SIEMENS

SIMATIC NET

TeleControl Configuración - IEC 60870-5

Manual de configuración

Configuración y diagnóstico

02/2024
C79000-G8978-C509-05

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 de 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 Aktiengesellschaft. 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 correcciones se incluyen en la siguiente edición.

Siemens Aktiengesellschaft
Digital Industries
Postfach 48 48
90026 NÜRNBERG
ALEMANIA

C79000-G8978-C509-05
Ⓟ 03/2024 Sujeto a cambios sin previo aviso

Prólogo

Ámbito de validez de este manual

El presente manual de configuración es válido para todos los siguientes módulos de comunicación SIMATIC NET que soportan el protocolo IEC 60870-5:

- TIM 1531 IRC - V2.4
- CP 1243-1 - V3.5
- CP 1243-7 LTE - V3.5
- CP 1243-8 IRC - V3.5
- CP 1542SP-1 IRC - V2.3

Las versiones de los dispositivos y los productos necesarios del software de configuración se mencionan en el capítulo Módulos de comunicación (Página 17).

Abreviaturas / designaciones de los dispositivos

En este manual se utilizan con frecuencia las abreviaturas siguientes:

- **Módulo / dispositivo / CP / TIM**
  Designaciones del respectivo módulo de comunicación
- **CP de telefonía móvil**
  CP 1243-7 LTE
- **STEP 7**
  Esta abreviatura se utilizará en adelante para la herramienta de configuración STEP 7 Basic/ Professional.
- **WBM**
  "WBM" es la abreviatura de "Web Based Management", las páginas del servidor web del TIM para datos de configuración y diagnóstico.

Novedades de la presente edición

- Nuevas versiones de firmware de los módulos de comunicación indicados anteriormente (ver también las respectivas instrucciones de servicio)
- CP 1200: Acceso a la nube vía MQTT
- CP 1243-7 LTE: Opciones para la reconexión con la red de telefonía móvil
- Ampliación de las funciones de la sincronización horaria

- Mejoras en las funciones de Telecontrol
  - Redundancia de dispositivos del TIM 1531 IRC (como estación)
  - Opción de transferencia del estado de los puntos de datos en la CPU con sello de tiempo
  - Puntos de datos de comando: retroalimentación del valor local y realimentación del resultado del comando
  - Registro de variables en la CPU (Configuración de puntos de datos > Ciclo de lectura)
  - Consulta manual de estaciones (TIM 1531 IRC / CP 1542SP1-IRC)
  - Filtrado de las interfaces en el editor de conexiones de Telecontrol
  - Ampliación de los parámetros en la exportación de puntos de datos
- Configuración con STEP 7 Basic / Professional V19 Update 1
- Revisión del contenido

Edición sustituida del manual

Edición 02/2023

Estructura de la documentación

La documentación de los módulos de comunicación por Telecontrol SIMATIC NET consta de los siguientes manuales:

- Instrucciones de servicio o manual de producto
- Manuales de configuración (1 manual de configuración para cada protocolo de Telecontrol)

Encontrará los enlaces de Internet para los manuales en Bibliografía (Página 219).

Para módulos que soportan el protocolo IEC 60870-5, la documentación consta de los documentos siguientes:

Módulos CP

- **Instrucciones de servicio**
  Válidas para el respectivo CP
  - Aplicación, funciones, requisitos (CPU, software, etc.)
  - Descripción del hardware
  - Montaje, conexión, puesta en marcha y operación
  - Configuración (funciones independientes de Telecontrol)
    En caso de utilizar funciones de Telecontrol debe leerse el manual de configuración correspondiente.
  - Diagnóstico y mantenimiento
  - Datos técnicos, homologaciones y accesorios
- **Manual de configuración IEC 60870-5**
  - Configuración y diagnóstico en STEP 7 Professional (TIA Portal)
    Excepción (CP 1200):
    La descripción de la configuración del acceso a la nube del CP 1200 (grupo de parámetros "CloudConnect") no aparece en este manual, sino en las instrucciones de servicio del respectivo CP.

TIM 1531 IRC

- **Manual de producto**
  - Aplicación y funciones
  - Requisitos (CPU, software de configuración, etc.)
  - Descripción del hardware
  - Montaje, conexión, puesta en marcha y operación
  - Diagnóstico y mantenimiento
  - Datos técnicos, homologaciones y accesorios
- **Manual de configuración IEC 60870-5**
  Configuración y diagnóstico en STEP 7 Professional (TIA Portal)

Versión actual del manual en Internet

También puede consultar la versión actual del presente manual en las páginas web de Siemens Industry Online Support:

Enlace: (https://support.industry.siemens.com/cs/ww/es/ps/21764/man)

Conocimientos necesarios

Para la configuración y el diagnóstico de los dispositivos se requieren conocimientos en los campos siguientes:

- SIMATIC STEP 7 Professional
- Transferencia de datos mediante redes WAN
- Estructura de redes industriales con funciones de seguridad

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 PDF utilizan el comando <Alt>+<flecha izquierda>.

Condiciones de la licencia

Nota

Open Source Software

Los productos contienen Open Source Software. Lea detenidamente las condiciones de la licencia para Open Source Software antes de utilizar los productos.

Para encontrar las condiciones de la licencia consulte las indicaciones que aparecen en las instrucciones de servicio del producto correspondiente.

Información de ciberseguridad

Siemens ofrece productos y soluciones con funciones de ciberseguridad 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 contra de amenazas cibernéticas, es necesario implementar - y mantener continuamente - un concepto de ciberseguridad industrial integral y holístico conforme al estado del arte. Los productos y las soluciones de Siemens constituyen una parte de este concepto.

Los clientes son responsables de impedir el acceso no autorizado a sus instalaciones, sistemas, máquinas y redes. Dichos sistemas, máquinas y 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. cortafuegos y segmentación de la red).

Para obtener información adicional sobre las medidas de ciberseguridad industrial que podrían ser implementadas, por favor visite https://www.siemens.com/cybersecurity-industry.

Los productos y las soluciones de Siemens están sometidos a un desarrollo constante con el fin de hacerlos más seguros. Siemens recomienda encarecidamente realizar actualizaciones en cuanto estén disponibles y utilizar únicamente las últimas versiones de los productos. El uso de versiones anteriores de los productos o sin soporte y la falta de aplicación de las nuevas actualizaciones, puede aumentar el riesgo de amenazas cibernéticas.

Para mantenerse informado de las actualizaciones de productos, recomendamos que se suscriba al Siemens Industrial Cybersecurity RSS Feed en https://www.siemens.com/cert.

Antes de configurar y poner en marcha los módulos, infórmese sobre sus funciones de seguridad:
Funciones, datos de prestaciones y capacidad funcional (Página 22)

Lea las recomendaciones de seguridad del anexo "Security":
Recomendaciones Security (Página 13)

Glosario de SIMATIC NET

El glosario de SIMATIC NET describe los términos técnicos que pueden utilizarse en el presente documento.

Encontrará el glosario de SIMATIC NET en la siguiente dirección de Siemens Industry Online Support:

Enlace: (http://support.automation.siemens.com/WW/view/es/50305045)

Índice

Recomendaciones Security

1

Tenga en cuenta las siguientes recomendaciones de seguridad para impedir accesos no autorizados al sistema.

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.
- Infórmese periódicamente sobre las novedades en las páginas web de Siemens.
  - Aquí encontrará información acerca de Industrial Security:
    Enlace: (http://www.siemens.com/industrialsecurity)
  - Aquí encontrará una relación de documentos relativos a la seguridad en la red:
    Enlace: (https://support.industry.siemens.com/cs/ww/es/view/92651441)
- Mantenga actualizado el firmware. Infórmese periódicamente sobre las actualizaciones de seguridad del firmware y aplíquelas.
  Encontrará indicaciones sobre novedades del producto y nuevas versiones de firmware en la dirección siguiente:
  Enlace: (https://support.industry.siemens.com/cs/ww/es/ps/21764/dl)

Acceso físico

Limite el acceso físico al equipo al personal cualificado.

Conexión de red

No conecte el módulo directamente a Internet. Si desea conectar el módulo a Internet, utilice las variantes de seguridad de los protocolos de Telecontrol o conecte dispositivos de protección delante del módulo. Son dispositivos de protección, por ejemplo, un router SCALANCE M o un módulo de seguridad SCALANCE S con cortafuegos.

Funciones de seguridad del producto

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

- Niveles de protección y funciones de seguridad de la CPU
  Configure el acceso en "Protección y seguridad" de la CPU.
  Utilice las funciones de seguridad adicionales de la CPU para impedir accesos no autorizados a la estación.
  Encontrará información al respecto en el sistema de información de STEP 7.
- Función de seguridad de la comunicación
  - Utilice las funciones de seguridad de los protocolos de Telecontrol.
  - Utilice las variantes de protocolo seguras, por ejemplo NTP (secure) o SNMPv3.
  - Mantenga desactivado el acceso al servidor web.

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).
  - El protocolo HTTP ofrece una alternativa segura con HTTPS para el acceso al servidor web.
- Desactive DHCP en las interfaces que conducen a redes públicas, como Internet, para prevenir la suplantación de IP.

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 módulo siempre es cliente para este servicio.
- **Autenticación**
  Indica si el protocolo autentica el interlocutor durante el acceso.

Son relevantes los siguientes puertos. No todos los tipos de dispositivos soportan todos los protocolos.

Tabla 1-1 Puertos de servidor

Protocolo/función	Número de puerto (protocolo)	Ajuste predeterminado del puerto	Estado del puerto	Autenticación
IEC 60870-5-104	2404 (TCP) ajustable	Cerrado	Abierto tras configuración	No
IEC 60870-5-104 con TLS	19998 (TCP) ajustable	Cerrado	Abierto tras configuración	Sí, si Secure Communication está activado.
Conexiones S7 y online	102 (TCP)	Abierto	Abierto tras configuración	No
Diagnóstico de seguridad online (CP)	8448 (TCP)	Cerrado **	Abierto tras configuración *	Sí
Comunicación vía SINEMA RC	443 (TCP), 5243 (UDP)	Cerrado	Abierto tras configuración	Sí
HTTP	80 (TCP)	Cerrado	Abierto tras configuración	No
HTTPS	443 (TCP)	Cerrado	Abierto tras configuración	Sí
SNMP	161 (UDP)	Cerrado	Abierto tras configuración	No (SNMPv1) Sí (SNMPv3)
IPsec (dispositivos de seguridad)	500 (UDP)	Cerrado	Abierto tras configuración	Sí

***** Algunos operadores del servicio consideran la apertura del puerto 102 una laguna de seguridad.
Para evitar que se abra el puerto 102 durante el diagnóstico online, consulte el capítulo Diagnóstico de seguridad online por el puerto 8448 del CP (Página 187).

****** En el TIM 1531 IRC, el puerto 8448 está abierto en el ajuste predeterminado.

Puertos de interlocutores de la comunicación y de routers

Asegúrese de habilitar los puertos cliente necesarios en el cortafuegos correspondiente de los interlocutores de la comunicación y de routers intermedios.

Pueden ser:

- NTP / NTP (secure) / 123 (UDP)
- DNS / 53 (UDP)
- DHCP / 67, 68 (UDP)
- SMTP / 25 (TCP)
- STARTTLS / 587 (TCP)
- SSL/TLS / 465 (TCP)
- Configuración automática de SINEMA RC / 443 (TCP) - ajustable
- SINEMA RC y OpenVPN / 1194 (UDP) - ajustables en SINEMA RC
- IPSec / 500 (TCP) / 4500 (UDP)
- OpenVPN / 1194 (UDP)
- Syslog / 514 (UDP)

Funciones y requisitos

2

2.1 Módulos de comunicación

Módulos de comunicación para el protocolo de Telecontrol IEC 60870-5

Los siguientes módulos de comunicación SIMATIC NET pueden utilizarse para el protocolo de Telecontrol IEC 60870-5.

Significado de los símbolos de la tabla:

- X = se soporta
- (X) = función de maestro de los diferentes puntos de datos
- - = no se soporta

Tabla 2-1 Módulos de comunicación para IEC 60870-5

Módulo Referencia	Número de interfaces *			Tipo de estación			Producto de STEP 7	Firmware necesario
	IE IEC 60870-5-104	RS IEC 60870-5-101	M	Maestro	Estación nodo	Estación		
TIM 1531 IRC 6GK7 543-1MX00-0XE0	3	1 **	- ***	X	X	X	STEP 7 Professional	V2.4
CP 1542SP-1 IRC 6GK7 542-6VX00-0XE0	1	-	- ***	(X)	-	X	STEP 7 Professional	V2.3
CP 1243-8 IRC 6GK7 243-8RX30-0XE0	1	-	-	(X)	-	X	STEP 7 Basic **** / Professional	V3.5
CP 1243-1 6GK7 243-1BX30-0XE0 6AG1 243-1BX30-2AX0	1	-	-	(X)	-	X	STEP 7 Basic **** / Professional	V3.5
CP 1243-7 LTE 6GK7 243-7KX30-0XE0 6GK7 243-7SX30-0XE0	-	-	1	(X)	-	X	STEP 7 Basic **** / Professional	V3.5

***** IE = interfaces Ethernet, RS = interfaces serie, M = interfaz de telefonía móvil integrada

****** Para la conexión a la interfaz serie no se soportan los módulos GSM.

******* Los módulos TIM pueden conectarse a redes de telefonía móvil a través de módems.

******** STEP 7 Basic para la conexión del CP a un maestro externo. Véase la observación más abajo.

Indicaciones relativas a la tabla

Indicaciones relativas a las columnas:

- **Tipo de estación "Estación nodo"**
  En la jerarquía de la instalación, una estación nodo se encuentra entre la central (maestro) y otras estaciones subordinadas. El módulo requiere como mínimo dos interfaces.
  En la configuración, el "tipo de nodo de red" de la interfaz conectada a la central se configura como "estación nodo". Consulte a este respecto el capítulo Conectar las interfaces en red (Página 50).
- **Producto de STEP 7 para CP S7-1200**
  Los CP de S7-1200 pueden configurarse en STEP 7 Basic para la conexión a un maestro externo.
  Para conectar los CP a maestros SIMATIC NET o estaciones nodo configurados en STEP 7 se requiere STEP 7 Professional.
- **Firmware**
  Las versiones de firmware necesarias para los módulos hacen referencia a la configuración completa descrita en el presente manual. Encontrará la versión de STEP 7 necesaria para tal fin en el capítulo Requisitos de software (Página 21).
  Los módulos con versiones de firmware inferiores también pueden configurarse con una funcionalidad distinta en la versión actual de STEP 7.

2.2 Routing PG

Routing PG entre módulos de Telecontrol

Entre los módulos listados en la tabla y por los medios indicados se soporta el routing PG.

Requisitos para CP

En el grupo de parámetros "Tipos de comunicación" debe estar activada la opción "Funciones online".

Módulo **Medio**	**TIM 1531 IRC**	**CP 1200**	**CP 1542SP-1 IRC**
TIM 1531 IRC	Ethernet (S7)	Ethernet (S7)	Ethernet (S7)

Número máx. de conexiones de routing S7: 4

2.3 Ejemplos de configuración

A continuación encontrará algunos ejemplos de configuración con los módulos de comunicación utilizables.

Comunicación vía Ethernet / Internet, envío de correos electrónicos

En el ejemplo de configuración representado, las estaciones S7 se comunican con la central a través de las interfaces Ethernet de los diferentes módulos.

Con sus interfaces Ethernet, los módulos TIM permiten la conexión a una central redundante.

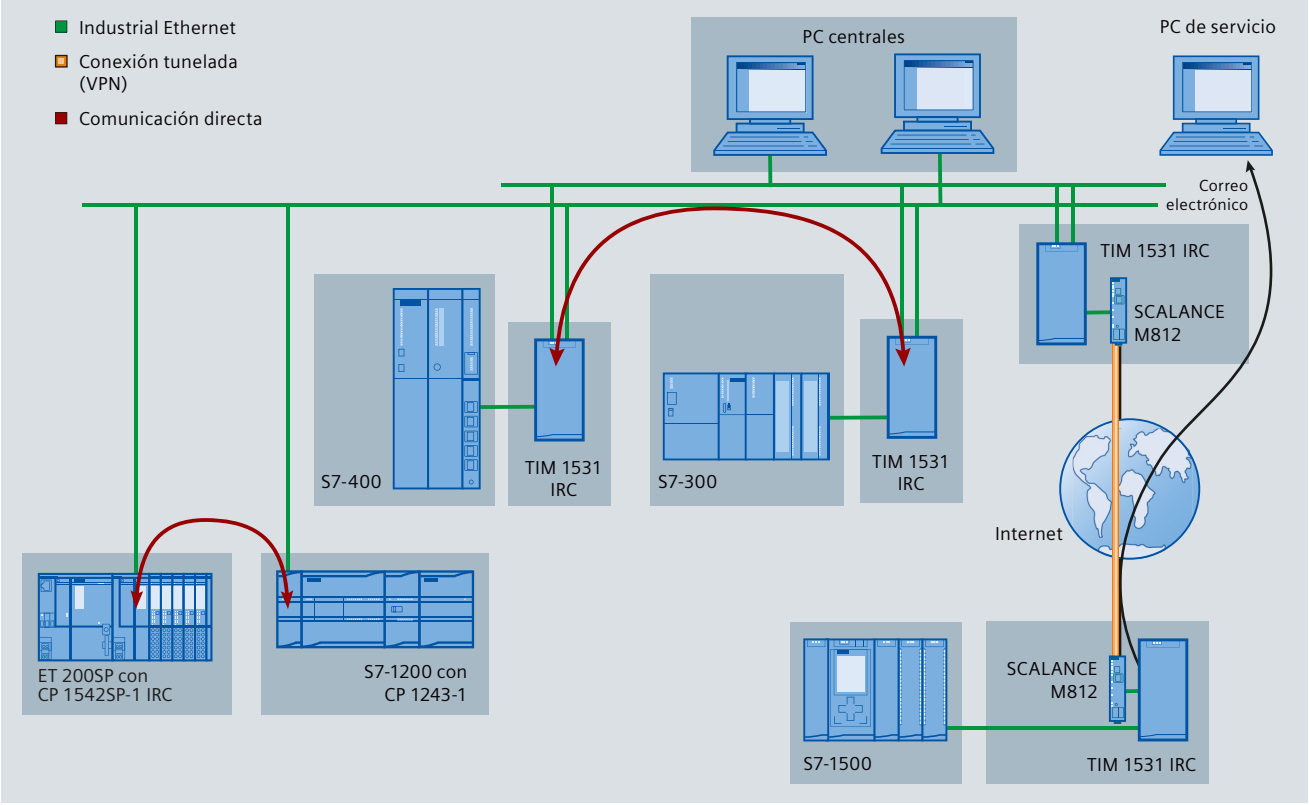


Figura 2-1 Comunicación vía Ethernet / Internet

Correos electrónicos

Los módulos pueden enviar correos electrónicos. Los destinatarios posibles son:

- Para correos electrónicos configurados y controlados por eventos:
  - PC con conexión a Internet
  - Teléfonos móviles
- Para correos electrónicos mediante bloques OUC:
  - Estaciones SIMATIC con los bloques de programa correspondientes

Comunicación directa

Con el módulo de comunicación es posible la comunicación directa entre estaciones S7 a través de redes basadas en IP. Los telegramas no pasan por la central.

La comunicación directa puede realizarse utilizando los mecanismos siguientes:

- Conexiones de Telecontrol configuradas
  Consulte los requisitos en Posibilidades de comunicación (Página 31).
- Bloques de programa de la Open User Communication
  Consulte Bloques de programa OUC (CP) (Página 195)

Redundancia de vías utilizando la interfaz serie

En el ejemplo siguiente, la interfaz Ethernet y la interfaz serie del TIM 1531 IRC se utilizan para crear vías de transmisión redundantes.

- Interfaz Ethernet para la comunicación vía Ethernet / Internet
- Interfaz serie para la comunicación vía red WAN (línea dedicada o red de marcación)

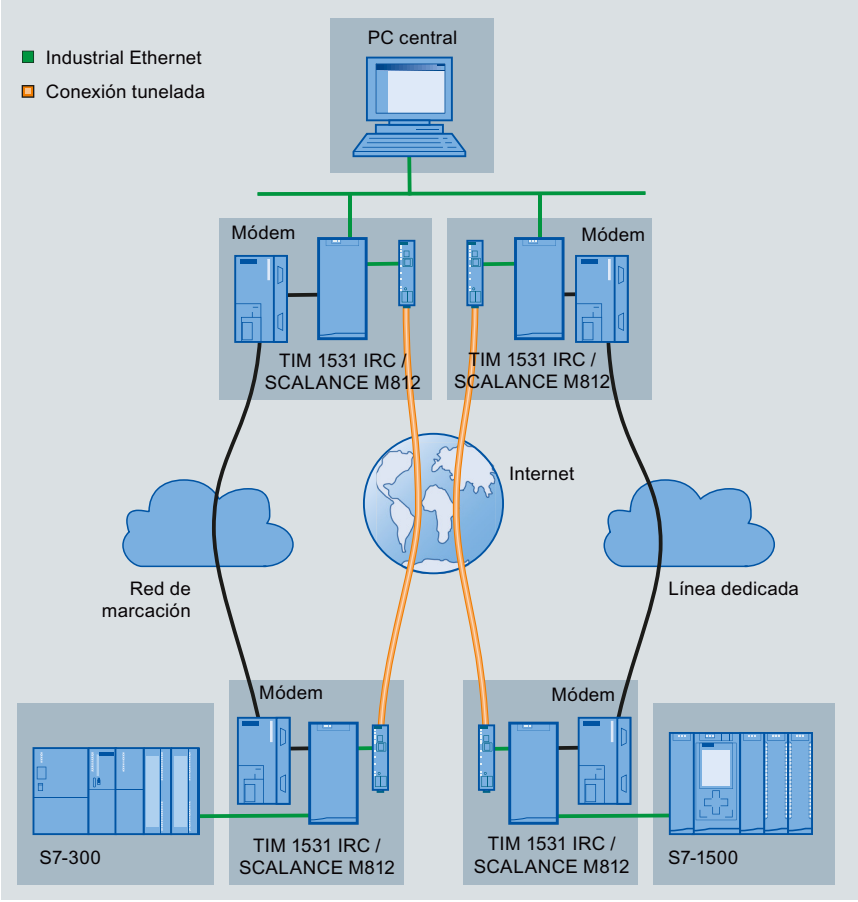


Figura 2-2 Comunicación a través de vías redundantes

La redundancia de vías también es posible a través de dos redes Ethernet.

Redundancia de dispositivos del TIM 1531 IRC

Para la redundancia de dispositivos del TIM 1531 IRC consulte el capítulo Redundancia de dispositivos del TIM 1531 IRC (Página 57).

2.4 CPU que pueden utilizarse

CPU compatibles

Los siguientes dispositivos pueden configurarse como CPU asignada de los módulos de comunicación:

- **TIM 1531 IRC**
  - S7-1500
    Todas las CPU estándar con versión V2.9
    Todas las CPU redundantes (CPU H, CPU R) con versión V3.1
  - ET 200SP
    Todas las CPU configurables en STEP 7 a partir de la versión V2.9
  - S7-300
    Todas las CPU con interfaz PROFINET
  - S7-400
    Todas las CPU configurables en STEP 7
- **CP 1243-1 / CP 1243-7 LTE / CP 1243-8 IRC**
  CPU con versión V4.6
- **CP 1542SP-1 IRC**
  CPU a partir de la versión V2.9:
  - CPU 1510SP-1 PN
  - CPU 1510SP F-1 PN
  - CPU 1512SP-1 PN
  - CPU 1512SP F-1 PN

  Encontrará más información sobre las CPU y los adaptadores de bus en el manual /6/ CP 1542SP-1, CP 1542SP-1 IRC, CP 1543SP-1 (Página 220).

2.5 Requisitos de software

Software para la configuración y funciones online

Para la configuración del volumen de funciones completo descrito en el presente manual se requiere la siguiente versión de STEP 7:

- STEP 7 Basic / Professional V19 Update 1

Consulte el producto de STEP 7 necesario en cada caso en el capítulo Módulos de comunicación (Página 17).

2.6 Funciones, datos de prestaciones y capacidad funcional

2.6.1 CP 1243-1

Número de CM/CP por estación

Pueden insertarse y configurarse hasta tres CM/CP por estación S7-1200.

Para usar la comunicación por Telecontrol se pueden conectar tres CP 1243-1 por estación.

Recursos de conexión

- **Conexiones de Telecontrol, incluidas comunicación cruzada / comunicación directa**
  El CP puede establecer conexiones con hasta 4 interlocutores.
  Un interlocutor puede ser un maestro de estructura sencilla o redundante o bien una estación (comunicación directa).
  Consulte la configuración de la comunicación directa entre estaciones en el capítulo Posibilidades de comunicación (Página 31).
- **Conexiones S7 y conexiones TCP / UDP / ISO-on-TCP**
  Máx. 14 recursos de conexión, distribuibles libremente para:
  - Conexiones S7 (PUT/GET)
    Incluidas las conexiones para routing S7
  - Conexiones a través de bloques de programa (OUC) con estaciones S7
- **Funciones online**
  1 recurso de conexión está reservado para funciones online.
- **Conexiones PG/OP**
  - 1 recurso para conexiones PG
  - 3 recursos para conexiones OP

Número de puntos de datos para su configuración

Número máximo de puntos de datos configurables por CP

- TeleControl Basic: 200
- DNP3: 500
- IEC: 500

Memoria de telegramas (búfer de transmisión)

El CP dispone de una memoria de telegramas (búfer de transmisión) para los valores de puntos de datos configurados como eventos y que deben enviarse al interlocutor.

El búfer de transmisión se distribuye por igual entre todos los interlocutores configurados. El tamaño de la memoria de telegramas puede ajustarse en STEP 7, consulte el capítulo Memoria imagen de proceso, tipo de transferencia, clases de eventos (Página 151).

El tamaño máximo del búfer de transmisión es de:

- TeleControl Basic: 64000 telegramas
- DNP3: 100000 eventos
- IEC: 100000 eventos

Mensajería (correo electrónico)

- Envío de hasta 10 mensajes (correos electrónicos) con configuración en el editor de mensajes

Túnel IPsec (VPN)

Pueden establecerse hasta 8 túneles IPsec para disponer de comunicaciones seguras con más 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:

- Un máximo de 226 reglas con direcciones individuales
- Un 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)
- Un máximo de 128 reglas con restricción de la velocidad de transferencia ("Limitación del ancho de banda")

2.6.2 CP 1243-7 LTE

Recursos de conexión

- **Conexiones de Telecontrol**
  - DNP3 / IEC
    El CP puede establecer conexiones con hasta 4 interlocutores.
    Un interlocutor puede ser un maestro de estructura sencilla o redundante o bien una estación (comunicación directa).
  - TeleControl Basic
    1 conexión reservada para el intercambio de datos útiles con el servidor de Telecontrol
    Adicionalmente, comunicación cruzada: La comunicación cruzada entre los CP de dos estaciones tiene lugar a través del servidor de Telecontrol. Se configura en el grupo de parámetros "Estaciones interlocutoras" > "Interlocutor para comunicación cruzada".
    Capacidad funcional para comunicación cruzada: Máx. 15 en total, de las cuales:
    - Enviar a interlocutores: máx. 3 (parámetro "Búfer de transmisión" activado)
    - Recibir de interlocutores: máx. 15 (parámetro "Búfer de transmisión" desactivado)
- **Conexiones S7 y conexiones TCP / UDP / ISO-on-TCP**
  Máx. 14 recursos de conexión, distribuibles libremente para:
  - Conexiones S7 (PUT/GET)
    Incluidas las conexiones para routing S7
  - Conexiones a través de bloques de programa (OUC) con estaciones S7
- **Conexiones PG/OP**
  - 1 recurso para conexiones PG
  - 3 recursos para conexiones OP
- **Funciones online**
  1 recurso de conexión está reservado para funciones online.
- **Conexiones TeleService**
  - Máx. 1 conexión TeleService
- **Conexiones a servidores NTP**
  Máx. 1 conexión a un servidor NTP

Datos útiles

En los tipos de conexión que se indican a continuación, los datos útiles de un telegrama representan un área de datos coherente en cuanto al instante de la transferencia.

Datos útiles por telegrama en los diferentes tipos de conexión:

- En conexiones TCP: máx. 8192 bytes
- En conexiones ISO-on-TCP: máx. 1452 bytes
- En conexiones UDP máx. 1472 bytes

En telegramas de la comunicación por Telecontrol, los diferentes valores de los puntos de datos están marcados con un sello de tiempo.

Número de puntos de datos para su configuración

El número máximo de puntos de datos configurables con los protocolos de Telecontrol es:

- TeleControl Basic: 200
- DNP3: 500
- IEC: 500

Memoria de telegramas (búfer de transmisión)

El CP dispone de una memoria de telegramas (búfer de transmisión) para los valores de puntos de datos configurados como eventos y que deben enviarse al interlocutor.

El búfer de transmisión tiene el siguiente tamaño máximo:

- TeleControl Basic: 64000 telegramas
- DNP3: 100000 eventos
- IEC: 100000 eventos

El búfer de transmisión se distribuye por igual entre todos los interlocutores configurados. El tamaño de la memoria de telegramas puede ajustarse en STEP 7 (grupo de parámetros "Comunicación con la CPU").

Mensajes: correo electrónico / SMS

En STEP 7 se pueden configurar hasta 10 mensajes, que se envían como correos electrónicos o SMS.

Número máximo de caracteres que pueden transmitirse por SMS: 160 caracteres ASCII, incluido un valor que pueda haberse enviado conjuntamente

Número máximo de caracteres que pueden transmitirse por correo electrónico: 256 caracteres ASCII, incluido un valor que pueda haberse enviado conjuntamente

Túnel IPsec (VPN)

Puede establecerse un túnel IPsec para disponer de comunicación segura con otro módulo 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:

- Un máximo de 226 reglas con direcciones individuales
- Un 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)
- Un máximo de 128 reglas con restricción de la velocidad de transferencia

2.6.3 CP 1243-8 IRC

Datos en las instrucciones de servicio

Encontrará los datos siguientes sobre la capacidad funcional en las instrucciones de servicio del CP 1243-8:

- Número de CM/CP por estación
- Recursos de conexión
- Número de puntos de datos (500)
- Memoria de telegramas (búfer de transmisión) (64000)
  Para ajustar el tamaño en STEP 7 consulte el capítulo Comunicación con la CPU (Página 80).
  Para detalles y las posibilidades de transferencia de datos consulte el capítulo Memoria imagen de proceso, tipo de transferencia, clases de eventos (Página 151).
- Correo electrónico (10)
- Túnel IPsec (VPN) (8)
- Reglas de cortafuegos

Consulte las instrucciones de servicio en /4/ CP 1243-8 IRC (Página 220).

2.6.4 CP 1542SP-1 IRC

Datos en las instrucciones de servicio

Encontrará los datos siguientes sobre la capacidad funcional en las instrucciones de servicio del CP:

- Número de CP por estación (2) y reglas de slots
- Recursos de conexión
- Número de puntos de datos
- Memoria de telegramas (búfer de transmisión)
  Para detalles y las posibilidades de transferencia de datos consulte el capítulo Memoria imagen de proceso, tipo de transferencia, clases de eventos (Página 151).
- Correo electrónico (10)
- Túnel IPsec (VPN) (4)
- Reglas de cortafuegos

Consulte las instrucciones de servicio en /6/ CP 1542SP-1, CP 1542SP-1 IRC, CP 1543SP-1 (Página 220).

2.6.5 TIM 1531 IRC

Recursos de conexión

- **Conexiones de Telecontrol**
  El número de conexiones o de interlocutores es limitado para ambos tipos de interfaz y para cada interfaz concreta.
  Tenga en cuenta que las vías de conexión redundantes de una conexión entre dos interlocutores requieren dos recursos de conexión en cada interlocutor.
  - Número máx. de conexiones: 128
    La distribución entre las 4 interfaces es aleatoria (máx. 128 por interfaz).
- **Correo electrónico**
  En el tiempo de ejecución es posible establecer una conexión para enviar correos electrónicos.
- **Conexiones S7**
  - Máx. 4 recursos de conexión para conexiones PG/OP (véase más adelante)
- **Conexiones PG/OP**
  4 recursos de conexión para conexiones con la estación de ingeniería o dispositivos HMI (incluidos en la capacidad funcional de las conexiones S7, véase más adelante)
- **Routing PG**
  Máx. 4 conexiones simultáneamente
- **Funciones online**
  Véase conexiones PG/OP
- **HTTP/HTTPS**
  Máx. 2 conexiones por interfaz Ethernet

Número de puntos de datos para su configuración

El número máximo de puntos de datos configurables es 3000.

Memoria de telegramas: Búfer de transmisión / tarjeta SD

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

El búfer de transmisión se distribuye por igual entre todos los interlocutores configurados. El tamaño de la memoria de telegramas puede ajustarse en STEP 7 (grupo de parámetros "Comunicación con la CPU").

El tamaño máximo del búfer de transmisión es de:

- ST7: 100 000 telegramas
- DNP3/IEC: 250 000 eventos

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 (Página 151).

Para guardar eventos en una tarjeta SD opcional consulte el capítulo Ajustes básicos (Página 37).

Mensajes: Correo electrónico

En STEP 7 es posible configurar hasta 10 mensajes que el TIM puede enviar como correo electrónico.

- Número de caracteres por correo electrónico
  Número máximo de caracteres que pueden transferirse por cada correo electrónico: 256 caracteres ASCII, incluido un valor que pueda haberse enviado conjuntamente

Funciones de seguridad de los protocolos de transferencia

Los protocolos de transferencia que pueden utilizarse para la comunicación por Telecontrol soportan las siguientes funciones de seguridad:

ST7

- **MSC**
  Este protocolo MSC soporta la autenticación de los interlocutores y un cifrado sencillo de los datos. El cifrado incluye un nombre de usuario y una contraseña. Entre la estación MSC y la central MSC se establece un túnel MSC.
- **MSCsec**
  MSCsec soporta la autenticación de los interlocutores y el cifrado de datos con nombre de usuario y contraseña.
  Además, la clave común de generación automática se renueva entre los interlocutores en un intervalo de cambio de clave configurable.

DNP3

- El TIM soporta el uso de conexiones TLS y la autenticación segura conforme a IEEE 1815.

IEC 60870-5-101 / 104

- El TIM soporta el uso de las siguientes funciones:
  - IEC 60870-5-101 / 104
    Autenticación segura conforme a IEC 60870-5-7
  - IEC 60870-5-104
    Conexiones TLS

Otras funciones de seguridad del TIM

Además, el TIM soporta las siguientes funciones de seguridad:

- **NTP (secure)**
  Para la transmisión segura en la sincronización horaria
- **STARTTLS / SSL/TLS**
  Para la transferencia segura de mensajes de correo electrónico

- **HTTPS**
  Para el acceso seguro al servidor web de la CPU
- **SNMPv3**
  Para la transferencia antiescucha de información de análisis de la red.

Nota

Recomendación para instalaciones críticas en materia de seguridad

Aproveche las siguientes posibilidades:

- En instalaciones con requisitos de seguridad exigentes, utilice protocolos seguros como, p. ej., HTTPS o SNMPv3.
- En caso de conexión a redes públicas conviene utilizar módulos de seguridad con cortafuegos.
  Los módulos de seguridad permiten proteger diferentes dispositivos, células de automatización o segmentos de una red Ethernet. Son especialmente adecuados para ello los siguientes módulos de seguridad: SCALANCE S, SCALANCE M800

Formateo de la tarjeta SD

La tarjeta SD del TIM 1531 IRC debe tener el formato siguiente para poder guardar datos de configuración.

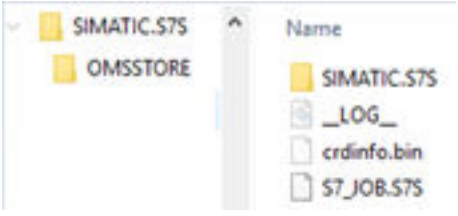


Figura 2-3 Formateo de la tarjeta SD

Encontrará indicaciones sobre el formateo de la tarjeta SD en el sistema de información de STEP 7, introduciendo el término de búsqueda "Formatear tarjeta de memoria S7-1500".

Mecanismos de comunicación 3

3.1 Posibilidades de comunicación

Vías de comunicación

Para la comunicación por Telecontrol son posibles las siguientes vías o conexiones:

- **Conexión maestro ⇔ estación**
- **Conexiones redundantes**
  Si hay accesibles dos dispositivos a través de redes diferentes, para establecer una redundancia de vías se pueden crear como máximo dos conexiones entre los dispositivos.
- **Comunicación directa (estación ⇔ estación)**
  En la comunicación directa, las estaciones se comunican directamente entre sí sin que los telegramas sean transmitidos desde una central. Dos estaciones pueden comunicarse directamente entre sí a través de diferentes puntos de datos.
  Consulte la configuración en el capítulo Función de maestro de los puntos de datos (Página 148).

3.2 Direccionamiento

La configuración y la puesta en marcha del módulo de comunicación requieren la siguiente información:

Información de dirección del módulo de comunicación

Para el direccionamiento deben configurarse los parámetros siguientes en el módulo:

- Dirección ASDU
  Dirección del objeto informativo (estación) en la capa de enlace
  Se requiere la dirección ASDU para identificar el maestro y las estaciones en la red IEC.
- Índices de los puntos de datos (índice de punto de datos = dirección del objeto informativo)
  Consulte la configuración en Índice de punto de datos (Página 149).
- Dirección, según el tipo de red y de módulo:
  - Dirección IP y máscara de subred; alternativa: dirección IP de un servidor DHCP
    Si se utiliza DNS debe haber un servidor DNS (véase abajo) que sea accesible por el módulo.
  - Número de teléfono (para red de marcación)
  - Dirección WAN (para línea dedicada)

- Puerto Listener
  - Puerto Listener de la estación. El maestro necesita el número de puerto para establecer la conexión.
  - Puerto Listener de un dispositivo de terceros con la función "maestro"
- Dirección o direcciones del servidor DNS
  - Se requiere un servidor DNS cuando la estación envía solicitudes a dispositivos a través de su FQDN, por ejemplo el servidor NTP.
  - Se requiere un servidor DNS cuando el maestro establece conexiones con las estaciones a través de su FQDN.

Univocidad de las direcciones

El direccionamiento dentro de una subred y dentro del proyecto STEP 7 debe ser unívoco.

Si desea utilizar números de dispositivos/direcciones de estación duplicados en diferentes subredes, deberá crear dos proyectos STEP 7.

Univocidad de la dirección ASDU

En módulos con conexiones de Telecontrol que están configuradas mediante el editor "Datos de red", se comprueba la coherencia y la univocidad de la dirección.

En CP con versión de firmware ≤ V3.0 cuyas conexiones de Telecontrol se configuran mediante el grupo de parámetros "Estaciones interlocutoras", no es posible comprobar la coherencia y la univocidad de la dirección. En este caso, el propio usuario debe procurar que las direcciones sean unívocas.

Información de dirección del maestro

La siguiente información del maestro es necesaria para la configuración del módulo:

- Dirección ASDU (dirección del objeto informativo del maestro en la capa de enlace)
- Dirección del maestro, según el tipo de red:
  - Dirección IP / Máscara de subred + Número de puerto del puerto Listener del maestro
    o
    Mediante nombre DNS descomponible
    (se necesita la dirección del servidor DNS; el módulo debe poder acceder al servidor DNS).
  - Número de teléfono (para red de marcación)
  - Dirección WAN (para línea dedicada)

Maestro IEC redundante

Ambos dispositivos de un maestro redundante tienen una dirección ASDU idéntica.

Solo se requieren direcciones IP o nombres de host diferentes.

Configuraciones con conexiones vía Internet: conexiones VPN

En las conexiones por Internet es posible utilizar direcciones IP dinámicas.

Para permitir la comunicación en ambos sentidos y, por consiguiente, transferir los datos de forma protegida, se requiere una conexión con túnel VPN. Para ello son adecuados los módulos de seguridad de las series SCALANCE S o SCALANCE M.

Para realizar la configuración tenga en cuenta los puntos siguientes:

- La dirección IP del maestro se configura del modo habitual.
- En la configuración de la interfaz del módulo se configura la dirección IP del router.
- La configuración VPN con SCALANCE S/SC/M se realiza en STEP 7 tanto para las estaciones como para la central de control.

3.3 Establecimiento de la conexión

Establecimiento de conexión

El maestro establece la conexión (modo de llamada /sondeo). también para estaciones con puntos de datos que tienen activada la opción "Función de maestro".

Si se interrumpe una conexión establecida desde el CP, un módulo maestro intenta establecer de nuevo la conexión.

Nota

Interrupción de la conexión por parte del operador de la red de telefonía móvil

Cuando utilice servicios de telefonía móvil, recuerde que las conexiones existentes pueden ser interrumpidas por los operadores de las redes de telefonía móvil con fines de mantenimiento.

Establecimiento de la conexión con Open User Communication y comunicación PG/OP

En la Open User Communication, la CPU es el interlocutor de la conexión en una estación S7.

Las conexiones se establecen en cuanto se llaman los bloques de programa correspondientes en la CPU.

Esto también se aplica cuando otra estación S7 envía datos. En este caso, la estación receptora llama los bloques de recepción correspondientes.

3.4 Acuse

Mecanismos de acuse con el protocolo IEC 60870-5-104

Configuración: Interfaz del módulo > "Opciones avanzadas" > Ajustes de transferencia - IEC 60870-5"

El módulo 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 del módulo.

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

Los telegramas de datos 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 módulo.

Parámetro:

- **k: Diferencia entre número de secuencia de emisión N(S) y el número de secuencia de recepción N(R)**
  Número máximo de telegramas de datos sin acusar (I-APDU) 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 módulo deja de enviar telegramas de datos hasta que el maestro ha acusado todos los telegramas de datos enviados.
  Si se alcanza k y t_1 ha concluido, se deshace la conexión TCP.
- **w: Número máximo de telegramas de datos no acusados**
  Número máximo de telegramas de datos (I-APDU) recibidos, alcanzado el cual el maestro debe confirmar el telegrama de datos recibido más antiguo.

Consulte la configuración en el capítulo Ajustes de transferencia - IEC 60870-5 (Página 71).

Recomendaciones de la especificación:

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

Configuración

4

4.1 Tipos de comunicación

"Tipos de comunicación"

En este grupo de parámetros se activa la capacidad de comunicación del módulo.

En función del tipo de módulo es posible definir el protocolo de Telecontrol y otros tipos de comunicación.

- **Activar comunicación por Telecontrol**
  Activa la comunicación por Telecontrol con los interlocutores de la comunicación.
- **Tipo de protocolo**
  - ST7
  - DNP3
  - IEC 60870-5
  - TeleControl Basic
- **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.
  Los siguientes módulos soportan el routing S7:
  - CP 1243-1, CP 124x-7, CP 1243-8
    A partir del firmware V2.1 del CP con CPU ≥ V4.2
  - CP 1542SP-1 IRC
    A partir del firmware V1.0 del CP con CPU ≥ V2.0
  - TIM 1531 IRC

  Recuerde:
  La desactivación de la función no es una medida de seguridad. Para proteger la estación utilice funciones de seguridad adecuadas, como cortafuegos, VPN o la protección por contraseña de la CPU.
- **Activar comunicación S7**
  Habilita en el módulo las funciones de la comunicación S7 con la CPU de la estación y el routing S7.
  Active esta opción si configura conexiones S7 con la estación en cuestión que pasan por el módulo.

No es necesario que la Open User Communication esté habilitada, pues en este caso deben crearse activamente los bloques de programa correspondientes. De este modo no es posible acceder involuntariamente al CP.

- **Activar la comunicación de Telecontrol a través de SINEMA Remote Connect**
  Configurable en:
  - CP 1243-1
  - CP 1243-7 LTE
  - CP 1243-8 IRC
  - CP 1542SP-1 IRC

  Encontrará más detalles en el anexo SINEMA Remote Connect (CP) (Página 213).

RTU3000C

Configuración

Para la RTU3000C deben configurarse los siguientes parámetros en el proyecto STEP 7:

- **Tipos de comunicación**
  - Tipo de protocolo
    El tipo de comunicación por Telecontrol configurado en la RTU
  - Conexión temporal
    Active la opción si la RTU está conectada por telefonía móvil y solo está conectada a la red temporalmente.
- **Interfaz Ethernet**
  - Ajustes WAN
    Tras seleccionar el protocolo de Telecontrol los ajustes son fijos.

  Dirección Ethernet
  - Dirección IP dinámica
    Esta opción debe activarse cuando el operador de la red de telefonía móvil asigna una dirección IP dinámica.
  - Dirección IP fija del operador de la red de telefonía móvil
    Introduzca aquí la dirección IP fija asignada a la RTU por el operador de red de telefonía móvil.
    Si hay un router de telefonía móvil intercalado, debe introducir aquí la dirección IP del router.
- **Números de dispositivos**
  - Número de dispositivo (RTU)
    Solo en ST7: Aquí se asigna el número de dispositivo de la RTU, tal como se ha configurado en el WBM de la RTU.
  - Número de dispositivo de la CPU (RTU)
    Aquí se asigna el número de dispositivo de la CPU, tal como se ha configurado en el WBM de la RTU.

- **Seguridad**
  Los ajustes de seguridad configurados en la RTU están activados de forma fija en STEP 7 en el ajuste predeterminado.
- **Conexión de Telecontrol**
  A continuación, cree la conexión de Telecontrol entre la RTU y su interlocutor de conexión en el editor "Datos de red > TeleControl".

Compilar y cargar

Los datos de configuración de STEP 7 no pueden cargarse en la RTU3000C. Por tanto, la RTU3000C no puede compilarse en STEP 7.

4.2 Ajustes básicos

Ajustes básicos de IEC

No todos los parámetros se muestran en cada tipo de módulo.

- **Puerto Listener**
  Puerto Listener propio del módulo. El maestro necesita el número de puerto para establecer la conexión.
  El número de puerto es válido para todas las interfaces del módulo de comunicación.
  Rango de valores: 1024...65535
  Ajuste predeterminado: 2404
- **Tamaño de la memoria de telegrama**
  Validez: TIM 1531 IRC
  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. Consulte el tamaño de la memoria de telegramas en "Prestaciones y capacidad funcional".
  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 (Página 151).
- **Duración máx. de comando**
  Validez: TIM 1531 IRC, CP 1542SP-1 IRC
  Antigüedad máxima de los comandos recibidos del tipo Single/Double command with time tag (<58>/<59>)
  Si en el momento de la recepción el sello de tiempo es más antiguo que el valor configurado aquí, el comando es rechazado sin señal de respuesta. El parámetro es evaluado por estaciones y estaciones nodo.
  Rango de valores: 1...65
  Ajuste predeterminado: 20

ASDU privadas

Validez: TIM 1531 IRC

Mediante el valor configurable se define la TYPE IDENTIFICATION del correspondiente tipo de ASDU. El "área privada" de 136...254 para la identificación de tipo está reservada para aplicaciones personalizadas.

El TIM comprueba la identificación de tipo de las ASDU privadas recibidas y evalúa el valor configurado en cada caso.

Si se ha configurado 0 (cero), el TIM no evalúa la identificación de tipo.

- **Tipo de ASDU para routing PG**
  Identificación de tipo para ASDU con el fin de transferir telegramas S7 (routing PG)
  Rango de valores: 136...254
  Ajuste predeterminado: 0
- **Tipo de ASDU para distribución de estado**
  Identificación de tipo para ASDU con el fin de transferir el estado de recorrido de la conexión
  Rango de valores: 136...254
  Ajuste predeterminado: 0
- **Tipo de ASDU para desconexión**
  Identificación de tipo para ASDU con el fin de anunciar la finalización de una conexión temporal
  Las conexiones temporales se establecen desde la RTU3000C.
  Rango de valores: 136...254
  Ajuste predeterminado: 0

Opciones de comunicación segura

Validez: TIM 1531 IRC, CP 1542SP-1 IRC

- **Puerto Listener seguro**
  Puerto Listener propio para la comunicación TLS.
  El número de puerto es válido para todas las interfaces del módulo de comunicación.
  Rango de valores: 1024...65535
  Ajuste predeterminado: 19998

Almacenamiento remanente de eventos

Validez: TIM 1531 IRC

Si en el TIM se utiliza una tarjeta SD opcional, en este grupo de parámetros se ajustan las condiciones para guardar los valores de telegramas cuyos puntos de datos están configurados como evento.

El comportamiento se ajusta con los parámetros siguientes:

- **Permitir almacenamiento remanente**
  En caso de fallos de conexión activa el almacenamiento remanente de eventos en la tarjeta SD.
- **Número de eventos antes del almacenamiento**
  El almacenamiento de los eventos en la tarjeta SD se aplica cuando en el búfer de transmisión se alcanza el número de eventos configurado aquí.

- **Tiempo de interrupción antes del almacenamiento**
  El almacenamiento de los eventos en la tarjeta SD se aplica cuando se alcanza el tiempo de interrupción de conexión configurado aquí.
- **Número máx. de eventos en archivo comprimido**
  Número máximo de eventos en el archivo comprimido guardado
  Cuando se rebasa este número se sobrescriben los eventos más antiguos.

Consulte el número máximo de eventos que se pueden almacenar en el capítulo Funciones, datos de prestaciones y capacidad funcional (Página 22).

Routing IP

Validez: TIM 1531 IRC

Nota

La función no está prevista para grandes volúmenes de datos.

Limite el routing a través del TIM a aproximadamente 1 Mbit/s para no perjudicar el funcionamiento productivo del TIM.

Routing IP

- **Permitir routing IP**
  Habilita el routing IP a través de las interfaces del módulo.
- **Recorrido de routing**
  Define las rutas para el routing IP:
  - Local: routing IP solo entre las interfaces Ethernet del módulo
  - A través de subredes routing IP a través de máx. 10 routers configurables, accesibles a través de las interfaces del módulo.

Direcciones de router

- **Interfaz Ethernet**
  Interfaz Ethernet del módulo a través de la cual debe configurarse el routing IP. Las direcciones IP de las interfaces utilizadas para el routing IP deben tener una configuración fija. Una interfaz puede seleccionarse varias veces para routers diferentes.

  Nota

  Coherencia de los parámetros de dirección

  STEP 7 no comprueba la coherencia entre las direcciones configuradas manualmente y los parámetros de las interfaces Ethernet del módulo.

  Asegúrese de que hay coherencia con los parámetros de dirección de la interfaz en cuestión.

- **Tipo de dirección**
  Selección de la versión IP de los parámetros de dirección (IPv4 / IPv6) configurados a continuación
  Si se utilizan direcciones IPv6 es necesario habilitar IPv6 para la interfaz correspondiente.
- **Dirección de red**
  Dirección de red del destino del routing (dirección IP ***** máscara de subred)

- **Máscara de subred / prefijo**
  Máscara de subred (IPv4) o prefijo (IPv6) del destino de routing
- **Dirección del router**

4.3 Ajustes de comunicación de telefonía móvil (CP 1243-7 LTE)

"Ajustes de telefonía móvil"

En este grupo de parámetros se configuran los parámetros siguientes:

- **Número de abonado del CP**
  Número de teléfono del CP
- **Activar PIN**
  Si el operador del servicio exige un PIN, active esta opción.
- **PIN**
  PIN de la tarjeta SIM
- **Activar servicios de datos**
  Activa para el CP la utilización de servicios de datos en la red móvil.

Nota

Desactivación posterior

En caso de que ya haya utilizado los servicios de datos durante el funcionamiento y los desactive posteriormente, deberá volver a cargar los datos de configuración y poner la CPU a STOP y seguidamente de nuevo a RUN.

- **GPRS (2G) / UMTS (3G) / LTE**
  Active el o los servicios de telefonía móvil que desee utilizar. Es posible habilitar servicios individuales o bien todos.
  "GPRS (2G)" solo se soporta en el CP 1243-7 LTE EU.
- **SMSC**
  Número de teléfono de la central SMS (Short Message Service Center)
  El campo dispone de las opciones siguientes:
  - Ningún número
    En el ajuste predeterminado, el CP incorpora los datos SMSC del operador del servicio directamente desde la tarjeta SIM insertada. Si desea utilizar el número de SMSC de la tarjeta SIM, deje el campo libre.
  - Número configurado
    Si desea utilizar otro SMSC, introduzca el número de teléfono de dicho SMSC.
    Tenga en cuenta lo siguiente:

    Nota

    Almacenamiento fijo del número de SMSC

    Cuando se configura un número de SMSC, el CP deja de acceder a los datos SMSC de la tarjeta SIM. Esto también sucede cuando se borra el número de SMSC de la configuración.

    Recomendación:
    cuando configure un número de SMSC, anote primero el número de SMSC de su operador del servicio, que se encuentra en la tarjeta SIM. De este modo, si lo desea podrá volver a utilizar más adelante el SMSC de su operador configurando el número de SMSC.

"Ajustes APN"

En este grupo de parámetros se configuran los datos del punto de acceso. El APN se necesita para enviar correos electrónicos.

El CP soporta APN con dirección IPv4 e IPv6.

Tenga en cuenta la consigna de seguridad del capítulo Recomendaciones Security (Página 13).

Introduciendo su país en el campo "País" puede seleccionar uno de los APN preasignados en la lista desplegable.

Otra posibilidad consiste en configurar el APN manualmente.

Nota

Configuración de nombre de usuario APN y contraseña

Si el operador del servicio exige un nombre de usuario APN y una contraseña, él mismo se los proporcionará.

Si el operador del servicio no exige ni nombre de usuario APN ni contraseña, es posible que sea necesario configurar un comodín para estos dos parámetros. Esto sucede, por ejemplo, cuando el operador utiliza el Provider Password Authentication Protocol (PAP) para la autenticación. En este caso, póngase en contacto con su operador para que le facilite los datos necesarios.

Los nombres de usuario y las contraseñas pueden contener hasta 64 caracteres. Encontrará los caracteres permitidos en el capítulo Juego de caracteres para nombres de usuario, contraseñas y mensajes (Página 179).

Si el operador del servicio no exige ni nombre de usuario APN ni contraseña, en determinados casos es aconsejable introducir de todos modos un comodín para estos dos parámetros.

"Lista de las redes preferentes"

En este grupo de parámetros se define el comportamiento de marcación del CP en diferentes redes de telefonía móvil.

"Configuración de TeleService"

TeleService solo puede utilizarse con la comunicación por Telecontrol activada. Encontrará la descripción de las funciones de TeleService en el manual de configuración; consulte SINEMA Remote Connect (CP) (Página 213).

Ajustes de restablecimiento de la conexión

En este grupo de parámetros existe la posibilidad de definir una condición controlada por disparo o una hora diaria en la cual el CP restablece la conexión de telefonía móvil.

Las conexiones de telefonía móvil pueden cortarse por diversos motivos. La causa puede ser intencionada (debido a bloques de programa o periodos de mantenimiento del operador de la red) o debida a fallos o dispositivos averiados en la red.

La función de este grupo de parámetros permite planificar con precisión la configuración de una conexión de telefonía móvil.

Mientras se establece la conexión se rechazan todas las solicitudes de funciones en el CP, hasta que este tiene una nueva dirección IP.

Parámetros

- Restablecimiento de la conexión
  Activa el restablecimiento previsto de una conexión de telefonía móvil
- Tipo de restablecimiento de la conexión
  - Rearranque completo incluido hardware
    Rearranque de las funciones de comunicación del CP, incluido el rearranque del motor de telefonía móvil
    Esta opción puede durar varios minutos.
  - Rearranque rápido
    Rearranque solo de la comunicación por telefonía móvil. El motor del telefonía móvil no se reinicia.
    Esta opción acorta ligeramente la duración del rearranque.

- Rearranque cíclico
  Activa el establecimiento de la conexión en una hora concreta.
  El rearranque cíclico está activado de forma fija en el ajuste predeterminado.
  Solo es posible desactivar el rearranque cíclico si se activa el "Disparo de rearranque".
- Tiempo de reconexión diario
  Aquí se especifica la hora diaria para establecer la conexión.
  Para ello, haga clic en las horas del campo de configuración e introdúzcalas con el teclado o con las teclas de flecha a la derecha. A continuación, haga clic en los minutos y ajústelos.
- Disparo de rearranque
  Activa el establecimiento de la conexión por medio de un disparo establecido por la CPU, por ejemplo, la aparición de un evento específico. Si se pone la variable de disparo a 1, se inicia el establecimiento de la conexión desde el CP.
- Variable de disparo
  Seleccione una variable (Bool) que ponga la CPU a 1 cuando se produzca el evento.
  Después de que se haya establecido la conexión de telefonía móvil, la variable de disparo se vuelve a poner a 0 automáticamente.

Para establecer la conexión puede combinar ambas opciones (cíclica y por disparo).

4.4 Sincronización horaria

Sincronización horaria y seguridad

Si en los módulos con seguridad están activadas las funciones de seguridad, encontrará el grupo de parámetros en "Security".

Con funciones de seguridad activadas hay que sincronizar periódicamente la hora del módulo de comunicación.

Fundamentos de la sincronización horaria

En las aplicaciones de Telecontrol que requieren sincronización horaria se debe sincronizar la hora del módulo de comunicación periódicamente. Si no se sincroniza la hora pueden producirse desviaciones de algunos segundos al día en los datos de tiempo de las estaciones.

El módulo de comunicación puede captar la hora externamente (consulte el procedimiento más adelante) y reenviar la hora a la estación o a las redes WAN conectadas.

Cuando se emplea una fuente horaria externa, la estación S7 conectada puede captar la hora actual tanto a través de la CPU como a través de un módulo de comunicación (TIM, CP).

Nota

Recomendaciones

- **Sincronización horaria solo mediante 1 módulo de la estación**
  Sincronice la hora de la estación de una fuente horaria externa con un solo módulo de la estación, para tener dentro de la estación una hora coherente.
  Si la CPU adopta la hora de un módulo de comunicación, desactive la sincronización horaria de la CPU.
  Si tanto en el módulo de comunicación como en la CPU la hora se sincroniza a través de NTP, siempre que sea posible utilice el mismo servidor NTP, para tener dentro de la estación una hora coherente.
- **Ciclos de sincronización más largos con redes inestables**
  Si una red presenta fallos de conexión frecuentes, es posible incrementar su ciclo de sincronización.
  De este modo se evita que, una vez transcurrido el instante de sincronización previsto por el cliente horario, los telegramas se marquen como "no válidos" y se rechacen.

Concepto horario

Antes de proceder a configurar la sincronización horaria especifique lo siguiente:

- Defina la fuente horaria en la red.
- Defina el reloj maestro de la red.
- Defina la o las redes a través de las cuales debe reenviarse la hora desde el reloj maestro a los relojes esclavos.

Métodos para recibir la hora

- **Sin origen de hora**
  El módulo no se sincroniza.
- **De WAN**
  El módulo adopta la hora de un interlocutor de la comunicación.
  IEC 60870-5 utiliza la hora local del maestro sin marca de horario de verano para la sincronización horaria de los módulos de comunicación.
- **De servidor NTP / NTP (secure)**
  El CP adopta la hora (UTC) de un servidor NTP configurable.
  - NTP
    NTP compatible con RFC5905
    Los servidores NTP pueden configurarse manualmente en la tabla.
  - NTP (secure)
    NTP compatible con RFC5905 y RFC5906 con Shared Key
    Los servidores NTP del tipo NTP (secure) se configuran en los ajustes globales de seguridad y pueden seleccionarse en el grupo de parámetros "Security > Sincronización horaria" del CP.

- **De estación local (CP)**
  El módulo adopta la hora (UTC) de la CPU.
  La CPU 1200 V4.2 y superior sincroniza todos los CM/CP de la estación con un ciclo de sincronización de 10 segundos.
  Parámetros de la CPU:
  Con la opción "La CPU sincroniza los módulos del dispositivo" se consigue que todos los CP de Telecontrol de la estación con firmware ≥ V2.1.77 se sincronicen con la hora de la CPU en un ciclo de sincronización de 10 segundos.
- **Establecimiento manual de la hora a través del WBM (TIM 1531 IRC)**
  Si se ha configurado una fuente horaria para el TIM, también es posible establecer la hora desde el WBM; consulte /2/ TIM 1531 IRC (Página 220).

Hora del CP durante el arranque

En CP del S7-1200 y del ET 200SP encontrará la siguiente opción dentro del grupo de parámetros "Recibir hora":

- Utilizar la hora del PLC antes de la primera sincronización por parte del maestro
  La opción puede activarse cuando se configura el origen de la hora "De WAN".
  - Si la opción está activada, durante el primer arranque, cuando todavía no se ha recibido ninguna hora del interlocutor por la WAN, el CP adopta la hora de la CPU.
  - Si la opción está desactivada, el CP no tiene ninguna hora válida durante el primer arranque.

En los CP con versión de firmware ≤ V2.0, el CP lee una vez durante el arranque la hora de la CPU, aunque como origen de la hora se haya seleccionado la opción "Sin origen de hora". En este caso, la siguiente sincronización horaria depende del método de sincronización configurado.

Grupo de parámetros "Hora": Ajustes de UTC y zona horaria

Los módulos de comunicación que usan el protocolo IEC 60870-5 utilizan la hora local de la central o del maestro con marca de horario de verano.

Validez:

Las funciones de este grupo de parámetros son válidas para:

- CP 1242-7, CP 1243-1, CP 1243-7 LTE, CP 1243-8 a partir de la versión de firmware V3.5
- CP 154xSP-1 a partir de la versión de firmware V2.3
- TIM 1531 IRC a partir de la versión de firmware V2.4

Interpretación de la hora por parte de los módulos de comunicación de Telecontrol

En STEP 7, los módulos de comunicación citados anteriormente guardan la hora como tipo de datos "DTL".

El módulo de comunicación interpreta la hora como hora local sin marca de horario de verano.

Parámetros:

- Aplicar valores de zona horaria con horario de verano del PLC
  Si la opción está activada, el módulo de comunicación adopta la zona horaria de la CPU con ajustes de horario de verano.
  TIM 1531 IRC: la opción se habilita cuando la CPU está asignada al TIM (grupo de parámetros "Números de dispositivos").
- Zona horaria
  Aquí se ajusta la zona horaria local que debe utilizar el módulo de comunicación.
- Utilizar UTC
  - Opción activada:
    El módulo utiliza UTC en la comunicación con su interlocutor. En caso de sincronización por WAN, el módulo de comunicación espera la hora del interlocutor como UTC.
  - Opción desactivada:
    El módulo de comunicación utiliza la hora local de la estación.

  Si el módulo de comunicación recibe la hora de WAN y sincroniza la CPU, transfiere la hora a la CPU como UTC, independientemente de si esta opción está activada o no.
  Las entradas de diagnóstico online de la estación y las entradas del WBM del TIM 1531 IRC se muestran como hora local del PC.

Si el módulo de comunicación no adopta la zona horaria de la CPU, tiene la posibilidad de configurar el cambio entre horario de verano y horario de invierno:

- Activar cambio de horario de verano
  Activa el cambio de horario (horario de verano/invierno)
- Diferencia entre horario de invierno y verano
  Diferencia horaria en minutos entre el horario de verano y de invierno
- Principio del horario de verano/horario de invierno
  Aquí se configura el momento en que cambia la hora:
  - Semana del mes
    Ejemplo:
    "Primero" significa el "primer domingo de marzo" si se han configurado "domingo" como día de la semana y "marzo" como mes.
  - Día de la semana
  - "en" = mes
  - "a las" = hora del cambio

Reenvío de la hora del CP a la CPU

Nota

Reenvío de la hora a la CPU

Dependiendo de la versión de firmware de los módulos participantes, la hora del CP puede reenviarse a la CPU de diferentes modos.

- Reenvío opcional de la hora del CP a la CPU mediante una variable PLC:
  - S7-1200
  - ET 200SP
- Reenvío de la hora del CP a la CPU mediante el bus de fondo, a partir de las versiones de firmware mencionadas más abajo:
  - S7-1200
  - ET 200SP

El reenvío de la hora del CP a la CPU depende de la versión de firmware del CP y de la CPU. Tenga en cuenta el comportamiento siguiente.

- **Reenvío de la hora del CP mediante una variable PLC**
  Esta es la única posibilidad de reenviar la hora del CP a la CPU en el caso de las versiones de firmware siguientes:
  - S7-1200: firmware del CP ≤ V2.1.5
  - ET 200SP: firmware del CP ≥ V2.0

  Opcionalmente, con esta versión de firmware la hora del CP puede ponerse a disposición de la CPU utilizando una variable PLC. Si esta variable PLC es leída cíclicamente por la CPU, esta adopta la hora del CP.
  La variable PLC se configura en el grupo de parámetros "Comunicación con la CPU" del CP.
- **Reenvío de la hora del CP a la CPU mediante el bus de fondo**
  La hora del CP se reenvía automáticamente a la CPU si en el CP se ha configurado un método de sincronización y el CP y la CPU tienen una de las versiones de firmware siguientes:
  - S7-1200: firmware del CP ≥ V3.0 y firmware de la CPU ≥ V4.2
    Si en la CPU está activada la opción "La CPU sincroniza los módulos del dispositivo" en "Interfaz PROFINET > Sincronización horaria", todos los módulos inteligentes de la estación se sincronizan con la hora de la CPU.
  - ET 200SP: firmware del CP ≥ V2.1 y firmware de la CPU ≥ V2.0
    A partir de la versión de firmware V2.1 del CP, solo 1 módulo puede ser servidor horario en la estación. Este módulo distribuye la hora dentro de la estación. Si desea que la hora de la estación se sincronice por medio de la CPU, desactive la sincronización horaria en el CP.
    Puesto que la CPU adopta automáticamente la hora del CP, con estas versiones de firmware ya no se requiere la opción de reenvío mediante la variable PLC.

Los CP no soportan el reenvío de la hora a las subredes conectadas.

Reenvío de la hora por parte del TIM

El TIM puede reenviar la hora de la siguiente forma:

- **A redes conectadas**
  Configuración mediante "Sincronización horaria" > "Enviar hora" o "Recibir hora"
  El procedimiento de configuración difiere en Ethernet y en las redes WAN clásicas, consulte más adelante.
- **A las CPU asignadas**
  Configuración mediante "Sincronización horaria" > "Enviar hora"

Configuración en la interfaz Ethernet del TIM

Servidor horario

1. En el grupo de parámetros "Recibir hora" del TIM que va a ser el servidor horario, configure el origen de la hora con una de las opciones siguientes:
   - De servidor NTP
   - De WAN
     (adoptar la hora de una red)
2. La interfaz del TIM a través de la que van a reenviarse los telegramas horarios se configura en el grupo de parámetros "Ajustes WAN" como tipo de noto de red "Estación central".
3. En el grupo de parámetros "Enviar hora", active la opción "Enviar hora a WAN..." para la interfaz del paso 2.
   Los telegramas horarios se reenvían a la red conectada.
4. En caso necesario, en el grupo de parámetros "Enviar hora" active la opción "A estación local" si también debe sincronizarse la CPU asignada.
   En caso de utilizar TD7onCPU:
   Active en este caso también el reenvío de la hora por la interfaz del TIM que está conectado en red con la CPU.

Clientes horarios

1. Las interfaces de los restantes módulos TIM que serán relojes esclavos se configuran en el grupo de parámetros "Ajustes WAN" como tipo de nodo de red "Estación nodo" o "Estación". La función es compatible con la interfaz Ethernet y con la interfaz serie.
2. Conecte entre sí en red las interfaces de los módulos TIM involucrados y con la interfaz del servidor horario.
3. En las estaciones ajuste los parámetros de la sincronización horaria en el grupo de parámetros "Recibir hora".
4. En caso necesario, en el grupo de parámetros "Enviar hora" active la opción "A estación local" si también debe sincronizarse la CPU asignada.
   En caso de utilizar TD7onCPU:
   Active en este caso también el reenvío de la hora por la interfaz del TIM que está conectado en red con la CPU.

Configuración en el TIM y en redes WAN

Grupos de parámetros para la sincronización horaria

Para configurar la sincronización horaria se dispone de los siguientes grupos de parámetros:

- **TIM**
  - **Recibir hora**
    Aquí se define de cuál de las redes conectadas va a recibir la hora el TIM.
    - TIM central: por lo general, de la central de control
    - Estación nodo: define por qué interfaz (tipo de nodo de red "Estación nodo") el TIM recibe la hora del TIM central.
    - Estación: define por qué interfaz el TM recibe la hora del TIM central o de una estación nodo.
  - **Enviar hora**
    - TIM central (servidor horario): define a qué redes reenvía la hora el TIM.
    - Estación nodo: define por qué interfaz (tipo de nodo de red "Estación central") el TIM reenvía la hora a redes subordinadas.
- **Red WAN clásica**
  Para redes clásicas la "Sincronización horaria" se activa en el grupo de parámetros homónimo de la red. Aquí también se define el ciclo de sincronización.
  A continuación, los ajustes de sincronización los incorporan todos los módulos TIM conectados; véase más abajo.
  El sentido de transmisión de los telegramas horarios se deduce automáticamente del tipo de nodo de red de las interfaces conectadas:
  Estación central ⇒ Estación nodo ⇒ Estación

Configuración de la sincronización horaria vía redes WAN clásicas

Módulos TIM (servidor horario y clientes)

1. En el grupo de parámetros "Recibir hora" del TIM que va a ser el servidor horario, configure el origen de la hora con una de las opciones siguientes:
   - De servidor NTP
   - De WAN
     (adoptar la hora de una red/central)
2. Configure la interfaz del TIM maestro al que están conectadas las estaciones subordinadas o estaciones nodo, con el tipo de nodo de red "Estación central".
3. Las interfaces de los restantes módulos TIM (clientes horarios) se configuran con el tipo de nodo de red "Estación nodo" o "Estación".
4. En caso necesario, en el grupo de parámetros "Enviar hora" de las estaciones active la opción "A estación local" si también debe sincronizarse la CPU asignada.
   En caso de utilizar TD7onCPU:
   Active en este caso también el reenvío de la hora por la interfaz del TIM que está conectado en red con la CPU.

Red WAN

1. Conecte en red con la red WAN pertinente las interfaces serie de los módulos TIM involucrados.
2. En el grupo de parámetros "Sincronización horaria" de la red WAN active la opción "Activar sincronización horaria para WAN".
3. En ella continúe configurando el ciclo de sincronización deseado.
4. En las interfaces serie de las estaciones (clientes horarios), active el origen de la hora "De WAN".
   En los módulos TIM conectados los ajustes configurados en la red WAN se incorporan en los siguientes grupos de parámetros:
   - En el servidor horario (Estación central): grupo de parámetros "Enviar hora" (interfaz serie)
   - En los clientes horarios (estaciones nodo/estación): grupo de parámetros "Recibir hora" (interfaz serie)

   El sentido de transmisión de los telegramas horarios se deduce automáticamente del tipo de nodo de red de las interfaces conectadas:
   Estación central ⇒ Estación nodo ⇒ Estación

Opcional: varios servidores horarios

Si hay varios servidores horarios conectados a la red, es posible definir un dispositivo concreto como servidor horario:

1. Configure las conexiones de Telecontrol utilizando las interfaces de ambos dispositivos.
2. Después de crear las conexiones de Telecontrol, existe la posibilidad de seleccionar en el cliente horario el interlocutor configurado mediante la conexión.
   Selección en el parámetro "Recibir hora > Obtener hora del interlocutor" de la interfaz serie

Alternativamente:
Con el ajuste "No hay interlocutores de conexión o son aleatorios", el módulo de comunicación acepta la hora de todos los servidores horarios conectados.

4.5 Configuración de interfaces, redes y nodos de red

4.5.1 Conectar las interfaces en red

Interfaces de los módulos

La ubicación de las interfaces de los módulos en el símbolo de dispositivo de STEP 7 (vista de redes) se corresponde en líneas generales con la configuración del dispositivo.

Las interfaces de un TIM 1531 IRC, por ejemplo, tienen la ubicación siguiente:

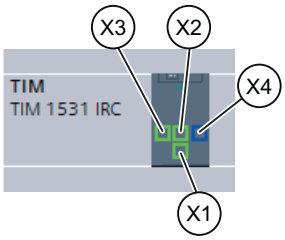


Figura 4-1 Símbolo de dispositivo del TIM con números de interfaces

Conexión de interfaces en red

Para conectar interfaces en red se dispone de diferentes oportunidades, en función de la situación de partida:

- Crear una subred
- Conectar dos dispositivos de destino a través de una nueva subred
- Conectar los dispositivos a una subred existente
- Seleccionar una subred existente en la lista "Subred"

Encontrará la descripción de cada uno de los métodos en el sistema de información de STEP 7.

Conexión en red de interfaces WAN

Recomendación para la conexión en red:

Para conectar en red las interfaces con una red WAN se recomienda el procedimiento siguiente:

1. Conecte en red las redes WAN en la vista de redes de STEP 7.
   La vista gráfica de redes ofrece una visión general de las subredes existentes en toda la instalación del proyecto.
2. Configure primero los parámetros de interfaz que se describen en el capítulo Ajustes WAN de las interfaces (Página 53):
   - Tipo WAN
   - Tipo de red
   - Tipo de nodo de red
   - Tipo de módem
3. Seleccione la interfaz correspondiente para crear una red WAN nueva. Alternativa:
   En el grupo de parámetros "Conectar interfaz en red con" de la interfaz:
   - Mediante el botón "Agregar nueva subred"

   En la interfaz, en el símbolo de dispositivo del módulo:
   - Mediante el menú contextual "Crear subred"
   - Gráficamente arrastrando (mantener pulsado el cursor del ratón) hasta el símbolo de interfaz del interlocutor

   Se crea una red WAN nueva que adopta el tipo de red de la interfaz conectada.

Representación de una red WAN clásica

En azul se representa una red WAN clásica.

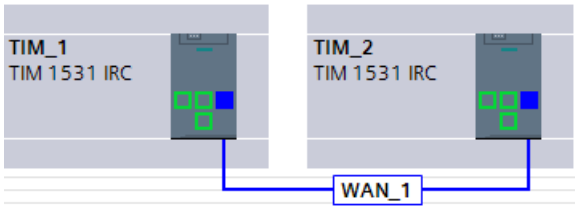


Figura 4-2 Módulos TIM, interfaces serie conectadas en red a través de WAN clásica.

Red con estación nodo

En la figura siguiente, el TIM central es una estación nodo. El parámetro "Tipo de nodo de red" de las interfaces está configurado del siguiente modo:

- Interfaz en dirección a la central: "Estación nodo"
- Interfaz en dirección a la red subordinada: "Estación central"

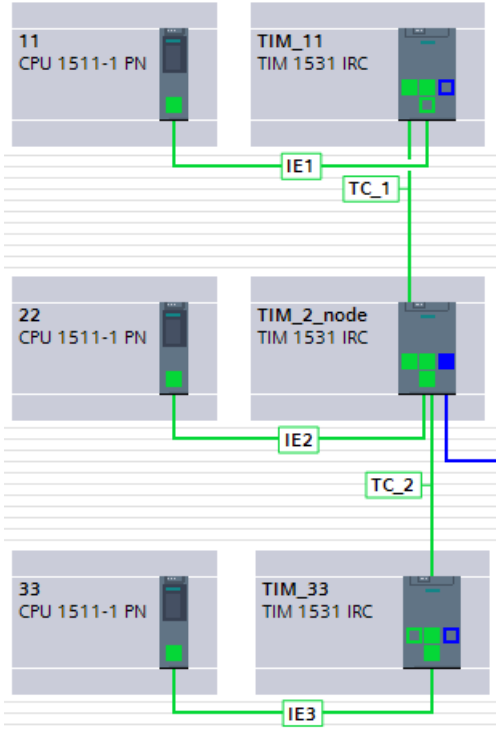


Figura 4-3 Red con estación central (arriba), estación nodo (centro) y estación (abajo)

4.5.2 Ajustes WAN de las interfaces

Ajustes WAN

Los parámetros siguientes determinan las propiedades de las interfaces y las redes WAN conectadas.

Configure primero la interfaz correspondiente del módulo. La red WAN conectada a continuación incorpora los ajustes más importantes.

- **Tipo WAN**
  Selección del tipo WAN de la interfaz:
  - Basado en IP
    Ajuste estándar de la interfaz Ethernet
  - WAN clásica
    Ajuste predeterminado de una interfaz serie
- **Tipo de red**
  Para WAN basada en IP:
  - IEC 60870-5
    Ajuste para interfaces que se utilizan para la transferencia de datos por Telecontrol.
  - Neutro
    Ajuste para interfaces en conexiones S7, por ejemplo, la conexión del TIM 1531 IRC con la CPU que tiene asignada.

  Adicionalmente, en las tres interfaces Ethernet del TIM 1531 IRC:
  - TIM primario
    (con redundancia de dispositivos)
  - TIM de reserva
    (con redundancia de dispositivos)

  Tenga en cuenta las particularidades de la redundancia de dispositivos del TIM 1531 IRC; consulte el capítulo Redundancia de dispositivos del TIM 1531 IRC (Página 57).
  Para WAN clásica:
  - Línea dedicada
  - Red de marcación

  Las redes WAN clásicas solo son compatibles con módulos TIM.

- **Tipo de nodo de red**
  Determina el Tipo de nodo de red de la interfaz:
  - Estación central
  - Estación nodo
    Para módulos que actúan de estación nodo, las interfaces se configuran del siguiente modo:
    - Interfaz en dirección a la central: "Estación nodo"
    - Interfaz en dirección a la red subordinada: "Estación central"
  - Estación

  Encontrará una figura en el capítulo Conectar las interfaces en red (Página 50).
- **Tipo de módem**
  El tipo de módem para la conexión a la interfaz serie debe configurarse para el tipo de red "Red de marcación" y, en los módulos TIM clásicos, también para el tipo de red "Línea dedicada".
  Las entradas tienen el siguiente significado:
  - MD2
    Módem para líneas dedicadas (tipo de red "línea dedicada")
  - MD3
    Módem para redes de marcación analógicas (tipo de red "red de marcación")
  - MD4
    Módem RDSI (tipo de red "red de marcación")
  - MD720
    El módem GSM MD720 no se soporta porque utiliza el formato de telegrama FT2.
  - Módem externo
    Cualquier módem compatible con los tipos de red "Línea dedicada" o "Red de marcación" (analógica / RDSI / GSM)

4.6 Interfaz Ethernet

4.6.1 Direcciones Ethernet

La interfaz Ethernet

- **CP Ethernet**
  La comunicación por Telecontrol de los CP Ethernet transcurre a través de la interfaz Ethernet. Configure los parámetros necesarios.
- **CP de telefonía móvil**
  Los CP de telefonía móvil no tienen ninguna interfaz Ethernet física.
  En STEP 7 se utiliza la interfaz Ethernet como comodín para configurar diferentes parámetros de dirección y vigilancia.
  Si se utilizan las funciones de seguridad hay que conectar en red la interfaz.

Direcciones Ethernet

Aquí se configura la dirección IP del CP y la conexión de red.

Si se activan las funciones de seguridad, por ejemplo para utilizar la comunicación por Telecontrol, deberá conectarse el CP en red por motivos de coherencia. Para ello debe crearse una red Ethernet cualquiera.

Recuerde:
Para las siguientes aplicaciones se requiere una dirección IP fija (IPv4/IPv6):

- Si se utiliza la comunicación S7
- Si se reciben datos vía Open User Communication
- Si se utiliza VPN
- Si se utiliza SINEMA Remote Connect

Utilizar protocolo IPv6

Además de IPv4, existe la posibilidad de activar IPv6 para el CP.

Opciones para CP de telefonía móvil:

- **Dirección IP dinámica**
  Active esta opción si el operador de red asigna dinámicamente la dirección IP al CP.
- **Dirección IP fija del operador de la red de telefonía móvil**
  Active esta opción si dispone de un contrato de telefonía móvil según el cual el operador de red asigna una dirección IP fija al CP.

Interfaz Ethernet > Puerto [Xn P1]

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

Para la configuración de los ajustes WAN consulte el capítulo Ajustes WAN de las interfaces (Página 53).

4.6.2 Opciones avanzadas

4.6.2.1 Vigilancia de conexión TCP

Interfaz Ethernet > Opciones avanzadas > Vigilancia de conexión TCP

Los ajustes de los dos parámetros en la interfaz Ethernet se aplican para todas las conexiones TCP a través de esta interfaz.

En los CP de telefonía móvil, la interfaz Ethernet es un comodín para la interfaz de telefonía móvil.

Los parámetros pueden adaptarse para cada sección de conexión en las propiedades de las conexiones de Telecontrol. El valor situado debajo de la sección de conexión es válido para dicha sección de conexión y sobrescribe el valor configurado en la interfaz.

Si hay valores distintos en la interfaz y en la sección de conexión, asegúrese de que el valor que hay en la interfaz sea mayor que el valor que hay en la sección de conexión.

- **Tiempo de supervisión de conexión TCP**
  Función: Si dentro del tiempo de vigilancia de conexión TCP no hay tráfico de datos, el módulo de comunicación envía un telegrama Keep Alive al interlocutor y espera su respuesta dentro del tiempo de vigilancia TCP Keep Alive.
  Ajuste predeterminado: 180 s
  Con cero (0) la vigilancia está desactivada.
  El rango admisible depende del tipo de módulo.
- **Tiempo de vigilancia TCP Keep Alive**
  Tras enviar un telegrama Keep Alive, el módulo espera una respuesta del interlocutor dentro del timeout de Keep Alive. Si el módulo no recibe ninguna respuesta tras tres telegramas Keep Alive, deshace la conexión.
  Con el valor 0 (cero) la función está desactivada.
  Ajuste predeterminado: 10 s
  El rango admisible depende del tipo de módulo.
  Si en una red de telefonía móvil se producen con frecuencia perturbaciones o retardos en la transmisión, es aconsejable aumentar el valor a 30 o 60 segundos, por ejemplo.

Si hay valores distintos en la interfaz y en la sección de conexión, asegúrese de que el valor que hay en la interfaz sea mayor que el valor que hay en la sección de conexión.

4.6.2.2 Ajustes de transferencia

Encontrará los parámetros específicos del protocolo de Telecontrol en el capítulo Parámetros IEC de las interfaces (Página 71).

4.6.2.3 Tamaño de MTU

Tamaño de MTU

Opción para reducir el tamaño máximo de paquetes para una interfaz en la capa OSI 3 (Maximum Transmission Unit - MTU)

Si en una instalación el tamaño de los telegramas (p. ej. segmentos) está limitado, esta opción permite reducir el tamaño de los paquetes que envía el módulo de comunicación.

Rango de valores: 1000 .. 1500 Byte

Ajuste predeterminado: 1500

4.6.3 Acceso al servidor web

4.6.3.1 CP

Acceso al servidor web de la CPU

El servidor web se encuentra en la CPU. A través del CP se accede al servidor web de la CPU.

Desde un PC es posible acceder al servidor web de la estación si el PC está conectado a la red de la instalación vía LAN.

Encontrará información sobre el servidor web del S7-1200 en el manual /7/ S7-1200 Manual de sistema (Página 221).

Encontrará información sobre el servidor web del ET 200SP en el manual /8/ ET 200SP Manual de sistema (Página 221).

4.6.3.2 TIM 1531 IRC

Acceso al servidor web

Es posible activar el acceso al servidor web del TIM a través de HTTP/HTTPS individualmente para cada interfaz Ethernet.

En el ajuste predeterminado el acceso está desactivado. Tenga en cuenta las indicaciones al respecto del capítulo Recomendaciones Security (Página 13).

La activación del servidor web y otros ajustes se realizan en el grupo de parámetros "Servidor web", consulte el capítulo Servidor web (TIM 1531 IRC) (Página 77). Allí también es posible activar y desactivar el acceso.

Para el acceso al servidor web es necesario habilitar el acceso a la interfaz Ethernet ("Acceso al servidor web") y activar el propio servidor web (grupo de parámetros "Servidor web").

4.7 Redundancia de dispositivos del TIM 1531 IRC

Validez de la redundancia de dispositivos

Las siguientes variantes de redundancia de dispositivos son válidas para:

- Módulo de comunicación
  - TIM 1531 IRC
    Versión de firmware: V2.4 o superior
    Uso como estación

  junto con:
- CPU
  - S7-1500R
  - S7-1500H
- Protocolos de Telecontrol
  - DNP3
  - IEC 60870-5
- Sistemas de central de control soportados
  - SIMATIC PCS 7 TeleControl

Posibilidades de la redundancia

- **Redundancia de la conexión**
  Con un solo módulo de comunicación de Telecontrol es posible establecer conexiones redundantes con un interlocutor.
  Consulte las conexiones redundantes en:
  Tabla de conexiones (Página 121)
  La siguiente figura muestra una posibilidad de configuración.

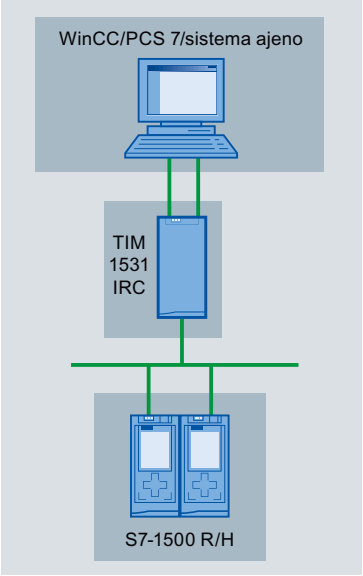


Figura 4-4 Ejemplo de redundancia de la conexión

- **Redundancia de dispositivos**
  Con el TIM 1531 IRC a partir de la versión citada arriba es posible establecer una redundancia de dispositivos en una estación con el fin de comunicarse con un PC PCS 7 redundante.
  Los dos módulos TIM se conectan en tiempo de ejecución para sincronizar los datos y para fines de vigilancia (conexión de sincronización). Con ello, el búfer de transmisión de ambos módulos TIM es idéntico.
  La conexión de sincronización de los dos módulos TIM puede establecerse a través de una interfaz Ethernet cualquiera del TIM.

  – El TIM primario es el módulo activo en estado normal.

  – El TIM de reserva es el módulo pasivo en estado normal.
    Solo se encarga de la comunicación en caso de que falle la conexión del TIM primario.

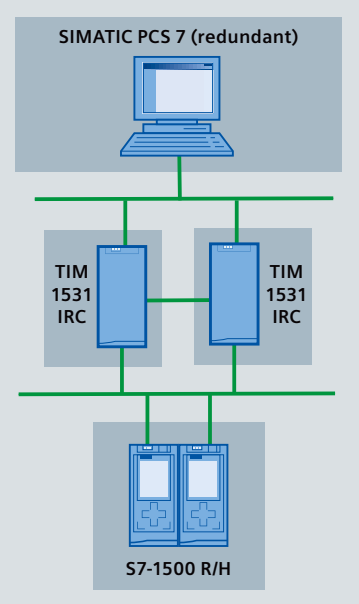


Figura 4-5 Redundancia de dispositivos del TIM 1531 IRC en una estación - estado normal

Casos de aplicación de la redundancia de dispositivos

La figura siguiente muestra en la parte superior el estado normal y, en la parte inferior, los escenarios de fallo en los que se mantiene la comunicación debido a la redundancia de dispositivos.

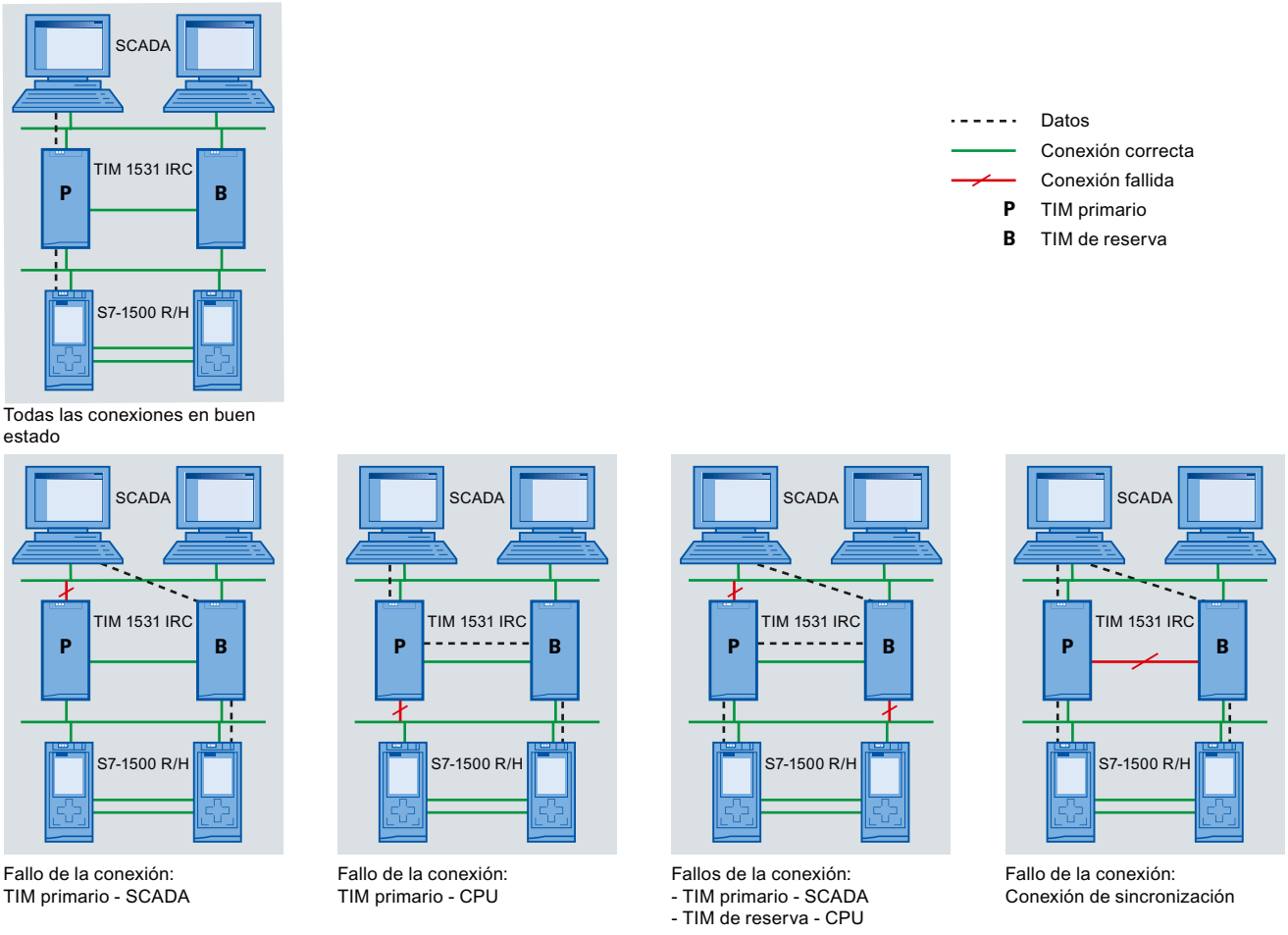


Figura 4-6 Fallos absorbidos por la redundancia de dispositivos (fallos de la conexión)

La redundancia de dispositivos mantiene la comunicación en los siguientes casos:

- Fallo de la conexión entre el TIM primario y un sistema SCADA
- Fallo de la conexión entre el TIM primario y la CPU local
- Fallo de la conexión entre el TIM primario y un sistema SCADA y fallo de la conexión entre el TIM de reserva y la CPU local
- Fallo de la conexión de sincronización entre el TIM primario y el TIM de reserva
  En este escenario, los datos del TIM primario y del TIM de reserva se respaldan para el sistema SCADA.

Nota

Fallos absorbidos

La redundancia de dispositivos está diseñada para los fallos de la conexión que se reproducen aquí.

En caso de que se produzcan a la vez varios fallos o bien otros fallos, es posible que se pierdan datos.

Nota

Fallos no absorbidos

La detección de un fallo de conexión entre el TIM y la CPU requiere cierto tiempo.

Los cambios realizados en la gestión de datos de la CPU durante el período comprendido entre el fallo de la conexión (TIM-CPU) y la detección del mismo se pierden.

Configuración de la redundancia de dispositivos

Para la configuración proceda del siguiente modo. Solo se ejecutan los pasos más importantes y necesarios para el modo redundante.

CPU

1. Cree una estación con una CPU R o una CPU H.
2. Configure los parámetros necesarios en "Protección y seguridad".
3. Asigne una dirección IP propia a ambas CPU redundantes.
4. Asigne a la CPU la dirección IP de sistema común.
   Los módulos TIM redundantes acceden a la CPU por la dirección IP de sistema.
   La dirección IP de sistema debe estar en la misma subred que las direcciones IP de las interfaces de las dos CPU.

TIM 1531 IRC

1. Cree dos TIM 1531 IRC.
2. Conecte en red los dos TIM a través de una interfaz cada uno con una interfaz libre de la respectiva CPU R/H.
   El "Tipo de red" (grupo de parámetros "Ajustes WAN") de las interfaces de los dos TIM conectados a la CPU es "Neutro".
   Los TIM se comunican con las CPU por su dirección IP de sistema.
3. Conecte en red los dos módulos TIM entre sí por una de sus interfaces Ethernet en cada caso (conexión de sincronización).
4. Seleccione uno de los dos TIM como TIM primario (el TIM activo en servicio normal).
   Para ello, en la interfaz de la conexión de sincronización ajuste el "Tipo de red" (grupo de parámetros "Ajustes WAN") de la interfaz a "TIM primario".
5. En caso necesario, cambie el puerto para redundancia de dispositivos (ajuste predeterminado 5000).
   La ID de redundancia de dispositivos se asigna automáticamente en el ajuste predeterminado y se muestra en los dos TIM del grupo de redundancia.
   Como alternativa, también es posible configurar manualmente la ID de redundancia de dispositivos. Sin embargo, en este caso STEP 7 no comprueba la coherencia.
6. Configure el otro TIM del grupo de redundancia como TIM de reserva (el TIM pasivo en servicio normal).
   Para ello, ajuste el "Tipo de red" (grupo de parámetros "Ajustes WAN") de la interfaz de la conexión de sincronización a "TIM de reserva".
   Debajo del número del puerto para redundancia de dispositivos se muestra en el TIM de reserva el valor que se ha configurado para el TIM primario.

7. Para el TIM de reserva, seleccione en el grupo de parámetros "Redundancia de dispositivos" el TIM primario en la lista desplegable "TIM primario".
8. Configure "Tipo WAN" y "Tipo de red" en las dos interfaces Ethernet restantes del TIM del siguiente modo:
   Interfaz hacia la CPU: "Basado en IP"/"Neutro"
   Interfaz hacia el CP Ethernet del PC PCS 7 (PC maestro):
   – DNP3: "Basado en IP"/"DNP3", Tipo de nodo de red "Estación"
   – IEC: "Basado en IP"/"IEC 60870-5", Tipo de nodo de red "Estación"
9. Asigne el TIM primario a su CPU local con la que está conectado en red (grupo de parámetros "Números de dispositivos").
   Si el grupo de redundancia se ha creado previamente, el TIM de reserva se asignará automáticamente a continuación a la CPU primaria.

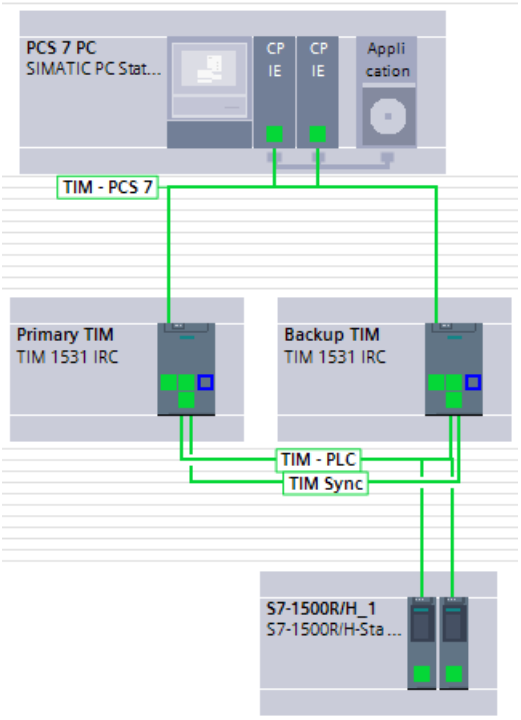


Figura 4-7 Configuración en STEP 7

Configure a continuación las conexiones de Telecontrol, los demás parámetros, variables y puntos de datos, etc.

Conexión de sincronización: Comunicación segura

Para la conexión de sincronización entre los módulos TIM redundantes existe la posibilidad de configurar una comunicación segura desde el siguiente grupo de parámetros:

- Interfaz > Ajustes WAN > Redundancia de dispositivos > Secure Communication (TLS)
  - ID de certificado propio
    ID del certificado propio
  - ID de certificado de interlocutor
    ID del otro TIM en el grupo de redundancia
  - Intervalo de cambio de clave de sesión
    Período (en minutos) tras el cual se renueva la clave de sesión.
    Los valores configurados en ambos TIM deben estar equiparados.

Nota

Recuerde que la velocidad de transferencia se reduce en conexiones protegidas por TLS.

Particularidades de la configuración del TIM con redundancia de dispositivos

El TIM primario se configura del modo habitual.

Parámetros idénticos para el TIM primario y el TIM de reserva

Los siguientes datos son idénticos en los dos TIM del grupo de redundancia. Cuando se configura un TIM se aplican del otro TIM redundante:

- Dirección en la capa de aplicación
  La dirección de estación/dirección ASDU del grupo de redundancia es idéntica.

Adopción de datos del TIM primario por parte del TIM de reserva

Las siguientes funciones y los siguientes parámetros se configuran por igual en el TIM primario y en el TIM de reserva. Un TIM adopta los datos de configuración del otro TIM redundante:

- Ajustes básicos (excepto routing IP)
- Tipo de comunicación
- Interfaz de la conexión de sincronización > Ajustes WAN > Redundancia de dispositivos
  - Redundancia de dispositivos > ID de redundancia de dispositivos
    En caso de generación automática, la ID de redundancia de dispositivos se forma después de compilar el TIM primario.
    Si la configuración es coherente, se aplica la misma ID para el TIM de reserva.
    Observe la nota más abajo (Configuración y carga).
  - Secure Communication (TLS) > Activar comunicación segura
    La activación de la comunicación segura (TLS) se aplica a los dos TIM.
    Los otros tres parámetros se configuran independientemente para los dos TIM.

- Comunicación con la CPU:
  - Tiempo de pausa de ciclo
  - Peticiones de escritura/lectura
- Configuración de correo electrónico
  Nota:
  El TIM de reserva no soporta el envío de mensajes de correo electrónico.
- Números de dispositivos:
  - CPU asignada
    El certificado de comunicación de la CPU debe introducirse por separado en los dos TIM.
  - Dirección de estación/dirección ASDU
    El TIM primario y el TIM de reserva tienen la misma dirección de estación.
- Ajustes de registro
- SNMP
- Protección
- Configuración de puntos de datos y mensajes en el editor de puntos de datos
  El editor de puntos de datos está desactivado en el TIM de reserva.

Configuración manual en los dos TIM del grupo de redundancia

Los datos siguientes deben configurarse individualmente para cada TIM del grupo de redundancia:

- General
- Tipos de comunicación
- Ajustes básicos > Routing IP
- Ajustes de las interfaces, p. ej. DHCP, parámetros IPv6, routing, etc.
- Interfaz de la conexión de sincronización > Ajustes WAN > Redundancia de dispositivos > Secure Communication (TLS)
  Si la comunicación segura (TLS) está activada, los tres parámetros se configuran independientemente para los dos TIM; véase más arriba.
- Servidor web
- Diagnóstico web
- Configuración DNS
- Comunicación con la CPU: bit Watchdog, estado del interlocutor
  La "Consulta manual" de interlocutores no es posible en el TIM redundante.
- Sincronización horaria
- Números de dispositivos
  El TIM de reserva adopta la CPU asignada y la dirección de estación del TIM primario.
  El certificado de comunicación de la CPU debe introducirse por separado en los dos TIM.

- Administrador de certificados
  El TIM primario y el TIM de reserva tienen certificados de comunicación propios.
- Conexiones de Telecontrol
  Como punto final de las conexiones de Telecontrol del grupo de redundancia solo puede seleccionarse la CPU primaria.
  Cuando se crea la conexión de Telecontrol entre el TIM primario y el maestro, al agregar las vías de conexión se encuentran también las vías de conexión del TIM de reserva; véase al respecto más abajo.
  La comunicación segura (TLS) no puede configurarse para estas conexiones.

Conexiones de Telecontrol

Tras seleccionar y agregar las dos vías de conexión de la conexión de Telecontrol del grupo de redundancia, ambas se muestran en la tabla de las conexiones.

Antes de crear las conexiones en la tabla de conexiones, visualice el parámetro "Interfaz/dirección final (red.)".

- En el ejemplo siguiente, el punto de inicio de la conexión es la CPU primaria "1500H_1".
- La interfaz inicial de las dos vías de conexión es en cada caso la interfaz Ethernet X3 de:
  - TIM_R1 (TIM primario)
  - TIM_R2 (TIM de reserva)
- El punto final de la conexión (maestro) es en este caso la aplicación PCS 7 y las interfaces son los dos CP PC "IE_1" e "IE_2".

Si después de crear la conexión se hace clic en el botón "Agregar nueva vía de conexión", deberían encontrarse 4 vías de conexión.

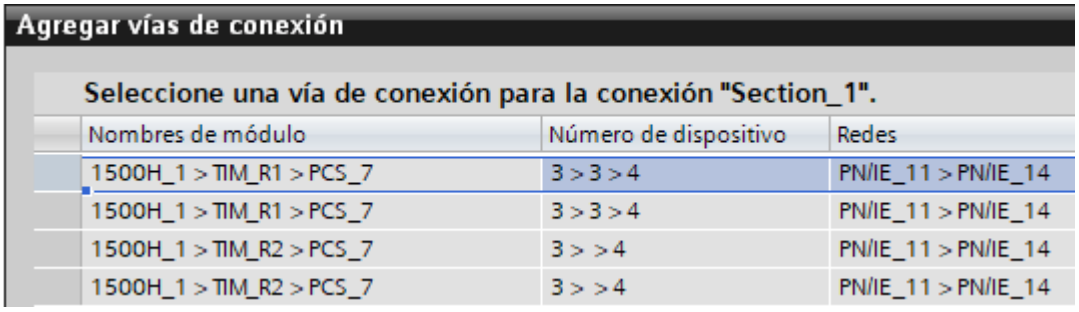


Figura 4-8 Agregar nueva vía de conexión: 4 vías de conexión encontradas

Agregue las 4 vías de conexión.

Después de incorporar las 4 vías de conexión, las conexiones del grupo de redundancia deberían ser parecidas a las de la figura siguiente.

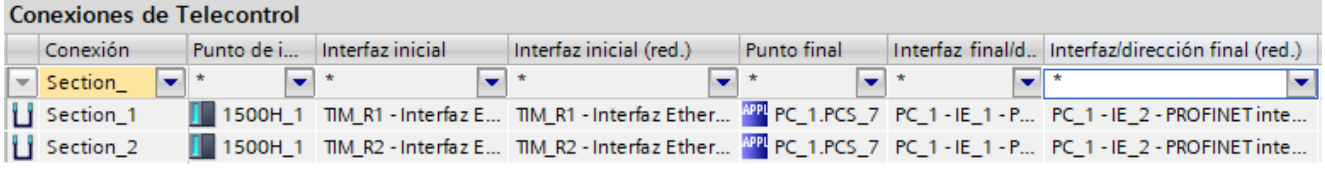


Figura 4-9 Ejemplo (DNP3): conexiones de Telecontrol del TIM 1531 IRC redundante

En cada una de las dos conexiones, la interfaz final y la interfaz final redundante contienen un CP de estación PC distinto. El grupo de redundancia consta de 4 conexiones.

Compilar y cargar

Nota

Compilar y cargar el TIM redundante

1. Compile siempre primero el TIM primario y después el TIM de reserva.
   - No vuelva a modificar la configuración después de compilarla.
     Si, a pesar de todo, fuera necesario un cambio, compile de nuevo los dos módulos a continuación en el orden indicado.
   - Después de la compilación, asegúrese de que la ID de redundancia de dispositivos es idéntica en ambos módulos.
2. Cargue siempre primero el TIM primario y después el TIM de reserva.

Conmutación en modo redundante

En servicio normal, solo el TIM primario envía datos al maestro. El TIM de reserva conserva los telegramas en su búfer de transmisión sin enviarlos. Tras el acuse por parte del maestro, el TIM de reserva también borra los telegramas correspondientes del búfer de transmisión.

La actividad de transmisión solo cambia del TIM primario al TIM de reserva en los siguientes casos:

- La conexión del TIM primario con el maestro falla.
  El TIM de reserva se convierte ahora en el TIM activo.
- Solo en IEC:
  El maestro conmuta.

En cuanto se recupera la conexión activa configurada del TIM primario tras un fallo, se regresa el estado normal.

Fallo de la conexión de sincronización

En caso de que falle la conexión de sincronización, ambos TIM pasan al estado activo.

Si la conexión de sincronización entre los dos TIM falla, el fallo se hace visible por el envío de un evento al maestro (punto de datos > ficha "Disparo" > Tipo de evento de estado de estación "Estado de la conexión de sincronización redundante modificado").

4.8 Interfaz serie

4.8.1 Parámetros WAN

Desde la lista desplegable "Subred" se conecta la interfaz en red.

Dirección WAN

Aquí se define la longitud del campo de dirección opcional (LADDR) para la dirección del nivel de enlace.

- **Formato de dirección (Dirección de 2 bytes)**
  Tenga en cuenta lo siguiente: El formato de dirección debe ser el mismo para todas las estaciones de la red IEC (60870-5-101).
  - Si la opción está desactivada, la dirección ASDU se guarda en 1 byte (byte menos significativo de la palabra).
    El rango de valores para la dirección del nivel de enlace es de 1...255.
  - Si la opción está activada, el rango de direcciones de la dirección del nivel de enlace (v. abajo) se incrementa hasta 1...65535.
- **Dirección WAN**
  Dirección opcional del nivel de enlace de la interfaz
  Rango de valores predeterminado: 1...255
  Rango de valores incrementado si el parámetro "Dirección de 2 bytes" está activado: 1...65535

4.8.2 Opciones avanzadas

4.8.2.1 Línea dedicada

Ajustes de línea dedicada

Ajustes de interfaz serie

- **Estándar de interfaz**
  Estándar de la interfaz serie: RS232 / RS485
  Seleccione el valor siguiente:
  - RS232
    En caso de conexión de un módem con interfaz RS-232 a la interfaz del TIM:
  - RS485
    En caso de conexión de un módem con interfaz RS-485
    En caso de conexión en paralelo de varios modems a la interfaz del TIM (red en estrella)
- **Terminación RS-485**
  Active esta opción al conectar una resistencia terminadora para el bus RS-485 en caso de conexión de una red en estrella.

Opciones de tiempo

- **Tiempo de retardo de transmisión (tras RTS)**
  El tiempo de retardo de transmisión (tras RTS) (ms) se inicia después de activar RTS.
  - Valor = 0
    El módulo espera a enviar los datos hasta que recibe la señal CTS (disponibilidad de envío) del módem.
  - Valor > 0
    El módulo no espera la señal CTS del módem, sino que envía en cuanto ha transcurrido el tiempo configurado.

  Ajuste predeterminado: 0. Rango admisible: 0...65535 ms
- **Tiempo de retardo de transmisión (tras CTS)**
  El tiempo de retardo (ms) se utiliza cuando se recibe la señal CTS (disponibilidad para la transmisión) del módem y cuando se ha configurado 0 (cero) para el "Tiempo de retardo de transmisión (tras RTS)".
  - Valor = 0
    No se espera la señal CTS del módem.
  - Valor > 0
    En cuanto se recibe la señal CTS del módem se inicia el tiempo de retardo de transmisión. La transmisión no empieza hasta que ha transcurrido el tiempo.

  Ajuste predeterminado: 0. Rango admisible: 0...65535 ms
- **Retardo a la desconexión RTS**
  Solo configurable en: TIM 1531 IRC
  El Retardo a la desconexión RTS (ms) especifica el momento en el que el módulo retira la señal RTS tras la transmisión.
  - Valor = 0
    El módulo retira la señal RTS justo después de enviar el último carácter.
  - Valor > 0
    Tras el envío del último carácter, el retardo a la desconexión RTS transcurre antes de que el módulo retire la señal RTS.

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

4.8.2.2 Red de marcación

Ajustes de red de marcación

Ajustes de interfaz serie

- **Estándar de interfaz**
  Estándar de la interfaz serie: RS232 / RS485 - conmutable
  Seleccione uno de los valores siguientes:
  - RS232
    En caso de conexión de un módem a la interfaz del TIM
  - RS485
    Conexión de la resistencia terminadora interna del TIM
    En caso de conexión en paralelo de varios modems a la interfaz del TIM (red en estrella)
- **Terminación RS485**
  Active la opción al conectar una resistencia terminadora para el bus RS485 en caso de conexión de una red en estrella.

Parámetros de llamada

- **Comando de marcación**
  Comando de marcación para el módem local
  Valores posibles:
  - D (comando AT)
  - DP (comando AT, marcación por impulsos)
  - DT (comando AT, marcación por tonos)

  En la medida de lo posible, utilice el comando de marcación "D".
- **Prefijo de marcación**
  Número de acceso (línea exterior) para una centralita (generalmente el 0 o el 9) o para un proveedor de telefonía alternativo.
  Rango admisible: Máx. 12 cifras
  Con conexión directa a la red de marcación y sin proveedor de telefonía alternativo, este parámetro se puede dejar vacío.
- **Número de teléfono propio**
  Entrada del número de teléfono propio del nodo de red, incluido el prefijo de localidad.
  Valores admisibles:
  - Cifras 0 ... 9
  - Signo más (+) como comodín para las cifras suprimibles (casi siempre 00 o 09) delante del prefijo de país.

  Ejemplo: +1230123456789

Inicialización AT

- **Definida por el usuario**
  Si la opción está activada, la cadena de inicialización AT debe asignarse manualmente para los ajustes básicos del módem.
  Si la opción está desactivada, la cadena de inicialización AT está preasignada específicamente para el módem:
  - MD3 : ATS45=3\N0F0&W
  - MD4 : ATS45=83$P1\N0&W
- **Cadena de inicialización**
  Campo de entrada para la cadena de inicialización AT

Opciones de tiempo

- **Intervalo de comprobación de la marcación**
  El intervalo de comprobación (min.) se inicia si el módulo de comunicación no ha podido establecer ninguna conexión tras agotarse los 3 intentos de repetición. Una vez transcurrido el intervalo de comprobación, el módulo de comunicación intenta de nuevo establecer una conexión.
  Si el establecimiento de la conexión vuelve a fallar, se inicia otra vez el intervalo de comprobación.
  Si en un TIM de central hay pendiente un nuevo telegrama durante el intervalo de comprobación, el TIM intenta inmediatamente establecer una conexión.
  Ajuste predeterminado: 5. Rango admisible: 0...255
- **Duración de conexión máx.**
  Solo para interfaces con el tipo de nodo de red "Central".
  Duración de conexión (s) máxima para una conexión de marcación. Una vez transcurrido el tiempo se deshace la conexión. Los telegramas que siguen pendientes para transmitir en la estación se transmiten la próxima vez que se establece la conexión.
  Con 0 (cero), la conexión de marcación se mantiene hasta que se han transmitido todos los datos pendientes.
  Ajuste predeterminado: 5. Rango admisible: 0...65535
- **Factor de repetición**
  El factor de repetición determina la frecuencia con la que se repite un telegrama de datos no acusado positivamente.

Ajustes de telefonía móvil

La comunicación por red de telefonía móvil no se soporta.

4.8.2.3 Ajustes de transferencia

Encontrará los parámetros específicos del protocolo de Telecontrol en el capítulo Parámetros IEC de las interfaces (Página 71).

4.9 Parámetros IEC de las interfaces

4.9.1 Ajustes de transferencia - IEC 60870-5

Ajustes de transferencia - IEC 60870-5

- **ACTTERM**
  Activa el envío de acuses con la causa de transferencia ACTTERM (cause of transmission <10>).
  Con ello se señaliza al interlocutor el final del procesamiento del comando.
  En la comunicación directa entre dos estaciones, ACTTERM debe tener la misma configuración en ambos interlocutores.
- **Tiempo máx. entre Select y Operate**
  Tiempo máximo (en segundos) entre Select y Operate. Para que un comando Select se transfiera a la CPU y, por tanto, sea efectivo, no debe enviarse ningún otro telegrama a la estación entre Select y Operate.
  Rango admisible: 1..65535
  Ajuste predeterminado: 1
  El modo de procesamiento de comandos se define para cada punto de datos de comando individual; consulte Opciones de comando (Página 168).
- **Tiempo de vigilancia para establecimiento de conexión (t_0)**
  Tiempo de vigilancia para el establecimiento de la conexión (t_0) en segundos. Si el interlocutor de la comunicación no confirma el establecimiento de la conexión dentro del tiempo de vigilancia, el módulo intenta volver a establecer la conexión.
  Rango admisible: 1..255
  Ajuste predeterminado: 30
- **Tiempo de vigilancia de telegrama (t_1)**
  Tiempo de vigilancia en segundos para el acuse por parte del interlocutor de telegramas enviados por el módulo. El tiempo de vigilancia es válido para todos los telegramas enviados por el módulo en formato I, S y U.
  Si el interlocutor no envía ninguna confirmación dentro del tiempo de vigilancia, el módulo deshace la conexión con el interlocutor.
  Rango admisible: 1..255
  Ajuste predeterminado: 15

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.

- **Tiempo de vigilancia para telegramas S y U (t_2)**
  Tiempo de vigilancia en segundos para el acuse de telegramas de datos del maestro por parte del módulo.
  Tras recibir los datos del maestro, el módulo acusa los datos recibidos de uno de los siguientes modos:
  - Si el módulo 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 módulo envía un telegrama de acuse (formato S) al maestro como muy tarde una vez transcurrido el tiempo t_2.

  Rango admisible: 1 ... 255
  Ajuste predeterminado: 10
  El valor de t_2 debe ser menor que el de t_1.
- **Tiempo de reposo para telegramas de prueba (t_3)**
  Tiempo de vigilancia en segundos en el que el módulo no recibe telegramas del maestro. Una vez transcurrido el tiempo t_3, el módulo envía un telegrama de prueba/control (formato U) al maestro.
  Este parámetro está previsto para casos con estados de reposo prolongados, es decir, en tiempos en los que no hay tráfico de datos.
  Rango admisible: 1 ... 255
  Ajuste predeterminado: 30
- **Diferencia (k) entre N(S) y N(R)**
  Diferencia entre el número secuencial de emisión $N(_S)$ y el de recepción $N(_R)$ de un telegrama. El maestro devuelve el número secuencial de emisión de un telegrama del módulo como acuse y el módulo emisor lo guarda como número secuencial de recepción. Los telegramas que tienen un número secuencial de emisión menor que el de recepción más la diferencia configurada aquí se evalúan como transferidos correctamente y se borran de la memoria de transmisión del módulo.
  Rango admisible: 1 ... 64
  Ajuste predeterminado: 12
- **Número máx. de telegramas de datos sin acusar (w)**
  w: Número máximo de telegramas de datos (I-APDUs) recibidos, alcanzado el cual el maestro debe confirmar el telegrama recibido más antiguo.
  Rango admisible: 1..8
  Ajuste predeterminado: 8
  El valor debe ser menor que el de "Diferencia entre número de secuencia de emisión y recepción" (k).

Mecanismo de acuse en el protocolo IEC

El módulo 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 módulo como acuse el número secuencial de emisión de ese telegrama de datos o, en caso de recepción de varios telegramas de datos, del último recibido. El módulo guarda el número secuencial de emisión devuelto por el maestro como número secuencial de recepción y lo utiliza como acuse.

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 módulo.

Recomendaciones de la especificación:

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

4.9.2 Ajustes de maestro IEC

Maestro IEC

Los siguientes parámetros se encuentran en el grupo de parámetros "Ajustes de maestro IEC" de las interfaces ajustadas en el Tipo de red IEC y el Tipo de nodo de red "Estación central" del módulo de comunicación.

- **Intervalo básico de sondeo**
  Aquí se define el intervalo básico para llamadas de estación desde la central.
  Rango de valores: 0 ... 65535 segundos
  Ajuste predeterminado: 30
  Con el valor 0 (cero) la función está desactivada. No se produce un sondeo cíclico, ni tan solo para los parámetros indicados a continuación, cuyo cálculo se basa en el Intervalo básico de sondeo.
  El intervalo básico se utiliza para calcular los parámetros siguientes en la configuración de conexiones:
  - Intervalo para consulta general
  - Intervalo para consulta general de contador
  - Intervalo para consulta de grupo
  - Intervalo para consulta de grupo de contador

  Consulte la configuración en el capítulo Opciones de consulta (Página 131).
- **Número máx. de eventos por llamada**
  Número máximo de eventos que pueden enviarse en el telegrama de respuesta de la estación tras una llamada por parte de la central.
  Rango de valores: 0 ... 65535
  Ajuste predeterminado: 0
  Con 0 (cero) la función está desactivada (no hay límite).

Encontrará más información sobre el parámetro "Tiempo de vigilancia del interlocutor" en el capítulo Ajustes de estación IEC (Página 74).

4.9.3 Ajustes de estación IEC

Ajustes de eventos

Requisitos

- El tipo de nodo de red de la interfaz es "estación" o "estación nodo".
- Los puntos de datos son del mismo tipo.
- Los índices de los puntos de datos son consecutivos sin huecos.
  Consulte el capítulo Índice de punto de datos (Página 149).

Función

Para los tipos de puntos de datos indicados a continuación es posible ajustar la forma de transferencia. Los ajustes son válidos para puntos de datos que están configurados como eventos (disparados).

La función corresponde al bit "SQ" del "VARIABLE STRUCTURE QUALIFIER field" conforme a IEC 60870-5-101.

- **Comportamiento de transferencia**
  - Transferencia individual:
    La dirección de los objetos se transfiere individualmente.
    SQ = 0
  - Transferencia secuencial
    Las direcciones de los objetos se crean de forma combinada para ahorrar volumen de datos durante la transferencia.
    SQ = 1

Ajustes de los tipos de puntos de datos soportados

Si en Comportamiento de transferencia se configura "Transferencia secuencial", para los tipos de puntos de datos listados rigen los parámetros siguientes.

La transferencia de los eventos respaldados se inicia en cuanto se cumple una de las dos condiciones siguientes:

- **Número de eventos**
  Hay transferencia cuando se alcanza el número configurado de eventos respaldados.
- **Tiempo de retardo**
  Hay transferencia cuando se alcanza el tiempo de retardo configurado (segundos).

Si se configura el valor 0 (cero), la función en cuestión está desactivada.

Otros parámetros relevantes para la estación

Los siguientes parámetros relevantes para la estación se definen al configurar las conexiones:

- Modo de sondeo

Consulte la configuración en el capítulo Tabla de conexiones (Página 121).

Encontrará más parámetros en los siguientes grupos de parámetros:

- Respuesta a consulta general / Asignación a consulta de grupo
  (cause of transmission 20 - 41)
  - La asignación de diferentes puntos de datos a una consulta general o a una consulta de grupo se configura en la configuración de puntos de datos; consulte el capítulo Ficha "General" (Página 147).
  - Los intervalos de las consultas se configuran en las conexiones de Telecontrol; consulte el capítulo Opciones de consulta (Página 131).

4.10 Configurar redes WAN

Parámetros de redes WAN clásicas

Configure primero el grupo de parámetros "Ajustes WAN" de las interfaces del módulo de comunicación; consulte el capítulo Ajustes WAN de las interfaces (Página 53).

Al generar una nueva red, la red WAN conectada aplica los principales ajustes de la interfaz.

Las redes WAN clásicas, que se representan de color azul en STEP 7, tienen los siguientes grupos de parámetros.

General

Aquí se configuran el nombre y la ID de subred S7, como en cada red.

Ajustes de red

Configuración de red

- **Tipo de protocolo**
  En función del tipo de módulo pueden estar disponibles los siguientes protocolos de acción remota:
  - ST7
  - DNP3
  - IEC 60870-5
- **Tipo de red**
  El tipo de red se aplica de la interfaz conectada:
  - Línea dedicada
  - Red de marcación

Métodos de acceso

Solo para línea dedicada

- **Métodos de acceso**
  El método de acceso está predefinido y no puede modificarse:
  - Sondeo

Parámetros de telegrama

Los parámetros están predefinidos y no pueden modificarse.

- **Formato de telegrama**
  - FT1.2
- **Tipo de confirmación**
  - Acuse corto (1 byte)
- **Factor de repetición**
  El factor de repetición determina la frecuencia con la que se repite un telegrama de datos no acusado positivamente:
  - 3
- **Longitud máx. de telegrama**
  Tamaño máximo de un telegrama de datos dentro de la red:
  - 240

Ajustes de red

- **Dependencia del sentido**
  Dependencia del sentido en la red
  - Dúplex
  - Semidúplex
- **Velocidad de transferencia**
  Velocidad con la que se comunican el módulo de comunicación y el módem.
  Seleccione en la lista desplegable un valor que sea soportado por todos los módems conectados.

Sincronización horaria

- Activar sincronización horaria para WAN
  Con el parámetro activado se especifica si debe transferirse la hora para la sincronización horaria de las estaciones conectadas a través de la red WAN.

Si el parámetro está activado, defina el Ciclo de sincronización.

Nota

Incorporación de los ajustes a las estaciones

Los módulos TIM conectados adoptan los ajustes realizados aquí en la red.

Consulte el concepto de hora en el capítulo Sincronización horaria (Página 43).

Lista de estación

Aquí encontrará una tabla sinóptica de las estaciones conectadas a la red con sus principales parámetros.

La dirección WAN es la dirección de la estación.

4.11 Servidor web (TIM 1531 IRC)

El servidor web del TIM

El TIM proporciona la función de un servidor web para acceder a través de un navegador web. A través del servidor web se dispone de las siguientes funciones:

- Acceso de lectura
  - Una selección de datos de diagnóstico
  - Una selección de datos de configuración
- Acceso de escritura
  - Ajustar la hora
  - Actualización de firmware
  - Reinicio del módulo
  - Restablecer configuración de fábrica
  - Grabación de valores estadísticos de las interfaces Ethernet

Encontrará la descripción de los contenidos en el manual de producto del TIM /2/ TIM 1531 IRC (Página 220).

Autorización de acceso mediante "Ajustes globales de seguridad"

Los derechos para el acceso al servidor web se configuran en STEP 7 en los ajustes globales de seguridad. Los usuarios creados en ellos son los únicos que pueden iniciar sesión en el servidor web del TIM a través de HTTP/HTTPS.

Para el acceso al servidor web son relevantes las siguientes funciones preasignadas:

- NET Standard
- NET Diagnose

Con ello se habilitan los derechos necesarios para el diagnóstico, el acceso al servidor web y la lectura y escritura de datos.

Encontrará más ayuda sobre las funciones y derechos de los usuarios en el sistema de información de STEP 7.

Acceso al servidor web e inicio del diagnóstico web

Para poder conectarse con el servidor web del TIM es necesario activar el acceso al servidor web para cada interfaz Ethernet, consulte el capítulo Acceso al servidor web (Página 56). En el ajuste predeterminado el acceso está desactivado.

Consulte cómo iniciar el diagnóstico web en el capítulo Diagnóstico web en el TIM 1531 IRC (Página 79).

Grupo de parámetros "Servidor web"

General

- **Activar servidor web en el módulo**
  Activa el procesamiento de datos en el servidor web del TIM y permite el acceso a dichos datos.
- **Permitir acceso solo vía HTTPS**
  Permite el acceso al servidor web solo con el protocolo seguro HTTPS.

Nota

Permitir acceso solo vía HTTPS (función de seguridad activada)

Tenga en cuenta lo siguiente si la opción "Permitir acceso solo vía HTTPS" está activada en el grupo de parámetros "Servidor web":

- Los datos se transfieren codificados.

Requisitos

- El usuario debe tener asignadas las funciones citadas anteriormente con los derechos correspondientes.
- Si el cortafuegos está activado, los protocolos HTTP/HTTPS deben estar autorizados.

Actualización automática

- **Activar actualización automática**
  Activa la actualización automática de los valores mostrados.
  Si la opción está desactivada solo se muestran los valores en el momento de establecerse la conexión con el servidor web.
- **Intervalo de actualización**
  Seleccione el intervalo en el que desea una actualización de los valores mostrados.
  Ajuste predeterminado: 30. Rango admisible: 5...999

Vista general de interfaces

Aquí se ve en forma de tabla la habilitación del acceso al servidor web a través de todas las interfaces Ethernet del TIM.

Es posible activar el acceso al servidor web del TIM a través de HTTP/HTTPS individualmente para cada interfaz Ethernet.

Los ajustes para activar los grupos de parámetros "Acceso al servidor web" y "Servidor web" se realizan recíprocamente en el otro grupo de parámetros correspondiente.

4.12 Diagnóstico web en el TIM 1531 IRC

Requisitos

- El servidor web del módulo está activado en el grupo de parámetros "Servidor web" de la configuración y la interfaz está seleccionada.
- La interfaz está habilitada en el grupo de parámetros "Interfaz Ethernet > Acceso al servidor web" de la configuración para el acceso al servidor web.

Inicio del diagnóstico web

1. Establezca un enlace físico entre la estación de ingeniería y la estación SIMATIC.
2. Ajuste la interfaz PC de manera que el módulo esté accesible.
   Encontrará más ayuda en la función "Ajustar interfaz PG/PC...".
3. En el proyecto STEP 7 haga clic en el botón "Diagnóstico web" del grupo de parámetros "Diagnóstico web" para establecer la conexión con el navegador web del módulo.

El servidor web integrado del módulo suministra los contenidos. Consulte el manejo y los contenidos en el manual de producto del TIM /2/ TIM 1531 IRC (Página 220).

4.13 Configuración DNS

Servidor DNS

Un servidor DNS puede ser necesario cuando el propio módulo, un interlocutor de la comunicación o un servidor de correo electrónico, por ejemplo, debe ser accesible a través del nombre de host (FQDN).

Servidor DNS para dirección de servidor de correo electrónico

En la configuración de correo electrónico hay que especificar la dirección del servidor de correo a través del cual se envían los mensajes. La dirección del servidor de correo puede indicarse como dirección IP o como FQDN.

Si la dirección de servidor se indica como FQDN, habrá que configurar un servidor DNS.
En ese caso la dirección IP del servidor de correo se determina a través del servidor DNS configurado.

4.14 Comunicación con la CPU

Comunicación con la CPU

Aquí se definen los parámetros para el acceso del módulo de comunicación dentro del ciclo de muestreo de la CPU.

- **Tiempo de pausa de 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.

Encontrará la estructura del ciclo de muestreo de la CPU en el capítulo Ciclo de lectura (Página 152).

Bit de vigilancia

- **Vigilancia TIM / Vigilancia del CP**
  A través del bit watchdog se puede comunicar a la CPU el estado de la comunicación de acción remota del módulo de comunicación.

Hora del CP

- **Hora del CP para la CPU**
  La función permite a la CPU leer la hora del CP. De este modo el CP puede sincronizar la hora de la CPU.
  Secuencia:
  - La CPU pone a 1 la entrada "Variable de disparo de hora" (BOOL) desde el programa de usuario.
  - A continuación, el CP escribe su hora en la "Variable de hora del CP" (DTL) y vuelve a poner a 0 el valor de "Variable de disparo de hora".
  - El programa de usuario lee la "Variable de hora del CP" para ajustar la hora de la CPU.

  Recomendación:
  No active la "Variable de disparo de hora" más de una vez por segundo para no sobrecargar innecesariamente el bus de fondo con comunicación.

Diagnóstico CP

El grupo de parámetros permite leer los datos de diagnóstico avanzados del CP mediante variables PLC.

- **Activar diagnóstico CP avanzado**
  Active la opción para utilizar el diagnóstico de CP avanzado.
  Su activación obliga a configurar como mínimo la "Variable de disparo de diagnóstico".
  Las variables PLC siguientes para los diferentes datos de diagnóstico pueden seleccionarse de forma selectiva de acuerdo con las funciones soportadas por el CP.
- **Variable de disparo de diagnóstico**
  Si la variable PLC (BOOL) del programa de usuario de la CPU se pone a 1, el CP actualiza los valores de las siguientes variables PLC para el diagnóstico avanzado.
  Después de escribir los valores actuales en las variables PLC siguientes, el CP pone a 0 la "Variable de disparo de diagnóstico", con lo que indica a la CPU que pueden leerse los valores actualizados de las variables PLC.

  Nota

  Activación rápida de la variable de disparo de diagnóstico

  Los disparos no deben activarse más de una vez por segundo.

- **Advertencia de desbordamiento de la memoria de telegrama**
  Variable PLC (tipo de datos Byte) para prealarma de desbordamiento del búfer de transmisión. El bit 0 se pone a 1 cuando se ha alcanzado el 80 % del nivel de llenado del búfer de transmisión.
- **Ocupación de la memoria de telegrama**
  Variable PLC (tipo de datos DWord) para la ocupación del búfer de transmisión. Se indica el número de telegramas guardados.
- **Dirección IP actual**
  Variable PLC (tipo de datos String) para la dirección IP actual de la interfaz del CP
- **Estado VPN IPsec**
  La variable PLC (BOOL) indica si hay un túnel VPN IPsec establecido:
  - 0 = no hay túnel establecido
  - 1 = hay túnel establecido
- **Conexión con SINEMA Remote Connect**
  La variable PLC (BOOL) indica si hay una conexión con el servidor SINEMA RC:
  - 0 = no hay conexión establecida
  - 1 = hay conexión establecida

Variables PLC para estado de interlocutor / estado de recorrido

Mediante la variable PLC que puede configurarse aquí se vigila la siguiente información sobre accesibilidad de los interlocutores:

- **Estado de interlocutor**
  Accesibilidad del interlocutor remoto
- **Estado de recorrido**
  Estado de la vía de conexión o de las vías de conexión redundantes con el interlocutor remoto
  Consulte la comunicación y las posibles vías de conexión en el capítulo Posibilidades de comunicación (Página 31).

Para cada interlocutor configurado para el que haya creada una conexión de Telecontrol simple o redundante es posible crear una variable PLC del tipo Word.

Asignación de la variable PLC para estado de interlocutor / estado de recorrido

En los dos bytes de la variable PLC del tipo de datos Word (DB, marca, salida) se emite la información siguiente:

- **Byte 0: Estado de interlocutor**
- **Byte 1: Estado de recorrido**

Byte 0 "Estado de interlocutor"

El byte 0 codifica información sobre la accesibilidad del interlocutor de la comunicación, las conexiones y vías de conexión existentes y el estado del búfer de transmisión del TIM.

Tabla 4-1 Asignación del byte 0: Significado de los estados de los bits

Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
Redundancia de vías	**Modo de conexión**	**Conexión temporal ***	*(Reservado)*	**Memoria de telegramas ****		**Estado de recorrido**	**Estado de interlocutor**
0: Sin redundancia 1: Hay redundancia	0: Permanente 1: Temporal	0: Interlocutor no accesible 1: Interlocutor accesible *	-	0: Búfer de transmisión en buen estado 1: Ocupación de la memoria > 80 % 3: Desbordamiento (100 %de memoria ocupada)		0: No todas las vías son accesibles 1: Todas las vías son accesibles	0: Interlocutor no accesible 1: Interlocutor accesible

***** Los interlocutores que soportan conexiones temporales se establecen como "accesibles" cuando el propio interlocutor deshace la conexión y no hay conexión alguna.

****** Estado del búfer de transmisión:

Si cuando se produce un desbordamiento del búfer de transmisión o una preadvertencia están activados los bits 2 o 2+3, los dos bits no se desactivan hasta que la ocupación de la memoria baja por debajo del 50 %.

Encontrará información sobre el búfer de transmisión en el capítulo Memoria imagen de proceso, tipo de transferencia, clases de eventos (Página 151).

Byte 1 "Estado de recorrido"

El byte 1 muestra desde la perspectiva del TIM local el estado de la vía de conexión (conexión configurada) hacia el interlocutor.

Como máximo es posible configurar 2 vías (vía principal y vía sustitutiva) hacia un interlocutor, consulte el capítulo Posibilidades de comunicación (Página 31).

Ambas vías de conexión deben comenzar o terminar en un TIM local.

El byte indica lo siguiente:

- Las vías a través de las cuales se accede al interlocutor.
- La vía utilizada actualmente.
- La interfaz TIM a través de la que se ha configurado la vía principal.
- La interfaz TIM a través de la que se ha configurado la vía sustitutiva.

La vía de una conexión se indica como combinación de las interfaces utilizadas del TIM y el estado del recorrido.

Ocupación de bytes

El byte 1 está asignado del siguiente modo:

- Dos bits para la interfaz de la vía principal
- Dos bits para la interfaz de la vía sustitutiva
- Dos bits para la estado de recorrido de la vía principal
- Dos bits para la estado de recorrido de la vía sustitutiva

Tabla 4-2 Asignación del byte 1

Bits 6 + 7	**Bits 4 + 5**	**Bits 2 + 3**	**Bits 0 + 1**
Interfaz configurada		**Estado de recorrido**	
Codificación para la vía sustitutiva	Codificación para la vía principal	Vía sustitutiva (2.ª vía)	Vía principal (1.ª vía)

- **Interfaz configurada**
  Las interfaces del TIM "Ethernet 1" (IE1), "Ethernet 2" (IE2), "Ethernet 3" (IE3) y WAN1 están numeradas correlativamente de 0 a 3 (decimal):
  - 0 = Interfaz Ethernet IE1 (X1)
  - 1 = Interfaz Ethernet IE2 (X2)
  - 2 = Interfaz Ethernet IE3 (X3)
  - 3 = Interfaz serie WAN1 (X4)

Estado del bit 5 (7)	Estado del bit 4 (6)	Significado
0	0	Codificación para la interfaz Ethernet X1 (decimal: n.º 0)
0	1	Codificación para la interfaz Ethernet X2 (decimal: n.º 1)
1	0	Codificación para la interfaz Ethernet X3 (decimal: n.º 2)
1	1	Codificación para la interfaz serie X4 (decimal: n.º 3)

- **Estado de recorrido**
  - Vía principal = 1.ª vía (bits 0 + 1)
  - Vía sustitutiva = 2.ª vía (bits 2 + 3)

Estado del bit 1 (3)	Estado del bit 0 (2)	Significado del bit 1	Significado del bit 0
0	0	Bit 1: la vía no es actual	Bit 0: dispositivo no accesible
0	1	Bit 1: la vía no es actual	Bit 0: dispositivo accesible
1	0	Bit 1: la vía es actual	Bit 0: dispositivo no accesible
1	1	Bit 1: la vía es actual	Bit 0: dispositivo accesible

Posibilidades de codificación del byte 1

La misma codificación de la interfaz configurada para la vía principal y la vía sustitutiva significa que no existe una redundancia de vía (solo una interfaz configurada). En este caso, el estado de la vía se emite mediante los bits de la vía principal (1.ª vía).

Tabla 4-3 Posibilidades de codificación para el Estado de recorrido

Interfaz configurada		Estado de recorrido	
Codificación para la vía sustitutiva	**Codificación para la vía principal**	**Vía sustitutiva (2.ª vía)**	**Vía principal (1.ª vía)**
0 0	0 0 (Codificación para IE1)	Irrelevante (no redundante)	Estado de IE1
0 0	0 1 (Codificación para IE2)	Estado de IE1	Estado de IE2
0 0	1 0 (Codificación para IE3)	Estado de IE1	Estado de IE3
0 0	1 1 (Codificación para WAN1)	Estado de IE1	Estado de WAN1
0 1	0 0	Estado de IE2	Estado de IE1
0 1	0 1	Irrelevante (no redundante)	Estado de IE2
0 1	1 0	Estado de IE2	Estado de IE3

Interfaz configurada		Estado de recorrido	
0 1	1 1	Estado de IE2	Estado de WAN1
1 0	0 0	Estado de IE3	Estado de IE1
1 0	0 1	Estado de IE3	Estado de IE2
1 0	1 0	Irrelevante (no redundante)	Estado de IE3
1 0	1 1	Estado de IE3	Estado de WAN1
1 1	0 0	Estado de WAN1	Estado de IE1
1 1	0 1	Estado de WAN1	Estado de IE2
1 1	1 0	Estado de WAN1	Estado de IE3
1 1	1 1	Irrelevante (no redundante)	Estado de WAN1

Consulta manual

Opción para disparar manualmente una consulta individual de un interlocutor de la comunicación o de una General Interrogation (IEC)

Validez

La función es soportada por:

- TIM 1531 IRC V2.4 junto con una CPU S7-300 / 400 / 1500
- CP 1542SP-1 IRC V2.3

Funciones

Además de las consultas de la estación central o del maestro durante el arranque, esta opción ofrece la posibilidad de realizar una consulta manual por medio de una variable de la CPU.

La opción soporta los siguientes tipos de consulta:

- Consultas individuales o de grupo de interlocutores de la comunicación (consultas individuales secuenciales)
- General Interrogation (consultas individuales secuenciales)

Por norma general se aplica lo siguiente:
Las consultas solo pueden realizarse específicamente por estación. La consulta de varias estaciones debe realizarse secuencialmente.

La consulta se dispara mediante la variable "Solicitud de lectura". En ella se indican también el tipo de consulta y las direcciones. La variable contiene un tipo de datos de usuario (UDT) que debe crearse previamente.

El resultado de la consulta se escribe en la variable (byte) "Resultado de lectura", que puede ser evaluado por la CPU o el usuario.

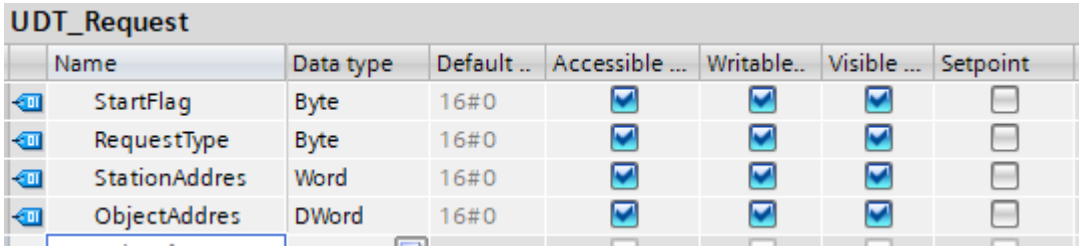
Requisitos

- La función de maestro de los puntos de datos está activada.
- El sondeo cíclico tiene que estar desactivado.

Variables

Las siguientes variables son necesarias para la función de consulta:

- **Consulta de interlocutor**
  Para iniciar la consulta es necesario indicar el tipo de consulta y para las direcciones se necesita un tipo de datos especial que debe crearse como tipo de datos de usuario (UDT). Para ello, proceda del siguiente modo:
  - En el árbol del proyecto vaya hasta la entrada "Tipos de datos PLC" de la CPU asignada.
  - Haga clic en la entrada "Agregar nuevo tipo de datos".
  - Seguidamente, cree los elementos necesarios del UDT (ver el apartado siguiente).



UDT_Request

	Name	Data type	Default ..	Accessible ...	Writable..	Visible ...	Setpoint
	StartFlag	Byte	16#0	☑	☑	☑	☐
	RequestType	Byte	16#0	☑	☑	☑	☐
	StationAddres	Word	16#0	☑	☑	☑	☐
	ObjectAddres	DWord	16#0	☑	☑	☑	☐

Figura 4-10 Estructura del UDT

  - Cree un bloque de datos e inserte en él el UDT que ha creado previamente.
    El UDT puede seleccionarse en la lista desplegable de los tipos de datos y tiene el nombre que se le ha asignado.

  Para la variable "Consulta de interlocutor", referencie la variable del UDT creado para tal fin en el bloque de datos que ha creado.

- **Resultado de la consulta**
  Para el resultado de la consulta, cree una variable del tipo Byte y referiéncela como variable "Resultado de la consulta".

Estructura y codificación del UDT "Consulta de interlocutor"

Estructura y contenido del UDT para el protocolo IEC 60870-5:

Tipo de datos	Parámetro	Rango de valores y significado
Byte	Marca de inicio	Con un cambio 0 → 1 el TIM inicia la consulta. Una vez ejecutada la consulta, el TIM vuelve a poner el valor a 0.
Byte	Tipo de consulta	Consulte el rango de valores más abajo
Word	Dirección de estación	0 ... 65534
DWord	Dirección del objeto	1 ... 16777215 La dirección del objeto permanece vacía (valor = 0) si no se necesita.

Tabla 4-4 Codificación del parámetro "Tipo de consulta"

Tipo de consulta	Valor
Global Interrogation	1
Group 1 Interrogation	2

Tipo de consulta	Valor
Group 2 Interrogation	3
Group 3 Interrogation	4
Group 4 Interrogation	5
Group 5 Interrogation	6
Group 6 Interrogation	7
Group 7 Interrogation	8
Group 8 Interrogation	9
Group 9 Interrogation	10
Group 10 Interrogation	11
Group 11 Interrogation	12
Group 12 Interrogation	13
Group 13 Interrogation	14
Group 14 Interrogation	15
Group 15 Interrogation	16
Group 16 Interrogation	17
Counter Interrogation	18
Group 1 Counter Interrogation	19
Group 2 Counter Interrogation	20
Group 3 Counter Interrogation	21
Group 4 Counter Interrogation	22
Consulta selectiva de un objeto *	23

***** La consulta individual de valores de contaje no se soporta.

Codificación del byte "Resultado de la consulta"

Los resultados de la consulta se escriben en la variable "Resultado de la consulta". El byte "Resultado de la consulta" debe desactivarse manualmente desde el programa de usuario tras una consulta.

Los valores (hexadecimales) tienen el siguiente significado:

Valor (hex)	Significado
Ningún resultado:	
0x00	#define TCH_DATA_REQUEST_RESULT_NO_RESULT
"Consulta correcta":	
0x01	#define TCH_DATA_REQUEST_RESULT_OK
"Interlocutor en mal estado":	
0x88	#define TCH_DATA_REQUEST_RESULT_STATION_NOT_OK
Error:	
0x80	#define TCH_DATA_REQUEST_RESULT_ERROR
0x81	#define TCH_DATA_REQUEST_RESULT_STATION_UNDEF
0x82	#define TCH_DATA_REQUEST_RESULT_TYPE_UNDEF
0x83	#define TCH_DATA_REQUEST_RESULT_GROUP_UNDEF
0x84	#define TCH_DATA_REQUEST_RESULT_VARIATION_UNDEF

Valor (hex)	Significado
0x85	#define TCH_DATA_REQUEST_RESULT_TIMEOUT
0x86	#define TCH_DATA_REQUEST_RESULT_ALREADY_ACTIVE
0x87	#define TCH_DATA_REQUEST_RESULT_REFUSED
0x89	#define TCH_DATA_REQUEST_RESULT_REFUSED_BY_PARTNER
0x90	#define TCH_DATA_REQUEST_RESULT_REQUEST_INCOMPLETE

Control de las consultas

Las consultas se controlan desde el programa de usuario de la CPU.

Desde la CPU se establecen tanto la marca de inicio que dispara una consulta como los diferentes contenidos de los parámetros "Tipo de consulta", "Dirección de estación" y "Dirección del objeto".

Nota

Recomendación

Establezca la marca de inicio en último lugar, después de haber indicado todos los demás parámetros.

Para consultar diferentes estaciones, grupos u objetos es necesario escribir en el UDT los contenidos relevantes en cada caso desde el programa de usuario.

4.15 Configuración de correo electrónico

Configuración de correos electrónicos

Con la entrada "Configuración de correo electrónico" se configuran el protocolo que debe utilizarse y los datos de acceso al servidor de correo electrónico.

En el editor de mensajes (entrada "Mensajes") se configuran los diferentes correos electrónicos; consulte el capítulo Mensajes (Página 173).

Requisitos para correo electrónico

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

- Las funciones de seguridad están activadas.
- La hora del CP está sincronizada.

Para la configuración se necesitan los datos del servidor SMTP y de la cuenta de usuario:

- Dirección del servidor, número de puerto, nombre de usuario, contraseña, dirección de correo electrónico del remitente (CP)
- En caso de transferencia cifrada: certificado de servidor

Configuración de correo electrónico

Si desea utilizar la transferencia segura de correo electrónico, el módulo debe tener la fecha y la hora actuales.

En el ajuste estándar del puerto SMTP 25, el módulo transmite mensajes de correo electrónico sin cifrar.

Si el operador del servicio de correo electrónico solo soporta la transmisión cifrada, debe utilizarse una de las opciones siguientes:

- N.º de puerto 587
  Si se utiliza STARTTLS, el módulo envía mensajes de correo electrónico cifrados al servidor SMTP del operador del servicio de correo electrónico.
  Recomendación: si el operador de correo electrónico ofrece las dos posibilidades (STARTTLS / SSL/TLS), debería utilizarse STARTTLS con el puerto 587.
- N.º de puerto 465
  Si se utiliza SSL/TLS (SMTPS), el módulo envía mensajes de correo electrónico cifrados al servidor SMTP del operador del servicio de correo electrónico.

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

Para la configuración de las contraseñas consulte Juego de caracteres para nombres de usuario, contraseñas y mensajes (Página 179).

Importar un certificado con transferencia cifrada

Para poder utilizar una transferencia cifrada hay que cargar el certificado de la cuenta de correo electrónico en el administrador de certificados de STEP 7. El certificado se obtiene del operador del servicio de correo electrónico.

Siga los pasos que se indican a continuación para utilizar el certificado:

1. Guarde el certificado del operador del servicio de correo electrónico en el sistema de archivos de la estación de ingeniería.
2. Importe el certificado al proyecto de STEP 7 desde "Ajustes globales de seguridad > Administrador de certificados".
3. Utilice el certificado importado en todos los módulos que usen correos electrónicos cifrados, mediante la tabla "Administrador de certificados" del grupo de parámetros "Security".

Consulte el procedimiento en el capítulo Administrador de certificados (Página 104).

4.16 Números de dispositivos

4.16.1 Números de dispositivos

Números de dispositivos

En este directorio se configuran la dirección de la estación y la asignación de la CPU en función del módulo de comunicación:

- **CP**
  - Dirección ASDU
    Dirección ASDU de la estación
    El módulo de comunicación y la estación (CPU) tienen la misma dirección ASDU.
  - Dirección ASDU estructurada
    Dirección ASDU estructurada de la estación

  La CPU está asignada automáticamente al módulo de comunicación a través del rack.
- **TIM**
  - CPU asignada
    En la lista desplegable solo se muestran las CPU que están conectadas en red con el TIM.
  - Contraseña de la CPU asignada
    Si la CPU asignada está protegida con "Sin acceso (protección completa)", introduzca aquí la contraseña configurada para la CPU en "Protección & Seguridad > Nivel de acceso".
  - Dirección ASDU
    Dirección ASDU de la estación
    El módulo de comunicación y la estación (CPU) tienen la misma dirección ASDU.
  - Dirección ASDU
    Dirección ASDU estructurada de la estación

La dirección ASDU debe ser unívoca dentro de una subred y dentro del proyecto STEP 7.

Observe las normas básicas de direccionamiento del capítulo Direccionamiento (Página 31).

Otros números de dispositivos

- **Dispositivo de terceros**
  Para dispositivos de terceros, por ejemplo maestros fuera del proyecto de STEP 7, configure el número de dispositivo en la conexión de Telecontrol.
- **RTU3000C**
  - **Número de dispositivo de la CPU (RTU)**
    Aquí se asigna el número de dispositivo de la CPU, tal como se ha configurado en el WBM de la RTU.

  Consulte la configuración de la RTU en Tipos de comunicación (Página 35).

Asignación de la CPU y configuración de las direcciones de dispositivo

Para módulos que se comunican mediante conexiones de Telecontrol (editor "Datos de red"), la asignación de la CPU y la configuración de las direcciones de módulo se lleva a cabo en el grupo de parámetros "Números de dispositivos".

- **CPU asignada**
  En los siguientes módulos de comunicación, que están en el mismo rack que la CPU, la CPU local se asigna automáticamente al módulo:

  – CP (S7-1200, ET 200SP)

  En los módulos de comunicación que no están en el mismo rack que una CPU hay que utilizar la lista desplegable para asignar el módulo a una CPU con la que esté conectado en red. Esto se aplica a:

  – TIM 1531 IRC
  Es posible asignar al TIM 1531 IRC una CPU de las siguientes familias SIMATIC: S7-300, S7-400, S7-1500, ET 200SP
  Si se asigna el TIM 1531 IRC a una CPU S7-1500R/H, para la comunicación del TIM con la CPU se utiliza la dirección IP del sistema de la CPU S7-1500R/H.

Direccionamiento estructurado en el protocolo IEC

La dirección ASDU puede configurarse en dos campos de entrada con un formato distinto:

- Dirección ASDU
  Aquí se configura la dirección sin estructurar como entero.
  Rango de valores: 0..65534
- Dirección ASDU estructurada
  Aquí se puede configurar la dirección estructurada conforme a IEC 60870-5-3. Mediante el direccionamiento estructurado es posible estructurar la dirección ASDU en función de la instalación.
  Pueden configurarse 2 niveles de direcciones (octetos).
  Rango de valores: 0.0..255.254
  Los valores configurados de los dos campos están acoplados. Un valor configurado se convierte y se muestra en el otro campo de entrada.

Conversión de los valores:

Los valores se identifican del siguiente modo para la conversión:

- Dirección ASDU
  Nombre del valor del entero: X
- Dirección ASDU estructurada
  Designación de los valores de los 2 octetos: A.B

El valor configurado se aplica al otro campo, respectivamente, siguiendo la fórmula que se indica:

X = A * 256 + B

Comunicación segura con certificados

Para el módulo de comunicación TIM 1531 IRC que no se encuentra en el mismo rack que la CPU, en los casos siguientes deberá indicar el certificado de la CPU:

- TIM 1531 IRC
  junto con
- CPU 1500 / CPU 1500SP-1 a partir de la versión V2.9

Adicionalmente para ST7:

- Se utiliza TD7onTIM
  Si se utiliza TD7onCPU no está permitido asignar la CPU al TIM.
  Consulte la configuración en "Ajustes básicos > Configuración > Configuración de Telecontrol = Configurar".

Generación del certificado de CPU y asignación de la CPU

Encontrará los requisitos y el procedimiento en TIM 1531 IRC: Certificado TLS de la CPU (Página 92).

4.16.2 TIM 1531 IRC: Certificado TLS de la CPU

Validez

El procedimiento descrito más abajo es válido para:

- TIM 1531 IRC V2.3 a partir de la versión de firmware V2.3
  junto con CPU 1500 a partir de la versión de firmware V2.9

Los módulos de comunicación utilizan TLS 1.2 y la comunicación se corresponde con IEC/TS 62351-3.

Comunicación entre CPU y módulo de Telecontrol

CP: comunicación a través del bus de fondo

Si la CPU y el CP de Telecontrol están en el mismo rack, la comunicación entre ellos tiene lugar por el bus de fondo. La CPU está asignada automáticamente al CP de Telecontrol.

TIM 1531 IRC: Comunicación con CPU vía Ethernet

El TIM 1531 IRC no se inserta en el rack de la CPU. El TIM puede estar conectado a una o varias CPU vía Ethernet. La CPU deseada para la comunicación por Telecontrol tiene que asignarse al TIM.

TIM 1531 IRC: comunicación TLS con la CPU

La conexión del TIM con la CPU emplea la comunicación segura por TLS en todos los protocolos de Telecontrol compatibles con el TIM.

Para la comunicación por TLS hay que utilizar un certificado de CPU recién creado e indicarlo en el grupo de parámetros "Números de dispositivos" del TIM.

Secuencia de pasos

Si se crea primero un certificado nuevo para la CPU y después se asigna la CPU al TIM, el certificado de la CPU se aplica automáticamente a la configuración del dispositivo.

Si primero se asigna la CPU al TIM y luego se crea el certificado de CPU, deberá buscar la ID del certificado de CPU e introducirlo manualmente en la configuración de dispositivos del TIM o eliminar la CPU del campo "CPU asignada" y volver a asignarla.

Generación del certificado de CPU y asignación de la CPU 1500

Requisitos

Para generar y asignar certificados deben cumplirse los siguientes requisitos:

- En calidad de usuario del proyecto de STEP 7 debe tener por lo menos el derecho de la función "NET Administrator".
  Ver al respecto "Configuración de seguridad > Usuarios y roles > Roles asignados".
  Si utiliza las funciones de seguridad del S7-1500 V3.0, también necesitará un usuario creado con los derechos necesarios; véase Usuario de seguridad (Página 97).
- Los dispositivos tienen la versión de firmware mínima necesaria; ver arriba.
- Los datos de configuración de la CPU están protegidos.
  Ver al respecto "Protección & Seguridad > Protección de datos de configuración confidenciales del PLC"

Para poder asignar la CPU local al TIM 1531 IRC deben cumplirse los requisitos siguientes:

- La CPU y el TIM 1531 IRC están conectados en red.
- Para el TIM está activado el protocolo de Telecontrol deseado en "Tipos de comunicación".

Generar el certificado de la CPU

Proceda del siguiente modo para generar el certificado de CPU:

1. Seleccione en la CPU el grupo de parámetros "Protección & Seguridad > Administrador de certificados > Ajustes globales de seguridad".
2. Active la opción "Utilizar ajustes globales de seguridad para el administrador de certificados". El certificado generado localmente por la CPU en el ajuste predeterminado no puede utilizarse para la comunicación TLS.
   Recuerde:
   Al activar la opción se borran los certificados existentes en la CPU.
3. Vaya a "Protección & Seguridad > Mecanismos de conexión > Modo de comunicación hacia TIA Portal y HMI".
4. En la fila "Certificado de comunicación del PLC" haga clic con el botón derecho del ratón en el icono de la lista de selección.

5. Debajo de la lista de selección que se abre, haga clic en el botón "Crear".
   Se abre el cuadro de diálogo "Crear certificado". Se recomienda seleccionar las siguientes opciones:
   - Uso previsto: TLS Server
   - Autoridad de certificación (CA): Firmado por la autoridad de certificación
   - Propietario del certificado: nombre de la CPU seleccionada
   - Método de cifrado: EC (recomendado)
   - Algoritmo Hash: sha256 (recomendado)

   En caso necesario, en "Nombre alternativo del propietario del certificado (SAN)" es posible complementar otro tipo de dirección para la CPU.
6. Conserve los ajustes y haga clic en "Aceptar".
   El certificado TLS recién creado se muestra en la CPU como "Certificado de comunicación del PLC" y en la tabla "Certificados de dispositivos".

La ID del certificado de CPU recién creado se introduce automáticamente en los siguientes lugares cuando se asigna la CPU al TIM (ver más abajo):

- En el cuadro de diálogo "Números de dispositivos" del TIM
- En el administrador de certificados del TIM como certificado de interlocutor

Asignar la CPU al TIM 1531 IRC

1. En el TIM que debe comunicarse con la CPU abra el grupo de parámetros "Números de dispositivos".
2. En la fila "CPU asignada" haga clic con el botón derecho del ratón en el icono de la lista de selección.
   Se abre la lista con las CPU conectadas en red.
3. Seleccione la CPU que debe asignarse al TIM y haga clic debajo en la marca de verificación verde.
   En la fila "CPU asignada" se muestra el nombre de la CPU.
   Al mismo tiempo, en la fila "Certificado de comunicación" se muestra automáticamente la ID del certificado generado previamente para la CPU.

Configuración ulterior

Configure a continuación las demás estaciones como interlocutores de la comunicación, así como las correspondientes conexiones de Telecontrol.

4.17 Ajustes de registro

Ajustes de registro

Validez: TIM 1531 IRC

Para fines de vigilancia es posible grabar eventos en archivos de registro. Existe la posibilidad de ajustar la forma en que deben grabarse dichos eventos:

- Registro local
  Los avisos sobre eventos y errores internos se guardan en el búfer de diagnóstico del TIM. Es posible grabar los siguientes eventos:
  - Registro de auditoría: eventos de auditoría
  - Registro del sistema: eventos de sistema
- Registro del sistema en red
  Los avisos relacionados con los eventos se envían a un servidor Syslog en formato UDP conforme a RFC 5424 o RFC 5426. Encontrará información detallada sobre la estructura de los telegramas Syslog y las entradas soportadas del búfer de eventos en el capítulo Recomendaciones Security (Página 13).

Puede encontrar más información sobre la funcionalidad y la configuración de las funciones en el sistema de información de STEP 7.

4.18 SNMP

SNMP

Encontrará el volumen de prestaciones de los módulos en el respectivo manual de producto.

Cuando las funciones de seguridad están activadas están disponibles las siguientes selecciones y posibilidades de ajuste en función del módulo.

SNMP

- **"Activar SNMP"**
  Si la opción está activada se habilita la comunicación vía SNMP en el dispositivo. SNMPv1 está desactivado por defecto.
  Si la opción está desactivada no se responderá a solicitudes de clientes SNMP ni a través de SNMPv1 ni a través de SNMPv3.
- **"Usar SNMPv1"**
  Activa el uso de SNMPv1 para el dispositivo. Encontrará la configuración de los Community Strings necesarios más abajo (SNMPv1).
- **"Usar SNMPv3"**
  Activa el uso de SNMPv3 para el dispositivo. Encontrará la configuración de los algoritmos necesarios más abajo (SNMPv3).

SNMPv1

Los Community Strings deben enviarse también al dispositivo vía SNMPv1 en caso de peticiones.

Tenga en cuenta la grafía en minúsculas de los Community Strings predeterminados.

- **"Community String de lectura"**
  El string es necesario para el acceso de lectura.
  Deje el string predeterminado "public" o configure un string.
- **"Permitir acceso de escritura"**
  Si se activa la opción se habilita el acceso de escritura al dispositivo y el Community String correspondiente pasa a ser editable.
- **"Community String de escritura"**
  El string es necesario para el acceso de escritura y también puede utilizarse para el acceso de lectura.
  Deje el string predeterminado "private" o configure un string.

Nota

Seguridad del acceso

Por motivos de seguridad se recomienda modificar los strings predeterminados y ampliamente conocidos "public" y "private".

SNMPv3

Los algoritmos deben configurarse para el acceso cifrado al dispositivo vía SNMPv3.

- **"Algoritmo de autenticación"**
  Seleccione el método de autenticación que debe utilizarse en la lista desplegable.
- **"Algoritmo de encriptación"**
  Seleccione el algoritmo de cifrado que debe utilizarse en la lista desplegable.

Administración de usuarios

En la administración de usuarios, que se encuentra en los ajustes globales de seguridad, se asignan funciones a los diferentes usuarios.

En las propiedades de las funciones se muestra la lista de derechos de cada función, como los diferentes tipos de acceso vía SNMP. Para nuevas funciones pueden configurarse libremente los diferentes derechos.

Encontrará información sobre usuarios, funciones y las directivas de contraseña en el sistema de información de STEP 7.

4.19 Administrador de certificados global

Certificados de dispositivos SIMATIC NET

Los módulos de comunicación SIMATIC NET utilizan básicamente el administrador de certificados global. Lo encontrará en el árbol del proyecto, bajo "Configuración de seguridad > Funciones de seguridad".

Todos los certificados locales de módulos de comunicación SIMATIC NET están también dentro del administrador de certificados global.

4.20 Seguridad y certificados

4.20.1 Usuario de seguridad

Creación de un usuario de seguridad

Para configurar funciones de seguridad se requieren los derechos de configuración adecuados. Para ello es preciso crear al menos un usuario de seguridad con los derechos correspondientes.

Navegue hasta los ajustes globales de seguridad > "Usuarios y funciones" > ficha "Usuarios".

1. Cree un usuario y configure los parámetros.
2. En la zona inferior "Funciones asignadas", asigne a dicho usuario la función "NET Standard" o "NET Administrator".

Una vez iniciada la sesión en el proyecto de STEP 7, el usuario puede realizar los ajustes necesarios.

Las próximas veces que trabaje en parámetros de seguridad, inicie sesión también con este usuario.

Funciones de seguridad del S7-1500 V3.0 junto con TIM 1531 IRC V2.4

Para poder utilizar conexiones TLS del TIM 1531 IRC junto con la CPU S7-1500 V3.0, es necesario activar el "control de acceso legacy" en la CPU (grupo de parámetros "Protección y seguridad > Control de acceso").

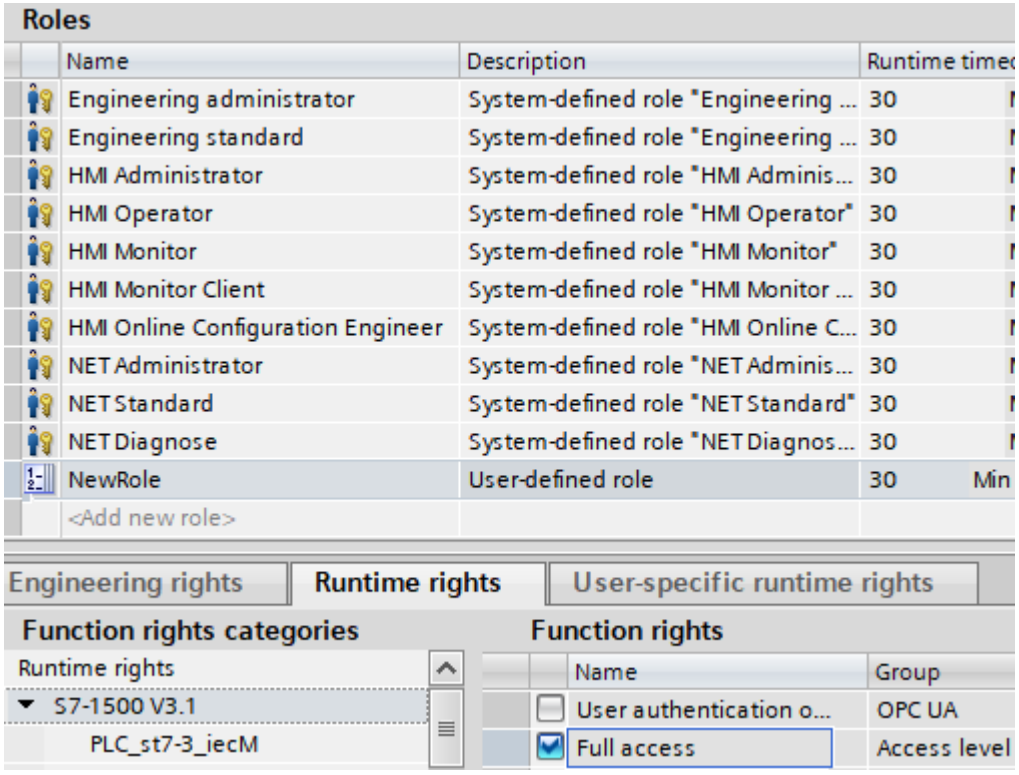
Usuario de seguridad para S7-1500 (general)

Ese apartado no es válido para el TIM 1531 IRC V2.4.

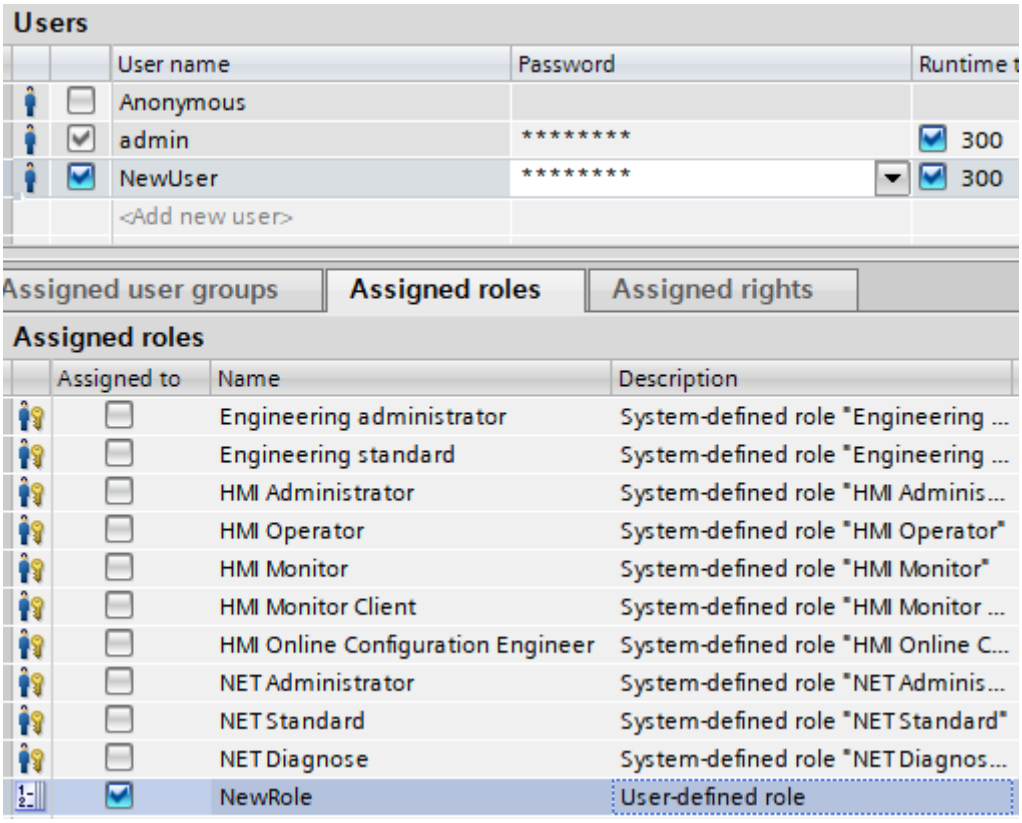
Para poder utilizar en general las funciones de seguridad del S7-1500 V3.0, es necesario crear un usuario de seguridad que tenga asignado un rol con acceso completo para el S7-1500 en el proyecto.

Proceda del siguiente modo en la configuración:

1. Cree un nuevo rol con acceso completo para el S7-1500.



2. Cree un usuario nuevo y asígnele el nuevo rol.



4.20.2 Ajustes del registro - 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.

4.20.3 SYSLOG

Utilización de SYSLOG solo con 1 conexión VPN

Si desea utilizar SYSLOG con nivel 7 (debug) a través de conexiones VPN, solo es posible hacerlo si hay una única conexión VPN configurada.

4.20.4 VPN

4.20.4.1 VPN (Virtual Private Network)

VPN - IPsec

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 IPsec) entre dos sistemas TI o redes seguros, sorteando de este modo una red insegura.

El túnel IPsec reenvía la totalidad de los datos, incluso de protocolos de capas superiores (HTTP, FTP, etc.).

El tráfico de datos entre dos componentes de la red se transporta de forma 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

4.20.4.2 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, 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: Inicie la sesión con este usuario.
2. Activar la opción "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.

Seleccionar "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.

El establecimiento de una conexión VPN con una estación de ingeniería que es, al mismo tiempo, servidor de Telecontrol (TCSB instalado) se realiza de forma paralela a la sincronización horaria del CP, del siguiente modo:

Desea que se establezca una conexión VPN con la estación de ingeniería (con el TCSB) a través del CP. Incluso aunque el CP aún no tenga la hora actual, se establece la conexión VPN. Los certificados utilizados se considerarán válidos y la comunicación segura funcionará.

Una vez establecida la conexión, el CP sincroniza su hora con el PC, ya que el servidor de Telecontrol actúa como maestro para la hora siempre que la comunicación por Telecontrol está activa.

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.

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

El establecimiento de la comunicación por túnel VPN entre SOFTNET Security Client y el CP se realiza de acuerdo con el capítulo Creación de túneles VPN para la comunicación S7 entre estaciones (Página 101).

La comunicación por túnel VPN solo tiene éxito con el dispositivo interno desactivado

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 tiene éxito.

4.20.4.4 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.

4.20.4.5 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".

4.20.5 Administrador de certificados

Administrador de certificados de dispositivos SIMATIC NET

Los módulos de comunicación SIMATIC NET utilizan básicamente el administrador de certificados global. Lo encontrará en el árbol del proyecto, bajo "Configuración de seguridad > Funciones de seguridad".

Todos los certificados generados y mostrados en el módulo de comunicación SIMATIC NET durante la configuración también están en el administrador de certificados global.

Certificados para la autenticación

Si para el módulo de comunicación se ha configurado la comunicación segura con autenticación, se necesitan certificados propios y certificados del interlocutor para que sea posible la comunicación.

Todos los dispositivos de un proyecto STEP 7 con las funciones de seguridad activadas disponen de certificados. El proyecto STEP 7 es la entidad emisora.

Ejemplos de servicios y funciones que necesitan certificados:

- Comunicación del TIM 1531 IRC con la CPU asignada
  La conexión del TIM con la CPU emplea la comunicación segura por TLS en todos los protocolos de Telecontrol compatibles con el TIM.
  Para la comunicación por TLS hay que utilizar un certificado de CPU recién creado e indicarlo en el grupo de parámetros "Números de dispositivos" del TIM.
  Consulte el procedimiento en el capítulo TIM 1531 IRC: Certificado TLS de la CPU (Página 92).
- Transferencia segura de mensajes de correo electrónico
  Para la transferencia de datos vía SSL/TLS se crea un certificado SSL para el módulo. Puede verse en STEP 7 dentro del administrador de certificados local y en "Ajustes globales de seguridad > Administrador de certificados > Certificados de dispositivos" con el servicio "WebServer".

Si un módulo de comunicación STEP 7 debe comunicarse con interlocutores ajenos a Siemens de forma segura, tienen que intercambiarse los certificados correspondientes de los interlocutores. Para ello, proceda del siguiente modo:

1. Importar certificado ajeno del interlocutor de la comunicación externo
   Ajustes globales de seguridad del proyecto > "Autoridades de certificación raíz y certificados acreditados"
2. Asignar el certificado al módulo de comunicación

Asignación de certificados

Si se crean a posteriori certificados para módulos en STEP 7 o se importan certificados ajenos a STEP 7 será necesario asignarlos al módulo correspondiente utilizando uno de los métodos siguientes:

- Administrador de certificados local del módulo de comunicación > "Certificados de los dispositivos interlocutores"
- Ajustes globales de seguridad del proyecto > "Autoridades de certificación raíz y certificados acreditados"

Consulte el procedimiento en el capítulo Manejo de los certificados TLS (Página 105).

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

4.20.6 Manejo de los certificados TLS

Comunicación entre CPU y módulo de Telecontrol

CP: comunicación a través del bus de fondo

Puesto que la CPU y el CP están en el mismo rack, la comunicación entre ellos tiene lugar por el bus de fondo. La CPU está asignada automáticamente al CP de Telecontrol.

TIM 1531 IRC: Comunicación con CPU vía Ethernet

El TIM 1531 IRC no se inserta en el rack de la CPU. El TIM puede estar conectado a una o varias CPU vía Ethernet. La CPU deseada para la comunicación por Telecontrol tiene que asignarse al TIM.

TIM 1531 IRC: comunicación TLS con la CPU

La conexión del TIM con la CPU emplea la comunicación segura por TLS en todos los protocolos de Telecontrol compatibles con el TIM.

Para la comunicación por TLS hay que utilizar un certificado de CPU recién creado e indicarlo en el grupo de parámetros "Números de dispositivos" del TIM.

Secuencia de pasos

Si se crea primero un certificado nuevo para la CPU y después se asigna la CPU al TIM, el certificado de la CPU se aplica automáticamente a la configuración del dispositivo.

Si primero se asigna la CPU al TIM y luego se crea el certificado de CPU, deberá buscar la ID del certificado de CPU e introducirlo manualmente en la configuración de dispositivos del TIM o eliminar la CPU del campo "CPU asignada" y volver a asignarla.

Validez y requisitos

Validez

La descripción que aparece a continuación tiene validez para los módulos siguientes:

- TIM 1531 IRC V2.3 a partir de la versión de firmware V2.3
  junto con CPU 1500 a partir de la versión de firmware V2.9
- CP 1542SP-1 IRC a partir de la versión de firmware V2.2
  junto con ET 200SP CPU a partir de la versión de firmware V2.9
- CP 1543-1 a partir de la versión de firmware V3.4
  junto con CPU 1200 a partir de la versión de firmware V4.5

Requisitos

Para el uso descrito a continuación de los certificados se deben cumplir los siguientes requisitos:

- En calidad de usuario del proyecto de STEP 7 debe tener por lo menos el derecho de la función "NET Administrator".
  Ver al respecto "Configuración de seguridad > Usuarios y roles > Roles asignados".
  Si utiliza las funciones de seguridad del S7-1500 V3.0, también necesitará un usuario creado con los derechos necesarios; véase Usuario de seguridad (Página 97).
- Los dispositivos tienen la versión de firmware mínima necesaria.
- Los datos de configuración de la CPU están protegidos.
  Ver al respecto "Protección & Seguridad > Protección de datos de configuración confidenciales del PLC"
- Para el TIM está activado el protocolo de Telecontrol deseado en "Tipos de comunicación".

- La CPU y el TIM 1531 IRC están conectados en red.
- El certificado de la CPU está generado y se encuentra en el administrador de certificados global; consulte el capítulo TIM 1531 IRC: Certificado TLS de la CPU (Página 92).

Configuración de TLS para conexiones de Telecontrol

La comunicación segura por TLS puede configurarse para las conexiones de Telecontrol de los módulos de comunicación:
Editor Datos de red > ficha "TeleControl")

Para los CP es imprescindible activar las funciones de seguridad.

Conexiones TLS con interlocutores del proyecto

1. Antes que nada, cargue las conexiones de Telecontrol.
2. Seleccione la conexión principal y, en las propiedades de la conexión, el grupo de parámetros "Comunicación segura (TLS)".
3. Active la opción "Activar comunicación segura".

Si todos los certificados de los interlocutores están presentes, en los dispositivos Siemens la "ID de certificado propio" y la "ID de certificado de interlocutor" se incluirán automáticamente en toda la conexión, incluidas las conexiones parciales.

Conexiones TLS con dispositivos de terceros

Si desea utilizar la comunicación segura por TLS para conexiones de Telecontrol con dispositivos de terceros, deberá realizar algunos pasos más.

1. Ajuste primero el puerto Listener seguro para TLS o compruebe el ajuste (Ajustes básicos > Puerto Listener seguro). El número de puerto es necesario para el interlocutor de la conexión.
2. Cree un certificado para el dispositivo de terceros en STEP 7.
   Alternativamente, importe el certificado a STEP 7 si hay uno disponible para el dispositivo de terceros.
   Para importar y generar certificados, véase más abajo (Certificados para conexiones TLS con dispositivos de terceros).
3. Asigne el certificado del dispositivo de terceros al interlocutor de la conexión STEP 7 como "Certificado de confianza".
   Consulte el procedimiento a continuación (Certificados para conexiones TLS con dispositivos de terceros).
4. Exporte el certificado de dispositivo del módulo de comunicación, el certificado de dispositivo del dispositivo de terceros (si se ha creado en STEP 7) y el certificado CA asociado de STEP 7 e impórtelos al dispositivo de terceros o a su herramienta de configuración.
5. Cree la conexión de Telecontrol y active la opción "Activar comunicación segura".
6. Aplique las ID a los parámetros de conexión.
   - Introduzca la ID del certificado de dispositivo de terceros importado o generado (desde el administrador de certificados global) en el campo "ID de certificado de interlocutor".
   - Introduzca la ID del certificado del interlocutor de conexión STEP 7 en el campo "ID de certificado propio".

Certificados para conexiones TLS con dispositivos de terceros

Importar o crear y asignar un certificado de dispositivo de terceros

El certificado de dispositivo de terceros puede ponerse a disposición del proyecto de STEP 7 de dos formas alternativas:

- **Importar**
  En caso de existir, puede guardar el certificado del dispositivo de terceros en el sistema de archivos de la estación de ingeniería e importarlo a STEP 7.
  Para la importación, abra en el administrador de certificados global la ficha "Autoridades de certificación raíz y certificados acreditados", haga clic en una fila libre y abra el menú contextual "Importar".
  Seguidamente, deberá asignar el certificado importado al módulo de comunicación (ver más abajo).
- **Crear**
  Alternativamente, puede crear un certificado para el dispositivo de terceros en STEP 7 e importarlo al dispositivo de terceros.
  Para ello, proceda del siguiente modo:

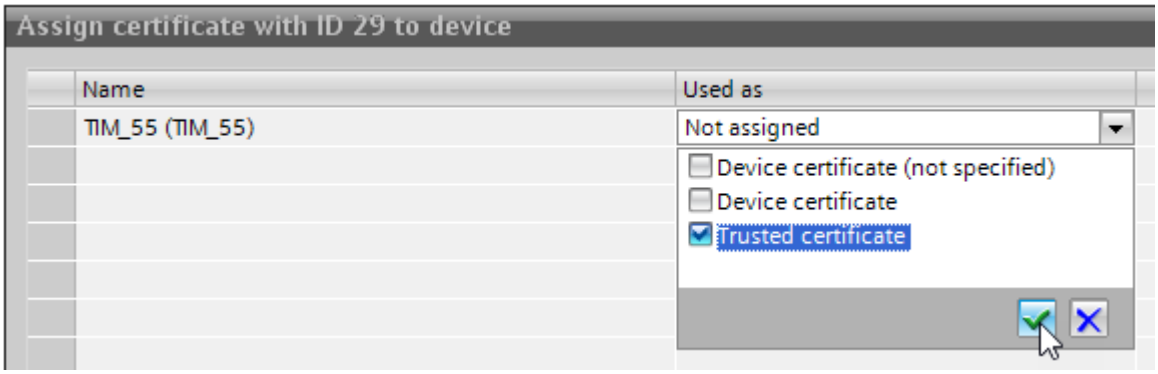
1. En el árbol del proyecto, abra el administrador de certificados global:
   "Configuración de seguridad > Funciones de seguridad > Administrador de certificados > ficha Certificados de dispositivos".
2. Haga clic en el menú contextual "Crear" de una fila libre.
   Se abre el cuadro de diálogo "Crear certificado".
3. Seleccione las siguientes opciones para el certificado del dispositivo de terceros:
   - Uso previsto: TLS Client / Server
   - Autoridad de certificación (CA): Autofirma
   - Propietario del certificado: Introduzca el nombre del dispositivo de terceros.

   Adapte los demás parámetros a la funcionalidad del dispositivo de terceros.
   Ajustes recomendados:
   - Método de cifrado: RSA
   - Longitud de clave: 2048
   - Algoritmo Hash: sha256
4. Cierre el cuadro de diálogo con "Aceptar".
   El certificado aparece en la tabla.
   La ID del certificado se necesita para la asignación y la conexión de Telecontrol.

- **Asignar**

1. En el administrador de certificados global, seleccione el certificado importado o recién creado y abra el menú contextual "Asignar".
2. Seleccione en la lista el módulo con el que el dispositivo de terceros debe comunicarse a través de la conexión de Telecontrol.

3. En la columna "Usado como", haga clic en la celda ("No asignado"), seleccione la opción "Certificado de confianza" y haga clic en la marca de verificación verde.



4. Cierre el cuadro de diálogo con Aceptar.
   La ID del certificado se necesita para la conexión de Telecontrol.

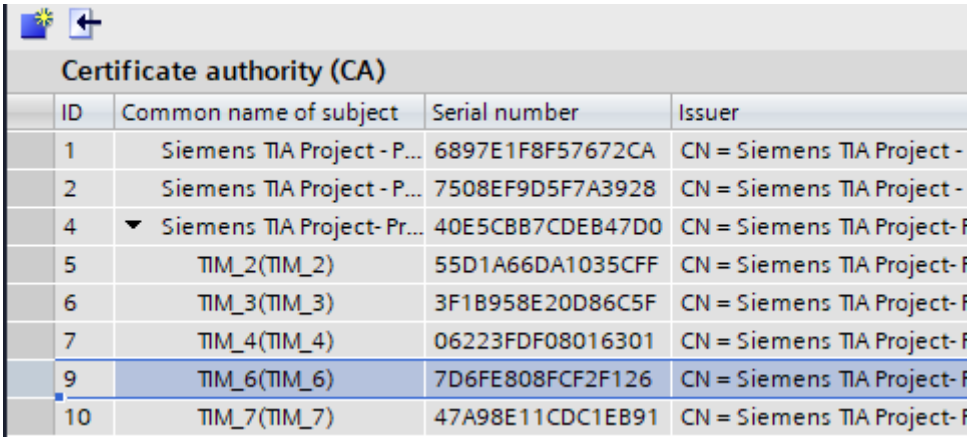
Crear una conexión de Telecontrol e introducir la ID del certificado

1. Cree una conexión de Telecontrol como se ha descrito anteriormente.
2. En las propiedades de la conexión, seleccione el grupo de parámetros "Comunicación segura (TLS)" y active la opción "Activar comunicación segura".
3. Introduzca manualmente los siguientes valores:
   - ID de certificado de interlocutor: ID del certificado importado o creado manualmente para el dispositivo de terceros
   - ID de certificado propio: ID del certificado del módulo de comunicación
4. Compruebe los números de puertos y los parámetros de dispositivos de terceros.
   - El puerto Listener seguro se configura en el grupo de parámetros "Ajustes básicos" del módulo correspondiente.
   - Configure el tipo de nodo de red en las propiedades de la conexión (grupo de parámetros "Parámetros de dispositivo de terceros").
     Si el dispositivo de terceros es el maestro, seleccione "Estación central".

Exportar certificados STEP 7 para dispositivo de terceros e importarlos al dispositivo de terceros

Para la conexión TLS con el dispositivo de terceros es necesario exportar un certificado de dispositivo del módulo de comunicación creado en STEP 7 y el certificado CA correspondiente.

1. Certificado de dispositivo creado en STEP 7 para el dispositivo de terceros
   - Abra la ficha "Certificados de dispositivo" en el administrador de certificados global.
   - Seleccione el certificado para el dispositivo de terceros y haga clic en el menú contextual "Exportar certificado".
   - Guarde el certificado en el sistema de archivos de la estación de ingeniería.
     Puede modificar el formato de archivo predeterminado "*.der".
     Encontrará una descripción de las funciones de los formatos de archivo de los certificados en el sistema de ayuda, capítulo "Exportar certificados".
2. Certificado de dispositivo del módulo de comunicación
   - Seleccione en la ficha "Certificados de dispositivos" el certificado de dispositivo del módulo de comunicación como certificado de interlocutor para el dispositivo de terceros.
   - Visualice por completo la columna "Emisor".
     El nombre del emisor se necesita para exportar el certificado CA emisor.
   - Exporte el certificado de dispositivo seleccionado del módulo con el menú contextual "Exportar certificado".
3. Certificado CA emisor
   - Cambie a la ficha "Autoridad de certificación (CA)".
   - Seleccione el certificado CA que ha firmado el certificado de dispositivo del módulo de comunicación.
     Si se despliega el certificado CA, debajo se muestran todos los certificados de dispositivos derivados, entre ellos también el del módulo de comunicación.



Certificate authority (CA)

ID	Common name of subject	Serial number	Issuer
1	Siemens TIA Project - P...	6897E1F8F57672CA	CN = Siemens TIA Project -
2	Siemens TIA Project - P...	7508EF9D5F7A3928	CN = Siemens TIA Project -
4	Siemens TIA Project- Pr...	40E5CBB7CDEB47D0	CN = Siemens TIA Project-
5	TIM_2(TIM_2)	55D1A66DA1035CFF	CN = Siemens TIA Project-
6	TIM_3(TIM_3)	3F1B958E20D86C5F	CN = Siemens TIA Project-
7	TIM_4(TIM_4)	06223FDF08016301	CN = Siemens TIA Project-
9	TIM_6(TIM_6)	7D6FE808FCF2F126	CN = Siemens TIA Project-
10	TIM_7(TIM_7)	47A98E11CDC1EB91	CN = Siemens TIA Project-

Figura 4-11 Administrador de certificados global: aquí, el certificado CA tiene la ID 4 y el certificado de dispositivo, la ID 9.

   - Exporte el certificado CA con el menú contextual "Exportar certificado".
4. Importe todos los certificados guardados como certificados de confianza al dispositivo de terceros o a su herramienta de configuración.
   Los certificados son necesarios para la comunicación segura en tiempo de ejecución.

Cambio de certificado: Nombre alternativo del propietario del certificado

STEP 7 adopta las propiedades "Nombre DNS", "Dirección IP" y "URI" del parámetro "Nombre alternativo del propietario del certificado" (Windows: "Nombre alternativo del solicitante") de los datos de configuración de STEP 7.

Este parámetro de un certificado se puede cambiar en el administrador de certificados de los ajustes globales de seguridad. Seleccione para ello un certificado en la tabla de certificados de dispositivos y ejecute el menú contextual "Renovar". Las propiedades del parámetro "Nombre alternativo del propietario del certificado" modificadas en STEP 7 no se aplican en el proyecto de STEP 7.

4.21 TIM 1531 IRC: Protección

4.21.1 Protección

Funciones de protección

El módulo ofrece diferentes niveles de acceso para restringir el acceso a determinadas funciones.

ATENCIÓN
La configuración de un nivel de acceso no sustituye la protección de know-how La parametrización de niveles de acceso impide que se realicen cambios ilegítimos en el módulo restringiendo los derechos de descarga. Sin embargo, por ello no están protegidos contra escritura o lectura los bloques de una tarjeta de memoria. Para proteger el código de los bloques de la tarjeta de memoria debe utilizarse la protección de know-how.

La tabla de los niveles de acceso

La configuración de los niveles de acceso se realiza en la tabla. Las marcas de verificación verdes que se muestran en las columnas situadas a la derecha del nivel de acceso correspondiente indican las operaciones que pueden llevarse a cabo como máximo sin conocer la contraseña del nivel de acceso en cuestión.

El nivel de acceso predeterminado es "Acceso completo (sin protección)". Todos los usuarios pueden leer y modificar la configuración. No hay ninguna contraseña configurad y tampoco se requiere para el acceso online.

Es posible configurar los niveles de protección siguientes:

- **Acceso completo (sin protección)**
  Cualquiera puede leer y modificar la configuración y los bloques.
- **Acceso de lectura**
  Con este nivel de acceso, si no se introduce la contraseña solo es posible acceder en modo de lectura a la configuración hardware y los bloques, es decir, sin introducir la contraseña no se pueden cargar ni bloques ni la configuración hardware en el TIM. Tampoco está permitido realizar funciones de test en modo de escritura ni actualizaciones de firmware sin contraseña.
- **Sin acceso (protección completa)**
  Cuando el módulo está completamente protegido no está permitido el acceso de lectura ni escritura a la configuración hardware ni a los bloques.

Para utilizar las funciones de los niveles de acceso sin marcar es necesario introducir una contraseña.

La legitimación con la contraseña permite volver a tener acceso completo al módulo.

Comportamiento de un módulo protegido por contraseña durante el funcionamiento

La protección del módulo es efectiva una vez que se han cargado los ajustes en el módulo.

Antes de ejecutar una función online se comprueba que esté permitida. Si está protegida por contraseña, deberá introducirse.

Ejemplo:
El módulo se ha configurado con acceso de lectura y el usuario desea ejecutar la función "Forzar variable". Puesto que esta función es un acceso de escritura, para ejecutarla debe introducirse la contraseña configurada.

Las funciones protegidas con contraseña solo pueden ejecutarse desde una PG/un PC en un mismo momento. Otra PG/otro PC no podrá iniciar sesión.

La autorización de acceso a los datos protegidos es válida mientras dure la conexión online o hasta que se suprima manualmente la autorización de acceso mediante "Online > Borrar derechos de acceso".

Todos los niveles de acceso permiten el acceso ilimitado a determinadas funciones sin necesidad de introducir la contraseña, p. ej. identificación por medio de la función "Dispositivos accesibles".

4.21.2 Configurar protección de acceso

Configuración

Es posible introducir varias contraseñas, con lo que se crean diferentes derechos de acceso para grupos de usuarios distintos.

La contraseñas se introducen en una tabla, de modo que cada contraseña tiene asignado un nivel de acceso concreto.

El efecto que tiene cada contraseña se explica en la columna "Nivel de acceso".

Ejemplo:

Seleccione el nivel de acceso "Sin acceso (protección completa)" para el módulo e introduzca una contraseña propia para cada uno de los niveles de acceso situados por encima en la tabla.

Para los usuarios que no conozcan ninguna de las contraseñas, el módulo está completamente protegido.

Para los usuarios que conozcan una de las contraseñas parametrizadas, el efecto depende de la fila de la tabla en la que esté la contraseña:

- La contraseña de la fila 1 "Acceso completo (sin protección)" actúa como si el módulo estuviera desprotegido. Los usuarios que conozcan esta contraseña tendrán acceso ilimitado al módulo.
- La contraseña de la fila 2 "Acceso de lectura" actúa como si el módulo estuviera protegido contra escritura. A pesar de conocer esta contraseña, los usuarios solo tendrán acceso de lectura al módulo.
- La contraseña de la fila 3 "Sin acceso (protección completa)" actúa como si el módulo estuviera protegido contra escritura y lectura. Los usuarios que conozcan esta contraseña solo tendrán acceso de lectura al módulo.

Procedimiento

Para parametrizar los niveles de acceso al módulo, proceda del siguiente modo:

1. Abra las propiedades del módulo en la ventana de inspección.
2. Abra la entrada "Protección" en la navegación local.
   En la ventana de inspección se muestra una tabla con los niveles de acceso posibles.
3. Seleccione el nivel de acceso deseado en la primera columna de la tabla. Las marcas de verificación verdes que se muestran en las columnas situadas a la derecha del nivel de protección correspondiente indican las operaciones que se pueden seguir realizando sin introducir la contraseña.
4. Si se ha seleccionado un nivel de acceso distinto a "Acceso completo":
   - Asigne una contraseña para el acceso completo en la columna "Contraseña" de la primera fila (acceso completo).
   - Repita la contraseña introducida en la columna "Confirmar contraseña" para evitar entradas incorrectas.
   - Asegúrese de que la contraseña sea lo suficientemente segura, es decir, de que no tenga un patrón reconocible por una máquina.
   - La entrada de una contraseña en la primera fila "Acceso completo (sin protección)" es obligatoria y permite a las personas que conocen la contraseña acceder sin limitaciones al módulo, independientemente del nivel de protección seleccionado.
5. En caso necesario, asigne otras contraseñas a otros niveles de acceso, siempre que el nivel de acceso seleccionado lo permita.
6. Cargue la configuración hardware para que el nivel de acceso sea efectivo.

Resultado

La configuración hardware y los bloques están protegidos contra accesos online no autorizados en función del nivel de acceso ajustado. Si una operación no puede ejecutarse

sin contraseña debido al nivel de acceso parametrizado, se abre un cuadro de diálogo para introducir una contraseña.

4.22 Conexiones de Telecontrol

4.22.1 Conexiones de Telecontrol

Conexiones de Telecontrol

Para la comunicación remota se necesitan relaciones de Telecontrol entre los módulos de comunicación intervinientes. Dependiendo del tipo de módulo y de la versión de firmware, la configuración se realiza en los grupos de parámetros siguientes:

- grupo de parámetros "Estaciones interlocutoras"
  o
- editor "Datos de red"

Configuración en el grupo de parámetros "Estaciones interlocutoras"

Para los siguientes CP, que solo actúan como estación, las relaciones con la estación central o con el maestro se configuran en el grupo de parámetros "Estaciones interlocutoras":

- CP 1243-1 / CP 1243-7 LTE / CP 1243-8 IRC hasta el firmware V3.0
- CP 1542SP-1 IRC hasta el firmware V1.0

Todos los demás ajustes necesarios para la comunicación con la estación central se toman de los restantes datos de configuración de los CP y no es necesario configurarlos específicamente para las conexiones.

Configuración en el editor "Datos de red"

Para los módulos siguientes, las conexiones de Telecontrol se configuran en el editor "Datos de red":

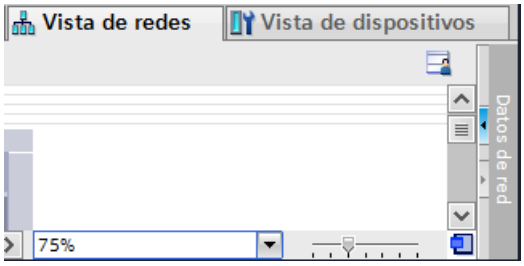
- CP 1243-1 / CP 1243-8 IRC a partir de versión de firmware V3.1
- CP 1243-7 LTE a partir de versión de firmware V3.3
- CP 1542SP-1 IRC a partir de versión de firmware V2.0
- TIM 1531 IRC a partir de versión de firmware V2.0
- Dispositivo de terceros
  Un dispositivo de terceros es un módulo que no puede configurarse en STEP 7, por ejemplo, la estación maestra de otro fabricante.

4.22.2 Editor "Datos de red"

Abrir el editor "Datos de red" > ficha "TeleControl"

Para abrir el editor proceda del siguiente modo:

1. Abra la vista de redes del proyecto.
   A la derecha encontrará sin desplegar el editor "Datos de red".



2. Abra el editor "Datos de red" con el símbolo de flecha.
   Se muestra el editor con varias fichas; a la izquierda está situada la ficha "Vista general de la red".
3. Arrastre hacia afuera el editor hasta que aparezca la ficha "TeleControl".
   Esta ficha está subdividida en las siguientes fichas:
   - ST7
   - DNP3
   - IEC 60870

   Según el protocolo utilizado, seleccione la ficha correspondiente para configurar conexiones de Telecontrol.

Visualizar y mostrar/ocultar columnas

	Conexión	Punto de in..	Dispositiv...	Interfaz inicial	Punto final	Disp...	Lista de int..	Interfaz final/dirección
	*	*	*		*	*		
	Section_1	1	1	TIM_1 - Interfaz Et..	2	2	2,3	TIM_2 - TIM_2 - Interfaz Et
	Section_2	2	2	TIM_2 - Interfaz Et..	1	1	2,3	TIM_1 - TIM_1 - Interfaz Et
	Section_3	TIM_2	2	TIM_2 - Serial Inter.	3	3	1	TIM_3 - TIM_3 - Serial Inte
	Section_4	3	3	TIM_3 - Serial Inter.	1	1	1	TIM_2 - TIM_2 - Serial Inte
	Section_5	TIM_2	2	TIM_2 - Interfaz Et..	1	1	3, 12	TIM_1 - TIM_1 - Interfaz Et
	Section_6	2	2	TIM_2 - Serial Inter.	3	3	3	TIM_3 - TIM_3 - Serial Inte
	Section_7	3	3	TIM_3 - Serial Inter.	2	2	2	TIM_2 - TIM_2 - Serial Inte
	Section_99	1	1	TIM_1 - Interfaz Et..	Dispositivo de terce.	99	99	192.168.2.99
	Section_8	1	1	TIM_1 - Interfaz Et..	1200	12	12	TIM_2 - TIM_2 - Interfaz Et
	Section_9	TIM_2	2	TIM_2 - Interfaz Et..	1200	12	1	S7-1200-Station_1 - CP 1..
	Section_10	1200	12	CP 1243-8 IRC - Int.	1	1	1	TIM_2 - TIM_2 - Interfaz Et

Figura 4-12 Editor "Datos de red", ficha "Telecontrol > ..."

En la tabla "Conexiones de Telecontrol" es posible mostrar, ocultar u organizar columnas y optimizar su ancho. Haga clic con el botón derecho del ratón en el encabezado de una columna para acceder al menú contextual.

- Organizar columnas
  Si se hace clic en el encabezado de una columna, es posible desplazar la columna dentro de la tabla manteniendo pulsado el botón izquierdo del ratón.
- Mostrar/ocultar
  Esta función del menú contextual permite mostrar u ocultar columnas individualmente. Eso permite mantener una mejor perspectiva de la tabla.
- Mostrar todas las columnas
  Muestra todas las columnas de la tabla.
- Optimizar ancho / Optimizar ancho de todas las columnas
  Con estos menús contextuales se optimiza el ancho de la columna seleccionada o bien de todas las columnas de la tabla.
  El ancho de la columna se adapta entonces a la entrada más ancha de la columna.

Algunos campos de la tabla son editables, en otros el parámetro se configura mediante una lista desplegable.

Los campos sin configurar o mal configurados se representan con fondo rojo.

Nombres de las conexiones

Es posible adaptar los nombres predeterminados de las conexiones.

Están permitidos como máximo 129 caracteres de los siguientes juegos de caracteres ASCII (números decimales):

- **N.º 32..126**
  espacio , ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~
- **N.º 128, 130..140, 142, 145..156, 158..159, 161..172**
  € , ƒ „ … † ‡ ˆ ‰ Š ‹ Œ Ž ‘ ’ “ ” • – — ˜ ™ š › œ ž Ÿ ¡ ¢ £ ¤ ¥ ¦ § ¨ © ª « ¬
- **N.º 174..255**
  ® ¯ ° ± ² ³ ´ µ ¸ ¹ º » ¼ ½ ¾ ¿ À Á Â Ã Ä Å Æ Ç È É Ê Ë Ì Í Î Ï Ð Ñ Ò Ó Ô Õ Ö × Ø Ù Ú Û Ü Ý Þ ß à á â ã ä å æ ç è é ê ë ì í î ï ð ñ ò ó ô õ ö ÷ ø ù ú û ü ý þ ÿ

Indicadores de error

En las tablas los puntos de conexión, redes o parámetros defectuosos se marcan sobre fondo rojo.

Las conexiones defectuosas pueden deberse, por ejemplo, a las siguientes causas:

- Los puntos de inicio y final son idénticos.
- La conexión se desarrolla a través de una red no permitida.
- La conexión se desarrolla a través de un dispositivo no permitido.

Borrar conexiones no válidas o redundantes

Si existen conexiones no válidas o redundantes no deseadas es necesario borrar una vía de conexión:

1. Seleccione la vía de conexión no deseada en la tabla "Vías de conexión configuradas".
2. Haga clic en el menú contextual "Borrar".

4.22.3 Definir vías de conexión

Reglas para la configuración de conexiones

Observe las siguientes reglas para la configuración de conexiones:

- Las conexiones de Telecontrol pueden configurarse para las siguientes redes y los siguientes tipos de módulo:
  - Conexiones en redes Ethernet
    Configurables entre módulos TIM, CP y dispositivos de terceros
  - Conexiones en redes WAN clásicas (línea dedicada/red de marcación)
    Configurables entre dos módulos TIM 1531 IRC y entre TIM 1531 IRC y dispositivo de terceros
- Es posible crear conexiones entre puntos finales (dispositivos) configurados en el proyecto STEP 7.
  Para los datos de dirección y los parámetros de interfaz de ambos puntos finales se dispone de campos en la tabla de conexiones.
- Es posible crear conexiones entre un punto final del proyecto STEP 7 y un "dispositivo de terceros" que no esté configurado en STEP 7, por ejemplo, el maestro de otro fabricante. Si el dispositivo de terceros se encuentra en una subred IP distinta y es accesible por una transición de red, la transición de red se configura como punto final de la conexión.
  Un dispositivo de terceros en una red WAN clásica también puede conectarse utilizando la interfaz serie del TIM 1531 IRC.
- El punto final de una conexión es siempre la CPU, una aplicación PC (no el módulo de comunicación) o un dispositivo de terceros.
- Para cada conexión con un interlocutor interno del proyecto (no un dispositivo de terceros) debe haberse creado una sección de conexión para el recorrido de ida y otra para el de vuelta. Ejemplo de conexión entre los interlocutores 1 (maestro) y 2 (estación):
  - Recorrido de ida: Sección de conexión 1 ⇒ 2
  - Recorrido de vuelta: Sección de conexión 2 ⇒ 1

  Cuando se configura el recorrido de ida se crea automáticamente el recorrido de vuelta.
- Entre dos dispositivos pueden configurarse conexiones simples y redundantes.
- No están permitidas dos conexiones a un interlocutor a través de la misma interfaz de un módulo.
- Una conexión que pasa por una red incoherente no es válida.

Ejemplos de redes incoherentes:

- Un dispositivo de una sección de conexión está configurado con otro protocolo de Telecontrol.
- Conexiones a través de nodos que no están configurados como estación nodo.
- Dispositivos con módems incompatibles
- Ajustes incompatibles de dos módems en una conexión
- Ajustes incompatibles entre parámetros de módem y red

Configurar específicamente para cada interfaz las secciones de conexión

Las conexiones entre dos puntos finales pueden transcurrir a través de varios dispositivos.

Una sección de conexión entre dos dispositivos puede utilizarse para varias conexiones.

Para determinadas secciones de conexión y las interfaces relacionadas de los módulos existe la posibilidad de configurar ajustes individuales. Por este motivo, en la tabla de conexiones las diferentes secciones de conexión entre las interfaces de dos dispositivos se muestran en filas independientes.

	Conexión	Punto de in..	Dispositiv...	Interfaz inicial	Punto final	Disp...	Lista de int..	Interfaz final/dirección
	*	*	*		*	*		
	Section_1	1	1	TIM_1 - Interfaz Et..	2	2	2,3	TIM_2 - TIM_2 - Interfaz Et
	Section_2	2	2	TIM_2 - Interfaz Et..	1	1	2,3	TIM_1 - TIM_1 - Interfaz Et
	Section_3	TIM_2	2	TIM_2 - Serial Inter.	3	3	1	TIM_3 - TIM_3 - Serial Inte
	Section_4	3	3	TIM_3 - Serial Inter.	1	1	1	TIM_2 - TIM_2 - Serial Inte
	Section_5	TIM_2	2	TIM_2 - Interfaz Et..	1	1	3, 12	TIM_1 - TIM_1 - Interfaz Et
	Section_6	2	2	TIM_2 - Serial Inter.	3	3	3	TIM_3 - TIM_3 - Serial Inte
	Section_7	3	3	TIM_3 - Serial Inter.	2	2	2	TIM_2 - TIM_2 - Serial Inte
	Section_99	1	1	TIM_1 - Interfaz Et..	Dispositivo de terce.	99	99	192.168.2.99
	Section_8	1	1	TIM_1 - Interfaz Et..	1200	12	12	TIM_2 - TIM_2 - Interfaz Et
	Section_9	TIM_2	2	TIM_2 - Interfaz Et..	1200	12	1	S7-1200-Station_1 - CP 1..
	Section_10	1200	12	CP 1243-8 IRC - Int.	1	1	1	TIM_2 - TIM_2 - Interfaz Et

Figura 4-13 Editor "Datos de red", ficha "Telecontrol > ..."

Símbolos de conexión

Los símbolos de conexión que se muestran en las filas de la tabla y en la ventana de la búsqueda de conexiones tienen el significado que se indica a continuación:

	• Vía de conexión principal (recorrido de ida), partiendo del punto de inicio de la conexión.
	• Vía de conexión parcial (recorrido de vuelta de una vía de conexión principal) • Conexión simple, p. ej. con un dispositivo de terceros.

Creación de conexiones y búsqueda de las vías de conexión

Para crear conexiones, proceda del siguiente modo:

1. Haga clic en el campo "Punto de inicio" de la primera fila libre.
   Se muestra una lista desplegable con los puntos finales disponibles.
   La primera fila que aparece debajo del encabezado de la tabla está reservada para entrar filtros; consulte el capítulo Tabla de conexiones (Página 121).
2. Seleccione el punto de inicio (CPU) en la tabla haciendo doble clic.
3. Haga clic en el campo "Punto final" de la misma fila.
   Seleccione el punto final (CPU o la aplicación PC) en la tabla haciendo doble clic.
   - Caso especial "dispositivo de terceros":
     Si en lugar de un punto final del proyecto STEP 7 desea crear un dispositivo de terceros como punto final, deje la entrada predeterminada "Dispositivo de terceros" de la celda tal como está.
     Configure la interfaz del punto de inicio, así como los datos de dirección y otros parámetros del dispositivo de terceros introduciendo los datos en los campos correspondientes.
     Si un dispositivo de terceros es un punto final, la búsqueda de conexiones mediante el cuadro de diálogo, que se describe a continuación, está desactivada.

   Tras seleccionar un punto final del proyecto STEP 7 se muestran en la fila de la tabla el punto de inicio y el punto final. Los demás campos suelen estar vacíos y tener el fondo rojo.
   Después de crear una conexión no siempre está especificado el recorrido real de la conexión. Especialmente en redes grandes a menudo hay varias vías de conexión posibles.
   Para buscar la vía de conexión haga clic en el símbolo "Agregar nueva vía de conexión".
   

4. Deje seleccionada la fila de la tabla con los puntos de inicio y fin seleccionados y haga clic en el símbolo "Agregar nueva vía de conexión".
   Se abre el cuadro de diálogo para definir las vías de conexión:
   Cuadro de diálogo "Agregar vías de conexión"
   Se buscan automáticamente las vías de conexión posibles, y el progreso de la búsqueda se muestra en la barra de progreso que aparece en la parte inferior del cuadro de diálogo.
   - El estado y el resultado de la búsqueda se muestran en el campo "Información".
   - Las vías de conexión encontradas se muestran en la tabla superior "Seleccione una vía de conexión ...".
   - Los detalles de una vía de conexión seleccionada se muestran en la tabla "Vía de conexión".
   - Al seleccionar una vía de conexión, haciendo clic en "Agregar", en la tabla "Vista preliminar" se muestran los puntos de conexión de la vía de conexión seleccionada que se han aplicado en el editor de conexiones.
5. Seleccione la vía o las vías de conexión deseadas.
   - Cuando en la tabla superior se muestre una o varias vías de conexión, seleccione la vía de conexión deseada y haga clic en "Agregar".
     En "Información" se indica si se ha agregado la vía de conexión o si ya está configurada.
   - Si se desea utilizar una vía de conexión redundante, hay que marcar en la tabla una segunda vía y hacer clic en "Agregar".
     Cierre el cuadro de diálogo con el botón "Cerrar" si las vías de conexión agregadas coinciden con las especificaciones del proyecto.
   - Si en la tabla no se muestra ninguna conexión, existe un error de configuración en las estaciones o redes correspondientes.
     En ese caso, cierre el cuadro de diálogo con el botón "Cerrar" y complete la configuración.

La tabla "Vía de conexión" le ayuda a comprobar las vías de conexión. En ella, para cada conexión configurada se muestra detallada la vía de conexión.

En la columna "Posición" se muestra un símbolo de estación con un identificador para el punto de conexión. El color del identificador indica la validez del punto de conexión:

- Azul: punto de conexión válido
- Rojo: punto de conexión no válido

Símbolo	Significado
	Punto de inicio
	Nodo-entrada
	Nodo-salida
	Punto final
	Ejemplos de puntos de conexión no válidos

Parámetros de la tabla de conexiones

Configure los parámetros de la tabla de conexiones para cada sección de conexión. Encontrará la descripción de los parámetros en el capítulo Tabla de conexiones (Página 121).

En la ventana de inspección, debajo de la tabla de conexiones hay la ficha "Propiedades", en la que se muestran otros parámetros de cada sección de conexión.

Ficha "Propiedades" de las conexiones

En los grupos de parámetros es posible comprobar y, en caso necesario, corregir cada sección de conexión, además de configurar otras propiedades.

Encontrará la descripción de los grupos de parámetros en el capítulo Propiedades de las conexiones IEC (Página 124).

4.22.4 Tabla de conexiones

Filtros

La primera fila situada debajo del encabezado de la tabla contiene una función de filtro que permite limitar la selección de los dispositivos configurables y las posibilidades de conexión. De este modo se reducen las combinaciones posibles y aumenta la claridad.

Si se han creado algunas secciones de conexión, active el filtro tecleando un nombre o parte de un nombre repetitivo en la celda de filtro. La celda se marca en color; véase la figura.

	Conexión	Punto de in..	Dispositiv...	Interfaz inicial	Punto final	Disp...	Lista de int..
	*	1	*		*	*	
	Section_1	1	1	TIM_1 - Interfaz Ethernet .	2	2	2,3
	Section_99	1	1	TIM_1 - Interfaz Ethernet .	Dispositivo de terce.	99	99
	Section_8	1	1	TIM_1 - Interfaz Ethernet .	1200	12	12
	Section_10	1200	12	CP 1243-8 IRC - Interf..	1	1	1

Figura 4-14 Tabla de conexiones

En la columna "Punto de inicio" está ajustado el filtro "1".

Ejemplo:
Se han creado conexiones con los puntos de inicio "1200", "1" y "2".
Si se introduce "1" en la celda de filtro, en la tabla solo se muestran las secciones cuyos puntos de inicio empiezan por dicha cadena de caracteres: "1" y "1200".

Los filtros aplicados a varias columnas se multiplican.

La selección "*****" muestra todas las secciones de conexión existentes.

El símbolo de filtrado a la izquierda de la primera fila ( ) muestra u oculta un filtro existente.

El filtro puede aplicarse a todas las columnas cuya primera fila empieza por un asterisco (*****).

Recuerde:
Una vez haya creado conexiones y activado un filtro, no podrá crear conexiones nuevas. Para crear conexiones nuevas deberá desactivar primero el filtro.

Parámetros

Si los parámetros ya están asignados en la configuración, los valores se aplican en las columnas correspondientes.

- **Nombre**
  Es posible adaptar el nombre predeterminado de la sección de conexión entre dos dispositivos.
  Consulte a este respecto el capítulo Editor "Datos de red" (Página 115).
- **Punto de inicio**
  Seleccione en la lista desplegable el punto de inicio deseado de la conexión.
  - El punto de inicio de una conexión es siempre una CPU.
- **Dispositivo inicial**
  Dirección de estación del punto de inicio
- **Interfaz inicial**
  Interfaz del módulo del punto de inicio a través de la que transcurre la conexión.
- **Punto final**
  Seleccione el punto final de la conexión.
  Pueden ser puntos finales de la conexión:
  - una CPU
  - un dispositivo de terceros
    El tipo de nodo de red de dispositivos de terceros se configura en el cuadro de diálogo de propiedades de la conexión; consulte el capítulo Parámetros de dispositivos de terceros (Página 132).

Nota

Modificar el punto final

Si el punto final de una conexión se modifica a posteriori, al buscar la vía de conexión se agregarán las nuevas secciones de conexión.

Tenga en cuenta que las secciones de la conexión anterior se conservan. Deben borrarse manualmente.

- **Dispositivo final**
  Dirección de estación del punto final
- **Lista de interlocutores**
  Al seleccionar un interlocutor (punto final) que se encuentra en el proyecto STEP 7, su dirección de estación se detecta automáticamente durante la búsqueda de conexiones y se registra en la lista de interlocutores.
  En secciones de conexión que se utilizan para varias conexiones se registran las direcciones de estación de todos los dispositivos de destino.

Nota

Entrada manual para un dispositivo de terceros

En un dispositivo de terceros que no está configurado en el proyecto de STEP 7, la dirección de estación debe introducirse manualmente.

Las direcciones de estación se introducen separadas por comas.

- **Interfaz final/dirección**
  Interfaz del módulo del punto final a través de la que transcurre la conexión.
  En un dispositivo de terceros que no está configurado en el proyecto de STEP 7, la dirección IP (Ethernet) debe introducirse manualmente.
  Para dispositivos de terceros en redes en serie, introduzca la dirección ASDU del dispositivo de terceros.

- **Puerto final**
  Relevante para dispositivo de terceros (maestro / estación)
  Número del puerto Listener del interlocutor
  En módulos del proyecto STEP 7 el valor se aplica de la configuración. Puede modificarse.
  Con dispositivos de terceros es necesario introducir el número de puerto.
  Rango de valores: 0 ... 65535
  Ajuste predeterminado: 2404

- **Tiempo de vigilancia del interlocutor**
  Relevante para todos los tipos de dispositivo
  Si el módulo de la estación no recibe ninguna señal de vida del maestro a nivel de aplicación dentro del tiempo configurado, clasifica la conexión como fallida y deshace la conexión.
  Tras el envío de datos, el módulo maestro espera durante el tiempo configurado una respuesta de la estación.

  Nota

  Vías de conexión redundantes

  Si se configuran vías de conexión redundantes entre dos interlocutores, debe configurarse el mismo tiempo para ambas vías.

  Rango de valores: 0 ... 65535
  Con el valor 0 (cero) la función está desactivada.

- **Modo de sondeo**
  Relevante para maestro, dispositivo de terceros (maestro)
  Aquí se define el modo con el que la central llama la estación.
  El valor configurado en la estación se transmite a la central, donde se guarda.
  Rangos de valores:

  – Cíclico
    La estación se llama cíclicamente. La duración del ciclo de sondeo se calcula a partir del parámetro "Intervalo de sondeo de clase 0"; consulte más arriba.

  – Tras arranque
    La estación se consulta solo después del primer arranque y tras un rearranque completo. Si un punto de datos no está configurado como evento, con esta opción no se transfieren datos durante el funcionamiento.
    En una sección de conexión de la estación al maestro (recorrido de vuelta), el ajuste es fijo en "Tras arranque". La transferencia durante el funcionamiento se especifica mediante el ajuste en el recorrido de ida (sección de maestro a estación).

- **Temporal**
  Los interlocutores con la opción "Temporal" activada se clasifican como "accesibles" si deshacen la conexión por sí mismos (p. ej. RTU3000C).

Parámetros para vías de conexión redundantes

En el caso de que haya configuradas vías de conexión redundantes, estas se configuran igual que las vías principales.

Los parámetros de las vías de conexión redundantes se distinguen mediante el sufijo siguiente:

- *** (red)**

Los parámetros de las vías de conexión redundantes tienen correspondientemente las mismas funciones que la vía principal. Consulte el significado más arriba.

Ejemplos:

- **Interfaz inicial (red.)**
  Interfaz del módulo del punto de inicio a través de la que transcurre la conexión redundante.
- **Interfaz final (red.)**
  Interfaz del módulo del punto final a través de la que transcurre la conexión redundante.

4.22.5 Propiedades de las conexiones IEC

4.22.5.1 General

Si en la tabla "Conexiones de Telecontrol" del editor "Datos de red" se selecciona una conexión, en la ficha "Propiedades" de la ventana de inspección se mostrarán otros grupos de parámetros de esa conexión.

En los grupos de parámetros es posible comprobar y, en caso necesario, corregir la conexión, además de configurar otras propiedades.

General

- **Conexión**
  Indica el nombre de la conexión y el protocolo.
  El nombre de la conexión también puede modificarse aquí.
- **Puntos finales de la conexión**
  Muestra los principales parámetros de la conexión.
  La dirección de estación de un dispositivo de terceros también puede modificarse aquí.

4.22.5.2 Vigilancia de conexión TCP

Interfaz Ethernet > Opciones avanzadas > Vigilancia de conexión TCP

Los ajustes de los dos parámetros en la interfaz Ethernet se aplican para todas las conexiones TCP a través de esta interfaz.

En los CP de telefonía móvil, la interfaz Ethernet es un comodín para la interfaz de telefonía móvil.

Los parámetros pueden adaptarse para cada sección de conexión en las propiedades de las conexiones de Telecontrol. El valor situado debajo de la sección de conexión es válido para dicha sección de conexión y sobrescribe el valor configurado en la interfaz.

Si hay valores distintos en la interfaz y en la sección de conexión, asegúrese de que el valor que hay en la interfaz sea mayor que el valor que hay en la sección de conexión.

- **Tiempo de supervisión de conexión TCP**
  Función: Si dentro del tiempo de vigilancia de conexión TCP no hay tráfico de datos, el módulo de comunicación envía un telegrama Keep Alive al interlocutor y espera su respuesta dentro del tiempo de vigilancia TCP Keep Alive.
  Ajuste predeterminado: 180 s
  Con cero (0) la vigilancia está desactivada.
  El rango admisible depende del tipo de módulo.
- **Tiempo de vigilancia TCP Keep Alive**
  Tras enviar un telegrama Keep Alive, el módulo espera una respuesta del interlocutor dentro del timeout de Keep Alive. Si el módulo no recibe ninguna respuesta tras tres telegramas Keep Alive, deshace la conexión.
  Con el valor 0 (cero) la función está desactivada.
  Ajuste predeterminado: 10 s
  El rango admisible depende del tipo de módulo.
  Si en una red de telefonía móvil se producen con frecuencia perturbaciones o retardos en la transmisión, es aconsejable aumentar el valor a 30 o 60 segundos, por ejemplo.

Si hay valores distintos en la interfaz y en la sección de conexión, asegúrese de que el valor que hay en la interfaz sea mayor que el valor que hay en la sección de conexión.

Si se ha configurado una conexión redundante con un interlocutor, los parámetros de las dos vías de conexión pueden ajustarse por separado.

4.22.5.3 Opciones de seguridad IEC 60870-5

Nota

Recuerde que la velocidad de transferencia se reduce en conexiones cifradas o protegidas por TLS.

Secure Authentication

Los ajustes del grupo de parámetros se llevan a cabo en el recorrido de ida de la conexión. Los ajustes se aplican a toda la sección de conexión y se transfieren también a las subsecciones.

Los ajustes realizados para la ida se aplican automáticamente para la vuelta. Allí se representan atenuados.

Si la opción está desactivada, los módulos solo se autentican con su dirección de estación ante el interlocutor (no protegido).

Si la opción está activada, los módulos utilizan el método "Secure Authentication" según IEC/TS 60870-5-7. El maestro IEC y la estación se autentican con una clave secreta, la Preshared Key.

Con la Preshared Key común, tras el primer establecimiento de conexión entre el maestro y la estación se acuerdan claves de sesión, que se renuevan cíclicamente a partir de entonces. La iniciativa para renovar la clave de sesión la toma el maestro. Los criterios para renovar las claves se definen en los parámetros siguientes.

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

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

Parámetros

- **Activar opciones de seguridad IEC**
  Active esta opción para poder utilizar Secure Authentication.
  Nota:
  Asegúrese de activar la opción en todas las conexiones del módulo que deben utilizar esta función.
- **Estadísticas de seguridad**
  Indica si se envían al maestro las estadísticas de los eventos de seguridad. Los eventos de seguridad son solicitudes de autenticación del maestro para el módulo de estación. Si se activa esta opción, todas las solicitudes de autenticación se guardarán en el módulo de estación con fecha, hora y resultado y se enviarán al maestro para su posterior evaluación. Los eventos de estadísticas de seguridad solo se emiten si hay un sistema SCADA conectado al maestro.
  Rango de valores:
  - No enviar estadísticas de seguridad
  - Enviar estadísticas de seguridad
    Si la opción está activada, los parámetros de estadística seleccionables situados debajo de la tabla se habilitarán para su configuración.

  Ajuste predeterminado: No enviar estadísticas de seguridad
- **Algoritmo Secure Hash (SHA)**
  Selección del Secure Hash Algorithm (SHA)
  Rango de valores:
  - SHA-256
- **Longitud de clave**
  Indica la longitud de la Pre-shared Key en bytes.
  Se utiliza la siguiente longitud:
  - 32 bytes (equivale a 64 caracteres para la Preshared Key)
- **Número máx. de solicitudes de estado de clave**
  Si se rebasa por exceso el número configurado aquí para solicitudes de estado de clave de un maestro dentro del intervalo de cambio de clave, el módulo avisa a todas las demás estaciones maestro conectadas. La estación maestro que ha planteado la solicitud no recibe el aviso.
  el módulo registra un aviso en el búfer de diagnóstico de la CPU.
  Rango de valores: 2...255. Ajuste predeterminado: 5

- **Solicitudes de autenticación previas al cambio de clave**
  Número máximo de solicitudes de autenticación del módulo al maestro. Cuando se alcanza este número se renueva la clave de sesión.
  Rango de valores: 1...10000. Ajuste predeterminado: 1000
  Recomendación: En el módulo de estación, ajuste un número que sea el doble de grande que el del maestro.
- **Intervalo de cambio de clave**
  Periodo tras el cual volverá a intercambiarse la clave entre el módulo de estación y el maestro. El intervalo debe sintonizarse en ambos interlocutores.
  Rango de valores: 0...65535 min. Con 0 (cero) no se cambia nunca la clave (función desactivada). Ajuste predeterminado: 15 min.
  Recomendación: Ajuste un intervalo de cambio de clave en el módulo de estación que sea el doble de grande que el del maestro.
- **Timeout de autenticación**
  Tiempo de espera máximo del módulo tras una solicitud de autenticación al maestro. Si se rebasa el tiempo de espera a la respuesta del maestro, el módulo genera un evento de seguridad y lo envía al maestro.
  Rango de valores: 1... 65535 s. Ajuste predeterminado: 5
- **Longitud de datos para el desafío de estado de clave y autenticación**
  Longitud de datos (CLN) de un Challenge de autenticación o de un Challenge de estado de clave de sesión
  Rango de valores: 1... 65535 s. Ajuste predeterminado: 4
- **Número máx. de errores de autenticación**
  Número máximo de errores de autenticación antes de que el Challenger envíe un mensaje de error y se modifique la clave de sesión.
  Rango de valores: 1... 65535 s. Ajuste predeterminado: 25
- **Número máx. de telegramas de error enviados**
  Número máximo de mensajes de error enviados. Cuando se alcanza el número configurado, la estación deja de enviar mensajes de error.
  Rango de valores: 1... 65535 s. Ajuste predeterminado: 100
- **Número máx. de cambios de clave**
  Número máximo de cambios de clave de sesión debidos a errores de autenticación. Cuando se alcanza el número configurado, los cambios de clave de sesión debidos a errores de autenticación dejan de producirse hasta que la clave de sesión se modifica por otro motivo.
  Rango de valores: 1... 65535 s. Ajuste predeterminado: 50
- **Número máx. de timeouts de respuesta**
  En el maestro: número máximo de timeouts de respuesta
  Cuando se alcanza el valor configurado, el maestro cancela la acción actual.
  Rango de valores: 1... 65535 s. Ajuste predeterminado: 20

- **Número máx. de cambios de clave debido a rearranque**
  En el maestro: número máximo de cambios de clave debidos a rearranque de la estación Cuando se alcanza el valor configurado, el maestro deja de enviar claves de sesión a la estación hasta que se produce el próximo timeout de cambio de clave.
  Rango de valores: 1... 65535 s. Ajuste predeterminado: 20
- **Pre-shared Key**
  La Pre-shared Key puede configurarse de dos formas:
  - Configuración manual
    Introduzca manualmente la Pre-shared Key en STEP 7 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. Un archivo de texto con codificación ANSI es adecuado, por ejemplo.

  La Preshared Key de un módulo de estación debe ser idéntica a la Preshared Key del maestro. Consulte el formato más arriba, parámetro "Longitud de clave".

Estadísticas de seguridad (IEC 60870-5-104)

Los parámetros de estadística se habilitan para su configuración cuando se activa la opción "Enviar estadísticas de seguridad" de las Opciones básicas de seguridad.

La tabla siguiente contiene las opciones de estadísticas de seguridad conforme a IEC/TS 60870-5-7 e IEC/TS 62351-5 que pueden configurarse para las diferentes secciones de conexión de Telecontrol.

Si las opciones están activadas, el módulo de comunicación envía eventos de estadísticas de seguridad al maestro en calidad de estación. Allí están disponibles para su evaluación. En función de la frecuencia de estos eventos puede sacar conclusiones sobre posibles intervenciones o puntos débiles del sistema.

Los eventos de estadísticas de seguridad solo se emiten si hay un sistema SCADA conectado al maestro.

Opciones de estadísticas de seguridad

Si se utiliza Secure Authentication, una estación lleva a cabo una estadística para diferentes valores.

Los eventos se transfieren mediante el tipo de ASDU "Information 41" (integrated total for the statistic).

La tabla siguiente presenta los parámetros de estadística que soporta el módulo conforme a IEC/TS 62351-5.

- Valor umbral
  Para cada valor estadístico es posible configurar un valor umbral que, si se sobrepasa, provoca la transferencia como evento al interlocutor.
  El rango de valores es de 0...65535 en cada caso.
  Con el valor 0 (cero) la función está desactivada y para el valor en cuestión no se transfieren datos estadísticos.
- IOA
  A cada valor de la estadística hay que asignarle una dirección IOA (IOA - Information object address) en la configuración.
  El rango de valores es de 0...16777215 en cada caso.

Para los telegramas críticos es posible configurar debajo de la tabla qué tipos de ASDU deben clasificarse como críticos.

Parámetro	**Ajuste predeterminado**
Valor umbral de telegramas imprevistos	3
Telegramas imprevistos (IOA)	0
Valor umbral de errores de autorización	5
Errores de autorización (IOA)	0
Errores de autorización (IOA)	5
Errores de autenticación (IOA)	0
Valor umbral de timeouts de respuesta	3
Timeouts de respuesta (IOA)	0
Valor umbral de cambios de clave debido a errores de autenticación	3
Cambios de clave debido a errores de autenticación (IOA)	0
Valor umbral de telegramas enviados (total)	100
Número total de telegramas enviados (IOA)	0
Valor umbral de telegramas recibidos (total)	100
Número total de telegramas recibidos (IOA)	0
Valor umbral de telegramas críticos enviados	100
Telegramas críticos enviados (IOA)	0
Valor umbral de telegramas críticos recibidos	100
Telegramas críticos recibidos (IOA)	0
Valor umbral de telegramas rechazados	10
Telegramas rechazados (IOA)	0
Valor umbral de telegramas de error enviados	10
Telegramas de error enviados (IOA)	0
Valor umbral de telegramas de error recibidos	10
Telegramas de error recibidos (IOA)	0
Valor umbral de autenticaciones correctas	100
Valor umbral de autenticaciones correctas	0
Valor umbral de cambios de clave de sesión	10
Cambios de clave de sesión (IOA)	0

Parámetro	Ajuste predeterminado
Valor umbral de cambios erróneos de clave de sesión	5
Cambios erróneos de clave de sesión (IOA)	0

4.22.5.4 Comunicación segura (TLS)

Configuración de conexiones TLS seguras

La opción "Activar comunicación segura" permite configurar una comunicación segura vía TLS entre interlocutores de Telecontrol del proyecto de STEP 7. En caso de utilizar el protocolo DNP3 también es posible la conexión con un dispositivo de terceros por medio de TLS.

En el grupo de parámetros anterior, configure los ajustes para la sección de conexión principal.

El segundo grupo de parámetros para la sección de conexión de repuesto puede editarse si se ha creado una conexión redundante.

Parámetros:

- Activar comunicación segura
  Activa la comunicación segura vía TLS para esta sección de conexión
- ID de certificado de interlocutor
  Identificador del certificado del interlocutor de la comunicación
  Para generar y gestionar los certificados consulte el capítulo TIM 1531 IRC: Certificado TLS de la CPU (Página 92).
- ID de certificado propio
  Identificador del certificado propio del módulo
- Puerto del interlocutor
  Puerto del interlocutor para comunicación segura
  (para el puerto propio consulte el grupo de parámetros "Ajustes básicos" del módulo > "Puerto Listener seguro")
- Intervalo de cambio de clave
  Periodo tras el cual volverá a intercambiarse la clave entre el módulo de estación y el maestro. El intervalo debe sintonizarse en ambos interlocutores.
  Rango de valores: 0...65535 minutos
  Con el valor 0 (cero) no se intercambia nunca la clave (función desactivada).
- Cambio de clave
  Número máximo de solicitudes de autenticación del módulo al maestro antes de que se renueve la clave de sesión.
  Rango de valores: 1...10000
  Ajuste predeterminado: 1000
- Timeout de autenticación
  Tiempo de espera máximo del módulo tras una solicitud de autenticación al maestro
  Cuando se alcanza el tiempo de espera a la respuesta del maestro, el módulo genera un evento de seguridad y lo envía al maestro.
  Rango de valores: 1...65535 s
  Ajuste predeterminado: 5

4.22.5.5 Opciones de consulta

Los siguientes parámetros se encuentran en los grupos de parámetros "Opciones 1ª vía" / "Opciones 2ª vía" de las conexiones IEC

Intervalos de llamada

Los siguientes parámetros establecen los intervalos de llamadas especiales del maestro para la estación (cause of transmission 20 - 41).

Todos los parámetros se configuran como múltiplo del "Intervalo básico de sondeo"; consulte el capítulo Ajustes de maestro IEC (Página 73).

- **Intervalo para consulta general**
  Define el intervalo con el que se responden las consultas generales del maestro.
- **Intervalo para consulta de grupo**
  Define el intervalo con el que se responde la consulta de grupo concreta del maestro.
- **Intervalo para consulta general de contador**
  Define el intervalo con el que se responden las consultas generales de contador del maestro.
- **Intervalo para consulta de grupo de contador**
  Define el intervalo con el que se responde la consulta de grupo de contador concreta del maestro.

El ajuste de si una consulta general se responde y la asignación a una consulta de grupo se definen en la configuración de puntos de datos individualmente para cada punto de datos.

4.22.5.6 Parámetros de dispositivos de terceros

Parámetros de dispositivos de terceros

Sólo válidos para interlocutores que no se configuran en el proyecto STEP 7. El grupo de parámetros solo es visible si se configura un dispositivo de terceros como interlocutor de la conexión. Estos interlocutores se crean como "Dispositivo de terceros" con el parámetro "Punto final" en la tabla de conexiones.

- **Dirección de estación de interlocutor /**
  Dirección de estación (red.)
  Dirección de estación (dirección ASDU) del dispositivo de terceros al que puede accederse a través de una conexión o a través de una vía de conexión redundante.
- **Tipo de nodo de red dispositivo de terceros /**
  Tipo de nodo de red dispositivo de terceros (red.)
  Defina el tipo de nodo de red del dispositivo de terceros al que puede accederse a través de una conexión o a través de una vía de conexión redundante:
  - Estación central
    (maestro)
    Si el dispositivo de terceros es el maestro, hay que configurar el tipo de nodo de red del dispositivo de terceros como "Estación central".
  - Estación nodo
    Para módulos que actúan de estación nodo rige lo siguiente:
    La interfaz que se dirige a la central se configura como "estación nodo".
    La interfaz que se dirige a la red subordinada se configura como "central".
  - Estación

4.23 Puntos de datos

4.23.1 Configuración de puntos de datos

Comunicación de puntos de datos con la CPU

La transferencia de datos útiles entre la estación y el interlocutor en módulos de Telecontrol con configuración de puntos de datos no requiere la creación de bloques de programa.

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

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

El requisito para la configuración de los puntos de datos es que las variables PLC o los DB correspondientes se hayan creado en la CPU.

⚠ ADVERTENCIA

Escribir valores en salidas

- Variables PLC
  A la hora de referenciar variables PLC, tenga en cuenta que con un acceso de escritura los valores es escriben inmediatamente en las salidas de la CPU sin que el programa de usuario los procese previamente.
  La escritura de valores influye de forma directa en el proceso.
- Variables DB
  A la hora de referenciar variables DB, los valores escritos no se utilizan hasta que los ha procesado el programa de usuario.

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

Las áreas de direcciones de las variables PLC son las áreas de entrada, de salida o de marcas en la CPU.

Nota

Número de variables PLC

Tenga en cuenta el número máximo admisible de variables PLC que pueden utilizarse para la configuración de puntos de datos.

Encontrará los formatos y tipos de datos S7 de las variables PLC compatibles con los tipos de puntos de datos de los módulos en el capítulo Tipos de puntos de datos (Página 142).

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 módulo.

El módulo escribe los datos recibidos por el interlocutor en la CPU mediante las variables PLC o los DB.

Configuración de los puntos de datos y mensajes en STEP 7

Los puntos de datos se configuran en el editor de puntos de datos y mensajes de STEP 7. Los dos editores pueden abrirse alternativamente mediante:

- Selección del módulo de comunicación
  Menú contextual "Abrir el editor de puntos de datos y mensajes"
- Desde el árbol del proyecto:
  Proyecto > Directorio de la estación correspondiente > Módulos locales > Módulo de comunicación deseado
  Haciendo doble clic en la entrada se abre el editor de puntos de datos y mensajes.

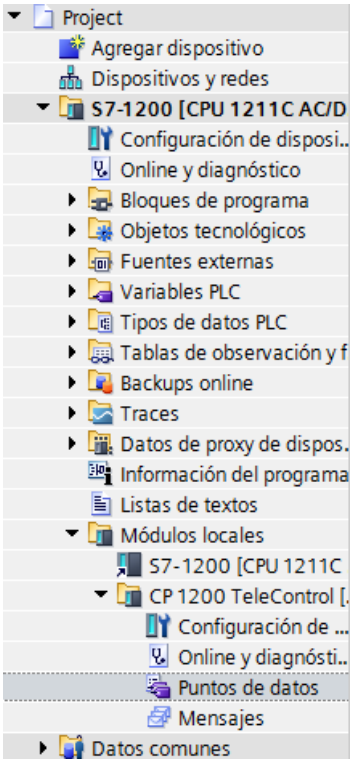


Figura 4-15 Configuración de puntos de datos y mensajes

Después de abrir la ventana del editor, puede cambiar entre el editor de puntos de datos y mensajes utilizando las dos entradas situadas a la derecha encima de la tabla.

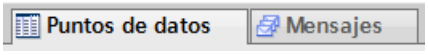


Figura 4-16 Cambiar entre los dos editores

Creación de objetos

Con el editor de puntos de datos y mensajes abierto se crea un objeto nuevo (punto de datos / mensaje) haciendo doble clic en la primera fila de la tabla con la entrada "<Agregar objeto>" atenuada.

En la celda se escribe un nombre predeterminado. Es posible adaptar el nombre según las necesidades, aunque debe ser unívoco dentro del módulo.

		Nombre	Variable PLC
1		DataPoint	"Tag_1-BI"
2		DataPoint_1	"Tag_2-BQ"
3		DataPoint_2	"Tag_1-BI"

Figura 4-17 Tabla de puntos de datos

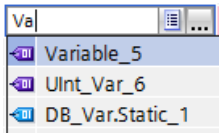
El resto de propiedades de cada objeto se configura mediante las listas desplegables del resto de columnas de la tabla y mediante los campos de parámetros mostrados.

Asignar puntos de datos a su origen

Un punto de datos nuevo debe asignarse a su origen. Dependiendo del tipo de datos del punto de datos debe considerarse como origen de los datos una variable PLC.

Existen las siguientes posibilidades para la asignación:

- Haga clic en el símbolo de la tabla en la celda de la columna "PLC-Tag".
  Se muestran todas las variables PLC configuradas y las variables de los bloques de datos creados. Seleccione con el ratón o con el teclado el origen de datos deseado.
- Haga clic en el símbolo ...
  Se muestra una lista desplegable de las variables PLC configuradas y de los bloques. Seleccione en la tabla correspondiente el origen de datos deseado.
- Introduzca en el campo de nombre de la variable PLC una parte del nombre del origen de datos deseado.
  Se muestran todas las variables y variables PLC configuradas de los bloques de datos cuyo nombre contienen las letras introducidas.



Seleccione el origen de datos deseado.

Nota

Asignación de valores de parámetro a variables PLC

Los mecanismos descritos aquí también son válidos para asignar el valor de un parámetro a una variable PLC. Los campos de entrada para la variable PLC (p. ej.: Variable PLC para estado de interlocutor) soportan las funciones descritas aquí para la selección de la variable PLC.

Organizar columnas y filas, mostrar/ocultar columnas

Igual que en muchos otros programas, en el editor de punto de datos o de mensajes es posible organizar las columnas y clasificar la tabla según las necesidades de cada caso:

- Organizar columnas
  Si se hace clic en el encabezado de la columna con el botón izquierdo del ratón es posible desplazar la columna.
- Clasificar objetos
  Si se hace clic brevemente con el botón izquierdo del ratón en el encabezado de la columna es posible clasificar los objetos de la tabla en orden ascendente o descendente en función de las entradas de dicha columna. La clasificación se visualiza mediante una flecha en el encabezado de la columna.
  Después de clasificar en orden descendente una columna es posible deshacer la clasificación haciendo de nuevo clic en el encabezado de la columna.
- Adaptar el ancho de la columna
  A esta función se accede a través de las siguientes acciones:
  - Desde el menú contextual, que se abre haciendo clic con el botón derecho del ratón en el encabezado de una columna:
    "Optimizar ancho", "Optimizar ancho de todas las columnas"
  - Si coloca el cursor cerca del límite derecho del encabezado de una columna, aparece el símbolo siguiente:

    Haga doble clic en ese momento en el encabezado de la columna. El ancho de la columna se adapta entonces a la entrada más ancha de la columna.
- Mostrar/ocultar columnas
  Se accede a esta función desde el menú contextual, que se abre haciendo clic con el botón derecho del ratón en el encabezado de una columna.

Copiar puntos de datos y mensajes

Igual que en muchos otros programas, en el editor de punto de datos o de mensajes también es posible copiar e insertar objetos.

Si se hace clic con el botón derecho del ratón en la fila de un objeto de la tabla, se accede a las funciones deseadas desde el menú contextual.

- Cortar
- Copiar
- Pegar
  Es posible pegar objetos cortados o copiados dentro de la tabla o en la primera fila libre debajo de la tabla.
  Los objetos cortados o copiados también se pueden insertar en tablas de otros módulos de comunicación del mismo tipo y con el mismo protocolo de Telecontrol.
- Borrar

Con la tecla <Ctrl> pulsada se pueden seleccionar varias filas no contiguas.

Con la tecla <Mayúsculas> pulsada se puede seleccionar el inicio y el final de un área completa de filas contiguas.

Activar/desactivar la validación de puntos de datos

A la hora de crear nuevos puntos de datos o durante la importación se comprueba la coherencia del índice de punto de datos, el número de objeto y el canal del objeto. Si los números son incoherentes, los campos en cuestión se marcan con fondo rojo en la tabla de puntos de datos.

Si desea desactivar la comprobación temporalmente, puede desactivar esta función utilizando el siguiente botón situado encima de la tabla de puntos de datos:

La coherencia de los parámetros mencionados se comprueba a muy tardar durante la compilación.

Exportar e importar puntos de datos

Para facilitar la ingeniería de grandes instalaciones es posible exportar los puntos de datos de un módulo configurado e importarlos en otros módulos del proyecto. Esto ofrece ventajas especialmente en proyectos con muchas estaciones o módulos de puntos de datos iguales o similares.

Los módulos de comunicación con el mismo protocolo de Telecontrol son compatibles entre sí. Se pueden importar y exportar puntos de datos entre módulos compatibles.

También puede accederse a la función de exportación/importación:

- Desde el menú contextual del módulo, en la vista de redes o la vista de dispositivos

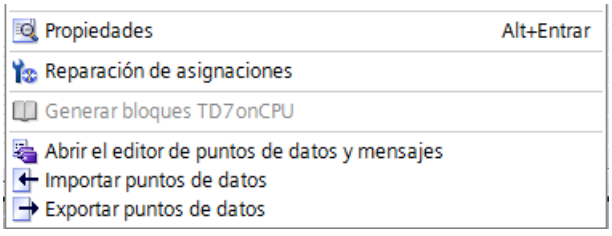


Figura 4-18 Menú contextual del módulo

- Mediante los dos símbolos de flecha de la lista de puntos de datos

Al realizar una exportación, la información de puntos de datos de un módulo se escribe en un archivo CSV.

La importación de puntos de datos de un proyecto antiguo a un proyecto nuevo es posible a partir de STEP 7 V18. Si hay parámetros que no se han complementado en el archivo CSV, la información que falta se rellenará con los valores predeterminados durante la importación. En estos casos, compruebe detenidamente los puntos de datos.

Recomendación:
Migre siempre su proyecto STEP 7 a la última versión de STEP 7 cuando esté disponible.

Exportación

Cuando se llama la función de exportación se abre el cuadro de diálogo correspondiente. Aquí se selecciona el o los módulos del proyecto cuya información de puntos de datos debe exportarse. En caso necesario, es posible exportar conjuntamente los puntos de datos de todos los módulos del proyecto.

En el cuadro de diálogo de exportación existe la posibilidad de seleccionar la ubicación en el directorio de archivos. Si se exportan los datos de un módulo, también es posible cambiar el nombre predeterminado de un archivo.

Cuando se exportan varios módulos, los archivos con nombre predeterminado se forman a partir del nombre de la estación y el nombre del módulo.

Además de la información de los puntos de datos, el archivo contiene la siguiente información:

- Nombre del módulo
- Tipo de módulo
- Nombre de la CPU
- Tipo de CPU

Editar los archivos de exportación

Es posible editar la información de puntos de datos en un archivo CSV exportado. De este modo existe la posibilidad de emplear este archivo como plantilla de configuración para muchas otras estaciones.

Si se dispone de un proyecto con muchas estaciones iguales, es posible copiar el archivo CSV con los puntos de datos de un módulo configurado para otras estaciones todavía no configuradas y adaptar cada uno de los parámetros a las estaciones correspondientes. De esta forma se evita tener que configurar los puntos de datos para cada módulo en STEP 7. En su lugar, solo hay que importar el archivo CSV copiado y adaptado a los otros módulos del mismo tipo. Al importar el archivo a otro módulo, los valores de parámetros modificados del archivo CSV se aplican a la configuración de puntos de datos de dicho módulo.

Las filas del archivo CSV tienen el contenido siguiente:

- Fila 1: ,Name,Type,TIA-Version;<Identificación de la versión de STEP 7>
  Esta fila no debe cambiarse.
- Fila 2: PLC,<Nombre de la CPU>,<Tipo de CPU>,
  Significado: PLC (Nombre de la clase de estación), nombre de la CPU, tipo de CPU
  Solo deben cambiarse los elementos <Nombre de la CPU> y <Tipo de CPU>.
  El tipo de CPU debe corresponderse exactamente con el nombre de la CPU en el catálogo.
- Fila 3: Module,<nombre del módulo>,<tipo de módulo>,
  Significado: Module (nombre de la clase de módulo), tipo de módulo, nombre del módulo
  Solo deben cambiarse los elementos <nombre del módulo> y <tipo de módulo>.
  Tenga cuidado al cambiar los nombres de módulo si desea importar los puntos de datos a varios módulos (véase más abajo).
  El tipo de módulo debe corresponderse exactamente con el nombre del módulo en el catálogo.

- Fila 4: Denominación del parámetro (en inglés) de los puntos de datos
  Esta fila no debe cambiarse.
  Consulte el significado más abajo (apartado "Parámetros").
- Filas 5..n: Valores de los parámetros según la fila 4 de cada uno de los puntos de datos
  Los valores de parámetros pueden modificarse para la importación a un nuevo módulo de comunicación.

Parámetros

Denominación y significado de los parámetros del archivo CSV exportado:

- Name: Nombre del punto de datos
- PLC tag: Variable de la CPU
- Master Side: Función de maestro
  Validez: DNP3 / IEC
- Datapoint type: Tipo de punto de datos
- Datapoint index: Índice de punto de datos
  Validez: DNP3 / IEC / TeleControl Basic
- Value monitoring: Vigilancia de valores
  Validez: ST7 / DNP3
- Type of transmission: Tipo de transferencia
- Priority in the scan cycle: Ciclo de lectura
- Response to general request: Respuesta a consulta general
  Validez: DNP3 / IEC / TeleControl Basic
  En TeleControl Basic, el parámetro suele ser TRUE.
- Assignment to group request no. 1 ... no. 16: Asignación a consulta de grupo n.º ...
  Validez: IEC
- Assignment to group request no.: Asignación a consulta de grupo n.º
  Validez: TeleControl Basic
  En TeleControl Basic, el parámetro suele ser FALSE.
- Threshold value trigger: Disparo de valor umbral
- Threshold value: Valor umbral
- Time trigger: Disparo de tiempo
- Time Trigger Cycle: Disparo
- Event trigger: Disparo de evento
- Trigger tag: Variable de disparo
- Transmission mode: Modo de transferencia
  Validez: ST7 / TeleControl Basic
- Meanvalue generation: Cálculo del valor medio
- Unipolar transfer: Transferencia unipolar
- Fault suppression time: Tiempo de supresión de errores
- Smoothing factor: Factor de filtrado

- Set limit value'high': Establecer calor límite 'alto'
- Limit value 'high': Valor límite 'alto'
- Set limit value 'low': Establecer valor límite 'bajo'
- Limit value 'low': Valor límite 'bajo'
- Control Code: Control Code (ficha Opciones de comando)
  Validez: ST7 / DNP3 / IEC
- Pulse Limit: Número máx. de impulsos
  Validez: ST7 / DNP3 / IEC
- Pulse control: Control de impulsos
  Validez: DNP3 / IEC
- Pulse OnTime Limit: Duración máx. de impulso
  Validez: DNP3
- Pulse OnTime Surrogate: Duración de impulso tiempo de sustitución
  Validez: DNP3
- Short Pulse Duration: Duración de impulso corta
  Validez: IEC
- Long Pulse Duration: Duración de impulso larga
  Validez: IEC
- Command execution mode: Modo de comando
  Validez: DNP3 / IEC
- Mirroring of local value: Duplicado del valor local
  Validez: ST7 / DNP3
- PLC tag for local value: Variable PLC para valor local
  Validez: ST7 / DNP3
- Partners of datapoint: Interlocutores activados en el punto de datos con los que se ha configurado una conexión de Telecontrol.
  Para dispositivo de terceros se indica el número de interlocutor.
  Si hay varios interlocutores, se separan con una coma y se ponen juntos entre comillas.
  Ejemplo: "PLC_1,Interlocutor_1,PLC_4"
- Enable archiving: Activar archivación (ficha "Disparo")
  Validez: TIM 1531 IRC
- Partnernumber (inter-station communication): Número de interlocutor (comunicación cruzada)
  Validez: TeleControl Basic
- Integration interval: Intervalo de integración (ficha Preprocesamiento de valores analógicos)
- Alarm event type: Eventos de estado de estación (ficha "Disparo")
  Validez: DNP3 / IEC
- Substation address: Dirección de subestación (ficha "Disparo")
  Validez: DNP3 / IEC
- With timestamp: Con sello de tiempo (ficha "General")
  Validez: DNP3

- Command result: Resultado del comando
  Validez: DNP3 / IEC
- PLC tag for command result: Variable para resultado del comando
  Validez: DNP3 / IEC
- Status trigger: Disparo de estado
  Validez: ST7 / DNP3 / IEC
- Timestamp trigger: Disparo de sello de tiempo
  Validez: ST7 / DNP3 / IEC
- S7 Repetition Factor: (solo se exporta para fines informativos, pero el valor no vuelve a importarse)
  Validez: ST7 / DNP3 / IEC
- S7 Data Type Value: (solo se exporta para fines informativos, pero el valor no vuelve a importarse)
  Validez: ST7 / DNP3 / IEC

Importación a un módulo

Antes de importar los puntos de datos, asegúrese de que se han creado las variables PLC necesarias para los puntos de datos.

Tenga en cuenta que cuando se importa un archivo CSV se borran todos los puntos de datos existentes en el módulo y se reemplazan por los puntos de datos importados.

Seleccione un módulo y elija la función de importación desde el menú contextual del módulo. Se abre un cuadro de diálogo de importación en el que se selecciona el archivo CSV en el directorio de archivos.

Si la información relacionada con la asignación de los diferentes puntos de datos a su correspondiente variable PLC concuerda con la asignación en el módulo original, los puntos de datos se asignan a la variable PLC correspondiente.

Si importa puntos de datos a un módulo pero en la CPU todavía no se han creado algunas variables PLC necesarias, la información de puntos de datos correspondientes no podrá asignarse. En ese caso, las variables PLC que falten pueden crearse a posteriori para asignarles después la información de puntos de datos importada. Para ello se dispone de la función "Reparación de asignaciones" (véase más abajo).

Si los nombres de las variables PLC en el módulo al que se realiza la importación se diferencian del módulo que ha realizado la exportación, los puntos de datos correspondientes no podrán asignarse a sus variables PLC.

Importación a varios módulos

Es posible importar los puntos de datos de varios módulos a los módulos de otro proyecto. Para ello, seleccione todos los archivos CSV necesarios en el cuadro de diálogo de importación utilizando la tecla de control.

Antes de importar los puntos de datos asegúrese de que las estaciones correspondientes con CPU homónimas, módulos homónimos y variables PLC homónimas están creadas.

Durante la importación se buscan las estaciones correspondientes del proyecto en función del nombre del módulo en los archivos CSV. Si una estación de destino no está en el

proyecto o si el módulo tiene un nombre distinto, se ignora la importación del archivo CSV correspondiente.

Limitaciones en la importación de puntos de datos

En los casos siguientes se cancela la importación de los puntos de datos:

- En el archivo CSV que debe importarse falta un atributo necesario para el módulo.
  Ejemplo: Si un punto de datos que debe importarse emplea un disparo de hora, se cancela la importación cuando para el módulo no se ha configurado ninguna sincronización horaria.
- El protocolo de Telecontrol empleado por el módulo difiere del módulo original.
  Los módulos con el mismo protocolo de Telecontrol son compatibles entre sí:

Solo cuando se importa a varios módulos:

- La importación se cancela cuando un nombre de módulo o CPU difiere de los datos del archivo CSV.

Durante la importación se crea un archivo de registro que señala los posibles errores.

Reparación de asignaciones

Si en una estación a la que debe importarse el archivo CSV las variables PLC tienen nombres distintos a los de la estación de la que debe exportarse el archivo CSV, se pierde la asignación entre el punto de datos y la variable PLC durante la importación.

En ese caso existe la posibilidad de cambiar convenientemente el nombre de variables PLC existentes o bien de agregar las variables PLC que faltan. A continuación es posible reparar la asignación entre puntos de datos no asignados y variables PLC. Se accede a esta función desde el menú contextual del módulo (véase más arriba) o mediante el símbolo siguiente situado en la parte superior izquierda del editor de puntos de datos: 

Si la función de reparación encuentra una variable PLC para un punto de datos con un nombre adecuado, la asignación se restablece. Sin embargo, no se comprueba el tipo de datos de la variable.

Tras reparar la asignación, compruebe siempre si las variables PLC reasignadas son correctas.

Recomendación:
Antes de importar los puntos de datos, copie la tabla de variables o el bloque de datos de la CPU de origen desde la que se exportarán los puntos de datos a la CPU de destino en cuyo módulo de comunicación se importarán los puntos de datos exportados.

4.23.2 Tipos de puntos de datos

Al configurar los datos útiles que deben transferirse, se asigna cada punto de datos a un tipo.

A continuación se listan los tipos de puntos de datos específicos del protocolo, junto con los tipos de datos S7 compatibles en cada caso.

La columna "Sentido" indica el sentido de la transferencia:

- "in": sentido de observación
- "out": sentido de control

En el protocolo ST7, el sentido de la transferencia se ve en el nombre de objeto.

Nota

Repercusión del cambio de arrays para puntos de datos

Si cambia posteriormente un array deberá volver a crearse el punto de datos.

Tipos de puntos de datos del protocolo "IEC 60870-5"

Tabla 4-5 Tipos 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 CP56Time2a [1]	<30>	in	Bool	I, Q, M, DB
	Single command	<45> [4]	out	Bool	Q, M, DB
	Single command with time tag CP56Time2a [1]	<58> [5] [6]	out	Bool	Q, M, DB
	Double command with time tag CP56Time2a [1]	<59>	out	Bool	DB [2]
Byte	Step position information	<5>	in	Byte, USInt	I, Q, M, DB
	Step position information with time tag CP56Time2a [1]	<32>	in	Byte, USInt	I, Q, M, DB
	Regulating step command with time tag CP56Time2a [1]	<60>	out	Byte, USInt	DB [2]
Integer (16 bits)	Measured value, normalized value	<9>	in	Int	I, Q, M, DB
	Measured value, normalized value with time tag CP56Time2a [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 CP56Time2a [1]	<35>	in	Int	I, Q, M, DB
	Set point command, normalized value	<48> [4]	out	Int	Q, M, DB
	Set point command, scaled value	<49> [4]	out	Int	Q, M, DB
	Set point command, normalized value with time tag CP56Time2a [1]	<61> [5]	out	Int	Q, M, DB
	Set point command, scaled value with time tag CP56Time2a [1]	<62> [5]	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> [4]	out	UDInt, DWord	Q, M, DB
	Bitstring of 32 bits with time tag CP56Time2a - control direction [1]	<64> [5]	out	UDInt, DWord	Q, M, DB

Formato (memoria necesaria)	Tipo de punto de datos	Tipo IEC	Sentido	Tipos de datos S7	Área de operandos
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> [4]	out	Real	Q, M, DB
	Set point command, short floating point with time tag CP56Time2a [1]	<63> [5]	out	Real	Q, M, DB
Bloque de datos (1...2 Bit) [2]	Double-point information	<3>	in	ARRAY [0...1] of Bool	DB
	Double-point information with time tag CP56Time2a [1]	<31>	in	ARRAY [0...1] of Bool	DB
	Double command	<46> [4]	out	ARRAY [0...1] of Bool	DB
	Regulating step command	<47> [4]	out	ARRAY [0...1] of Bool	DB
	Double command with time tag CP56Time2a [1]	<59> [5] [6]	out	ARRAY [0...1] of Bool	DB
	Regulating step command with time tag CP56Time2a [1]	<60> [5] [6]	out	ARRAY [0...1] of Bool	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> [4]	out	[3]	DB
	Bitstring of 32 bits with time tag CP56Time2a - control direction [1] [3]	<64> [5]	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.

[4] Para IEC 60870-5-104 existe la posibilidad de configurar estos tipos IEC como alternativa a los de la nota a pie de página [5], pero no pueden mezclarse ambos tipos IEC.

[5] Estos tipos IEC solo se soportan para IEC 60870-5-104.

[6] La "Duración máx. de comando" de los comandos se configura en el grupo de parámetros "Ajustes básicos" de los módulos.

Retroalimentación con Single Command

En los siguientes comandos es posible activar la retroalimentación del valor actual de la estación al maestro.

- Single Command <45>

Existe la posibilidad de supervisar los cambios en el valor local de este punto de datos y transferirlos al maestro cuando se produzcan. 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. Para ello se

requiere un segundo punto de datos "Single-point information <1>". Proceda del siguiente modo para configurar la función de retroalimentación.

Cree los puntos de datos:

- En el módulo maestro
  - Single Command <45>
  - Single-point information <1>

  El valor retroalimentado debe escribirse en una variable del maestro. Por este motivo hay que asignar los dos puntos de datos a variables distintas en el módulo maestro.
  Asigne el mismo índice a ambos puntos de datos.
- En el módulo de estación
  - Single Command <45>
  - Single-point information <1>

  Asigne ambos puntos de datos a la misma variable en el módulo de estación.
  Asigne el mismo índice a ambos puntos de datos.

El valor retroalimentado por la estación se escribe en el tipo de punto de datos "Single-point information <1>" del maestro.

Sellos de tiempo de los datos en el protocolo IEC

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

4.23.3 Identificaciones de estado de los puntos de datos

Identificaciones de estado

Las identificaciones de estado de puntos de datos listadas en las tablas siguientes se transfieren con el valor en cada telegrama de datos dirigido al interlocutor de la comunicación. Pueden ser evaluados por el interlocutor de la comunicación.

En la tabla, las entradas de la línea "Significado" se refieren a la entrada correspondiente de la línea "Estado del bit".

Quality descriptor - IEC 60870-5

Las identificaciones de estado corresponden a los elementos siguientes de las especificaciones:

Quality descriptor - IEC 60870 Part 5-101

Asignación de bits del byte de estado en los diferentes objetos: Tipo de punto de datos <tipo IEC>

Tabla 4-6 Information object <1, 30>

Bit	7	6	5	4	3	2	1	0
Nombre de la marca	IV invalid	NT not topical	SB substituted	BL blocked	-	-	-	SPI
Significado	Valor válido	Valor no actualizado	Valor sustitutivo	Valor bloqueado	-	-	-	-
Estado del bit	0	1	1	1	*(siempre 0)*	*(siempre 0)*	*(siempre 0)*	*(siempre 0)*

Tabla 4-7 Double-point information object <3, 31>

Bit	7	6	5	4	3	2	1	0
Nombre de la marca	IV invalid	NT not topical	SB substituted	BL blocked	-	-	DPI	
Significado	Valor válido	Valor no actualizado	Valor sustitutivo	Valor bloqueado	-	-	-	
Estado del bit	0	1	1	1	*(siempre 0)*	*(siempre 0)*	*(siempre 0)*	

Tabla 4-8 Step position <5, 32>, Bitstring <7, 33>, Analog input <9, 11, 13, 34, 35, 36>

Bit	7	6	5	4	3	2	1	0
Nombre de la marca	IV invalid	NT not topical	SB substituted	BL blocked	-	-	-	OV overflow *
Significado	Valor válido	Valor no actualizado	Valor sustitutivo	Valor bloqueado	-	-	-	Rango de valores rebasado por exceso, valor analógico
Estado del bit	0	1	1	1	*(siempre 0)*	*(siempre 0)*	*(siempre 0)*	1

* Para los valores límite configurados del punto de datos, el bit "OV overflow" se activa del siguiente modo al transmitir el valor analógico:

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

Tabla 4-9 Counter (Integrated totals) <15, 37>

Bit	7	6	5	4	3	2	1	0
Nombre de la marca	IV invalid	CA counter adjusted	CY carry	SB substituted	SQ sequence number			
Significado	Valor válido	Valor de contaje corregido	Desbordamiento del valor de contaje antes de leer el valor	Valor sustitutivo				
Estado del bit	0	1	1	1				

4.23.4 Ficha "General"

Tabla de puntos de datos

Encontrará los principales parámetros de la primera ficha del editor de puntos de datos en el ajuste estándar de la tabla de puntos de datos.

Si va con el ratón hasta la barra de título de la tabla de puntos de datos, puede visualizar todos los parámetros de la configuración de puntos de datos en el menú contextual.

General

Parámetros:

- **Nombre**
  nombre unívoco del punto de datos
- **Variable PLC**
  Consulte la asignación en el capítulo Configuración de puntos de datos (Página 132).
- **Tipo de punto de datos**
  Consulte el capítulo Tipos de puntos de datos (Página 142)
- **Índice de punto de datos**
  Consulte el capítulo Índice de punto de datos (Página 149)
- **Función de maestro**
  Activa la función de maestro del punto de datos.
  Consulte el significado en el capítulo Función de maestro de los puntos de datos (Página 148).
- **Tipo de transferencia**
  Consulte el tipo de transferencia en el capítulo Memoria imagen de proceso, tipo de transferencia, clases de eventos (Página 151).
- **Ciclo de lectura**
  Solo con entradas
  Consulte el ciclo de lectura en el capítulo Ciclo de lectura (Página 152).

- **Respuesta a consulta general**
  Activa el punto de datos para la respuesta a una consulta general. Si la función está desactivada, el valor del punto de datos no se envía al interlocutor de la comunicación tras una consulta general.
- **Asignación a consulta de grupo**
  Asigna el punto de datos a una consulta de grupo.
  Si el maestro realiza una consulta de grupo al grupo en cuestión, se envía al maestro el valor del punto de datos.

4.23.5 Función de maestro de los puntos de datos

La función de maestro para la comunicación directa

La comunicación directa entre dos estaciones de Telecontrol, en la que los telegramas no son transmitidos por una central, es posible activando la función de maestro de los puntos de datos.

Requisitos

Los requisitos para la configuración de la comunicación directa entre dos puntos de datos de dos interlocutores son:

- Entre los dos interlocutores debe haberse creado una conexión de Telecontrol.
  Adicionalmente para DNP3: En la conexión de Telecontrol está activada la opción "Espontáneo".
- El punto de datos debe estar asignado a un interlocutor.
  Configuración en la columna "Interlocutor del punto de datos" de la tabla de puntos de datos.

Significado de la función de maestro

- **"Función de maestro" activada**
  Los valores del punto de datos se tratan igual que en el caso de un maestro:
  - **Puntos de datos de entrada (sentido "in")**
    Los puntos de datos de entrada son recibidos por el interlocutor de acuerdo con los parámetros ajustados en el interlocutor.
    El tipo de transferencia "Transferencia tras llamada" está ajustado de forma fija.
    Las opciones del "Preprocesamiento de valores analógicos" están desactivadas.
  - **Puntos de datos de salida (sentido "out")**
    Los puntos de datos de salida se envían al interlocutor de acuerdo con la configuración de disparo.
    El tipo de transferencia "Todos los valores disparados" está ajustado de forma fija.

  Para activar la opción consulte el capitulo Ficha "General" (Página 147).
- **"Función de maestro" desactivada**
  - **Puntos de datos de entrada (sentido "in")**
    Los puntos de datos de entrada se tratan de acuerdo con la configuración.
    El tipo de transferencia y las opciones del "Preprocesamiento de valores analógicos" pueden configurarse libremente.
  - **Puntos de datos de salida (sentido "out")**
    Los puntos de datos de salida se tratan de acuerdo con la configuración.
    El tipo de transferencia "Transferencia tras llamada" está seleccionado automáticamente y no puede modificarse.

4.23.6 Índice de punto de datos

El índice de un punto de datos es la dirección del objeto informativo.

En el programa, los índices se asignan en orden ascendente al crear los puntos de datos. Existe la posibilidad de configurar los índices de acuerdo con sus exigencias y las siguientes reglas.

Configuración del índice de punto de datos

Direccionamiento estructurado

El índice puede configurarse en dos campos de entrada con un formato distinto:

- Índice de punto de datos
  Aquí se configura el índice sin estructurar como entero.
  Rango de valores: 1..16777215
- Índice estructurado
  Aquí se puede configurar el índice estructurado conforme a IEC 60870-5-3. Mediante el direccionamiento estructurado es posible estructurar los puntos de datos en función de la instalación.
  Pueden configurarse 3 niveles de direcciones (octetos).
  Rango de valores: 0.0.1..255.255.255

Los valores configurados de los dos campos están acoplados. Un valor configurado se convierte y se muestra en el otro campo de entrada.

Conversión de los valores configurados

Los valores se identifican del siguiente modo para la conversión:

- Índice de punto de datos
  Nombre del valor del entero: X
- Índice estructurado
  Designación de los valores de los 3 octetos: A.B.C

El valor configurado se aplica al otro campo, respectivamente, siguiendo la fórmula que se indica:

X = A * 256 * 256 + B * 256 + C

Reglas de configuración

Las reglas siguientes son válidas para la configuración del índice de puntos de datos.

- Los índices deben ser unívocos dentro de un módulo para cada interlocutor de la comunicación.
  Los índices asignados por duplicado se notifican como errores durante la comprobación de la coherencia e impiden que se compile el proyecto.
- Los índices de dos puntos de datos pueden ser idénticos si los dos puntos de datos están configurados para interlocutores distintos.
  Ejemplo:
  - Punto de datos 1, índice 1, interlocutor 1
  - Punto de datos 2, índice 1, interlocutor 2
  - Punto de datos 3, índice 2, interlocutor 1
  - Punto de datos 4, índice 2, interlocutor 7
- Los índices de interlocutor correspondientes tienen que ser idénticos en el lado emisor y receptor.

Índice y "Transferencia secuencial"

Validez:

- Módulos
  - CP 1243-7 LTE
  - TIM 1531 IRC
- Tipo de nodo de red de la interfaz para la comunicación por Telecontrol: estación o estación nodo
- Grupo de parámetros: Interfaz > Opciones avanzadas > Ajustes de estación IEC > Ajustes de eventos > Comportamiento de transferencia

Es posible configurar la transferencia conjunta de telegramas de eventos en una secuencia para puntos de datos sin sello de hora.

Para la transferencia secuencial se tienen que cumplir los requisitos siguientes:

- Los puntos de datos son del mismo tipo.
- Los índices de los puntos de datos son consecutivos sin huecos.

4.23.7 Memoria imagen de proceso, tipo de transferencia, clases de eventos

Almacenamiento de valores

Por lo general, los valores de todos los puntos de datos se guardan en la memoria imagen del módulo. Los valores de la memoria imagen no se transfieren hasta que se produce una llamada por parte del TIM central.

Los valores de puntos de datos que están configurados como eventos se guardan adicionalmente en el búfer de transmisión.

Memoria imagen, la memoria imagen de proceso del módulo

La memoria imagen es la memoria imagen de proceso del TIM. 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) o junto con un telegrama proveniente del búfer de transmisión que debe transferirse de inmediato.

El búfer de transmisión

El búfer de transmisión del TIM es la memoria para los diferentes valores de puntos de datos que están configurados como eventos. Encontrará el tamaño del búfer de transmisión en el manual del módulo correspondiente.

La capacidad del búfer de transmisión se reparte equitativamente entre todos los interlocutores activados (destinatarios de telegramas).

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 de la comunicación, 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 procedimiento es el siguiente:

- Cuando el búfer de transmisión alcanza un nivel de llenado de 80 %, se emite una advertencia.
- Cuando el búfer de transmisión está lleno en un 100 % de su capacidad, no se guardan más valores hasta que el nivel de llenado baja por debajo del 100 %.

Tipo de transferencia de los valores de puntos de datos guardados

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

Los eventos se guardan también en el búfer de transmisión.

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 registran en la memoria imagen (memoria imagen de proceso). Los valores estáticos corresponden al siguiente tipo de transferencia "Transferencia tras llamada (class 0)".
- **Evento**
  Los valores de puntos de datos que están configurados como eventos (tipo de transferencia por disparo) también se registran en la memoria imagen del módulo. Adicionalmente, los valores se registran en el búfer de transmisión.

Tipos de transferencia y clases de eventos

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. Los valores nuevos de un punto de datos sobrescriben el último valor guardado en la memoria imagen.
  Tras una llamada del interlocutor se transfiere el valor actual en ese momento.
  Para puntos de datos de salida esta opción está predeterminada y no se puede modificar.
- **Disparado**
  Mediante un tipo de transferencia por disparo los puntos de datos se configuran como eventos. Los valores de estos puntos de datos se registran en la memoria imagen y también en el búfer de transmisión.
  Los valores de un evento se guardan en cuanto se cumplen las condiciones de disparo configuradas.
  Se dispone de las siguientes clases de eventos:
  - **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.

  Consulte los diferentes tipos de disparo en el capítulo Ficha "Disparo" (Página 154).

4.23.8 Ciclo de lectura

La lectura y escritura cíclicas de variables PLC o DB de la CPU por parte del módulo de comunicación se controla limitando el número de variables que deben leerse y escribirse. Esto se realiza en el grupo de parámetros "Comunicación con la CPU".

La lectura cíclica de los valores de puntos de datos de entrada desde sus variables 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, la actualización de puntos de datos de entrada importantes sí puede priorizarse. La priorización se realiza para cada punto de datos individual en la ficha "General" de la configuración de puntos de datos, con el parámetro "Ciclo de lectura".

Opciones del parámetro "Ciclo de lectura"

- Ciclo normal
  Los valores de las variables en el ciclo normal se leen proporcionalmente en todos los ciclos de muestreo.
- Ciclo rápido
  El ciclo rápido es adecuado para datos que deben registrarse rápidamente, p. ej. alarmas. El valor se lee en cada ciclo.

Adicionalmente para S7-1200/1500/ET 200SP:

- Espontáneo
  El punto de datos se registra en la CPU para la vigilancia y deja de ser consultado cíclicamente por el módulo de comunicación.
  En cuanto el valor de la CPU cambia, la CPU lo transfiere activamente al módulo de comunicación.
  Esto garantiza la transferencia rápida de todos los valores modificados, al mismo tiempo que limita la carga del bus de fondo.
- Sin vigilancia
  El punto de datos ni se vigila ni se consulta. El valor consultado por una central siempre es cero.
  Esta opción puede servir para salidas que no deben vigilarse y que no devuelven valores de duplicado.

Estructura del ciclo de muestreo de la CPU

El ciclo con el que el módulo de comunicación muestrea el área de memoria de la CPU consta de las fases siguientes:

- **Peticiones de lectura**
  - **Peticiones de lectura con prioridad alta (Ciclo rápido)**
    Para todos los puntos de datos con la asignación "Ciclo rápido" se leen las variables de CPU en cada ciclo de muestreo.
    El número de peticiones de lectura de alta prioridad no está limitado.
    Generalmente es suficiente con asignar al ciclo rápido solo los datos que deben registrarse rápidamente, como alarmas o mensajes transitorios.
  - **Peticiones de lectura con prioridad baja - proporcionalmente (Ciclo normal)**
    Para los puntos de datos con la asignación "Ciclo normal" se leen los valores de sus variables proporcionalmente en cada ciclo de muestreo.
    Como máximo, en un ciclo de muestreo se leen tantas variables como se han configurado para "Número máx. de peticiones de lectura" ("Comunicación con la CPU").
    Los valores de las demás variables de prioridad baja que no se han podido leer en un ciclo se leen en el próximo ciclo.
- **Peticiones de escritura**
  En cada ciclo se escriben en la CPU los valores de un número configurable de peticiones de escritura espontáneas. El número de valores que se escriben en cada ciclo se especifica con el parámetro "Número máx. de peticiones de escritura" en el grupo de parámetros "Comunicación con la CPU". Las variables que no se han podido escribir en un ciclo (variables > valor configurado) se escriben en el próximo ciclo.
- **Tiempo de pausa de ciclo**
  El tiempo de espera entre dos ciclos de muestreo sirve para reservar tiempo suficiente para otros procesos que acceden a la CPU por el bus de fondo.

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.

Nota

Restricción en caso de escritura rápida de consignas conforme a IEC 60870-5

Si se envían dos puntos de datos de consigna prácticamente al mismo tiempo, es posible que se ignore la transmisión de la segunda consigna. Mantenga una distancia mínima de 70 milisegundos entre la transmisión de consignas.

4.23.9 Ficha "Disparo"

Momento de transferencia

Los puntos de datos se configuran mediante el parámetro "Tipo de transferencia" como valor estático ("Transferencia tras llamada (class 0)") o como evento (disparado).

Los valores estáticos se introducen en la memoria imagen de proceso y se transfieren después de que o el maestro llame a la estación; véase Memoria imagen de proceso, tipo de transferencia, clases de eventos (Página 151).

Los eventos se registran en el búfer de transmisión. Para enviar un valor de evento es imprescindible que el punto de datos esté configurado como evento en la ficha "General".

- Tipo de transferencia = "Todos los valores disparados"
  o
- Tipo de transferencia = "Valor actual disparado"

La activación de un disparador hace que se guarde el valor.

Según los ajustes de disparo, el valor de un evento se transferirá al interlocutor de inmediato o con retardo tras iniciar el disparo.

En la interfaz del módulo (tipo de nodo de red "Estación"), dentro del grupo de parámetros "Ajustes de estación IEC > Propiedades de evento", se especifica qué datos se transmiten inmediatamente o con retardo en función de la clase de evento.

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 159).
- **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 módulo pone a 0 (cero) la variable de disparo en cuanto se ha transferido 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.

Disparo de estado / Disparo de sello de tiempo

Validez: TIM 1531 IRC V2.4, CP 1200 V3.5

Los dos disparos inician el envío del valor del punto de datos cuando cambia el estado o el sello de tiempo en la CPU. Al mismo tiempo, se transfieren con el valor el estado de la CPU o el sello de tiempo de la CPU.

El sello de tiempo de la CPU debe interpretarse como hora local o UTC, dependiendo de los ajustes de hora. El módulo de comunicación reenvía el sello de tiempo de la CPU a los interlocutores conectados.

Requisitos de los puntos de datos:

- El punto de datos es un evento (tipo de transferencia "disparado")
- La "Función de maestro" (ficha "General") del punto de datos está desactivada.
- Para cada punto de datos que debe utilizar estas funciones se crea un UDT; véase más abajo.

Para utilizar estos dos disparadores hay que crear un punto de datos cuya variable haga referencia al UDT indicado abajo.

- **Disparo de estado**
  Inicia el envío del valor del punto de datos cuando cambia el estado en la CPU. El valor del punto de datos se transfiere junto con el estado de la variable que se ha formado en la CPU.
  Válido para los siguientes tipos de puntos de datos (tipo de punto de datos <tipo IEC>):
  - Information objects <1, 3, 5, 30, 31, 32>
  - Measured value <9, 11, 13, 34, 35, 36>
  - Integrated totals <15, 37>
  - Bitstring <7, 33>

  Consulte la codificación del byte de estado en el capítulo Identificaciones de estado de los puntos de datos (Página 145).
- **Disparo de sello de tiempo**
  Inicia el envío del valor del punto de datos cuando cambia el sello de tiempo en la CPU. El valor del punto de datos se transfiere junto con el sello de tiempo de la CPU.
  Válido para los siguientes tipos de puntos de datos (tipo de punto de datos <tipo IEC>):
  - Information objects <30, 31, 32>
  - Measured value <34, 35, 36>
  - Integrated totals <37>
  - Bitstring <33>

Estructura del UDT común para las variables "Valor", "Disparo de estado" y "Disparo de sello de tiempo"

Los valores de "Valor", "Disparo de estado" y "Disparo de sello de tiempo" se escriben juntos en un tipo de datos de usuario (UDT), incluso si solo se utiliza uno de los dos disparadores.

El UDT tiene la estructura siguiente:

- Variable "Valor"
  El tipo de datos debe corresponderse con el tipo de punto de datos cuyo valor debe transferirse.
  Los tipos de puntos de datos soportados se mencionan arriba.
- Variable "Estado"
  Tipo de datos: Byte
- Variable "Tiempo"
  Tipo de datos: DTL

Para cada punto de datos que desee transferir con las opciones "Disparo de estado" y "Disparo de tiempo" debe crearse un UDT separado.

Creación del UDT

Para las tres variables hay que crear primero un tipo de datos de usuario (UDT). Para ello, proceda del siguiente modo:

1. En el árbol del proyecto vaya hasta la entrada "Tipos de datos PLC" de la CPU asignada.
2. Haga clic en la entrada "Agregar nuevo tipo de datos".
3. Opcional: cambie el nombre del UDT
   (seleccione un tipo de datos de usuario nuevo > menú contextual "Propiedades" > ficha "General")
4. Seguidamente, cree las variables necesarias en el UDT.
   El tipo de datos de la variable "Value" debe corresponderse con el tipo de datos del punto de datos que debe transferirse en cada caso.

ValueStatusTime

	Name	Data type	Default value	Accessible f...	Writa...	Visible ...
	Value	Real	0.0	☑	☑	☑
	Status	Byte	16#0	☑	☑	☑
	Time	DTL	DTL#1970-01-0...	☑	☑	☑
	YEAR	UInt	1970	☑	☑	☑
	MONTH	USInt	1	☑	☑	☑
	DAY	USInt	1	☑	☑	☑
	WEEKDAY	USInt	5	☑	☑	☑
	HOUR	USInt	0	☑	☑	☑
	MINUTE	USInt	0	☑	☑	☑
	SECOND	USInt	0	☑	☑	☑
	NANOSECOND	UDInt	0	☑	☑	☑

Figura 4-19 Estructura del UDT para un valor medido con tipo de datos "Real"

5. Abra un bloque de datos o cree uno nuevo.
6. Inserte el UDT creado previamente en el bloque de datos.
   El UDT puede seleccionarse por el nombre que se le ha asignado automáticamente o que el usuario ha cambiado.

Nota

Transferencia conjunta de los datos del UDT

Asegúrese de transferir los datos del UDT juntos en un ciclo del OB1 para garantizar la coherencia de los datos.

Activar archivación

Validez: TIM 1531 IRC

El TIM 1531 IRC permite guardar los valores de puntos de datos disparados en la tarjeta SD de la CPU.

En caso de fallos de conexión, la opción activa el almacenamiento remanente de valores de eventos (búfer de transmisión) en la tarjeta SD.

Requisitos para poder activar la función:

- Activación del parámetro "Permitir almacenamiento remanente" (grupo de parámetros "Ajustes básicos")
- Desactivación de la "Función de maestro" (editor de puntos de datos > ficha "General")

La archivación es posible en los siguientes tipos de puntos de datos:

- Information objects <1/5/30/32>
- Measured value <9/11/13/34/35/36>
- Integrated totals <15/37>
- Bitstring <7/33>

Eventos de estado de estación

Solo configurable en TIM 1531 IRC y con el tipo de puntos de datos "Single-point information" <1/30>

La opción "Función de maestro" tiene que estar desactivada.

- **Tipo de evento de estado de estación**
  Elija el evento con el que la estación enviará telegramas a los interlocutores definidos. El telegrama se transmite junto con el número de objeto.
  - No hay eventos de estado de estación
  - Estado de CPU local modificado
    (True = RUN, False = STOP)
  - Estado de conexión con CPU local modificado
    (True = conexión correcta, False = conexión incorrecta)
  - Estado de conexión con subestación modificado
    (True = conexión correcta, False = conexión incorrecta)
  - Error en tarjeta SD
    (True = tarjeta SD defectuosa, False = tarjeta SD en buen estado)
  - Estado de la conexión de sincronización redundante modificado
    (True = estado de la conexión modificado; solo con redundancia de dispositivos)
- **Dirección de subestación**
  Si se selecciona la opción "Estado de conexión con subestación modificado", introduzca aquí la dirección de estación de la subestación cuyo estado de conexión ha cambiado.

4.23.10 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.

Los factores de filtrado y el intervalo de integración, si se ha configurado, se tienen en cuenta al realizar el cálculo.

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

Nota

Disparo de valor umbral si está configurado el cálculo del valor medio

Si está activado el cálculo del valor medio, para valores analógicos se aplica el método absoluto para calcular la desviación del valor de umbral en el disparo de valor umbral.

Respecto al proceso de Preprocesamiento de valores analógicos consulte el capítulo Preprocesamiento de valores analógicos (Página 161).

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.
  Mediante el "Intervalo de integración" (Preprocesamiento de valores analógicos) es posible desactivar la aplicación del método integrativo a valores analógicos.

Método absoluto

Para cada valor binario se comprueba si el valor actual (quizá filtrado) se encuentra fuera del margen del valor 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 puede ajustarse; consulte el apartado "Intervalo de integración" en el capítulo Preprocesamiento de valores analógicos (Página 161).
(Anotación: 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 4-10 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

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
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.

4.23.11 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 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 siguiendo el esquema descrito a continuación:

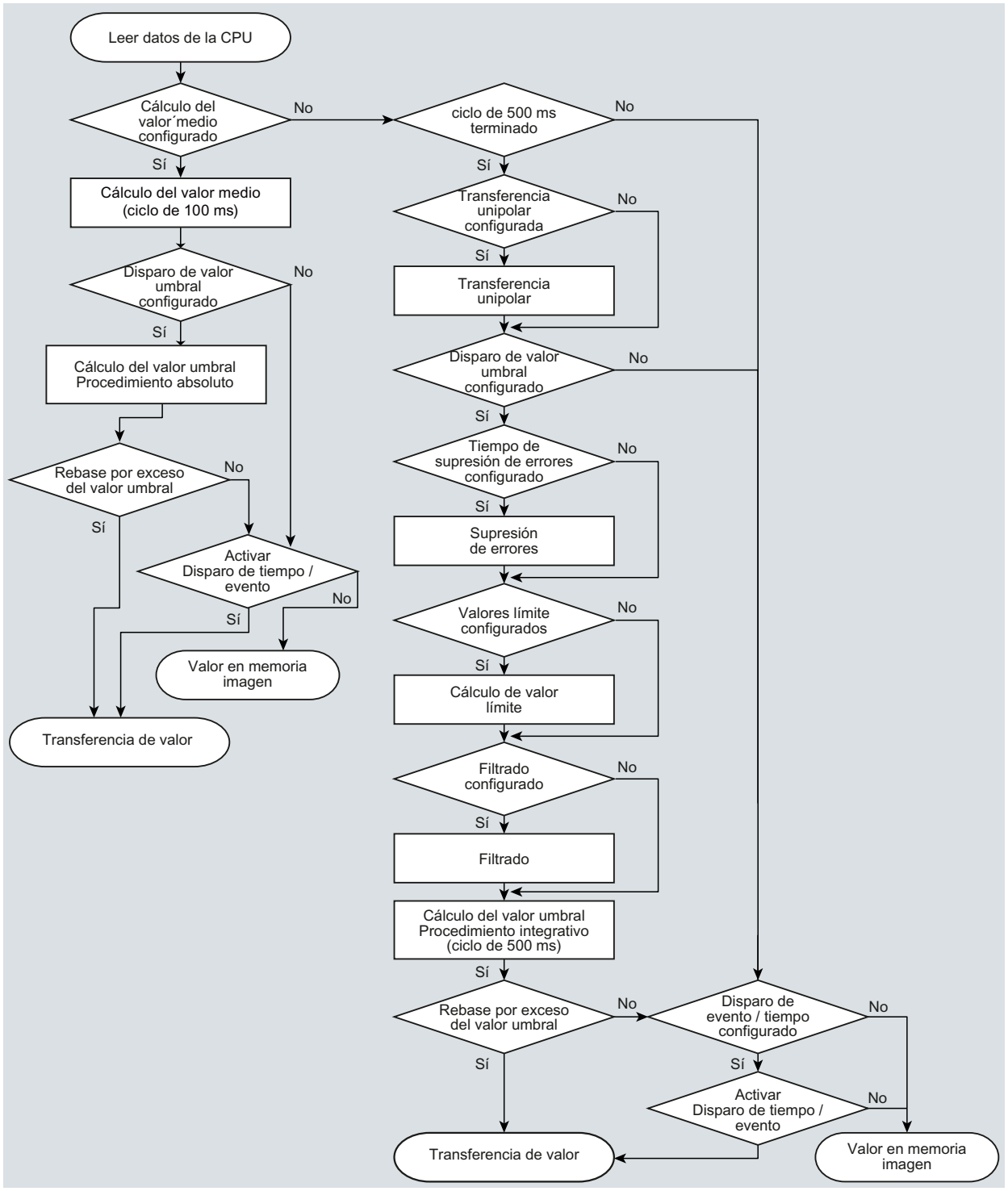


Figura 4-20 Ejecución del preprocesamiento de valores analógicos

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

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

El cálculo del valor medio solo se soporta para enteros del tipo "Int" en el caso de los protocolos siguientes:

- TeleControl Basic
- DNP3
- IEC 60870-5

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
- Cálculo del valor umbral solo con el método absoluto

Función

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.

Intervalo de integración

El intervalo de integración se utiliza para el procesamiento de valores umbrales de valores analógicos según el principio de integración. El valor umbral se utiliza para el disparo de valor umbral; consulte el capítulo Disparo de valor umbral (Página 159).

El valor introducido determina el intervalo de tiempo en el que se integran valores analógicos.

Con 0 (cero), el valor umbral se calcula sin integración. Con ello se reduce el volumen de datos. En este caso se aplica el método absoluto.

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
y_{n-1} = valor filtrado en el ciclo anterior n-1
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
- Tipos de variables soportados de la CPU
  El punto de datos del valor analógico debe estar enlazado con una de las variables siguientes:
  - Variable PLC en el área de marcas
  - Variable DB (variable en el bloque de datos)

  Para variables PLC que acceden a módulos de hardware (área de operandos de entrada/ salida) 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.

Recomendación para valores analógicos que sufren oscilaciones rápidas:

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

Identificación de estado "OVER_RANGE" / "OV overflow"

En los protocolos que soportan identificaciones de estado, cuando se rebasa por defecto o exceso el valor límite se activa la identificación de estado del punto de datos para rebase por exceso del rango de medición.

Configuración del valor límite

Un valor límite se configura como número decimal entero o como número en coma flotante, según sea el tipo de datos.

Tabla 4-11 Rangos de los valores límite

Tipo de datos	Rango de valores
Int	-32768 ... 32767
DInt	-2147483648 ... 2147483647
Real/LReal	-7.9000E+028..7.9000E+028

Nota

Valor límite 0 (cero)

- En la mayoría de módulos, la entrada del valor 0 se interpreta como valor límite desactivado. Excepciones:
- En los siguientes módulos a partir de la versión de firmware indicada también es posible un 0 como valor límite:
  - CP 1243-7 LTE V3.3
  - CP 1542-1 IRC V2.2
  - TIM 1531 IRC V2.2

La tabla siguiente indica los rangos de un número de 32 bits con respecto a los rangos del valor bruto de un módulo de entradas o salidas analógicas.

Rango	Valor de la variable PLC de 16 bits *		Salida del módulo [mA]			Rango de medición [%]
	Decimal	Hexadecimal	0 .. 20 (unipolar)	-20 .. +20 (bipolar)	4 .. 20 (life zero)	
Desbordamiento	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	Valor de la variable PLC de 16 bits *		Salida del módulo [mA]			Rango de medición [%]
	Decimal	Hexadecimal	0 .. 20 (unipolar)	-20 .. +20 (bipolar)	4 .. 20 (life zero)	
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

***** Los rangos de valores (rebase por defecto / rebase por exceso) en variables PLC con diferentes tipos de datos son los siguientes:

- Int
  - -32768
  - 32767
- DInt
  - -2147483648
  - 2147483647
- Real/LReal
  - -7.9000E+028
  - 7.9000E+028

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.

Consulte también

Identificaciones de estado de los puntos de datos (Página 145)

4.23.12 Opciones de comando

Opciones de salida

Las opciones de salida corresponden a la especificación IEC 60870-5-101 - Qualifier of command.

Parámetros

Las dos opciones de salida situadas debajo de "Control Code" pueden activarse de forma alternativa:

- **LATCH_ON/OFF**
  - Qualifier of command - QU (Type 1.1) <1> persistent output
    Esta función bloquea una salida de comando en el valor 0 o 1 de forma permanente.
    Recuerde:
    El valor bloqueado no se anula hasta que hay otro comando. El comando también puede anularse desde el programa de usuario.
- **PULSE_ON**
  Qualifier of command - QU (Type 1.1)
  La función evalúa el número y la longitud de señales (impulsos) de salidas de comandos procedentes de la central.
  Codificación:
  - <1> short pulse duration
    Parámetro correspondiente en el módulo: "Duración de impulso corta"
  - <2> long pulse duration
    Parámetro correspondiente en el módulo: "Duración de impulso larga"

La opción de salida "Modo de comando" puede activarse de forma independiente:

- **Modo de comando**
  Qualifier of command / Qualifier of set-point command - S/E (Type 6)
  Codificación:
  - <0> execute
  - <1> select

  La función especifica si un comando se transfiere directamente a la CPU (direct command transmission) o si se espera una confirmación de ejecución (execute) tras la selección (select) antes de reenviar el comando.
  El módulo de estación acusa la recepción de la ASDU de selección con el Qualifier <1> select. Tras recibir el acuse, el maestro envía el ASDU de ejecución con el Qualifier <0> execute".

Procesamiento

- LATCH_ON/OFF
  Esta función bloquea el valor de un comando de la forma descrita anteriormente.
- PULSE_ON/OFF
  El maestro codifica la función mediante un "Qualifier of command". El módulo de comunicación evalúa las codificaciones siguientes en la estación:
  - QU (Type 1.1) <0> no additional definition
    Parámetro correspondiente en el módulo: "Control de impulsos"
  - QU (Type 1.1) <1> short pulse duration
    Parámetro correspondiente en el módulo: "Duración de impulso corta"
  - QU (Type 1.1) <2> long pulse duration
    Parámetro correspondiente en el módulo: "Duración de impulso larga"
  - S/E (Type 6) <0> execute
    Parámetro correspondiente en el módulo: "Modo de comando"
  - S/E (Type 6) <1> select
    Parámetro correspondiente en el módulo: "Modo de comando"

Tipos de puntos de datos

Las opciones de salida pueden configurarse para los siguientes tipos de puntos de datos:

- Control Code (LATCH_ON/OFF / PULSE_ON)
  - Single command ... <45>, <58>
  - Double command ... <46>, <59>
  - Regulating step command ... <47>, <60>
- Modo de comando
  - Single command ... <45>, <58>
  - Double command ... <46>, <59>
  - Regulating step command ... <47>, <60>
  - Set-point command ... <48>, <49>, <61>, <62>

Parámetros

Nombre:	**Control Code**
Rango de valores:	• PULSE_ON • LATCH_ON/OFF
Explicación:	Opción de salida para la salida de comando. Consulte el significado más arriba.

Nombre:	**Número de impulsos / Número máx. de impulsos**
Ajuste predeterminado:	1
Explicación:	Número de impulsos que el punto de datos del maestro transfiere al correspondiente punto de datos de la estación. En la estación, el parámetro vigila el número de impulsos enviados por el maestro. Si el número de impulsos recibido por el maestro supera el valor especificado, el comando se rechaza.

Nombre:	**Control de impulsos** (solo "Double command")
Rango de valores:	• Duración de impulso corta • Duración de impulso larga
Explicación:	• Duración de impulso corta Los impulsos cortos están previstos para operaciones críticas en el tiempo, por ejemplo para controlar interruptores automáticos. • Duración de impulso larga Los impulsos largos están previstos para operaciones que no son críticas en el tiempo.

Nombre:	**Duración de impulso corta (s)**
Rango de valores:	0 ... 65535
Ajuste predeterminado:	0
Explicación:	El módulo de comunicación emite comandos del maestro con Qualifier of command = <1> (short pulse duration) durante el tiempo configurado aquí. Si "Duración de impulso corta" está configurada con 0 (cero), el módulo rechaza los comandos con Qualifier of command de <1>.

Nombre:	**Duración de impulso larga (s)**
Rango de valores:	0 ... 65535
Ajuste predeterminado:	0
Explicación:	El módulo de comunicación emite comandos del maestro con Qualifier of command = <2> (long pulse duration) durante el tiempo configurado aquí. Si "Duración de impulso larga" está configurada con 0 (cero), el módulo rechaza los comandos con Qualifier of command de <2>.

Nombre:	**Modo de comando**
Rango de valores:	• Ejecución directa • Selección y ejecución
Ajuste predeterminado:	Ejecución directa
Explicación:	• Ejecución directa "direct command transmission" El comando se transfiere inmediatamente a la CPU de la estación para su ejecución. • Selección y ejecución "select / execute" Secuencia: – Activación del comando en el módulo maestro La central transfiere el telegrama "Selección" al módulo de comunicación de la estación. – La estación acusa la recepción. – Tras recibir el acuse de la estación, el punto de datos maestro envía el telegrama de ejecución. – La estación solo reenvía el comando a la CPU si dentro del "Tiempo máx. entre Select y Operate" configurado recibe el telegrama "Ejecución" del maestro. La estación no debe recibir ningún otro telegrama de datos entre Selección y ejecución. Nota: "Tiempo máx. entre Select y Operate" se configura en los ajustes de transferencia de la interfaz correspondiente.

Resultado del comando

Función y validez

Esta función está prevista para devolver una respuesta al interlocutor de la comunicación acerca de si se ha recibido un comando o una consigna del módulo de comunicación. La posterior ejecución del comando en la CPU no se registra ni se evalúa.

Validez: puntos de datos de comando y consigna con opción "Función de maestro" activada.

La confirmación de recepción se escribe en la "Variable para resultado del comando" (byte, véase abajo) y se envía a la variable correspondiente del interlocutor.

La respuesta debe ser evaluada en el interlocutor de la comunicación.

Tipos de datos

- Single / double / regulating step command <45, 46, 47>
- Single / double / regulating step command with time tag CP56Time2a <58, 59, 60>
- Set point command, normalized value / scaled value / short floating point value <48, 49, 50>

- Set point command, normalized value / scaled value / short floating point value with time tag CP56Time 2a <61, 62, 63>
- Bitstring of 32 bits without/with time tag <51, 64>

Parámetros

Nombre:	**Resultado del comando**
Ajuste predeterminado:	0
Explicación:	Activa la realimentación de la recepción del comando o la consigna al interlocutor de la comunicación.

Nombre:	**Variable para resultado del comando**
Tipo de datos:	Mismo tipo de datos que el punto de datos correspondiente
Explicación:	El valor local debe ubicarse en esta variable.

Codificación de la "Variable para resultado del comando"

El resultado de la recepción del comando/consigna se devuelve en la respuesta sobre la "Cause of Transmission".

Se admiten los siguientes resultados:

- unknown type identification <44>
- unknown cause of transmission <45>
- unknown common address of ASDU <46>
- unknown information object address <47>

4.23.13 Estaciones interlocutoras

Activación de los interlocutores del punto de datos

En la tabla se muestran como interlocutores las estaciones con las que se ha configurado una conexión de Telecontrol.

Utilice la casilla de verificación para activar el o los interlocutores con los que el punto de datos seleccionado debe intercambiar datos: ☑

4.24 Mensajes

Configuración de los mensajes

El módulo de comunicación puede enviar mensajes configurados cuando se producen eventos importantes. Para la configuración no es necesario emplear bloques de programa.

Para transferir mensajes ya no es necesario que la comunicación por Telecontrol (grupo de parámetros "Tipos de comunicación") esté activada.

Pueden configurarse:

- Correos electrónicos
  El destinatario puede ser un PC con conexión a Internet o una estación S7.
- SMS (solo CP de telefonía móvil o módulos TIM)
  El destinatario puede ser un teléfono móvil o una estación S7.

En cada módulo se pueden configurar como máximo 10 mensajes (correo electrónico o SMS).

Los mensajes se configuran en el editor de mensajes del módulo, que puede consultarse de uno de los siguientes modos:

- Menú contextual del módulo
- Desde el árbol del proyecto: directorio de la estación > Módulos locales > Módulo de comunicación

Respecto a la vista en STEP 7 consulte el capítulo Configuración de puntos de datos (Página 132).

Iniciar la transferencia de mensajes

La transmisión del mensaje se inicia mediante un evento que se configura en la ficha "Disparo" (véase más abajo).

Requisitos, información necesaria y procedimiento

Correos electrónicos

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

- Activación de la comunicación por Telecontrol (grupo de parámetros "Tipos de comunicación")
- Activación de las funciones de seguridad
- Configuración del grupo de parámetros "Configuración de correo electrónico"

Información necesaria:

- Datos de acceso del servidor SMTP: dirección, número de puerto, nombre de usuario y contraseña
- Si se utiliza STARTTLS o SSL/TLS: certificado del operador del servicio de correo electrónico
- Direcciones de correo electrónico de los destinatarios
- APN (CP de telefonía móvil)
  Su operador de red le facilitará los datos de acceso a la red de telefonía móvil y a un APN para la transferencia de correos electrónicos. Dichos datos se configuran en el grupo de parámetros "Ajustes de comunicación de telefonía móvil".

La configuración se realiza en los grupos de parámetros siguientes:

- Activación de las funciones de seguridad
  Para utilizar correos electrónicos es necesario activar las funciones de seguridad del CP en el grupo de parámetros "Security".
- Configuración del servicio / protocolo:
  "Configuración de correo electrónico"
- Si se utiliza STARTTLS o SSL/TLS:
  - Importación del certificado del operador del servicio de correo electrónico:
    "Ajustes globales de seguridad"
  - Uso del certificado importado para el módulo:
    Grupo de parámetros "Security" > "Administrador de certificados"

SMS (CP de telefonía móvil o TIM)

Información necesaria:

- Número del SMSC

La configuración se realiza en los grupos de parámetros siguientes:

- Activación de la función de SMS:
  "Tipos de comunicación" > "Activar SMS"
- Configuración del SMSC
  "Ajustes de comunicación de telefonía móvil"
- Configuración de SMS
  Editor de mensajes

"Parámetros de mensaje"

Aquí se configuran el número de abonado o los destinatarios, el asunto (correo electrónico) y el texto del mensaje.

Texto: número de caracteres

Número máximo de caracteres que pueden transferirse en el texto del mensaje:

- SMS: máx. 160 caracteres ASCII, incluido un valor que pueda haberse enviado conjuntamente
- Correo electrónico: 256 caracteres ASCII, incluido un valor que pueda haberse enviado conjuntamente

Con respecto al valor, consulte más abajo el parámetro "Incluir valor en el envío".

Juego de caracteres para textos de mensajes

Se indican los caracteres permitidos a continuación en juegos de caracteres ASCII (valor hexadecimal y nombre de carácter):

- 0x20
  Espacio
- 0x21 ... 0x5F
  ! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [\ ] ^ _
- 0x61 ... 0x7E
  a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~
- 0x7C, 0x7E
  | ~
- Salto de línea manual (↲)
  En los textos de los mensajes puede insertarse un salto de línea mediante <Mayús>+<ENTRAR>.

"Disparo"

Mediante el grupo de parámetros "Disparo" se configura el inicio de la transmisión del mensaje, además de otros parámetros.

- **Disparo de correo electrónico / Disparo de SMS**
  Define el evento que inicia la transmisión del correo electrónico:
  - **Utilizar variable PLC**
    Como señal de disparo para la transmisión del correo electrónico se evalúa el cambio de flanco (0 → 1) del bit de disparo "Variable PLC para disparo" activado por el programa de usuario. En caso necesario es posible configurar un bit de disparo independiente para cada mensaje. Véase el bit de disparo más abajo.
    Desactivación del bit de disparo:
    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 mensaje.
    En todos los demás casos hay que desactivar el bit de disparo desde el programa de usuario.

    Nota

    Activación rápida de la variable de disparo de diagnóstico

    Los disparos no deben activarse más de una vez por segundo.

    Transmisión frecuente de SMS

    La transmisión de un SMS puede tardar hasta 2 minutos, según sea el entorno del sistema. Para garantizar una transmisión segura de SMS en módulos de telefonía móvil, se recomienda mantener una distancia mínima de 10 segundos entre disparos de SMS.

  - **La CPU pasa a STOP**
  - **La CPU pasa a RUN**
  - **Conexión con un interlocutor interrumpida**
    Inicia la transmisión del mensaje cuando se interrumpe la conexión de Telecontrol con un interlocutor.
    Para definir el interlocutor consulte más abajo el parámetro "Interlocutor para disparo".
  - **Conexión con un interlocutor establecida**
    Inicia la transmisión del mensaje cuando se restablece la conexión.
    Para definir el interlocutor consulte más abajo el parámetro "Interlocutor para disparo".
  - **Error al establecer conexión con un interlocutor**
    Inicia la transmisión del mensaje cuando no se ha podido establecer la conexión de Telecontrol con un interlocutor.
  - **Sesión de TeleService iniciada**
    (CP de telefonía móvil)
    Inicia la transmisión del mensaje cuando la comunicación por Telecontrol está activada y se ha establecido una conexión de TeleService.
  - **Sesión de TeleService finalizada**
    (CP de telefonía móvil)
    Inicia la transmisión del mensaje cuando la comunicación por Telecontrol está activada y se ha finalizado una conexión de TeleService.

  - **Red de telefonía móvil débil**
    (solo SMS)
    Si la conexión de telefonía móvil es demasiado débil para la comunicación por Telecontrol, se inicia un SMS y se envía al destinatario configurado.
  - **Conexión VPN establecida**
    (CP 1243-7 LTE, CP 1243-1, CP 1542SP-1 IRC)
    Inicia la transmisión del mensaje cuando se establece o restablece la conexión VPN.
  - **Conexión VPN deshecha**
    (CP 1243-7 LTE, CP 1243-1, CP 1542SP-1 IRC)
    Inicia la transmisión del mensaje cuando se interrumpe la conexión VPN.
  - **Conexión SINEMA RC establecida**
    (CP 1243-7 LTE, CP 1243-1, CP 1542SP-1 IRC)
    Inicia la transmisión del mensaje cuando se establece o restablece la conexión VPN u OpenVPN.
  - **Conexión SINEMA RC deshecha**
    (CP 1243-7 LTE, CP 1243-1, CP 1542SP-1 IRC)
    Inicia la transmisión del mensaje cuando se interrumpe la conexión VPN u OpenVPN.

- **Interlocutor para disparo**
  Aquí se escoge, entre los interlocutores configurados del dispositivo, aquél cuya conexión se ve afectada en las opciones de disparo "Conexión con un interlocutor establecida" o "Conexión con un interlocutor interrumpida".
- **Variable PLC para disparo**
  Variable PLC para el disparo "Utilizar variable PLC"
- **Activar identificación de estado de procesamiento**
  Si se activa esta opción, después de cada intento de transmisión se devuelve un estado que informa del estado de procesamiento del mensaje enviado.
  El estado se escribe en la "Variable PLC para estado de procesamiento". Si hay problemas con la entrega de los mensajes, se puede definir el estado a través del servidor web de la CPU, visualizando en él el valor de la variable PLC.
  Respecto al significado de los estados emitidos en formato hexadecimal, consulte el capítulo Estado de procesamiento de los mensajes (SMS, correo electrónico) (Página 191).
- **Variable PLC para estado de procesamiento**
  Variable PLC del tipo DWORD para el estado de procesamiento
- **Incluir valor en el envío**
  Si la opción está activada, el módulo 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 $$ dentro del texto del mensaje.
  $$ como comodín para el valor de una variable PLC soporta los siguientes tipos de datos:
  - Bool, Byte, Char, USInt, Int, UInt, Word, DWord, UDInt, DInt, Real, String
  - Arrays de los tipos de datos citados
- **Variable PLC para valor**
  Variable PLC en la que debe escribirse el valor que se enviará junto con el mensaje.

Mensajes de error

Si cuando se compila la estación se muestra un mensaje de error sobre el tipo de disparo, debe comprobarse la configuración.

Si el tipo de disparo configurado para el mensaje es una de las opciones siguientes:

- VPN / IPSec / SINEMA RC
- Compruebe lo siguiente:
  - ¿Están activadas las funciones de seguridad?
  - ¿Está activado VPN?
  - ¿Están bien ajustadas otras opciones?

4.25 Juego de caracteres para nombres de usuario, contraseñas y mensajes

Juego de caracteres para nombres de usuario, contraseñas y textos de mensajes

Los siguientes caracteres permitidos son válidos para:

- Servidor de correo electrónico:
  - nombre de usuario y contraseña
- Mensajes en el editor de mensajes:
  - textos de mensajes

Se indica en juegos de caracteres ASCII (valor hexadecimal y nombre de carácter):

- 0x20
  Espacio
- 0x21 ... 0x5F
  ! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z [\ ] ^ _
- 0x61 ... 0x7E
  a b c d e f g h i j k l m n o p q r s t u v w x y z { | } ~
- 0x7C, 0x7E
  | ~

Adicionalmente, para textos de mensajes:

- Salto de línea manual (↲)
  En los textos de los mensajes puede insertarse un salto de línea mediante <Mayús>+<ENTRAR>.

Puesta en servicio

5

5.1 Puesta en servicio del CP

Requisitos: Configuración antes de la puesta en marcha

Para la completa puesta en marcha del módulo es imprescindible que los datos del proyecto de STEP 7 estén completos.

Poner en servicio el módulo

La puesta en servicio posterior incluye los pasos siguientes:

1. Compilar los datos del proyecto
2. Cargar los datos del proyecto de STEP 7 en el dispositivo
   Los datos de configuración de STEP 7 del CP se transfieren durante la operación de carga de la estación.
   Para cargar la estación conecte a la CPU la estación de ingeniería en la que se encuentran los datos del proyecto.

Encontrará más detalles en el sistema de información de STEP 7, dentro del capítulo "Compilar y cargar datos de proyecto".

5.2 Ajustar la hora durante el funcionamiento con seguridad / SINEMA RC

Ajustar la hora durante la puesta en marcha

Nota

Sincronización horaria si se emplea seguridad / SINEMA RC

Si se utilizan funciones de seguridad, como SINEMA Remote Connect, el CP necesita la hora actual para la autenticación en el interlocutor o en el servidor SINEMA RC.

El CP obtiene la hora de la CPU o de un servidor NTP antes de establecer la primera conexión.

Recomendación:

Durante la puesta en marcha debe ajustarse manualmente la hora de la CPU por lo menos una vez mediante las funciones online de STEP 7. Esto es especialmente necesario cuando para la sincronización horaria se ha configurado la opción "Hora del interlocutor". De este modo se garantiza que la CPU tiene una hora válida al arrancar la estación y que el CP puede intercambiar los certificados necesarios con el interlocutor o el servidor SINEMA RC.

Diagnóstico y mantenimiento 6

6.1 Posibilidades de diagnóstico

Las siguientes posibilidades de diagnóstico están disponibles en la mayoría de módulos. Algunas funciones están limitadas a determinados tipos de dispositivos o protocolos.

LED del módulo

Encontrará información sobre los indicadores LED en el manual de producto del respectivo módulo.

STEP 7: La ficha "Diagnóstico" en la ventana de inspección

Si la estación de ingeniería está conectada con un módulo vía Ethernet, aquí se proporciona la información siguiente sobre el módulo seleccionado:

- Estado de conexión de la estación de ingeniería con el módulo

STEP 7: Funciones de diagnóstico en el menú "Online > Online y diagnóstico"

Las funciones online permiten leer desde el módulo correspondiente diferentes informaciones de diagnóstico de una estación de ingeniería en la que está guardado el proyecto de STEP 7 y ejecutar funciones de mantenimiento.

Para obtener más información sobre las funciones de diagnóstico de STEP 7, consulte el sistema de información de STEP 7.

Accesos online

Aquí se establece la conexión online con el módulo.

Consulte el procedimiento en el sistema de información de STEP 7.

Diagnóstico

Aquí aparece la siguiente información estática sobre el módulo seleccionado:

- **General**
  Información general sobre el módulo
- **Estado de diagnóstico > Eventos específicos del dispositivo**
  Aquí encontrará las entradas del búfer de diagnóstico del módulo y una vista general de los mensajes (SMS / correos electrónicos) enviados.
- **Interfaz Ethernet[X1/2/3]**
  Información de direccionamiento y estadística

- **Industrial Remote Communication**
  Aquí se obtiene información específica de la WAN sobre el módulo TIM:
  - **Interlocutor**
    Aquí aparecen los datos de dirección y configuración de los interlocutores, una estadística de la conexión y más información de diagnóstico. Haga clic en un dispositivo para mostrar información adicional.
    También encontrará información sobre los interlocutores en el WBM; consulte más abajo.
  - **Lista de puntos de datos**
    Información sobre los puntos de datos, como datos de configuración, valor, estado de la conexión, etc.
  - **Diagnóstico de protocolo de telegramas**
    Esta función permite activar la generación de informes de telegramas del módulo, evaluarlos y visualizarlos.
    El archivo de texto generado puede analizarse mediante el monitor de telegramas del TIM de la herramienta de diagnóstico de SINAUT.
    Consulte la descripción en el capítulo Diagnóstico de protocolo de telegramas (Página 187).
  - **Diagnóstico Ethernet**
    La función de registro permite generar informes con fines de diagnóstico sobre el intercambio de datos del TIM, utilizando la funcionalidad PCAP.
    En caso de error o de comportamiento no deseado del TIM permite grabar el comportamiento de comunicación del TIM. Se registra el intercambio de telegramas del TIM durante un tiempo definido o para un número de telegramas configurable.
    Los archivos de registro pueden guardarse como archivo PCAP en el PC conectado y evaluarse con el programa Wireshark, por ejemplo.
- **Seguridad**
  - Estado
    Muestra información sobre datos generales del módulo.
  - Registro del sistema
    Lee las entradas del registro del sistema.
  - Registro de auditoría
    Lee las entradas del registro de auditoría.
  - Registro de filtros de paquetes
    Lee las entradas del registro de filtros de paquetes.
  - Estado de la comunicación
    Esta página de diagnóstico muestra los estados de los módulos de seguridad conocidos del grupo VPN, sus puntos finales y las propiedades del túnel.
  - SINEMA RC - Configuración VPN automática
    Esta página de diagnóstico muestra el estado de la configuración OpenVPN automática y de las conexiones OpenVPN.
- **Hora**
  Indica la hora actual del módulo y el origen de la hora. Posibilidad de ajustar la hora del módulo.

Funciones

Aquí pueden ejecutarse las funciones siguientes:

- **Actualización de firmware**
- **Asignar dirección IP**
- **Restablecer configuración de fábrica**
  Consulte las funciones en el capítulo Mantenimiento (Página 193).
- **Guardar datos de servicio**
  La función permite protocolizar procesos internos del módulo en situaciones en las que no es posible solucionar por uno mismo comportamientos del módulo no deseados o inesperados.
  El botón "Guardar datos de servicio" genera el archivo de protocolización. Los datos se guardan en un archivo con formato "*.dmp", que puede ser evaluado por el servicio técnico de Siemens.

Servidor web (WBM) del TIM 1531 IRC

Desde un PC es posible acceder a las páginas web (WBM) del TIM por medio de HTTP/HTTPS. El WBM proporciona diversa información.

Para el acceso y los contenidos, consulte el manual de producto del TIM /2/ TIM 1531 IRC (Página 220).

Estado del interlocutor y estados de la conexión en el WBM

Los interlocutores configurados y el estado de las conexiones con los interlocutores locales y remotos del TIM se muestran en la página "Telecontrol" > "Información sobre interlocutores" del WBM. Consulte los detalles en /2/ TIM 1531 IRC (Página 220).

Información del interlocutor y la conexión a la CPU

El TIM puede notificar a su CPU local, a través de una variable PLC, el estado de la conexión y de las vías de conexión con el interlocutor. Consulte la configuración en el capítulo Comunicación con la CPU (Página 80).

SNMP

Consulte las funciones en el capítulo SNMP (Página 190).

6.2 Servidor web S7-1200: establecimiento de conexión

Establecer una conexión con el servidor web de la CPU

Proceda del siguiente modo para conectarse al servidor web de la CPU desde un PC.

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 de una CPU con versión V4.0 o superior, cree un usuario con los derechos necesarios.

En función de si se ha activado o desactivado la opción "Permitir acceso solo vía HTTPS" en el grupo de parámetros "General", el procedimiento difiere del establecimiento de una conexión con el servidor web.

- **Establecimiento de conexión vía HTTP**
  Procedimiento con la opción "Permitir acceso solo vía HTTPS" desactivada
- **Establecimiento de conexión vía HTTPS**
  Procedimiento con la opción "Permitir acceso solo vía HTTPS" activada

Las dos variantes están descritas en los apartados siguientes.

Encontrará los requisitos para el acceso al servidor web de la CPU (navegadores web permitidos) y la descripción del procedimiento en el sistema de información de STEP 7, bajo la palabra clave "Información importante sobre el servidor web".

Establecimiento de conexión vía HTTP

1. Conecte el PC a la CPU a través de la interfaz Ethernet.
2. Introduzca la dirección de la CPU en el campo de dirección del 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, bajo las palabras clave "HTTPS" y "Acceso para HTTPS (S7-1200)".
6. Si la conexión está cambiada al modo seguro HTTPS ("https://<dirección IP>/..." en el campo de dirección del servidor web), puede continuar tal como se describe en 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. Conecte el PC a la CPU a través de la interfaz Ethernet.
2. Introduzca la dirección de la CPU en el campo de dirección del navegador web: https://<Dirección IP>
3. Pulse la tecla de entrada <Intro>.
   Se abre la página de inicio del servidor web.

4. Inicie sesión como usuario con los derechos necesarios en la página de inicio del servidor web.
   Utilice los datos de usuario configurados en la administración de usuarios del servidor web de la CPU.
5. Tras el inicio de sesión, elija la entrada "Estado del módulo" en la navegación del servidor web.
6. Seleccione el CP en la lista de módulos.
   Se muestran los contenidos propios del CP.

6.3 Diagnóstico de seguridad online por el puerto 8448 del CP

Diagnóstico de seguridad a través del puerto 8448

Requisitos:

- Si el cortafuegos está activado, el acceso debe estar habilitado.

Si quiere llevar a cabo un diagnóstico de seguridad en STEP 7 Professional, haga lo siguiente:

1. Seleccione el CP en STEP 7.
2. Abra el menú contextual "Online y diagnóstico".
3. Haga clic en el botón "Establecer conexión online" en el grupo de parámetros "Seguridad".

De ese modo realizará el diagnóstico de seguridad a través del puerto 8448.

Puerto 8448 del TIM 1531 IRC

En el TIM 1531 IRC, el puerto 8448 está abierto en el ajuste predeterminado.

6.4 Diagnóstico de protocolo de telegramas

El diagnóstico de protocolo de telegramas está disponible para los módulos siguientes:

- CP de Telecontrol S7-1200
- CP 1542SP-1 IRC
- TIM 1531 IRC

6.4.1 Protocolo de telegramas: estructura y funciones

El "Diagnóstico de protocolo de telegramas" sirve para registrar los telegramas transmitidos.

Para activar la función consulte el apartado "Manejo" más adelante.

Estructura del cuadro de diálogo "Protocolo de telegramas"

Tras la activación, las columnas muestran los siguientes datos:

- N.º
  - Símbolo de un telegrama entrante o saliente
  - Número de telegrama correlativo.
- Bloque
  Longitud del bloque de telegramas en el que se ha transferido el telegrama.
- Campos del encabezado
  Representación hexadecimal de algunos datos del encabezado
  Consulte el significado en el capítulo Detalles (Página 189).
- Dispositivo (origen > destino)
  Números de dispositivo, tanto del emisor (origen) como del receptor (destino)
- Objeto (origen > destino)
  Número del objeto de datos en el telegrama, tanto en el dispositivo de origen como en el de destino
- Índice
  Parámetro de dirección para datos netos en telegramas de datos (número de canal)
- Fecha, hora y estado
  Sello de tiempo del telegrama y estado de la hora en el momento de la transferencia
  Consulte la representación en el capítulo Detalles (Página 189).
- Datos netos
  Representación hexadecimal de los datos netos del telegrama
  Consulte el significado en el capítulo Detalles (Página 189).

Manejo

La función se maneja con los tres botones situados debajo del cuadro de diálogo descrito arriba.

- Activar el diagnóstico de protocolo de telegramas
  Haciendo clic en el botón se inicia el registro de los telegramas transmitidos.
  Se registran 400 telegramas en cada ciclo. Es posible guardar como máximo 10 000 telegramas en un búfer en anillo.
- Actualizar
  Actualiza el registro; se inicia un nuevo ciclo de registro.
- Guardar
  Guarda los telegramas registrados en un archivo binario. La ubicación se determina con el botón.
- Mostrar los guardados
  Muestra los telegramas grabados y guardados.

6.4.2 Detalles

Información detallada

Campos del encabezado

Los 5 campos en formato hexadecimal tienen el siguiente significado:

- 1.er campo: contador de telegramas
  0...7
- 2.º campo: código de control
- 3.er campo: selección de funciones
  - 0: edición en el TIM
  - 1: edición en la CPU
- 4.º campo: ampliación de la dirección
  - 0: telegrama ST1 sin ampliación de la dirección
  - 1: telegrama ST1 con ampliación de la dirección
  - 2: telegrama ST7
- 5.º campo: bit de sentido
  - 0: sentido de vigilancia
  - 1: sentido de control

Datos netos

La columna muestra los datos netos del telegrama.

Los valores se muestran en formato hexadecimal.

Fecha, hora y estado

La columna muestra el sello de tiempo del telegrama en el formato siguiente:

año/mes/día_hora:minutos:segundos_estado

Asignación del estado de la hora:

- 2^0
  - 0: la hora no es válida
  - 1: la hora es válida
- 2^1
  - 0: horario de invierno (hora normal)
  - 1: horario de verano

- 2^2
  No asignado
- 2^3
  - 0: sin significado
  - 1: hora de aviso para el cambio entre horario de verano e invierno
    Solo en el telegrama de sincronización horaria

6.5 SNMP

SNMP (Simple Network Management Protocol)

SNMP es un protocolo para la gestión y el diagnóstico 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 están depositadas en los archivos MIB (MIB = Management Information Base).

Prestaciones de los módulos como SNMP-Agent

No todas las funciones descritas a continuación están disponibles para cada módulo. En el manual de producto del respectivo módulo encontrará información sobre las prestaciones del mismo.

Los módulos de comunicación soportan la consulta de datos vía SNMP en las siguientes versiones:

- SNMPv1 (estándar)
- SNMPv3 (Security)

Suministran los contenidos de objetos MIB del MIB II estándar según RFC1213.

- **MIB II**
  El MIB soporta los siguientes grupos de objetos MIB:
  - System
  - Interfaces
    El objeto MIB "Interfaces" proporciona información de estado sobre las interfaces del módulo.
  - IP
  - ICMP
  - TCP
  - UDP
  - SNMP

  Los siguientes grupos de MIB II estándar no se soportan:
  - Adress Translation (AT)
  - EGP
  - Transmission

Los módulos no soportan traps.

Encontrará más información sobre los archivos MIB y SNMP en el manual /9/ SNMP (Página 221).

Configuración

Consulte la configuración en el capítulo SNMP (Página 95).

6.6 Estado de procesamiento de los mensajes (SMS, correo electrónico)

Estado de procesamiento de mensajes

Si en la ficha "Disparo" de la configuración de mensajes de STEP 7 se activa la opción "Activar identificación de estado de procesamiento", el módulo emite un estado.

Este estado 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".

El estado de procesamiento es devuelto por el propio módulo o por los servidores del servicio una vez transmitido un mensaje que debía enviarse.

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).

Los estados filtrados tienen el siguiente significado:

Estado de procesamiento de los mensajes de Telecontrol

Tabla 6-1 SMS: Significado de la identificación de estado en formato hexadecimal

Estado	Significado
0000	Transferencia concluida sin fallos
0001	Error en la transferencia; causas posibles: • Tarjeta SIM no válida • No hay red • Número de teléfono de destino erróneo (número no disponible)

Tabla 6-2 Correo electrónico: 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 módulo. 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 módulo.

Estado	Significado
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).
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 en la configuración los parámetros "Nombre de usuario" y "Contraseña".
8550	No es posible acceder al servidor SMTP. No tiene derechos de acceso. Compruebe los siguientes datos de configuración: • Configuración de módulos > 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.

6.7 Mantenimiento

Funciones de mantenimiento

Encontrará la descripción de las siguientes funciones de mantenimiento en el manual de producto o en las instrucciones de servicio del respectivo módulo; consulte Bibliografía (Página 219).

- Actualización de firmware
- Restablecer
- Sustitución de módulos

Bloques de programa OUC (CP)

A

A.1 Validez y requisitos

Validez

Las funciones descritas a continuación son soportadas por los siguientes módulos:

- CP 1243-1
  - Firmware ≥ V3.1 o superior
- CP 1243-7 LTE
  - Firmware ≥ V3.1 o superior
- CP 1243-8 IRC
  - Firmware ≥ V3.1 o superior
- CP 1542SP-1 IRC
  - Firmware ≥ V2.0 o superior

Tenga en cuenta las diferencias en las versiones de firmware para la comunicación segura (Secure OUC); véase más abajo.

A.2 Bloques de programa para OUC

Uso de los bloques de programa para la Open User Communication (OUC)

Las instrucciones que aparecen más adelante (bloques de programa) pueden utilizarse para la comunicación directa entre estaciones S7.

A diferencia de la comunicación por Telecontrol, la Open User Communication no debe activarse en la configuración, pues para ello deben crearse activamente los bloques de programa correspondientes. Encontrará más detalles sobre los bloques de programa en el sistema de información de STEP 7.

Nota

No debe haber diferentes versiones de los bloques de programa

Tenga en cuenta que no es posible utilizar en una misma estación versiones diferentes de un bloque de programa.

Requisitos para Secure OUC

Requisitos para utilizar la transferencia segura mediante Secure OUC:

- STEP 7: V16 o superior
- Firmware de la CPU
  - CPU-1200: V4.4 o superior
  - CPU 151xSP: V2.0 o superior
- Firmware del CP
  - CP 1200: V3.2 o superior
  - CP 1542SP-1 IRC: V2.1 o superior

Bloques de programa soportados para OUC

Las instrucciones siguientes en la versión mínima indicada están disponibles para la parametrización de la Open User Communication:

- **TSEND_C V3.0 / TRCV_C V3.0**
  Bloques compactos para:
  - Establecimiento/interrupción de conexión y envío de datos
  - Establecimiento/interrupción de conexión y recepción de datos

Utilice de forma alternativa:

- **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
  Para la transferencia de correos electrónicos cifrados con este bloque es necesario que el módulo tenga la hora exacta. Configure la sincronización horaria.

Nota

Datos personales sin cifrar en TMAIL_C

Tenga en cuenta que TMAIL_C utiliza datos personales en sus parámetros, como nombre de usuario y contraseña. Estos datos se depositan sin cifrar en un bloque de datos.

Para cambiar los datos de configuración del módulo en tiempo de ejecución:

- **T_CONFIG V1.0**
  Configuración de los parámetros IP controlada por programa
  Observe las indicaciones sobre T_CONFIG y los SDT "IF_CONF_..." en el capítulo Modificación de la dirección IP en tiempo de ejecución (Página 199).

  Nota

  Sin retroalimentación del CP

  "T_CONFIG" no soporta la retroalimentación del CP a la CPU. Los errores en la llamada de bloque o al activar el parámetro de dirección no se notifican. Tanto si el parámetro de dirección se ha activado como si no, el bloque devuelve "BUSY" o "DONE".

  Los parámetros de dirección solo pueden configurarse con una validez temporal. En el correspondiente SDT "IF_CONF_..." debe activarse el parámetro "Mode" = 2.

- **TC_CONFIG**
  Cambio controlado por programa en los datos de configuración de los CP de telefonía móvil

Los bloques de programa se encuentran en la Task Card "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. TMAIL_C utiliza el parámetro MAIL_ADDR_PARAM.

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

Para cada descripción de conexión, cree el SDT necesario como bloque de datos (DB global).

El tipo SDT se genera introduciendo manualmente el nombre, por ejemplo "TCON_IP_V4", 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.

SDT empleables

- **TCON_IP_V4**
  Para la transferencia de telegramas vía TCP o UDP
- **TCON_QDN**
  Para la comunicación TCP o UDP mediante el nombre de dominio plenamente cualificado (FQDN) (IPv4 / IPv6)
- **TCON_IP_RFC**
  Para la transferencia de telegramas vía ISO-on-TCP (comunicación directa entre dos estaciones S7)
- **TADDR_Param**
  Para la transferencia de telegramas vía UDP

- **TMail_V4**
  Para la transferencia de correos electrónicos con direccionamiento del servidor de correo electrónico a través de una dirección IPv4
  Recomendación para aplicaciones de telefonía móvil:
  Ponga el parámetro "WatchdogTime" de "MAIL_ADDR_PARAM" a un valor mayor que 3 minutos.
- **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 de su nombre (FQDN)
- **IF_CONF**
  Para el cambio de los datos de configuración de los CP de telefonía móvil por medio de TC_CONFIG
- **TCON_IP_V4_SEC**
  Solo CP 1200
  Para la transferencia segura de datos a través de TCP
- **TCON_QDN_SEC**
  Solo CP 1200
  Para la transferencia segura de datos a través del nombre de host
- **TMail_V4_SEC**
  Para la transferencia segura de correos electrónicos con direccionamiento del servidor de correo electrónico a través de una dirección IPv4
- **TMail_V6_SEC**
  Para la transferencia segura de correos electrónicos con direccionamiento del servidor de correo electrónico a través de una dirección IPv6
- **TMail_QDN_SEC**
  Para la transferencia segura de correos electrónicos con direccionamiento del servidor de correo electrónico a través del nombre de host

Nota sobre TMail_Vx_SEC / TMail_QDN_SEC:
En estos SDT se comprueba el certificado del servidor de correo, pero no la ID del certificado "TLSServerCertRef" (referencia interna de STEP 7).

Encontrará la descripción de los SDTs con sus parámetros en el sistema de información de STEP 7, bajo el respectivo nombre.

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 parametrización.

A.3 Modificación de la dirección IP en tiempo de ejecución

Modificación de la dirección IP en tiempo de ejecución

Los siguientes parámetros de dirección del CP pueden modificarse en tiempo de ejecución mediante control por programa:

- Dirección IP
- Máscara de subred
- Dirección del router

Aparte de los parámetros de dirección del CP, con T_CONFIG también es posible modificar con control por programa los datos de dirección de servidores DNS (IF_CONF_DNS) y servidores NTP (IF_CONF_NTP).

Nota

Modificación de los parámetros IP con dirección IP dinámica

Tenga en cuenta las repercusiones de la modificación controlada por programa de los parámetros IP en caso de que el CP obtenga una dirección IP dinámica del router conectado: En este caso no es posible acceder al CP desde interlocutores de la comunicación.

Requisitos - Configuración

Para poder modificar los parámetros IP con control por programa, en la configuración de la dirección IP de la interfaz Ethernet del CP debe estar activada la opción "Permitir ajustar la dirección IP directamente en el dispositivo".

Requisitos - Versión de STEP 7

- STEP 7 ≥ V14

Requisitos - Versiones de firmware

- **CP 1243-1 / CP 1243-8 IRC**
  - Firmware del CP ≥ V2.1.7x
  - Firmware de la CPU ≥ V4.2
- **CP 1542SP-1 IRC**
  - Firmware del CP ≥ V1
  - Firmware de la CPU ≥ V2.0 (CPU 151xSP)

Bloques de programa

La modificación controlada por programa de los parámetros IP es soportada por bloques de programa. Los bloques de programa acceden a datos de dirección almacenados en un tipo de datos de sistema (SDT) adecuado.

Es posible utilizar los siguientes bloques de programa y tipos de datos de sistema:

- **T_CONFIG**
  Junto con:
  - IF_CONF_V4
  - IF_CONF_NTP
  - IF_CONF_V6
  - IF_CONF_DNS

  Los parámetros de dirección solo pueden configurarse en el CP con una validez temporal. En el correspondiente SDT "IF_CONF_..." debe activarse el parámetro "Mode" = 2.

Nota

Sin retroalimentación del CP

"T_CONFIG" no soporta la retroalimentación del CP a la CPU. Los errores en la llamada de bloque o al activar el parámetro de dirección no se notifican. Tanto si el parámetro de dirección se ha activado como si no, el bloque devuelve "BUSY" o "DONE".

Encontrará información detallada sobre la parametrización de los bloques y SDT en el sistema de información de STEP 7.

A.4 SMS vía OUC

Envío de correos electrónicos / SMS vía OUC

Con CP de telefonía móvil, los bloques de programa y tipos de datos de sistema (SDT) descritos a continuación solo son necesarios para transferir SMS por medio de Open User Communication (OUC).

En cambio, el envío controlado por eventos de correos electrónicos o SMS es independiente de los bloques de programa y se configura en el editor de mensajes de STEP 7 del respectivo módulo.

Nota

Transmisión frecuente de SMS

La transmisión de un SMS puede tardar hasta 2 minutos, según sea el entorno del sistema.

Para garantizar una transmisión segura de SMS, se recomienda mantener una distancia mínima de 10 segundos entre disparos de SMS.

Esto puede controlarse, por ejemplo, estableciendo el parámetro "REC" en los bloques TCON y TSEND_C.

SMS vía bloques de programa

Enviar SMS a un interlocutor

Para tal fin deben crearse los siguientes bloques y tipos de datos de sistema, alternativamente:

- TCON + TDISCON + TSEND + TCON_Phone
- TSEND_C + TCON_Phone

Recibir SMS de un interlocutor

Para tal fin deben crearse los siguientes bloques y tipos de datos de sistema, alternativamente:

- TCON + TDISCON + TRCV + TCON_Phone
- TRCV_C + TCON_Phone

Si en el parámetro "PhoneNumber" del tipo de datos de sistema TCON_Phone no se parametrizan números de abonado, el CP no puede recibir SMS.

Recibir SMS de varios interlocutores

También existe la posibilidad alternativa de crear un juego de bloques separado para cada interlocutor, tal como se describe arriba para 1 interlocutor, o bien crear un solo juego de bloques con la particularidad siguiente en el bloque TCON_PHONE:

Si en el parámetro "PhoneNumber" del bloque TCON_Phone se introduce un asterisco (*) después del cuerpo del número de teléfono, dicho asterisco actúa de comodín para todos los números autorizados con el mismo cuerpo.

Los números de teléfono autorizados para acceder al CP se configuran en el grupo de parámetros "Security" del CP en STEP 7.

Texto del mensaje que se enviará en el parámetro "DATA"

El texto del mensaje se introduce como string en el parámetro "DATA" de TSEND o TSEND_C.

Un mensaje puede contener 160 caracteres como máximo. Si el texto del mensaje contiene más de 160 caracteres, se repartirá entre dos o más SMS.

Leer el texto del mensaje en el parámetro "DATA"

Para recibir un SMS, parametrice el texto del mensaje que se leerá en los bloques TRCV / TRCV_C con el parámetro "DATA", utilizando un bloque de datos (DB).

Cree un DB del tipo de datos "Struct". Abra el cuadro de diálogo de propiedades del DB (menú contextual del DB) y desactive en el grupo de parámetros "Atributos" el acceso optimizado al bloque.

En la estructura del DB, cree para los SMS los tipos de datos siguientes:

- DTL
  12 bytes para el sello de tiempo de los SMS recibidos (sello de tiempo de la red)
- String[22]
  String de 22 bytes para el número de teléfono del remitente (+ 2 bytes para el encabezado del string)
- String[160]
  String de 160 bytes para el texto del mensaje (+ 2 bytes para el encabezado del string)
  El texto del SMS puede tener como máximo 160 caracteres.

La estructura necesita 198 bytes de memoria por cada SMS.

Guardar los 10 últimos SMS recibidos

Es posible emitir un máximo de 10 SMS recibidos del bloque de recepción introduciendo la entrada "SMSSTORE" en el parámetro "PhoneNumber" de TCON_PHONE.

Para guardar los datos de recepción de 10 SMS es necesario crear para el parámetro "DATA" del bloque de recepción una estructura suficientemente grande (2000 bytes). Como se ha descrito anteriormente, la estructura es como sigue:

- Datos recibidos del SMS 1 (DTL, String[22], String[160], Byte)
- Datos recibidos del SMS 2 (DTL, String[22], String[160], Byte)
  ... hasta
- Datos recibidos del SMS 10 (DTL, String[22], String[160], Byte)

Los datos recibidos de cada SMS tienen la estructura siguiente:

- DTL
  12 bytes para el sello de tiempo de los SMS recibidos (sello de tiempo de la red)
- String[22]
  String de 22 bytes para el número de teléfono del remitente (+ 2 bytes para el encabezado del string)
- String[160]
  String de 160 bytes para el texto del mensaje (+ 2 bytes para el encabezado del string)
- Byte
  Estado del SMS
  Si se recibe más de un SMS, el estado de cada SMS se guarda en este byte de estado:
  - 0 = no válido
    1 = no leído
    2 = leído

En caso de recibir varios SMS, la estructura necesita 200 bytes de memoria por cada SMS.

Datos de longitud en "LEN" y "DATA" con bloques "TRCV" / "TRCV_C"

Si en la recepción de SMS se indica la longitud a través de los bloques TRCV o "TRCV_C" en el parámetro "LEN", puede producirse información falsa en el almacenamiento de datos de la información recibida.

Recomendación: Ajuste LEN = 0 e indique la longitud en el parámetro "DATA".

Juego de caracteres para el texto del SMS

El CP soporta el siguiente juego de caracteres ASCII (valor hexadecimal y nombre de carácter) para textos de SMS que se envían a través de bloques de programa:

- 0x0A
  LF (salto de línea)
- 0x0D
  CR (Carriage Return)
- 0x20
  Espacio
- 0x21 ... 0x5A
  ! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
- 0x61 ... 0x7A
  a b c d e f g h i j k l m n o p q r s t u v w x y z

A.5 TC_CONFIG para cambiar los datos de configuración del CP

Significado

El bloque de programa TC_CONFIG permite modificar los parámetros del CP de telefonía móvil configurados en STEP 7. Los valores configurados no se sobrescriben de forma remanente. Los valores sobrescritos siguen siendo válidos hasta una nueva llamada de TC_CONFIG o hasta el siguiente arranque de la estación (arranque en frío mediante la tensión OFF → ON).

Si los datos de configuración del CP en STEP 7 deben modificarse permanentemente, entonces el bloque debe llamarse de nuevo después de cada arranque de la estación (arranque en frío) o se debe cargar un proyecto modificado en la estación.

El parámetro CONFIG hace referencia al área de memoria con los datos de configuración. Los datos de configuración se guardan en un bloque de datos (DB). No es posible crear el DB con acceso optimizado al bloque. La estructura del DB está predeterminada por el tipo de datos de sistema (SDT) IF_CONF_v4.

Los datos de configuración que deben modificarse en el CP se compilan en el SDT como bloques "IF_CONF_..." para los diferentes parámetros, según sea necesario.

Los parámetros que no deben modificarse con el bloque no se introducen en el SDT. Estos conservan el valor configurado en STEP 7.

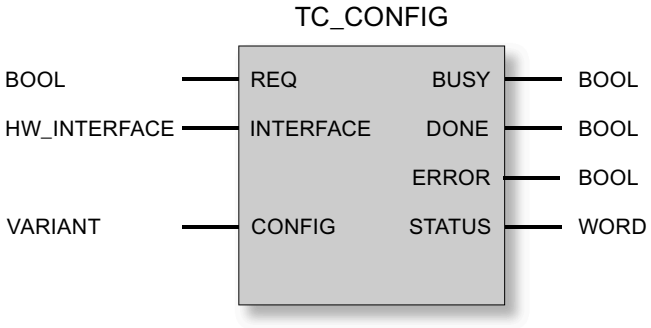
Encontrará información detallada sobre la parametrización del SDT IF_CONF_v4 en el apartado IF_CONF_*: SDT para datos de configuración del CP (Página 206).

El parámetro INTERFACE referencia el nombre de la interfaz GPRS del CP de telefonía móvil. El nombre de la interfaz figura en el proyecto de STEP 7, en la tabla de variables estándar de la estación, en la ficha "Constantes del sistema" bajo la entrada que contiene el valor de la "ID de hardware" del CP.

Requisitos

- Para poder utilizar esta función, en la configuración básica del CP en STEP 7 debe haber valores configurados.
- Para utilizar el bloque de parámetros "IF_CONF_PrefProvider" (redes de telefonía móvil preferentes) del SDT "IF_CONF_v4":
  La red de telefonía móvil que se utilizará debe ajustarse del siguiente modo en la configuración del CP:
  "Ajustes de comunicación de telefonía móvil > Lista de las redes preferentes":
  "Red de telefonía móvil preferente" = "Red contractual y redes alternativas"

Interfaz de llamada en representación FUP



Explicación de los parámetros formales

La tabla siguiente muestra los parámetros formales de la instrucción TC_CONFIG.

Parámetro	Declaración	Tipo de datos	Rango de valores	Descripción
REQ	INPUT	BOOL	0, 1	Con un flanco ascendente se inicia el procesamiento del bloque y se inicializan los indicadores de estado. Actualización de los indicadores de estado DONE, ERROR y STATUS cuando no hay ningún flanco ascendente.
INTERFACE	INPUT	HW_Interface (WORD)		Referencia a la interfaz del CP local
CONFIG	INOUT	VARIANT	Véase también "IF_CONF: SDT para datos de configuración de Telecontrol"	Referencia al área de memoria con la compilación de los datos de configuración que deben modificarse
ENO	OUTPUT	BOOL	0: error 1: correcto	Salida de habilitación Si la instrucción presenta un error en el tiempo de ejecución, se pondrá ENO = 0.

Parámetro	Declaración	Tipo de datos	Rango de valores	Descripción
BUSY	OUTPUT	BOOL	0: procesamiento de la instrucción todavía no iniciado, finalizado o cancelado 1: procesamiento de la instrucción en curso	Indicador del estado de procesamiento del bloque
DONE	OUTPUT	BOOL	0: - 1: procesamiento de la instrucción finalizado correctamente	El parámetro de estado indica si la petición se ha desarrollado correctamente. Consulte el significado en relación con los parámetros ERROR y STATUS en Indicadores del bloque.
ERROR	OUTPUT	BOOL	0: - 1: error	Indicador de error Consulte el significado en relación con los parámetros DONE y STATUS en Indicadores del bloque.
STATUS	OUTPUT	WORD		Indicador de estado Consulte el significado en relación con los parámetros DONE y ERROR en Indicadores del bloque.

Indicadores BUSY, DONE y ERROR

Los indicadores DONE y ERROR solo son relevantes si BUSY = 0.

BUSY	DONE	ERROR	Significado
0	0	0	Ninguna petición en proceso

Encontrará todas las demás combinaciones de los indicadores DONE y ERROR en la tabla siguiente.

Indicadores DONE, ERROR y STATUS

La tabla siguiente informa sobre la indicación a evaluar por el programa de usuario, formada por DONE, ERROR y STATUS.

DONE	ERROR	STATUS	Significado
1	0	0000_H	Petición ejecutada correctamente
0	0	7000_H	No se está procesando ninguna petición (primera llamada del bloque)
0	0	7001_H	Procesamiento de petición iniciado (primera llamada del bloque)
0	0	7002_H	Petición en proceso (nueva llamada del bloque si BUSY = 1)
0	1	$80E0_H$	Error interno
0	1	$80E6_H$	No se está procesando ninguna petición (llamada del bloque no iniciada)
0	1	$80EB_H$	Solicitud rechazada temporalmente (el CP es configurado momentáneamente por STEP 7).
0	1	$80F6_H$	Error de formato de un parámetro en el bloque de datos llamado (tamaño erróneo, formato incorrecto o valor no válido) Compruebe el SDT "IF_CONF".
0	1	$80F7_H$	ID incorrecta en los bloques de parámetros de los datos de configuración: Compruebe el SDT "IF_CONF".

A.6 IF_CONF_*: SDT para datos de configuración del CP

Estructura del DB IF_CONF para el bloque de programa TC_CONFIG

El parámetro CONFIG del bloque de programa TC_CONFIG referencia el área de memoria con los datos de configuración del CP de telefonía móvil que deben modificarse. Los datos de configuración almacenados en un bloque de datos se describen como estructura del tipo de datos del sistema (SDT) IF_CONF_*.

Para poder utilizar esta función, en la configuración básica del CP en STEP 7 debe haber valores configurados.

El DB IF_CONF está formado por un encabezado y los bloques siguientes, correspondientes a los parámetros de la configuración del CP.

Los datos de configuración del CP que deben modificarse se compilan a modo de bloques IF_CONF. Los parámetros que no deben modificarse no se tienen en cuenta en la estructura de IF_CONF y se quedan tal como se han configurado en el proyecto de STEP 7.

Creación de un DB y de las estructuras IF_CONF

Los parámetros del CP los puede crear dentro del DB IF_CONF en una o más estructuras y cada una con uno o más bloques.

Los tipos de datos de cada bloque deben introducirse con el teclado. No se muestran en la lista de selección. No se tienen en cuenta las mayúsculas/minúsculas al introducir los tipos de datos.

Proceda del siguiente modo para crear el DB IF_CONF:

1. Cree un bloque de datos del tipo "DB global" con acceso al bloque "estándar".
2. Cree una estructura en la tabla de la configuración del parámetro del DB (tipo de datos "Struct").
   Puede determinar el nombre libremente.
3. Inserte un encabezado en esta estructura asignando el nombre del encabezado e introduciéndolo en la celda del tipo de datos "IF_CONF_Header".
   Se crea el encabezado de la estructura con sus tres parámetros (ver abajo).
4. Cree una estructura adicional para el primer parámetro que debe modificarse introduciendo el tipo de datos deseado (por ejemplo, "IF_CONF_APN") en la celda del tipo de datos.
5. Repita el último paso para todos aquellos parámetros que desee modificar con ayuda de la TC_CONFIG en el CP.
6. A continuación actualice en el encabezado el número de bloques en el parámetro "subfieldCnt".

Encabezado de IF_CONF

Tabla A-1 IF_CONF_Header

Byte	Parámetro	Tipo de datos	Valor inicial	Descripción
0 ... 1	fieldType	UINT		Tipo de bloque: tiene que ser siempre 0.
2 ... 3	fieldId	UINT		ID de bloque: tiene que ser siempre 0.
4 ... 5	subfieldCnt	UINT		Número total de bloques incluidos en el DB (estructuras) para los parámetros que deben modificarse

Parámetros generales de los bloques de parámetros

Cada bloque contiene los siguientes parámetros generales:

- Id
  Este parámetro identifica el bloque correspondiente y no puede modificarse.
- Length
  Este parámetro indica el tamaño del bloque. El valor solo sirve para fines informativos. Los bloques que contienen strings y/o arrays tienen una longitud variable. Debido a los bytes ocultos, la longitud real de los bloques puede ser mayor que la suma de los parámetros mostrados.
- Mode
  Para este parámetro se admiten los valores siguientes:

Tabla A-2 Valores de "Mode"

Valor	Significado
1	Validez permanente de los datos de configuración Irrelevante en el CP
2	Validez temporal de los datos de configuración, inclusive el borrado de los datos de configuración permanentes existentes Los datos de configuración permanentes se reemplazan por las estructuras parametrizadas en el bloque.

"Ajustes APN"

Grupo de parámetros correspondiente en la configuración:
"Ajustes de comunicación de telefonía móvil > Ajustes APN"

Tabla A-3 IF_CONF_APN

Parámetro	Tipo de datos	Valor inicial	Descripción
Id	UINT	4	Identificación del bloque de parámetros
Length	UINT		Tamaño del bloque de parámetros en bytes: 174
Mode	UINT		Validez (1, 2) - véase arriba (parámetros generales)
AccesspointGPRS	STRING [98]		APN: Nombre del punto de acceso de la red de telefonía móvil para Internet

Parámetro	Tipo de datos	Valor inicial	Descripción
AccesspointUser	STRING [42]		Nombre de usuario APN
AccesspointPassword	STRING [22]		Contraseña APN

"Identificación CP"

Grupo de parámetros correspondiente en la configuración:
"Security > Identificación CP"

Tabla A-4 IF_CONF_Login

Parámetro	Tipo de datos	Valor inicial	Descripción
Id	UINT	5	Identificación del bloque de parámetros
Length	UINT		Tamaño del bloque de parámetros en bytes: 54
Mode	UINT		Validez (1, 2) - véase arriba (parámetros generales)
ModemName	STRING [22]		ID de acceso El valor no es parametrizable.
ModemPassword	STRING [22]		Contraseña de Telecontrol La contraseña del CP 1242-7 (6GK7 242-7KX30-0XE0) no puede cambiarse con el SDT.

"Servidor de Telecontrol" (DNS)

Grupo de parámetros correspondiente en la configuración:
"Estaciones interlocutoras > Servidor de Telecontrol"

Este bloque solo debe utilizarse si el servidor de Telecontrol se direcciona con un nombre que puede resolverse mediante DNS. Si el servidor de Telecontrol se direcciona con su dirección IP, se utilizará el bloque "IF_CONF_TCS_IP_V4".

Si hay varios servidores de Telecontrol, utilice el bloque una vez por servidor.

Tabla A-5 IF_CONF_TCS_Name

Parámetro	Tipo de datos	Valor inicial	Descripción
Id	UINT	6	Identificación del bloque de parámetros
Length	UINT		Tamaño del bloque de parámetros en bytes: 266
Mode	UINT		Validez (1, 2) - véase arriba (parámetros generales)
TcsName	-	-	- reservado -
	STRING [254]		Nombre resoluble por DNS del servidor de Telecontrol o dirección IP como string
RemotePort	UINT		Puerto del servidor Telecontrol
Rank	UINT		Prioridad del servidor [1, 2] 1 = primer servidor de Telecontrol, 2 = segundo servidor de Telecontrol (segundo servidor irrelevante)

"SMSC"

Grupo de parámetros correspondiente en la configuración:
"Ajustes de comunicación de telefonía móvil > Ajustes de telefonía móvil"

Tabla A-6 IF_CONF_SMS_Provider

Parámetro	Tipo de datos	Valor inicial	Descripción
Id	UINT	10	Identificación del bloque de parámetros
Length	UINT		Tamaño del bloque de parámetros en bytes: 28
Mode	UINT		Validez (1, 2) - véase arriba (parámetros generales)
SMSProvider	STRING [20]		Número de dispositivo de la central de SMS (SMSC) correspondiente al operador de la red de telefonía móvil con el que se firmó el contrato de telefonía móvil para esta estación.

"PIN"

Grupo de parámetros correspondiente en la configuración:
"Ajustes de comunicación de telefonía móvil > Ajustes de telefonía móvil"

Tabla A-7 IF_CONF_PIN

Parámetro	Tipo de datos	Valor inicial	Descripción
Id	UINT	11	Identificación del bloque de parámetros
Length	UINT		Tamaño del bloque de parámetros en bytes: 16
Mode	UINT		Validez (1, 2) - véase arriba (parámetros generales)
Pin	STRING [8]		PIN de la tarjeta SIM insertada en el CP Este parámetro no es relevante si se ha configurado el PIN correctamente. En caso de haber configurado el PIN erróneamente, el PIN correcto puede introducirse aquí.

"Número de llamada autorizado"

Grupo de parámetros correspondiente en la configuración:
"Security > Números de abonado autorizados"

Tabla A-8 IF_CONF_WakeupList

Parámetro	Tipo de datos	Valor inicial	Descripción
Id	UINT	13	Identificación del bloque de parámetros
Length	UINT		Tamaño del bloque de parámetros en bytes: 246
Mode	UINT		Validez (1, 2) - véase arriba (parámetros generales)
WakeupPhone [1...10]	ARRAY [1...10] of STRING [22]		Número de llamada del dispositivo autorizado como despertador El asterisco (*) al final de un número de abonado sirve de comodín para números con extensiones.

"Redes de telefonía móvil preferentes"

Grupo de parámetros correspondiente en la configuración:
"Ajustes de comunicación de telefonía móvil > Lista de las redes preferentes"

Requisitos:
La red de telefonía móvil que se utilizará debe ajustarse del siguiente modo en la configuración del CP:

"Ajustes de comunicación de telefonía móvil > Lista de las redes preferentes":
"Red de telefonía móvil preferente" = "Red contractual y redes alternativas"

Tabla A-9 IF_CONF_PrefProvider

Parámetro	Tipo de datos	Valor inicial	Descripción
Id	UINT	14	Identificación del bloque de parámetros
Length	UINT		Tamaño del bloque de parámetros en bytes: 46
Mode	UINT		Validez (1, 2) - véase arriba (parámetros generales)
Provider [1...5]	ARRAY [1...5] of STRING [6]		Parámetro "Red contractual y redes alternativas" 1.ª a 5.ª red de telefonía móvil preferente a la que puede conectarse el CP aparte de la red contractual. La n.° 1 tiene la máxima prioridad y la n.° 5 la mínima. Entrada del Public Land Mobile Network (PLMN) del operador de red, consistente en Mobile Country Code (MCC) y Mobile Network Code (MNC). Ejemplo (red de pruebas de Siemens AG): 26276

Acceso de TeleService (nombre DNS / dirección IP del servidor)

Grupo de parámetros correspondiente en la configuración:
"Ajustes de comunicación de telefonía móvil > Ajustes de TeleService"

Datos de acceso del servidor de TeleService (centralita). Si hay dos servidores de TeleService, utilice el bloque una vez por servidor.

Con IF_CONF_TS_Name es posible modificar un servidor de TeleService configurado en STEP 7, pero no crear uno nuevo. Cuando se intenta crear la configuración de un servidor de TeleService con el bloque se emite el error interno 80E0 en TC_CONFIG.

Tabla A-10 IF_CONF_TS_Name

Parámetro	Tipo de datos	Valor inicial	Descripción
Id	UINT	20	Identificación del bloque de parámetros
Length	UINT		Tamaño del bloque de parámetros en bytes: 266
Mode	UINT		Validez (1, 2) - véase arriba (parámetros generales)
ts_name	String [254]		Nombre resoluble por DNS del servidor de TeleService o dirección IP como string
RemotePort	UINT		Puerto de la estación de ingeniería
Rank	UINT		Prioridad del servidor [1] o [2]: • 1 = servidor 1 • 2 = servidor 2 (irrelevante)

Acceso de TeleService (dirección IP del servidor)

Dirección IP del servidor de TeleService. No puede utilizarse a partir de la versión de firmware V2.1 del CP.

Si hay dos servidores de TeleService, utilice el bloque una vez por servidor.

Tabla A-11 IF_CONF_TS_IF_V4

Parámetro	Tipo de datos	Valor inicial	Descripción
Id	UINT	21	Identificación del bloque de parámetros
Length	UINT		Tamaño del bloque de parámetros en bytes: 14
Mode	UINT		Validez (1: permanente, 2: temporal)
RemoteAddress	IP_V4		Dirección IP del servidor de TeleService
RemotePort	UINT		Puerto del servidor de TeleService
Rank	UINT		Prioridad del servidor [1] o [2] 1 = servidor 1, 2 = servidor 2

SINEMA Remote Connect (CP)

B

B.1 Validez y requisitos

Validez

La comunicación vía SINEMA Remote Connect es soportada por los módulos siguientes:

- CP 1243-1
  - Firmware V3.1 o superior
- CP 1243-7 LTE
  - Firmware V3.1 o superior
- CP 1243-8 IRC
  - Firmware V3.1 o superior
  - Con ST7 como estación MSC a partir del firmware V3.2
- CP 1542SP-1 IRC
  - Firmware V2.0 o superior
  - Con ST7 como estación MSC a partir del firmware V2.1

Las funciones son soportadas por las siguientes versiones de software:

- SINEMA Remote Connect
  - Versión de software V1.3 o superior

B.2 Conexión a SINEMA RC

Comunicación vía SINEMA Remote Connect (SINEMA RC)

La aplicación "SINEMA RC Server" ofrece una gestión de conexiones global de redes distribuidas a través de Internet. Eso incluye también el acceso remoto seguro a estaciones subordinadas. La comunicación entre el servidor SINEMA RC y los dispositivos remotos se desarrolla a través de túneles VPN en función de los derechos de acceso especificados.

SINEMA RC utiliza OpenVPN para el cifrado de datos. El centro de la comunicación es el servidor SINEMA RC, por el que transcurre la comunicación entre los dispositivos y que administra la configuración del sistema de comunicación.

Los routers SCALANCE M que pueden utilizarse para la conexión también soportan OpenVPN y la conexión a SINEMA Remote Connect.

El CP también puede procesar la comunicación por Telecontrol a través del servidor SINEMA RC.

Grupos de parámetros

La configuración de la comunicación vía SINEMA RC y de la comunicación por Telecontrol vía SINEMA RC se configura en dos grupos de parámetros:

- Comunicación vía SINEMA RC:
  > "Security > VPN"
- Comunicación por Telecontrol vía SINEMA RC:
  > "Tipos de comunicación"
  Consulte los protocolos soportados y la configuración en el capítulo Telecontrol vía SINEMA RC (Página 215).

Aplicaciones

De la combinación de parámetros para la comunicación por Telecontrol y SINEMA RC resultan las siguientes posibilidades de aplicación del CP:

- (1) No se utiliza Telecontrol ni SINEMA RC (CP solo para separar redes)
- (2) CP solo para telemantenimiento vía SINEMA RC
- (3) CP solo para comunicación por Telecontrol
- (4) El CP utiliza la comunicación por Telecontrol, pero SINEMA RC solo para telemantenimiento.
- (5) El CP utiliza SINEMA RC para la comunicación por Telecontrol y el telemantenimiento.

La tabla proporciona una sinopsis de los casos de aplicación con los ajustes de parámetros correspondientes.

- "Activado" significa que el parámetro está activado.
- "Desactivado" significa que el parámetro está desactivado.

Tabla B-1 Casos de aplicación y parámetros que deben activarse

Caso de aplicación	Ajustes de parámetros (parámetros abreviados) *		
	SRC	TC	TC-SRC
(1)	Desactivado	Desactivado	Desactivado
(2)	Activado	Desactivado	Desactivado
(3)	Desactivado	Activado	Desactivado
(4)	Activado	Activado	Desactivado
(5)	Activado	Activado	Activado

***** Significado de las abreviaturas de los parámetros:

SRC - Security > VPN (activado) > "Tipo de conexión VPN":
"Configuración OpenVPN automática a través de SINEMA Remote Connect Server"

TC - Tipos de comunicación > Comunicación por Telecontrol activada

TC-SRC - Tipos de comunicación >
"Activar la comunicación de Telecontrol a través de SINEMA Remote Connect"

B.3 Telecontrol vía SINEMA RC

Consulte las posibilidades de uso de la comunicación con SINEMA Remote Connect en el capítulo Conexión a SINEMA RC (Página 213).

Requisitos

Antes de configurar el CP en STEP 7, realice la configuración necesaria de SINEMA Remote Connect - Server (no en STEP 7). El CP y su interlocutor de la comunicación deben configurarse en el servidor SINEMA RC.

Configuración de la comunicación por Telecontrol vía SINEMA Remote Connect

Para configurar el módulo de forma que pueda utilizar la comunicación por Telecontrol vía SINEMA RC, proceda del siguiente modo:

1. En el grupo de parámetros "Tipos de comunicación" active la comunicación por Telecontrol y seleccione el protocolo.
   La opción de comunicación vía SINEMA RC todavía no es visible.
2. Cambie al grupo de parámetros "Security" y active las funciones de seguridad.
   (En el grupo de parámetros "Tipos de comunicación", la opción SINEMA RC aparece desactivada y atenuada.)
3. Abra el grupo de parámetros "Security > VPN" y active VPN.
4. En el parámetro "Tipo de conexión VPN" elija la opción "Configuración OpenVPN automática a través de SINEMA Remote Connect Server" si todavía no está seleccionada.
   (En el grupo de parámetros "Tipos de comunicación", la opción SINEMA RC se vuelve operativa.)
5. Cambie al grupo de parámetros "Tipos de comunicación" y active la opción "Activar la comunicación de Telecontrol a través de SINEMA Remote Connect".
6. Siga configurando la conexión SINEMA RC del CP en "Security > VPN".
   Consulte la configuración en el capítulo Security > VPN > SINEMA Remote Connect (Página 215).

B.4 Security > VPN > SINEMA Remote Connect

Telemantenimiento con SINEMA Remote Connect (SINEMA RC)

La aplicación "SINEMA Remote Connect" (SINEMA RC) sirve para fines de telemantenimiento.

SINEMA RC utiliza OpenVPN para el cifrado de datos. El centro de la comunicación es el servidor SINEMA RC, por el que transcurre la comunicación entre los dispositivos y que administra la configuración del sistema de comunicación.

Preparativos

Ejecute los pasos siguientes antes de iniciar la configuración de la conexión SINEMA RC para el módulo en STEP 7. Son imprescindibles para obtener un proyecto de STEP 7 coherente.

- Configuración de SINEMA Remote Connect Server
  Realice la configuración necesaria de SINEMA RC Server (no en STEP 7). El módulo de comunicación y sus interlocutores deben configurarse en el servidor SINEMA RC.
- Exportación del certificado CA (opcional)
  Si como método de autenticación del módulo de comunicación desea utilizar el certificado del servidor a la hora de establecer la conexión, exporte el certificado CA de SINEMA RC Server.
  Seguidamente, importe el certificado CA de SINEMA RC Server a la estación de ingeniería.
  Otra posibilidad consiste en utilizar como método de autenticación del módulo de comunicación la huella del certificado de servidor. El periodo de validez de la huella puede ser inferior al del certificado.
  Tenga en cuenta que, en caso de reemplazar el módulo, tendrá que repetir la importación del certificado.

Configuración de SINEMA Remote Connect

Importación del certificado propio

1. Navegue por el CP hasta el grupo de parámetros "Security > Administrador de certificados > Certificados de los dispositivos interlocutores".
2. Abra el cuadro de diálogo para seleccionar el certificado haciendo doble clic en la primera fila libre de la tabla.
3. Seleccione el certificado CA de SINEMA RC Server.

A continuación, navegue hasta el grupo de parámetros "Security > VPN".

VPN > General

1. Active VPN.
2. En "Tipo de conexión VPN" elija la opción "Configuración OpenVPN automática a través de SINEMA Remote Connect Server" si desea utilizar la comunicación vía SINEMA Remote Connect.

Servidor SINEMA Remote Connect

Introduzca la dirección y el número de puerto del servidor.

Comprobación de servidor

Seleccione aquí el método de autentificación del módulo de comunicación al establecer la conexión.

- Certificado CA
  En "Certificado CA" seleccione el certificado CA de SINEMA RC Server que se ha importado previamente y se ha asignado en el administrador local de certificados.
  El módulo comprueba básicamente el certificado CA del servidor y su validez. Las dos opciones no pueden modificarse.
- Huella
  Si se elige este método de autenticación hay que introducir la huella del certificado de servidor de SINEMA RC Server.

Autenticación

- ID del dispositivo
  Introduzca la ID de dispositivo generada en SINEMA RC para el módulo.
- Contraseña de dispositivo
  Introduzca la contraseña de dispositivo configurada en SINEMA RC para el módulo.
  Número máx. de caracteres: 127

Ajustes opcionales

El establecimiento de la conexión se configura con el parámetro "Tipo de conexión" en el grupo de parámetros "Security > VPN > Ajustes opcionales".

- **Intervalo de actualización**
  Mediante este parámetro se ajusta el intervalo en el que el CP consulta la configuración al servidor SINEMA RC.
  Con el ajuste 0 (cero), tenga en cuenta que los cambios en la configuración del servidor SINEMA RC pueden tener como consecuencia que el CP no pueda establecer más conexiones con el servidor SINEMA RC.
- **"Tipo de conexión"**
  Las dos opciones del parámetro tienen la repercusión siguiente en el establecimiento de la conexión:
  - Automático
    El módulo establece una conexión con el servidor SINEMA RC. La conexión OpenVPN se mantiene hasta que el servidor SINEMA Remote Connect cambia los parámetros de conexión. En caso de que se cancele la conexión, el CP la restablece automáticamente. Si el servidor SINEMA Remote Connect cambia los parámetros de conexión, el CP consulte los nuevos datos de conexión una vez transcurrido el intervalo de actualización configurado anteriormente.
  - Disparo de PLC
    Esta opción está prevista para la comunicación esporádica del módulo a través del servidor SINEMA RC.
    La opción puede utilizarse cuando deben establecerse conexiones temporales entre el módulo y un PC. Las conexiones temporales se establecen por medio de una variable PLC y pueden utilizarse para casos de servicio técnico, por ejemplo.

Nota

Cancelación de la conexión

En caso de STOP de la CPU, por ejemplo debido a una actualización de firmware o al "Cargar en dispositivo", se cancela la conexión OpenVPN.

Estas funciones solo pueden utilizarse si se activa la opción "Automático".

- **Variable PLC para establecimiento de conexión**
  Si está seleccionada la opción "Disparo de PLC", el módulo establece una conexión cuando la variable PLC (Bool) adopta el valor 1. Durante el funcionamiento es posible activar la variable PLC si fuera necesario, por ejemplo desde un panel HMI.
  Al poner la variable PLC de nuevo a 0 finaliza la conexión.

Bibliografía

C

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.

Encontrará otras fuentes de bibliografía en la bibliografía de los diferentes manuales de producto.

C.1 /1/ TeleControl Manuales de configuración

SIMATIC NET - TeleControl
Siemens AG
Manuales de configuración para los protocolos:
- TeleControl Basic
- SINAUT ST7
- DNP3
- IEC 60870-5
Enlace: (https://support.industry.siemens.com/cs/ww/es/ps/21764/man)

C.2 /2/ TIM 1531 IRC

SIMATIC NET
TIM 1531 IRC
Manual de producto
Siemens AG
Enlace: (https://support.industry.siemens.com/cs/ww/es/ps/24710/man)

C.3 /3/ CP 1243-1

SIMATIC NET
CP 1243-1
Instrucciones de servicio
Siemens AG
Enlace: (https://support.industry.siemens.com/cs/ww/es/view/103948898)

C.4 /4/ CP 1243-8 IRC

SIMATIC NET
CP 1243-8 IRC
Instrucciones de servicio
Siemens AG
Enlace: (https://support.industry.siemens.com/cs/ww/es/ps/21162/man)

C.5 /5/ CP 1243-7 LTE

SIMATIC NET
CP 1243-7 LTE
Instrucciones de servicio
Siemens AG
Enlace: (https://support.industry.siemens.com/cs/ww/es/ps/15924/man)

C.6 /6/ CP 1542SP-1, CP 1542SP-1 IRC, CP 1543SP-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)

C.7 /7/ S7-1200 Manual de sistema

SIMATIC
Controlador programable S7-1200
Manual de sistema
Siemens AG
Enlace: (http://support.automation.siemens.com/WW/view/es/34612486)

C.8 /8/ ET 200SP Manual de sistema

Sistema de periferia descentralizada SIMATIC
ET 200SP -
Manual de sistema
Siemens AG
Enlace: (http://support.automation.siemens.com/WW/view/es/58649293)

C.9 /9/ SNMP

SIMATIC NET
Diagnóstico y configuración con SNMP
Manual de diagnóstico
Siemens AG
Enlace: (https://support.industry.siemens.com/cs/ww/es/ps/15392/man)

C.10 /10/ Industrial Ethernet Manual de sistema

SIMATIC NET
Industrial Ethernet
Manual de sistema
Siemens AG

- Volumen 1: Industrial Ethernet
  Enlace: (https://support.industry.siemens.com/cs/ww/es/view/27069465)
- Volumen 2: Componentes pasivos de la red
  Enlace: (https://support.industry.siemens.com/cs/ww/es/view/84922825)

C.10 /10/ Industrial Ethernet Manual de sistema

Índice alfabético

T

V

W