La dirección IP también se puede obtener de un servidor DHCP.
  - Se soporta DCP (Discovery and Configuration Protocol).

- **Sincronización horaria**
  - NTP

    El CP puede sincronizar su hora a través de NTP en la interfaz Ethernet.
  - Solo CP 1542SP-1 IRC

    Si la comunicación por Telecontrol está activa, el CP obtiene su hora local del interlocutor en forma de hora UTC. La CPU puede leer la hora del CP a través de una variable PLC. Consulte el formato de los sellos de tiempo de los telegramas de datos en el capítulo Tipos de puntos de datos (Página 60).

    Con la comunicación Telecontrol desactivada, el CP puede sincronizar su hora a través de NTP.
  - Solo CP 1543SP-1

    Con las funciones Security activadas puede utilizarse el procedimiento seguro NTP (secure).

  Encontrará más información en el capítulo Sincronización horaria (Página 43).
- **SNMP**

  Como agente SNMP, el CP soporta consultas sobre SNMPv1.

  El CP 1543SP-1 soporta además SNMPv3.

  Encontrará más información en el capítulo SNMP (Página 45).

1.6 Funciones Security (CP 1542SP-1 IRC, CP 1543SP-1)

Las funciones Security descritas a continuación se activan para cada CP en la configuración.

Respecto a las funciones Security de la Open User Communication consulte el capítulo Programación (OUC) (Página 97).

Nota

Recomendación para instalaciones de seguridad crítica

Observe las indicaciones del capítulo Recomendaciones Security (Página 39).

Funciones Security del CP 1542SP-1 IRC

- **Correo electrónico**

  Para la transmisión segura de información mediante mensajes de correo electrónico encriptados se puede utilizar alternativamente:
  - SSL/TLS
  - STARTTLS

  Consulte la configuración en el capítulo Security > Configuración de correo electrónico (Página 87).

- **Certificados**

  Para la autenticación segura de los interlocutores se utilizan certificados.

- **Comunicación segura por Telecontrol**

  Los protocolos de Telecontrol ofrecen las siguientes funciones Security:

  – TeleControl Basic

    Como función Security integrada, el protocolo de Telecontrol cifra los datos en la transmisión entre el CP y el servidor de Telecontrol. El intervalo de intercambio de claves entre el CP y el servidor de Telecontrol está configurado en 1 hora.

    La contraseña de Telecontrol posibilita la autenticación del CP en el servidor de Telecontrol.

  – DNP3

    El CP soporta los mecanismos recogidos en la especificación Security.

Funciones Securitydel CP 1543SP-1

Industrial Ethernet Security permite proteger diferentes dispositivos, células de automatización o segmentos de una red Ethernet. Combinando diferentes medidas de seguridad es posible proteger la transferencia de datos a través del CP 1543SP-1 de los ataques siguientes:

- Espionaje de datos
- Manipulación de datos
- Accesos no autorizados

El uso de interfaces Ethernet/PROFINET adicionales de la CPU permite utilizar redes subordinadas seguras.

Con el uso del CP como módulo de seguridad se hacen accesibles para la estación ET 200SP las siguientes funciones Security en la interfaz hacia la red Ethernet:

- **Cortafuegos**

  El cortafuegos protege el dispositivo mediante:

  – Cortafuegos IP con Stateful Packet Inspection (capa 3 y 4)

  – Cortafuegos también para tramas Ethernet "No IP" conforme a IEEE 802.3 (capa 2)

  – Restricción de la velocidad de transferencia ("Limitación del ancho de banda")

- **Certificados**

  Para la autenticación segura de los interlocutores se utilizan certificados.

- **Comunicación protegida por túnel IPsec (VPN)**

  La comunicación por túnel VPN permite establecer túneles IPsec seguros para la comunicación con uno o varios módulos de seguridad. El CP puede agruparse en VPN con otros módulos mediante configuración. Entre todos los módulos de seguridad de un grupo VPN se establecen túneles IPsec (VPN).

- **Registro**

  Para fines de vigilancia es posible guardar eventos en archivos de registro que se leen utilizando la herramienta de configuración o se envían automáticamente a un servidor Syslog.

- **NTP (secure)**

  Para la transmisión segura en la sincronización horaria

- **SNMPv3**

  Para la transferencia antiescucha de información de análisis de la red.

Encontrará información sobre la configuración de funciones de seguridad en el capítulo Configuración de seguridad (CP 1543SP-1) (Página 88).

Puede encontrar más información sobre la funcionalidad y la configuración de las funciones de seguridad en el sistema de información de STEP 7 y en el manual /4/ (Página 124).

1.7 Capacidad funcional y prestaciones

Número de CPs por estación

Por cada estación ET 200SP pueden insertarse y configurarse hasta tres módulos especiales, de los cuales como máximo dos pueden ser CP 154xSP-1.

Para conocer más detalles sobre los módulos especiales permitidos y las reglas de slots consulte el capítulo Montar el CP (Página 32).

Recursos de conexión

Número total de conexiones vía Industrial Ethernet máximo 32,
de las cuales:

- S7: máx. 16
- TCP/IP: máx. 32
- ISO-on-TCP: máx. 32
- UDP: máx. 32

Adicionalmente:

- Conexiones online de la estación de ingeniería (STEP 7): Máx. 2
- Conexiones TCP para HTTP

  Para accesos HTTP hay disponibles hasta 12 recursos de conexión TCP utilizados por uno o más navegadores web para mostrar datos del CP.

- Conexiones PG/OP (HMI): máximo 16 en total,
  de las cuales:
  - recursos para conexiones PG: máx. 16
  - recursos para conexiones OP: máx. 16

Memoria de telegramas (búfer de transmisión)

Solo CP 1542SP-1 IRC

El CP dispone de una memoria de telegramas (búfer de transmisión) para los valores de puntos de datos configurados como eventos.

El volumen del búfer de transmisión se distribuye por igual entre todos los interlocutores configurados.

El tamaño del búfer de transmisión puede ajustarse en STEP 7, consulte el capítulo Comunicación con la CPU (Página 57).

El tamaño máximo del búfer de transmisión depende del protocolo de telecontrol utilizado y comprende:

- TeleControl Basic

  64000 eventos
- DNP3

  100000 eventos
- IEC 60870-5-104

  100000 eventos

Encontrará detalles sobre la función del búfer de transmisión, como el almacenamiento y la transmisión de eventos, y sobre las posibilidades de transferencia de datos en el capítulo Memoria imagen de proceso, tipo de transferencia, clases de eventos, disparos (Página 65).

Correo electrónico (a través del editor de mensajes)

Solo CP 1542SP-1 IRC

Con la comunicación Telecontrol activada, en STEP 7 se pueden configurar hasta 10 mensajes. Los mensajes se envían en forma de correos electrónicos.

Conexiones de Telecontrol y puntos de datos

Solo CP 1542SP-1 IRC

- **Conexiones Telecontrol**
  - TeleControl Basic

    Puede establecerse una conexión con un servidor de Telecontrol estructurado como sencillo o como redundante.
  - DNP3

    Se pueden establecer conexiones con hasta cuatro maestros.
  - IEC 60870-5-104

    Se pueden establecer conexiones con hasta cuatro maestros.
- **Puntos de datos**

  Los datos que deben transferirse desde el CP se asignan a diferentes puntos de datos en la configuración de STEP 7. El tamaño de los datos útiles para cada punto de datos

depende del tipo de datos del punto de datos correspondiente. Encontrará más detalles en el capítulo Tipos de puntos de datos (Página 60).

El número máximo de puntos de datos configurables es 500.

En la asignación de la memoria interna del CP para puntos de datos también se incluye la longitud del nombre del punto de datos. Tenga en cuenta al respecto la indicación del capítulo Configuración de los puntos de datos (Página 59).

Funciones Security

Solo CP 1543SP-1

- **Túnel VPN**

  Pueden establecerse como máximo cuatro túneles VPN para la comunicación segura con otros módulos Security.

- **Reglas de cortafuegos**

  El número máximo de reglas de cortafuegos en el modo de cortafuegos avanzado está limitado a 256. Las reglas de cortafuegos se dividen de la siguiente forma:

  – Máximo de 226 reglas con direcciones individuales

  – Máximo de 30 reglas con áreas de direccionamiento o direcciones de red (p. ej., 140.90.120.1 - 140.90.120.20 o bien 140.90.120.0/16)

  – Máximo de 128 reglas con restricción de la velocidad de transferencia ("Limitación del ancho de banda")

1.8 Requisitos de aplicación

1.8.1 Requisitos de hardware

BusAdapter

Para la conexión a la red Ethernet el CP necesita un BusAdapter. El BusAdapter no está incluido en el volumen de suministro del CP.

El CP soporta los siguientes BusAdapter:

- BA 2xRJ45
- BA 2xFC
- BA 2xSCRJ
- BA SCRJ/RJ45
- BA SCRJ/FC

Consulte los detalles de los BusAdapter en el capítuloBusAdapter (Página 121) y en el manual /2/ (Página 123).

CPU y otros componentes del ET 200SP

El CP soporta el servicio en estaciones que contienen una de las siguientes CPUs:

- CPU 1510SP-1 PN

  Referencia: 6ES7510-1DJ01-0AB0
- CPU 1510SP F-1 PN

  Referencia: 6ES7510-1SJ01-0AB0
- CPU 1512SP-1 PN

  Referencia: 6ES7512-1DK01-0AB0
- CPU 1512SP F-1 PN

  Referencia: 6ES7512-1SK01-0AB0

Aquí no se describen otros componentes y módulos necesarios para el montaje de la estación ET 200SP, como rieles, módulos de periferia o el cableado. Consulte a ese respecto /2/ (Página 123).

Componentes de los interlocutores

Aquí no se describen los componentes que requieren los interlocutores del CP 1542SP-1 IRC. Encontrará las referencias a la documentación de otros productos (p. ej. TCSB) en la bibliografía incluida en el anexo del manual.

1.8.2 Requisitos de software

Software de configuración

Para la configuración del CP es preciso utilizar la siguiente herramienta de configuración:

- STEP 7 Professional a partir de la versión 14

Software para funciones online

Para el uso de las funciones online se requiere el siguiente software:

- STEP 7 en la versión indicada anteriormente

Firmware de la CPU

Para el uso del CP se requiere una CPU 151xSP con una versión de firmware ≥ V2.0.

Protocolos de telecontrol (CP 1542SP-1 IRC)

Encontrará las versiones de los protocolos de telecontrol soportadas por el CP en el capítulo Comunicación Telecontrol del CP 1542SP-1 IRC (Página 13).

1.9 Ejemplos de configuración

A continuación encontrará los ejemplos de configuración para el uso de las tres variantes de CP.

Separación de red CP 1542SP-1 -

En el ET 200SP el CP se utiliza para utilizar redes subordinadas por separado o bien para conseguir separar la red de nivel superior.

El ET 200SP puede ampliarse con flexibilidad con interfaces Ethernet adicionales mediante el CP. Gracias a la separación de redes es posible montar máquinas idénticas con la misma dirección IP. El CP se encarga de la comunicación y descarga la CPU.

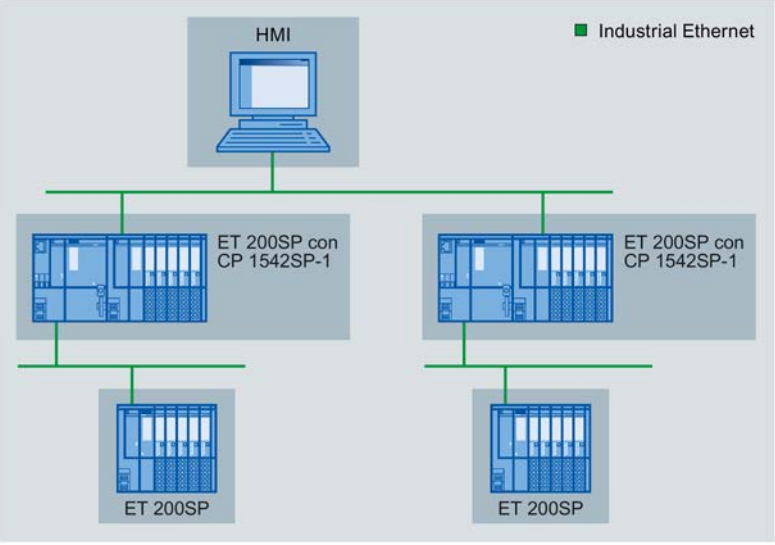


Figura 1-1 Ejemplo de configuración de un ET 200SP con CP 1542SP-1

Protección de células del CP 1543SP-1 - mediante funciones Security

El CP se comunica de forma codificada con los interlocutores de la red conectada. El cortafuegos vigila el acceso al ET 200SP, protegiendo con ello las redes subordinadas. Con ello se evita pérdida de datos, fallos en la producción y daños en las máquinas.

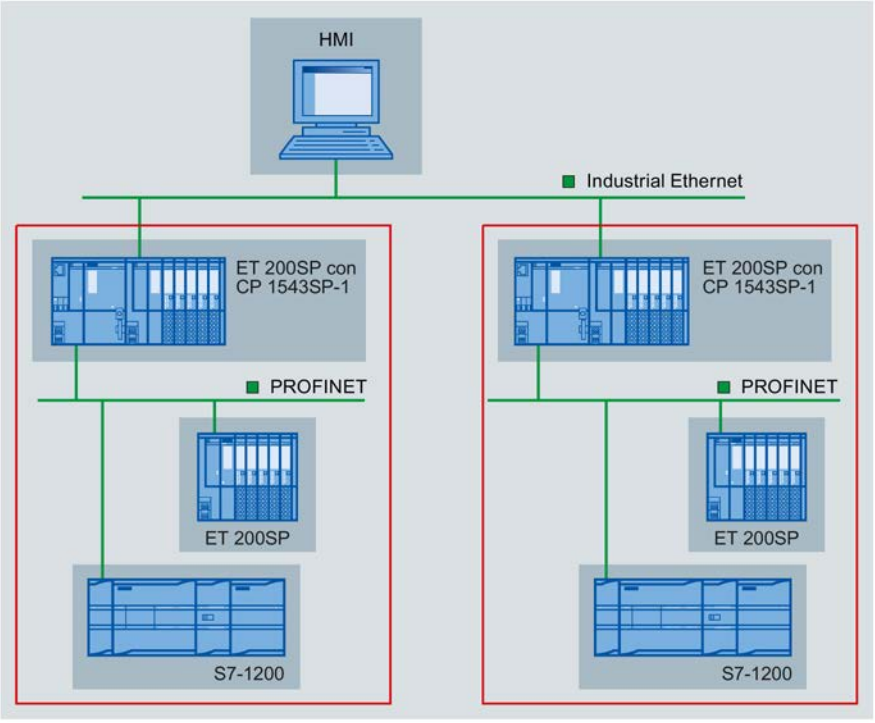


Figura 1-2 Ejemplo de configuración de un ET 200SP con CP 1543SP-1

Conexión CP 1542SP-1 IRC - a centrales de control

El uso del CP permite utilizar el ET 200SP como Remote Terminal Unit. Para la comunicación se pueden utilizar los siguientes protocolos de Telecontrol:

- TeleControl Basic

  El protocolo de telecontrol de Siemens para la integración en centrales con TCSB
- IEC 60870-5-104
- DNP3

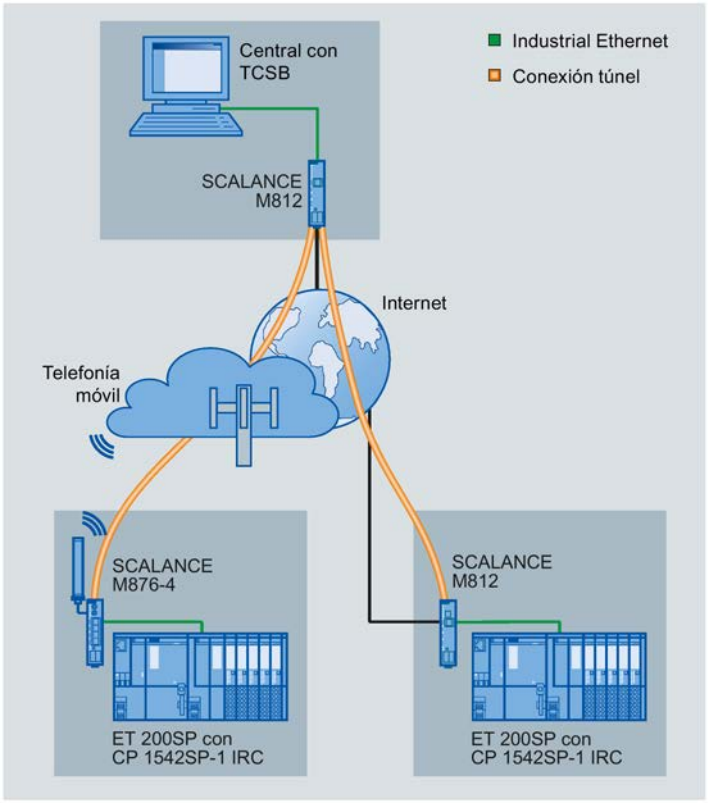


Figura 1-3 Ejemplo de configuración de un ET 200SP con CP 1542SP-1 IRC; protocolo: TeleControl Basic

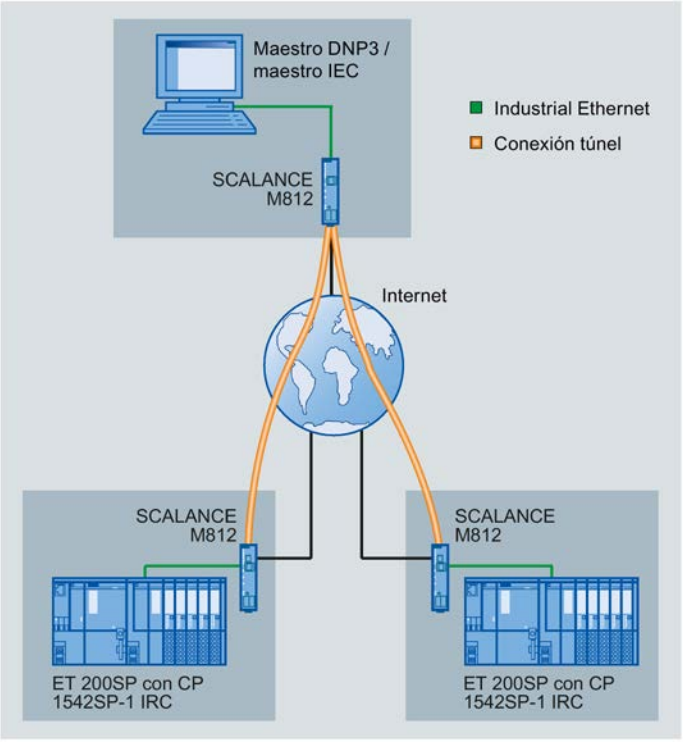


Figura 1-4 Ejemplo de configuración de un ET 200SP con CP 1542SP-1 IRC; protocolo: DNP3 o IEC 60870-5-104

LEDs y conexiones

2

2.1 LEDs

Significado de los indicadores LED del CP

El CP cuenta con los siguientes diodos luminosos (LEDs) en la cara frontal:

Nombre del LED	Significado
PWR	Alimentación
RN	Estado operativo
ER	Errores
MT	Mantenimiento

Tabla 2- 1 Leyenda de las tablas siguientes

Símbolo				-
Significado / Estado del LED	ON (LED encendido)	OFF	LED intermitente	Cualquiera

Tabla 2- 2 Significado de los indicadores LED del CP

PWR (verde)	RN (verde)	ER (rojo)	MT (amarillo)	Significado
○	○	○	○	Tensión de alimentación nula o insuficiente en el CP
●	●	●	●	Arranque del CP
●	●	○	○	CP en estado operativo RUN
●	-	✳	○	Error. Estado de los LEDs con los siguientes eventos: • Dirección IP duplicada • BusAdapter no insertado o extraído • Sin conexión Telecontrol (CP 1542SP-1 IRC)
●	✳	✳	✳	Error: CP defectuoso
●	✳	○	○	Faltan datos de configuración
●	●	○	✳	Actualización de firmware en curso.
●	●	○	●	Hay una solicitud de mantenimiento del CP activa. Ejemplo: • Fin de la actualización del firmware

LEDs del BusAdapter

Cada uno de los puertos de un BusAdapter dispone de un LED "LKx", que informa del estado de conexión con Ethernet y del tráfico de telegramas del puerto.

Tabla 2- 3 Significado de los indicadores LED de los BusAdapter

LK (verde)	Significado
○	Sin conexión Ethernet. Causas posibles: • Sin conexión física con la red • Puerto desactivado en la configuración
☼	Test de intermitencia de LEDs
●	Existe conexión Ethernet entre puerto e interlocutor.

2.2 Alimentación

Alimentación externa requerida

La conexión para la alimentación externa de 24 V DC se encuentra en la cara frontal del CP.

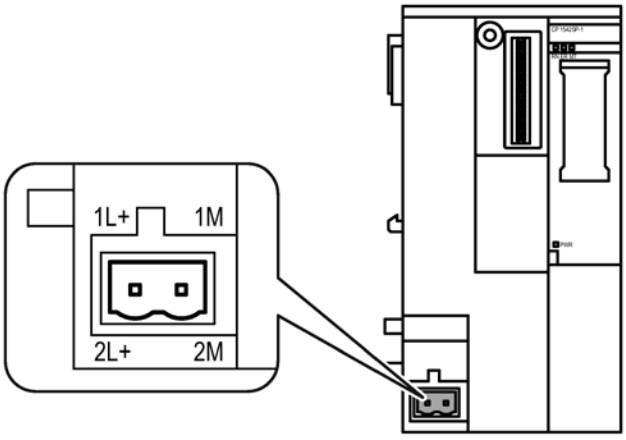


Figura 2-1 Alimentación del CP

Se ha previsto una conexión X80 para la conexión a una alimentación sencilla o redundante. La alimentación se conecta al bloque de terminales insertable suministrado con el CP. El bloque de terminales se enchufa en el conector hembra X80 del CP.

Encontrará información sobre el montaje y la conexión en los capítulos Montar el CP (Página 32) y Conexión del CP (Página 36).

Protección contra inversión de polaridad

El bloque de terminales enchufable para la conexión X80 está diseñado de tal modo que solo se puede enchufar en una posición. Este diseño proporciona protección contra la inversión de polaridad.

La conexión X80 posee además una protección electrónica contra la inversión de polaridad.

Encontrará más datos sobre la alimentación en el capítulo Datos técnicos (Página 111)

2.3 Conexión para el BusAdapter

Funcionamiento del dispositivo solo con BusAdapter

Para la conexión a Ethernet el CP necesita un BusAdapter. El BusAdapter no está incluido en el volumen de suministro del CP.

El slot se encuentra en la cara frontal del dispositivo.

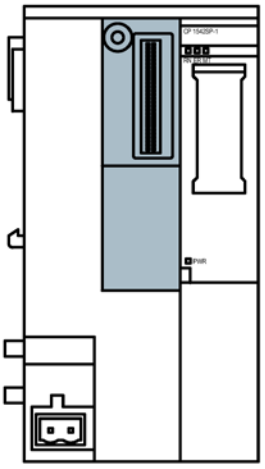


Figura 2-2 Cara frontal del CP, el slot del BusAdapter está identificado en gris.

Encontrará los BusAdapter soportados por el CP en el capítulo BusAdapter (Página 121).

Encontrará información sobre el montaje y la conexión en los capítulos Montar el CP (Página 32) y Conexión del CP (Página 36).

Encontrará la asignación de la interfaz Ethernet en el capítulo Asignación de la interfaz Ethernet de los BusAdapter (Página 122). Encontrará los datos técnicos de los BusAdapter en el manual /2/ (Página 123).

Montaje y conexión

3

3.1 Indicaciones importantes sobre el uso del dispositivo

Consignas de seguridad para el uso del equipo

Tenga en cuenta las siguientes consignas de seguridad para la instalación y el uso del equipo y para todos los trabajos relacionados, como el montaje y la conexión del equipo o la sustitución de este.

Protección contra sobretensiones

ATENCIÓN
Protección de la alimentación externa Cuando el módulo o la estación se alimentan por redes o cables de alimentación de gran extensión, se pueden producir acoplamientos de pulsos electromagnéticos fuertes en los cables de alimentación, p. ej., provocados por rayos o la conexión de grandes cargas. La conexión de la alimentación externa no está protegida contra pulsos electromagnéticos fuertes. Para ello es necesario un módulo de protección contra sobretensiones externo. Los requisitos de la norma EN61000-4-5, "Surge - Comprobación de cables de alimentación eléctrica" solo se cumplen si se utiliza un elemento de protección adecuado. Se puede utilizar el Dehn Blitzductor BVT AVD 24, referencia 918 422 o un elemento protector de las mismas características. Fabricante: DEHN+SÖHNE GmbH+Co.KG, Hans Dehn Str.1, Postfach 1640, D-92306 Neumarkt

3.1.1 Indicaciones sobre el uso en la zona Ex

⚠ ADVERTENCIA
RIESGO DE EXPLOSIÓN NO ABRA EL APARATO ESTANDO CONECTADA LA TENSIÓN DE ALIMENTACIÓN.

⚠ ADVERTENCIA
El aparato solo debe utilizarse en entornos con clase de contaminación 1 o 2 (véase IEC60664-1).

⚠ADVERTENCIA

El equipo se ha concebido para trabajar con una baja tensión de seguridad (Safety Extra Low Voltage, SELV) directamente conectable, suministrada por una fuente de alimentación de potencia limitada (Limited Power Source, LPS).

Por esta razón se deben conectar sólo bajas tensiones de seguridad (SELV) de potencia limitada (Limited Power Source, LPS) según IEC 60950-1 / EN 60950-1 / VDE 0805-1 a las tomas de alimentación, o bien la fuente de alimentación del equipo tiene que ser conforme a NEC Class 2 según el National Electrical Code (r) (ANSI / NFPA 70).

Si el equipo se conecta a una alimentación redundante (dos fuentes de alimentación independientes), ambas fuentes han de cumplir los requisitos citados.

⚠ADVERTENCIA

RIESGO DE EXPLOSIÓN

En un entorno inflamable o combustible no se deben conectar cables al dispositivo ni se deben desenchufar del mismo.

⚠ADVERTENCIA

RIESGO DE EXPLOSIÓN

La sustitución de componentes puede repercutir negativamente en la compatibilidad con Class I, Division 2 o Zone 2.

⚠ADVERTENCIA

Para el uso en atmósferas potencialmente explosivas según Class I, Division 2 o Class I, Zone 2, el dispositivo se tiene que montar en un armario de distribución o en una carcasa.

⚠ADVERTENCIA

Perfil DIN simétrico

En el campo de aplicación de ATEX e IECEx solo está permitido montar los módulos con el perfil DIN simétrico de Siemens 6ES5 710-8MA11.

3.1.2 Indicaciones sobre el uso en zona Ex según ATEX / IECEx

⚠ ADVERTENCIA

Requisitos exigidos al armario de distribución

Para cumplir la directiva de la Unión Europea 94/9 (ATEX 95), la carcasa o el armario de distribución ha de satisfacer como mínimo los requisitos de IP54 según EN 60529.

⚠ ADVERTENCIA

Si se presentan temperaturas superiores a 70 °C en el cable o en el conector de la caja, o si la temperatura en los puntos de bifurcación de los conductores de los cables es superior a 80 °C, se han de tomar precauciones especiales. Si el equipo se utiliza a temperaturas ambiente superiores a 50 °C, se tienen que utilizar cables con una temperatura de servicio admisible de como mínimo 80 °C.

⚠ ADVERTENCIA

Tome las medidas necesarias para evitar sobretensiones transitorias que superen en más del 40% la tensión nominal. Esto está garantizado si los dispositivos trabajan solo con baja tensión de seguridad (SELV).

3.1.3 Indicaciones sobre el uso en zona Ex según UL HazLoc

⚠ ADVERTENCIA

RIESGO DE EXPLOSIÓN

No desconecte el dispositivo de los cables conductores de tensión hasta estar seguro de que la atmósfera no tiene peligro de explosión.

Este dispositivo solo es apto para el uso en áreas según Class I, Division 2, Groups A, B, C y D y en áreas sin peligro de explosión.

Este dispositivo solo es apto para el uso en áreas según Class I, Zone 2, Group IIC y en áreas sin peligro de explosión.

3.1.4 Notas para el uso en zona con peligro de explosión según FM

⚠ ADVERTENCIA
RIESGO DE EXPLOSIÓN
Solo está permitido desconectar o conectar cables con tensión eléctrica si la fuente de alimentación está desconectada y el aparato se encuentra en una zona donde no haya concentraciones de gases inflamables.

Este dispositivo solo es apto para el uso en áreas según Class I, Division 2, Groups A, B, C y D y en áreas sin peligro de explosión.

Este dispositivo solo es apto para el uso en áreas según Class I, Zone 2, Group IIC y en áreas sin peligro de explosión.

⚠ ADVERTENCIA
RIESGO DE EXPLOSIÓN
The equipment is intended to be installed within an ultimate enclosure. The inner service temperature of the enclosure corresponds to the ambient temperature of the module. Use installation wiring connections with admitted maximum operating temperature of at least 30 ºC higher than maximum ambient temperature.

3.2 Montar el CP

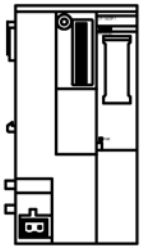
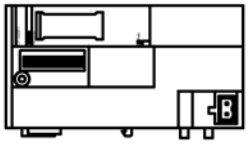
ATENCIÓN
Realizar el montaje y desmontaje del CP siempre en estado libre de tensión
Desconecte la alimentación del ET 200SP y del CP antes de montar o desmontar los módulos. El montaje o desmontaje con la alimentación conectada puede dañar los módulos y provocar una pérdida de datos.

Nota

Observar las directivas de instalación

Para el montaje y la conexión del CP tenga en cuenta las explicaciones del manual /2/ (Página 123).

ATENCIÓN
Posición de montaje - Dependencia del rango de temperatura El montaje debe realizarse de manera que las rejillas de ventilación superiores e inferiores de los módulos no queden cubiertas, garantizando así una buena ventilación. Por encima y por debajo de los módulos debe haber un espacio de 25 mm para la circulación de aire, lo que sirve como protección frente al sobrecalentamiento. Tenga en cuenta la dependencia del rango de temperatura permitido en relación a la posición de montaje. • El montaje horizontal del rack (perfil DIN simétrico) implica la posición vertical del CP. • El montaje vertical del rack (perfil DIN simétrico) implica la posición horizontal del CP. Encontrará los rangos de temperatura admisibles en el capítulo Datos técnicos (Página 111).

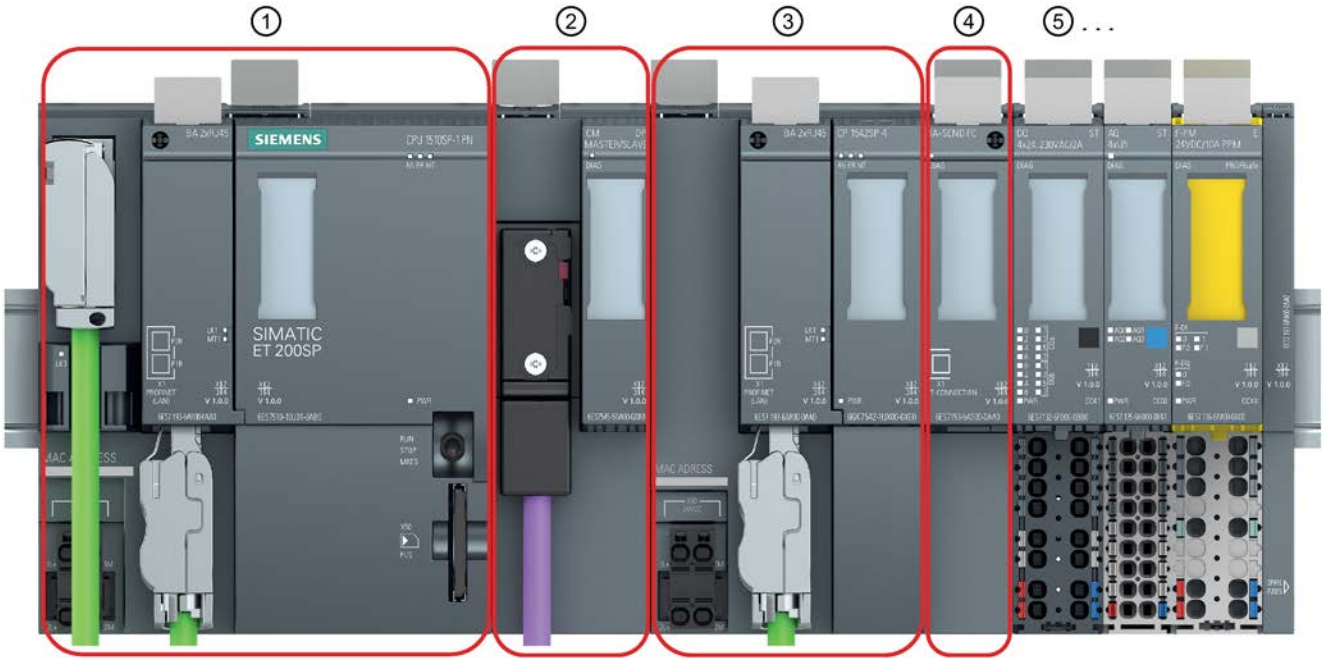
Montaje del rack	Posición de montaje del CP
Montaje horizontal del rack	
Montaje vertical del rack	

Reglas de asignación de slots

La CPU siempre ocupa el slot 1. En un ET 200SP se pueden insertar en los slots 2 a 4 (consulte la figura) hasta tres de los siguientes módulos a la derecha de la CPU:

- CMs
- CPs
- BusAdapter Send

De estos tres módulos pueden insertarse hasta dos CP 154xSP-1. Estos dos CPs pueden ser del mismo tipo o diferentes.



① Slot 1: solo permitido para la CPU.

② Slot 2: para CM / CP / BusAdapter Send *****
Si utiliza un CM PROFIBUS, tiene que insertarlo inmediatamente al lado de la CPU en el slot 1.

③ Slot 3: para CM / CP / BusAdapter Send *****

④ Slot 4: para CM / CP / BusAdapter Send *****

⑤ Slot 5 y siguientes: para periferia

***** Si utiliza un BusAdapter Send, este debe insertarse en el slot inmediatamente junto a los módulos de periferia.

Figura 3-1 Slots del ET 200SP

Montaje en perfil DIN simétrico

Nota

Fijación de los módulos asegurados contra deslizamiento en el perfil DIN simétrico

Si monta los módulos en un área sometida a carga mecánica, utilice mecanismos de sujeción adecuados para asegurar los módulos sobre el perfil DIN simétrico a ambos extremos del grupo de dispositivos, como p. ej. un soporte extremo de Siemens 8WA1808.

Los soportes extremos impiden que los módulos se deslicen y se separen entre sí en caso de carga mecánica.

Para uso en áreas clasificadas ATEX o IECEx, lea las indicaciones relativas al perfil DIN simétrico en el capítulo Indicaciones sobre el uso en la zona Ex (Página 29).

El sistema ET 200SP es adecuado para el montaje en un perfil DIN simétrico conforme a EN 60715 (35 × 7,5 mm o 35 × 15 mm)

1. Enganche la CPU o el módulo de interfaz en el perfil DIN simétrico.
2. Incline la CPU o el módulo de interfaz hacia atrás hasta que el desbloqueo del perfil encastre de forma audible.
3. Enganche el CP a la derecha de la CPU.
4. Incline el CP hacia atrás hasta que el desbloqueo del perfil encastre de forma audible.
5. Desplace el CP hacia la izquierda hasta que encastre de forma audible en la CPU.
6. Monte las BaseUnits y los módulos restantes de la forma correspondiente.

   Consulte al respecto el manual /2/ (Página 123).

Inserción del BusAdapter

ATENCIÓN
Contacto con los contactos enchufables
No toque los contactos enchufables si no hay ningún BusAdapter insertado.

1. Conecte el cable correspondiente al BusAdapter si utiliza un BusAdapter con conexión óptica o eléctrica directa (sin conector).
2. Inserte el BusAdapter en el slot del CP.

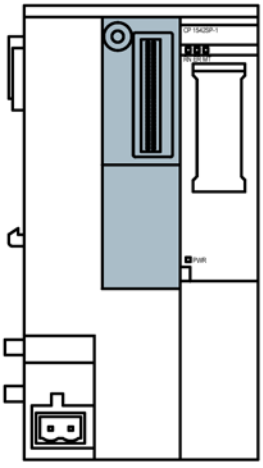


Figura 3-2 Cara frontal del CP, la ranura del BusAdapter está identificada en gris.

3. Atornille el BusAdapter al CP.

   El tornillo de sujeción se encuentra en la parte superior izquierda de la cara frontal del BusAdapter.

   Utilice para ello un destornillador con un ancho de hoja de entre 3 y 3,5 mm o un destornillador Torx adecuado (T15).

   El par de apriete máximo es de 0,25 Nm.

4. Enchufe el conector del cable de conexión en el conector hembra del BusAdapter si utiliza un BusAdapter con conector.

Respecto a la conexión de los BusAdapter y a la confección de cables consulte el manual /2/ (Página 123).

Desmontaje del perfil DIN simétrico

Realice los pasos siguientes para desmontar un CP del perfil DIN simétrico:

1. Desconecte la alimentación de toda la estación, incluido el CP y la CPU.
2. Accione el desbloqueo del perfil DIN simétrico de los módulos que deben desplazarse (CPU, CPs) y desplácelos paralelos a la izquierda hasta que se suelten del resto del grupo de montaje (espacio libre aprox. 16 mm).

   Presione el deslizador de bloqueo identificado con "PUSH" situado en la parte superior de un módulo hacia abajo para poder mover el módulo en cuestión sobre el perfil.
3. Presione el desbloqueo del perfil DIN por el CP y desplácelo hacia la derecha hasta que se suelte de la CPU (espacio libre aprox. 8 mm).
4. Con el desbloqueo del perfil DIN presionado, incline el CP para extraerlo del perfil.

3.3 Conexión del CP

Secuencia de las operaciones

ATENCIÓN
Conexión solo cuando no exista tensión eléctrica
Conecte el CP siempre en estado libre de tensión Tenga en cuenta las indicaciones del manual de sistema, consulte /2/ (Página 123)

El BusAdapter ya está conectado al cable en cuestión, consulte el capítulo Montar el CP (Página 32).

1. Conecte la alimentación externa en el bloque de terminales de la conexión X80.

   Utilice la misma alimentación que la CPU.
2. No conecte la alimentación de tensión hasta que el CP esté completamente cableado y conectado.

Alimentación en la conexión X80

La posición de la conexión X80 para la alimentación del CP se indica en el capítulo Alimentación (Página 26). Allí encontrará también indicaciones relativas a la protección contra la inversión de polaridad.

El bloque de terminales enchufable de 2 polos para el conector hembra X80 tiene la asignación siguiente:

Terminal	Asignación
1L+ / 2L+	24 V DC
1M / 2M	Masa

Los dos terminales 1L+/L2+ y 1M/2M del bloque de terminales están puenteados respectivamente de forma interna, lo que permite conectar una alimentación sencilla o redundante.

Secciones de cable conectables:

- Sin puntera: 0,2 .. 2,5 mm^2 / AWG 24 .. 13
- Con puntera: 0,25 .. 1,5 mm^2 / AWG 24 .. 16
- Con puntera TWIN: 0,5 .. 1,0 mm^2 / AWG 20 .. 17

Encontrará indicaciones sobre la potencia consumida y otros datos técnicos de las conexiones en el capítulo Datos técnicos (Página 111).

Configuración y servicio

4

4.1 Recomendaciones Security

Observe las siguientes recomendaciones sobre Security para impedir accesos no autorizados al sistema.

Nota

Funciones Securityde los tipos de CP

Las indicaciones que siguen, dependiendo de la función soportada, no son válidas para todos los tipos de CP descritos en el presente manual.

General

- Compruebe regularmente si el equipo cumple las presentes recomendaciones y otras directivas internas de Security.
- Realice una evaluación integral de la seguridad de su instalación. Utilice un sistema de protección de celdas con los productos correspondientes.
- No conecte el equipo directamente a Internet. Utilice el equipo dentro de un área de red protegida.
- Mantenga actualizado el firmware. Infórmese periódicamente sobre las actualizaciones de seguridad del firmware y aplíquelas.
- Infórmese periódicamente sobre las novedades en las páginas web de Siemens.
  - Aquí encontrará información acerca de la seguridad de la red:

    Enlace: (http://www.siemens.com/industrialsecurity)
  - Aquí encontrará información acerca de Industrial Ethernet Security:

    Enlace: (http://w3.siemens.com/mcms/industrial-communication/es/ie/industrial-ethernet-security/Seiten/industrial-security.aspx)
  - Encontrará una introducción al tema Industrial Security en el impreso siguiente:

    Enlace: (http://w3app.siemens.com/mcms/infocenter/dokumentencenter/sc/ic/InfocenterLanguagePacks/Netzwerksicherheit/6ZB5530-1AP02-0BA4_BR_Network_Security_en_112015.pdf)

Acceso físico

Limite el acceso físico al equipo al personal cualificado.

Conexión de red

No conecte el CP directamente a Internet. Si desea conectar el CP a Internet, conecte los dispositivos de protección adecuados delante del CP, p. ej. un SCALANCE S con cortafuegos, o utilice el CP 1543SP-1.

Funciones de seguridad del producto

Aproveche las posibilidades de los ajustes de seguridad en la configuración del producto. Incluyen, entre otros:

- Niveles de protección

  Configure un nivel de protección para la CPU.

  Encontrará información al respecto en el sistema de información de STEP 7.

- Desactivación de puertos de BusAdapter

  Desactive en la configuración los puertos del BusAdapter utilizado que no sean necesarios.

- Función de Security de la comunicación
  - Active las funciones de Security del CP y configure el cortafuegos.

    En caso de conexión a redes públicas conviene utilizar el cortafuegos. Piense con qué servicios desea permitir el acceso a la estación a través de redes públicas. Con la "Limitación del ancho de banda" del cortafuegos puede restringir la posibilidad de ataques de flood y DoS.
  - Utilice las variantes de protocolo seguras NTP (secure) y SNMPv3.
  - Utilice las funciones Security de los protocolos Telecontrol, como por ejemplo las opciones Security de DNP3.
  - Utilice la Open User Communication segura (Secure OUC) mediante los bloques de programa correspondientes.
  - Deje el acceso al servidor web de la CPU (configuración de la CPU) y al servidor web del CP desactivado.

- Protección de las contraseñas para el acceso a bloques de programa

  Proteja las contraseñas que se guardan en bloques de datos para los bloques de programa, evitando que puedan verse. Encontrará indicaciones sobre el procedimiento en el sistema de información de STEP 7, en el título "Protección de know-how".

- Función de registro

  Active la función desde la configuración de Security y compruebe regularmente que no se hayan producido accesos no autorizados a los eventos registrados.

Contraseñas

- Defina reglas para la utilización de los equipos y la asignación de contraseñas.
- Para aumentar la seguridad, actualice regularmente las contraseñas.
- Utilice exclusivamente contraseñas de alto grado de seguridad. Evite utilizar contraseñas débiles, p. ej., "contraseña1", "123456789" o similares.

- Asegúrese de que todas las contraseñas están protegidas y no permiten el acceso de personal no autorizado.

  Consulte a este respecto también el apartado anterior.
- No utilice una misma contraseña para diversos usuarios y sistemas.

Protocolos

Protocolos seguros y no seguros

- Active únicamente los protocolos que necesite para utilizar el sistema.
- Si el acceso al equipo no está protegido por medidas de protección físicas, utilice protocolos seguros.

  El protocolo NTP ofrece una alternativa segura con NTP (secure).

Tabla: Significado de los títulos de columna y las entradas

La tabla siguiente le ofrece una panorámica de los puertos abiertos de este equipo.

- **Protocolo/función**

  Protocolos que soporta el equipo.
- **Número de puerto (protocolo)**

  Número de puerto asignado al protocolo.
- **Ajuste predeterminado del puerto**
  - Abierto

    El puerto está abierto al empezar la configuración.
  - Cerrado

    El puerto está cerrado al empezar la configuración.
- **Estado del puerto**
  - Abierto

    El puerto está siempre abierto y no puede cerrarse.
  - Abierto tras configuración

    El puerto está abierto si se ha configurado.
  - Abierto (inicio de sesión si está configurado)

    El puerto está abierto de forma predeterminada. Una vez configurado el puerto, el interlocutor debe iniciar sesión.
  - Cerrado tras configuración

    El puerto está cerrado, dado que el CP siempre es cliente para este servicio.
- **Autenticación**

  Indica si el protocolo autentica el interlocutor durante el acceso.

Protocolo / función	Número de puerto (protocolo)	Ajuste predeterminado del puerto	Estado del puerto	Autenticación
DHCP	68 (UDP)	Cerrado	Abierto tras configuración (mientras el CP recibe una nueva dirección)	No
Conexiones S7 y online	102 (TCP)	Abierto	Abierto tras configuración	No
Diagnóstico online (CP 1543SP-1)	8448 (TCP)	Cerrado	Abierto tras configuración	No
Puerto Listener **DNP3**	20000 (TCP/UDP) ajustable	Cerrado	Abierto tras configuración	Sí, si Security está activado.
Puerto Listener IEC	2404 (TCP) ajustable	Cerrado	Abierto tras configuración	No
SMTP	25 (TCP) ajustable	Cerrado	Cerrado tras configuración	No
SSL/TLS	587 (TCP) ajustable	Cerrado	Cerrado tras configuración	No
NTP	123 (TCP)	Cerrado	Cerrado tras configuración	No
HTTP	80 (TCP)	Cerrado	Abierto tras configuración	Sí
HTTPS	443 (TCP)	Cerrado	Abierto tras configuración	Sí
SNMP	161 (UDP)	Abierto	Abierto tras configuración	Sí (con SNMPv3)

4.2 Configuración en STEP 7

Configuración en STEP 7

La configuración de los módulos y las redes se realiza en SIMATIC STEP 7. La versión necesaria se menciona en el capítulo Requisitos de software (Página 20). Para un ET 200SP se pueden configurar como máximo dos CP 154xSP-1.

Encontrará información amplia sobre la configuración en el sistema de información de STEP 7 y en los siguientes capítulos.

Sinopsis de la configuración del CP

Para realizar la configuración proceda del siguiente modo:

1. Cree un proyecto de STEP 7.
2. Inserte las estaciones SIMATIC necesarias.
3. Inserte los CPs y los módulos de entrada y salida necesarios en las estaciones.
4. Cree una red Ethernet.

5. Conecte las estaciones con la subred Ethernet.
6. Configure los CPs insertados.
7. Opcional: Cree los bloques de programa para la Open User Communication.
8. Guarde y compile el proyecto.

En los capítulos siguientes encontrará información sobre los diferentes grupos de parámetros. La información sobre los parámetros que no se describen en este manual se recoge en el sistema de información de STEP 7.

Consulte los detalles relacionados con los parámetros de la comunicación Telecontrol del CP 1542SP-1 IRC en el capítulo Comunicación Telecontrol(CP 1542SP-1 IRC) (Página 46).

Consulte los detalles relacionados con los parámetros de las funciones Security en el capítulo Configuración de seguridad (CP 1543SP-1) (Página 88).

Cargar y guardar datos de configuración

Al cargar la estación, se almacenan en la CPU los datos de configuración de la estación, incluidos los del CP. Consulte el sistema de información de STEP 7 para obtener más información sobre la carga de la estación.

4.3 Interfaz Ethernet

4.3.1 IPv6

Configuración de las direcciones Ethernet

Encontrará información sobre la configuración en el sistema de información de STEP 7.

Nota

Comunicación vía IPv6

Para utilizar direcciones IPv6 y conectar el CP a Internet, asegúrese de que el router conectado a Internet y los proveedores de los servicios de Internet utilizados (p. ej. correo electrónico) también soportan direcciones IPv6.

4.3.2 Sincronización horaria

Procedimientos de la sincronización horaria

El grupo de parámetros para la sincronización horaria se encuentra en la interfaz Ethernet.

Con las funciones Security activadas el grupo de parámetros se muestra en "Security".

Nota

Recomendación para la especificación del tiempo

Se recomienda ajustar una sincronización con un reloj externo en períodos de aprox. 10 segundos. Así se consigue una desviación mínima de la hora interna respecto a la hora absoluta.

Nota

Sin sincronización horaria con NTP / NTP (secure)

Tanto la CPU como el CP pueden permitir la sincronización horaria a través de NTP. Si activa la sincronización horaria en ambos módulos, se recomienda utilizar los mismos servidores NTP para garantizar la coherencia de la hora dentro de la estación.

El CP soporta básicamente el siguiente método de sincronización horaria:

- **NTP**

  Se configuran las direcciones del servidor o los servidores NTP, el intervalo de sincronización y la opción "Aceptar hora de servidores NTP no sincronizados".

CP 1542SP-1 IRC

Con la comunicación Telecontrol activada (grupo de parámetros "Tipos de comunicación"), en general el interlocutor adopta la hora:

- **Hora del interlocutor**

  El CP ajusta su hora con ayuda de la hora que obtiene de los telegramas del interlocutor.

El CP 1542SP-1 IRC ofrece a la CPU la posibilidad de adoptar la hora a través de una variable PLC del CP. Consulte a este respecto el capítulo Comunicación con la CPU (Página 57).

Nota

Sin sincronización horaria de la CPU en caso de adopción de la hora del CP

Si la CPU adopta la hora del CP a través de una variable PLC, desactive la sincronización horaria propia de la CPU.

CP 1543SP-1

Nota

Garantizar una hora válida

Si se utilizan funciones de seguridad es muy importante disponer de una hora válida. Se recomienda emplear el método NTP (secure).

El CP soporta los siguientes métodos de sincronización horaria:

- **NTP**
- **NTP (secure)**

  El procedimiento seguro NTP (secure) emplea la autenticación a través de claves simétricas según el algoritmo Hash MD5 o SHA-1.

  En los ajustes globales de Security es posible crear y gestionar servidores NTP adicionales, incluso del tipo NTP (secure).

4.4 SNMP

Grupo de parámetros "SNMP"

- **Activar SNMP**

  Habilita la función del agente SNMP en el CP.

Nota

Si en el CP 1543SP-1 están activadas las funciones Security, encontrará el grupo de parámetros "SNMP" en "Security".

Prestaciones de los CPs

Los CPs soportan las siguientes versiones de SNMP:

- **CP 1542SP-1, CP 1542SP-1 IRC**
  - SNMPv1
- **CP 1543SP-1**
  - SNMPv1
  - SNMPv3 (con funciones Security activadas)

El CP no soporta "traps".

Consulte los detalles de las funciones soportadas en el capítulo Diagnóstico a través de SNMP (Página 102).

4.5 Comunicación Telecontrol(CP 1542SP-1 IRC)

4.5.1 Configuración

Puntos de datos para la comunicación Telecontrol

En el CP 1542SP-1 IRC la transferencia de datos de usuario entre la estación y el interlocutor no requiere la programación de bloques de programa.

Las áreas de datos de la memoria de la CPU destinadas a la comunicación con el interlocutor se configuran en el CP vinculadas a puntos de datos. Cada punto de datos está vinculado a una variable PLC o elemento de un bloque de datos de la CPU.

Los diferentes puntos de datos pueden transferirse individualmente al sistema de control para procesarse en él.

Para la transferencia de los datos de proceso y para algunas opciones de los grupos de parámetros "Estaciones interlocutoras" y "Comunicación con la CPU" se requieren puntos de datos configurados.

Encontrará más información en el capítulo Configuración de puntos de datos (Página 59).

4.5.2 Tipos de comunicación

En este grupo de parámetros se activan los tipos de comunicación que se deseen utilizar para el CP correspondiente.

Para minimizar el riesgo de accesos no autorizados a la estación, deberá activar individualmente los servicios de comunicación que tenga que ejecutar el CP.

La Open User Communication no está presente en el grupo de parámetros, ya que estos servicios de comunicación no se configuran, sino que se programan mediante bloques de programa.

El grupo de parámetros no está presente en el CP 1542SP-1 ya que los servicios de comunicación soportados por este CP siempre están habilitados.

Grupo de parámetros "Tipos de comunicación"

- **Activar la comunicación Telecontrol**

  Solo con el CP 1542SP-1 IRC

  Habilita la comunicación Telecontrol en el CP. Pueden utilizarse los siguientes protocolos de forma alternativa:

  – **TeleControl Basic**

    Activa la comunicación con el servidor Telecontrol

  – **DNP3**

    Activa la comunicación con hasta cuatro maestros DNP3

  – **IEC 60870-5-104**

    Activa la comunicación con hasta cuatro maestros IEC

  Nota

  Plena funcionalidad Telecontrol solo con funciones Security activadas

  Para las siguientes funciones deben activarse las funciones Security:

  - Envío de mensajes (correo electrónico) a través de la funcionalidad Telecontrol
  - Uso del protocolo "TeleControl Basic" (general)
  - Uso de las funciones Security DNP3
  - Uso de certificados

  Nota

  Pérdida de datos de configuración al cambiar el protocolo Telecontrol

  Si cambia el protocolo en un CP configurado, se perderán los datos de configuración específicos de protocolo, por ejemplo la configuración de puntos de datos e interlocutores, así como los mensajes (correo electrónico).

- **Activar funciones online**

  Habilita el acceso a la CPU en el CP para las funciones online (diagnóstico, carga de datos de proyecto, etc.). Si esta función está activada, la estación de ingeniería puede acceder a la CPU a través del CP.

  Si la opción está desactivada, no es posible acceder a la CPU a través del CP con las funciones online. De todas formas, sigue siendo posible realizar un diagnóstico online de la CPU con conexión directa a la interfaz de la CPU.

- **Activar comunicación S7**

  Habilita en el CP las funciones de la comunicación S7 con un S7 SIMATIC y el routing S7.

  Active esta opción si configura conexiones S7 con la estación en cuestión que pasan por el CP.

4.5.3 Información de direccionamiento y autenticación

Información de direccionamiento y autenticación para la comunicación Telecontrol

Dependiendo del protocolo Telecontrol utilizado, los interlocutores del CP necesitan la siguiente información de direccionamiento y autenticación del CP, que debe configurarse para el CP:

- **TeleControl Basic**

  El servidor de Telecontrol necesita:

  – número de proyecto

  – número de estación

  – contraseña de Telecontrol (para la autenticación)

  Encontrará los parámetros en el grupo de parámetros "Identificación del CP" en "Security".

  – dirección IP (en el grupo de parámetros "Interfaz Ethernet")

    Dado que en general el CP establece la conexión con el servidor de Telecontrol, no hay que configurar la dirección IP del CP en TCSB.

- **DNP3**

  El maestro necesita:

  – número de estación (en el grupo de parámetros "Identificación del CP")

  – dirección IP (en el grupo de parámetros "Interfaz Ethernet")

  – número de puerto del CP

- **IEC**

  El maestro necesita:

  – número de estación (en el grupo de parámetros "Identificación del CP")

  – dirección IP (en el grupo de parámetros "Interfaz Ethernet")

  – número de puerto del CP

Información de direccionamiento requerida por el CP

Encontrará indicaciones sobre la información de direccionamiento del interlocutor requerida por el CP en el capítulo Estaciones interlocutoras (Página 52).

4.5.4 Interfaz Ethernet (X1) > Opciones avanzadas

Configure los parámetros disponibles en general igual que para cada una de las interfaces Ethernet restantes:

- datos generales (nombre, etc.)
- direcciones y, dado el caso, routers

- configuración de puerto
- acceso al servidor web

A continuación encontrará únicamente la descripción de los parámetros específicos para la comunicación de Telecontrol.

Vigilancia de conexión TCP

El ajuste realizado se aplica globalmente a todas las conexiones TCP del CP. Recuerde que puede sobrescribir el valor configurado aquí para diferentes interlocutores de la comunicación; consulte a continuación.

- **Tiempo de supervisión de conexión TCP**

  Si dentro del tiempo de vigilancia de conexión no hay tráfico de datos, el CP envía un telegrama Keep Alive al interlocutor.

  Rango admisible: 1 ... 65535 s. Ajuste predeterminado: 180

  El tiempo de vigilancia se configura en la interfaz Ethernet como ajuste predeterminado para todas las conexiones TCP. El valor predeterminado puede adaptarse individualmente para cada conexión en "Estaciones interlocutoras", consulte el capítuloEstaciones interlocutoras (Página 52). La función solo puede desactivarse en los interlocutores introduciendo 0 (cero).

- **Tiempo de vigilancia TCP Keep Alive**

  Tras enviar un telegrama Keep Alive, el CP espera una respuesta del interlocutor dentro del tiempo de vigilancia Keep Alive. Si el CP no recibe ninguna respuesta en el tiempo configurado, deshace la conexión.

  Rango admisible: 1 ... 65535 s. Ajuste predeterminado: 10

  El tiempo de vigilancia se configura en la interfaz Ethernet como ajuste predeterminado para todas las conexiones TCP. El valor predeterminado puede adaptarse individualmente para cada conexión en "Estaciones interlocutoras". La función solo puede desactivarse en los interlocutores introduciendo 0 (cero).

Ajustes de transferencia - TeleControl Basic

- **Retardo al establecer la conexión**

  Valor básico del tiempo de espera hasta el próximo establecimiento de conexión después de fallar el presente. Tras 3 intentos se duplica cada vez el valor básico hasta un máximo de 900 s.

  Rango admisible: 10 ... 300. Ajuste predeterminado: 10

  Ejemplo: el valor básico de 20 da los siguientes tiempos de espera: 3 x 20 s, 3 x 40 s, 3 x 80 s etc. hasta máx. 3 x 900 s.

- **Tiempo de vigilancia de emisión**

  Tiempo (segundos) para la entrada del acuse del interlocutor de comunicación (servidor de Telecontrol) tras enviar telegramas espontáneos. El tiempo se inicia tras el envío de un telegrama espontáneo. Si no ha llegado ningún acuse del interlocutor una vez transcurrido el tiempo de vigilancia de conexión, el telegrama se repite un máximo de

tres veces. Después de tres intentos fallidos se deshace la conexión y vuelve a establecerse.

Rango admisible: 1 ... 65535. Ajuste predeterminado: 5

- **Intervalo de cambio de clave**

  Aquí se introduce el intervalo en horas tras cuyo transcurso volverá a intercambiarse la clave entre el CP y el interlocutor (TCSB V3). La clave es una función de seguridad del protocolo de Telecontrol empleado por el CP y TCSB V3.

  Rango admisible: 0 ... 65535. Ajuste predeterminado: 8

  Con el valor 0 (cero) la función está desactivada.

Ajustes de transferencia - DNP3

Encontrará información sobre las funciones, los rangos admisibles y los ajustes predeterminados en los tooltips de STEP 7.

- **Bit de fallo**

  El bit de fallo puede utilizarse como bit 1.6 (IIN1.6) de los "Internal Indication Bytes" para indicar al maestro cuándo la CPU se encuentra en estado STOP.

- **Tiempo máx. entre Select y Operate**
- **Repeticiones de telegrama**
- **Confirmación de conexión**
- **Tiempo de vigilancia de conexión**
- **Modo de transferencia "espontáneo"**
- **Número máx. de telegramas espontáneos**
- **Tiempo de vigilancia para telegramas espontáneos**
- **Búfer para clase de evento 1 / 2 / 3**

  Aquí se especifica, para cada una de las tres clases de eventos, a partir de qué número de evento se envían los eventos guardados al interlocutor de la comunicación.

  Rango admisible: 1 ... 255

- **Tiempo de retardo clase de evento 1 / 2 / 3**

  Aquí se especifica en segundos, para cada una de las tres clases de eventos, durante cuánto tiempo deben guardarse los eventos como máximo en el búfer de transmisión antes de enviarlos al interlocutor de comunicación.

  Rango admisible: 0 ... 255

  Con el valor 0 (cero) la función está desactivada.

Encontrará detalles sobre el modo de funcionamiento del búfer de transmisión (almacenamiento y transmisión de eventos) y sobre las posibilidades de transferencia de datos en el capítulo Memoria imagen de proceso, tipo de transferencia, clases de eventos, disparos (Página 65).

Ajustes de transferencia - IEC

Nota

Ajustes en el maestro

Al configurar los tiempos de vigilancia t_1 y t_2, tenga en cuenta los ajustes correspondientes del maestro para que no se produzcan interrupciones de la conexión o mensajes de error involuntarios.

Encontrará información sobre las funciones, los rangos admisibles y los ajustes predeterminados en los tooltips de STEP 7.

- **Tiempo máx. entre Select y Operate**
- **Tiempo de vigilancia para establecimiento de conexión (t_0)**
- **Tiempo de vigilancia de telegrama (t_1)**

  Tiempo de vigilancia para el acuse por parte del interlocutor de telegramas enviados por el CP. El tiempo de vigilancia es válido para todos los telegramas enviados por el CP en formato I, S y U.

  Si el interlocutor no envía ningún acuse dentro del tiempo de vigilancia, el CP interrumpe la conexión con el interlocutor.

- **Tiempo de vigilancia para telegramas S y U (t_2)**

  Tiempo de vigilancia para el acuse de telegramas de datos del maestro por parte del CP.

  Tras recibir los datos del maestro, el CP acusa los datos recibidos de uno de los siguientes modos:

  – Si el CP envía él mismo datos al maestro dentro del tiempo t_2, con el telegrama de datos enviado (formato I) acusa también los telegramas de datos recibidos por el maestro dentro del tiempo t_2.

  – El CP envía un telegrama de acuse (formato S) al maestro como muy tarde una vez transcurrido el tiempo t_2.

  El valor de t_2 debe ser menor que el de t_1.

- **Tiempo de reposo para telegramas de test (t_3)**

  Tiempo de vigilancia en el que el CP no recibe telegramas del maestro.

  Una vez transcurrido el tiempo t_3, el CP envía un telegrama de test/control (formato U) al maestro.

  Este parámetro está previsto para tiempos prolongados en los que no hay tráfico de datos.

- **Diferencia entre número de secuencia de emisión N(S) y el número de secuencia de recepción N(R) (k)**

  Número máximo de telegramas de datos sin acusar (I-APDUs) como diferencia máxima entre Número de secuencia de emisión N(S) y Número de secuencia de recepción N(R).

  Si se alcanza k y todavía no ha finalizado t_1, el CP deja de enviar telegramas hasta que el maestro ha acusado todos los telegramas enviados.

  Si se alcanza k y t_1 ha concluido, se deshace la conexión TCP.

- **Número máximo de telegramas de datos no acusados (w)**

  Número máximo de telegramas de datos (I-APDUs) recibidos, alcanzado el cual el maestro debe confirmar el telegrama recibido más antiguo.

Mecanismo de acuse en el protocolo IEC

El CP envía junto con cada telegrama de datos un número secuencial de emisión correlativo. Inicialmente el telegrama de datos queda guardado en el búfer de transmisión.

Cuando el maestro lo recibe, devuelve al CP como confirmación el número secuencial de transmisión de ese telegrama o, en caso de recepción de varios telegramas, del último recibido. El CP guarda el número secuencial de transmisión devuelto por el maestro como número secuencial de recepción y lo utiliza como confirmación.

Los telegramas que tienen un número secuencial de emisión igual o menor que el de recepción actual se evalúan como transferidos correctamente y se borran del búfer de transmisión del CP.

Recomendaciones de la especificación:

- w no debe ser mayor que 2/3 de k.
- Valor recomendado para k: 12
- Valor recomendado para w: 8

Puerto [X1 Px]

Si no utiliza ambos puertos del BusAdapter, puede desactivar uno de ellos.

Encontrará información sobre los parámetros restantes en el sistema de información de STEP 7.

4.5.5 Estaciones interlocutoras

4.5.5.1 Configuración del interlocutor

La configuración de los interlocutores del CP (servidor de Telecontrol, maestro DNP3 o IEC) y de las conexiones con los interlocutores en STEP 7 no es posible ni necesaria.

Información de direccionamiento de los interlocutores

Para los interlocutores del CP se requiere la siguiente información en la configuración del CP:

- TeleControl Basic
  - Dirección IP del interlocutor

    Consulte a este respecto el capítulo Direccionamiento de interlocutores sencillos y redundantes (Página 56).
  - Puerto del interlocutor (número del puerto Listener del TCSB)

- DNP3 / IEC
  - Dirección de estación maestra

    Dirección de estación establecida en el maestro

    En el protocolo IEC la Dirección de estación maestra no se valora.
  - Dirección IP del interlocutor

    Dirección IP del maestro

    Respecto al direccionamiento de interlocutores redundantes consulte el capítulo Direccionamiento de interlocutores sencillos y redundantes (Página 56).
  - Puerto del interlocutor

"Estaciones interlocutoras" (solo con DNP3 / IEC)

- **Puerto Listener**

  Puerto Listener propio del CP

"Servidor de Telecontrol" / "Interlocutor"

- **Activar interlocutor**

  Active la opción para poder utilizar el interlocutor configurado a continuación para la comunicación.

  Con "TeleControl Basic" el servidor de Telecontrol siempre está activado como interlocutor.
- **Número de interlocutor**

  El número de interlocutor es asignado por STEP 7.
- **Dirección de estación / Dirección de estación maestra**

  El sistema asignará automáticamente la dirección de estación del servidor de Telecontrol cuando se active la comunicación por Telecontrol.

"Conexión con interlocutor"

Encontrará información sobre los rangos admisibles y los ajustes predeterminados en los tooltips de STEP 7.

- **Dirección IP del interlocutor**

  Dirección IP o nombre de host (FQDN) del servidor de Telecontrol. Por ejemplo, puede ser también el FQDN de un servicio DynDNS.
- **Vigilancia de conexión**

  Si se activa esta función se vigila la conexión con el interlocutor enviando telegramas Keep Alive.

  El tiempo de vigilancia de conexión TCP se ajusta en el grupo de parámetros de la interfaz Ethernet para todas las conexiones TCP del CP, consulte el capítulo Interfaz

Ethernet (X1) > Opciones avanzadas (Página 48). Este ajuste se aplica a todas las conexiones TCP del CP.

Aquí, en el grupo de parámetros "Estaciones interlocutoras", se puede ajustar por separado para este interlocutor el tiempo de vigilancia ajustado globalmente. El valor ajustado aquí sobrescribe para este parámetro el valor global que se había ajustado en el grupo de parámetros "Interfaz Ethernet (X1) > Opciones avanzadas > Vigilancia de conexión TCP".

- **Tiempo de supervisión de conexión TCP**

  Solo con TCP: Si dentro del tiempo de vigilancia de conexión no hay tráfico de datos, el CP envía un telegrama Keep Alive al interlocutor.

  El tiempo de vigilancia se configura en la interfaz Ethernet como ajuste predeterminado para todas las conexiones TCP. El valor predeterminado puede adaptarse individualmente para cada conexión en "Estaciones interlocutoras", y para este interlocutor sobrescribe el valor global que se había ajustado en "Interfaz Ethernet".

  Si se introduce 0 (cero) se puede desactivar la función para interlocutores individuales.

- **Tiempo de vigilancia TCP Keep Alive**

  Solo con TCP: tras enviar un telegrama Keep Alive, el CP espera una respuesta del interlocutor dentro del tiempo de vigilancia Keep Alive. Si el CP no recibe ninguna respuesta en el tiempo configurado, deshace la conexión.

  El tiempo de vigilancia se configura en la interfaz Ethernet como ajuste predeterminado para todas las conexiones TCP. El valor predeterminado puede adaptarse individualmente para cada conexión en "Estaciones interlocutoras".

  Si se introduce 0 (cero) se puede desactivar la función para interlocutores individuales.

- **Modo de conexión**

  En el modo de conexión "Permanente" existe una conexión permanente con el interlocutor.

- **Establecimiento de la conexión**

  Define el interlocutor de la comunicación que establece la conexión (siempre el CP).

- **Puerto del interlocutor**

  Número de puerto del interlocutor

"Conexión con interlocutor redundante" (solo con DNP3 / IEC)

- **Modo de redundancia**

  Active la opción si el interlocutor es un maestro redundante.

Respecto a los parámetros restantes, consulte arriba.

"Ajustes avanzados"

- **Tiempo de vigilancia de interlocutor (solo con DNP3 / IEC)**

  Si el CP no recibe ninguna señal de vida del interlocutor de la comunicación dentro del tiempo configurado, lo clasifica como fallo del interlocutor. Con el valor 0 se desactiva la función.

- **Notificar estado del interlocutor (enlace con el interlocutor)**

  Al activar esta función el CP notifica a la CPU el estado de la conexión con el interlocutor.

  – El bit 0 de "Variable PLC para estado del interlocutor" (tipo de datos WORD) se pone a 1 cuando el interlocutor está accesible.

  – El bit 1 se pone a 1 cuando todas las vías hacia el interlocutor remoto están en buen estado (se utiliza en caso de vías redundantes).

  – Los bits 2-3 indican el estado del búfer de transmisión (memoria de telegramas). Se admiten los valores siguientes:

    - 0: búfer de transmisión OK

    - 1: el búfer de transmisión está a punto de desbordarse (se ha sobrepasado el 80% de su capacidad).

    - 3: el búfer de transmisión se ha desbordado (se ha alcanzado el 100% de su capacidad).

    En cuanto se rebasa por defecto el 50 % de capacidad, los bits 2 y 3 vuelven a ponerse a 0.

  Los bits 4 a 15 de las variables PLC no están asignados y no tienen que evaluarse desde el punto de vista de la técnica del programa.

Ajustes específicos de DNP3

- **DNP3 level**

  Nivel de conformidad DNP3 soportado por el interlocutor.

- **Modo de transferencia de eventos**

  Modo según el cual se transfieren los telegramas del búfer de transmisión del CP (eventos):

  – transmisión cronológica de telegramas individuales

    o bien

  – transmisión por bloques de los telegramas de un punto de datos

4.5.5.2 Direccionamiento de interlocutores sencillos y redundantes

Direccionamiento del servidor de Telecontrol

- **Direccionamiento de un servidor de Telecontrol de configuración sencilla**

  Configure la dirección IP del servidor de Telecontrol o del router DSL para la conexión a través de Internet.

  Si se utiliza un servicio DynDNS se puede indicar el nombre de host (FQDN).

- **Direccionamiento del grupo de redundancia TCSB por medio de las estaciones a través de una única dirección IP**

  En la LAN de la central a la que están conectados los PC servidores TCSB y el router DSL (p. ej., SCALANCE M), se asigna una dirección IP virtual común a los dos PC servidores por medio del Network Load Balancing (NLB) del sistema operativo del equipo.

  Dicha dirección IP se configura en función de la estructura de la red:

  – Si hay conectado un CP sin router DSL, en el CP debe configurarse la dirección virtual asignada por el NLB como dirección IP del servidor de Telecontrol.

  – En caso de utilizar un router DSL, para el direccionamiento del servidor de Telecontrol redundante en las estaciones se configura una sola dirección IP, la dirección pública del router DSL.

    Ajuste la redirección de puertos (TCP) en el router DSL de manera que la dirección IP pública (red externa) conduzca a la dirección IP virtual del PC servidor del TCSB (red interna). Desde Internet solo se puede acceder a la dirección IP pública. De este modo, la estación no recibe información sobre con cuál de los dos equipos del grupo de redundancia está conectada.

Direccionamiento de maestros DNP3 o IEC redundantes

Indique para cada maestro la dirección de estación maestra y la dirección IP utilizada.

4.5.5.3 Interlocutor para comunicación cruzada

Solo si se utiliza el protocolo "TeleControl Basic".

Comunicación cruzada

En esta tabla se determinan las estaciones S7 y los CPs con los que la estación actual debe utilizar la comunicación cruzada. Las conexiones para la comunicación cruzada se desarrollan a través del servidor de Telecontrol.

Interlocutor

El número del interlocutor es asignado por el sistema. Es necesario en el marco de la configuración de puntos de datos para asignar puntos de datos a sus interlocutores de comunicación.

El direccionamiento del interlocutor para la comunicación cruzada se realiza mediante los parámetros "Proyecto", "Estación" y "Slot".

Proyecto

Introduzca aquí el número de proyecto del CP en la estación interlocutora. (Grupo de parámetros "Security > Identificación CP" en el interlocutor)

Estación

Introduzca aquí el número de estación del CP en la estación interlocutora. (Grupo de parámetros "Security > Identificación CP" en el interlocutor)

Slot

Introduzca aquí el número de slot del CP en la estación interlocutora por el cual se establece la conexión.

Memoria de telegrama

Cuando se activa, los telegramas se guardan en el búfer de transmisión (memoria de telegramas) del CP en caso de fallos de conexión. Tenga en cuenta que la capacidad de la memoria de telegramas se divide entre todos los interlocutores de la comunicación.

Si la opción está desactivada, los telegramas de eventos se guardan en la memoria imagen del CP, es decir, en caso de fallos de conexión los valores antiguos se sobrescriben con valores nuevos.

ID de acceso

La ID de acceso mostrada aquí se forma a partir de los valores hexadecimales del número de proyecto, el número de estación y el slot. El parámetro del tipo DWORD tiene la asignación siguiente:

- Bits 0 - 7: slot
- Bits 8 - 20: número de estación
- Bits 21 - 31: número de proyecto

4.5.6 Comunicación con la CPU

Comunicación con la CPU

Con los primeros tres parámetros se define el acceso del CP a la CPU en el ciclo de muestreo de la CPU. Encontrará la estructura del ciclo de muestreo de la CPU en el capítulo Ciclo de lectura (Página 72).

El cuarto parámetro "Tamaño de la memoria de telegramas" determina el tamaño del búfer de transmisión en el CP para telegramas de puntos de datos configurados como evento.

- **Tiempo de pausa del ciclo**

  Tiempo de espera entre dos ciclos de muestreo del área de memoria de la CPU.

- **Número máx. de peticiones de escritura**

  Número máximo de peticiones de escritura al área de memoria de la CPU dentro de un ciclo de muestreo de la CPU.

- **Número máx. de peticiones de lectura**

  Número máximo de peticiones de lectura de baja prioridad del área de memoria de la CPU dentro de un ciclo de muestreo de la CPU.

- **Tamaño de la memoria de telegramas**

  Aquí se ajusta el tamaño de la memoria de telegramas para eventos (búfer de transmisión).

  La capacidad de la memoria de telegramas se reparte a partes iguales entre todos los interlocutores de la comunicación. Puede consultar el tamaño de la memoria de telegramas en el capítulo Capacidad funcional y prestaciones (Página 17).

  Encontrará detalles sobre la función del búfer de transmisión (almacenamiento y transmisión de eventos) así como sobre las posibilidades de transferencia de datos en el capítulo Memoria imagen de proceso, tipo de transferencia, clases de eventos, disparos (Página 65).

Bit de vigilancia

- **Vigilancia del CP**

  A través del bit de vigilancia se puede comunicar a la CPU el estado de la comunicación de telecontrol del CP.

Hora del CP

- **Hora del CP para la CPU**

  A través de esta función el CP puede proporcionar su hora a la CPU.

  Encontrará más detalles en el sistema de información de STEP 7.

4.5.7 Configuración de puntos de datos

4.5.7.1 Configuración de los puntos de datos

Creación de puntos de datos y mensajes

La configuración de los puntos de datos y los mensajes se realiza en el editor de configuración de puntos de datos y mensajes de STEP 7. Lo encontrará en el árbol del proyecto:

Proyecto > Directorio de la estación correspondiente > Módulos locales > CP

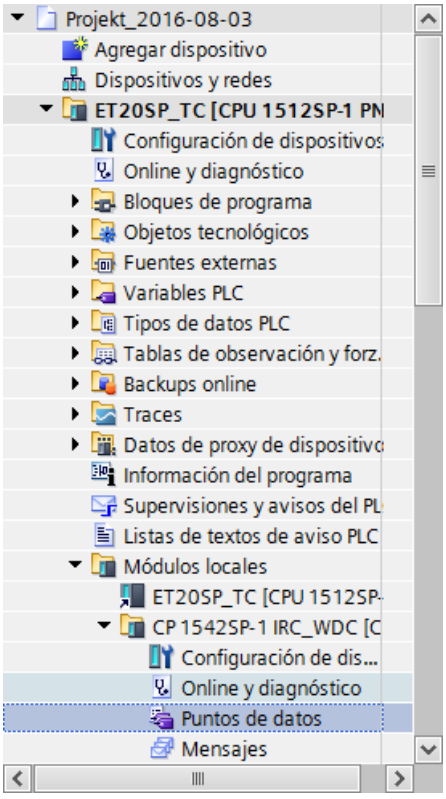


Figura 4-1 Acceso al editor de puntos de datos y mensajes

Abra el editor de puntos de datos y mensajes haciendo doble clic en la entrada "Puntos de datos" o "Mensajes".

Requisitos para puntos de datos: Variables PLC y/o bloques de datos (DB)

Para la configuración de los puntos de datos es imprescindible que las variables PLC o los DBs correspondientes se hayan creado en el programa de la CPU.

Las variables PLC de la configuración de puntos de datos pueden crearse en la tabla de variables estándar o en una tabla de variables definida por el usuario.

Consulte el número máximo admisible de variables PLC para la configuración de puntos de datos en el capítulo Capacidad funcional y prestaciones (Página 17).

Acceso a las áreas de memoria de la CPU

Los valores de las variables PLC o los DB referenciados por los puntos de datos se leen y son transferidos al interlocutor por el CP. El CP escribe los datos recibidos por el interlocutor en la CPU mediante las variables PLC o los DB.

Encontrará las áreas de direccionamiento, los formatos y los tipos de datos S7 de las variables PLC compatibles con los tipos de puntos de datos del CP específicos del protocolo en el capítulo Tipos de puntos de datos (Página 60).

Propiedades de los puntos de datos

Todas las variables PLC que deben utilizarse para la configuración de puntos de datos deben marcarse con el atributo "Visible en HMI".

Nota

Longitud de los nombres de puntos de datos

Si desea aprovechar al máximo el número máximo de puntos de datos configurables, asigne nombres lo más cortos posible a los puntos de datos, a los CPs y a las estaciones.

Juego de caracteres para nombres de puntos de datos

Al crear un punto de datos se aplica un nombre preasignado "DataPoint_n". En la tabla de puntos de datos y en la ficha "General" del punto de datos es posible cambiar el nombre del punto de datos.

Al asignar el nombre sólo está permitido utilizar caracteres ASCII de la banda 0x20 ... 0x7e, con las excepciones que se indican a continuación.

Los caracteres siguientes están prohibidos, pues no cumplen las reglas de sintaxis de TCSB para elementos OPC:

Caracteres no permitidos: . ' [ ] / \ |
punto, apóstrofe, corchetes, barra oblicua, barra inversa, barra vertical (pipe)

4.5.7.2 Tipos de puntos de datos

Tipos de puntos de datos soportados por el CP 1542SP-1IRC

Al configurar los datos de usuario que debe transferir el CP 1542SP-1 IRC, se asigna cada punto de datos a un tipo de punto de datos específico del protocolo. Los tipos de datos están listados a continuación, junto con los tipos de datos S7 compatibles en cada caso. Están agrupados por su formado (memoria necesaria).

TeleControl Basic: Tipos de puntos de datos

Tabla 4- 1 Tipos de puntos de datos soportados y tipos de datos S7 compatibles

Formato (memoria necesaria)	Tipo de punto de datos	Tipos de datos S7	Área de operandos
Bit	Entrada digital	Bool	I, Q, M, DB
	Salida digital	Bool	Q, M, DB
Byte	Entrada digital	Byte, USInt	I, Q, M, DB
	Salida digital	Byte, USInt	Q, M, DB
Entero con signo (16 bits)	Entrada analógica	Int	I, Q, M, DB
	Salida analógica	Int	Q, M, DB
Contador (16 bits)	Entrada de contador	Word, UInt	I, Q, M, DB
Entero con signo (32 bits)	Entrada analógica	DInt	Q, M, DB
	Salida analógica	DInt	Q, M, DB
Contador (32 bits)	Entrada de contador	UDInt, DWord	I, Q, M, DB
Número en coma flotante con signo (32 bits)	Entrada analógica	Real	Q, M, DB
	Salida analógica	Real	Q, M, DB
Número en coma flotante con signo (64 bits)	Entrada analógica	LReal	Q, M, DB
	Salida analógica	LReal	Q, M, DB
Bloque de datos (1 .. 64 bytes)	Datos	ARRAY [1)]	DB
	Datos	ARRAY [1)]	DB

[1)] Consulte el apartado siguiente sobre los formatos posibles del tipo de datos ARRAY.

Bloque de datos (ARRAY)

El tipo de datos ARRAY permite transferir áreas de memoria relacionadas de hasta 64 bytes de tamaño. Los componentes compatibles de ARRAY son los siguientes tipos de datos S7:

- Byte, USInt (en total hasta 64 por bloque de datos)
- Int, UInt, Word (en total hasta 32 por bloque de datos)
- DInt, UDInt, DWord (en total hasta 16 por bloque de datos)

Sello de tiempo en formato UTC

Los sellos de tiempo se transfieren en formato UTC (48 bits) e incluyen la diferencia de tiempo en milisegundos desde el 01-01-1970.

DNP3: Tipos de puntos de datos

Tabla 4- 2 Tipos soportados de puntos de datos, grupos de objetos DNP3, variantes y tipos de datos S7 compatibles

Formato (memoria necesaria)	Tipo de punto de datos	Grupo de objetos DNP3 [variations]	Sentido	Tipos de datos S7	Área de operandos
Bit	Binary Input	**1** [1, 2]	in	Bool	I, Q, M, DB
	Binary Input Event	**2** [1, 2]	in	Bool	I, Q, M, DB
	Binary Output [1)]	**10** [2]	out		
	Binary Output Event [1)]	**11** [1, 2]	out		
	Binary Command	**12** [1]	out	Bool	Q, M, DB

Formato (memoria necesaria)	Tipo de punto de datos	Grupo de objetos DNP3 [variations]	Sentido	Tipos de datos S7	Área de operandos
Integer (16 bits)	Counter Static	**20** [2]	in	UInt, Word	I, Q, M, DB
	Frozen Counter [2]	**21** [2, 6]	in		
	Counter Event	**22** [2, 6]	in	UInt, Word	I, Q, M, DB
	Frozen Counter Event [3]	**23** [2, 6]	in		
	Analog Input	**30** [2]	in	Int	I, Q, M, DB
	Analog Input Event	**32** [2]	in	Int	I, Q, M, DB
	Analog Output Status [4]	**40** [2]	out		
	Analog Output	**41** [2]	out	Int	Q, M, DB
	Analog Output Event [4]	**42** [2, 4]	out		
Integer (32 bits)	Counter Static	**20** [1]	in	UDInt, DWord	I, Q, M, DB
	Frozen Counter [2]	**21** [1, 5]	in		
	Counter Event	**22** [1, 5]	in	UDInt, DWord	I, Q, M, DB
	Frozen Counter Event [3]	**23** [1, 5]	in		
	Analog Input	**30** [1]	in	DInt	Q, M, DB
	Analog Input Event	**32** [1]	in	DInt	Q, M, DB
	Analog Output Status [4]	**40** [1, 3]	out		
	Analog Output	**41** [1]	out	DInt	Q, M, DB
	Analog Output Event [4]	**42** [1]	out		
Número en coma flotante (32 bits)	Analog Input	**30** [5]	in	Real	Q, M, DB
	Analog Input Event	**32** [5, 7]	in	Real	Q, M, DB
	Analog Output Status [4]	**40** [3]	out		
	Analog Output	**41** [3]	out	Real	Q, M, DB
	Analog Output Event [4]	**42** [5, 7]	out		
Número en coma flotante (64 bits)	Analog Input	**30** [6]	in	LReal	Q, M, DB
	Analog Input Event	**32** [6, 8]	in	LReal	Q, M, DB
	Analog Output	**41** [4]	out	LReal	Q, M, DB
	Analog Output Event [4]	**42** [6, 8]	out		
Bloque de datos (1...64 bytes) [5]	Octet String / Octet String Output	**110** [-]	in, out	[5]	DB
	Octet String Event [5]	**111** [-]	in, out	[5]	DB

[1] Este grupo de objetos puede configurarse en el editor de puntos de datos de STEP 7 mediante el grupo de objetos sustitutivos 12.

[2] Este grupo de objetos puede configurarse en el editor de puntos de datos de STEP 7 mediante el grupo de objetos sustitutivos 20.

[3] Este grupo de objetos puede configurarse en el editor de puntos de datos de STEP 7 mediante el grupo de objetos sustitutivos 22.

[4] Este grupo de objetos puede configurarse en el editor de puntos de datos de STEP 7 mediante el grupo de objetos sustitutivos 41.

[5] Con estos tipos de puntos de datos pueden transferirse áreas de memoria relacionadas de hasta 64 bytes de tamaño. Son compatibles todos los tipos de datos S7 de 1 a 64 bytes de tamaño.

Información sobre las notas 1), 2), 3) y 4) de la tabla: configuración de puntos de datos mediante grupos de objetos sustitutivos

Los tipos de puntos de datos de partida para los grupos de objetos siguientes pueden configurarse mediante los grupos de objetos sustitutivos citados anteriormente:

- 10 [2]
- 11 [1, 2]
- 21 [1, 2, 5, 6]
- 23 [1, 2, 5, 6]
- 40 [1, 2, 3]
- 42 [1, 2, 4, 5, 6, 7, 8]

Utilice para la configuración en el CP DNP3 el grupo de objetos sustitutivo indicado en cada caso.

Asigne el punto de datos correspondiente en el maestro utilizando el índice de puntos de datos configurable en STEP 7. El punto de datos del CP DNP3 se asignará a continuación al punto de datos correspondiente en el maestro.

Ejemplo de configuración del punto de datos Binary Output (10 [2])
El punto de datos se configura del siguiente modo:
en el CP DNP3 como Binary Command (12 [1])
en el maestro como Binary Output (10 [2])

Para los tipos de puntos de datos Binary Output Event (11) y Analog Output Event (42) debe activarse adicionalmente la retroalimentación; consulte el apartado siguiente.

Configuración de la retroalimentación para Output Events (grupos de objetos 11 y 42)

Los tipos de puntos de datos Binary Output Event (grupo de objetos 11) y Analog Output Event (grupo de objetos 42) se crean primero como puntos de datos de los grupos de objetos 12 y 41, respectivamente, tal como se ha descrito anteriormente.

Existe la posibilidad de supervisar los cambios en los valores locales de ambos grupos de objetos y transferirlos al maestro. La modificación de un valor local puede ser causada por una operación manual local, por ejemplo.

Para que pueda transferirse al maestro el valor provocado por eventos o intervenciones locales, el punto de datos en cuestión requiere un canal de retroalimentación. La función de retroalimentación se configura en la ficha "General" de la configuración de puntos de datos con la opción "Vigilancia de valores".

Tenga en cuenta que para la función de retroalimentación es necesario reubicar los valores locales del controlador en la variable PLC correspondiente del punto de datos.

Sello de tiempo en el CP DNP3 en formato UTC

Los sellos de tiempo se transfieren en formato UTC (48 bits) e incluyen milisegundos desde el 01-01-1970.

IEC: Tipos de puntos de datos

Tabla 4- 3 Tipos soportados de puntos de datos, tipos IEC y tipos de datos S7 compatibles

Formato (memoria necesaria)	Tipo de punto de datos	Tipo IEC	Sentido	Tipos de datos S7	Área de operandos
Bit	Single point information	<1>	in	Bool	I, Q, M, DB
	Single point information with time tag [1]	<30>	in	Bool	I, Q, M, DB
	Single command	<45>	out	Bool	Q, M, DB
Byte	Step position information	<5>	in	Byte, USInt	I, Q, M, DB
	Step position information with time tag [1]	<32>	in	Byte, USInt	I, Q, M, DB
Integer (16 bits)	Measured value, normalized value	<9>	in	Int	I, Q, M, DB
	Measured value, normalized value with time tag [1]	<34>	in	Int	I, Q, M, DB
	Measured value, scaled value	<11>	in	Int	I, Q, M, DB
	Measured value, scaled value with time tag [1]	<35>	in	Int	I, Q, M, DB
	Set point command, normalised value	<48>	out	Int	Q, M, DB
	Set point command, scaled value	<49>	out	Int	Q, M, DB
Integer (32 bits)	Bitstring of 32 bits	<7>	in	UDInt, DWord	I, Q, M, DB
	Bitstring of 32 bits with time tag CP56Time2a [1]	<33>	in	UDInt, DWord	I, Q, M, DB
	Integrated totals	<15>	in	UDInt, DWord	I, Q, M, DB
	Integrated totals with time tag CP56Time2a [1]	<37>	in	UDInt, DWord	I, Q, M, DB
	Bitstring of 32 bits	<51>	out	UDInt, DWord	Q, M, DB
Número en coma flotante (32 bits)	Measured value, short floating point number	<13>	in	Real	Q, M, DB
	Measured value, short floating point number with time tag CP56Time2a [1]	<36>	in	Real	Q, M, DB
	Set point command, short floating point number	<50>	out	Real	Q, M, DB
Bloque de datos (1...2 Bit) [2]	Double-point information	<3>	in	[2]	DB
	Double-point information with time tag CP56Time2a [1]	<31>	in	[2]	DB
	Double command	<46>	out	[2]	DB
	Regulating step command	<47>	out	[2]	DB
Bloque de datos (1...32 Bit) [3]	Bitstring of 32 bits [3]	<7>	in	[3]	DB
	Bitstring of 32 bits with time tag CP56Time2a [1] [3]	<33>	in	[3]	DB
	Bitstring of 32 bits [3]	<51>	out	[3]	DB

[1] Consulte el formato de los sellos de tiempo en el apartado siguiente.

[2] Cree un bloque de datos para estos tipos de puntos de datos con un array de exactamente 2 Bool.

[3] Con estos tipos de puntos de datos pueden transferirse áreas de memoria relacionadas de hasta 32 bits de tamaño. Solo es compatible el tipo de datos S7 Bool.

Sello de tiempo en el CP IEC

En el CP IEC, los sellos de tiempo se transfieren en formato "CP56Time2a" conforme a la especificación IEC. Tenga en cuenta que en los telegramas solo se transfieren los 3 primeros bytes correspondientes a milisegundos y minutos.

4.5.7.3 Memoria imagen de proceso, tipo de transferencia, clases de eventos, disparos

Almacenamiento de los valores de puntos de datos

Por norma general, los valores de puntos de datos se guardan en la memoria imagen del CP y no se transfieren hasta que son solicitados por el interlocutor.

Los eventos se guardan también en el búfer de transmisión y pueden transferirse de forma espontánea.

Los puntos de datos se configuran como valores estáticos o como eventos por medio del parámetro "Tipo de transferencia" (véase más adelante):

- **Valor estático (sin evento)**

  Los valores estáticos se introducen en la memoria imagen (memoria imagen de proceso del CP).

  Valores estáticos de las siguientes clases:

  – DNP3: Class 0

  – IEC: Clase 2

- **Evento**

  Los valores de puntos de datos que están configurados como eventos también se introducen en la memoria imagen del CP. El valor del evento se envía espontáneamente al interlocutor de la comunicación cuando esta función está habilitada por parte del maestro.

  Adicionalmente, los valores de eventos se introducen en el búfer de transmisión del CP.

  Los eventos equivalen a las siguientes clases:

  – DNP3: Class 1 / 2 / 3

  – IEC: Clase 1

Memoria imagen, la memoria imagen de proceso del CP

En la memoria imagen se guardan todos los valores actuales de los puntos de datos configurados. Los valores nuevos de un punto de datos sobrescriben el último valor guardado en la memoria imagen.

Los valores se envían tras una consulta del interlocutor de la comunicación. Consulte "Transferencia tras llamada" en el apartado "Tipos de transferencia" más adelante.

El búfer de transmisión

El búfer de transmisión del CP es la memoria para los diferentes valores de puntos de datos configurados como eventos. El número configurado se distribuye por igual entre todos los interlocutores configurados y activados. El tamaño del búfer de transmisión se configura a través del parámetro "Tamaño de la memoria de telegramas", consulte el capítulo Comunicación con la CPU (Página 57).

En caso de que se haya interrumpido la conexión con un interlocutor, los valores de los diferentes eventos se conservan gracias al respaldo. Cuando se recupera la conexión se envían los valores respaldados. La memoria de telegramas funciona cronológicamente, es decir, los telegramas más antiguos se envían en primer lugar (principio FIFO).

Cuando se transfiere un telegrama al interlocutor, el valor transmitido se borra del búfer de transmisión.

Cuando no es posible transmitir telegramas durante un tiempo prolongado y el búfer de transmisión está a punto de desbordarse, el comportamiento será el siguiente en función del protocolo utilizado:

- TeleControl Basic

  El método de memoria imagen forzada

  Cuando el búfer de transmisión está lleno en un 80% de su capacidad, el CP cambia al método de memoria imagen forzada. Los valores nuevos de los puntos de datos que están configurados como eventos ya no se registran adicionalmente en el búfer de transmisión sino que sobrescriben los valores más antiguos que ya están en la memoria imagen.

  Cuando se recupera la conexión con el interlocutor, el CP cambia de nuevo al método de búfer de transmisión una vez se ha rebasado por defecto el 50% de la capacidad.

- DNP3 / IEC

  Cuando el búfer de transmisión está lleno en un 100% de su capacidad, se sobrescriben los valores más antiguos.

  Si se utiliza el protocolo DNP3 existe la posibilidad de definir condiciones adicionales para la transmisión de eventos:

  – Un número máximo de eventos en el búfer de transmisión, configurable para cada clase de evento.
  – Una duración máxima configurable de almacenamiento de eventos en el búfer de transmisión.

Tipo de transferencia

Son posibles los siguientes tipos de transferencia:

- **Transferencia tras llamada (class 0)**

  El valor actual del punto de datos en cada caso se introduce en la memoria imagen del CP. Los valores nuevos de un punto de datos sobrescriben el último valor guardado en la memoria imagen.

  Tras una llamada del interlocutor de la comunicación se transfiere el valor actual en ese momento.

- **Con disparo (eventos)**

  Los valores de puntos de datos que están configurados como eventos se registran en la memoria imagen y también en el búfer de transmisión del CP.

  Los valores de eventos se guardan en los casos siguientes:

  – Se cumplen las condiciones de disparo configuradas en cada caso (configuración de puntos de datos > ficha "Disparo", véase más adelante).

  – Varía el valor de un bit de estado de las identificaciones de estado del punto de datos, consulte el capítulo Identificaciones de estado de los puntos de datos (Página 69).

Clases de evento en el tipo de transferencia "Con disparo"

En función del protocolo utilizado están disponibles las siguientes clases de evento:

- **TeleControl Basic**
  - **Todos los valores disparados**

    Cada cambio de valor se introduce en el búfer de transmisión en orden cronológico.
  - **Valor actual disparado**

    Solo se introduce en el búfer de transmisión el valor actual, que es el último en cada caso. Sobrescribe el valor que estaba guardado allí previamente.
- **DNP3**

  El maestro debe evaluar la clasificación siguiente.
  - **Clase de evento 1**

    Clase según el protocolo DNP3: Class 1

    Cada cambio de valor se introduce en el búfer de transmisión en orden cronológico.
  - **Clase de evento 2**

    Clase según el protocolo DNP3: Class 2

    Cada cambio de valor se introduce en el búfer de transmisión en orden cronológico.
  - **Clase de evento 3**

    Clase según el protocolo DNP3: Class 3

    Solo se introduce en el búfer de transmisión el valor actual en el momento en que se cumple la condición de disparo y este sobrescribe el último valor guardado allí.
- **IEC**

  Las dos siguientes clases de evento equivalen a la clase de datos de usuario 1 del protocolo IEC
  - **Todos los valores disparados**

    Cada cambio de valor se introduce en el búfer de transmisión en orden cronológico.
  - **Valor actual disparado**

    Solo se introduce en el búfer de transmisión el valor actual en el momento en que se cumple la condición de disparo y este sobrescribe el último valor guardado allí.

Disparo

Tipos de disparo

Para la transferencia controlada por evento están disponibles diferentes tipos de disparo:

- **Disparo de valor umbral**

  El valor del punto de datos se transfiere cuando alcanza un umbral determinado. El umbral se calcula como diferencia respecto del último valor guardado, consulte el capítulo Disparo de valor umbral (Página 74).

- **Disparo de tiempo**

  El valor del punto de datos se transfiere en un espacio de tiempo configurable o a una hora determinada.

- **Disparo de evento**

  El valor del punto de datos se transfiere cuando se lanza una señal de disparo configurable. Como señal de disparo se evalúa el cambio de flanco (0 → 1) de un bit de disparo activado por el programa de usuario. En caso necesario es posible configurar un bit de disparo independiente para cada punto de datos.

  Desactivación de la variable de disparo en el área de marcas/DB:

  Cuando el área de memoria de la variable de disparo está en el área de marcas o en un bloque de datos, la variable de disparo se pone a cero al transferir el valor del punto de datos.

Instante de transmisión del telegrama

Según el protocolo utilizado y los ajustes el valor de un punto de datos se transferirá al interlocutor de inmediato o con retardo tras iniciar el disparo.

- **TeleControl Basic**

  El momento de transmisión se define con el parámetro "Modo de transmisión" en la ficha "Disparo" del punto de datos:

  – **Espontáneo**

    El valor se transfiere de inmediato.

  – **Espontáneo con limitaciones**

    El valor no se transfiere hasta que se cumple una de las condiciones siguientes:

    - El servidor de Telecontrol consulta la estación.

    - Se transfiere el valor de otro evento con el modo de transferencia "Espontáneo".

    - El grado de llenado del búfer de transmisión ha alcanzado el 80 % de su capacidad máxima.

- **DNP3 / IEC**

  Con estos protocolos la transferencia espontánea depende de si en la red es posible el envío espontáneo o la comunicación asimétrica.

4.5.7.4 Identificaciones de estado de los puntos de datos

Identificaciones de estado para puntos de datos

Las identificaciones de estado de los puntos de datos listadas a continuación se transfieren para cada punto de datos con cada telegrama. La diferencia en los tres tipos de protocolo es mínima.

Consulte más a bajo el significado de los bits de estado. El "significado" (2.º fila de la tabla) hace referencia al estado correspondiente del bit (3.ª fila de la tabla).

Generación de eventos al cambiar el estado del punto de datos

Para los puntos de datos configurados como eventos, el cambio de un bit de estado provoca las identificaciones de estado que se describen a continuación, además de la generación de un evento.

Ejemplo: Si el valor del estado "RESTART" de un punto de datos configurado como evento cambia de 1 (valor no actualizado) a 0 (valor actualizado) al arrancar la estación, se genera un evento.

Identificaciones de estado - TeleControl Basic

TCSB convierte los bits de estado en el OPC quality code del modo siguiente:

- Quality = BAD, si:

  NON_EXISTENT o OVER_RANGE = 1

- Quality = UNCERTAIN, si:

  RESTART o CARRY o SB = 1

- Quality = GOOD, si:

  bits 1, 2, 3, 5 y 6 = 0

Tabla 4- 4 Asignación de bits del byte de estado 0

Bit	7	6	5	4	3	2	1	0
Nombre de la marca	-	NON_ EXISTENT	SB	LOCAL_ FORCED	CARRY	OVER_ RANGE	RESTART	ONLINE
Significado	-	Punto de datos no disponible o dirección S7 no accesible	Valor sustitutivo	*(El bit no se activa)*	Desbordamiento del valor de contaje antes de leer el valor	Valor límite del preprocesamiento de valores analógicos rebasado por exceso o defecto	El valor sigue sin actualizar tras el inicio	El valor es válido, CPU en RUN.
Estado del bit	*(siempre 0)*	1	1	*(irrelevante)*	1	1	1	1

Identificaciones de estado - DNP3

El maestro puede evaluar las identificaciones de estado. Estas corresponden a los elementos siguientes de las especificaciones:

OBJECT FLAGS - DNP3 Specification, Volume 6, Data Object Library - Part 1

Tabla 4- 5 Asignación de bits del byte de estado

Bit	7	6	5	4	3	2	1	0
Nombre de la marca	-	-	-	LOCAL_ FORCED	DISCONTI NUITY	OVER_ RANGE	RESTART	ONLINE
Significado	-	-	-	Operación local	Desborda-miento del valor de contaje antes de leer el valor	Valor límite del preproce-samiento de valores ana-lógicos reba-sado por exceso o defecto	El valor sigue sin actualizar tras el inicio	Valor válido
Estado del bit	*(siempre 0)*	*(siempre 0)*	*(siempre 0)*	1	1	1	1	1

Identificaciones de estado -

El maestro puede evaluar las identificaciones de estado. Estas corresponden a los elementos siguientes de las especificaciones:

Quality descriptor - IEC 60870 Part 5-101

Tabla 4- 6 Asignación de bits del byte de estado

Bit	7	6	5	4	3	2	1	0
Nombre de la marca	-	-	SB substituted	-	CY carry	OV overflow	NT not topical	IV invalid
Significado	-	-	Valor sustitu-tivo	-	Desborda-miento del valor de contaje antes de leer el valor	Rango de valores reba-sado por exceso, valor analógico	Valor no actualizado	Valor válido
Estado del bit	*(siempre 0)*	*(siempre 0)*	1	*(siempre 0)*	1	1	1	0

4.5.7.5 Reglas para configurar el índice de punto de datos

Configuración del índice de punto de datos

A continuación encontrará las reglas de configuración del índice de puntos de datos en función del protocolo utilizado.

TeleControl Basic

Dentro de un CP, los índices de las clases de puntos de datos deben cumplir las reglas siguientes:

- Entrada

  El índice de un punto de datos del tipo Entrada debe ser unívoco en todos los tipos de puntos de datos (entradas digitales, entradas analógicas, etc.).

- Salida
  - Un punto de datos del tipo Salida puede tener el mismo índice que un punto de datos del tipo Entrada.
  - Varios puntos de datos del tipo Salida pueden tener el mismo índice.

Nota

Puntos de datos para la comunicación cruzada con un CP en otra estación S7

Tenga en cuenta que en la comunicación cruzada los índices de los dos puntos de datos correspondientes (parejas de puntos de datos) deben ser idénticos tanto en el CP que envía como en el que recibe.

DNP3

En un CP, los índices de puntos de datos deben ser unívocos dentro de uno de los grupos de objetos siguientes:

- Binary Input / Binary Input Event
- Binary Output / Binary Command
- Counter / Counter Event
- Analog Input / Analog Input Event
- Analog Output
- Octet String / Octet String Event

Los índices de dos puntos de datos en diferentes grupos de objetos pueden ser idénticos.

IEC

Los índices de puntos de datos deben ser unívocos dentro de un CP.

Los índices de puntos de datos asignados por duplicado se notifican como errores durante la comprobación de la coherencia e impiden que se guarde el proyecto.

4.5.7.6 Ciclo de lectura

Prioridad de los puntos de datos

La lectura cíclica de los valores de puntos de datos de entrada desde sus variables PLC asignadas en la CPU puede priorizarse.

No es necesario leer en cada ciclo de muestreo de la CPU los puntos de datos de entrada menos importantes. En cambio, los puntos de datos de entrada importantes pueden priorizarse para una actualización en cada ciclo de muestreo de la CPU.

En STEP 7 la priorización se realiza en la ficha "General" de la configuración de puntos de datos, con el parámetro "Ciclo de lectura". Allí encontrará las dos opciones siguientes para puntos de datos de entrada:

- Ciclo rápido
- Ciclo normal

Los puntos de datos se leen de acuerdo con el comportamiento descrito a continuación.

Estructura del ciclo de muestreo de la CPU

El ciclo (incluida la pausa) con el que el CP muestrea el área de memoria de la CPU consta de las fases siguientes:

- **Peticiones de lectura con prioridad alta**

  Los valores de puntos de datos de entrada con la prioridad de muestreo "alta" se leen en todos los ciclos de muestreo.

- **Peticiones de lectura de prioridad baja**

  Los valores de puntos de datos de entrada con la prioridad de muestreo "baja" se leen proporcionalmente en todos los ciclos de muestreo.

  El número de valores que se leen en cada ciclo se especifica para el CP con el parámetro "Número máx. de peticiones de lectura" en el grupo de parámetros "Comunicación con la CPU". Los valores que pasan de dicho valor y, por tanto, no se leen en un ciclo, se leerán en el próximo ciclo o en otro ulterior.

- **Peticiones de escritura**

  En cada ciclo se escriben en la CPU los valores de un número determinado de peticiones de escritura espontáneas. El número de valores que se escriben en cada ciclo se especifica para el CP con el parámetro "Número máx. de peticiones de escritura" en el grupo de parámetros "Comunicación con la CPU". Los valores cuyo número excede este valor se escriben en el próximo ciclo o en uno de los siguientes.

- **Tiempo de pausa del ciclo**

  Es el tiempo de espera entre dos ciclos de muestreo. Sirve para reservar tiempo suficiente para otros procesos que acceden a la CPU por medio del bus de fondo de la estación.

Duración del ciclo de muestreo de la CPU

Puesto que para el ciclo no es posible configurar un tiempo fijo y las diferentes fases no tienen asignado un número fijo de objetos, la duración del ciclo de muestreo es variable y puede cambiar dinámicamente.

4.5.7.7 Ficha "Disparo"

Disparo

Los puntos de datos se configuran como valores estáticos o como eventos por medio del parámetro "Tipo de transferencia":

Almacenamiento del valor de un punto de datos configurado como evento

El almacenamiento del valor de un punto de datos configurado como evento en el búfer de transmisión (memoria de telegrama) puede iniciarse utilizando diferentes tipos de disparo:

- **Disparo de valor umbral**

  El valor del punto de datos se guarda cuando alcanza un umbral determinado. El umbral se calcula como diferencia respecto del último valor guardado, consulte el capítulo Disparo de valor umbral (Página 74).

- **Disparo de tiempo**

  El valor del punto de datos se guarda en un espacio de tiempo configurable o a una hora determinada.

- **Disparo de evento (variable de disparo)**

  El valor del punto de datos se guarda cuando se lanza una señal de disparo configurable. Como señal de disparo se evalúa el cambio de flanco (0 → 1) de una variable de disparo activada por el programa de usuario. En caso necesario es posible configurar una variable de disparo independiente para cada punto de datos.

  Desactivación de la variable de disparo en el área de marcas/DB:

  Cuando el área de memoria de una variable de disparo está en el área de marcas o en un bloque de datos, el propio CP pone a 0 (cero) la variable de disparo al transferir el valor del punto de datos. Esto puede tardar 500 milisegundos como máximo.

Nota

Activación rápida de disparos

Los disparos no puede activarse con más rapidez que con una distancia mínima de 500 milisegundos. Lo mismo es válido para disparos de hardware (área de entrada).

Nota

Disparo de hardware

Los disparos de hardware se desactivan mediante el programa de usuario.

Transferencia del valor de un punto de datos configurado como evento

Con el parámetro "Modo de transferencia" se especifica si el valor de un punto de datos se transfiere al interlocutor de inmediato o con retardo tras iniciar el disparo.

Modo de transferencia

El modo de transferencia de un telegrama se ajusta en la ficha "Disparo" del punto de datos. Con esta opción se especifica si los telegramas de eventos se envían de inmediato o con retardo:

- Transmisión espontánea - Espontáneo

  El valor se transfiere de inmediato.

- Transmisión con búfer - Espontáneo con limitaciones

  El valor no se transfiere hasta que se cumple una de las condiciones siguientes:

  – El interlocutor de la comunicación consulta la estación.

  – Se transfiere el valor de otro evento con el modo de transferencia "Espontáneo".

4.5.7.8 Disparo de valor umbral

Nota

Disparo de valor umbral: cálculo después del Preprocesamiento de valores analógicos

Tenga en cuenta que el preprocesamiento de valores analógicos se lleva a cabo antes de la comprobación de un valor umbral configurado y antes de calcular el valor umbral.

Esto afecta al valor que se configura en Disparo de valor umbral.

Nota

No hay disparo de valor umbral si cálculo del valor medio está configurado

Si el cálculo del valor medio está configurado, no es posible configurar un disparo de valor umbral para el evento de valor analógico correspondiente.

Respecto al proceso de Preprocesamiento de valores analógicos consulte el capítulo Preprocesamiento de valores analógicos (Página 76).

Disparo de valor umbral

Función

Si el valor de proceso difiere en el valor de umbral, se guarda el valor de proceso.

Para calcular la desviación del valor de umbral se aplican dos métodos:

- **Método absoluto**

  Para valores binarios o numéricos, así como para valores analógicos, para los que se ha configurado la formación del promedio, se aplica el método absoluto para calcular la desviación del valor de umbral.

- **Método integrativo**

  Para valores analógicos, para los que no se ha configurado la formación del promedio, se aplica el método integrativo para calcular la desviación del valor de umbral.

  En el cálculo integrador del valor umbral no se evalúa el valor absoluto de la desviación del valor de proceso respecto del último valor guardado, sino la diferencia integrada.

Método absoluto

Para cada valor binario se comprueba si el valor actual (quizá filtrado) se encuentra fuera del margen del valor de umbral. El margen aplicable en cada caso resulta del último valor almacenado y del valor absoluto del valor de umbral configurado:

- Límite superior del margen del valor de umbral: último valor almacenado + valor de umbral
- Límite inferior del margen del valor de umbral: último valor almacenado - valor de umbral

En cuanto el valor de proceso alcanza el límite superior o inferior del margen del valor de umbral, se almacena el valor. El nuevo valor guardado sirve de base para calcular el nuevo margen del valor de umbral.

Método integrativo

El cálculo integrador del valor umbral trabaja con una comparación cíclica del valor actual integrado con el último valor guardado. El ciclo de cálculo en el que se comparan ambos valores es de 500 milisegundos.
(Observación: el ciclo de cálculo no debe confundirse con el ciclo de muestreo de las áreas de memoria de la CPU).

Las desviaciones del valor de proceso actual se totalizan en cada ciclo de cálculo. El disparo no se activa hasta que el valor totalizado alcanza el valor configurado para el disparo de valor umbral y entonces se registra un valor de proceso nuevo en el búfer de transmisión.

El método se explica con el ejemplo siguiente, que tiene configurado un valor umbral de 2,0.

Tabla 4- 7 Ejemplo de cálculo integrador de un valor umbral configurado con 2,0

Tiempo [s] (ciclo de cálculo)	Valor de proceso guardado en el búfer de transmisión	Valor de proceso actual	Diferencia absoluta respecto del valor guardado	Diferencia integrada
0	**20,0**	**20,0**	0	0
0,5		20,3	+0,3	0,3
1,0		19,8	-0,2	0,1
1,5		20,2	+0,2	0,3
2,0		20,5	+0,5	0,8
2,5		20,3	+0,3	1,1
3,0		20,4	+0,4	1,5
3,5	**20,5**	**20,5**	+0,5	**2,0**
4,0		20,4	-0,1	-0,1
4,5		20,1	-0,4	-0,5
5,0		19,9	-0,6	-1,1
5,5		20,1	-0,4	-1,5
6,0	**19,9**	**19,9**	-0,6	**-2,1**

En el desarrollo del valor de proceso mostrado en el ejemplo, el disparo de valor umbral configurado con 2,0 se lanza dos veces:

- En el instante 3,5 s: El importe de la diferencia integrada es de 2,0. El nuevo valor de proceso guardado en el búfer de transmisión es 20,5.
- En el instante 6,0 s: El importe de la diferencia integrada es de 2,1. El nuevo valor de proceso guardado en el búfer de transmisión es 19,9.

Si en este ejemplo una desviación del valor de proceso de aprox. 0,5 debiera originar el disparo, debería configurarse un valor umbral de entre 1,5 y 2,5 en el comportamiento representado del valor de proceso.

4.5.7.9 Preprocesamiento de valores analógicos

Los CPs con configuración de punto de datos soportan el preprocesamiento de valores analógicos. Para puntos de datos de valores analógicos pueden configurarse algunas o todas las funciones descritas a continuación.

Requisitos y restricciones

Encontrará los requisitos para la configuración de las opciones de preprocesamiento así como las restricciones mutuas en el apartado correspondiente a cada función.

Nota

Restricciones debidas a disparos configurados

Las opciones de preprocesamiento de valores analógicos "Tiempo de supresión de errores", "Cálculo de valores límite" y "Filtrado" no se ejecutan si no se ha configurado un disparo de valor umbral para el punto de datos correspondiente. En estos casos, el valor de proceso leído del punto de datos se registra en la memoria imagen del CP antes de que finalice el ciclo de preprocesamiento del cálculo de valor umbral (500 ms) y se transfiere de forma transparente.

Ejecución de las opciones de preprocesamiento de valores analógicos

Los valores de entradas analógicas que están configuradas como eventos se procesan en el CP siguiendo el esquema descrito a continuación:

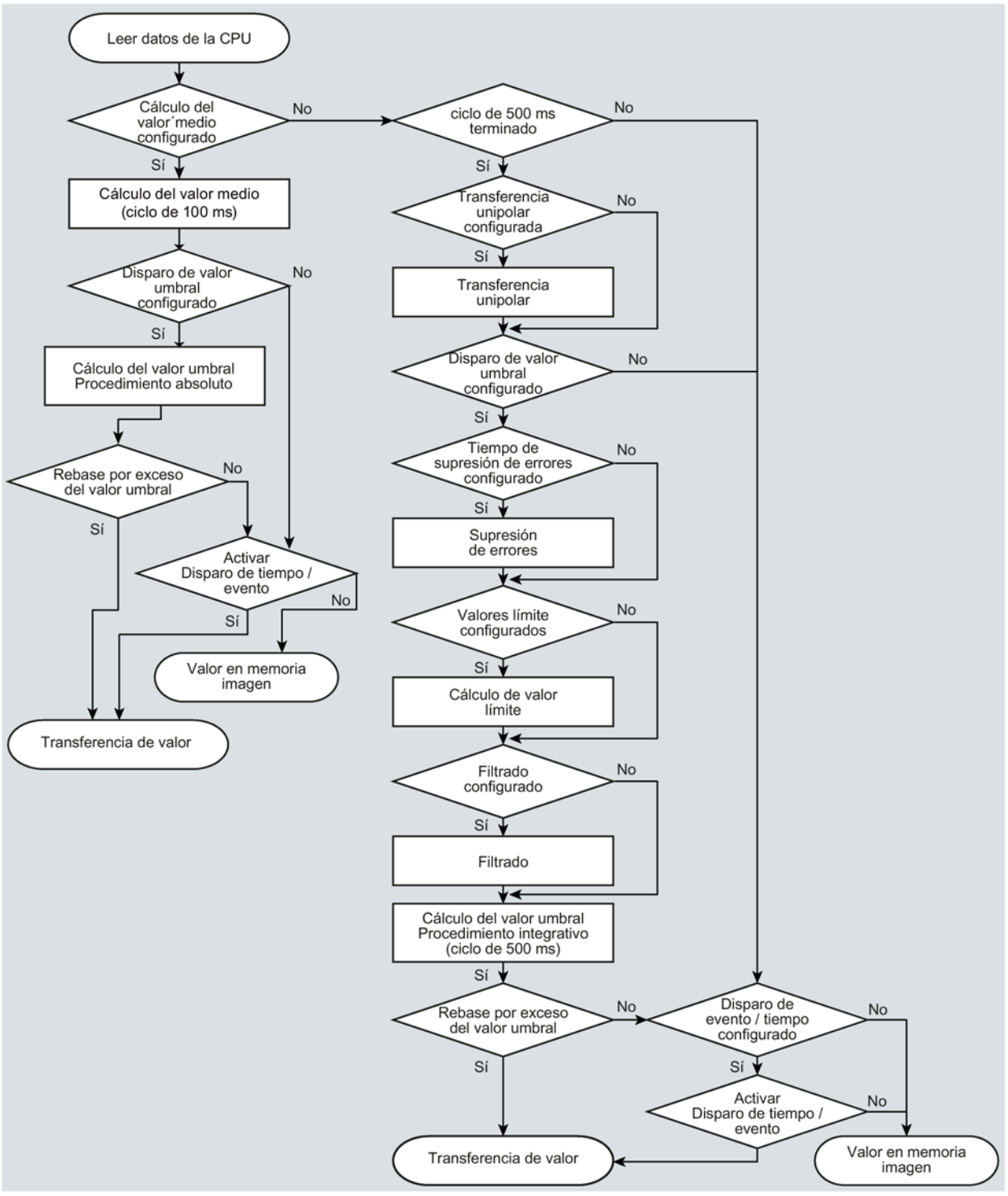


Figura 4-2 Ejecución del preprocesamiento de valores analógicos

El ciclo de 500 milisegundos se aplica mediante el cálculo integrativo del valor umbral. En este ciclo, los valores se guardan también cuando se activan las siguientes opciones de preprocesamiento:

- Transferencia unipolar
- Tiempo de supresión de errores
- Cálculo de valores límite
- Filtrado

Cálculo del valor medio

Nota

Opciones de preprocesamiento limitadas en caso de configurar el cálculo del valor medio

Si se configura el cálculo del valor medio para un evento de valor analógico, no estarán disponibles las siguientes opciones de preprocesamiento:

- Transferencia unipolar
- Tiempo de supresión de errores
- Filtrado

Función

Con este parámetro se transfieren valores analógicos captados como valores medios.

Si el cálculo del valor medio está activado es conveniente configurar un disparo de tiempo.

Los valores actualmente pendientes para un punto de datos de valor analógico se leen y totalizan en un ciclo de 100 milisegundos. El número de valores leídos por unidad de tiempo depende del ciclo de lectura de la CPU y del ciclo de muestreo de la CPU para el CP.

A partir de los valores totalizados se calcula el valor medio en cuanto se lanza la transferencia por medio de un disparo. A continuación se reinicia la totalización para calcular el próximo valor medio.

El valor medio también se calcula cuando la transferencia del telegrama de valores analógicos es lanzada por una consulta del interlocutor. En este caso, la duración del período de cálculo es el tiempo que transcurre entre la última transferencia (p. ej. lanzada por el disparo) y el instante de la consulta. Después de esta transferencia también se reinicia la totalización para calcular el próximo valor medio.

Módulos de entrada: Rango de rebase por exceso / Rango de rebase por defecto

En cuanto se capta un valor en el rango de desbordamiento por exceso o defecto se cancela el cálculo del valor medio. Para el período de cálculo en curso, el valor 32767 / $7FFF_h$ o -32768 / 8000_h se guarda como valor medio no válido y se transfiere en el próximo telegrama.

Posteriormente se inicia un nuevo cálculo del valor medio. Si el valor analógico sigue estando en el rango de desbordamiento por exceso o defecto, uno de los dos valores citados se guarda como valor medio no válido y se transfiere con el próximo lanzamiento del telegrama.

Nota

Tiempo de supresión de errores > 0 configurado

Si se ha configurado un tiempo de supresión de errores y posteriormente se activa el cálculo del valor medio, el valor del tiempo de supresión de errores se atenúa y deja de aplicarse. El tiempo de supresión de errores se pone a 0 (cero) internamente cuando el cálculo del valor medio está activado.

Transferencia unipolar

Restricciones

La transferencia unipolar no puede configurarse simultáneamente con el cálculo del valor medio. La activación de la transferencia unipolar deja de tener efecto en el momento de activarse el cálculo del valor medio.

Función

Al activar la transferencia unipolar se corrigen los valores negativos a cero. Esto puede ser aconsejable si los valores del rango de saturación por debajo no deben transmitirse como valores medidos reales.

Excepción: En los datos de proceso de módulos de entrada, el valor -32768 / 8000_h se transfiere para la rotura de hilo de un entrada Life Zero.

En cambio, en una entrada de software se corrigen a cero todos los valores inferiores a cero.

Tiempo de supresión de errores

Requisitos para la función

Configuración del disparo de valor umbral para este punto de datos

Restricciones

El tiempo de supresión de errores no puede configurarse simultáneamente con el cálculo del valor medio. Un valor configurados deja de tener efecto en el momento de activarse el cálculo del valor medio.

Función

Un caso típico de aplicación para este parámetro es la supresión de valores de corriente de pico al arrancar motores potentes que, en caso de no hacerse, se notificarían como fallo al punto de control.

La transmisión de un valor analógico que se encuentra en el rango de desbordamiento por exceso ($7FFF_h$) o defecto (8000_h) se suprime mientras dure el intervalo de tiempo indicado.

Una vez transcurrido el tiempo de supresión de errores se transmitirá el valor de $7FFF_h$ o 8000_h, siempre que siga pendiente.

Si el valor vuelve a entrar en el rango asignado antes de que transcurra el tiempo de supresión de errores se transferirá el valor actual.

Módulos de entrada

La supresión está ajustada a valores analógicos que son captados directamente como valores brutos por los módulos de entradas analógicas S7. Dichos módulos suministran para todas las áreas de entrada los valores citados para el rango de desbordamiento por exceso y defecto, incluso para entradas Life Zero.

Un valor analógico en el rango de desbordamiento por exceso (32767 / $7FFF_h$) o defecto (-32768 / 8000_h) no se transfiere mientras dure el tiempo de supresión de errores. Lo mismo es válido para entradas Life Zero. Una vez transcurrido el tiempo de supresión de errores se transferirá el valor en el rango de desbordamiento por exceso o defecto, siempre que siga pendiente.

Recomendación para valores listos que han sido preprocesados por la CPU:

Si en el área de marcas o en un bloque de datos se preparan valores listos preprocesados por la CPU, solo es posible o aconsejable una supresión cuando los valores listos también adoptan los valores citados de 32767 / $7FFF_h$ o -32768 / 8000_h en el rango de desbordamiento por exceso o defecto, respectivamente. En caso contrario, no debería configurarse el parámetro para valores preprocesados.

Los valores de desbordamiento por exceso y defecto pueden asignarse libremente para valores listos preprocesados en la CPU.

Factor de filtrado

Requisitos para la función

Configuración del disparo de valor umbral para este punto de datos

Restricciones

El factor de filtrado no puede configurarse simultáneamente con el cálculo del valor medio. Un valor configurados deja de tener efecto en el momento de activarse el cálculo del valor medio.

Función

Los valores analógicos que sufren oscilaciones rápidas pueden estabilizarse utilizando la función de filtrado.

Los factores de filtrado se calculan siguiendo la fórmula siguiente, igual que en los módulos de entradas analógicas S7.

$$y_n = \frac{x_n + (k-1)y_{n-1}}{k}$$

siendo
y_n = valor filtrado en el ciclo actual n

x_n = valor captado en el ciclo actual n
k = factor de filtrado

Los valores siguientes pueden configurarse como factor de filtrado para el módulo.

- 1 = sin filtrado
- 4 = filtrado débil
- 32 = filtrado medio
- 64 = filtrado fuerte

Establecer valor límite 'bajo' / Establecer valor límite 'alto'

Requisitos para la función

- Configuración del disparo de valor umbral para este punto de datos
- Variable PLC en el área de operandos de marcas o datos

  El punto de datos de valor analógico debe estar enlazado con una variable PLC en el área de marcas o datos (bloque de datos). Para variables PLC de módulos de hardware (área de operandos de entrada) no es posible la configuración de valores límite.

Para valores medidos que ya se han preprocesado en la CPU, no tiene sentido configurar valores límite.

Función

En estos dos campos de entrada existe la posibilidad de establecer un valor límite en el sentido del principio del rango de medición o en el sentido del fin de rango de medición. Así, por ejemplo, los valores límite pueden evaluarse también como principio del rango de medición o fin del rango de medición.

Identificación de estado "OVER_RANGE"

Cuando se rebasa por defecto o exceso un valor límite se activa la identificación de estado "OVER_RANGE" del punto de datos. Las identificaciones de estado se describen en el capítulo Identificaciones de estado de los puntos de datos (Página 69).

El bit "OVER_RANGE" de la identificación de estado del punto de datos se activa cuando se transfiere el valor analógico correspondiente, de la forma siguiente:

- Valor límite "alto":
  - Cuando se rebasa por exceso el valor límite: OVER_RANGE = 1
  - Cuando seguidamente se rebasa por defecto el valor límite: OVER_RANGE = 0
- Valor límite "bajo":
  - Cuando se rebasa por defecto el valor límite: OVER_RANGE = 1
  - Cuando seguidamente se rebasa por exceso el valor límite: OVER_RANGE = 0

Configuración del valor límite

El valor límite se configura como número decimal entero. El rango de valores se orienta en el rango del valor bruto de módulos de entradas analógicas.

Rango	Valor bruto (16 bits) de las variables PLC		Salida del módulo [mA]			Rango de medición [%]
	Decimal	Hexadecimal	0 .. 20 (unipolar)	-20 .. +20 (bipolar)	4 .. 20 (life zero)	
Rebase por exceso	32767	7FFF	> 23,515	> 23,515	> 22,810	> 117,593
Rango de saturación por encima	32511 ... 27649	7EFF ... 6C01	23,515 ... 20,001	23,515 ... 20,001	22,810 ... 20,001	117,593 ... 100,004
Rango nominal (unipolar / life zero)	27648 ... 0	6C00 ... 0000	20 ... 0		20 ... 4	100 ... 0
Rango nominal (bipolar)	27648 ... 0 ... -27648	6C00 ... 0000 9400		20 ... 0 ... -20		100 ... 0 ... -100
Rango de saturación por debajo (unipolar / life zero)	-1 ... -4864	FFFF ... ED00	-0,001 ... -3,518		3,999 ... 1,185	-0,004 ... -17,59
Rango de saturación por debajo (bipolar)	-27649 ... -32512	93FF ... 8100		-20,001 ... -23,516		-100,004 ... -117,593
Rebase por defecto / rotura de hilo	-32768	8000	< -3,518		< 1,185	< -17,593

Nota

Evaluación del valor con la opción desactivada

Si se activa una o las dos opciones, se configura un valor y, a continuación, se desactiva de nuevo la opción, el valor atenuado se evaluará de todos modos.

Para desactivar las dos opciones deben borrarse los valores límite configurados anteriormente de los campos de entrada y desactivar seguidamente la opción correspondiente.

Recomendación para valores analógicos que sufren oscilaciones rápidas:

Si el valor analógico sufre oscilaciones rápidas, en los valores límites configurados puede ser útil filtrar previamente el valor analógico.

4.5.8 Configuración de mensajes

Configuración de correos electrónicos

En eventos importantes, el CP puede enviar correos electrónicos a un interlocutor de la comunicación.

La configuración de los mensajes de correo electrónico se realiza en el editor de configuración de puntos de datos y mensajes de STEP 7. La encontrará en el árbol del proyecto:

Proyecto > Directorio de la estación correspondiente > Módulos locales > CP

Respecto a la vista en STEP 7 consulte el capítulo Configuración de los puntos de datos (Página 59).

Requisitos e información necesaria

Tenga en cuenta los requisitos siguientes en la configuración del CP para la transferencia de correos electrónicos:

- Activación de la comunicación por Telecontrol (grupo de parámetros "Tipos de comunicación")
- Configuración del grupo de parámetros "Configuración de correo electrónico" (consulte el grupo de parámetros "Security")

  Para ello se requiere la información siguiente:

  – Datos de acceso del servidor SMTP: dirección, número de puerto, nombre de usuario y contraseña

  – Dirección de correo electrónico del destinatario

Disparo: Iniciar la transferencia de correos electrónicos

A través del grupo de parámetros "Disparo" de la tabla de mensajes se define a través de cuál de los siguientes eventos se activa el envío del correo electrónico:

- La CPU pasa a STOP.
- La CPU pasa a RUN.
- La conexión con el interlocutor se interrumpe.
- La conexión con el interlocutor se establece (se recupera).
- Se lanza una señal de disparo.

  Como señal de disparo para la transmisión de correos electrónicos se evalúa el cambio de flanco (0 → 1) de un bit de disparo activado por el programa de usuario. En caso necesario es posible configurar un bit de disparo independiente para cada correo electrónico.

  Cuando el área de memoria del bit de disparo está en el área de marcas o en un bloque de datos, el bit de disparo se pone a cero al enviar el correo electrónico.

En el protocolo "TeleControl Basic" pueden configurarse los siguientes eventos adicionales como activadores de un correo electrónico:

- Error al establecer la conexión con el interlocutor.
- Se ha iniciado una sesión TeleService.
- Ha finalizado una sesión TeleService.

Enable Value Tag Transferir valor de una variable PLC con un mensaje

Si en el grupo de parámetros "Disparo" se activa la opción "Enable Value Tag", el CP envía un valor del área de memoria de la CPU junto con el mensaje, en el lugar que ocupa el comodín $$. Para ello, en el texto del mensaje se introduce "$$" como comodín del valor que se enviará.

Seleccione una variable PLC cuyo valor va a integrarse en el mensaje. El valor se coloca en lugar del comodín $$ dentro del texto del mensaje.

$$ puede ser un comodín para tipos de puntos de datos con tipo de datos simple hasta 32 bits de tamaño.

Activar identificación de estado de procesamiento

Si está opción está activada en STEP 7, en el CP se emite un estado que informa del estado de procesamiento del mensaje enviado. El estado se escribe en una variable PLC del tipo DWORD. Seleccione esta variable a través del campo "Variable PLC para estado de procesamiento".

Si hay problemas con la entrega de los mensajes, se puede definir el estado p. ej. a través del servidor web de la CPU, visualizando en él el valor de la variable PLC.

Respecto al significado de los diferentes estados, consulte el capítulo Estado de edición de los correos electrónicos de Telecontrol (Página 106).

4.5.9 Security > Identificación del CP

Identificación del CP

Solo válido para CPs con uso del protocolo "TeleControl Basic".

- Número de proyecto

  El número de proyecto es el mismo para todos los CPs de Telecontrol de un proyecto STEP 7. TCSB evalúa los números de proyecto comprendidos entre 1 y 2000. Si se cambia el número de proyecto, este parámetro cambia en todos los CPs del proyecto STEP 7.

- Número de estación

  Para cada estación con CP de Telecontrol se configura un número de estación individual. TCSB evalúa los números de estación comprendidos entre 1 y 8000.

- Contraseña de Telecontrol

  Contraseña para autenticación del CP en el servidor de Telecontrol. 8 a 29 caracteres del juego de caracteres ASCII 0x20...0x7e. La contraseña puede ser la misma para todos los CPs del proyecto de STEP 7.

  La misma contraseña se configura en la aplicación "TCSB" para esta estación.

4.5.10 Security > Opciones de seguridad DNP3

Autenticación y cambio de clave en el protocolo DNP3

Con las funciones Security activadas el maestro y la estación (CP) se autentifican con una clave secreta, la pre-shared key.

Con la pre-shared key común, tras el primer establecimiento de conexión entre el maestro y el CP se acuerdan claves de sesión que se renuevan cíclicamente a partir de entonces. Por norma general, la iniciativa para renovar la clave de sesión la toma el maestro. Los criterios para renovar las claves se definen en los parámetros siguientes.

- Solicitudes de autenticación previas al cambio de clave
- Intervalo de cambio de clave

En cuanto se cumple una de estas dos condiciones se renueva la clave de sesión.

Opciones de seguridad DNP3

- **Activar opciones de seguridad DNP3**

  Método con el que se autentica el CP ante el maestro.

  – Desactivado

    Autenticación no segura: Si se selecciona esta opción, el CP inicia sesión utilizando únicamente su dirección de estación.

  – Activado

    Autenticación segura: Si se selecciona esta opción el CP y el maestro utilizan los mecanismos de Security DNP3. Los parámetros se configuran a continuación.

- **Modo IKE**

  Selección del modo de cambio de clave (IKE).

  – El modo predeterminado es Main Mode.

  – El Aggressive Mode es un poco más rápido pero transfiere la identidad sin codificar.

- **Estadísticas de seguridad**

  Indica si se envían al maestro las estadísticas de los eventos de seguridad. Los eventos de seguridad son solicitudes de autenticación para el CP. Si se activa esta opción, todas las solicitudes de autenticación se guardarán en el CP con fecha, hora y resultado y se enviarán al maestro para su posterior evaluación.

- **Enclavamiento SHA-1**

  Determina si el CP está autorizado a utilizar el algoritmo Secure Hash SHA-1 cuando se ha configurado "SHA-256" como algoritmo Secure Hash y el maestro no soporta SHA-256. Significado de las opciones:

  – Modo SHA-1 permitido

    El CP puede utilizar SHA-1 cuando el maestro no soporta SHA-256.

  – Modo SHA-1 no permitido

    El CP no puede utilizar SHA-1.

    Tenga en cuenta lo siguiente: Si el maestro no soporta SHA-256, con esta opción activada no se lleva a término la conexión.

- **Algoritmo Secure Hash**

  Selección del Secure Hash Algorithm (SHA). Posibilidades de selección:

  – SHA-1

  – SHA-256

- **Algoritmo Key Wrap**

  Selección del Advanced Encryption Standard (AES). Posibilidades de selección:

  – AES-128

  – AES-256

- **Longitud de clave**

  Longitud de la pre-shared key en bytes

  En función del algoritmo key wrap se utilizan las longitudes siguientes:

  – Para AES-128: 16 bytes

  – Para AES-256: 32 bytes

- Número máx. de solicitudes de cambio de clave

  La función está desactivada.

- **Solicitudes de autenticación previas al cambio de clave**

  Número máximo de solicitudes de autenticación del CP al maestro antes de que se renueve la clave de sesión.

  Si se introduce el valor 0 (cero) se desactiva la función y la clave de la sesión solo se renueva conforme al intervalo de cambio de clave.

  Recomendación: En el CP, ajuste un número que sea el doble de grande que el del maestro.

- **Intervalo de cambio de clave**

  Período tras el cual volverá a intercambiarse la clave de sesión entre el CP y el maestro.

  Si se introduce el valor 0 (cero) se desactiva la función y la clave nunca de renueva.

  El intervalo debe sintonizarse en ambos interlocutores.

- **Tiempo de vigilancia de autenticación**

  Tiempo de espera máximo (segundos) hasta recibir la respuesta del maestro a una solicitud de autenticación del CP.

  Si se rebasa por exceso el tiempo de espera, el CP lo evalúa como un error. En ese caso, el CP genera un evento deSecurity y lo envía al maestro.

  Rango de valores: 1 ... 65535

- **Pre-shared Key**

  La pre-shared key del CP debe ser idéntica a la pre-shared key utilizada por el maestro.

  La clave debe coincidir con la longitud de clave configurada arriba (2 caracteres por byte).

  La pre-shared key puede configurarse de dos formas:

  – Configuración manual

    Introduzca manualmente la pre-shared key en formato de valor hexadecimal.

  – Importación en formato de archivo

    Importe la pre-shared key desde el sistema de archivos de la estación de ingeniería si ha sido generada por el maestro u otro sistema.

4.5.11 Security > Configuración de correo electrónico

Configuración de correo electrónico

- **Ninguna configuración**

  En el ajuste predeterminado está desactivado el envío de correo electrónico.

- **Activar SMTP**

  Active esta opción para utilizar el envío no cifrada de correo electrónico a través del puerto SMTP 25.

- **Activar SSL/TLS**

  Si el operador del servicio de correo electrónico solo soporta la transmisión cifrada, active esta opción: El protocolo se selecciona a través del número de puerto:

  – N.º de puerto 587

    El CP envía correos electrónicos cifrados usando STARTTLS.

  – N.º de puerto 465

    El CP envía correos electrónicos cifrados usando SSL/TLS (SMTPS).

  Pregunte al operador del servicio de correo electrónico cuál es la opción compatible.

  Para utilizar una conexión de Internet con infraestructura IPv6, observe la indicación del capítulo IPv6 (Página 43).

4.6 Configuración de seguridad (CP 1543SP-1)

4.6.1 VPN

4.6.1.1 VPN (Virtual Private Network)

Túnel VPN

Virtual Private Network (VPN) es una tecnología para el transporte seguro de datos confidenciales por redes IP públicas, por ejemplo Internet. Con VPN se establece y se utiliza una conexión segura (túnel) entre dos sistemas TI o redes seguros, sorteando de este modo una red insegura.

El túnel VPN se caracteriza por reenviar la totalidad de los telegramas, incluso de protocolos de capas superiores (HTTP, FTP, etc.).

El tráfico de datos entre dos componentes de la red se transporta de forma prácticamente ilimitada a través de otra red. De este modo es posible conectar redes completas entre sí, traspasando una red adyacente o intercalada.

Propiedades

- VPN crea una subred lógica que se incrusta en una red adyacente (asignada). Aunque VPN aprovecha los mecanismos de direccionamiento habituales de la red asignada, desde el punto de vista del procesamiento de datos transporta telegramas propios y, por lo tanto, trabaja de forma independiente al resto de esa red.
- VPN permite la comunicación de los interlocutores VPN que contiene con la red asignada.
- VPN se basa en una tecnología de túnel y se puede configurar de forma individual.
- La comunicación a prueba de escuchas y de manipulaciones entre los interlocutores VPN queda asegurada por el uso de contraseñas, claves públicas y un certificado digital (autenticación).

Ámbitos de aplicación/uso

- Las redes locales se pueden conectar entre sí de forma segura por Internet (conexión "site-to-site").
- Acceso seguro a una red corporativa (conexión "end-to-site")
- Acceso seguro a un servidor (conexión "end-to-end")
- Comunicación entre dos servidores sin que pueda ser vista por terceros (conexión "end-to-end" o "host-to-host")
- Garantía de seguridad de la información en instalaciones conectadas en red en el campo de la automatización

- Protección de sistemas de ordenadores y de la respectiva comunicación de datos dentro de una red de automatización o del acceso remoto seguro a través de Internet.
- Accesos remotos seguros desde el PC/la programadora a redes o autómatas programables protegidos por módulos de seguridad, más allá de las redes públicas.

Concepto de protección de células

Industrial Ethernet Security permite proteger diferentes dispositivos o segmentos de una red Ethernet:

- Se permite el acceso a dispositivos y segmentos de red concretos protegidos por módulos de seguridad.
- Posibilidad de conexiones seguras a través de topologías de red no seguras.

Gracias a la combinación de distintas medidas de seguridad, como cortafuegos, routers NAT/NAPT y VPN por túnel IPsec, los módulos de seguridad protegen de:

- Espionaje de datos
- Manipulación de datos
- Accesos no deseados

4.6.1.2 Creación de túneles VPN para la comunicación S7 entre estaciones

Requisitos

A la hora de crear un túnel VPN para la comunicación S7 entre dos estaciones S7, o entre una estación S7 y una estación de ingeniería con CP de seguridad (como CP 1628), se deben cumplir los siguientes requisitos:

- Se han configurado las dos estaciones.
- Los CP de ambas estaciones deben soportar funciones de seguridad.
- Las interfaces Ethernet de ambas estaciones se encuentran en la misma subred.

Nota

Posibilidad de comunicación también por router IP

La comunicación entre las dos estaciones también es posible mediante un router IP. Sin embargo, para esta vía de comunicación es preciso realizar ajustes adicionales.

Procedimiento

Para crear un túnel VPN hay que ejecutar los pasos siguientes:

1. Creación de un usuario de seguridad

   Si el usuario de seguridad ya está creado: Iniciar la sesión como usuario.
2. Seleccionar la casilla de control "Activar funciones de seguridad"

3. Creación de un grupo VPN y asignación de módulos de seguridad
4. Configurar las propiedades del grupo VPN
5. Configurar las propiedades VPN locales de los dos CP

La descripción exacta de cada uno de los pasos figura en los apartados siguientes de este capítulo.

Creación de un usuario de seguridad

Para crear un túnel VPN se necesitan los derechos de configuración pertinentes. Para activar las funciones de seguridad es preciso crear al menos un usuario de seguridad.

1. Haga clic en los ajustes de seguridad locales del CP, en el botón "Inicio de sesión de usuario".

   Resultado: Se abre una ventana nueva.
2. Escriba el nombre de usuario, la contraseña y la confirmación de la contraseña.
3. Haga clic en el botón "Iniciar sesión".

   Ha creado un nuevo usuario de seguridad. Ahora ya tiene disponibles las funciones de seguridad.

En todos demás inicios de sesión, inicie la sesión como usuario.

Seleccionar la casilla de control "Activar funciones de seguridad"

Tras iniciar sesión, en la configuración de ambos CP debe seleccionar la casilla de control "Activar funciones de seguridad".

Ahora dispone de funciones de seguridad para ambos CP.

Creación de un grupo VPN y asignación de módulos de seguridad

1. En los ajustes de seguridad globales, elija la entrada "Cortafuegos" > "Grupos VPN" > "Agregar nuevo grupo VPN".
2. Haga doble clic en la entrada "Agregar nuevo grupo VPN" para crear un grupo VPN.

   Resultado: Debajo de la entrada seleccionada se muestra un nuevo grupo VPN.
3. Haga doble clic en la entrada "Grupos VPN" > "Asignar módulo a un grupo VPN" de los ajustes Security globales.
4. Asigne al grupo VPN los módulos de seguridad entre los cuales se va a crear el túnel VPN.

Nota

Fecha y hora actuales en CP para las conexiones VPN

Por norma general, para establecer una conexión VPN con el consiguiente reconocimiento de los certificados intercambiados, será necesario establecer la fecha y hora actuales en ambas estaciones.

Configurar las propiedades del grupo VPN

1. Haga doble clic en el grupo VPN recién creado.

   Resultado: las propiedades del grupo VPN se muestran en "Autenticación".

2. Asigne un nombre el grupo VPN. En las propiedades, configure los ajustes del grupo VPN.

   Estas propiedades definen los ajustes predeterminados del grupo VPN, los cuales pueden modificarse en cualquier momento.

Nota

Definición de las propiedades VPN de los CP

Las propiedades VPN de los CP se definen en el grupo de parámetros "Security" > "Cortafuegos" > "VPN" del módulo correspondiente.

Resultado

Ha creado un túnel VPN. El cortafuegos de los CP se activa de forma automática: La casilla de control "Activar cortafuegos" se activa automáticamente cuando se crea un grupo VPN. No es posible desactivar esta casilla de control.

Cargue la configuración en todos los módulos pertenecientes al grupo VPN.

4.6.1.3 Comunicación VPN con SOFTNET Security Client (estación de ingeniería)

La comunicación por túnel VPN solo tiene éxito con la estación interna desactivada

En determinadas condiciones, el establecimiento de una comunicación por túnel VPN entre SOFTNET Security Client y el CP no tiene éxito.

SOFTNET Security Client también intenta establecer una comunicación por túnel VPN con una estación interna subordinada. Este establecimiento de comunicación con un dispositivo no presente impide el establecimiento de comunicación con el CP.

Para establecer correctamente una comunicación por túnel VPN con el CP, deben desactivarse los dispositivos internos.

El siguiente procedimiento de desactivación de la estación solo debe aplicarse si se produce el problema descrito.

Desactive la estación en la vista general del túnel SOFTNET Security Client:

1. Quite la marca de la casilla de control "Enable active learning".

   Por el momento, la estación subordinada desaparece de la lista de túneles.

2. Seleccione la conexión deseada con el CP en la lista de túneles.
3. Seleccione mediante el botón derecho del ratón "Enable all Members" en el menú contextual.

   La estación subordinada aparece temporalmente de nuevo en la lista de túneles.

4. Seleccione la estación subordinada de la lista de túneles.
5. Seleccione "Delete Entry" mediante el botón derecho del ratón en el menú contextual.

Resultado: la estación subordinada está desactivada definitivamente. El establecimiento de una comunicación por túnel VPN con el CP tiene éxito.

4.6.1.4 Establecimiento de la comunicación por túnel VPN entre CP y SCALANCE M

Cree un túnel VPN entre el CP y un router SCALANCE M de acuerdo con el procedimiento descrito para las estaciones.

Solo si en los ajustes globales de seguridad del grupo VPN creado ("Grupos VPN > Autenticación") se ha seleccionado la casilla de control "Perfect Forward Secrecy", se establece una comunicación por túnel VPN.

Si la casilla de control no está seleccionada, el CP rechaza el establecimiento de la conexión.

4.6.1.5 CP como dispositivo pasivo de conexiones VPN

Ajustar el permiso para establecer conexiones VPN en dispositivos pasivos

Si el CP está conectado a otro dispositivo VPN a través de una pasarela y dicho CP es un dispositivo pasivo, el permiso para establecer conexiones VPN debe ajustarse en "Responder".

Este caso se da en la siguiente configuración típica:

dispositivo VPN (activo) ⇔ pasarela (dirección IP din.) ⇔ Internet ⇔ pasarela (dirección IP fija) ⇔ CP (pasivo)

El permiso para establecer conexiones VPN por parte del CP como dispositivo pasivo se configura del siguiente modo:

1. Vaya a la vista de dispositivos y redes de STEP 7.
2. Seleccione el CP.
3. En los ajustes locales de seguridad abra el grupo de parámetros "VPN".
4. Para cada conexión VPN que tenga el CP como dispositivo VPN pasivo, cambie el ajuste estándar "Initiator/Responder" por el ajuste "Responder".

4.6.2 Cortafuegos

4.6.2.1 Comprobación priorizada de telegramas mediante el cortafuegos MAC

Cada telegrama entrante o saliente atraviesa primero el cortafuegos MAC (capa 2) Si el telegrama se rechaza ya en este nivel, el cortafuegos de IP (capa 3) no lo comprueba de forma adicional. Así es posible limitar o bloquear la comunicación IP por medio de las reglas de cortafuegos MAC oportunas.

4.6.2.2 Diagnóstico online y carga a la estación con cortafuegos activado

Modo de proceder para configurar el cortafuegos

Si está activada la función de seguridad, proceda del siguiente modo:

1. En los ajustes Security globales (consulte el árbol del proyecto), elija la entrada "Cortafuegos > Servicios > Definir servicios para las reglas IP".
2. Elija la ficha "ICMP".
3. Agregue una nueva entrada de tipo "Echo Reply" y otra de tipo "Echo Request".
4. A continuación, seleccione el CP en la estación ET200SP.
5. En los ajustes Security locales del CP, active el modo avanzado del cortafuegos en el grupo de parámetros "Security > Cortafuegos".
6. Abra el grupo de parámetros "Reglas IP".
7. Agregue en la tabla una nueva regla IP para cada servicio creado previamente en los ajustes globales. Proceda del siguiente modo:
   - Acción: Allow; "De externo -> A estación" con el servicio global "Echo Request"
   - Acción: Allow; "De estación -> A externo" con el servicio global "Echo Reply"
8. Introduzca la dirección IP de la PG/el PC en "Dirección IP de origen" para la regla IP relacionada con el Echo Request. De este modo se consigue que los telegramas PING solo puedan pasar el cortafuegos desde la PG/el PC.

4.6.2.3 Notación de la dirección IP de origen (modo de cortafuegos avanzado)

Si indica un área de direccionamiento en los ajustes avanzados del cortafuegos del CP en la dirección IP de origen, tenga en cuenta la notación correcta:

- Separe las dos direcciones IP únicamente con un guion.

  Correcto: 192.168.10.0-192.168.10.255
- No introduzca ningún otro carácter entre ambas direcciones IP.

  Incorrecto: 192.168.10.0 - 192.168.10.255

Si introduce el área de forma incorrecta, no se aplica la regla de cortafuegos.

4.6.2.4 Ajustes del cortafuegos para conexiones S7 a través de túnel VPN

Reglas IP en modo de cortafuegos avanzado

Si se configuran conexiones (S7, OUC) con túnel VPN entre el CP y un interlocutor, hay que adaptar los ajustes de cortafuegos locales del CP:

Para las conexiones, en el modo de cortafuegos avanzado ("Security > Cortafuegos > Reglas IP") seleccione la acción "Allow*" en ambos sentidos de comunicación del túnel VPN.

4.6.3 Filtrado de los eventos de sistema

Problemas de comunicación con valores demasiado elevados para el filtrado de eventos del sistema

Si el valor ajustado para el filtrado de los eventos del sistema es demasiado elevado, es posible que no pueda usar el volumen de prestaciones máximo de la comunicación. La elevada cantidad de mensajes de error emitidos puede retardar o impedir el procesamiento de los enlaces de comunicación.

En "Security > Ajustes de registro > Configurar eventos del sistema", ajuste el parámetro "Nivel:" al valor "3 (Error)" para garantizar el diseño seguro de los enlaces de comunicación.

4.7 Tabla "Administrador de certificados" (CP 1542SP-1 IRC, CP 1543SP-1)

Con las funciones Securityen el proyecto STEP 7 se generan automáticamente los certificados necesarios para todos los módulos Security afectados, por ejemplo para poder comunicarse a través de conexiones VPN.

Los certificados generados por STEP 7, como los certificados SSL o los certificados de grupos VPN, se asignan automáticamente a los módulos correspondientes y no deben asignarse a estos mediante los ajustes de seguridad locales.

El Administrador de certificados local

Los certificados que han sido importados mediante el administrador de certificados en los ajustes de seguridad globales no se asignan automáticamente a los módulos correspondientes. Los certificados importados deben transferirse manualmente mediante la entrada "Administrador de certificados" en los ajustesSecurity locales a la lista de los certificados de interlocutor de confianza. Cuando se asigna un certificado CA también se asignan al módulo los certificados derivados.

Grupo de parámetros "Security" > tabla "Administrador de certificados"

A través del Administrador de certificados local se asignan al CP certificados para determinados servicios (p. ej. el envío seguro de correos electrónicos).

1. Para ello haga clic en la celda "Agregar nuevo" de la tabla.
2. Haga clic en el botón "..." sobre fondo blanco
3. En la lista de certificados que se abre, inserte un certificado nuevo con el botón "Agregar" o seleccione un certificado existente en el proyecto colocando la marca de verificación.

   El tipo y las propiedades de los certificados mostrados puede verse en el administrador de certificados global.

Certificados para el CP 1542SP-1 IRC

Requisitos en los ajustes Security globales

Importe al administrador de certificados el certificado del proveedor de servicios de correo electrónico para el envío seguro de correo electrónico.

Asignar certificados en la configuración de CPs

Seleccione el siguiente certificado en la configuración del CP:

- Tabla "Certificados de cliente de confianza":

  El certificado del proveedor de servicios de correo electrónico

Certificados para el CP 1543SP-1

Antes de poder referenciar certificados en bloques de programa para la Secure Communication hay que asignarlos al módulo Security como certificados de dispositivo a través del administrador de certificados.

Requisitos en los ajustes Security globales

Para poder asignar al CP certificados de un interlocutor hay que importar primero los certificados del interlocutor en el administrador de certificados global (Ajustes Security globales).

Para dar a conocer el certificado asignado al módulo interlocutor, es necesario incluirlo en la lista de certificados de interlocutor de confianza después de la importación.

Asignar certificados en la configuración de CPs

Seleccione los siguientes certificados en la configuración del CP:

- Tabla "Certificados de dispositivo":

  El certificado de dispositivo del CP generado por el proyecto STEP 7

- Tabla "Certificados de los dispositivos interlocutores":

  El certificado importado del interlocutor

Programación (OUC) 5

5.1 Bloques de programa para OUC

Uso de los bloques de programa para la Open User Communication (OUC)

Las conexiones de la Open User Communication no se configuran.

Para la comunicación TCP/UDP/ISO-on-TCP a través de Ethernet se utilizan los bloques de Open User Communication (OUC) indicados a continuación. Para ello se crean los bloques de programa correspondientes. Encontrará más detalles sobre los bloques de programa en el sistema de información de STEP 7.

Nota

Diferentes versiones de los bloques de programa

Tenga en cuenta que en STEP 7 no es posible utilizar en una misma estación versiones diferentes de un bloque de programa.

Bloques de programa soportados para OUC

Bloques de programa para los tres tipos de CP

Las instrucciones siguientes en la versión mínima indicada están disponibles para la programación de la Open User Communication para los tres tipos de CP:

- **TSEND_C V3.0 / TRCV_C V3.1**

  Bloques compactos para el establecimiento y la desconexión de conexiones, así como para el envío y la recepción de datos.

  o bien

- **TCON V4.0 / TDISCON V2.1**

  Establecer / deshacer la conexión

- **TUSEND V4.0 / TURCV V4.0**

  Enviar y recibir datos mediante UDP

- **TSEND V4.0 / TRCV V4.0**

  Enviar y recibir datos mediante TCP o ISO-on-TCP

- **TMAIL_C V4.0**

  Enviar correos electrónicos

Los bloques de programa se encuentran en la ventana "Instrucciones > Comunicación > Open User Communication" de STEP 7.

Descripciones de conexiones en tipos de datos del sistema (SDTs)

Para la correspondiente descripción de la conexión, los bloques citados anteriormente utilizan el parámetro CONNECT (o MAIL_ADDR_PARAM para TMAIL_C). La descripción de la conexión se deposita en un bloque de datos cuya estructura se define mediante un tipo de datos del sistema (SDT).

Crear un SDT para los bloques de datos

El SDT necesario para cada descripción de conexión se crea como bloque de datos. El tipo SDT se genera introduciendo manualmente en STEP 7 el nombre (p. ej. "TCON_Param"), en el campo "Tipo de datos" de la tabla de declaración del bloque, en lugar de seleccionar una entrada de la lista desplegable "Tipo de datos". Entonces se crea el SDT correspondiente con sus parámetros.

Dependiendo de las funciones Security soportadas, los tres tipos de CPs soportarán los siguientes SDTs:

SDTs para los tres tipos de CP

Los siguientes SDTs pueden ser utilizados por los tres tipos de CP:

- TCON_Param

  Para la transferencia de telegramas vía TCP

- TADDR_Param

  Para la transferencia de telegramas vía UDP

- TCON_IP_RFC

  Para la transferencia de telegramas vía ISO-on-TCP

- TMail_V4

  Para la transferencia de correos electrónicos con direccionamiento del servidor de correo electrónico a través de una dirección IPv4

- TMail_V6

  Para la transferencia de correos electrónicos con direccionamiento del servidor de correo electrónico a través de una dirección IPv6

- TMail_FQDN

  Para la transferencia de correos electrónicos con direccionamiento del servidor de correo electrónico a través del nombre de host

Encontrará la descripción de los SDTs con sus parámetros en el sistema de información de STEP 7, bajo el nombre del SDT.

SDT para CP 1542SP-1 IRC y CP 1543SP-1

Estos dos tipos de CP pueden utilizar el siguiente SDT para conexiones de correo electrónico con función Security:

- TMail_V4_SEC

  Para la transferencia segura de correos electrónicos con direccionamiento del servidor de correo electrónico a través de una dirección IPv4

- TMail_QDN_SEC

  Para la transferencia segura de correos electrónicos con direccionamiento del servidor de correo electrónico a través del nombre de host

SDT solo para CP 1543SP-1

El CP 1543SP-1 puede utilizar el siguiente SDT para la transmisión de datos con función Security:

- TCON_IP_V4_SEC

  Para la transmisión segura de datos a través de TCP

Establecer y deshacer la conexión

Con el bloque de programa TCON se establecen conexiones. Tenga en cuenta que para cada conexión se debe llamar a un bloque de programa TCON propio.

Para cada interlocutor se deberá establecer una conexión propia aunque se envíen bloques de datos idénticos.

Cuando se hayan transmitido los datos, se podrá desconectar la conexión. Una conexión se desconecta llamando a la instrucción TDISCON.

Nota

Cancelación de la conexión

Si una conexión existente es cancelada por el interlocutor o se interrumpe por interferencias en la red, también se deberá desconectar la conexión llamando a la instrucción TDISCON. Tenga esto en cuenta durante la programación.

Diagnóstico y mantenimiento 6

6.1 Posibilidades de diagnóstico

Están disponibles las siguientes posibilidades de diagnóstico.

LEDs del módulo

Encontrará información sobre los indicadores LED en el capítulo LEDs (Página 25).

STEP 7: La ficha "Diagnóstico" en la ventana de inspección

Aquí aparece la siguiente información sobre el módulo seleccionado:

- Entradas en el búfer de diagnóstico de la CPU
- Información sobre el estado online del módulo

STEP 7: Funciones de diagnóstico en el menú "Online > Online y diagnóstico"

Las funciones online permiten leer información de diagnóstico del CP desde una estación de ingeniería en la que esté guardado el proyecto con el CP. Se obtiene la siguiente información estática sobre el módulo seleccionado:

- Información general sobre el módulo
- Estado de diagnóstico
- Información sobre las interfaces del módulo

  Información sobre otras funciones del módulo

Para utilizar el diagnóstico online con la estación a través del CP, es imprescindible activar las funciones online en el grupo de parámetros "Tipos de comunicación", consulte el capítulo Tipos de comunicación (Página 46).

Para obtener más información sobre las funciones de diagnóstico de STEP 7, consulte el sistema de información de STEP 7.

Servidor web de la CPU

A través del CP se puede acceder al servidor web de la CPU y a la información disponible en él. Consulte el acceso en el capítulo Servidor web de la CPU (Página 104).

SNMP

Consulte las funciones en el capítulo Diagnóstico a través de SNMP (Página 102).

6.2 Diagnóstico a través de SNMP

Requisitos

Para el uso de SNMP es imprescindible activar la función en la configuración, consulte el capítulo SNMP (Página 45).

SNMP (Simple Network Management Protocol)

SNMP es un protocolo para el diagnóstico y la gestión de redes y dispositivos de la red. Para la transferencia de datos, SNMP utiliza el protocolo UDP sin conexión.

La información sobre las propiedades de los dispositivos aptos para SNMP está depositada en los archivos MIB (MIB = Management Information Base).

Encontrará información detallada sobre SNMP y Siemens Automation MIB en el manual /6/ (Página 124).

Prestaciones de los CPs

Los CPs soportan las siguientes versiones de SNMP:

- **CP 1542SP-1, CP 1542SP-1 IRC**
  - SNMPv1
- **CP 1543SP-1**
  - SNMPv1
  - SNMPv3 (con funciones Security activadas)

El CP no soporta "traps".

MIBs soportadas en SNMPv1

Los CPs soportan las siguientes MIBs:

- **MIB II (según RFC1213)**

  El CP soporta los siguientes grupos de objetos MIB:
  - System
  - Interfaces
  - IP
  - ICMP
  - TCP
  - UDP
  - SNMP
- **LLDP MIB**
- **Siemens Automation MIB**

  Tenga en cuenta los derechos de escritura en los objetos MIB, consulte el siguiente apartado (SNMPv3).

Objetos MIB soportados en SNMPv3

Con SNMPv3 activado el CP proporciona los contenidos de los siguientes objetos MIB:

- **MIB II (según RFC1213)**

  El CP soporta los siguientes grupos de objetos MIB:

  – System

  – Interfaces

    El objeto MIB "Interfaces" suministra información de estado sobre las interfaces del CP.

  – IP (IPv4/IPv6)

  – ICMP

  – TCP

  – UDP

  – SNMP

  Los siguientes grupos de MIB II estándar no se soportan:

  – Adress Translation (AT)

  – EGP

  – Transmission

- **LLDP MIB**
- **Siemens Automation MIB**

  Tenga en cuenta que los accesos de escritura se permiten solo para los siguientes objetos MIB del grupo "System":

  – sysContact

  – sysLocation

  – sysName

    Un sysName establecido se envía como nombre de host al servidor DHCP utilizando la opción DHCP 12 para el registro en un servidor DNS.

  Por motivos de seguridad, para todos los demás objetos MIB y grupos solo es posible el acceso de lectura.

Derechos de acceso vía Community Name (SNMPv1)

El CP utiliza los siguientes Community Strings para controlar los derechos de acceso al agente SNMP:

Tabla 6- 1 Derechos de acceso en agentes SNMP

Tipo de acceso	Community String *)
Acceso de lectura	public
Acceso de lectura y escritura	private

*) Tenga en cuenta la grafía en minúsculas.

6.3 Servidor web de la CPU

El servidor web de la CPU

La CPU tiene un servidor web al que se puede acceder desde una estación de ingeniería a través del CP vía HTTP/HTTPS.

El servidor web de la CPU ofrece múltiples funciones de diagnóstico y para fines de servicio, como por ejemplo la carga de archivos de firmware. Encontrará información detallada en el manual de sistema /2/ (Página 123) y en el sistema de información de STEP 7 bajo el título "Servidores web".

Requisitos para el acceso al servidor web

Navegadores web autorizados

Encontrará los navegadores web soportados en la estación de ingeniería para el acceso al servidor web de la CPU en el sistema de información de STEP 7, bajo el título "Servidores web".

Requisitos en la configuración de la CPU

1. Abra el proyecto correspondiente en la estación de ingeniería.
2. Seleccione la CPU de la estación correspondiente en STEP 7.
3. Seleccione la entrada "Servidor web".
4. Active en el grupo de parámetros "General" la opción "Activar servidor web en el módulo".
5. En la administración de usuarios cree un usuario en la CPU con los derechos correspondientes.

   Para cargar el firmware hay que asignar a ese usuario el derecho de realización de actualizaciones de firmware en el nivel de acceso.

   El nombre de usuario y la contraseña se requieren posteriormente para el acceso.
6. Configuración de la opción "Permitir acceso solo a través de HTTPS" en el grupo de parámetros "General"

   Dependiendo de si desea acceder al servidor web vía HTTP o vía HTTPS, la configuración del parámetro será diferente:

   – "Permitir acceso solo a través de HTTPS" activado

     La conexión solo puede establecerse a través de HTTPS.

   – "Permitir acceso solo a través de HTTPS" desactivado

     La conexión puede establecerse a través de HTTP y de HTTPS.

Requisitos adicionales en la configuración del CP 1543SP-1

Active el cortafuegos en el grupo de parámetros "Security".

Dependiendo del protocolo utilizado deberán realizarse los siguientes ajustes adicionales en el grupo de parámetros del cortafuegos "De externo a estación".

- En caso de establecimiento de conexión vía HTTP
  - Active la opción "Permitir HTTP"
  - Active la opción "Permitir HTTPS"
    Razón: después de la autenticación en el servidor web se conmuta a HTTPS.
- En caso de establecimiento de conexión vía HTTPS
  - Desactive la opción "Permitir HTTP"
  - Active la opción "Permitir HTTPS"

Establecer conexión con el servidor web

Proceda del siguiente modo para conectarse al servidor web de la CPU desde la estación de ingeniería.

Las dos variantes están descritas en los apartados siguientes.

Establecimiento de conexión vía HTTP

1. Utilice la interfaz Ethernet para conectar al CP el PC que tiene el nuevo archivo de firmware.
2. Introduzca la dirección del CP en el campo de direcciones de su navegador web: http://<dirección IP>
3. Pulse la tecla de entrada <Intro>.

   Se abre la página de inicio del servidor web.
4. Haga clic en la entrada "Certificado para descargar" en la parte superior derecha de la ventana.

   Se abre el cuadro de diálogo "Certificado".
5. Cargue el certificado en el PC haciendo clic en el botón "Instalar certificado ...".

   El certificado se carga en el PC.

   Encontrará información sobre la carga de un certificado en la ayuda del navegador web y en el sistema de información de STEP 7, en el título "Certificados para servidores web".

Si la conexión ha cambiado al modo seguro HTTPS ("https://<Dirección IP>/..." en el campo de dirección del servidor web), puede manejar el servidor web y, por ejemplo, cargar un archivo de firmware (consulte el apartado siguiente).

Si deshace la conexión con el servidor web, la próxima vez podrá iniciar sesión en el servidor web vía HTTP sin cargar el certificado.

Establecimiento de conexión vía HTTPS

1. Utilice la interfaz Ethernet para conectar al CP o la CPU el PC que tiene el nuevo archivo de firmware.
2. Introduzca la dirección del CP en el campo de direcciones de su navegador web: https://<dirección IP>
3. Pulse la tecla de entrada <Intro>.

   Se abre la página de inicio del servidor web.

El servidor web puede manejarse.

Carga de archivos de firmware del CP a través del servidor web de la CPU

Requisitos: El archivo de firmware nuevo está guardado en la estación de ingeniería.

1. Inicie sesión en la página de inicio del servidor web.
2. Tras el inicio de sesión, elija la entrada "Estado del módulo" en la navegación del servidor web.
3. Seleccione el CP en la lista de módulos.
4. Elija la ficha "Firmware" en la parte inferior de la ventana.
5. Busque el archivo de firmware en el PC pulsando el botón "Examinar..." y cargue el archivo en la estación utilizando el botón "Ejecutar actualización".

Observe las indicaciones del capítulo Cargar firmware (Página 108) referentes a la duración de la actualización de firmware.

6.4 Estado de edición de los correos electrónicos de Telecontrol

Configuración del estado de edición de correos electrónicos de Telecontrol (CP 1542SP-1 IRC)

Los siguientes identificadores de estado son válidos para correos electrónicos configurados a través del editor de mensajes del CP 1542SP-1 IRC, consulte el capítulo Configuración de mensajes (Página 83).

Los correos electrónicos enviados a través de bloques de programa de la Open User Communication devuelven otros estados a través del bloque (consulte la ayuda de los bloques).

Estado de edición de los correos electrónicos de Telecontrol

Los estados proporcionados de la "Variable PLC para el estado de edición" tienen el siguiente significado:

Tabla 6- 2 Significado de la identificación de estado en formato hexadecimal

Estado	Significado
0000	Transferencia concluida sin fallos
82xx	Otro mensaje de error del servidor de correo electrónico Excepto el "8" de la izquierda, el mensaje se corresponde con el número de error de tres cifras del protocolo SMTP.
8401	Ningún canal disponible. Posible causa: ya existe una conexión de correo electrónico a través del CP. No es posible crear una segunda conexión en paralelo.
8403	No se ha podido establecer ninguna conexión TCP/IP con el servidor SMTP.
8405	El servidor SMTP ha rechazado la solicitud de inicio de sesión.
8406	El cliente SMTP ha detectado un error SSL interno o un problema con la estructura del certificado.
8407	La solicitud para utilizar SSL se ha rechazado.
8408	El cliente no ha podido determinar ningún socket para establecer una conexión TCP/IP con el servidor de correo.
8409	No es posible escribir a través de la conexión. Posible causa: el interlocutor de la comunicación ha realizado un reset de la conexión o bien esta se ha interrumpido.
8410	No es posible leer a través de la conexión. Posible causa: el interlocutor de la comunicación ha cancelado la conexión o la conexión se ha interrumpido.
8411	Error al enviar el correo electrónico. Causa: no había suficiente memoria para llevar a cabo el proceso de transmisión.
8412	El servidor DNS configurado no ha podido descifrar el nombre de dominio indicado.
8413	Debido a un error interno en el subsistema DNS no ha sido posible descifrar el nombre de dominio.
8414	Se ha indicado una cadena de caracteres vacía como nombre de dominio.
8415	Se ha producido un error interno en el módulo Curl. Se ha cancelado la ejecución.
8416	Se ha producido un error interno en el módulo SMTP. Se ha cancelado la ejecución.
8417	Solicitud para SMTP en un canal ya utilizado o ID de canal no válido. Se ha cancelado la ejecución.
8418	Se ha cancelado la transmisión del correo electrónico. Posible causa: rebase por exceso del tiempo de ejecución.
8419	El canal se ha interrumpido y no puede utilizarse hasta que se cancele la conexión.
8420	No ha sido posible verificar la cadena de certificados del servidor con el certificado raíz del CP.
8421	Se ha producido un error interno. Se ha detenido la ejecución.
8450	Acción no ejecutada: bandeja de entrada no disponible / no accesible. Vuélvalo a intentar más adelante.
84xx	Otro mensaje de error del servidor de correo electrónico Excepto el "8" de la izquierda, el mensaje se corresponde con el número de error de tres cifras del protocolo SMTP.
8500	Error de sintaxis: comando desconocido. Esto incluye el error de una cadena de comandos demasiado larga. La causa puede ser que el servidor de correo electrónico no soporte el método de autenticación LOGIN. Intente enviar correos electrónicos sin autenticación (sin nombre de usuario).

Estado	Significado
8501	Error de sintaxis. Compruebe los siguientes datos de configuración: Configuración de avisos > Datos de correo electrónico (Content): • Dirección del destinatario ("Para" y "Cc").
8502	Error de sintaxis. Compruebe los siguientes datos de configuración: Configuración de avisos > Datos de correo electrónico (Content): • Dirección de correo electrónico (remitente)
8535	Autenticación SMTP incompleta. Compruebe los parámetros "Nombre de usuario" y "Contraseña" en la configuración del CP.
8550	No es posible acceder al servidor SMTP. No tiene derechos de acceso. Compruebe los siguientes datos de configuración: • Configuración del CP > Configuración de correo electrónico: – Nombre de usuario – Contraseña – Dirección de correo electrónico (remitente) • Configuración de avisos > Datos de correo electrónico (Content): – Dirección del destinatario ("Para" y "Cc").
8554	Transferencia fallida
85xx	Otro mensaje de error del servidor de correo electrónico Excepto el "8" de la izquierda, el mensaje se corresponde con el número de error de tres cifras del protocolo SMTP.

6.5 Cargar firmware

Nuevas versiones de firmware del CP

Cuando se disponga de una versión de firmware nueva para el CP, la encontrará en las páginas web de Siemens Industry Online Support:

Enlace: (https://support.industry.siemens.com/cs/ww/es/ps/22144/dl)

Enlace: (https://support.industry.siemens.com/cs/ww/es/ps/22143/dl)

Para cargar un archivo de firmware nuevo en el CP, tiene tres opciones a su disposición:

- Guardar el archivo de firmware en la Memory Card de la CPU

  Puede encontrar la descripción del proceso de carga en la Memory Card de la CPU en la página de Internet de Industry Online Support mencionada anteriormente.
- Cargar el firmware con las funciones online de STEP 7 a través de Ethernet/Internet

  A continuación encontrará la descripción de estos métodos.
- Carga de firmware a través del servidor web de la CPU

  Encontrará la descripción de estos métodos en el capítuloServidor web de la CPU (Página 104).

Nota

Duración de la actualización del firmware

El proceso de carga del nuevo archivo de firmware puede durar varios minutos.

Tenga en cuenta que la duración del proceso será mayor cuanto mayor sea la extensión de la estación con módulos de periferia.

Espere siempre hasta que los LEDs indiquen que la actualización de firmware ha concluido (estado de los LEDs "Solicitud de mantenimiento" - Fin de la actualización de firmware).

Cargar el firmware con las funciones online de STEP 7 a través de Ethernet/Internet

Requisitos:

- El CP o la CPU es accesible a través de la dirección IP.
- La estación de ingeniería y el CP se encuentran en la misma subred.
- El archivo de firmware nuevo está guardado en la estación de ingeniería.
- La estación de ingeniería está conectada a la red.
- El proyecto de STEP 7 correspondiente está abierto en la estación de ingeniería.

Procedimiento:

1. Seleccione el CP o la CPU de la estación cuyo CP desee actualizar con el firmware nuevo.
2. Active las funciones online mediante el símbolo "Conexión online".
3. Seleccione la interfaz Ethernet en el cuadro de diálogo "Conexión online", en la lista desplegable "Tipo de interfaz PG/PC".
4. Seleccione el slot del CP o de la CPU.

   Ambos métodos son válidos.
5. Haga clic en "Iniciar búsqueda" para buscar el módulo en la red y determinar la vía de conexión.

   Si el módulo se localiza, aparece en la tabla.
6. Use el botón "Conectar" para conectarse.

   El asistente "Conexión online" le guiará por los siguientes pasos.
7. Seleccione el CP en la vista de redes y elija el menú contextual "Online y diagnóstico" (botón derecho del ratón).
8. En la navegación de la vista Online y diagnóstico seleccione la entrada "Funciones > Actualizar firmware".

9. Busque el archivo de firmware nuevo en el sistema de archivos de la estación de ingeniería con ayuda del botón "Examinar" (grupo de parámetros "Cargador de firmware").
10. Inicie la carga del firmware con el botón "Iniciar actualización" si en el campo de indicación "Estado" se muestra la versión correcta del firmware firmado.

Puede obtener ayuda adicional acerca de las funciones online en el sistema de información de STEP 7.

6.6 Sustitución de módulos

⚠ PRECAUCIÓN

Lea el manual de sistema "Sistema de periferia descentralizada SIMATIC NET 200SP"

Antes de cualquier operación de montaje, conexión o puesta en servicio, lea los apartados correspondientes del manual de sistema "Sistema de periferia descentralizada SIMATIC NET 200SP" (consulte la bibliografía en el anexo).

Durante el montaje y la conexión proceda tal como se describe en el manual de sistema "Sistema de periferia descentralizada SIMATIC NET 200SP".

Asegúrese de que la tensión de alimentación está desconectada durante el montaje/desmontaje de los dispositivos.

Sustitución de módulos

Los datos de proyecto de STEP 7 del CP se almacenan en la CPU local correspondiente. Gracias a esto, en caso de recambio este CP se puede sustituir fácilmente, sin necesidad de volver a cargar los datos de configuración en la estación.

Al volver a arrancar la estación, el nuevo CP lee los datos de configuración de la CPU.

Datos técnicos

7

Datos técnicos		
Referencias	CP 1542SP-1	6GK7542-6UX00-0XE0
	CP 1542SP-1 IRC	6GK7542-6VX00-0XE0
	CP 1543SP-1	6GK7543-6WX00-0XE0
Conexión a Industrial Ethernet		
Número	1	
Ejecución	Slot para BusAdapter	
Propiedades	100BASE-TX, IEEE 802.3-2005, semidúplex/dúplex, autocrossover, autonegotiation, con separación galvánica	
Velocidad de transmisión	10/100 Mbits/s	
Longitudes de cable permitidas Ethernet, cobre, a 100 Mbits/s *		
Tipo de cable - cobre	Longitudes máx.	
TP Torsion Cable	• Máx. 55 m TP Torsion Cable con IE FC RJ45 Plug 180 • Máx. 45 m TP Torsion Cable con IE FC RJ45 + 10 m TP Cord mediante IE FC RJ45 Outlet	
TP FC Marine Cable, TP FC Trailing Cable, TP FC Flexible Cable, TP FC FRNC Cable, TP FC Festoon Cable, TP FC Food Cable	• Máx. 85 m TP FC Marine/Trailing/Flexible/FRNC/Festoon/Food Cable con IE FC RJ45 Plug 180 • Máx. 75 m TP FC Marine/Trailing/Flexible/FRNC/Festoon/Food Cable + 10 m TP Cord mediante IE FC RJ45 Outlet	
TP FC Standard Cable	• Máx. 100 m TP FC Standard Cable con IE FC RJ45 Plug 180 • Máx. 90 m TP FC Standard Cable + 10 m TP Cord mediante IE FC RJ45 Outlet	
Longitudes de cable permitidas Ethernet, fibra óptica (FO), a 100 Mbits/s *		
Tipo de cable - FO fibra de vidrio (multimodo):	Longitudes máx.	
• FO FRNC Cable GP, FO Standard Cable GP, FO Ground Cable, FO Trailing Cable, FO Trailing Cable GP, FO Robust Cable GP	• Máx. 2000 m	
• Cable interior INDOOR FO, cable estándar FO, cable de arrastre flexible FO	• Máx. 750 m	
• FO Robust Cable GP	• Máx. 2000 m	
Tipo de cable - FO PCF y de plástico	Longitudes máx.	
• POF Standard Cable GP 980/1000, POF Trailing Cable 980/1000	• Máx. 50 m	

Datos técnicos		
• PCF Standard Cable GP, PCF Trailing Cable, PCF Trailing Cable GP	• Máx. 100 m	
Datos eléctricos		
Alimentación externa (X80), tipo	Conector hembra Bloque de terminales para conector hembra	De dos polos con protección contra inversión de polaridad 2 de dos polos para alimentación sencilla o redundante
Tensión de alimentación (externa)	• Tipo de tensión • Límite inferior permitido • Límite superior permitido	• 24 V DC • 19,2 V • 28,8 V
Consumo de corriente	• De 24 V DC (externa) • De bus de fondo (3,3 V)	• 250 mA (típ.) • 4 mA (típ.)
Corriente de conexión máxima	(valor nominal)	12 A
Potencia activa disipada	(típico)	6 W
Categoría de sobretensión según IEC / EN 60664-1	Categoría I	
Condiciones ambientales admisibles		
Temperatura ambiente	Durante el servicio con el rack montado en horizontal	0 .. + 60 °C
	Durante el servicio con el rack montado en vertical	0 .. + 50 °C
	Durante el almacenamiento	-40 .. +70 °C
	Durante el transporte	-40 .. +70 °C
Humedad relativa	Durante el funcionamiento	≤ 95% a 25 °C, sin condensación
Forma, medidas y peso		
Formato del módulo	Módulos compactos ET 200SP	
Clase de protección	IP20	
Peso		
• Sin BusAdapter	• 180 g	
• Con BusAdapter 2xRJ45	• 230 g	
Dimensiones (an x al x p)	60 x 117 x 74 mm	
Posibilidades de montaje	Perfil DIN simétrico (35 mm)	
Mean Time Between Failures (MTBF)		
• Con + 40 °C	• 56,87 años	
• Con + 60 °C	• 24,78 años	
Funciones del producto **		

***** Consulte los detalles sobre las longitudes de cable en el manual de sistema del ET 200SP /2/ (Página 123).

****** Encontrará más propiedades y datos característicos en el capítulo Aplicación y funciones (Página 11).

Homologaciones

A

Homologaciones concedidas

Nota

Homologaciones otorgadas en la placa de características del dispositivo

Las homologaciones indicadas solo se consideran otorgadas si el producto está provisto de la correspondiente identificación. Las identificaciones de la placa de modelo indican cuál de las siguientes homologaciones se ha otorgado para su producto.

Campo de validez de las homologaciones

Las homologaciones indicadas a continuación son válidas para el CP.

Las comprobaciones necesarias para las homologaciones se han realizado con BusAdapter insertado.

Los BusAdapter cuentan con homologaciones propias, que no se describen aquí.

Declaración de conformidad CE

El CP cumple los requisitos y los objetivos en materia de seguridad de las directivas de la UE siguientes y, además, cumple las normas armonizadas europeas (EN) de autómatas que se mencionan en los documentos oficiales de la UE.

- **2014/34/UE (directiva de protección frente a explosiones ATEX)**

  Directiva del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, relativa a la aproximación de las legislaciones de los Estados miembros sobre los aparatos y sistemas de protección para uso en atmósferas potencialmente explosivas; boletín oficial de la UE L96, 29/03/2014, pág. 309-356

- **2014/30/UE (CEM)**

  Directiva CEM del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, relativa a la aproximación de las legislaciones de los Estados miembros en materia de compatibilidad electromagnética; boletín oficial de la UE L96, 29/03/2014, pág. 79-106

- **2011/65/UE (RoHS)**

  Directiva del Parlamento Europeo y del Consejo, de 8 de junio de 2011, sobre restricciones a la utilización de determinadas sustancias peligrosas en aparatos eléctricos y electrónicos; boletín oficial de la UE L174, 01/07/2011, pág. 88-110

La declaración de conformidad de la UE se encuentra a disposición de todas las autoridades competentes en:

Siemens Aktiengesellschaft
Division Process Industries and Drives
Process Automation
DE-76181 Karlsruhe
Alemania

Encontrará también la declaración de conformidad UE en la dirección de Internet:

Enlace: (https://support.industry.siemens.com/cs/ww/es/ps/)

> Tipo de artículo: "Certificados", Tipo de certificado: "Declaración de conformidad UE"

IECEx

El CP cumple los requisitos de protección contra explosión según IECEx.

Certificación IECEx: IECEx DEK 14.0025X

El CP cumple las exigencias de las siguientes normas:

- IEC 60079-0

  Áreas con peligro de explosión - Parte 0: Recursos - Requisitos generales

- EN 60079-15

  Atmósferas explosivas - Parte 15: Protección del equipo por modo de protección 'n'

Las versiones actuales de las normas pueden consultarse en la certificación IECEx, que encontrará en Internet en la dirección siguiente:

Enlace: (https://support.industry.siemens.com/cs/ww/es/ps/)

Deben cumplirse las siguientes condiciones para el uso seguro del CP conforme al capítulo Indicaciones sobre el uso en zona Ex según ATEX / IECEx (Página 31).

Tenga también en cuenta las indicaciones del documento "Use of subassemblies/modules in a Zone 2 Hazardous Area", que encontrará en Internet en la dirección siguiente:

Enlace: (https://support.industry.siemens.com/cs/ww/es/view/78381013)

ATEX

El CP cumple los requisitos de la Directiva Comunitaria 2014/34/UE "Aparatos y sistemas de protección para uso en atmósferas potencialmente explosivas".

Normas aplicadas:

- EN 60079-0

  Áreas con peligro de explosión - Parte 0: Recursos - Requisitos generales

- EN 60079-15

  Atmósferas explosivas - Parte 15: Protección del equipo por modo de protección 'n'

Las redacciones actualizadas de las normas pueden consultarse en la declaración de conformidad UE, véase más arriba.

Homologación ATEX: II 3 G Ex nA IIC T4 Gc

Número de ensayo: KEMA 07ATEX0145 X

Deben cumplirse las siguientes condiciones para el uso seguro del CP conforme al capítulo Indicaciones sobre el uso en zona Ex según ATEX / IECEx (Página 31).

Tenga también en cuenta las indicaciones del documento "Use of subassemblies/modules in a Zone 2 Hazardous Area", que encontrará en Internet en la dirección siguiente:

Enlace: (https://support.industry.siemens.com/cs/ww/es/view/78381013)

CEM

El CP cumple los requisitos de la Directiva Comunitaria 2014/30/UE "Compatibilidad electromagnética" (directiva CEM).

Normas aplicadas:

- EN 61000-6-4

  Compatibilidad electromagnética (CEM) - Parte 6-4: Normas genéricas - Norma de emisión en entornos industriales

- EN 61000-6-2

  Compatibilidad electromagnética (CEM) - Parte 6-2: Normas genéricas - Inmunidad en entornos industriales

RoHS (restricciones a la utilización de determinadas sustancias peligrosas)

El CP cumple los requisitos de la Directiva Europea 2011/65/UE sobre restricciones a la utilización de determinadas sustancias peligrosas en aparatos eléctricos y electrónicos.

Norma aplicada:

- EN 50581:2012

c(UL)us

Normas aplicadas:

- Underwriters Laboratories, Inc.: UL 61010-1 (Safety Requirements for Electrical Equipment for Measurement, Control, and Laboratory Use - Part 1: General Requirements)
- IEC/UL 61010-2-201 (Safety requirements for electrical equipment for measurement, control and laboratory use. Particular requirements for control equipment)
- Canadian Standards Association: CSA C22.2 No. 142 (Process Control Equipment)

Report / UL file: E85972 (NRAG, NRAG7)

cULus Hazardous (Classified) Locations

Underwriters Laboratories, Inc.: CULUS Listed E223122 IND. CONT. EQ. FOR HAZ. LOC.

Normas aplicadas:

- ANSI ISA 12.12.01
- CSA C22.2 No. 213-M1987

APPROVED for Use in:

- Cl. 1, Div. 2, GP. A, B, C, D T4
- Cl. 1, Zone 2, GP. IIC T4

Ta: Véase la clase de temperatura indicada en la placa de características del CP

Report / UL file: E223122 (NRAG, NRAG7)

Observe las condiciones para el uso seguro del CP conforme al capítulo Indicaciones sobre el uso en zona Ex según UL HazLoc (Página 31).

FM

Factory Mutual Approval Standard Class Number 3600, 3611, 3810

Class I, Division 2, Group A, B, C, D, T4 or Class I, Zone 2, Group IIC, T4

Ta: Véase la clase de temperatura indicada en la placa de características del CP

Deben cumplirse las siguientes condiciones para el uso seguro del CP conforme al capítulo Notas para el uso en zona con peligro de explosión según FM (Página 32).

Australia - RCM

El CP cumple las exigencias de la norma AS/NZS 2064 (Clase A).

Certificación de la unión aduanera euroasiática

EAC (Eurasian Conformity)

Unión aduanera de Rusia, Bielorrusia y Kazajstán

Declaración de conformidad según las normas técnicas de la unión aduanera (TR CU)

MSIP 요구사항 - For Korea only

Registration Number: MSIP REI S7M ET200SP

A급 기기(업무용 방송통신기자재)

이 기기는 업무용(A급) 전자파 적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정 외의 지역에서 사용하는것을 목적으로 합니다.

Homologaciones actuales

Los productos SIMATIC NET se entregan periódicamente a autoridades y oficinas de homologación para proceder a su homologación para los mercados y las aplicaciones que correspondan.

Póngase en contacto con su representante de Siemens si necesita una lista de las homologaciones actuales para los diferentes aparatos o infórmese en las páginas de Internet de Siemens Industry Online Support:

Enlace: (http://support.automation.siemens.com/WW/view/es/45605894)

Planos acotados

B

Todas las medidas de los planos acotados se indican en milímetros.

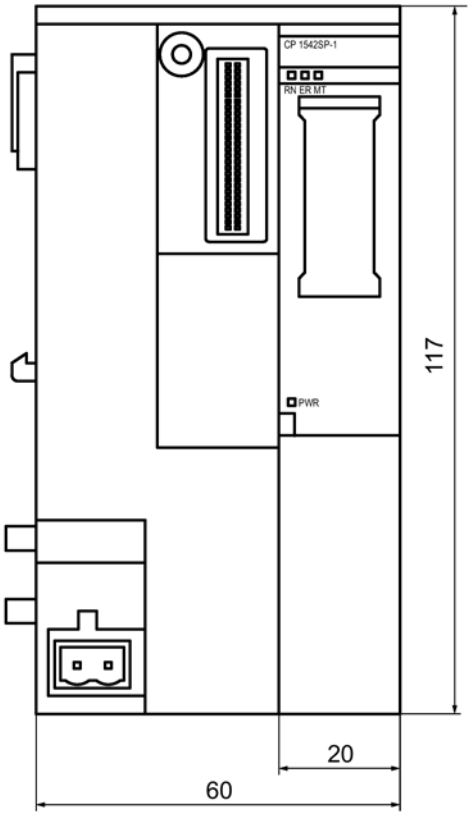


Figura B-1 Vista frontal del CP

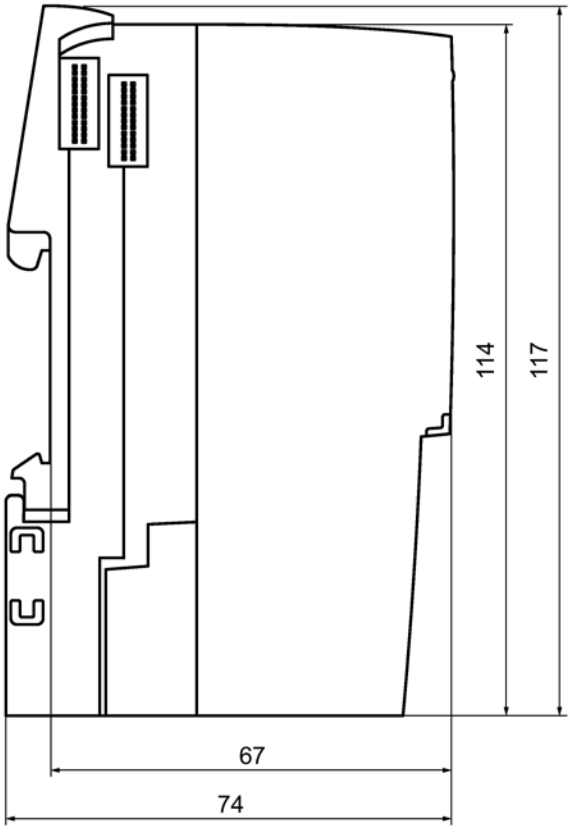


Figura B-2 Vista lateral (izquierda) del CP

Accesorios

C

C.1 BusAdapter

BusAdapter

Para la conexión a la red Ethernet el CP necesita un BusAdapter. El BusAdapter no está incluido en el volumen de suministro del CP.

Figura C-1 Ejemplo de un BusAdapter, en este caso: BA SCRJ/RJ45

El CP soporta los siguientes BusAdapter:

- BA 2×RJ45

  BusAdapter PROFINET con las siguientes conexiones:

  – 2 conectores hembra Ethernet RJ45

  Referencia: 6ES7193-6AR00-0AA0

- BA 2xFC

  BusAdapter PROFINET con las siguientes conexiones:

  – 2 conexiones directas del cable de bus (FastConnect)

  Referencia: 6ES7193-6AF00-0AA0

- BA 2xSCRJ

  BusAdapter PROFINET con las siguientes conexiones:

  – 2 cables de fibra óptica POF/PCF

  Referencia: 6ES7193-6AP00-0AA0

- BA SCRJ/RJ45

  BusAdapter PROFINET, convertidor de medios FO - cobre con las siguientes conexiones:

  – 1 cable de fibra óptica POF/PCF

  – 1 conector hembra Ethernet RJ45

  Referencia: 6ES7193-6AP20-0AA0

- BA SCRJ/FC

  BusAdapter PROFINET, convertidor de medios FO - cobre con las siguientes conexiones:

  – 1 cable de fibra óptica POF/PCF

  – 1 conexión directa del cable de bus (FastConnect)

  Referencia: 6ES7193-6AP40-0AA0

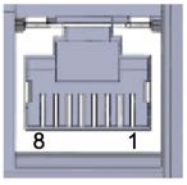
Encontrará más detalles en el manual /2/ (Página 123) y en el Siemens Industry Mall en Enlace: (https://mall.industry.siemens.com).

C.2 Asignación de la interfaz Ethernet de los BusAdapter

Asignación de la interfaz Ethernet

La tabla siguiente contiene la asignación de pines de la interfaz Ethernet. La asignación corresponde al estándar Ethernet 802.3-2005 en la ejecución 100BASE-TX.

Tabla C- 1 Asignación de pines de la interfaz Ethernet

Vista del conector hembra RJ45	Pin	Nombre de la señal	Asignación
	1	TD	Transmit Data +
	2	TD_N	Transmit Data -
	3	RD	Receive Data +
	4	GND	Ground
	5	GND	Ground
	6	RD_N	Receive Data -
	7	GND	Ground
	8	GND	Ground

Bibliografía

D

Cómo encontrar la documentación Siemens

- Referencias

  Los números de artículo para los productos Siemens relevantes aquí se encuentran en los catálogos siguientes:

  – Comunicación industrial SIMATIC NET / identificación industrial, catálogo IK PI

  – Productos SIMATIC para Totally Integrated Automation y microautomatización, catálogo ST 70

  Puede solicitar catálogos e información adicional a la subsidiaria o sucursal correspondiente de Siemens. También encontrará la información de producto en el Siemens Industry Mall, bajo la dirección siguiente:

  Enlace: (https://mall.industry.siemens.com)

- Manuales en Internet

  Los manuales SIMATIC NET están disponibles en las páginas de Internet de Siemens Industry Online Support:

  Enlace: (https://support.industry.siemens.com/cs/ww/es/ps/15247/man)

  Desplácese dentro del árbol de productos al producto deseado y realice los ajustes siguientes:

  Tipo de artículo "Manuales"

- Manuales en soporte de datos

  Los manuales de los productos SIMATIC NET se encuentran también en el soporte de datos que acompaña a muchos de los productos SIMATIC NET.

/1/

SIMATIC
CP 1542SP-1, CP 1542SP-1 IRC, CP 1543SP-1
Instrucciones de servicio
Siemens AG
Enlace: (https://support.industry.siemens.com/cs/ww/es/ps/22144/man)
Enlace: (https://support.industry.siemens.com/cs/ww/es/ps/22143/man)

/2/

Sistema de periferia descentralizada SIMATIC
ET 200SP -
Manual de sistema
Siemens AG
Enlace: (http://support.automation.siemens.com/WW/view/es/58649293)

/3/

SIMATIC NET
TeleControl Server Basic (versión V3)
Instrucciones de servicio
Siemens AG
Enlace: (https://support.industry.siemens.com/cs/ww/es/ps/15918/man)

/4/

SIMATIC NET
Industrial Ethernet Security
Conceptos básicos y aplicación
Manual de configuración
Siemens AG
Enlace: (https://support.industry.siemens.com/cs/ww/es/ps/15326/man)

/5/

SIMATIC NET
TIM DNP3
Manual de sistema
Siemens AG
Enlace: (https://support.industry.siemens.com/cs/ww/es/ps/15940/man)

/6/

SIMATIC NET
Diagnóstico y configuración con SNMP
Manual de diagnóstico
Siemens AG
Enlace: (https://support.industry.siemens.com/cs/ww/es/ps/15392/man)

/7/

SIMATIC NET
Industrial Ethernet / PROFINET
Manual de sistema
Siemens AG

- Industrial Ethernet
  Enlace: (https://support.industry.siemens.com/cs/ww/de/view/27069465)
- Passive network components
  Enlace: (https://support.industry.siemens.com/cs/ww/en/view/84922825)

Índice alfabético

S

T

V