

SIEMENS

SIMATIC NET

LOGO! - Industrial Ethernet LOGO! CMR2020, LOGO! CMR2040

Instrucciones de servicio

Prólogo

Aplicación y funciones

1

LED, conexiones,
pulsadores y slots para
tarjetas

2

Montaje, conexión, puesta
en marcha

3

Operación: Acceso al BM

4

Configuración (WBM)

5

Diagnóstico y mantenimiento

6

Croquis acotados

7

Datos técnicos

8

Homologaciones

9

Accesorios

A

Información complementaria
sobre SMS

B

Bibliografía

C

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

Exención de responsabilidad

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

Prólogo

Ámbito de validez de este manual

En este documento encontrará información acerca de los siguientes productos LOGO!:

- LOGO! CMR2020

Versión de hardware: a partir de la versión 1.0

Versión de firmware: V2.1

Referencia: 6GK7 142-7BX00-0AX0

Módulo de comunicación para la conexión de LOGO! 8 a la red GSM/GPRS (2G)

- LOGO! CMR2040

Versión de hardware: a partir de la versión 1.0

Versión de firmware: V2.1

Referencia: 6GK7 142-7EX00-0AX0

Módulo de comunicación para la conexión de LOGO! 8 a la red LTE (4G)



Figura 1 LOGO! CMR2020

Ambos dispositivos se diferencian por los estándares de telefonía móvil que soportan. Por lo demás, el volumen de funciones es el mismo en ambos dispositivos.

Designaciones de producto y abreviaturas

- CMR o dispositivo

En este documento también se utilizan en adelante las denominaciones "CMR" y "dispositivo" en vez del nombre completo del producto "LOGO! CMR2020" o "LOGO! CMR2040". CMR es la abreviatura de Communication Module Radio.

- BM o LOGO! BM

Módulo básico: LOGO! 8

- WBM

Web Based Management; interfaz web a través de la que se configura el CMR.

- Tarjeta SD

En adelante se utilizará la denominación "tarjeta SD" para designar una tarjeta micro SD.

Finalidad de este manual

El presente manual le ayuda a configurar, montar, poner en marcha y utilizar los módulos de comunicación LOGO! CMR2020 y LOGO! CMR2040.

Un ejemplo (Página 132) detallado ayuda al usuario en la puesta en marcha.

Novedades de la presente edición

- Detección de errores de e-mails
- Actualización de homologaciones radioeléctricas:

Enlace: (www.siemens.com/mobilenetwork-approvals)

Documentación sustituida

El presente manual sustituye a la edición 04/2019 del manual.

Versión actual del manual en Internet

Encontrará la edición actual de este manual en las páginas web de Siemens Industry Online Support en la dirección siguiente:

Enlace: (<https://support.industry.siemens.com/cs/ww/es/view/109477418>)

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>.

Documentación complementaria

En el apartado Bibliografía de este manual encontrará una lista de la bibliografía existente en torno al tema.

Uso del dispositivo

Conexión de un LOGO! BM a una red de telefonía móvil LTE, UMTS o GSM/GPRS y a un sistema GPS.

ADVERTENCIA

Problemas en dispositivos médicos y soportes de datos

El dispositivo contiene un emisor de radiofrecuencia que puede perturbar también el funcionamiento de dispositivos electrónicos médicos, como audífonos o marcapasos. No use el dispositivo en zonas en las que esté prohibido el uso de dispositivos de radiotransmisión. Su médico o el fabricante de tales dispositivos podrá asesorarle.

Para que no se desmagneticen los soportes de datos, no deposite disquetes, tarjetas de crédito ni otros soportes magnéticos de datos en las proximidades del dispositivo.

Consulte también

System time (Página 77)

Homologaciones (Página 157)

Condiciones de la licencia

Nota

Open Source Software

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

Las condiciones de la licencia para Open Source Software están depositadas en el dispositivo y pueden leerse desde el WBM. En el encabezado del WBM encontrará un símbolo que le permitirá guardar los textos de la licencia OSS en el PC para poder descomprimirlos y abrirlos a continuación.

Información de seguridad

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

Para proteger las instalaciones, los sistemas, las máquinas y las redes de amenazas cibernéticas, es necesario implementar (y mantener continuamente) un concepto de seguridad industrial integral que sea conforme a la tecnología más avanzada. Los productos y las soluciones de Siemens constituyen 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 seguridad industrial que podrían ser implementadas en el campo de la seguridad industrial, por favor visite:

Enlace: (<http://www.siemens.com/industrialsecurity>)

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

Para mantenerse informado acerca de las actualizaciones de productos, recomendamos que se suscriba al Siemens Industrial Security RSS Feed en la siguiente dirección:

Enlace: (<http://www.siemens.com/industrialsecurity>)

Reciclado y eliminación



El producto contiene pocas sustancias perjudiciales, es reciclable y cumple las exigencias de la directiva WEEE 2012/19/UE "Aparatos eléctricos y electrónicos".

No deseche el producto en puntos de gestión de residuos públicos. Para un reciclaje y eliminación de su aparato viejo compatible con el medio ambiente contacte con una empresa homologada para la eliminación de chatarra electrónica o con su representante de Siemens.

Observe las especificaciones locales.

Encontrará información sobre la devolución del producto en las páginas de Internet de Siemens Industry Online Support:

Enlace: (<https://support.industry.siemens.com/cs/ww/es/view/109479891>)

Marcas

Las siguientes denominaciones y otras no marcadas con el símbolo de protección legal ® son marcas registradas de Siemens AG:

SIMATIC NET

Glosario de SIMATIC NET

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

Encontrará el glosario de SIMATIC NET en la siguiente dirección de Internet:

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

Service & Support

Además de la documentación de productos, tiene a su disposición la completa plataforma online de Siemens Automation Customer Support, accesible a toda hora y desde cualquier lugar del mundo Encontrará las páginas de Service & Support en la siguiente dirección de Internet:

Enlace: (<https://support.industry.siemens.com/cs/ww/es/>)

Además de las novedades, allí encontrará la siguiente información:

- Información sobre productos, Support al producto, Applications & Tools
- Technical Forum
- Technical Support: pregunte a los expertos de Siemens
- Nuestra oferta de servicio:
 - Technical Consulting, soporte de ingeniería
 - Servicio in situ
 - Reparaciones y piezas de recambio
 - Mantenimiento, optimización, modernización y mucho más

Encontrará los datos de contacto en la siguiente dirección de Internet:

Enlace: (www.automation.siemens.com/partner)

SITRAIN - la oferta de formación de Siemens para automatización y soluciones industriales

SITRAIN comprende más de 300 cursillos diferentes que abarcan la gama completa de productos y sistemas de Siemens en el sector de automatización y accionamientos. Además de la oferta de cursillos tradicional, ofrecemos cursillos personalizados de formación permanente así como una combinación de distintos medios de aprendizaje y secuencias como, por ejemplo, programas autodidácticos en CD-ROM o en Internet.

Encontrará información detallada sobre la oferta de formación y los datos de contacto de los asesores de clientes en la siguiente dirección de Internet:

Enlace: (www.siemens.com/sitrain)

Índice

	Prólogo	3
1	Aplicación y funciones.....	13
1.1	Aplicación y funciones de comunicación	13
1.2	Otras funciones.....	15
1.3	Requisitos de aplicación	18
1.4	Ejemplos de aplicación	22
1.4.1	Comunicación de telefonía móvil por SMS y correo electrónico sin LOGO! BM.....	22
1.4.2	Comunicación de telefonía móvil por SMS y correo electrónico con LOGO! BM	23
1.4.3	Acceso del PC a través de Internet y de una red de telefonía móvil.....	25
1.4.4	Detección de posición (GPS).....	26
1.4.5	Sincronización horaria	28
2	LED, conexiones, pulsadores y slots para tarjetas.....	31
2.1	Vista del dispositivo	31
2.2	LED para la indicación del funcionamiento	32
2.3	Interfaces	34
2.4	El pulsador "SET"	35
2.5	Slots para tarjeta SIM y tarjeta SD	36
3	Montaje, conexión, puesta en marcha	39
3.1	Indicaciones importantes sobre el uso del dispositivo.....	39
3.1.1	Indicaciones para el uso en la zona Ex	39
3.1.2	Notas sobre el uso en áreas Ex según ATEX / IECEx	41
3.1.3	Indicaciones para el uso en la zona Ex según UL HazLoc	41
3.2	Montar el dispositivo	42
3.3	Conectar el dispositivo.....	43
3.3.1	Interfaz X1P1 (LAN).....	43
3.3.2	Entradas y salidas.....	44
3.3.3	Conectar la antena.....	45
3.3.4	Alimentación	46
3.4	Puesta en servicio del dispositivo.....	47
3.4.1	Pasos para la puesta en marcha	47
3.4.2	Insertar la tarjeta SIM e introducir el PIN.....	48
3.4.3	Insertar la tarjeta SD	50
4	Operación: Acceso al BM.....	51
4.1	Sinopsis	51
4.2	Lectura y escritura de valores.....	51

5	Configuración (WBM)	57
5.1	Recomendaciones Security	57
5.2	Funciones generales del WBM	60
5.3	Datos de prestaciones y capacidad funcional	63
5.4	Caracteres permitidos y longitudes de strings	64
5.5	Establecer la conexión con el CMR	68
5.5.1	Establecer la conexión de configuración	69
5.6	Start page.....	72
5.7	System	75
5.7.1	General	75
5.7.2	Device info	76
5.7.3	Tarjeta SD	76
5.7.4	System time	77
5.8	Diagnóstico	81
5.8.1	Diagnostics buffer	81
5.8.2	Notifications.....	82
5.9	Maintenance.....	83
5.9.1	Configuration.....	83
5.9.2	Firmware	85
5.9.3	Operating status.....	86
5.9.4	Online Support	89
5.10	LAN	90
5.10.1	Configuration.....	90
5.11	WAN.....	92
5.11.1	Overview	92
5.11.2	Mobile wireless settings	94
5.11.3	Wireless cell.....	97
5.11.4	SMS	99
5.11.5	SMS alias	100
5.11.6	E-mail.....	101
5.11.7	DynDNS	102
5.12	Security	104
5.12.1	Sinopsis.....	104
5.12.2	OpenVPN-PSK.....	106
5.12.3	HTTPS	109
5.13	Users / groups.....	112
5.13.1	Users.....	112
5.13.2	Recipient groups	114
5.14	Monitoring	115
5.14.1	Vigilancia - ¿Qué debo hacer?	116
5.14.2	Funciones de vigilancia.....	117
5.14.3	Overview	119
5.14.4	LOGO! BM	120
5.14.5	Constantes	120
5.14.6	Message texts.....	121

5.14.7	Signals	122
5.14.8	Events	125
5.14.9	Actions	126
5.14.10	Assignments	130
5.14.11	Ejemplo de configuración de la vigilancia.....	132
6	Diagnóstico y mantenimiento	141
6.1	Posibilidades de diagnóstico	141
6.2	SMS de diagnóstico	142
6.3	Detección de errores de e-mails.....	143
6.4	Fallos y causas posibles.....	145
6.5	Cargar firmware	146
6.6	Restablecer la configuración de fábrica.....	147
6.7	Sustitución del CMR	148
7	Croquis acotados.....	151
8	Datos técnicos	153
9	Homologaciones	157
A	Accesorios	165
A.1	Antenas.....	165
A.2	Cable de antena.....	167
A.3	Aislador pasante de armario / acoplamiento de antena	170
A.4	Protección contra sobretensiones	171
A.5	Tarjeta SD.....	171
B	Información complementaria sobre SMS.....	173
B.1	Comportamiento del CMR al recibir o responder SMS	173
B.2	Avisos de error de SMS.....	175
B.3	Sintaxis de todos los comandos SMS	176
B.4	Comandos SMS.....	176
B.5	SMS de respuesta del comando "MONITOR?"	181
C	Bibliografía.....	187
C.1	/1/	187
C.2	/2/	187
	Índice alfabético.....	189

Aplicación y funciones

1.1 Aplicación y funciones de comunicación

Funciones de comunicación

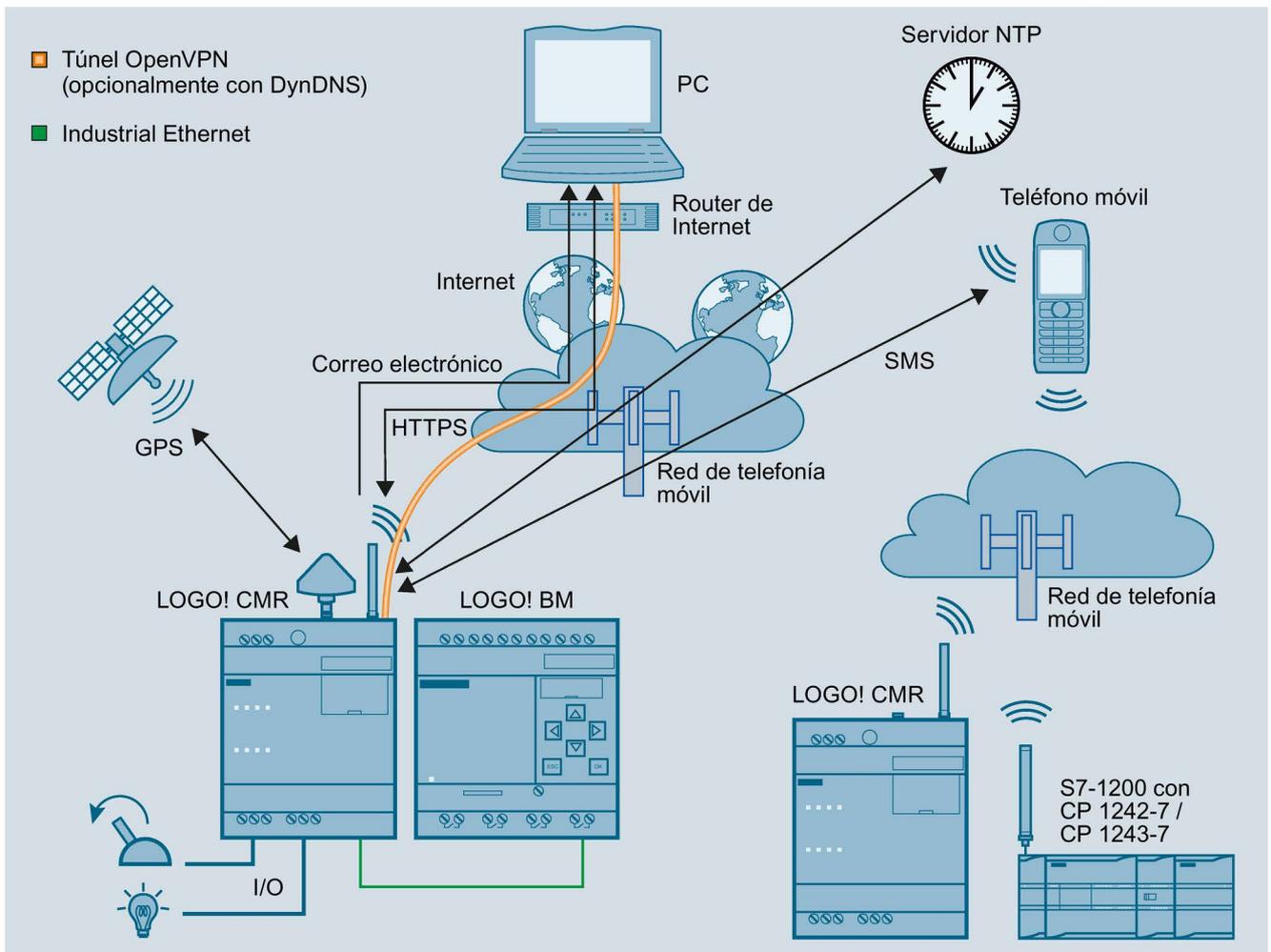


Figura 1-1 Descripción general de las funciones de comunicación del LOGO! CMR

Comunicación y acceso a datos de proceso

Acceso a datos de proceso

Desde el CMR es posible acceder a los datos de proceso en una configuración con BM: memoria imagen de proceso, entradas/salidas, marcas, etc.

En funcionamiento autónomo (véase más abajo) existe la posibilidad de acceder a la periferia mediante las entradas y salidas del CMR.

La información se lee y puede transferirse por SMS o correo electrónico. Es posible la notificación basada en eventos mediante SMS o correo electrónico; consulte "Telefonía móvil".

Telefonía móvil

Con el CMR se establece una conexión de datos con una red de telefonía móvil: Se soportan las siguientes especificaciones:

- **LOGO! CMR2020**

Estándares de telefonía móvil:

- GSM/GPRS

- **LOGO! CMR2040**

Estándares de telefonía móvil:

- 4G (LTE)
- 3G (UMTS)
- 2G (GSM/GPRS/EDGE)

Estrategia de reserva:

Si se produce un error al establecer una conexión entre el CMR2040 y la red LTE, al repetir la marcación se pasará automáticamente al siguiente estándar inferior de telefonía móvil (LTE > UMTS > GPRS).

Encontrará las frecuencias soportadas en el capítulo Datos técnicos (Página 153).

Las homologaciones radioeléctricas nacionales de los dispositivos están en el capítulo Homologaciones (Página 157) y en la siguiente página web:

Enlace: (<https://support.industry.siemens.com/cs/ww/es/ps/15383/cert>)

GPS

El CMR puede recibir datos de posición y la hora de un sistema de GPS.

HTTPS

En un PC de configuración / teléfono inteligente / tableta puede utilizarse HTTPS para acceder al CMR. HTTPS se soporta en las dos interfaces del CMR: LAN y WAN (telefonía móvil)

Configuración de una estación con CMR

El CMR puede utilizarse en las siguientes variantes de configuración:

- **CMR con BM**

El CMR está conectado localmente al BM a través de Ethernet. El CMR establece la conexión con una red de telefonía móvil.

- **Funcionamiento autónomo**

El CMR también puede utilizarse en modo independiente, es decir, sin un BM conectado. Para la conexión de la periferia se utilizan las dos entradas y salidas del CMR.

1.2 Otras funciones

Funciones

El CMR soporta las siguientes funciones:

- **WBM**

Una interfaz web (WBM - Web Based Management) para la configuración del CMR, protegida con nombre de usuario y contraseña; consulte el apartado "WBM" más abajo.

- **OpenVPN**

Tecnología de túnel OpenVPN para la transferencia de datos segura por telefonía móvil; consulte el apartado "OpenVPN" más abajo.

- **Posición GPS**

- Consultar la posición por SMS
- Transferir la posición al BM

- **DynDNS**

Uso de DNS dinámico en la interfaz WAN (telefonía móvil)

- **Mensajes (SMS, correo electrónico)**

- Envío y recepción de SMS
- Envío de correo electrónico

Consulte las funciones en el apartado "Mensajes" más abajo.

- **Lectura de la memoria imagen de proceso**

La memoria imagen de proceso del BM puede leerse mediante SMS (comando "MONITOR?").

- **Escritura de salidas**

Las dos salidas del CMR pueden escribirse mediante SMS.

- **Lectura de señales**

Mediante correo electrónico y SMS es posible acceder en modo de lectura a la memoria imagen de proceso del BM, la memoria de variables y la memoria imagen de proceso del CMR utilizando señales configurables.

- **Acceso a la memoria de variables (VM)**

Desde la memoria de variables se accede en modo de lectura y escritura a los valores actuales de los bloques de función del BM mediante SMS.

- **Eventos / memoria imagen de proceso**

Configuraciones de eventos y reacciones, p. ej. SMS de alarma en caso de cambio de un valor en la memoria imagen de proceso.

La imagen de proceso del BM consta de los siguientes elementos, que pueden utilizarse para configurar eventos o alarmas:

- Entradas digitales y analógicas
- Salidas digitales y analógicas
- Marcas digitales y analógicas
- Registros de desplazamiento
- Teclas de manejo
- Teclas de función

- **Sincronización horaria**

- NTP
- GPS
- Red de telefonía móvil (en función del operador de telefonía móvil)

- **Reenvío de la hora al BM**

- **Tarjeta SD**

Existe la opción de guardar los datos de configuración del CMR y una copia del búfer de diagnóstico en una tarjeta SD.

WBM

El CMR se configura localmente mediante una interfaz web (WBM) que se visualiza con un navegador web. El WBM ofrece las siguientes funciones:

- Habilitación de la recepción de GPS
- Ajuste de la hora del sistema y sincronización del BM
- Configuración del CMR para enviar y recibir mensajes
- Configuración de las interfaces LAN y WAN y sus funciones
- Configuración de las funciones de seguridad
- Creación y administración de usuarios y grupos
- Vigilancia del CMR mediante diferentes parámetros y funciones

- Funciones de mantenimiento como actualización de firmware y re arranque completo
- Asimismo, desde el WBM se recibe mucha información de estado y diagnóstico.

Encontrará más información en el capítulo Configuración (WBM) (Página 57).

Mensajes

Envío de SMS y correos electrónicos

A partir de eventos internos y surgidos del proceso es posible generar reacciones de salida mediante el WBM que resultan en el envío de SMS o correos electrónicos de información, diagnóstico y alarma.

Recepción de SMS

Las salidas del CMR y del BM pueden escribirse por SMS. La autorización se comprueba comparando el número de teléfono del remitente con los números de teléfono configurados. La protección por contraseña es opcional.

Ejemplo de un texto de SMS para escribir un bit individual con el valor cero:

<contraseña>;LOGO=VM115.1,0,BIT

Funciones que simplifican la sintaxis del SMS:

- SMS alias
Configuración de nombres simbólicos que se utilizan como comodines de todo el texto del SMS
- Constantes para valores repetitivos
Configuración de constantes simbólicas que se utilizan como comodines para valores repetitivos que deben escribirse
- Uso de nombres de señal como parámetros en SMS
Configuración de señales que se utilizan como comodines para variables del BM

Encontrará la información correspondiente en los capítulos siguientes:

- Diagnóstico > Notifications (Página 82)
- WAN > SMS (Página 99) y siguientes
- Usuarios / Grupos > Users (Página 112) y > Recipient groups (Página 114)
- Vigilancia > Constantes (Página 120)
- Vigilancia > Message texts (Página 121)
- Vigilancia > Signals (Página 122)
así como
- Comportamiento del CMR al recibir o responder SMS (Página 173) y siguientes

OpenVPN

Existe la posibilidad de utilizar la tecnología VPN de OpenVPN para la transmisión segura de datos a través de la conexión de telefonía móvil del CMR. Entre el CMR y el interlocutor (teléfono móvil/tableta, PC) se establece un túnel VPN. El CMR es el servidor OpenVPN, mientras que el interlocutor (teléfono móvil, PC) es el cliente OpenVPN.

Además, es posible utilizar OpenVPN para la comunicación directa con el BM si el CMR está registrado como router en el BM.

El CMR utiliza la versión V2.3.11 de OpenVPN.

OpenVPN está implementado en el CMR como dispositivo TUN (modo routing). Se soportan las funciones de seguridad siguientes:

- **Cifrado**
Los datos que se transfieren se cifran con el método AES-128 CBC.
- **Autenticación de los interlocutores**
Como algoritmos Hash para autenticar los datos de usuario se utiliza SHA-256.

Los requisitos para el cliente OpenVPN en el interlocutor VPN se indican en el capítulo Requisitos de aplicación (Página 18).

Diagnóstico vía LAN y WAN

Desde el WBM es posible visualizar el búfer de diagnóstico para fines de diagnóstico. También es posible guardar el búfer de diagnóstico en la tarjeta SD o el PC.

Encontrará más detalles en el capítulo Posibilidades de diagnóstico (Página 141).

1.3 Requisitos de aplicación

Requisitos para el funcionamiento

- **Contrato de telefonía móvil con tarjeta SIM**
Para el uso de la comunicación de telefonía móvil a través de la interfaz WAN del CMR se necesita un contrato con un operador de red de telefonía móvil.
Encontrará información sobre el contrato y la tarjeta SIM más abajo.
- **Red de telefonía móvil**
Para poder utilizar la interfaz de telefonía móvil debe haber una red de telefonía móvil cerca del CMR.
- **Contrato de datos**
Para todos los servicios de datos siguientes que se utilicen se necesita un contrato de datos con un operador de red de telefonía móvil:
correo electrónico, NTP, DynDNS, OpenVPN, HTTPS vía telefonía móvil

- **NTP**

Además de los requisitos citados anteriormente (tarjeta SIM, contrato de datos y red de telefonía móvil), para la sincronización horaria vía NTP se necesitan los datos de dirección de un servidor NTP.

- **OpenVPN**

Además de los requisitos citados anteriormente (tarjeta SIM, contrato de datos y red de telefonía móvil), para utilizar OpenVPN a través de la red de telefonía móvil se necesita:

- una dirección IP pública para el CMR
- un cliente OpenVPN como interlocutor de la comunicación (p. ej. PC para acceder al WBM del CMR)
- una clave compatible con el cliente OpenVPN (Preshared Key)

La clave puede generarse en el WBM del CMR, aunque también puede generarla el interlocutor de la comunicación e importarse mediante el WBM del CMR.

El cliente OpenVPN en el interlocutor OpenVPN debe soportar las funciones siguientes:

- OpenVPN V2.3.11 o superior

La información del servidor OpenVPN del CMR puede exportarse para el cliente en forma de archivo; consulte el capítulo OpenVPN-PSK (Página 106).

- **DynDNS**

Además de los requisitos citados anteriormente (tarjeta SIM, contrato de datos y red de telefonía móvil), para el uso de DynDNS se necesita lo siguiente:

- un operador de servicios adecuado
- una dirección IP pública
- Tenga en cuenta también el punto "Hora" más abajo.

- **HTTPS**

- Para HTTPS vía telefonía móvil se necesita una dirección IP pública para el CMR.
- Tenga en cuenta también el punto "Hora" más abajo.

- **Hora**

Si se utilizan certificados, p. ej. al usar HTTPS, correo electrónico (seguro) o DynDNS, se necesitan la hora y la fecha exactas para comprobar los certificados.

Antenas

Utilice solamente antenas del programa de accesorios del CMR. Encontrará más información en el capítulo Antenas (Página 165).

- Telefonía móvil

Para utilizar el CMR se necesita una antena adaptada al estándar de la red de telefonía móvil utilizada.

Encontrará información sobre el uso de una red LTE para el comportamiento de reserva en el capítulo Aplicación y funciones de comunicación (Página 13).

Encontrará las bandas de frecuencia soportadas por el CMR en el capítulo Datos técnicos (Página 153).

- GPS

Si desea utilizar GPS necesitará una antena GPS adecuada, consulte el capítulo Antenas (Página 165).

Alimentación

Se requiere una fuente de tensión de entre 12 V DC y 24 V DC que proporcione suficiente tensión e intensidad. Encontrará más información en el capítulo Datos técnicos (Página 153).

Tarjeta SIM

Se requiere una tarjeta SIM del operador de telefonía móvil.

Recomendaciones

Tenga en cuenta las siguientes recomendaciones para el contrato de telefonía móvil y la tarjeta SIM:

- En la medida de lo posible, contrate un servicio de telefonía móvil con un operador que le ofrezca todas las funciones que necesita.

Para utilizar DynDNS, por ejemplo, se necesita una dirección IP pública.

Para enviar SMS, la tarjeta SIM debe estar habilitada para dicha función y disponer de un número de teléfono.

- En la medida de lo posible, no utilice tarjetas multiSIM. Pueden provocar errores en la sincronización horaria.
- Siempre que sea posible, cierre un contrato de telefonía móvil fijo y no utilice tarjetas de prepago.

Es recomendable contratar una tarifa plana para SMS y datos.

No obstante, si desea utilizar una tarjeta de prepago, debe tener en cuenta lo siguiente:

- Una vez haya consumido el saldo, el CMR dejará de enviar advertencias automáticas.
- Puede consultar el saldo actual al operador.

- Para un tráfico de datos más rápido con el CMR2040 se recomienda disponer de un contrato (con la tarjeta SIM correspondiente) que soporte el estándar de telefonía móvil LTE.

De todas formas, el CMR2040 soporta también UMTS.

- En la medida de lo posible, utilice una tarjeta SIM estándar sin adaptador.
- Por lo general, el operador asigna un PIN (Personal Identification Number) a la tarjeta SIM.

Las tarjetas SIM que solo se utilizan para servicios de datos (véase más arriba), pueden utilizarse casi siempre sin PIN. En la configuración del CMR no hay que asignar ningún PIN.

- Debe disponerse de los siguientes datos de acceso a la red de telefonía móvil:
 - Access Point Name (APN)
 - En función del operador del servicio, también nombre y contraseña para el APN
 - El método de autenticación

Encontrará más información en el capítulo Mobile wireless settings (Página 94).

Tarjetas compatibles

El compartimento del CMR para la tarjeta SIM es compatible con los formatos siguientes:

- tarjeta SIM mini, 25 x 15 mm (ISO/IEC 7810 ID-000)
- tarjeta SIM micro, 15 x 12 mm (ETSI TS 102 221 V9.0.0), en caso de que exista adaptador.
- tarjeta SIM nano, 12,3 x 8,8 mm (ETSI TS 102 221, TS 102 221 V11.0.0), en caso de que exista adaptador.

Accesorios opcionales: Tarjeta SD

Como accesorio opcional es posible utilizar una tarjeta SD, que no está incluida en el suministro del CMR. Encontrará las tarjetas SD compatibles en el anexo Tarjeta SD (Página 171).

La tarjeta SD ofrece las funciones siguientes:

- Guardar archivos de configuración
 - En caso de repuesto puede utilizarse la tarjeta SD para transferir al nuevo dispositivo los datos de configuración del CMR antiguo guardados en la tarjeta. Consulte a este respecto el capítulo Sustitución del CMR (Página 148).
- Guardar entradas del búfer de diagnóstico
- Guardar automáticamente todo el búfer de diagnóstico en caso de errores graves (configurable)

1.4 Ejemplos de aplicación

Posibilidades de aplicación

El CMR ofrece una gran variedad de aplicaciones posibles en diferentes campos. A continuación encontrará algunos ejemplos de configuración para aplicaciones del CMR.

1.4.1 Comunicación de telefonía móvil por SMS y correo electrónico sin LOGO! BM

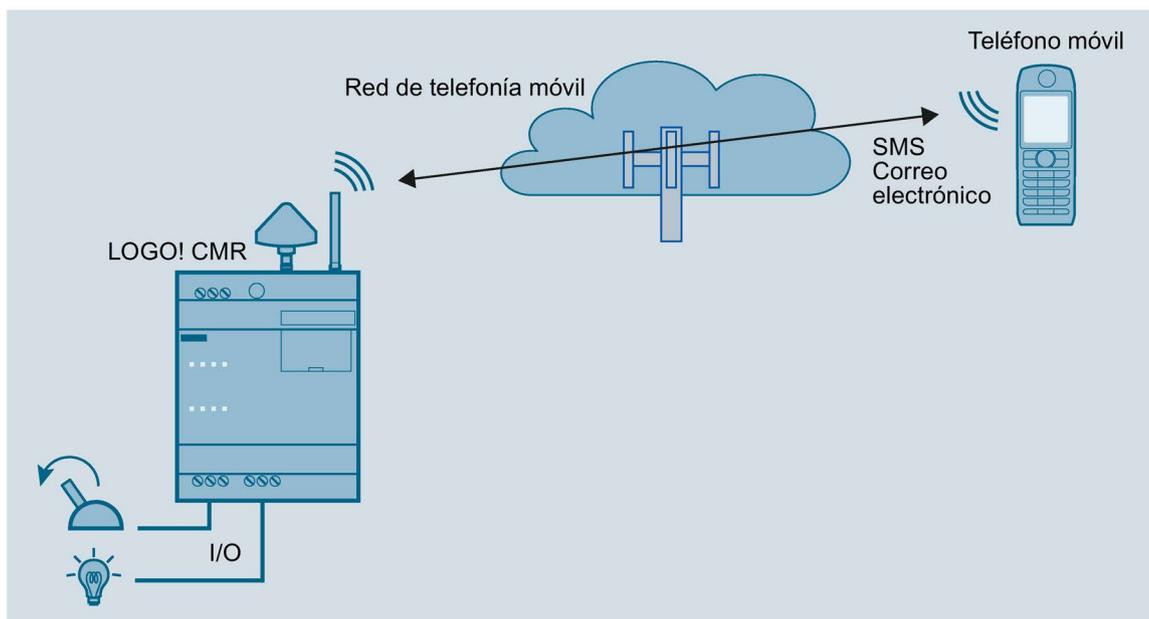


Figura 1-2 Comunicación de telefonía móvil sin LOGO! BM

El CMR puede utilizarse sin un BM conectado. Si el CMR está conectado a una antena de telefonía móvil, se dispone de las siguientes funciones:

- Envío de un SMS o un correo electrónico debido a una señal en la entrada del CMR
- Recepción de un SMS:
 - Activación de una salida del CMR
 - Solicitud de un SMS con información de estado del CMR

El WBM del CMR permite configurar acciones y eventos como el cambio de señales de entrada. Las acciones se disparan al producirse eventos configurables.

Requisitos

- El montaje, la conexión y la puesta en marcha están realizados.
- La antena para la recepción de telefonía móvil está conectada.

Procedimiento

Para configurar el acceso a través de la red de telefonía móvil, proceda del siguiente modo:

1. En primer lugar, establezca una conexión de configuración entre el CMR y un PC conectado. Use para ello un cable Patch Ethernet, véase Establecer la conexión con el CMR (Página 68).
2. Configure la conexión de telefonía móvil, véase Mobile wireless settings (Página 94).
3. Configure el dispositivo mediante el WBM.

1.4.2 Comunicación de telefonía móvil por SMS y correo electrónico con LOGO! BM

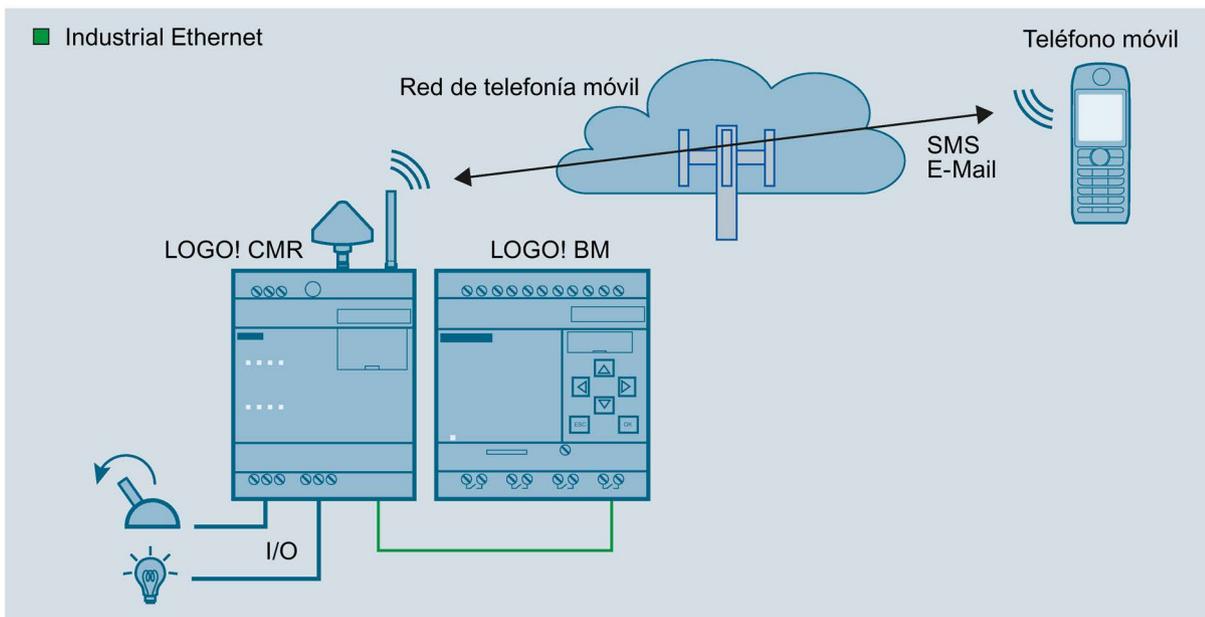


Figura 1-3 Comunicación de telefonía móvil con LOGO! BM

Si el CMR está conectado al BM y la antena de telefonía móvil está conectada, se dispone de todas las funciones que ofrece el funcionamiento sin el BM conectado. Además, el acceso al LOGO! BM se ve ampliado:

- Envío de un SMS o un correo electrónico debido a un evento en el BM conectado
- Recepción de un SMS:
 - Disparo de una acción en el BM conectado
 - Solicitud de un SMS con información de estado del CMR

La configuración mediante el WBM también incluye el acceso a componentes del BM.

Requisitos

- El montaje, la conexión y la puesta en marcha están realizados.
- La antena para la recepción de telefonía móvil está conectada.

Procedimiento

Para configurar el acceso a través de la red de telefonía móvil y establecer una conexión con el BM, proceda del siguiente modo:

1. En primer lugar, establezca una conexión de configuración entre el CMR y un PC conectado. Use para ello un cable Patch Ethernet, véase Establecer la conexión con el CMR (Página 68).
2. Configure la conexión de telefonía móvil, véase Mobile wireless settings (Página 94).
3. Configure el dispositivo mediante el WBM.
4. Una vez finalizada la configuración, desconecte el CMR del PC.

Nota

Uso de un switch

Si se utiliza un switch, p. ej. LOGO! CSM, no es necesario deshacer las conexiones. El BM, el CMR y el PC pueden funcionar simultáneamente.

5. Si no se utiliza ningún switch, el CMR debe conectarse con el BM.

1.4.3 Acceso del PC a través de Internet y de una red de telefonía móvil

Si el PC de configuración está conectado con el CMR a través de Internet y la red de telefonía móvil, es posible acceder al CMR y al BM utilizando un túnel OpenVPN.

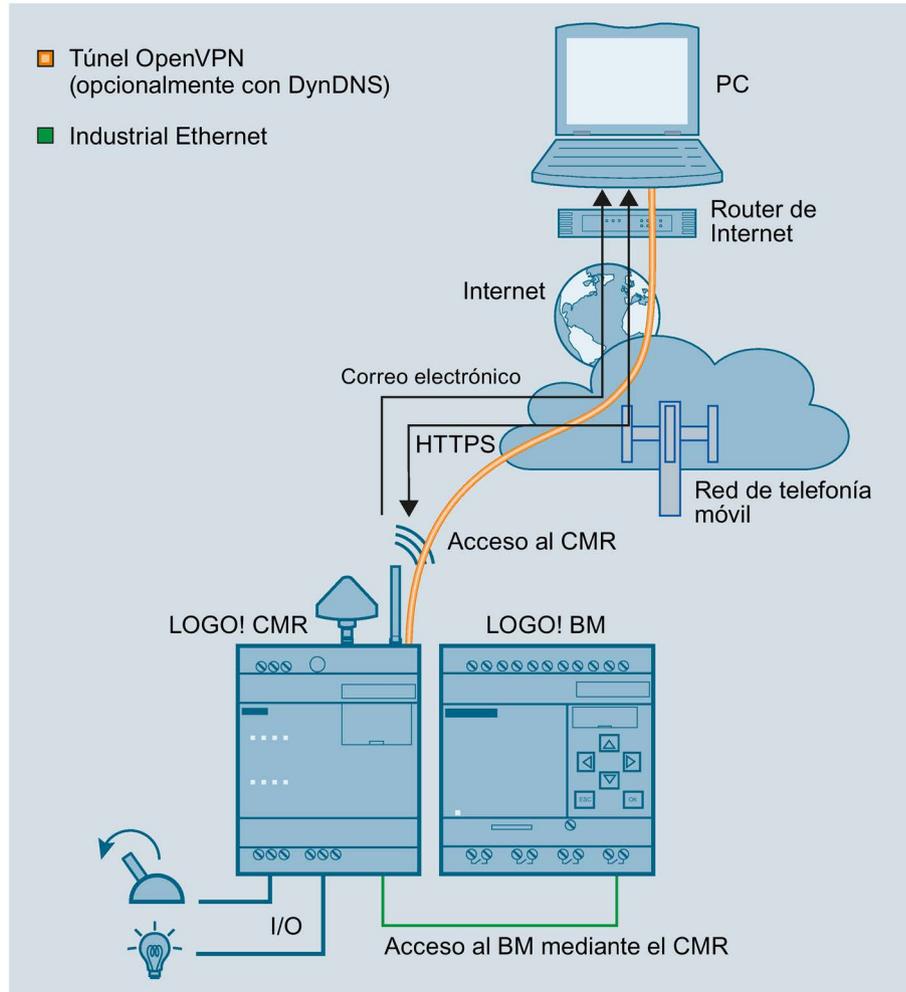


Figura 1-4 Acceso al LOGO! a través de Internet y de una red de telefonía móvil

Existen las siguientes posibilidades:

- Acceso protegido del PC al CMR con OpenVPN
 - Acceso protegido del PC al BM con OpenVPN
- El CMR debe registrarse como router en el BM para esta aplicación.
- De este modo es posible volver a cargar el programa del BM, por ejemplo.
- Acceso del PC de configuración al CMR por HTTPS a través de la red de telefonía móvil
- Consulte el procedimiento en el capítulo Establecer la conexión con el CMR (Página 68).
- Enviar correos electrónicos, opcionalmente cifrados mediante STARTTLS
 - Opcional: uso de DNS dinámico con el fin de simplificar la conexión por medio de la dirección IP de acceso público del CMR.

Requisitos

- Los servicios utilizados están activados mediante el WBM del CMR.
- Dispone de contratos con operadores de servicios adecuados.

1.4.4 Detección de posición (GPS)

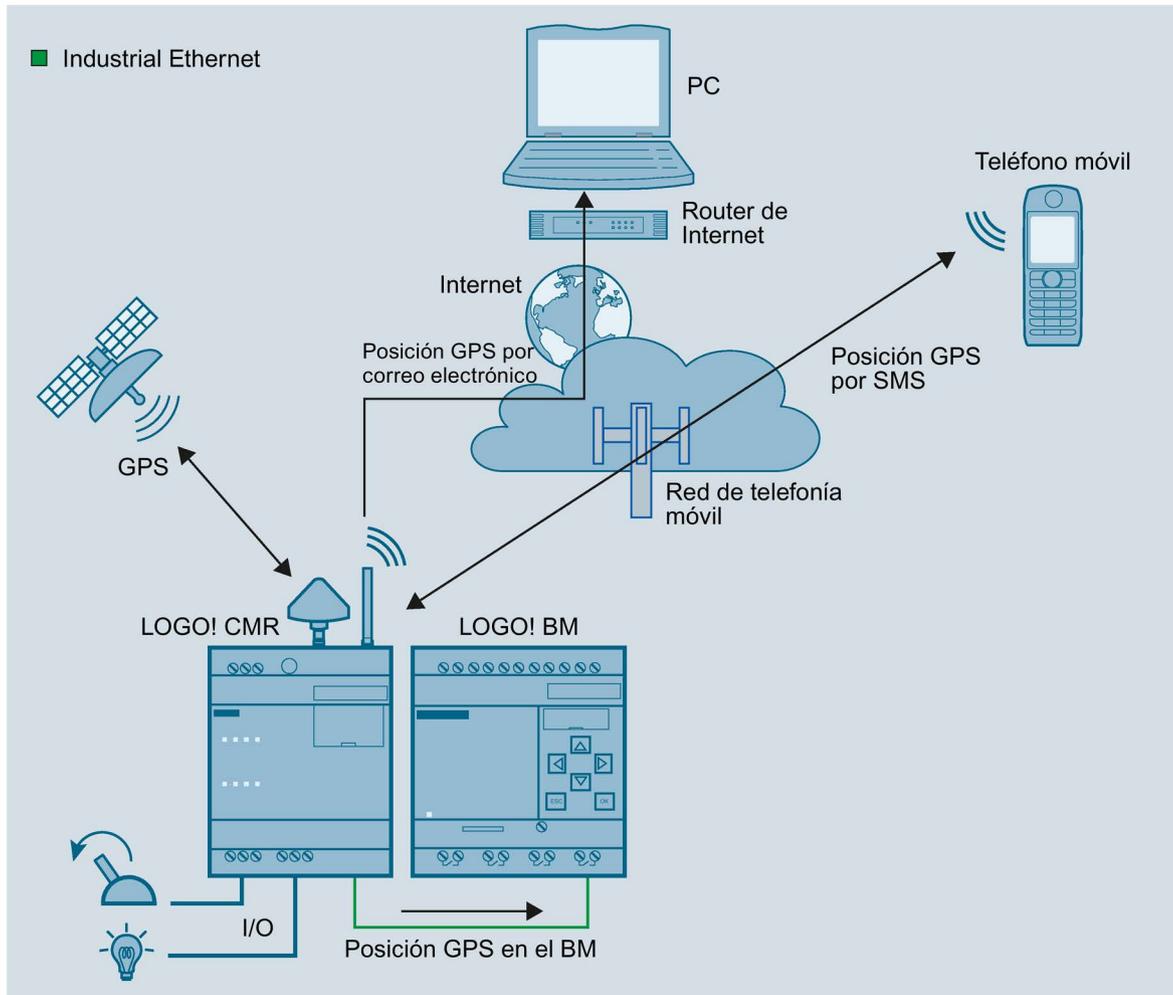


Figura 1-5 Detección de posición (GPS)

El CMR está equipado con una interfaz GPS que permite determinar los datos de posición de la estación LOGO!. Si hay una antena GPS conectada a la interfaz GPS, se dispone de las siguientes funciones:

- Determinación de datos de posición:
 - Debido a un evento en una entrada del CMR
 - Debido a un evento del BM
 - Debido a la recepción de un SMS (con la antena de telefonía móvil conectada)
- Envío de los datos de posición determinados:
 - Por SMS o correo electrónico
 - Al BM

Para poder utilizar las funciones mencionadas, primero debe activarse (Página 75) la interfaz GPS en el WBM del CMR. Para detectar la posición correctamente, deben recibirse las señales GPS de tres satélites.

Requisitos

- El montaje, la conexión y la puesta en marcha están realizados.
- La antena GPS está conectada.

Procedimiento

Para configurar el acceso a través de la red de telefonía móvil y establecer una conexión con el BM, proceda del siguiente modo:

Nota

Uso del CMR en caso de comunicación de telefonía móvil sin BM

Si se utiliza el CMR en caso de Comunicación de telefonía móvil por SMS y correo electrónico sin LOGO! BM (Página 22), se omiten los dos últimos pasos del procedimiento descrito a continuación.

1. En primer lugar, establezca una conexión de configuración entre el CMR y un PC conectado. Utilice para ello un latiguillo Ethernet.
Consulte Establecer la conexión con el CMR (Página 68)
2. Configure la conexión de telefonía móvil:
Consulte Mobile wireless settings (Página 94)
3. Active la recepción GPS (Página 75).

4. Una vez finalizada la configuración, desconecte el CMR del PC.

Nota

Utilización de un switch

Si se utiliza un switch, p. ej., LOGO! CSM, no deshaga las conexiones: el BM, el CMR y el PC pueden funcionar simultáneamente.

5. Si no utiliza ningún switch, conecte el CMR con el BM.

1.4.5 Sincronización horaria

La hora del CMR se sincroniza utilizando uno de los tres procedimientos siguientes:

- NTP

Sincronización con un servidor NTP externo accesible a través de la red de telefonía móvil.

- GPS
- Telefonía móvil

El suministro de la señal horaria depende del operador de telefonía móvil.

El procedimiento utilizado para la sincronización horaria se ajusta en la ficha "System" del WBM; consulte el capítulo System time (Página 77).

También existe la posibilidad de que el CMR obtenga la hora del PC de configuración.

Reenviar la hora al BM

Si se activa la hora en el WBM, el WBM permite además ajustar que el CMR sincronice también la hora en el BM (transmisión de la hora). Active para ello "Forward time of day to LOGO! BM".

Incluso si la sincronización horaria está desactivada, se transmite la hora al LOGO! BM . En tal caso, al LOGO! BM solo se transfieren los ajustes manuales.

Nota

Si la hora del BM se sincroniza mediante el CMR, debe activarse el cambio de horario de verano e invierno en el BM para garantizar que la hora sea coherente.

La siguiente figura ofrece una vista general:

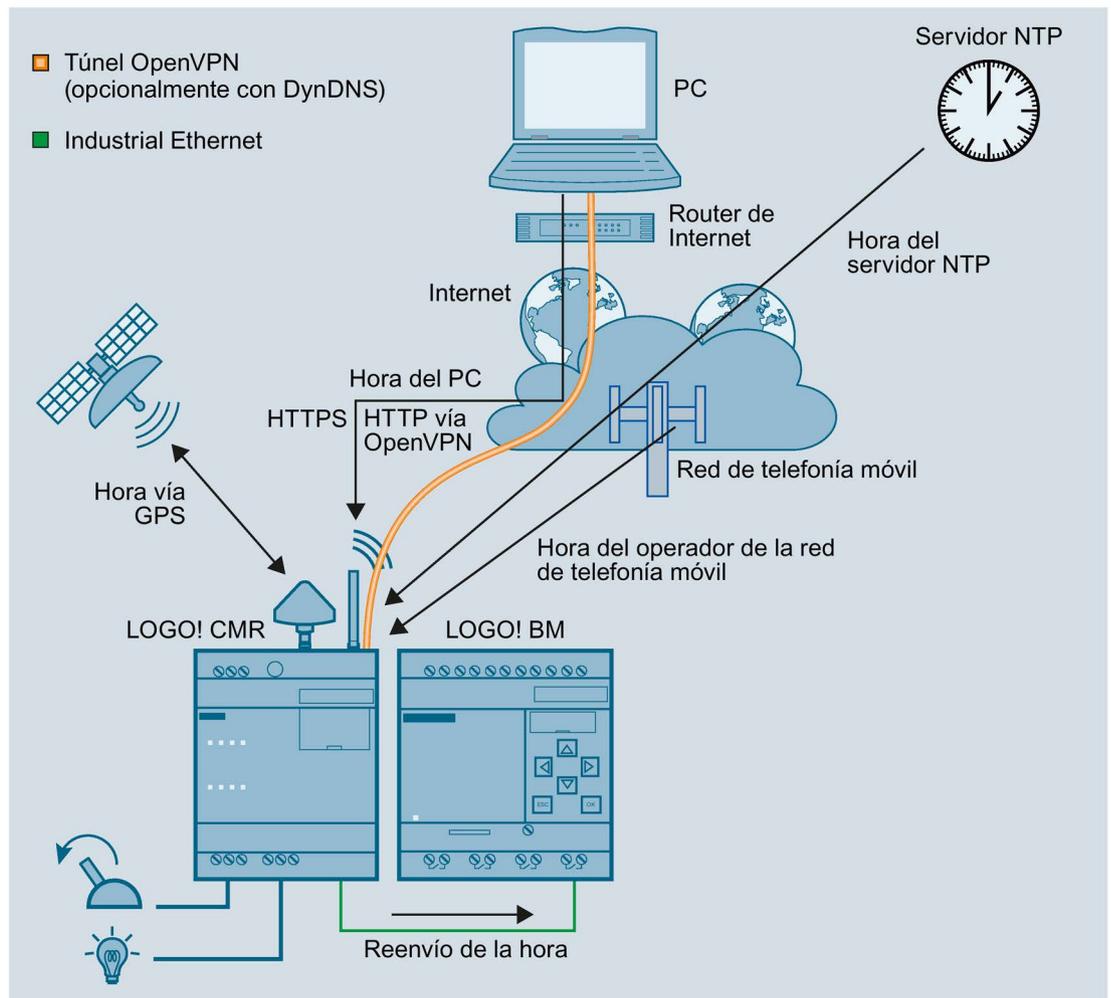


Figura 1-6 Sincronización horaria

Hora en caso de uso de certificados

Si se utilizan certificados, por ejemplo para los servicios de correo electrónico o DynDNS, se requiere la hora exacta.

Nota

Hora exacta para certificados

Para comprobar los certificados es imprescindible que el CMR disponga de la hora exacta. En caso de utilizar certificados, active la sincronización horaria del CMR.

Requisitos

- El CMR está montado y conectado.
- La antena para la recepción de telefonía móvil está conectada.

- El CMR está configurado.
- Solo si se ha configurado el método de sincronización horaria a través de la señal GPS: La antena para la recepción de GPS está conectada.

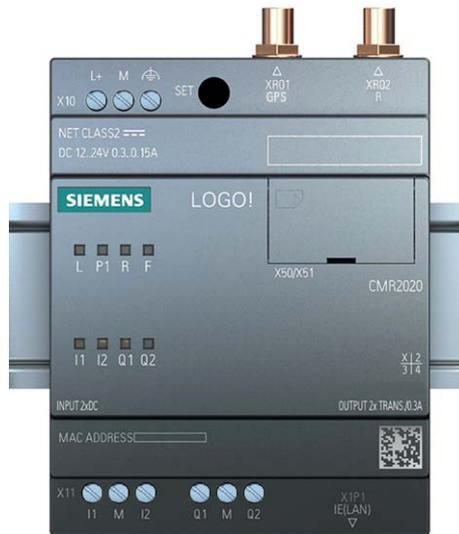
Procedimiento

Para configurar la sincronización horaria proceda del siguiente modo:

1. Establezca una conexión de configuración entre el CMR y un PC conectado. Use para ello un cable Patch Ethernet.
Encontrará los detalles en el capítulo Establecer la conexión con el CMR (Página 68).
2. Seleccione el procedimiento deseado.

LED, conexiones, pulsadores y slots para tarjetas

2.1 Vista del dispositivo



Elementos de mando, conexión y visualización del CMR

Elemento	Función
X10 (L+, M)	Conexión de la alimentación
SET	Pulsador SET
XR01	Conexión de la antena GPS
XR02	Conexión de la antena de telefonía móvil
LED "L"	Indicador de la alimentación
LED "P1"	Indicador de la interfaz LAN
LED "R"	Indicador de la intensidad de señal de la red de telefonía móvil
LED "F"	Indicador de error
X50/X51	Ranura para la tarjeta SIM y la tarjeta Micro SD
LED I1	Indicador de la entrada 1
LED I2	Indicador de la entrada 2
LED Q1	Indicador de la salida 1
LED Q2	Indicador de la salida 2
I1	Conexión de la entrada 1
M	Masa
I2	Conexión de la entrada 2
Q1	Conexión de la salida 1
M	Masa

2.2 LED para la indicación del funcionamiento

Elemento	Función
Q2	Conexión de la salida 2
X1P1	Conexión LAN

2.2 LED para la indicación del funcionamiento

Los diodos luminiscentes (LED) del CMR informan sobre el estado operativo del dispositivo y de las dos entradas y salidas.

Significado de los LED

LED	Estado	Significado
Todos los LED	Intermitente	Error grave
	Encendido	El firmware se actualiza
	Apagado	<ul style="list-style-type: none"> No hay tensión o no se recibe Dispositivo apagado
L Alimentación	Apagado <input type="checkbox"/>	No hay ninguna alimentación conectada
	Encendido 	Alimentación conectada
	Intermitente 	Inicialización o cambio de la configuración en curso.
P1 LAN	Encendido en verde 	Conexión con Ethernet establecida.
	Amarillo intermitente con luz verde en reposo 	Datos
	Apagado <input type="checkbox"/>	No hay conexión con Ethernet o no hay ningún cable conectado.
R Intensidad de señal (red de telefonía móvil)	Encendido en verde 	Muy buena
	Encendido en amarillo 	Media
	Apagado <input type="checkbox"/>	No hay señal o es muy mala
	Intermitente 	Datos
F Error	Apagado <input type="checkbox"/>	Ningún error

2.3 Interfaces

LED	Estado	Significado
	Encendido 	Error, consulte también el capítulo Fallos y causas posibles (Página 145).
	Intermitente 	Detección de dirección IP repetida. La interfaz Ethernet no está accesible.
I1 Entrada 1	Apagado 	$U < 5 \text{ V}$
	Encendido en verde 	$U > 8,5 \text{ V}$
I2 Entrada 2	Apagado 	$U < 5 \text{ V}$
	Encendido en verde 	$U > 8,5 \text{ V}$
Q1 Salida 1	Apagado 	No hay tensión en la salida
	Encendido en verde 	Alimentación en la salida
Q2 Salida 2	Apagado 	No hay tensión en la salida
	Encendido en verde 	Alimentación en la salida

2.3 Interfaces

Encontrará información sobre cómo conectar las interfaces y conexiones en el capítulo Conectar el dispositivo (Página 43).

Encontrará datos detallados sobre las interfaces y conexiones en el capítulo Datos técnicos (Página 153).

Conexión a la alimentación eléctrica

Para la conexión a la alimentación eléctrica está disponible el borne X10.

Conexión a la red local

Para la conexión LAN a la red local/PC y para la conexión con el BM, el CMR dispone del puerto X1P1. La dirección IP del puerto X1P1 puede configurarse.

Conexión a la red de telefonía móvil y GPS

Para la conexión inalámbrica, el CMR posee dos conectores hembra SMA:

- Conector hembra SMA XR02 para la red de telefonía móvil
- Conector hembra SMA XR01 para la recepción de GPS

Entradas y salidas

Para la conexión de elementos periféricos están disponibles las siguientes entradas y salidas:

- Entradas digitales
I1 + I2
- Salidas digitales
Q1 + Q2

2.4 El pulsador "SET"

Elementos de manejo/conexión y visualización del CMR

El pulsador SET tiene funciones distintas dependiendo del tiempo que se mantenga pulsado.

Manejo	Función
Pulsar brevemente (máx. 5 s)	Reinicio
Mantener pulsado entre 5 y 10 s	Apagar el dispositivo para llevarlo a un estado seguro Resultado: <ul style="list-style-type: none"> • Todos los indicadores LED están apagados. • El dispositivo puede desconectarse de la alimentación. No es posible volver a activar el CMR cuando está apagado. Para reactivarlo hay que desconectar la alimentación de tensión y volver a conectarla.
Mantener pulsado más de 10 s	Restablecer configuración de fábrica Consulte las repercusiones en el capítulo Restablecer la configuración de fábrica (Página 147).

2.5 Slots para tarjeta SIM y tarjeta SD

Ambos slots están en la parte frontal del CMR, detrás de la tapa.

"X50": slot para la tarjeta SIM

X50 es el slot para la tarjeta SIM que le entrega con el contrato de abonado el operador de la red de telefonía móvil.

Tarjetas compatibles

Encontrará información sobre los formatos compatibles de tarjetas SIM en el capítulo Requisitos de aplicación (Página 18).

Error de tarjeta / Diagnóstico

Los errores de tarjeta se indican a través del LED "SIM" y de entradas en el búfer de diagnóstico

Introducción de la tarjeta

El procedimiento para introducir la tarjeta SIM se describe en el capítulo Insertar la tarjeta SIM e introducir el PIN (Página 48).

"X51": slot para una tarjeta SD opcional

Una tarjeta SD puede utilizarse opcionalmente como medio de almacenamiento extraíble para guardar los datos de configuración y de diagnóstico.

El CMR no se suministra con tarjeta SD.

Tarjetas compatibles

Encontrará una lista de tarjetas compatibles en el anexo Tarjeta SD (Página 171).

Error de tarjeta / Diagnóstico

Los errores de tarjeta se indican mediante entradas en el búfer de diagnóstico

Introducción de la tarjeta

El procedimiento para introducir la tarjeta SD se describe en el capítulo Insertar la tarjeta SD (Página 50).

Almacenamiento remanente de datos importantes en la tarjeta SD

La tarjeta SD es un medio alternativo para guardar una copia de seguridad de diversos datos a prueba contra fallos de tensión.

En la tarjeta SD pueden almacenarse los datos siguientes:

- **Datos de configuración**

Después de cada modificación se guarda una copia de seguridad de los datos de configuración en un archivo de configuración en la tarjeta SD. El almacenamiento de los datos de configuración en la tarjeta SD tiene las finalidades siguientes:

- Copiar datos de configuración en otros CMR del mismo tipo

El archivo de configuración es editable y puede utilizarse para copiar datos de configuración en diferentes CMR desde el WBM.

- Sustitución de dispositivo sin PC de configuración

En caso de que haya que sustituir un CMR para fines de mantenimiento, los datos de configuración pueden proporcionarse al nuevo CMR transfiriendo la tarjeta SD del CMR antiguo al nuevo. En ese caso no se necesita un PC de configuración.

Encontrará información sobre el almacenamiento de los datos de configuración en la tarjeta SD en el capítulo Configuration (Página 83).

Encontrará información sobre el cambio de dispositivo en el capítulo Sustitución del CMR (Página 148).

- **Entradas del búfer de diagnóstico**

En el WBM puede configurarse que las entradas del búfer de diagnóstico se almacenen en la tarjeta SD si se producen eventos graves.

Manualmente es posible almacenar en la tarjeta SD el búfer de diagnóstico completo del CMR.

Montaje, conexión, puesta en marcha

3.1 Indicaciones importantes sobre el uso del dispositivo

Consignas de seguridad para el uso de los equipos

Las siguientes consignas de seguridad deben tenerse en cuenta para la instalación y el uso del equipo, así como para todos los trabajos relacionados, como el montaje, la conexión o la sustitución del dispositivo.

Protección contra sobretensiones

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

3.1.1 Indicaciones para el uso en la zona Ex

 ADVERTENCIA
RIESGO DE EXPLOSIÓN
No está permitido abrir el dispositivo.

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

Alimentación externa

- Utilice únicamente una alimentación externa que cumpla la norma EN 60950.
- La tensión de salida de la alimentación externa no debe superar los 30 V DC.
- La salida de la alimentación externa debe ser resistente a cortocircuitos.

ATENCIÓN
Alimentación El CMR solo debe ser abastecido por fuentes de alimentación según IEC/EN 60950-1 apartado 2.5 "Fuente de corriente de potencia limitada". La alimentación externa para el CMR tiene que cumplir lo dispuesto para circuitos NEC clase 2, tal como se estipula en el National Electrical Code ® (ANSI/NFPA 70).

Tenga en cuenta lo indicado en este capítulo y las normas de montaje y uso del fabricante de la fuente de alimentación.

 ADVERTENCIA
El equipo se ha concebido para trabajar con una baja tensión de seguridad (Safety Extra Low Voltage, SELV) directamente conectable, suministrada por una fuente de alimentación de potencia limitada (Limited Power Source, LPS). Por esta razón se deben conectar sólo bajas tensiones de seguridad (SELV) de potencia limitada (Limited Power Source, LPS) según IEC 60950-1 / EN 60950-1 / VDE 0805-1 a las tomas de alimentación, o bien la fuente de alimentación del equipo tiene que ser conforme a NEC Class 2 según el National Electrical Code (r) (ANSI / NFPA 70). Si el equipo se conecta a una alimentación redundante (dos fuentes de alimentación independientes), ambas fuentes han de cumplir los requisitos citados.

 ADVERTENCIA
RIESGO DE EXPLOSIÓN EN UNA ATMÓSFERA FÁCILMENTE INFLAMABLE O COMBUSTIBLE NO SE DEBEN CONECTAR CABLES AL DISPOSITIVO NI DESCONECTARLOS DEL MISMO.

 ADVERTENCIA
RIESGO DE EXPLOSIÓN LA SUSTITUCIÓN DE COMPONENTES PUEDE MERMAR LA APTITUD PARA LA CLASS I, DIVISION 2 O ZONE 2.

 **ADVERTENCIA**

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

3.1.2 Notas sobre el uso en áreas Ex según ATEX / IECEx

 **ADVERTENCIA**

Requisitos exigidos al armario de distribución

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

 **ADVERTENCIA**

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

 **ADVERTENCIA**

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

3.1.3 Indicaciones para el uso en la zona Ex según UL HazLoc

 **ADVERTENCIA**

RIESGO DE EXPLOSIÓN

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

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

3.2 Montar el dispositivo

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

Connectors with LAN (Local Area Network) marking

 ADVERTENCIA
Safety notice for connectors with LAN (Local Area Network) marking
A LAN or LAN segment, with all its associated interconnected equipment, shall be entirely contained within a single low-voltage power distribution and within single building. The LAN is considered to be in an "environment A" according IEEEE802.3 or "environment 0" according IEC TR 62102, respectively.
Never make direct electrical connection to TNV-circuits (Telephone Network) or WAN (Wide Area Network).

3.2 Montar el dispositivo

El montaje previsto para el CMR es sobre perfil DIN simétrico de 35 mm según DIN EN 50 022. En la parte posterior del dispositivo se encuentra un soporte correspondiente que lleva un pestillo con resorte.

Montaje en un perfil DIN simétrico/desmontaje de un perfil DIN simétrico

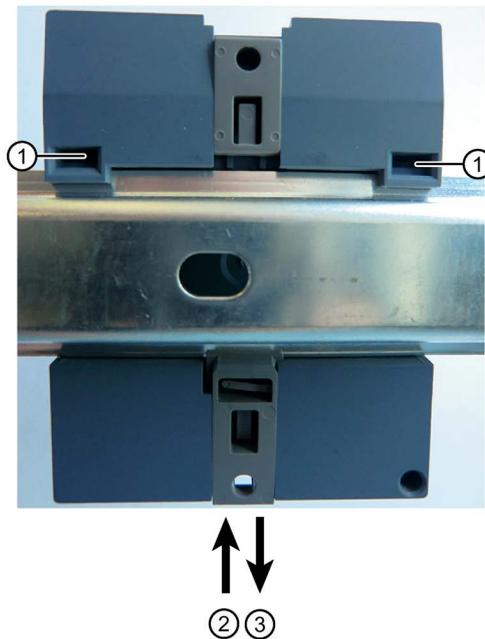


Figura 3-1 Montaje en un perfil DIN simétrico/desmontaje de un perfil DIN simétrico

Montaje

Para montar el CMR en un perfil DIN simétrico, proceda del siguiente modo:

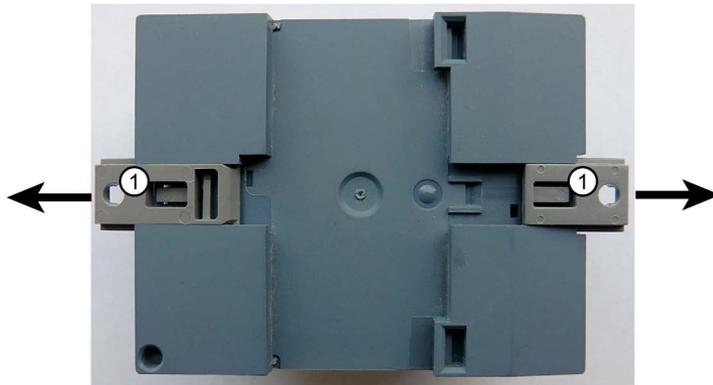
1. Enganche la guía de fijación superior ① del dispositivo en el perfil DIN simétrico.
2. Presione el dispositivo hacia abajo, contra el perfil DIN simétrico, hasta que el pestillo con resorte ② quede encajado.

Desmontaje

Para desmontar el CMR de un perfil DIN simétrico, proceda del siguiente modo:

1. Utilizando un destornillador, tire hacia abajo del pestillo con resorte situado en la parte posterior del dispositivo ③.
2. Quite el dispositivo del perfil DIN simétrico.

Montaje mural



Para montar el CMR en una pared, proceda del siguiente modo:

1. Utilizando un destornillador, tire hacia fuera de los dos pestillos con resorte ① situados en la parte posterior del dispositivo.
2. Pase los tornillos por los orificios de los pestillos y fije el dispositivo a la pared.

3.3 Conectar el dispositivo

3.3.1 Interfaz X1P1 (LAN)

Conectar la interfaz X1P1 (LAN)

Conecte su red local, el PC o el BM a la interfaz X1P1 (conexión LAN) del CMR.

La interfaz soporta "autonegotiation" y "autocrossing". Para la conexión utilice un latiguillo con conector RJ45. Consulte los requisitos y la puesta a tierra más abajo.

Encontrará las propiedades de la interfaz X1P1 en los datos técnicos.

Requisitos relativos al cable

Requisitos relativos al cable de red:

- Utilice un cable Ethernet apantallado para la conexión a la interfaz Ethernet.
- Con el fin de minimizar las perturbaciones electromagnéticas, utilice un cable Ethernet apantallado con un par de hilos trenzados (categoría 5) y un conector RJ45 apantallado en ambos extremos.
- Para evitar sobrecargas mecánicas del cable Ethernet, fije el cable a poca distancia del conector con una guía o carril.

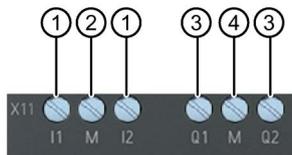
3.3.2 Entradas y salidas

Tenga en cuenta la capacidad de carga de las entradas y salidas indicada en los datos técnicos.

Utilice preferentemente interruptores con inhibición de rebote para la conexión a una entrada LOGO! CMR.

Entradas y salidas

El CMR dispone de dos entradas digitales y dos salidas digitales. Los bornes de conexión se encuentran en la parte inferior del dispositivo.



- ① Entradas I1 e I2
- ② Potencial de referencia de las entradas
- ③ Salidas Q1 y Q2
- ④ Potencial de referencia de las salidas

Entradas I1 e I2

Los bornes de conexión de las entradas están identificados con I1 e I2. El potencial de referencia para ambas entradas es "M".

Desde la interfaz web es posible asignar una función cualquiera a cada entrada, p. ej. la activación de un SMS de alarma; consulte el capítulo Monitoring (Página 115).

Además, el estado de una entrada puede leerse vía SMS.

Salidas Q1 y Q2

Los bornes de conexión de las salidas están identificados con Q1 y Q2. El potencial de referencia para ambas salidas es "M".

Desde la interfaz web es posible asignar una función cualquiera a cada salida; consulte el capítulo Monitoring (Página 115). Las salidas pueden activarse y desactivarse vía SMS.

Nota

Tenga en cuenta la capacidad de carga eléctrica de la salida.

Encontrará los valores eléctricos para las entradas y salidas en el capítulo Datos técnicos (Página 153).

3.3.3 Conectar la antena

 ADVERTENCIA
En caso de montaje exterior, peligro por rayos
Si monta una antena a la intemperie, debe poner a tierra la antena para protegerla contra rayos. Estos trabajos deben encomendarse a personal cualificado.

ATENCIÓN
Daños en el dispositivo por accesorios incorrectos
Seleccione la antena adecuada para su banda de frecuencias de la gama de accesorios. Las demás antenas pueden afectar a las características del producto o provocar fallos.

Nota

Longitud máxima del cable de antena

La longitud máxima admisible del cable de antena es de 15 m.

Para conectar las antenas, el CMR dispone de dos conectores hembra de antena del tipo SMA. Las antenas deben tener una impedancia de aprox. 50 Ω.

Tenga en cuenta las instrucciones de servicio de las antenas utilizadas. Consulte también el capítulo Antenas (Página 165).

Encontrará figuras de configuración con cables de antena para diferentes variantes de montaje en el capítulo Cable de antena (Página 167).

Bandas de frecuencia en Europa y en otras regiones

Seleccione la antena adecuada para su banda de frecuencia. Consulte el capítulo Antenas (Página 165).

Encontrará las bandas de frecuencia soportadas por el CMR en el capítulo Datos técnicos (Página 153).

Intensidad de señal

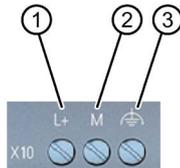
Al realizar la instalación asegúrese de tener una buena intensidad de señal. Encontrará el significado de los estados del LED "R" en el capítulo LED para la indicación del funcionamiento (Página 32).

Si el LED está encendido en color verde significa que la intensidad de señal es muy buena. Si está encendido en amarillo, la calidad es media.

Los grandes objetos de metal alrededor de las antenas, como hormigón armado, perjudican la intensidad de señal.

3.3.4 Alimentación

Bornes con tornillos para la alimentación eléctrica



- ① L+ = conductor de tensión, polo positivo de la tensión continua de 12/24 V DC
- ② M = polo negativo/masa de la tensión continua de 12/24 V DC
- ③ Puesta a tierra funcional
 - Sirve para mejorar la compatibilidad electromagnética y definir un potencial de referencia común para todas las señales.
 - Conviene efectuarla mediante una conexión con el perfil DIN simétrico.

Nota

La fuente de alimentación del CMR carece de aislamiento galvánico

Carecer de aislamiento galvánico significa que el circuito de entrada y el de salida no están aislados galvánicamente entre sí.

El CMR funciona con una tensión continua de 12 V a 24 V DC; tensión nominal de 24 V DC. El consumo de corriente nominal con 12 V es de 250 mA como máximo.

- Conecte una alimentación adecuada a los bornes con tornillos.
- Utilice solamente cables de cobre.
- Utilice únicamente conductores homologados para temperaturas de 70 °C como mínimo.

Hilo:	0,5 ... 3 mm ² (AWG 20 ... 18)
Trenza:	0,5 ... 2,5 mm ²
Par de apriete de los bornes con tornillos:	0,6 ... 0,8 Nm

Desconexión del CMR

ATENCIÓN

Evitar la desconexión repentina de la alimentación

Evite que el CMR se desconecte de la alimentación de forma repentina: en contadas ocasiones podría dañarse el CMR.

Antes de desconectar la alimentación de tensión, ponga el CMR al estado seguro.

1. Mantenga accionado el pulsador SET entre 5 y 10 s.

El CMR pasa al estado seguro. Todos los indicadores LED están apagados.

2. Desconecte el CMR de la alimentación.

También es posible poner el CMR en estado seguro desde el WBM.

No es posible volver a activar el CMR cuando está apagado. Para reactivarlo hay que desconectar la alimentación de tensión y volver a conectarla.

3.4 Puesta en servicio del dispositivo

3.4.1 Pasos para la puesta en marcha

Para poner en marcha el CMR, realice los siguientes pasos:

Vista general de la puesta en marcha

1. Tenga en cuenta los requisitos para el funcionamiento del CMR; consulte el capítulo Requisitos de aplicación (Página 18).
2. Tarjeta SIM: antes de insertar la tarjeta SIM, es imprescindible que tenga en cuenta las indicaciones del apartado Insertar la tarjeta SIM e introducir el PIN (Página 48) en cuanto a los diferentes métodos:
 - Método 1: en un dispositivo nuevo
 - Método 2: sustitución de la tarjeta SIM en un dispositivo ya utilizado
3. Conecte un PC con navegador web a la interfaz local X1P1 del CMR; consulte el capítulo Establecer la conexión con el CMR (Página 68).
4. Inserte la tarjeta SIM; consulte el capítulo Insertar la tarjeta SIM e introducir el PIN (Página 48).
5. Conecte las antenas.
6. Conecte el CMR a la alimentación.
7. Introduzca el PIN de la tarjeta SIM a través de la interfaz web del CMR; consulte el capítulo Mobile wireless settings (Página 94).

- Orienta la antena; consulte el capítulo Wireless cell (Página 97).
- Configure el CMR según sus necesidades; consulte el capítulo Configuración (WBM) (Página 57).

3.4.2 Insertar la tarjeta SIM e introducir el PIN

ATENCIÓN
Desconectar el CMR de la alimentación antes de insertar o extraer la tarjeta SIM
No extraiga la tarjeta SIM durante el funcionamiento.
1. Apague el dispositivo para llevarlo a un estado seguro.
2. Desconecte el CMR de la alimentación antes de insertar o extraer la tarjeta SIM.

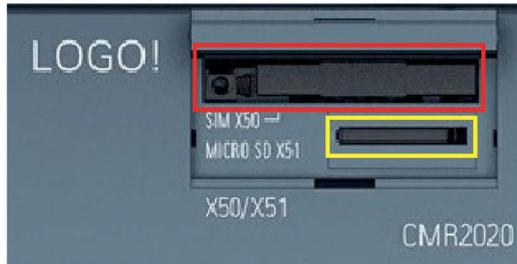


Figura 3-2 Ranura para la tarjeta SIM (recuadro rojo)

La ranura para la tarjeta SIM se encuentra en la parte frontal del CMR.

Estado del CMR antes de insertar/extraer la tarjeta SIM

El CMR es nuevo de fábrica o se ha restablecido a la configuración de fábrica:

- Se inserta una tarjeta SIM por primera vez.

El CMR está o ya ha estado en funcionamiento:

- Simplemente se inserta otra tarjeta SIM.

Inserción/extracción de la tarjeta SIM

- En el WBM, en "WAN", ficha "Mobile wireless settings", desactive la casilla de verificación "Activate mobile wireless interface": se desconecta la interfaz de telefonía móvil.
- Apague el CMR para llevarlo a un estado seguro: "Desconexión del CMR" (Página 46).
- Desconecte el CMR de la alimentación.

4. Solo si el CMR está o ha estado en funcionamiento: extraiga la tarjeta SIM y cierre la ranura.
Presione el pulsador de expulsión hundido en el lado izquierdo con un objeto puntiagudo para extraer la tarjeta SIM.
5. Inserte la tarjeta SIM en la ranura hasta que se perciba cómo queda encajada.
6. Reinicie el CMR conectándolo a la alimentación.
7. En el WBM, en "WAN", ficha "Mobile wireless settings", active la casilla de verificación "Activate mobile wireless interface":
la interfaz de telefonía móvil vuelve a estar lista para el uso.
8. En el WBM, en "WAN", ficha "Mobile wireless settings", introduzca el PIN de su tarjeta SIM.

Nota

Introducción de un PIN erróneo

El PIN introducido en último lugar (erróneo) queda guardado. Si se modifica la configuración (excepto el PIN) o si se reinicia el CMR, dicho número no consume ningún intento de introducción de PIN.

Por lo tanto, no cambie el PIN de la tarjeta SIM fuera del CMR al PIN erróneo guardado anteriormente.

9. Haga clic en el botón "Apply": se aplica el PIN de su tarjeta SIM.
10. Realice los ajustes correspondientes, consulte el capítulo Configuración (WBM) (Página 57).

Desbloquear la tarjeta SIM

Si introduce un PIN erróneo por 3.^a vez, se bloqueará la tarjeta SIM.

Desbloquee la tarjeta SIM del siguiente modo:

1. Apague el CMR para llevarlo a un estado seguro: "Desconexión del CMR" (Página 46).
2. Desconecte el CMR de la alimentación.
3. extraiga la tarjeta SIM y cierre la ranura.

Presione el pulsador de expulsión hundido en el lado izquierdo con un objeto puntiagudo para extraer la tarjeta SIM.

4. Inserte la tarjeta SIM extraída en un teléfono móvil.
5. Desbloquee la tarjeta SIM introduciendo el PUK o el SuperPIN.

El operador de telefonía móvil le habrá enviado el PUK o el SuperPIN junto con la tarjeta SIM.

Resultado: la tarjeta SIM está desbloqueada y puede volver a utilizarse.

3.4.3 Insertar la tarjeta SD

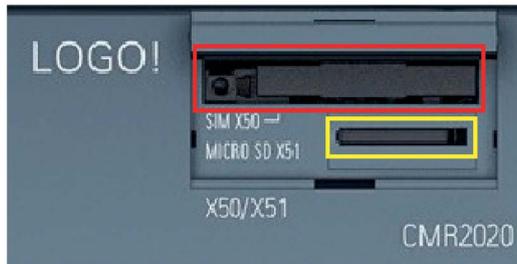


Figura 3-3 Ranura para la tarjeta Micro SD (recuadro amarillo)

Encontrará las tarjetas SD soportadas por el CMR en el anexo Tarjeta SD (Página 171).

ATENCIÓN

No extraer/insertar la tarjeta SD durante el funcionamiento

La tarjeta SD solo debe extraerse o insertarse cuando el CMR se encuentra desconectado o apagado.

Si se extrae o inserta la tarjeta SD durante el funcionamiento, pueden producirse daños en los datos guardados en la tarjeta.

Inserción de la tarjeta Micro SD

1. Introduzca la tarjeta SD en la ranura hasta que encaje.

Extracción de la tarjeta Micro SD

1. Presionando la tarjeta se desenclava.
2. Extraiga la tarjeta del slot una vez desenclavada.

Operación: Acceso al BM

4.1 Sinopsis

Acceso de lectura y escritura

Desde un teléfono móvil o una tableta es posible acceder en modo de lectura y escritura al CMR o al BM mediante SMS.

Encontrará una relación de las funciones en el capítulo Otras funciones (Página 15).

Vigilancia del LOGO! BM

Funciones

Para la vigilancia del CMR y de un BM conectado están disponibles varias funciones que se configuran en el WBM.

El capítulo Monitoring (Página 115) describe las funciones siguientes:

- Vigilancia de valores del BM
- Creación de una acción en función del cambio de valor de un evento
Puede ser, por ejemplo, el envío de un SMS a un número de teléfono configurado a causa de una alarma.
- Creación de destinatarios y grupos de destinatarios para mensajes del CMR
- Notificación a un grupo de destinatarios con textos de SMS y correo electrónico libres en caso de eventos

Ejemplo

Encontrará el modo de configurar rápidamente una vigilancia en el capítulo Ejemplo de configuración de la vigilancia (Página 132).

Allí se muestra un ejemplo que enseña a configurar eventos, acciones y destinatarios.

A continuación se representa el modo de vincular eventos, acciones y destinatarios en una lista de forma aleatoria.

4.2 Lectura y escritura de valores

Lectura/escritura de "valores actuales" mediante la memoria de variables (VM) del BM

Los "valores actuales" (p. ej. marcas o contadores) se leen y escriben únicamente mediante la memoria de variables (VM) del BM.

4.2 Lectura y escritura de valores

Por razones de seguridad, los valores actuales de los bloques de función del BM (p. ej., contadores) se ajustan y se leen exclusivamente a través de su dirección en la memoria de variables del BM.

Por lo tanto, todos los componentes de un programa de conmutación LOGO! deben transferirse primero a la memoria de variables interna del BM mediante el programa "LOGO! Soft Comfort". Solo entonces el CMR podrá ver los componentes con su dirección inicial y su longitud (tipo) en la memoria de variables del BM.

Tipos de datos y rangos de valores al leer y escribir

Los diferentes bits deben activarse utilizando los tipos de datos disponibles.

LOGO! CMR y LOGO! BM interpretan todos los valores de los tipos de datos BYTE, WORD y DWORD como valores con signo.

Téngalo en cuenta al transferir valores por SMS.

Tipo de datos	Longitud en la memoria de variables	Rango de valores
BIT	1 bit	0, 1
BYTE	1 byte	-128 ... 127
WORD	2 bytes	-32 768 ... 32 767
DWORD	4 bytes	-2 147 483 648 ... 2 147 483 647

Leer y escribir valores en la memoria de variables (VM) del LOGO! BM por medio de SMS

El LOGO! CMR permite leer y escribir valores en la memoria de variables (VM) de un LOGO! BM utilizando SMS.

En los comandos del SMS deben indicarse los parámetros de dirección y tipo (<dirección>,<tipo de datos>); consulte el capítulo Comandos SMS (Página 176).

En la página "Vigilancia" > "Eventos" del WBM del LOGO! CMR puede indicarse un valor límite o umbral para un valor del LOGO! 8. Si se rebasa por exceso o defecto el umbral del valor en el LOGO! 8, puede configurarse como evento el envío de un SMS a uno o varios destinatarios, por ejemplo.

Tenga en cuenta la interpretación del signo en los valores también en los siguientes casos de aplicación:

- Establecimiento de valores límite/umbral para valores del LOGO! BM desde el WBM del LOGO! CMR
- Visualización de valores en el LOGO! BM desde el WBM del LOGO! CMR
- Lectura/escritura de valores en el LOGO! BM mediante SMS con el LOGO! CMR

Lectura y escritura directamente desde LOGO!Soft Comfort (sin CMR)

Nota

Acceso solo a los primeros 128 bytes de la VM (Variable Memory)

En LOGO!Soft Comfort, la VM llega hasta la dirección 850. Sin embargo, desde el CMR solo es posible acceder a los primeros 128 bytes.

Por razones de seguridad, solo se puede acceder a la dirección de la VM en modo de lectura y escritura mediante SMS si la dirección se ha creado previamente como señal mediante el WBM.

Tabla 4- 1 Vista general de las posibilidades de acceso al LOGO! BM

Valor del LOGO! BM	Acceso de lectura	Acceso de escritura mediante acción	Acceso de escritura mediante SMS
Entradas digitales (I)	x	-	-
Marcas digitales (M)	x	-	-
Salidas digitales (Q)	x	-	-
Entradas analógicas (AI)	x	-	-
Marcas analógicas (AM)	x	-	-
Salidas analógicas (AQ)	x	-	-
Teclas de cursor (C)	x	-	-
Teclas de función (F)	x	-	-
Bits de registro de desplazamiento (S)	x	-	-
Memoria de variables (VM)	x	x ¹⁾	x
Estado de programa (PS)	x	x	x
Estado de comunicación (CS)	x	-	-

¹⁾ A la memoria de variables del LOGO! BM se accede en modo de escritura mediante la acción "Forward GPS position".

Ejemplo para escribir un valor mediante LOGO!Soft Comfort

A continuación encontrará un ejemplo del procedimiento para escribir un valor mediante LOGO!Soft Comfort. Seguidamente, se accede al valor escrito mediante SMS desde el CMR.

1. En el programa "LOGO! Soft Comfort", haga clic en "Tools" > "Parameter VM Mapping":

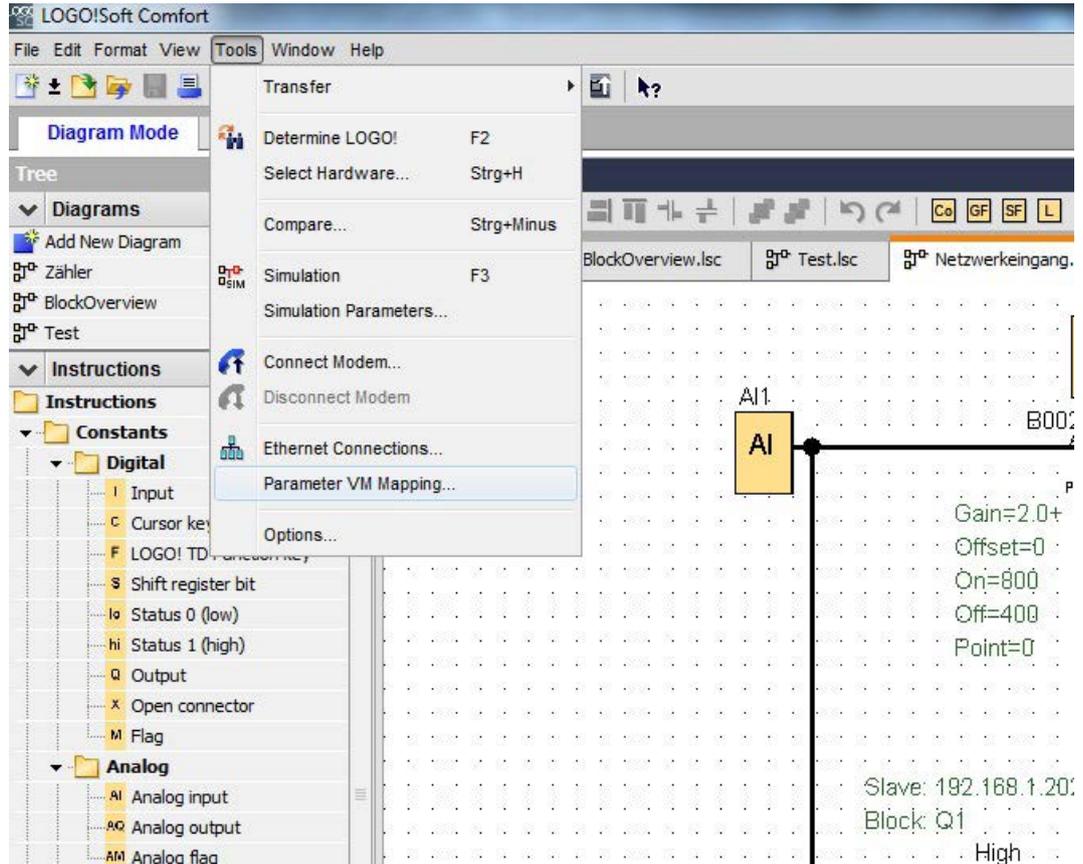


Figura 4-1 LOGO! Soft Comfort - Tools

2. Seleccione un bloque de su programa de conmutación que desee transferir a la VM.

En la figura siguiente, elija el bloque B007 del programa de conmutación con función de cronómetro.

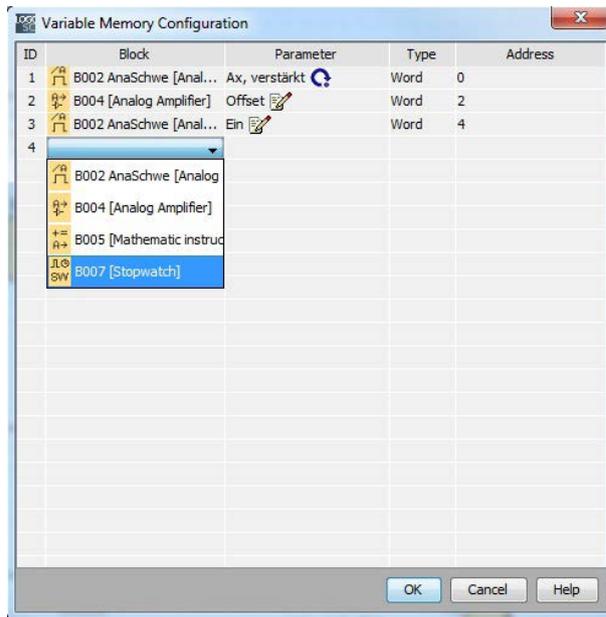


Figura 4-2 Variable Memory Configuration

3. A continuación, dentro del bloque B007, seleccione una variable que desee vigilar.
4. Haga clic en el botón "OK" para confirmar la selección.

La variable elegida se transfiere a la VM.

Las opciones "Type" y "Address" de la variable seleccionada se muestran en la VM.

Encontrará más detalles en la descripción de LOGO! Soft Comfort.

Leer variables desde el CMR mediante SMS

Las palabras clave "dirección", "valor" y "tipo de datos" permiten leer y escribir el valor de una variable mediante SMS; consulte el capítulo Comandos SMS (Página 176).

Configuración (WBM)

5.1 Recomendaciones Security

Observe las siguientes recomendaciones sobre Security 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.
- Mantenga actualizado el firmware. Infórmese periódicamente sobre las actualizaciones de seguridad del firmware y aplíquelas.
- Infórmese periódicamente sobre las novedades en las páginas web de Siemens.
 - Aquí encontrará información acerca de la seguridad de la red:
Enlace: (<http://www.siemens.com/industrialsecurity>)
 - Aquí encontrará información acerca de Industrial Ethernet Security:
Enlace: (<http://w3.siemens.com/mcms/industrial-communication/es/ie/industrial-ethernet-security/Seiten/industrial-security.aspx>)
 - Encontrará una introducción al tema Industrial Security en el impreso siguiente:
Enlace:
(http://w3app.siemens.com/mcms/infocenter/dokumentencenter/sc/ic/InfocenterLanguagePacks/Netzwerksicherheit/6ZB5530-1AP01-0BA4_BR_Netzwerksicherheit_en_112015.pdf)

Acceso físico

Limite el acceso físico al equipo al personal cualificado.

Funciones de seguridad del producto

Aproveche las posibilidades de los ajustes de seguridad en la configuración del producto. Incluyen, entre otras, la siguiente función de Security de la comunicación:

- Active las funciones de Security del dispositivo.
Piense con qué servicios desea permitir el acceso a la estación a través de redes públicas.
- Utilice variantes de protocolo seguras como, por ejemplo, HTTPS o STARTTLS.
- Utilice la comunicación segura vía OpenVPN.

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.
- 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 HTTP ofrece una alternativa segura con HTTPS.

Tablas de puertos

Las tablas siguientes le ofrecen 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 dispositivo siempre es cliente para este servicio.
- **Autenticación**
Indica si el protocolo autentica el interlocutor durante el acceso.

Tabla 5- 1 Puertos de la interfaz LAN

Protocolo / función	Número de puerto (protocolo)	Ajuste predeterminado del puerto	Estado del puerto	Autenticación
HTTP	80 (TCP)	Abierto	Abierto (inicio de sesión si está configurado)	Sí
HTTPS	443 (TCP)	Abierto	Abierto (inicio de sesión si está configurado)	Sí
LOGO!	Dinámico (TCP)	Cerrado	Abierto (de salida) tras configuración	No

Tabla 5- 2 Puertos de la interfaz WAN

Protocolo / función	Número de puerto (protocolo)	Ajuste predeterminado del puerto	Estado del puerto	Autenticación
HTTPS	443 (TCP)	Cerrado	Abierto tras configuración	Sí
OpenVPN	1194 (UDP) ajustable	Cerrado	Abierto tras configuración	Sí
NTP	123 (UDP)	Cerrado	Abierto (de salida) tras configuración	No
SMTP	Dinámico (TCP)	Cerrado	Abierto (de salida) tras configuración	Sí
DynDNS	Dinámico (TCP)	Cerrado	Abierto (de salida) tras configuración	Sí
DNS	Dinámico (UDP)	Cerrado	Abierto (de salida) tras configuración	No

5.2 Funciones generales del WBM

Para configurar el CMR está disponible una interfaz de administración basada en web (WBM - Web Based Management).



- En el margen izquierdo se encuentra el índice de navegación.
- Haciendo clic en una entrada principal (grupo) de la navegación se muestran en la parte derecha de la barra de título las fichas correspondientes a dicho grupo.
- En las diferentes páginas de las fichas se muestran los campos de visualización y entrada de los parámetros.

Símbolos de la barra de título

Los símbolos de la barra de título del WBM tiene las funciones siguientes:

Símbolo	Función
2015-01-28 14:30:37	Fecha y hora de la última actualización de páginas del WBM en la hora local del CMR (yyyy-mm-dd hh:mm:ss)
English	Lista desplegable para configurar el idioma del WBM
User: 1	Nombre del usuario actual que ha iniciado sesión
Log out	Cierre de sesión del usuario
Number of active sessions: 1	Número de conexiones con PC de configuración
	La actualización automática de la pantalla del WBM está activada. Los datos se consultan cada 5 segundos.
	La actualización automática de la pantalla del WBM está desactivada.

Símbolo	Función
	Activa la actualización automática de la pantalla del WBM.
	Desactiva la actualización automática de la pantalla del WBM.
	Actualiza la pantalla actual del WBM en las páginas "Configuration".
	Impresión de la página actual del WBM
	Abre la página web del CMR en el Siemens Industry Online Portal. En ella encontrará todos los artículos sobre el producto.
	Abrir y guardar las condiciones de la licencia de Open Source Software del CMR.

Ajuste del idioma

El WBM del CMR está disponible en alemán e inglés.

Ajuste predeterminado

Si el navegador web está ajustado al idioma inglés, por ejemplo, el WBM del CMR se muestra también de forma automática en inglés.

Si el idioma ajustado para el navegador web no se soporta, el WBM del CMR se muestra también en inglés.

Cambiar el ajuste del idioma

En la parte superior derecha hay una lista desplegable para la selección del idioma. El idioma puede cambiarse en todo momento:

- Seleccione el idioma deseado en la lista desplegable de la parte superior derecha.
El ajuste del idioma se guarda para el próximo acceso.
- Si el idioma no cambia de inmediato, actualice la representación del navegador web, normalmente pulsando la tecla de función F5.

Configurar

En las páginas de las diferentes fichas se lleva a cabo la configuración de los parámetros. Para ello se dispone de lo siguiente:

- Campos de entrada para introducir números y textos
- Listas desplegables para seleccionar parámetros
- Casillas de verificación para activar y desactivar funciones
- Botones para ejecutar acciones específicas de la página y para guardar las entradas ("Apply")
- Indicaciones e informaciones

Entradas erróneas en la configuración

En muchos campos de entrada del WBM, al guardar se verifica si falta contenido y si los contenidos son congruentes. Los campos con errores detectados o con caracteres no permitidos se marcan con un recuadro en rojo.



192.168.0.999

Figura 5-1 Ejemplo de un campo de entrada con una entrada errónea detectada

En algunas entradas erróneas aparece además una indicación. Los ajustes solo se aplican una vez realizadas las correcciones oportunas.

Agregar, modificar y borrar ("Users / groups", "Monitoring")

En las páginas de estos dos grupos de parámetros se crean elementos nuevos y se borran elementos existentes. Los elementos son:

usuarios, grupos destinatarios, textos de mensajes, señales, eventos, acciones y asignaciones

Los elementos que ya están configurados se muestran en la parte superior de una tabla en la página correspondiente.

- **Add**

Para crear un elemento nuevo haga clic en el botón "Add".

Se muestra un campo de entrada vacío que permite asignar el nombre del nuevo elemento.

Configure los parámetros del elemento a continuación.

- **Modificar**

Seleccione un elemento de la tabla en la página correspondiente y realice los cambios en los campos de parámetros situados en la parte inferior.

- **Delete**

Solo es posible borrar elementos que no se utilizan. Si, por ejemplo, un texto se utiliza para un mensaje, un usuario dentro de un grupo de destinatarios o una señal dentro de un evento, dichos elementos no se pueden borrar.

Seleccione en la tabla la fila que contiene el elemento que debe borrarse y haga clic en el botón "Delete".

Se muestra una consulta de seguridad.

Si se confirma haciendo clic en el botón "Delete", el elemento seleccionado se borra y se quita de la lista.

Guardar

Confirme todas sus entradas haciendo clic en el botón "Apply". El dispositivo aplicará los ajustes efectuados. En el caso de algunos parámetros el proceso puede durar algunos segundos. Si se cambia la configuración de telefonía móvil, puede durar incluso varios minutos.

Los campos atenuados están predeterminados por el sistema y no pueden modificarse.

Nota

Pérdida de datos al cambiar de página del WBM sin guardar

Si no se guardan las entradas mediante el botón "Apply", se rechazarán sin consultar cuando se cambie de página del WBM.

Guardar archivos de configuración

Los ajustes relacionados con la configuración de un dispositivo pueden guardarse en un archivo de configuración. Dicho archivo puede volver a cargarse en caso necesario o transferirse a otro dispositivo del mismo tipo. Encontrará información al respecto en el capítulo Configuration (Página 83).

5.3 Datos de prestaciones y capacidad funcional

Se puede definir...	Número máximo/observación
Usuarios	20
Grupos destinatarios	10; a cada grupo destinatario se le pueden asignar 10 usuarios como máximo.
Contraseña	1
Números de teléfono	20
Direcciones de correo electrónico	20
Textos de mensajes	20; 160 caracteres por texto como máximo. El texto del mensaje se puede emplear al mismo tiempo para SMS y correo electrónico.
Señales	32
Eventos	32
Acciones	32
Comandos SMS alias	20
Constantes	10
Conexiones	
• a LOGO! BM	1
• vía HTTP	1
• vía HTTPS	2; HTTP y HTTPS se pueden combinar (no más de 2 conexiones). En la interfaz de telefonía móvil se permite 1 conexión vía HTTPS como máximo.
• como cliente de correo electrónico	1
• como servidor VPN	1

5.4 Caracteres permitidos y longitudes de strings

Nota

Recepción correcta de mensajes SMS

CMR solamente puede recibir mensajes SMS correctamente si los mensajes cumplen con el juego de caracteres GSM 03.38 o UCS-2.

Nota

Espacios en blanco al principio y al final

En los nombres no se permiten espacios en blanco al principio ni al final. El WBM muestra un aviso de que la entrada es incorrecta. Excepción: descripciones y textos de mensajes SMS.

Uso de caracteres especiales

Si se utilizan caracteres especiales, no puede garantizarse que no se exceda la longitud máxima.

A continuación encontrará los caracteres permitidos y las longitudes de strings que pueden utilizarse para la configuración de nombres de usuario, contraseñas, parámetros y textos. Suelen indicarse juegos de caracteres ASCII. A continuación encontrará los juegos de caracteres ASCII junto con el código hexadecimal y los caracteres correspondientes.

Caracteres estándar

- 0x30 .. 0x39

0 1 2 3 4 5 6 7 8 9

- 0x41 .. 0x5A

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

Caracteres especiales

- 0x21 .. 0x2F

! " # \$ % & ' () * + , - . /

- 0x3A .. 0x40

: ; < = > ? @

- 0x5B .. 0x60

[\] ^ _ `

- 0x7B .. 0x7E

{ | } ~

Caracteres especiales ≥ 0x80

- 0x80, 0xA3, 0x8A, 0x9A, 0x8E, 0x9E, 0xB5

€ £ Š š Ž ž μ

- 0xC0 .. 0xFF

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

Tabla 5- 3 Caracteres permitidos y no permitidos, longitudes de strings

Campo de entrada	Longitud de string mínima	Longitud de string máxima	Caracteres permitidos	Caracteres no permitidos
General				
<ul style="list-style-type: none"> • Name excepto nombres de módulos y servidores (NTP, correo electrónico, DynDNS) 	1	20	Todos los caracteres	
<ul style="list-style-type: none"> • Description excepto Plant description 	0	50		
System				
<ul style="list-style-type: none"> • Module name • Nombre del servidor NTP 	1	20 63	Nombre DNS según RFC1035 y RFC1123: <ul style="list-style-type: none"> • Caracteres estándar 0x30 .. 0x39, 0x41 .. 0x5A, 0x61 .. 0x7A • Caracteres especiales: raya (0x2D), punto (0x2E) 	
<ul style="list-style-type: none"> • Plant description 	0	20	Todos los caracteres	
WAN				
<ul style="list-style-type: none"> • PIN de la SIM ¹⁾ 	4	8	0 ... 9	a ... z, A ... Z
<ul style="list-style-type: none"> • APN 	1	63	Nombre DNS según RFC1035 y RFC1123: <ul style="list-style-type: none"> • Caracteres estándar 0x30 .. 0x39, 0x41 .. 0x5A, 0x61 .. 0x7A • Caracteres especiales: raya (0x2D), punto (0x2E) 	
<ul style="list-style-type: none"> • Name • Password 	0 0	20 20	<ul style="list-style-type: none"> • Caracteres estándar 0x30 .. 0x39, 0x41 .. 0x5A, 0x61 .. 0x7A • Caracteres especiales 0x21 .. 0x2F, 3A .. 40, 0x5B .. 0x60, 0x7B .. 0x7E 	

5.4 Caracteres permitidos y longitudes de strings

Campo de entrada	Longitud de string mínima	Longitud de string máxima	Caracteres permitidos	Caracteres no permitidos
<ul style="list-style-type: none"> Contraseña SMS 	1	8	<ul style="list-style-type: none"> 0x21 .. 0x2F 0x30 .. 0x39 0x41 .. 0x5A 0x61 .. 0x7A 0x3A 0x3C .. 0x40 	; [\]^`{ }~° '€
Correo electrónico				
<ul style="list-style-type: none"> Servidor de correo 	1	63	Nombre DNS según RFC1035 y RFC1123: <ul style="list-style-type: none"> Caracteres estándar 0x30 .. 0x39, 0x41 .. 0x5A, 0x61 .. 0x7A Caracteres especiales: raya (0x2D), punto (0x2E) 	
<ul style="list-style-type: none"> Dirección de correo electrónico 	1	127	<ul style="list-style-type: none"> Caracteres estándar 0x30 .. 0x39, 0x41 .. 0x5A, 0x61 .. 0x7A Caracteres especiales 0x21 .. 0x2F, 0x3D, 0x3F .. 0x40, 0x5B .. 0x60, 0x7B .. 0x7E: <ul style="list-style-type: none"> ! " # \$ % & ' () * + , - . / = ? @ [\] ^ _ ` { } ~ 	
<ul style="list-style-type: none"> Nombre del usuario de correo electrónico 	1	127	Todos los caracteres	
<ul style="list-style-type: none"> Contraseña 	1	32	<ul style="list-style-type: none"> Caracteres estándar 0x30 .. 0x39, 0x41 .. 0x5A, 0x61 .. 0x7A Caracteres especiales 0x21 .. 0x2F, 3A .. 40, 0x5B .. 0x60, 0x7B .. 0x7E 	ß ä ö ü Ä Ö Ü § ' € é è
DynDNS				
<ul style="list-style-type: none"> Nombre de host 	1	63	Nombre DNS según RFC1035 y RFC1123: <ul style="list-style-type: none"> Caracteres estándar 0x30 .. 0x39, 0x41 .. 0x5A, 0x61 .. 0x7A Caracteres especiales: raya (0x2D), punto (0x2E) 	
<ul style="list-style-type: none"> Nombre del usuario de DynDNS 	1	127	Todos los caracteres	
<ul style="list-style-type: none"> Contraseña 	1	32	<ul style="list-style-type: none"> Caracteres estándar 0x30 .. 0x39, 0x41 .. 0x5A, 0x61 .. 0x7A Caracteres especiales 0x21 .. 0x2F, 3A .. 40, 0x5B .. 0x60, 0x7B .. 0x7E 	ß ä ö ü Ä Ö Ü § ' € é è

5.4 Caracteres permitidos y longitudes de strings

Campo de entrada	Longitud de string mínima	Longitud de string máxima	Caracteres permitidos	Caracteres no permitidos
Users / groups				
<ul style="list-style-type: none"> Números de teléfono 	0	20	Formato: +<Código de país><Número de destinatario> Cifras y los siguientes caracteres especiales: <ul style="list-style-type: none"> 0x22 ... 0x7E 0x2B (signo más: comodín para las cifras de prefijo internacional delante del código de país) 0x2A (asterisco al final: comodín para extensiones) 0x2F, 0x28, 0x29 (/ () como separador) 0x32 (espacio en blanco) 	
<ul style="list-style-type: none"> User name 	1	20	0 ... 9, a ... z, A ... Z , - @ _ .	ß ä ö ü Ä Ö Ü \$ ' € é è
<ul style="list-style-type: none"> Password Nota: Si la opción "Do not use password rules" está activada, no se aplican reglas de contraseña y la longitud mínima se reduce a cero.	8	20	<ul style="list-style-type: none"> Caracteres estándar 0x30 .. 0x39, 0x41 .. 0x5A, 0x61 .. 0x7A 0 ... 9, a ... z, A ... Z Caracteres especiales 0x21 .. 0x2F, 3A .. 40, 0x5B .. 0x60, 0x7B .. 0x7E ! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { } ~ 	ß ä ö ü Ä Ö Ü \$ ' € é è

Campo de entrada	Longitud de string mínima	Longitud de string máxima	Caracteres permitidos	Caracteres no permitidos
Monitoring				
<p>Textos de mensajes SMS, incluidos hasta 16 comodines para valores de proceso con indicaciones de formateado.</p> <p>Tenga en cuenta lo siguiente: los comodines se reemplazan por valores reales antes de enviarse, lo que puede provocar que la longitud del texto exceda el límite de 160 caracteres. Si se excede la longitud máxima de caracteres, se generan y envían hasta 2 mensajes SMS.</p>	0	160	<ul style="list-style-type: none"> Caracteres estándar 0x30 .. 0x39, 0x41 .. 0x5A, 0x61 .. 0x7A 0 ... 9, a ... z, A ... Z Espacio 0x32 Caracteres especiales 0x21 .. 0x2F, 0x3A .. 0x40, 0x5F, 0xA7 ! " # \$ % & ' () * + , - . / : ; < = > ? @ _ ` { } ~ Diéresis y ß: 0xC4, 0xE4, 0xD6, 0xF6, 0xDC, 0xFC, 0xDF, 0xE8, 0xE9 Ä ä Ö ö Ü ü ß è é <p>Los corchetes [y] (0x1B y 0x1D) están reservados para los comodines.</p> <p>Para los comodines de los valores de proceso se admiten los formatos siguientes; V significa un nombre de señal configurado. Los nombres de señal no deben contener los caracteres [y]:</p> <ul style="list-style-type: none"> [V]: valor decimal de la señal <p>Otros comodines:</p> <ul style="list-style-type: none"> [DATE]: fecha actual Formato: yyyy-mm-dd [GPS]: su valor es la posición GPS Formato: ddd:mm:ss.hs N/S ddd:mm:ss.hs W/E Alt m [TIME]: hora actual Formato: hh:mm:ss [DEVNAME]: Module name 	[\] ^ ` { } ~

1) También se permite que no haya PIN.

5.5 Establecer la conexión con el CMR

Para configurar el CMR se necesita un PC con uno de los siguientes navegadores web.

- Internet Explorer: a partir de la versión 11.0
- Firefox: a partir de la versión 28.0
- Google Chrome: a partir de la versión 33.0
- Apple Safari: a partir de la versión de iOS 9.0

La configuración se realiza con ayuda de la interfaz web (WBM) del CMR.

Son posibles 2 sesiones simultáneas como máximo (2 usuarios que hayan iniciado sesión). Ambas poseen acceso de escritura completo.

Nota

Por telefonía móvil y HTTPS solo es posible una sesión.

Existe la posibilidad de establecer una segunda sesión a través de la interfaz LAN local.

Configuración mediante la interfaz local

Deben cumplirse los siguientes requisitos para realizar la configuración mediante la interfaz local X1P1:

- El PC debe estar conectado al conector hembra Ethernet X1P1 del CMR o bien disponer de acceso directo al CMR a través de la red local.
- El adaptador de red del PC debe tener la siguiente configuración IP:
 - La misma subred: 255.255.255.0
 - La dirección del PC debe estar en la subred de la interfaz LAN del CMR.
 - Dirección IP (por ejemplo): 192.168.0.4

5.5.1 Establecer la conexión de configuración

Para configurar el CMR, primero debe establecerse una conexión con el dispositivo mediante un navegador web. Para ello, proceda del siguiente modo:

Configurar el navegador web

1. Inicie el navegador web en el PC.
2. Configure el navegador de forma que no seleccione automáticamente una conexión al iniciarse.

Por ejemplo, en Microsoft Internet Explorer realice los siguientes ajustes:

- En el menú, elija el comando "Herramientas" > "Opciones de Internet".
- Elija la ficha "Conexiones".
- Para borrar entradas de "Configuración de acceso telefónico y de redes privadas virtuales", haga clic en el botón "Quitar".
- Active el botón de opción "No marcar nunca una conexión".

Llamar la página inicial del CMR

Introduzca la dirección IP completa del CMR en la barra de direcciones del navegador.

En el ajuste de fábrica la dirección IP es: <http://192.168.0.3> o <https://192.168.0.3>

Pulse la tecla Intro.

Nota

Advertencia sobre el certificado (HTTPS)

Cuando se establece la conexión vía HTTPS, al iniciar la sesión se genera una advertencia indicando que la página web no es segura o que el certificado no es fiable. Si está seguro de que ha introducido la dirección correcta, ignore el aviso. En caso necesario, agregue la conexión a las excepciones de su navegador web (depende del navegador).

Introducir el nombre de usuario y la contraseña

Se le pide que introduzca el nombre de usuario y la contraseña. Los ajustes de fábrica son:

Datos de usuario	Valores preconfigurados de fábrica
User name	admin
Password	admin

Después de iniciar sesión por primera vez, se le pedirá que cambie la contraseña. Al hacerlo, tenga en cuenta las reglas básicas para contraseñas seguras (consulte las indicaciones en el WBM).

Nota

Cambiar los datos de usuario estándar

Por razones de seguridad se recomienda crear otro usuario después de iniciar la primera sesión. Encontrará la descripción en el capítulo Users / groups (Página 112).

Nota

Pérdida de datos de usuario estándar modificados

Anote los nombres de usuario y las contraseñas modificados o de nueva asignación.

Si se modifican los datos del usuario estándar, se pierden los datos de usuario modificados y no se ha creado un segundo usuario, ya no será posible acceder al WBM del CMR. En ese caso no será posible volver a acceder al WBM del CMR hasta que se restablezca la configuración de fábrica. Al restablecerla se pierden los datos de configuración.

Se muestra la página inicial

Al introducir el nombre de usuario y la contraseña, aparece la Start page del CMR en el navegador web. La Start page muestra una vista general del estado operativo del dispositivo.

No se muestra la página inicial

Si el navegador notifica que la página no puede mostrarse incluso después de varias tentativas, pruebe lo siguiente:

Comprobar la conexión de hardware

1. Abra el símbolo del sistema DOS seleccionando el comando de menú "Inicio" > "Todos los programas" > "Accesorios" > "Símbolo del sistema".

Resultado: aparece la ventana "Símbolo del sistema".

2. Introduzca el comando "ping 192.168.0.3".

Si funciona correctamente, en un lapso de escasos segundos se recibirán cuatro respuestas.

Si pasados unos segundos no se han recibido las cuatro respuestas, hay que comprobar si el cable de red, las conexiones y la tarjeta de red están bien conectados.

No utilizar ningún servidor proxy

En función del sistema operativo, proceda del siguiente modo:

1. Elija el comando de menú "Herramientas" > "Opciones de Internet".
2. Elija la ficha "Conexiones".
3. Haga clic en el botón "Configuración de LAN".

Se abre el cuadro de diálogo "Configuración de la red de área local".

4. Desactive la casilla de verificación "Usar un servidor proxy para la LAN" de la entrada "Servidor proxy".

Desactivar otras conexiones LAN

Si hay otras conexiones LAN activas en el PC, desactive dichas conexiones LAN durante la configuración.

En Windows 7, proceda del siguiente modo:

1. En el menú Inicio, elija el comando "Inicio" > "Panel de control" > "Redes e Internet" > "Centro de redes y recursos compartidos"
2. En "Ver las redes activas" se muestran las conexiones LAN actuales.
3. Haga clic con el botón izquierdo del ratón en las denominaciones correspondientes de las conexiones en "Tipos de acceso de las conexiones".

Se abre el cuadro de diálogo correspondiente a la conexión elegida.

4. Haga clic en el botón "Deshabilitar".

Se cierra el cuadro de diálogo. Se ha deshabilitado la conexión LAN deseada.

Cambiar la interfaz del CMR tras la configuración

Es posible que deba adaptarse la interfaz LAN del CMR para el equipo conectado o la red local tras configurar el CMR.

Para ello proceda del siguiente modo:

1. Seleccione en la navegación la página "LAN > Configuration".
2. Realice allí los cambios de direcciones.
3. Haga clic en el botón "Apply".

Resultado: El CMR aplica los ajustes realizados.

5.6 Start page

Una vez iniciada la sesión se muestra la página inicial del CMR.

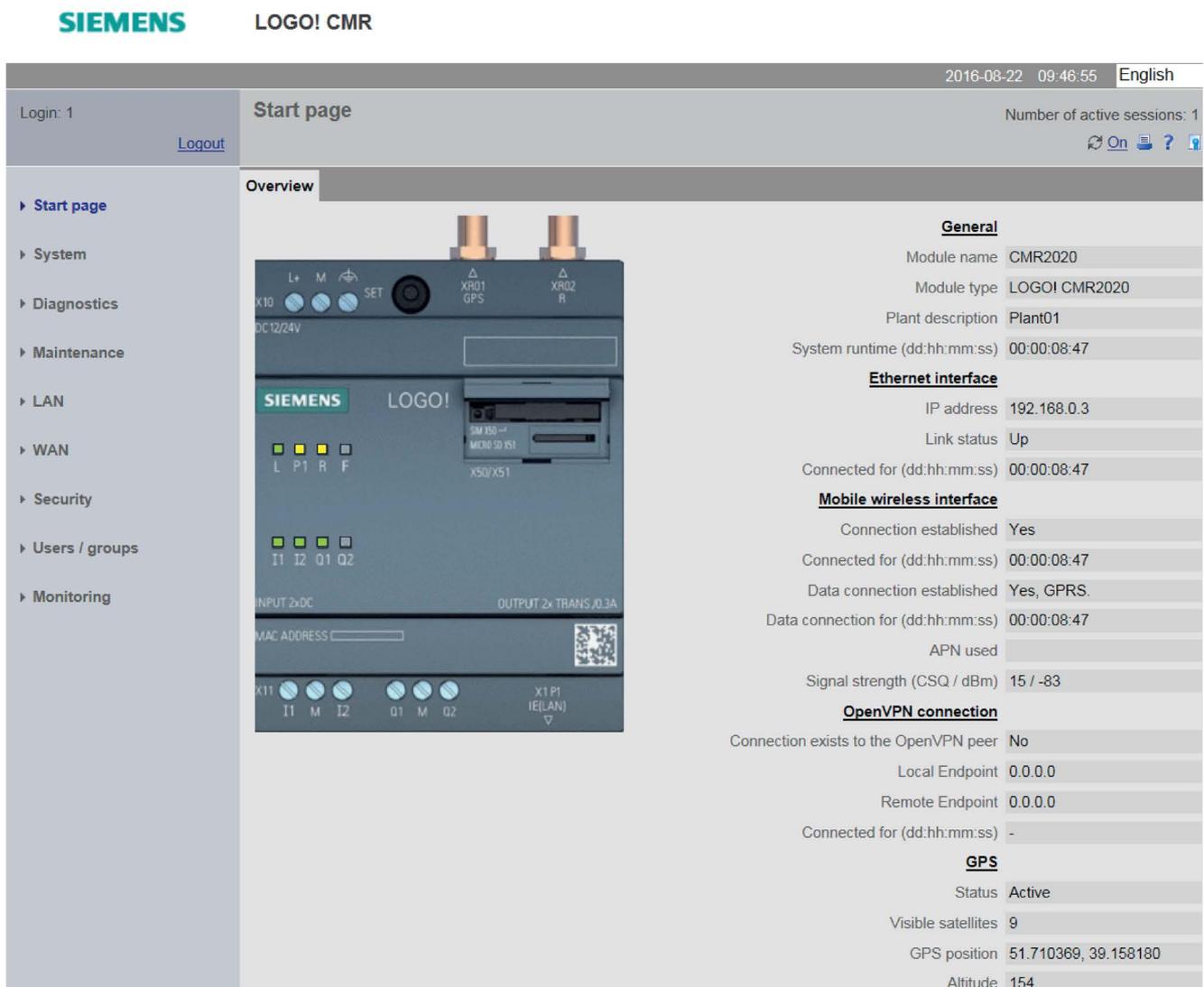


Figura 5-2 Start page: ficha "Overview"

La página inicial muestra una sinopsis del estado operativo actual del CMR.

Haciendo clic en las entradas principales, que están en negrita y subrayadas, se va directamente a la página de configuración correspondiente del WBM.

Indicación del estado operativo actual

General	
Module name	Indica el nombre de dispositivo asignado en la página "System" > "General" (Página 75).
Module type	Indica el tipo de dispositivo
Plant description	Indica el nombre de la instalación asignado por el usuario
System runtime (dd:hh:mm:ss)	Indica el tiempo de ejecución del sistema del CMR tras el último re arranque completo
Ethernet interface	
IP address	Dirección IP del CMR
Connection status	Indica el estado de la conexión entre el PC y el CMR
Connected for (dd:hh:mm:ss)	Indica la duración de la conexión entre el PC y el CMR
Mobile wireless interface	
Connection established	Indica el estado de la conexión a la red de telefonía móvil
Connected for (dd:hh:mm:ss)	Indica la duración de la conexión con la red de telefonía móvil desde la última marcación
Connection to data service established	Indica la duración de la conexión con el servicio de datos de la red de telefonía móvil desde la última marcación Entre paréntesis se muestra el tipo del servicio de datos, por ejemplo: <ul style="list-style-type: none"> • LOGO! CMR2020: (GPRS) • LOGO! CMR2040: (LTE)
Data connection for (dd:hh:mm:ss)	Muestra la duración desde la última conexión de datos.
APN used	Indica el nombre del punto de acceso (APN) de la red de telefonía móvil a Internet
Signal strength	Indica la intensidad de señal de la red de telefonía móvil en la ubicación del CMR <ul style="list-style-type: none"> • ≤ -113 dBm: No existe conexión con la red de telefonía móvil • ≥ -111 dBm: Intensidad de señal mala • ≥ -79 dBm: Intensidad de señal media • ≥ -65 dBm: Intensidad de señal buena • ≥ -51 dBm: Intensidad de señal excelente
OpenVPN connection	
Connection exists to the OpenVPN server	Indica el estado para el interlocutor de la conexión
Local endpoint	Dirección IP del servidor OpenVPN (CMR)
Remote endpoint	Dirección IP del cliente OpenVPN
Connected since (dd:hh:mm:ss)	Duración de la conexión actual con el interlocutor
GPS	
Status	Indica el estado de la recepción de GPS del CMR La recepción de GPS se activa en la página "System" > "General" (Página 75).
Visible satellites	Si la recepción de GPS está activada, se muestra el número de satélites de los que se reciben señales.

GPS position	Posición actual: <latitud>, <longitud> Conversión a coordenadas sexagesimales: <ul style="list-style-type: none">• Enteros: grados• 1.º y 2.º decimal: minutos• 3.º y 4.º decimal: segundos• 5.º y 6.º decimal: centésimas de segundo Indicación del hemisferio y la posición respecto del meridiano: <ul style="list-style-type: none">• Grado de latitud: valores positivos para el norte, valores negativos para el sur• Grado de longitud: valores positivos para el este, valores negativos para el oeste
Altitude	Altitud (metros sobre nivel del mar)

Nota

Actualización de los satélites GPS mostrados en el CMR2040

Si la recepción de GPS empeora, por ejemplo debido a un cambio de posición o a la retirada de la antena, la indicación de los satélites en el CRM2040 se muestra con un retardo de hasta 10 minutos.

Actualización de los valores mostrados

Si se activa la actualización automática de la visualización en la parte superior derecha de la página inicial, los valores visualizados se actualizan cada 5 segundos.

Para la actualización manual, en algunos navegadores web también puede utilizarse la tecla F5.

5.7 System

5.7.1 General

The screenshot shows the 'System' configuration page with the 'General' tab selected. The page header includes the date and time (2016-08-23 17:14:30) and the language (English). The user is logged in as '1' and has one active session. The left sidebar contains navigation options: Start page, System (selected), Diagnostics, Maintenance, LAN, WAN, Security, Users / groups, and Monitoring. The main content area has tabs for General, Hardware information, SD card, and System time. The 'General' tab contains the following fields:

- Module name:
- Plant description:
- End session after inactive period (minutes):
- Activate GPS:

An 'Apply' button is located at the bottom right of the form.

Figura 5-3 System: ficha "General"

Module name

Introduzca el nombre que desee para el módulo.

Utilice solamente nombres conformes con DNS para los módulos. Los nombres conformes con DNS se utilizan, p. ej, para el diagnóstico.

Plant description

Introduzca un texto cualquiera para su instalación.

End session after inactive period (minutes)

Tiempo de inactividad tras el cual se cierra una sesión.

A continuación, deberá volver a iniciar sesión con User name y Password.

Activate GPS

Active/desactive la recepción GPS.

Asegúrese de que haya una antena conectada en la entrada GPS:

- Para activar el GPS, seleccione la entrada "Yes" en la lista desplegable "Activate GPS".
- Para desactivar el GPS, seleccione la entrada "No" en la lista desplegable "Activate GPS".

En el CMR2040 tenga en cuenta la nota sobre la actualización de los satélites GPS mostrados en el capítulo Start page (Página 72).

Botón "Apply"

Al hacer clic en el botón "Apply" se adoptan todos los ajustes realizados en la ficha "General".

5.7.2 Device info

System

Indica los parámetros siguientes:

- tiempo de ejecución del sistema desde el último re arranque completo
- referencia del CMR
- número de serie del CMR
- versión de hardware del CMR

5.7.3 Tarjeta SD

SD card

Datos mostrados

- **Tarjeta SD insertada**
- **Memoria libre / total (kB)**

Se muestra la memoria libre (aún disponible) y la memoria total de la tarjeta SD que puede ser utilizada por los usuarios.

Archivos que se pueden guardar debajo del área de parámetros

Debajo del área de parámetros se indican los nombres de los archivos guardados en la tarjeta SD. Haciendo clic en el nombre, el archivo correspondiente se abre y se guarda de la tarjeta SD en el sistema de archivos de su PC.

Convenciones para los nombres de archivo y el sistema de archivos

Sistema de archivos

Los archivos que el CMR escribe en la tarjeta SD están en formato DOS o 8.3. Los nombres de archivo siguen el patrón siguiente:

<1...8 caracteres>.<1...3 caracteres>

Los directorios también se muestran en formato DOS (hasta 8 caracteres). Al guardar archivos con más de 8 letras, tenga en cuenta que el nombre se cortará tras el 8.º carácter.

Convenciones para los nombres de archivo

Los nombres de archivos tienen la estructura que se indica a continuación:

- **Archivos de configuración**

Archivos con datos de configuración del CMR:

*.CFG

- El archivo "default.cfg" lo crea automáticamente el CMR y se actualiza cada vez que se cambia la configuración.
- El archivo "user.cfg" es un archivo con datos de configuración guardado manualmente por el usuario.

Respecto al almacenamiento y al significado de los archivos, consulte el capítulo Configuration (Página 83).

- **Archivo del búfer de diagnóstico**

Archivo con entradas del búfer de diagnóstico del CMR:

diagbuf.txt

- **Otros archivos**

Archivos guardados por el usuario en la tarjeta SD:

.

5.7.4 System time

En esta ficha se realiza el ajuste básico de la hora y se determina lo siguiente:

- El método de sincronización horaria y los intervalos de tiempo en los que se sincroniza la hora.
- El cambio automático del horario de verano
- El reenvío de la hora del CMR al BM

Nota

En caso de rearranque completo se restablece la hora. Para tener una hora actualizada debe utilizarse siempre un método de sincronización horaria.

En caso de utilizar certificados, tenga en cuenta las indicaciones sobre la hora en el capítulo Requisitos de aplicación (Página 18).

Procedimiento y requisitos

Para los diferentes métodos de sincronización horaria se tienen que cumplir los requisitos siguientes:

- **NTP**
 - El CMR está conectado a la red de telefonía móvil y la interfaz de telefonía móvil está activada.

La conexión con el servidor NTP solo puede establecerse mediante la interfaz de telefonía móvil, no mediante la interfaz Ethernet.
 - La opción "Data service in the mobile wireless network" de la ficha WAN > Mobile wireless settings (Página 94) está activada.
 - Hay una antena conectada.
 - La cobertura es suficiente.
- **GPS**
 - GPS está activado: System > General (Página 75)
 - Hay una antena conectada.
 - La cobertura es suficiente.
- **By mobile wireless network**
 - Su operador de telefonía móvil soporta este servicio. Pregunte a su operador de telefonía móvil por él.
 - Hay una antena conectada.
 - La cobertura es suficiente.

Con este procedimiento hay que tener en cuenta que los instantes de la sincronización horaria pueden ser muy variables. Con la primera marcación para entrar en la red de telefonía móvil se transfiere la hora del operador de telefonía móvil. En función del operador de telefonía móvil, es posible que los intervalos de los próximos puntos de sincronización horaria después de la primera marcación varíen considerablemente. En determinadas circunstancias, los intervalos pueden ser de varios días.

Local time zone

- Seleccione en la lista desplegable una zona horaria adecuada para su ubicación.
También puede ajustar la zona horaria local manualmente.

Al hacer clic en el botón "Apply" se adoptan los ajustes realizados sobre la zona horaria local.

- **Automatic daylight saving time switch**

Con la casilla de verificación "Automatic daylight saving time switch" se activa un cambio automático al horario de verano.

Las fechas para el cambio de horario solo pueden cambiarse libremente si se ajusta manualmente la zona horaria. En las siguientes listas desplegables, seleccione las fechas vigentes en su ubicación para el cambio de horario.

Para las zonas horarias UTC, los ajustes están predeterminados y no pueden modificarse.

- **Enable time-of-day synchronization**

Con esta opción se activa la sincronización horaria del CMR.

- **Time-of-day synchronization method**

Seleccione un método de sincronización.

- **Last time-of-day synchronization (dd:hh:mm:ss) ago**

Muestra cuándo se ha efectuado la última sincronización horaria.

- **Now synchronize**

Si se ha seleccionado "NTP" o "GPS" como método de sincronización horaria, es posible sincronizar la hora espontáneamente en caso de existir una conexión de telefonía móvil.

- **Accept time-of-day from non-synchronized NTP servers**

Si la opción está activada, el CMR también toma la hora de servidores NTP no sincronizados con estrato 16.

- **IP address or DNS name of the NTP server**

Introduzca en este campo el FQDN (formato URL) o la dirección IP del servidor NTP.

- **Update interval**

Mediante la lista desplegable se definen los intervalos en los que debe realizarse la sincronización horaria.

Con el método "By mobile wireless network" no es posible especificar ningún intervalo de actualización, ya que la hora es enviada activamente por el operador.

- **Forward time of day to LOGO! BM**

Con esta opción se activa el reenvío de la hora del CMR a LOGO! BM. La hora se reenvía al BM en los intervalos de tiempo ajustados.

En caso de sincronización horaria a través de la red de telefonía móvil, se transmite la hora en cuanto el CMR recibe una hora nueva. La hora también se transmite al establecer la conexión con el BM.

Nota

Evitar ajustes distintos en el BM y el CMR

Si desea evitar que haya ajustes distintos en el BM y en el CMR, con las diferencias de tiempo resultantes, hay que activar el reenvío de la hora al BM:

Active en el BM el cambio automático del horario de verano. De este modo se asegura de que los bloques funcionen correctamente, como el reloj astronómico.

Nota

Sincronización horaria con precisión de segundo con LOGO! BM

Al sincronizar la hora del LOGO! BM desde el CMR es posible conseguir una sincronización horaria al segundo exacto con las siguientes versiones de firmware:

- LOGO! BM: a partir de V1.81.01 (FS:04)
- LOGO! CMR: V2.0 o superior

Con versiones de firmware anteriores es posible que haya pequeñas diferencias entre el CMR y el BM.

Al hacer clic en el botón "Apply" se inicia la sincronización horaria con los parámetros modificados.

Set system time manually

La hora del sistema para el CMR puede obtenerse del PC o introducirse manualmente:

- **New system time**

Para especificar la hora manualmente, introduzca la hora del sistema que desee en el campo de entrada.

- **Adopt new system time**

Haciendo clic en el botón se escribe la hora en el CMR.

- **Adopt PC time**

Haciendo clic en el botón se lee la hora del sistema del PC y se escribe en el CMR.

5.8 Diagnóstico

5.8.1 Diagnostics buffer

El búfer de diagnóstico

El búfer de diagnóstico contiene avisos de diagnóstico sobre eventos y errores internos. Comprende como máximo 200 entradas. Cuando se rebasa el número máximo, se sobrescriben las entradas más antiguas.

La tabla de esta ficha muestra como máximo las 20 últimas entradas. Mediante la lista desplegable del encabezado pueden visualizarse entradas más antiguas.

Las entradas del búfer de diagnóstico contienen un número correlativo, una clasificación, un sello de tiempo y el texto del aviso.

A continuación encontrará algunos ejemplos de eventos que se registran en el búfer de diagnóstico:

- Arranque del CMR
- Cambio de la configuración
- Establecimiento o cancelación de una conexión de comunicación
- Establecimiento o cancelación de una conexión de datos
- Establecimiento o interrupción de la conexión con el BM
- Advertencias a la hora de leer la configuración de la tarjeta SD o del PC
- Sincronización horaria
- Fallo de tensión

Los avisos de diagnóstico se clasifican de la manera siguiente:

- INFO
Información sobre un evento especial
- WARNING
Advertencia sobre un posible evento indeseado
- ERROR
Error interno. El CMR sigue funcionando.
- FATAL
Error grave que perjudica o interrumpe el funcionamiento del CMR.
Si el CMR ejecuta un rearranque completo debido a un error fatal, se desconectará brevemente la tensión de las salidas.

Copy of the diagnostics buffer

Los botones descritos a continuación permiten guardar el búfer de diagnóstico completo.

El nombre de archivo para los avisos del búfer de diagnóstico es fijo: diagbuf.txt

- **Save on SD card**

Se guarda manualmente en la tarjeta SD

- **Save to PC**

Se guarda manualmente en el sistema de archivos del PC de configuración

- **Save a copy of the diagnostics buffer automatically on SD card if serious errors occur**

Si se activa esta opción, al producirse errores de la categoría FATAL es posible hacer automáticamente una copia de seguridad del búfer de diagnóstico en la tarjeta SD.

Envío del búfer de diagnóstico

En la ficha "Notifications" existe la posibilidad de configurar que el búfer de diagnóstico se envíe por correo electrónico en función de la categoría de entradas que se generan.

5.8.2 Notifications

Nota

Para enviar SMS y correos electrónicos se necesitan usuarios y grupos configurados.

- **Send notifications**

Aquí se determina si, cuando se produce un evento (aviso), el CMR debe enviar un mensaje por SMS o correo electrónico.

En el mensaje se envían el texto explícito del aviso, la categoría y el sello de tiempo.

El asunto de los correos electrónicos es: "Diag Notification From: <nombre del módulo>"

- **Message class**

Aquí se ajusta la categoría del aviso.

El mensaje se envía en función de la categoría de las entradas que se generan.

- **Recipient group**

Aquí se define como destinatario del mensaje uno de los grupos configurados en "Users / groups".

Si todavía no se ha configurado ningún grupo destinatario no es posible activar las notificaciones.

Solo en caso de envío por correo electrónico:

- **Attachment**

Aquí se selecciona el anexo que se envía con el correo electrónico. Existen las siguientes opciones:

- Current process image
- Entire diagnostics buffer

5.9 Maintenance

5.9.1 Configuration

Load configuration

Cargar la configuración del PC

Esta función permite cargar en el CMR una configuración creada anteriormente y guardada en el PC.

Los archivos de configuración tienen la extensión ".cfg".

1. Para buscar configuraciones en el PC, haga clic en el botón "Browse".
2. Haga doble clic en el archivo de configuración deseado.
3. Haga clic en el botón "Load on device" para cargar la configuración en el CMR.

Resultado: Ahora se utiliza la configuración que se ha cargado del PC.

Cargar la configuración de la tarjeta SD

Esta función permite cargar en el CMR una configuración creada anteriormente y guardada en la tarjeta SD.

El archivo de configuración guardado se llama "user.cfg".

1. Haga clic en el botón "Load from SD card" para cargar la configuración en el CMR.

Resultado: Ahora se utiliza la configuración que se ha cargado de la tarjeta SD.

Save configuration

Guardar la configuración en el PC

Existe la posibilidad de guardar en el PC la configuración que se utiliza actualmente en el CMR como archivo "user.cfg". Para ello, haga clic en el botón "Save to PC". Seleccione la ubicación correspondiente.

Un archivo de configuración guardado puede transferirse en caso necesario a otros dispositivos del mismo tipo; consulte también el apartado siguiente.

Guardar la configuración en la tarjeta SD

Nota

Solo un archivo de configuración de un tipo

En la tarjeta SD solo es posible guardar un archivo de configuración con el nombre "user.cfg" o "default.cfg" a la vez.

Existe la posibilidad de guardar en la tarjeta SD la configuración que se utiliza actualmente en el CMR como archivo "user.cfg". Para ello, haga clic en el botón "Save on SD card".

Archivos de configuración para cambio de dispositivo y CMR adicionales

Si hay una tarjeta SD insertada, el archivo de configuración "default.cfg" se guarda automáticamente en la tarjeta SD al arrancar el dispositivo. En caso de que cambie la configuración, el archivo se actualiza haciendo clic en el botón "Apply".

Los archivos de configuración guardados mediante las funciones descritas anteriormente pueden utilizarse tanto para cambiar dispositivos como de plantillas para dispositivos adicionales del mismo tipo.

- **Cambio de dispositivo**

Los archivos de configuración permiten reutilizar fácilmente una configuración ya utilizada en caso de cambio de dispositivo sin tener que crear la configuración del nuevo dispositivo.

Si se inserta la tarjeta SD que contiene el archivo "default.cfg" en un CMR nuevo de fábrica o con la configuración de fábrica restablecida, el archivo "default.cfg" se carga automáticamente del dispositivo durante el arranque. El nuevo dispositivo puede utilizarse de inmediato con los datos de configuración del dispositivo antiguo.

- **Transferencia de la configuración a otros dispositivos**

El archivo de configuración "user.cfg" permite utilizar una configuración creada como plantilla para CMR adicionales del mismo tipo.

Si se utilizan varios CMR con una configuración similar, es posible guardar en el PC la configuración del primer dispositivo configurado como archivo de configuración "user.cfg".

A continuación, el archivo de configuración guardado puede copiarse y los parámetros especiales, como dirección IP, nombre de la instalación, etc. pueden adaptarse a cada dispositivo que debe utilizarse mediante un editor (véase más abajo). Si los archivos de configuración adaptados se guardan en tarjetas SD y estas se insertan en los dispositivos correspondientes, tras arrancar los dispositivos se carga el archivo de la tarjeta SD al dispositivo en cuestión. De este modo se ahorra tiempo en la configuración completa de cada dispositivo individual.

Editar archivos de configuración

Los archivos de configuración "*.cfg" pueden editarse con los editores de textos habituales.

Nota

Editar configuraciones con el editor de textos

Al editar archivos de configuración con un editor de textos tenga en cuenta lo siguiente:

- No modifique la estructura del archivo.
 - Introduzca solo parámetros correctos.
 - No pueden cambiarse los datos sensibles, pues se guardan cifrados.
Aquí se incluyen contraseñas y claves, p. ej. para HTTPS y OpenVPN.
 - Guarde el archivo en formato UTF-8 o bien no utilice caracteres especiales, es decir, utilice solo caracteres ASCII de la banda numérica (decimal) 32 .. 126.
-

5.9.2 Firmware

Firmware status

Se muestra la siguiente información:

- Module name configurado en la página web "System".
- Activated firmware version
- Activated on (indicación de la fecha)
- Bootstrap version
- Mobile wireless module version

Firmware update

ATENCIÓN
<p>El firmware cifrado y con firma digital impide manipulaciones de terceros</p> <p>Para poder comprobar la autenticidad del firmware, Siemens lo firma digitalmente. Esto permite detectar e impedir manipulaciones de terceros. El cifrado del firmware sirve para impedir cambios en su programación.</p>

Nota

Desde que se descomprime y actualiza el firmware hasta que se reinicia el CMR, la interfaz de administración no está bloqueada.

- Durante este intervalo, no realice ningún ajuste en la interfaz web, puesto que no puede garantizarse que dichos ajustes se adopten correctamente.

No desconecte el CMR durante la actualización.

Para cargar una nueva versión de firmware en el CMR, proceda del siguiente modo:

1. Antes de comenzar con la actualización: tenga en cuenta las indicaciones que figuran en "Firmware update".
2. Haga clic en el botón "Browse".
3. Seleccione el archivo de firmware correspondiente, p. ej., "LOGO!CMR_v2.0-v2.1.sfw".
4. Haga clic en el botón "Load".
5. Una vez transferida correctamente, se muestra la versión de firmware actualizada.
6. A continuación, haga clic en el botón "Activate and restart".
7. El CMR se reinicia.
8. Una vez reiniciado, se actualiza el firmware. Todos los LED se encienden durante unos segundos antes de que se inicie el CMR.

Campos de visualización con información adicional sobre el firmware

- **Status**
Muestra errores durante la carga del firmware: p. ej., errores de formato si se carga un archivo distinto del que contiene el firmware deseado.
- **Signature status**
Muestra el resultado de la comprobación de la firma.
- **Description**
Muestra el nombre del firmware.
- **Version**
Muestra la versión del firmware cargado.

5.9.3 Operating status

Acciones posibles en la ficha "System":

- Llevar el dispositivo a un estado seguro
- Ejecutar un re arranque completo
- Restablecer la configuración de fábrica

Change to the safe status

Hay dos formas de llevar el CMR al estado seguro:

- Mediante el WBM
- Mediante el pulsador SET en la cara frontal del dispositivo.

Si se lleva el CMR al estado seguro, este se desconecta de la red de telefonía móvil.

A continuación es posible desconectar el dispositivo de la tensión de alimentación.

Llevar al estado seguro mediante el WBM

En la ficha "Maintenance" > "System", haga clic en el botón "Change to the safe status" para llevar el CMR al estado seguro.

Llevar al estado seguro mediante el pulsador SET

Presione el pulsador SET con un objeto adecuado. Mantenga pulsado el pulsador entre 5 y 10 segundos.

Run a restart

Existen dos posibilidades para reiniciar el CMR:

- Mediante el WBM

En la ficha "Maintenance" > "System", haga clic en el botón "Run a restart".

- Mediante el pulsador SET del CMR

Presione el pulsador SET brevemente (< 5 segundos) con un objeto adecuado.

Repercusiones:

- El CMR se reinicia.

- La configuración actual no cambia.

Después del reinicio, el CMR continúa funcionando con los mismos ajustes.

- Durante un reinicio se interrumpen las conexiones existentes.
- Durante el reinicio se desactivan brevemente las salidas del CMR.

Por este motivo, solo debe ejecutarse un reinicio en caso necesario.

Reset to factory settings

Existen dos posibilidades para restablecer la configuración de fábrica del dispositivo:

- Mediante el WBM

- Mediante el pulsador SET en la cara frontal del dispositivo.

Tenga en cuenta las siguientes indicaciones antes de restablecer la configuración de fábrica del CMR.

ATENCIÓN

Borrado de datos

Al restablecer la configuración de fábrica se borran todos los datos de configuración del CMR. El borrado también incluye los siguientes datos:

- Nombres de usuario y contraseñas
- PIN configurado
- Búfer de diagnóstico
- Con la tarjeta SD insertada:
 - La configuración guardada automáticamente (default.cfg)
 - La configuración guardada manualmente (user.cfg)

A continuación se reinicia el CMR. Después del reinicio, se puede acceder al CMR a través de la interfaz Ethernet con la dirección IP predeterminada 192.168.0.3.

Nota

Guardar los datos de configuración en el PC o en la tarjeta SD

Si no desea descartar los datos de configuración introducidos, puede guardarlos externamente y volver a cargarlos una vez restablecida la configuración de fábrica.

Encontrará información al respecto en el capítulo Configuration (Página 83).

Al guardar los datos de configuración en la tarjeta SD, tenga en cuenta lo siguiente:

- Extraiga la tarjeta SD antes de restablecer la configuración de fábrica: consulte "Reutilizar la configuración de un CMR".
- Extraiga la tarjeta SD solo si el dispositivo está desconectado de la alimentación.

Restablecer desde el WBM

En la ficha "Maintenance" > "System", haga clic en el botón "Reset to factory settings" para resetear el CMR.

Tras restablecer la configuración de fábrica, el CMR ejecuta un arranque completo.

Vuelva a poner en marcha el dispositivo como se describe en Pasos para la puesta en marcha (Página 47) y Configuración (WBM) (Página 57).

Restablecer mediante el pulsador SET

Presione el pulsador SET con un objeto adecuado. Mantenga pulsado el pulsador más de 10 segundos.

Tras restablecer la configuración de fábrica, el CMR ejecuta un arranque completo.

Vuelva a poner en marcha el dispositivo como se describe en Pasos para la puesta en marcha (Página 47) y Configuración (WBM) (Página 57).

Reutilizar la configuración de un CMR

La configuración de un CMR puede transferirse a otros CMR tantas veces como se quiera.

Requisitos: El CMR es nuevo de fábrica o se ha restablecido su configuración de fábrica (sin tarjeta SD)

Si antes de iniciar el CMR se inserta la tarjeta SD de otro CMR, se utiliza la configuración guardada automáticamente (default.cfg) de ese otro CMR.

5.9.4 Online Support

Aquí puede abrir las páginas de Internet de Siemens Industry Online Support.

Online Support

Enlace al portal de Siemens Industry Online Support

Haga clic en "Siemens Industry Online Support" para conectarse a las páginas de Internet del Siemens Industry Online Support.

En ellas podrá buscar información sobre el producto o plantear una consulta al Support del producto.

Configuración del registro

En algunos casos, el Product Support le enviará un archivo de registro del tipo *.sup para registrar eventos. Guarde este archivo de registro en el sistema de archivos del PC de configuración. Cargue el archivo en el CMR en este sitio WBM.

Para el registro se necesita una tarjeta SD que tenga como mínimo 8 MB de memoria libre.

- **Archivo**

Tras seleccionar un archivo de registro guardado en el PC de configuración con el botón "Examinar" se muestra el nombre del archivo.

- **Examinar**

Examina el sistema de archivos del PC de configuración en busca de un archivo de registro guardado que deba cargarse en el CMR.

- **Cargar en dispositivo**

Haciendo clic en este botón se carga el archivo de registro seleccionado en el CMR.

- **Ajuste predeterminado**

Carga el archivo de registro estándar preconfigurado de fábrica en lugar de un archivo de registro proporcionado por el Product Support.

- **Borrar**

Borra del CMR un archivo de registro que no se necesite.

Después de borrar el archivo de registro vuelve a estar desactivado el registro.

Activar generación de informes

Después de cargar el archivo de registro (generación de informes) es preciso habilitar el registro.

- **Activar generación de informes y guardar archivo en tarjeta SD**

Al activar esta opción, se inicia el registro en cuanto se hace clic en el botón "Aplicar".

El archivo de registro (generación de informes) se guarda en la tarjeta SD, y durante el funcionamiento se actualiza cuando se producen eventos relevantes.

Uso del registro

Utilice el registro de eventos exclusivamente cuando tenga problemas con el CMR que no pueda solucionar por su cuenta.

Nota

Protección de la tarjeta SD desactivando el registro

Para no acortar excesivamente la vida útil de la tarjeta SD, desactive el registro (generación de informes) durante el funcionamiento normal del CMR.

Si está activado el registro (generación de informes), mientras el CMR esté en funcionamiento se almacenará constantemente información sobre los eventos importantes que se produzcan. Los datos guardados contienen información sobre la configuración, sobre los procesos activos y sobre casos de error.

Los datos se depositan en la tarjeta SD en un archivo de registro con el nombre "support.bin". La información contenida en ese archivo está cifrada y solo puede leerla el Siemens Industry Online Support. Una vez finalizado el registro, devuelva el archivo de registro a su persona de contacto del Siemens Industry Online Support.

5.10 LAN

5.10.1 Configuration

Función de la interfaz LAN X1P1

- La interfaz X1P1 (Ethernet RJ45) del CMR sirve para conectar un PC local para la configuración.
- Si el CMR no se utiliza en modo autónomo, la interfaz X1P1 sirve para la conexión con el BM una vez finalizada la configuración.

Encontrará las posibilidades de operación en el capítulo Comunicación de telefonía móvil por SMS y correo electrónico sin LOGO! BM (Página 22).

Encontrará las propiedades de la interfaz X1P1 en el capítulo Datos técnicos (Página 153).

Por medio de autonegotiation y autocrossing se detectan y ajustan automáticamente propiedades de transferencia de la interfaz.

Configuration of the Ethernet interface

Nota

Dirección IP y máscara de subred según RFC 1918

Las direcciones IP y las máscaras de subred de la configuración de fábrica pueden modificarse como se desee, pero deben cumplir la especificación RFC 1918. El CMR no comprueba las bandas de direcciones de forma estricta.

No ajuste una dirección IP ya asignada en su LAN, p. ej., para otros BM.

Si se detecta una dirección IP duplicada, el LED de error rojo empieza a parpadear. Ya no es posible acceder al CMR a través de la interfaz Ethernet. El resto de la funcionalidad no se ve afectado: p. ej. enviar SMS sobre la base de eventos.

Parámetros fijos

- MAC address
- Connection status
- Transmission properties (posibilidades: 10/100 Mbits/s; semidúplex/dúplex)
- Connected for (dd:hh:mm:ss)

Parámetros modificables

- IP address
- Subnet mask
- Default router

El router predeterminado está previsto para la conexión directa del CMR a Internet a través de la interfaz LAN.

5.11 WAN

5.11.1 Overview

Mobile wireless connection

En la sinopsis se muestra la información que sigue sobre la interfaz de telefonía móvil:

- **Connection established**
Estado de la conexión a la red de telefonía móvil
- **Connected since (dd:hh:mm:ss)**
Duración de la conexión establecida de telefonía móvil
- **Connection to data service established**
Estado de la conexión al servicio de datos GPRS / UMTS / LTE
- **Data connection since (dd:hh:mm:ss)**
Duración de la conexión establecida al servicio de datos
- **Signal strength (CSQ / dBm)**
 - CSQ = 0 .. 8 (-112 .. ≤ -97 dBm): No hay cobertura
 - CSQ = 9 .. 16 (-95 .. -81 dBm): Calidad de señal media
 - CSQ = 17 .. 31 (≥ -79 dBm): Calidad de señal buena
 - CSQ = 99 (≤ -113 dBm): No puede detectarse ninguna señal
- **APN used**
- **IMEI**
International Mobile Equipment Identity del operador de red de telefonía móvil
- **IMSI**
International Mobile Subscriber Identity del operador de red de telefonía móvil
- **IP address**
Dirección IP del CMR, asignada por el operador de red de telefonía móvil.
Para la accesibilidad del CMR a través de telefonía móvil, el CMR necesita una dirección IP pública.
- **DNS server**
Dirección IP del servidor DNS asignado por el operador de red de telefonía móvil.

Statistics

Las cifras son válidas para el tiempo transcurrido desde el último re arranque completo del CMR.

- **SMS sent**

Número de SMS enviados correctamente por el CMR

- **Sending the SMS failed**

Número de SMS que el CMR no pudo enviar (con entrada en el búfer de diagnóstico).

- **SMS received**

Número de SMS recibidos y procesados por el CMR

- **SMS discarded**

Número de SMS recibidos que el CMR ha rechazado.

Los SMS se rechazan en los siguientes casos:

- La opción "SMS received" de la ficha "SMS" está desactivada.
- El número de teléfono del interlocutor que transmite no está configurado entre los usuarios.

- **Data sent (kB)**

Número de datos (kilobytes) que el CMR ha enviado.

- **Data received (kB)**

Número de datos (kilobytes) que el CMR ha recibido.

- **E-mails sent**

Número de correos electrónicos enviados correctamente por el CMR

- **E-mails sent unsuccessfully**

Número de correos electrónicos que el CMR no ha podido enviar correctamente.

Nota

Número de intentos de transmisión

Si el CMR no puede enviar un correo electrónico, lo vuelve a intentar dos veces. Después se borra el correo electrónico.

- **Reset statistics**

Este botón pone a cero todos los contadores de estadísticas del CMR.

5.11.2 Mobile wireless settings

La interfaz de telefonía móvil del CMR conecta el dispositivo con la red de telefonía móvil.

Nota

Costes de una conexión de datos móviles

Tenga en cuenta que para intentar establecer una conexión de datos móviles (tanto si se consigue como si no) y para mantenerla una vez establecida, se intercambian tramas sujetas a pago.

Parámetros de acceso

En la ficha "Mobile wireless settings" se configura la conexión de telefonía móvil.

Para acceder a la red de telefonía móvil GSM y a los servicios HSPA, UMTS, GPRS o LTE se necesitan los siguientes parámetros:

- El PIN protege la tarjeta SIM del uso no autorizado.
- El APN es el nombre del punto de transición entre la red de telefonía móvil y otras redes IP conectadas, en el caso del CMR Internet.

"Name" y "Password" sirven para proteger el acceso al APN.

Obtendrá estos parámetros de acceso de su operador de telefonía móvil.

La red de telefonía móvil se selecciona automáticamente.

Nota

Marcación en la red de telefonía móvil con LOGO! CMR2020

LOGO! CMR2020 solo se conecta a una red GSM/GPRS.

Marcación en la red de telefonía móvil con LOGO! CMR2040

LOGO! CMR2040 intenta en primer lugar establecer una conexión con una red LTE.

Si no es posible establecer la conexión con la red LTE, el CMR intenta hacerlo con una red UMTS.

Si no es posible establecer la conexión con la red UMTS, el CMR intenta hacerlo con una red GSM/GPRS.

Al activar la casilla de verificación "Activate mobile wireless interface", la interfaz de telefonía móvil pasa a estar operativa.

Si la casilla de verificación está desactivada, la interfaz de telefonía móvil no puede utilizarse, ya que está desconectada.

PIN of the SIM Card

Nota

Tarjeta SIM sin PIN

El CMR también funciona con tarjetas SIM sin PIN. En tal caso, deje vacío el campo de entrada "PIN of the SIM card".

Introducción de un PIN erróneo

El PIN introducido en último lugar (erróneo) queda guardado. Si se modifica la configuración (excepto el PIN) o si se reinicia el CMR, dicho número no consume ningún intento de introducción de PIN.

Por lo tanto, no cambie el PIN de la tarjeta SIM fuera del CMR al PIN erróneo guardado anteriormente.

Bloqueo si se introduce un PIN erróneo

Introduzca el PIN correcto. Si introduce un PIN erróneo por 3.^a vez, se bloqueará la tarjeta SIM. Tenga en cuenta también las indicaciones del capítulo Insertar la tarjeta SIM e introducir el PIN (Página 48).

Desbloqueo de la tarjeta SIM

El desbloqueo de la tarjeta SIM se describe en el capítulo Insertar la tarjeta SIM e introducir el PIN (Página 48).

El operador de telefonía móvil le habrá facilitado un PIN para la tarjeta SIM.

1. Introduzca el PIN de la tarjeta SIM en el campo de entrada.

Si utiliza una tarjeta SIM sin PIN, deje vacío este campo.

2. Al hacer clic en el botón "Apply" se guarda el PIN junto con los demás ajustes.

- Una marca de verificación verde debajo del campo de entrada indica que el PIN se ha guardado correctamente en el dispositivo.
- Un punto rojo con una cruz blanca debajo del campo de entrada indica que la configuración no es correcta y se muestra un mensaje de error al respecto.

No se establece la conexión de telefonía móvil.

Allow roaming

"Roaming" (itinerancia) significa que la red de telefonía móvil de su operador ya no está accesible, y otro operador de telefonía móvil acepta el CMR en su red de telefonía móvil.

Si la red de telefonía móvil predeterminada ya no está accesible, especifique si el CMR debe conectarse a otra red de telefonía móvil.

- Activación de la casilla de verificación "Allow roaming".

Si la red de telefonía móvil predeterminada no está disponible, el dispositivo se conecta a una red de telefonía móvil disponible.

La conexión a otro operador de telefonía móvil puede conllevar mayores costes.

- Desactivación de la casilla de verificación "Allow roaming".

Si la red de telefonía móvil predeterminada no está disponible, no se establece ninguna conexión con ninguna otra red de telefonía móvil.

Número de SMSC

El número de teléfono del SMSC del operador de telefonía móvil no puede modificarse desde el CMR. Si desea modificar el número, extraiga la tarjeta SIM del CMR, inserte la tarjeta SIM en un teléfono móvil y modifique el número del SMSC con las funciones del teléfono móvil.

Enable data service in the mobile wireless network

Nota

Habilitar las conexiones de datos móviles

Habilite las conexiones de datos móviles necesarias a través del operador de telefonía móvil.

Para su dispositivo, puede activar o desactivar la conexión de datos móviles.

- Activación de la casilla de verificación "Activate data connection via the mobile wireless network":

Si, además de enviar y recibir SMS, desea utilizar los servicios de datos basados en IP de su operador de telefonía móvil, p. ej., la sincronización horaria mediante NTP.

- Desactivación de la casilla de verificación "Activate data connection via the mobile wireless network":

El CMR solo podrá enviar y recibir SMS.

APN / nombre de usuario / contraseña

- **APN**

Introduzca el APN del operador de telefonía móvil en el campo de entrada.

El APN (Access Point Name) es el nombre del host DNS para el punto de acceso de la red de telefonía móvil hacia una red externa de paquetes de datos (LTE/UMTS/GPRS).

Obtendrá información sobre estos datos de acceso de su operador de telefonía móvil o bien en Internet.

- **Authentication method**

En la lista desplegable "Authentication method" seleccione un método para transmitir el nombre y la contraseña del APN al interlocutor de la comunicación:

CHAP tiene mayor prioridad. Si el interlocutor de la comunicación no soporta CHAP, el nombre y la contraseña se transmiten vía PAP.

- none

Sin autenticación

- CHAP

Transmisión codificada de nombre y contraseña utilizando el Challenge Handshake Authentication Protocol.

- PAP

Transmisión no codificada de nombre y contraseña utilizando el Password Authentication Protocol.

Los dos parámetros siguientes solo se necesitan si la autenticación está activada.

- **Name**

En el campo de entrada, introduzca el nombre que le haya facilitado el operador de telefonía móvil.

Algunos operadores de telefonía móvil renuncian a controlar el acceso mediante un nombre. En tal caso, deje vacío el campo de entrada.

- **Password**

En el campo de entrada, introduzca la contraseña del proveedor correspondiente.

Algunos operadores de telefonía móvil renuncian a controlar el acceso mediante una contraseña. En tal caso, deje vacío el campo de entrada.

5.11.3 Wireless cell

Orientar las antenas de forma óptima

Para orientar la antena conectada al conector hembra SMA de forma óptima, se dispone de la ficha "Wireless cell". La ficha "Wireless cell" permite comprobar la intensidad de señal con la antena en diferentes posiciones.

Los datos se actualizan en intervalos de escasos segundos. En consecuencia, para determinar la posición óptima dispone de información continua sobre la intensidad de señal en las posiciones de prueba.

Status of the wireless cells

Visualización de parámetros de la célula de telefonía móvil a la que se ha conectado el CMR:

- Wireless cell identifier (CI)
- Signal strength (CSQ / dBm)

Intensidad de señal de la red de telefonía móvil como CSQ (Cell Signal Quality) y como intensidad del campo de recepción RSSI [dBm]

CSQ y RSSI corresponden respectivamente a:

- CSQ = 0 .. 8 (-112 .. ≤ -97 dBm): No hay cobertura
- CSQ = 9 .. 16 (-95 .. -81 dBm): Calidad de señal media
- CSQ = 17 .. 31 (≥ -79 dBm): Calidad de señal buena
- CSQ = 99 (≤ -113 dBm): No puede detectarse ninguna señal

- Signal quality

Calidad de la señal en porcentaje

- Location Area Code

Identificador de localización

- Mobile wireless standard of the wireless cell
- Network type
- Network name
- PLMN

Public Land Mobile Network

Identificación única en todo el mundo para redes de telefonía móvil, compuesta por:

- MCC (Mobile Country Code)
- MNC (Mobile Network Code) del operador de red

Ejemplo: la PLMN 26276 está compuesta por MCC = 262 y MNC = 76.

5.11.4 SMS

En esta ficha se permite o se bloquea la recepción de SMS por el CMR.

Encontrará información sobre cómo escribir datos por SMS en el anexo Información complementaria sobre SMS (Página 173).

- **Allow receipt of SMS messages**

- Si esta opción está desactivada, el CMR puede recibir SMS y los evalúa.
- Si esta opción está desactivada, el CMR puede recibir SMS pero no los evalúa.

El CMR no evalúa SMS recibidos, independientemente de los derechos de SMS que se hayan asignado a los usuarios en la página Users / groups (Página 112).

Nota

Costes de itinerancia con opción desactivada

El CMR recibe SMS incluso si la opción está desactivada. Por lo tanto, incluso con la recepción SMS bloqueada pueden surgir costes de itinerancia.

- **Enable SMS password**

Con esta opción se activa opcionalmente una contraseña para comandos de escritura que se transfieren por SMS. La asignación de una contraseña protege mejor el acceso de escritura al CMR a través de SMS.

Si la opción está activada, el CMR solo evalúa SMS que contienen la contraseña configurada en el texto.

Tenga en cuenta que, si la opción está desactivada, los SMS no deben incluir contraseña.

- **Password for writing commands**

Introduzca aquí la contraseña que debe transferirse con SMS de escritura.

- **Send positive acknowledgments**

Cuando se ha recibido un SMS con el que se produce un error, el CMR envía siempre acuses con el mensaje de error correspondiente al remitente. Esto puede suceder, por ejemplo, en caso de parámetros no válidos o de una configuración de SMS incompleta.

Tras recibir un SMS con datos de escritura que han podido transferirse al módulo de destino, se produce el comportamiento siguiente:

- Si la opción está activada, el CMR envía siempre un acuse positivo al remitente del SMS una vez se ha procesado la petición.
- Si la opción está desactivada, el CMR reacciona del siguiente modo:

Tras recibir un SMS con datos de escritura que han podido transferirse al módulo de destino, el CMR no envía ningún acuse al remitente del SMS.

Tras recibir un SMS con comandos de lectura (p. ej. "STATUS?"), el CMR envía siempre una respuesta.

Test SMS

Para comprobar los ajustes seleccionados y la conexión, puede ordenarse al CMR que envíe un SMS de prueba a un grupo destinatario configurado.

- **Recipient group**
Grupo de usuarios que debe recibir el SMS de prueba.
- **Text**
Texto configurado que se envía en el SMS de prueba.
- **Send test SMS**
Con este botón se dispara el envío del SMS de prueba con el bloque de texto seleccionado (configurado previamente en "Message texts").

5.11.5 SMS alias

Configuración del alias de SMS

En la tabla se configuran 20 valores como máximo para los textos alias de SMS que debe recibir el CMR. Son SMS con acceso de escritura o SMS con un comando de lectura, p. ej. "DIAG?" para solicitar un SMS de diagnóstico.

Deben configurarse nombres simbólicos que se utilizan como comodines de todo el texto del SMS.

- **Name**
Nombre simbólico del texto
- **Content**
Texto correspondiente del SMS alias en sintaxis correcta.

Ejemplo:

- El nombre alias es: Lamp3ON
(este texto se transfiere como texto del SMS)
- El contenido configurado es: <contraseña>;LOGO=VM125,1,WORD
(la variable VM125 del tipo WORD está vinculada a la salida de la lámpara 3)

Cuando se recibe un SMS con el texto "Lamp3ON", el CMR comprueba antes que nada la contraseña configurada.

Seguidamente, el CMR traduce el texto en "LOGO=VM125,1,WORD" de acuerdo con la configuración de la tabla y pone la variable VM125 del tipo WORD a 1.

5.11.6 E-mail

En esta ficha se configuran los datos para el envío de correos electrónicos por parte del CMR.

Si el CMR no debe enviar correos electrónicos, deje esta página sin editar.

- **SMTP server name**

Nombre del servidor SMTP. Los datos se los proporciona el operador del servicio.

- **Port number**

Número de puerto del servidor SMTP. Los datos se los proporciona el operador del servicio.

- **Encryption method**

Elija una de las opciones siguientes:

- Only STARTTLS

Con este ajuste, los correos electrónico solo se envían si el operador del servicio soporta STARTTLS.

Para esta opción debe importarse un certificado de origen del operador del servicio; véase más abajo.

- STARTTLS, if possible

Con este ajuste, los correos electrónico se envían incluso si el operador del servicio no soporta STARTTLS.

- **Own e-mail address**

Dirección de correo electrónico del CMR. Los datos se los proporciona el operador del servicio.

- **Name**

Nombre exigido por el servidor SMTP. Los datos se los proporciona el operador del servicio.

- **Password**

Contraseña, exigida por el servidor SMTP. Los datos se los proporciona el operador del servicio.

CA certificate

Existe la posibilidad de importar vía STARTTLS el certificado de origen del operador del servicio para el envío de correos electrónicos.

- **Currently used file**

Muestra el nombre del archivo utilizado actualmente

- **Delete**

Con este botón se borra el archivo utilizado actualmente.

El borrado no se ejecutará hasta que se haga clic en el botón "Apply".

- **File used after applying**

Después de cargar el certificado se muestra el nombre del archivo cargado.

- **Load new file**

Al seleccionar un archivo guardado en el PC de configuración utilizando el botón "Search" se muestra el nombre del archivo.

- **Search**

Examina el sistema de archivos del PC de configuración en busca de un archivo de certificado guardado en el mismo que debe cargarse en el CMR.

- **Load on device**

Con el botón "Load on device" se carga en el CMR el archivo seleccionado.

Test e-mail

Existe la posibilidad de comprobar los ajustes y el establecimiento de la conexión enviando un correo electrónico de prueba.

Para ello, es imprescindible que los parámetros siguientes (destinatario, asunto, texto) de "Users / groups" y "Monitoring" estén configurados y que el PC de configuración esté conectado a Internet.

- Recipient group
- Subject
- Text
- Send test e-mail

Haciendo clic en el botón se envía el correo electrónico de prueba.

5.11.7 DynDNS

En esta ficha se puede activar el uso de la asignación de direcciones mediante DNS dinámico (DynDNS) en la interfaz de telefonía móvil. Para ello se requieren uno de los operadores de servicio que pueden seleccionarse más abajo y los datos de acceso correspondientes.

Se recomienda DynDNS si se utiliza OpenVPN y HTTPS.

Nota

DynDNS solo con dirección IP pública

DynDNS solo puede utilizarse con dirección IP pública. Compruébelo con su operador de red.

Si se inicia sesión con el CMR en un servicio DynDNS, será posible acceder al dispositivo desde Internet utilizando un nombre de host, p. ej. "myName.dyndns.org".

Por lo general, el CMR no tendrá una dirección IP fija en la interfaz de telefonía móvil y no estará registrado con un nombre de host. Sin embargo, si se utiliza un Domain Name

System dinámico (DynDNS), será accesible desde Internet. En este caso, la dirección IP pública se dará a conocer mediante el servicio DynDNS.

Cada vez que se entre en la red de datos y cuando se cambie la dirección IP en la interfaz de telefonía móvil, el servidor DynDNS será informado de la dirección IP recibida mediante HTTPS. Se escribirá una entrada con la dirección IP en el búfer de diagnóstico.

El operador del servicio debe autorizar la accesibilidad de la dirección IP desde Internet.

- **Active**

- Si la opción está activada, se activa el uso de DynDNS.
- Si la opción está desactivada, no se autoriza el uso de DynDNS.

- **DynDNS provider**

Puede seleccionar los siguientes operadores de servicio:

- DynDNS
Dirección: <http://www.dyndns.org/>
- No-IP
Dirección: <http://www.noip.com/>

- **Host**

Nombre de host del CMR acordado con el operador del servicio (DynDNS) o seleccionado por el usuario (No-IP).

- **User Name**

Nombre de usuario que le ha notificado el operador del servicio (DynDNS) o que ha seleccionado el propio usuario (No-IP).

- **Password**

Contraseña que le ha notificado el operador del servicio (DynDNS) o que ha seleccionado el propio usuario (No-IP).

CA certificate

Aquí se importa el archivo del certificado de origen del operador del servicio DynDNS. El certificado sirve para autenticar el operador del servicio frente al CMR.

Los certificados no son imprescindibles para el funcionamiento.

En función del operador de servicio se necesitará el certificado siguiente:

- DynDNS
DigiCert CA
- No-IP
Geo Trust Global CA

Solicite a su operador el certificado válido en cada caso.

Parámetro

- **Currently used file**

Muestra el nombre del archivo utilizado actualmente

- **Delete**

Con este botón se borra el archivo utilizado actualmente.

El borrado no se ejecutará hasta que se haga clic en el botón "Apply".

- **File used after applying**

Después de cargar el certificado se muestra el nombre del archivo cargado.

- **Load new file**

Al seleccionar un archivo guardado en el PC de configuración utilizando el botón "Search" se muestra el nombre del archivo.

- **Search**

Examina el sistema de archivos del PC de configuración en busca de un archivo de certificado guardado en el mismo que debe cargarse en el CMR.

- **Load on device**

Con el botón "Load on device" se carga en el CMR el archivo seleccionado.

5.12 Security

5.12.1 Sinopsis

OpenVPN connection

- **Connection exists to the OpenVPN partner**

Estado de la conexión con el cliente OpenVPN

- **IP address of the OpenVPN client**

Muestra la dirección IP pública del cliente OpenVPN.

- **Local endpoint**

Muestra la dirección IP del servidor OpenVPN (CMR).

La dirección IP del servidor OpenVPN dentro del túnel VPN está ajustada de forma fija a 10.8.0.2.

Nota

Ajustes de red si se utiliza OpenVPN

En caso de utilizar OpenVPN, asegúrese de que la subred LAN del CMR y la subred OpenVPN no se solapen, pues de lo contrario no será posible establecer conexiones con el CMR a través de OpenVPN.

Consulte los ajustes LAN en el capítulo LAN (Página 90).

- **Remote endpoint**

Muestra la dirección IP del cliente OpenVPN.

La dirección IP del cliente OpenVPN dentro del túnel VPN está ajustada de forma fija a 10.8.0.1.

- **Connected since (dd:hh:mm:ss)**

Duración de la conexión establecida con el interlocutor de comunicación

Statistics of the current connection

Las cifras son válidas para la conexión establecida actualmente.

Consulte más a bajo el significado de los parámetros.

Statistics since restart

Las cifras son válidas para todas las conexiones establecidas desde el último rearranque completo del CMR.

- **Bytes received**

Número de bytes que el CMR ha recibido.

- **Frames received**

Número de frames que el CMR ha recibido.

- **Received frames lost**

Número de frames recibidos por el CMR que no ha podido procesar.

- **Bytes sent**

Número de bytes que el CMR ha enviado.

- **Frames sent**

Número de frames que el CMR ha enviado.

- **Frames to be sent lost**

Número de frames que esperaban en el CMR a ser enviados pero que no pudieron enviarse.

5.12.2 OpenVPN-PSK

Encontrará información sobre las funciones y los requisitos en los capítulos siguientes:

Otras funciones (Página 15)

Requisitos de aplicación (Página 18)

Nota

DynDNS si se utiliza OpenVPN

Con el fin de simplificar el establecimiento de la conexión cuando se utiliza OpenVPN, se recomienda usar DynDNS.

Ejemplos de aplicación

El túnel VPN se puede utilizar para los siguientes fines:

- Conexión con el CMR mediante HTTP desde un teléfono móvil o el PC de configuración
Es posible acceder al CMR vía HTTP a través de la interfaz de telefonía móvil (no vía HTTPS). Para ello debe utilizarse la siguiente dirección IP de túnel del CMR:
`http://10.8.0.2`
- Conexión con el BM a través del túnel
Es posible acceder directamente al LOGO! BM desde la dirección IP configurada, p. ej. 192.168.0.1. En este caso, el CMR actúa como router para el intercambio de datos. Para ello, introduzca el CMR como router en el BM.
Tras comprobar el establecimiento de la conexión, existe la posibilidad de vigilar el BM (desde la web o una aplicación móvil) y configurarlo mediante LOGO!Soft Comfort.

Crear una conexión OpenVPN

A continuación se explican de forma resumida los pasos a seguir para crear una conexión OpenVPN.

1. Configure y compruebe la conexión de telefonía móvil
2. Opcional: Configure y compruebe DynDNS
3. Genere la Preshared Key, ya sea en el CMR o en el cliente OpenVPN.
Si genera la Preshared Key en el cliente OpenVPN, cárguela en el CMR (véase más abajo).
4. En caso necesario, adapte en el CMR el puerto y el tiempo de vigilancia de inactividad.
Asegúrese de que el puerto se habilita en el interlocutor (cliente OpenVPN) o de que el reenvío de puertos está habilitado en el router al que está conectado el interlocutor.
5. Cargue la configuración del servidor estándar ("vpnpeer.conf") en el PC de configuración. Cambie el nombre del archivo "vpnpeer.conf" por "vpnpeer.ovpn" y guárdelo en el cliente OpenVPN. En caso necesario, modifique el archivo: dirección IP, dirección DNS, PSK en formato Unified

6. Active OpenVPN en el CMR.
7. Active el cliente OpenVPN y compruebe el estado de la conexión en el WBM: "Security > Overview", en su caso el búfer de diagnóstico

OpenVPN-PSK

- **Active**

Active esta opción para habilitar la comunicación segura a través de OpenVPN.

- **Port number**

Aquí se configura el número del puerto OpenVPN del CMR. En el ajuste predeterminado, el puerto tiene el número 1194.

- **Keep-alive monitoring time (s)**

Intervalo de tiempo sin tráfico de telegramas tras el cual el CMR envía un telegrama Keep-Alive al cliente OpenVPN.

Este parámetro suele utilizarse cuando el interlocutor tiene una dirección IP dinámica y se utiliza un nombre DNS para él.

Rango de valores (segundos): 60...65535

- **Save standard server configuration for client**

El CMR ofrece la posibilidad de exportar los ajustes predeterminados propios (servidor OpenVPN) para el cliente OpenVPN al sistema de archivos del PC conectado por medio del archivo "vpnpeer.conf". El archivo contiene ajustes que garantizan el establecimiento de una conexión del CMR con el cliente OpenVPN. El archivo puede importarse al cliente OpenVPN (teléfono móvil o PC). Cambie el nombre del archivo "vpnpeer.conf" por "vpnpeer.ovpn" y guárdelo en el cliente OpenVPN.

El manejo del archivo depende del método de asignación de direcciones del CMR:

- Si se utiliza DynDNS, es posible emplear el archivo directamente para el cliente OpenVPN.
- Si no se utiliza DynDNS hay que adaptar los datos de dirección en el archivo. Para ello es posible editar el archivo con un editor de textos; consulte el apartado más abajo.

Pre-shared key

Este bloque ofrece la posibilidad de generar una clave nueva o de cargar un archivo de claves del sistema de archivos del PC de configuración conectado. Puede ser, por ejemplo, una Preshared Key generada por el cliente OpenVPN.

Están disponibles las siguientes funciones:

- **Generate new key**

Con este botón se genera una nueva Preshared Key en el CMR.

(Esta función equivale a la función "genkey" de un cliente OpenVPN.)

Para guardar la clave consulte la entrada "Save standard server configuration for client" más abajo.

- **Currently used file**

Muestra el nombre del archivo de claves utilizado actualmente

- **File used after applying**

Tras cargar un archivo de claves del sistema de archivos se muestra el nombre del archivo cargado.

- **Load new file**

Al seleccionar un archivo guardado en el PC de configuración utilizando el botón "Search" se muestra el nombre del archivo.

- **Search**

Examina el sistema de archivos del PC de configuración en busca de un archivo de claves guardado en el mismo que debe cargarse en el CMR.

- **Load on device**

Con este botón se carga en el CMR el archivo seleccionado.

- **Save standard server configuration for client**

Esta entrada permite guardar el archivo de configuración del CMR en el sistema de archivos de su PC de configuración. El archivo se llama "vpnpeer.conf" y contiene la Preshared Key generada por el CMR, entre otros datos.

Archivo "vpnpeer.conf"

A continuación encontrará el contenido del archivo de configuración exportado por el CMR para el cliente OpenVPN (interlocutor de comunicación del CMR).

Nota

Archivo de configuración sin cifrar: Transferencia cifrada

El archivo de configuración para el cliente OpenVPN no está cifrado. La Preshared Key está incluida en el archivo sin cifrar.

Transfiera el archivo al interlocutor utilizando un método seguro, p. ej. HTTPS.

Tabla 5- 4 Contenido del archivo de configuración "vpnpeer.conf"

Archivo original	Archivo adaptado
<pre>dev tun0 disable-occ # Please update your OpenVPN peer's address on the next line remote vpn.example.com 1194 ifconfig 10.8.0.1 10.8.0.2 nobind keepalive 15 60 route 192.168.0.0 255.255.255.0 tun-mtu 1500 fragment 1371 mssfix 1282 persist-key replay-window 512 15 cipher AES-128-CBC auth SHA256 comp-lzo verb 4 #key-direction 1 #<secret> # Please insert your key here and uncomment these lines #</secret></pre>	<pre>dev tun0 disable-occ remote 192.168.229.29 1196 ifconfig 10.8.0.1 10.8.0.2 nobind keepalive 15 60 route 192.168.0.0 255.255.255.0 tun-mtu 1500 fragment 1371 mssfix 1282 persist-key replay-window 512 15 cipher AES-128-CBC auth SHA256 comp-lzo verb 4 key-direction 1 <secret> # # 2048 bit OpenVPN static key # -----BEGIN OpenVPN Static key V1----- 1a17c9b9737c0fd0b33eb540ba845340e2dad229b8d6fd9b82 f934563d8169843021d0bc1fcec0862d560b0917685cbe0315 7aa9cb952de7566dd43f120d7278c1d672dad724457eaed3c6 412a14434d9da2f97158465e95b711e68f1b80d681 ca4e3f3f6d7cdac38cc6dddfb74f23b175becbb6125093d41a 3af1456824760db3e46e0bc8d20539c7fc1a4111c7cdb57155 2c1a7bfd707848bbe3eca036e9a2092eea5d9041001bd07a3d c0a8b6636fce42fc94b1446c283c24daa458460ef9ab8a18eb b9c4791f45d87f11e0918f002bfdbbc955d74d7ffc7fa4bacd 6f15f10137ebde93b8219ae38ebae9b029e97cd79d204255f3 0a048865ffbb3eabb6b9-----END OpenVPN Static key V1----- </secret></pre>
<p>Observaciones:</p> <ul style="list-style-type: none"> Este es el contenido original del archivo exportado por el CMR. <p>El archivo puede importarse al cliente OpenVPN en esta forma si se utiliza DynDNS.</p> <ul style="list-style-type: none"> En caso de exportar el archivo en esta forma, en el CMR faltará todavía la Preshared Key. Deberá importarse la Preshared Key al cliente (interlocutor) y al servidor (CMR). 	<p>Observaciones:</p> <p>El contenido se ha adaptado para el ejemplo al uso de OpenVPN sin DynDNS:</p> <ul style="list-style-type: none"> La tercera fila del archivo original, marcada como comentario, se ha borrado y se ha adaptado la dirección en la próxima fila. La penúltima fila del archivo original, marcada como comentario, y los comentarios se han borrado y la Preshared Key se ha complementado.

5.12.3 HTTPS

Para el uso de HTTPS para la comunicación segura a través de Internet y la red de telefonía móvil con el CMR es imprescindible una tarjeta SIM para el CMR con una dirección IP de acceso público.

Encontrará información sobre las funciones y los requisitos en los capítulos siguientes:

Otras funciones (Página 15)

Requisitos de aplicación (Página 18)

HTTPS

- **Enable HTTPS on the mobile wireless interface**

Active esta opción para habilitar la comunicación segura a través de Internet y la red de telefonía móvil con el CMR vía HTTPS. De este modo se abre el puerto 443 en la interfaz WAN.

Observación:

En la interfaz LAN, HTTPS siempre está activo.

Nota

Conexiones con el acceso HTTPS a través de la interfaz de telefonía móvil

El CMR pone a disposición una sola conexión en la interfaz de telefonía móvil. Por este motivo debe utilizarse un navegador que también trabaje con una sola conexión (Mozilla Firefox, Apple Safari). En los navegadores que necesitan un mínimo de dos conexiones (p. ej. Internet Explorer 11, Edge, Chrome), no se establece ninguna conexión operativa o bien las páginas web no se muestran correctamente.

Nota

Actualización de páginas en el acceso HTTPS

Utilice las posibilidades siguientes para actualizar y recargar una página web:

- El botón "Refresh" del WBM
- Haga clic en el enlace de la página deseada dentro del área de navegación izquierda de la ventana del navegador
- Repita la entrada en la barra de direcciones

Impida que se actualice la página utilizando los mecanismos estándar del navegador ("Volver a cargar página" o F5).

En función del dispositivo y de la red de telefonía móvil disponible, es posible que las páginas tarden unos segundos en cargarse y, si la conexión es mala o se cambia la celda, puede que se interrumpa.

Own certificate

En los ajustes de fábrica, el CMR utiliza un certificado de servidor expedido por él mismo para la autenticación en el interlocutor de la comunicación (cliente). En este caso, al establecer la conexión se genera un aviso en el navegador del PC desde el que debe conectarse al CMR.

Nota

Advertencia sobre el certificado (HTTPS)

Cuando se establece la conexión vía HTTPS, al iniciar la sesión se genera una advertencia indicando que la página web no es segura o que el certificado no es fiable. Si está seguro de que ha introducido la dirección correcta, ignore el aviso. En caso necesario, agregue la conexión a las excepciones de su navegador web (depende del navegador).

Otra posibilidad consiste en importar un certificado ajeno, por ejemplo un certificado expedido por la aplicación del cliente.

- **Currently used file**

Muestra el nombre del archivo utilizado actualmente

- **Delete**

Con este botón se borra el archivo utilizado actualmente. El borrado no se ejecutará hasta que se haga clic en el botón "Apply".

Después de borrar un certificado importado, el CMR utiliza de nuevo el certificado que ha expedido él mismo de los ajustes de fábrica.

- **File used after applying**

Después de cargar el certificado se muestra el nombre del archivo cargado.

- **Load new file**

Al seleccionar un archivo guardado en el PC de configuración utilizando el botón "Search" se muestra el nombre del archivo.

- **Search**

Examina el sistema de archivos del PC de configuración en busca de un archivo de certificado guardado en el mismo que debe cargarse en el CMR.

- **Load on device**

Con el botón "Load on device" se carga en el CMR el archivo seleccionado.

Own key

En los ajustes de fábrica, el CMR utiliza una clave privada que él mismo ha generado para cifrar los datos que deben transferirse mediante SSL/TLS.

Otra posibilidad consiste en importar una clave ajena, por ejemplo una clave privada. Es necesario utilizar una clave privada sin contraseña.

- **Currently used file**

Muestra el nombre del archivo utilizado actualmente

- **Delete**

Con este botón se borra el archivo utilizado actualmente.

El borrado no se ejecutará hasta que se haga clic en el botón "Apply".

- **File used after applying**

Después de cargar el archivo de claves se muestra el nombre del archivo cargado.

- **Load new file**

Al seleccionar un archivo de claves guardado en el PC de configuración utilizando el botón "Search" se muestra el nombre del archivo.

- **Search**

Examina el sistema de archivos del PC de configuración en busca de un archivo de claves guardado en el mismo que debe cargarse en el CMR.

- **Load on device**

Con el botón "Load on device" se carga en el CMR el archivo seleccionado.

5.13 Users / groups

En el CMR es posible crear y configurar como máximo 20 usuarios.

A continuación pueden crearse hasta 10 grupos destinatarios. A los diferentes grupos destinatarios se les asignan entre 1 y 10 usuarios.

Encontrará la descripción para crear, modificar y borrar usuarios y grupos en el capítulo Funciones generales del WBM (Página 60).

5.13.1 Users

En la ficha pueden introducirse como máximo 20 usuarios. Asigne a dichos usuarios atributos y derechos.

Al hacer clic en el botón "Apply" se adoptan todos los ajustes realizados en la ficha "Users".

Nota

Caracteres permitidos y longitudes de contraseñas

Encontrará las condiciones para contraseñas en el capítulo Caracteres permitidos y longitudes de strings (Página 64).

Add a new user / Change user

- Haga clic en el botón "Add" para agregar un usuario nuevo.

Se abre el grupo de parámetros "Add a new user", en cuyos campos de entrada y listas desplegables se configuran los parámetros.

- Para modificar los datos de un usuario existente, seleccione el usuario en cuestión en la lista de la parte superior.

El grupo de parámetros "Change user" permite modificar todos los datos del usuario, excepto el nombre de usuario y la contraseña.

Para modificar también el nombre de usuario y la contraseña de un usuario, haga clic en el botón "Change login data". Seguidamente se habilitarán los campos de entrada para el nombre de usuario y la contraseña.

Configuración

- **Name**

Nombre de libre elección, por ejemplo nombre y apellido. Este nombre no se utiliza para iniciar sesión en el WBM y puede contener caracteres especiales.

- **Description**

Texto de libre elección para describir al usuario con mayor detalle, p. ej., "Empleado del servicio técnico".

- **Phone number**

Número de teléfono para ponerse en contacto con el usuario.

También existe la posibilidad de crear grupos de números de teléfono utilizando el carácter * (asterisco). Así, p. ej., con la entrada "+49172*" se autoriza a enviar SMS al CMR a todos los números de teléfono que empiecen por "+49172".

Nota

Para tener en cuenta si se utilizan grupos de números de teléfono

Si se utilizan grupos de números de teléfono, tenga en cuenta que los usuarios de estos grupos no pueden recibir mensajes SMS. Los usuarios de estos grupos solo tienen autorización para enviar mensajes SMS al CMR.

- **Allow receipt of SMS messages**

"Allow receipt of SMS messages" significa que el usuario creado puede enviar comandos por SMS al CMR.

- Un SMS del usuario con el número de teléfono indicado se recibe y se evalúa (permitir recepción).
- Un SMS del usuario con el número de teléfono indicado se rechaza: el SMS no se evalúa (no permitir recepción).

- **Phone number can be changed for this user by SMS message**

El número de teléfono de este usuario puede cambiarse mediante SMS a través del comando "CHANGEUSER".

El cambio de número de teléfono mediante SMS puede ser útil en los siguientes casos:

- Si desea configurar una sustitución por vacaciones durante un periodo determinado.
- Si un número de teléfono ha cambiado y no puede o no desea realizar dicho cambio in situ mediante el WBM.

- **E-mail address**

Dirección de correo electrónico del usuario para recibir correos electrónicos.

Si no se introduce ninguna dirección de correo electrónico, el usuario no puede recibir correos electrónicos del CMR.

- **Change login data**

Haga clic en este botón para modificar el nombre de usuario y la contraseña del usuario.

- **User Name**

Es el nombre de usuario con el que el usuario inicia sesión en el WBM del CMR.

- **Password**

Contraseña del usuario para iniciar la sesión en el WBM del CMR.

La contraseña debe cumplir las reglas de contraseña mostradas.

- **Repeat password**

- **Do not use password rules**

Si se activa esta opción, las reglas de contraseña ajustadas de fábrica se desactivan y puede asignarse una contraseña de libre elección. La longitud sigue estando limitada a 20 caracteres como máximo.

Con el botón "Apply" se aplican todos los cambios y la lista se actualiza.

5.13.2 Recipient groups

En esta ficha se configuran los grupos de destinatarios o se realizan modificaciones en grupos de destinatarios ya configurados.

Pueden crearse como máximo 10 grupos con 10 usuarios por grupo.

Add new group / Edit group data

- Haga clic en el botón "Add new group" para agregar un grupo nuevo.

En el grupo de parámetros "Add new group" se configuran los campos de entrada y las listas desplegables de los parámetros.

- Para modificar los datos de un grupo existente, seleccione el grupo en cuestión en la lista de la parte superior.

En el grupo de parámetros "Edit group data" se modifican los campos de entrada y las listas desplegables de los parámetros.

En la parte inferior de la página se encuentran todos los usuarios configurados con número de teléfono y dirección de correo electrónico.

Cuando se selecciona un grupo de la lista superior en la página, se marcan con un marca de verificación los usuarios que forman parte de dicho grupo.

Configuración

- **Name**

Nombre de grupo de libre elección. Este nombre puede contener caracteres especiales.

- **Description**

Texto de libre elección para describir el grupo con más detalle.

- **Group type**

Aquí se especifica si este grupo está previsto para recibir SMS o correos electrónicos.

Con el botón "Apply" se aplican todos los cambios y la lista se actualiza.

5.14 Monitoring

Antes de empezar a configurar la vigilancia del BM o del CMR en modo autónomo, es recomendable familiarizarse con el principio de la vigilancia y sus funciones en el capítulo siguiente.

En los capítulos correspondientes a las diferentes fichas del WBM encontrará una descripción detallada de la funciones.

Encontrará la descripción para crear, modificar y borrar elementos de las diferentes fichas (textos, señales, acciones, etc.) en el capítulo Funciones generales del WBM (Página 60).

Encontrará un ejemplo para configurar la vigilancia al final del capítulo Ejemplo de configuración de la vigilancia (Página 132).

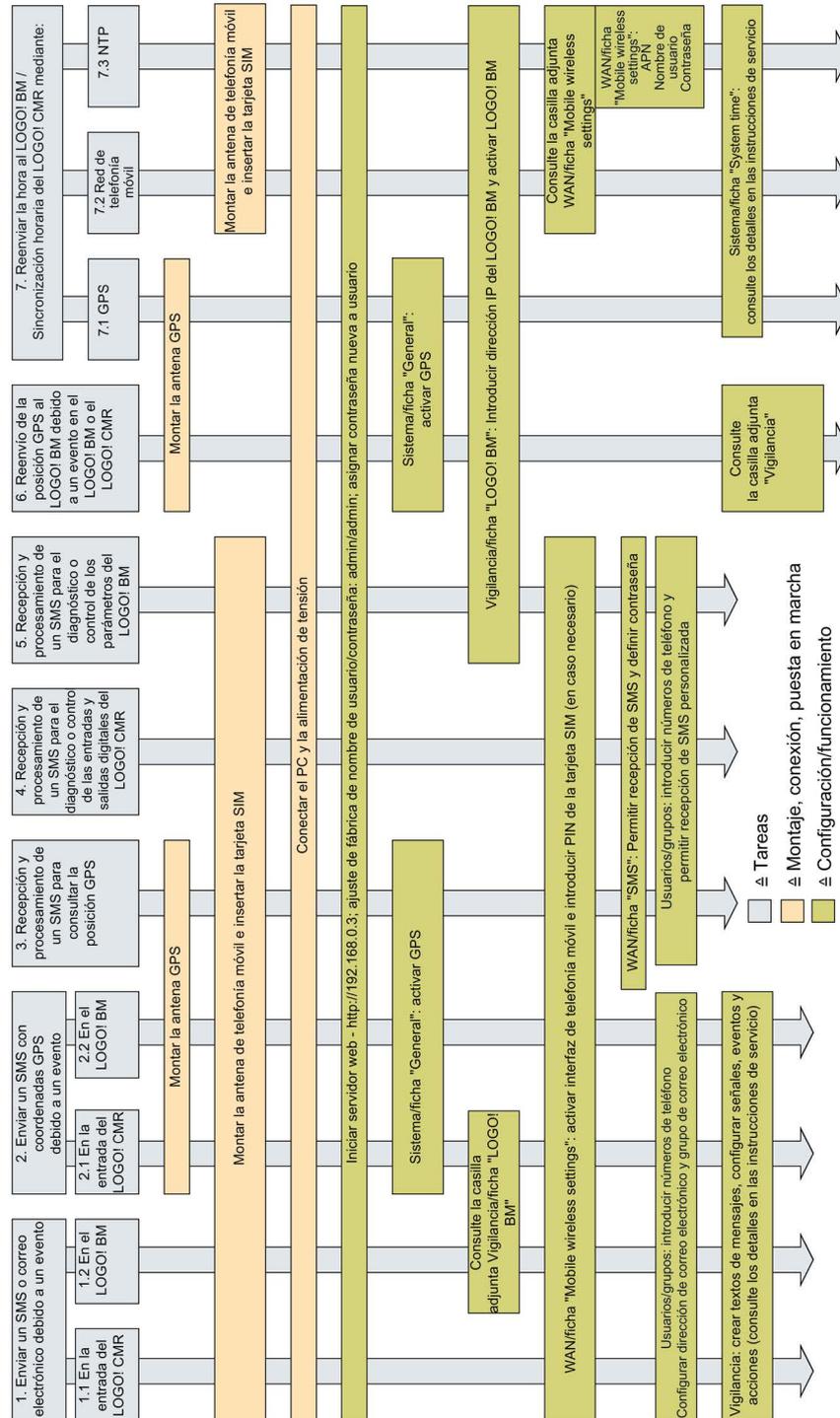
Nota

Mayor volumen de datos debido a la vigilancia del BM

Tenga en cuenta que la vigilancia del BM conlleva un mayor volumen de datos.

5.14.1 Vigilancia - ¿Qué debo hacer?

A continuación se ofrece un esquema general de las distintas aplicaciones/tareas y los pasos necesarios para realizarlas a fin de facilitar su comprensión:



5.14.2 Funciones de vigilancia

Las funciones de vigilancia

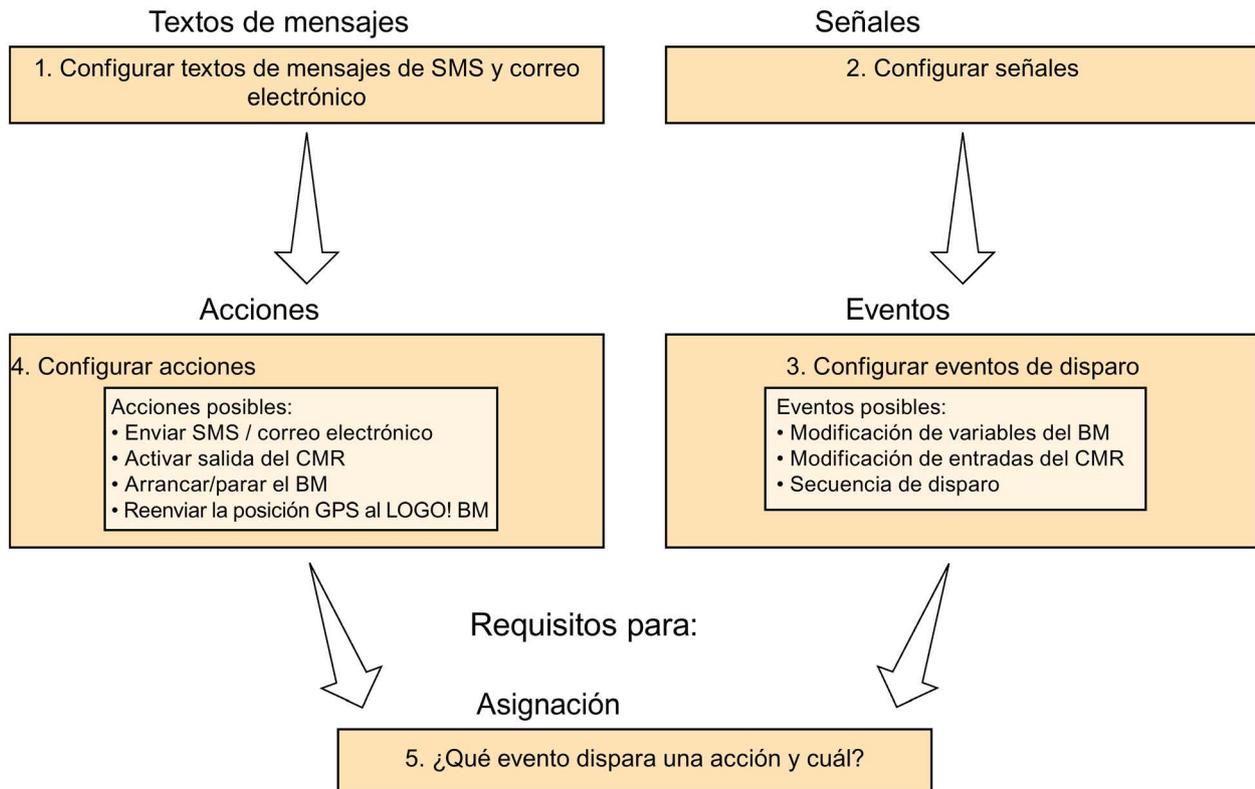


Figura 5-4 Monitoring: procedimiento durante la configuración

Fichas del grupo "Monitoring" - Sinopsis

- **Ficha "Overview"**

En la ficha "Overview" se muestran todas las señales configuradas con su estado actual.

En el estado de suministro, las entradas y salidas del CMR ya están creadas como señales.

Las señales que provienen del LOGO! BM se muestran en rojo cuando no hay conexión entre el CMR y el BM.

- **Ficha "LOGO! BM"**

Solo se establece una conexión entre el CMR y el BM si se ha activado la opción "Active".

Si la opción está desactivada, no se establece conexión alguna con el BM.

- Introduzca la dirección IP del BM.

- Compruebe que la dirección IP introducida sea accesible para el CMR.

- Query interval for process image: Defina los intervalos de tiempo en los que el CMR debe leer la memoria imagen de proceso del BM.

- **Ficha "Constants"**

Aquí se definen valores fijos para variables que deben escribirse para el acceso de escritura al BM por SMS.

- **Ficha "Message texts"**

Deben crearse textos que se enviarán por SMS o correo electrónico. Los textos del mensaje reciben nombres simbólicos.

El envío de estos textos a un destinatario o a un grupo destinatario se configura como acción en la ficha "Actions". Esta acción se asigna a un evento en la ficha "Assignments".

- **Ficha "Signals"**

En primer lugar, determine las señales que desee que vigilen el BM o el CMR, p. ej., la entrada digital 1 (I1) del BM.

Todas las señales pueden recibir nombres simbólicos.

- **Ficha "Events"**

Para la señal seleccionada se configura un evento, p. ej. I1 "Changes to 0".

- **Ficha "Actions"**

Defina una o varias acciones, primero independientemente de cualquier evento:

- Enviar un SMS o un correo electrónico a un grupo destinatario
- Activar una salida en el CMR
- Enviar un SMS con la memoria imagen de proceso
- Reenviar una posición GPS al LOGO! BM
- Cambiar el estado de programa del LOGO! BM

Todas las acciones pueden recibir nombres simbólicos.

- **Ficha "Assignments"**

Deben asignarse acciones concretas a los eventos configurados, p. ej. enviar un SMS a un grupo destinatario concreto cuando cambia una salida del BM.

En la parte inferior de la página, en "If:" y "Then:", se muestra la acción que debe ejecutarse con todos los parámetros ajustados.

5.14.3 Overview

Todas las señales configuradas del BM y del CMR se muestran con nombres simbólicos y el estado actual.

Las entradas y salidas del CMR se muestran en el estado de suministro una vez restablecida la configuración de fábrica.

Indicación si se interrumpe la conexión entre el CMR y el BM

- Ha configurado una conexión entre el CMR y el BM en la ficha "LOGO! BM".
- Se han configurado tipos de señales del LOGO! BM en la ficha "Signals".

La conexión entre el CMR y el BM se interrumpe, p. ej., retirando el cable Ethernet:

- El LED de error del CMR se enciende en rojo.
- En la ficha "Overview" se representan todos los tipos de señal configurados del BM con letra roja.
- Si la señal "LOGO! BM" se ha configurado con el tipo de señal "CS - communications status", la señal cambia al estado "Off".

Nota

Indicación retardada de la interrupción de la conexión

El CMR detecta la interrupción de la conexión con un retardo de varios segundos.

5.14.4 LOGO! BM

Establecer la comunicación entre el BM y el CMR

1. Introduzca la dirección IP del BM en el campo de entrada "IP address of the LOGO! BM".
2. Active la casilla de verificación "Active". De este modo se establecerá una conexión entre el CMR y el BM.

Si la casilla de verificación está desactivada, no existe ninguna conexión entre el CMR y el BM.

3. Con el "Update interval for process image" se definen los intervalos (selección: "1 second" y "10 seconds") en los que el CMR debe leer la memoria imagen de proceso del BM.

El CMR tiene una copia de la memoria imagen de proceso actual y la envía por SMS o correo electrónico en caso de solicitud; consulte los capítulos Comandos SMS (Página 176) y SMS de respuesta del comando "MONITOR?" (Página 181).

4. A continuación, haga clic en el botón "Apply". Se adoptan los ajustes realizados.
5. Haga clic en el botón "Ping LOGO! BM":

compruebe si la dirección IP introducida para el CMR está accesible. Se muestra un aviso indicando si la dirección IP es accesible o no.

5.14.5 Constantes

Configuración de las constantes

En la tabla se configuran los valores de las constantes para SMS de escritura. Esto es útil cuando suelen transferirse valores idénticos por SMS. En este caso, no es necesario escribir el valor de escala en el texto del SMS, sino que en su lugar se escribe el nombre de la constante.

Los nombres simbólicos se configuran como comodines del valor que debe escribirse.

- Name

Nombre de la constante

- Value

Valor que debe escribirse y que reemplaza el nombre de la constante cuando se recibe el SMS.

Ejemplo 1

- El nombre de la constante es: OFF

El nombre de la constante se transfiere en el texto del SMS en lugar del valor real.

- El valor configurado de la constante es: 0
- El texto del SMS es: <Password>;LOGO=VM125,OFF,BYTE

Cuando se recibe un SMS con el texto "<Password>;LOGO=VM125,OFF,BYTE", el CMR comprueba antes que nada la contraseña configurada.

Seguidamente, el CMR traduce el texto siguiente en "LOGO=VM125,0,BYTE" de acuerdo con la configuración de la tabla y lo escribe en la memoria de variables del BM.

Ejemplo 2

En este ejemplo, en lugar de la dirección de la memoria de variables se utiliza un señal configurada; consulte a este respecto el capítulo Signals (Página 122).

- El nombre de la constante es: OFF

El nombre de la constante se transfiere en el texto del SMS en lugar del valor real.

- El valor configurado de la constante es: 0
- La señal "Light" está configurada como: VM125,BYTE
- El texto del SMS es: <Password>;LOGO=Light,OFF

Tenga en cuenta lo siguiente: Cuando se utiliza una señal configurada, no está permitido enviar el tipo de datos (en este caso: BYTE) junto con el texto del SMS.

Cuando se recibe un SMS con el texto "<Password>;LOGO=Light,OFF", el CMR comprueba antes que nada la contraseña configurada.

El CMR traduce el texto siguiente en "LOGO=VM125,0,BYTE" de acuerdo con la configuración de la constante y la señal y lo escribe en la memoria de variables del BM.

5.14.6 Message texts

Agregar un nuevo texto de mensaje

Existe la posibilidad de crear diferentes textos de mensajes para SMS y correos electrónicos.

Cada texto de mensaje puede recibir un nombre simbólico. El texto puede crearse como se desee, con un máximo de 160 caracteres por texto de mensaje.

- En la ficha Actions (Página 126) se configuran los textos que se envían a los grupos destinatarios y a cuáles.
- Al hacer clic en el botón "Apply" se adoptan todos los ajustes realizados en la ficha "Message texts".

Enviar también valores de proceso y parámetros

En los textos de mensajes de SMS y correo electrónico, así como en el asunto de los correos electrónicos es posible enviar también valores de proceso y parámetros como hora, fecha y posición GPS.

Utilizando comodines en ciertos casos pueden enviarse 2 mensajes SMS.

Encontrará los formatos permitidos para los comodines de los valores de proceso en Caracteres permitidos y longitudes de strings (Página 64).

5.14.7 Signals

En esta ficha se configuran señales individuales para utilizarlas más adelante.

Pueden configurarse como máximo 32 señales.

Señales para la vigilancia

Aquí se especifican los datos de proceso, cambios, estados, disparos u otros datos internos que deben utilizarse como señales para la vigilancia posterior. Estas señales se utilizan después para configurar los eventos.

Señales para textos de SMS y correo electrónico

Las señales que provienen del BM con el tipo de señal "memoria de variables", así como las señales del CMR pueden utilizarse también como comodín para variables en el texto de SMS y correos electrónicos.

Tenga en cuenta lo siguiente: Cuando se utiliza una señal configurada, no está permitido enviar el tipo de datos junto con el texto del SMS.

Ejemplos

• Ejemplo 1

Debe configurarse lo siguiente:

- Signal name = Motor_2
- Signal source = LOGO! CMR
- Signal type = I/O
- I/O type = Output
- Number = 1

Recepción de SMS:

Cuando se recibe un SMS con el texto "OUTPUT=Motor_2,0", el CMR interpreta el texto del SMS como "OUTPUT=O1,0".

El comando pone la señal "Motor_2", es decir, la salida 1 del CMR, al valor cero.

• Ejemplo 2

El SMS debe conseguir que un valor de la memoria de variables del BM se escriba en otra variable del BM. Para ello se utilizan dos señales.

Debe configurarse lo siguiente:

- Signal name 1 = Basin_1
- Signal source = LOGO! BM
- Signal type = VM - Variable memory
- Data type = WORD
- Dirección = 107

y

- Signal name 2 = Volume_3
- Signal source = LOGO! BM
- Signal type = VM - Variable memory
- Data type = WORD
- Dirección = 50

Recepción de SMS:

Cuando se recibe un SMS con el texto "LOGO=Basin_1,Volume_3", el CMR copia el valor de "Volume_3" en la señal "Basin_1".

Signal source y Signal type

Como origen de las señales puede configurarse el BM o el CMR con sus propios tipos de señales. Están disponibles los siguientes tipos de señales:

- **Tipos de señales BM**

En el "LOGO! BM" son todos los componentes de la memoria imagen de proceso del BM, las áreas de la memoria de variables, el estado del programa y el estado de la conexión con el CMR.

- Digital input
- Digital output
- Digital memory bit
- Analog input
- Analog output
- Analog memory bit
- Function key
- Cursor key
- Digital shift register
- Program status
- Communication status (estado de la comunicación con el CMR)
- Variable memory

- **Tipos de señales CMR**

En el "LOGO! CMR" sin las entradas y salidas, disparos o los estados de conexión de la interfaz de telefonía móvil.

- I/O (entrada/salida)
- Trigger

Alternativamente, es posible crear los siguientes tipos de disparo:

- disparo periódico que se lanza cíclicamente.
- disparo de hora que se lanza una vez al día.
- Connection status wireless mobile network
- Connection status data service

Change signal / Add new signal

- **Name**

Nombre simbólico de la señal

A continuación, el nombre de la señal se utilizará para la configuración de eventos y asignaciones y podrá emplearse en comandos de SMS.

- **Signal source**

"LOGO! BM" para el BM o "LOGO! CMR" para el CMR

- **Signal type**

(véase la lista anterior)

En función del tipo de señal se muestran otras listas desplegables:

- **Trigger type**

- **Number**

- **Address**

- **Bit**

5.14.8 Events

Para una señal seleccionada se configura un evento, p. ej. I1 "Changes to 0".

En la parte superior de la página se muestra una lista con los eventos configurados actualmente.

Pueden configurarse como máximo 32 eventos.

Add new event / Change event

Acto seguido aparecerán un campo de entrada y dos listas desplegables para la configuración:

- **Name**

Nombre de evento simbólico, de libre elección.

A continuación, el nombre del evento se utilizará para la configuración de asignaciones.

- **Signal name**

Seleccione la señal correspondiente en la lista desplegable.

Se ofrecen todas las señales configuradas con sus nombres simbólicos.

- **Event**

Debe configurarse el evento. Ejemplos:

La entrada digital cambia de "1" a "0".

La marca analógica rebasa por exceso o por defecto el valor definido en este punto.

De acuerdo con la selección realizada, en "Signal name" e "Event" se muestran otros botones que permiten completar el evento.

5.14.9 Actions

Configure una o varias acciones que pueda vincular a eventos más adelante en la ficha "Assignments".

En la parte superior de la página se muestra una lista con las acciones configuradas actualmente.

Pueden configurarse como máximo 32 acciones.

Add new action / Change action

Agregar una acción

En la parte inferior de la página, haga clic en el botón "Add".

Acto seguido aparecerán un campo de entrada y tres listas desplegables para la configuración:

Modificar una acción

Proceda del modo correspondiente para modificar una acción.

1. Seleccione en la lista la fila con la acción que desea modificar.
2. Modifique la acción mediante "Change action" en la parte inferior de la página.
3. Finalmente, haga clic en "Apply".

Parámetros**• Name**

Nombre simbólico de libre elección para esta acción.

A continuación, el nombre de la acción se utilizará para la configuración de asignaciones.

• Target system

Sistema de destino de la acción:

– LOGO! CMR

Si se selecciona el CMR, las dos salidas del CMR pueden utilizar una acción como Target element, p. ej. abrir una salida.

– LOGO! BM

Si se selecciona el BM como sistema de destino, es posible modificar el estado del programa del BM o reenviar la posición GPS al BM.

– Send e-mail

Con esta selección se configuran el grupo destinatario (véase más abajo), el asunto, el texto del mensaje y el anexo, si lo hubiera.

– Send SMS

Con esta selección se configuran el grupo destinatario (véase más abajo) y el texto del mensaje.

– Send PA-SMS (enviar SMS de la memoria imagen de proceso)

Con esta selección se configura el grupo destinatario (véase más abajo).

• Target element

Solo si se seleccionan los sistemas de destino "CMR" y "BM". Seleccione aquí el elemento deseado.

– CMR: Output**– BM: Program status, GPS position**

De acuerdo con la selección realizada se muestran otras listas desplegables que permiten especificar la acción.

Otros parámetros

- **Recipient group**

Cuando se selecciona un elemento de destino para enviar un SMS o un correo electrónico se elige un grupo destinatario, pero no usuarios o números de teléfono concretos.

Si se selecciona el sistema de destino "Send e-mail" se ofrecen adicionalmente las opciones "Subject" y "Text", para los que deben seleccionarse Message texts configurados, así como la opción de enviar un Attachment junto con el correo electrónico.

Si se selecciona como sistema de destino "Send SMS" o "Send PA-SMS", se ofrecen los grupos destinatarios de SMS que se han configurado.

- **Subject / Message text**

En función del tipo de mensaje que deba enviarse (correo electrónico / SMS), se configuran un asunto y un texto del mensaje. Los textos deben haberse configurado previamente en la ficha "Message texts".

Puede seleccionar la transmisión de los datos de posición GPS actuales al LOGO! BM como acción. Los eventos que se disparan pueden ser, p. ej., la finalización de un temporizador o el cambio de estado de una entrada del BM o del CMR.

El desarrollo básico de la configuración no varía:

1. Configurar los ajustes del LOGO! BM
2. Configurar la señal
3. Configurar el evento
4. Configurar la acción con el destino "LOGO! BM" y el Target element "Forward GPS position"
5. Configurar la asignación

La dirección inicial a partir de la cual se guardan los datos de posición GPS en la VM del LOGO! BM debe estar entre 0 y 112.

Estructura de los datos de posición GPS

El bloque de datos transferido al BM se escribe byte por byte y abarca una longitud de 16 bytes. La estructura del bloque de datos es la siguiente:

Nota

Representación de las letras

Las letras se representan como caracteres ASCII decimales: P. ej. "78" para "N" y "83" para "S" así como "69" para "E" y "87" para "W".

Nota**Aplicación en el BM: evaluar "state" y "count"**

Para garantizar la coherencia de los datos, la aplicación del BM debe evaluar los bytes "state" y "count":

1. Si "state" = "invalid": el CMR está escribiendo los datos.
Solo si está ajustado "state" = "valid", es posible el acceso.
2. Si "state" = "valid": a continuación se lee el Write Counter y se guarda el valor leído.
3. Una vez leída toda la estructura de datos, compruebe si el Write Counter ha variado su valor:
 - Si el valor no ha variado, la estructura de datos puede volver a utilizarse.
 - Si el valor ha variado, repita el ciclo de lectura y comience por el paso "1."

Número del byte	Parámetro	Significado
0	latNS	North / South (N/S)
1	latD	Degrees (0 ... 179)
2	latM	Minutes (0 ... 59)
3	latS	Seconds (0 ... 59)
4	latSF	Seconds Fraction (0 ... 99)
5	IngEW	East / West (E/W)
6	IngD	Degrees (0 ... 179)
7	IngM	Minutes (0 ... 59)
8	IngS	Seconds (0 ... 59)
9	IngSF	Seconds Fraction (0 ... 99)
10 11	alt	Altitude meters (-32767 ... +32767)
12	satNum	Number of satellites in use
13	state	GPS signal state (0,1,2) <ul style="list-style-type: none"> • 0: invalid <p>"invalid = 0" se establece durante una operación de escritura por parte del CMR.</p> <ul style="list-style-type: none"> • 1: current position • 2: not current position
14	count	Write Counter: se incrementa cada vez que se escriben datos GPS desde el CMR.
15	res1	reserved for later use

5.14.10 Assignments

Asigne una acción a un evento que haya configurado.

En la parte superior de la página se muestra una lista con las asignaciones configuradas hasta el momento:

- Se admiten como máximo 32 asignaciones.

Si aún no se ha definido ninguna asignación, la lista está vacía.

En la parte inferior de la página, en "Change assignment", encontrará el área necesaria para configurar una asignación.

Nota

Solo al asignar un evento a una acción se activa la vigilancia del evento

1. Se han configurado textos de mensajes, señales, eventos y acciones.
2. Asigne el evento a una acción.
3. Active la casilla de verificación "Activate assignment".

De esta forma se activa la asignación para una vigilancia.

Solo si esta asignación está activa, al asignar una acción a un evento se vigila dicho evento.

Nota

Acciones derivadas de eventos del LOGO! BM

Los requisitos siguientes son válidos para la vigilancia de eventos del BM y su configuración como asignación:

- La conexión entre el CMR y el BM está establecida.
 - El estado del programa del LOGO! BM es 1 (RUN).
-

Add new assignment

1. En la parte inferior de la página, haga clic en el botón "Add".
2. A continuación se ofrecen tres bloques con campos de entrada, listas desplegables, casillas de verificación y campos de texto atenuados para la configuración:

Name

- Nombre de asignación simbólico, de libre elección.
- Active/desactive la asignación en la casilla de verificación "Activate assignment".

If:**Event**

- En la lista desplegable, seleccione la entrada del evento que ha creado.

La entrada se muestra con el nombre simbólico asignado.

Los campos atenuados "Signal name", "Signal" y "Event" indican qué evento debe aplicarse como condición Si con los datos mostrados:

- Signal name

Este ajuste ya se ha realizado en la ficha Signals (Página 122):

Indica el nombre simbólico que se ha asignado para una señal.

- Signal definition

Este ajuste ya se ha realizado en la ficha Signals (Página 122):

Muestra la señal (fuente, tipo) que se utiliza con el nombre de señal simbólico que ha seleccionado.

- Event definition

Este ajuste ya se ha realizado en la ficha Events (Página 125):

Indica el evento que se ha configurado. El nombre proviene de la columna "Event configuration".

Then:**Action**

- En la lista desplegable, seleccione la entrada de la acción que ha creado.

La entrada se muestra con el nombre simbólico asignado.

El campo atenuado "Action configuration" muestra la acción configurada a modo de control. El contenido equivale a la columna correspondiente de la tabla que se encuentra en la ficha "Actions".

5.14.11 Ejemplo de configuración de la vigilancia

El siguiente ejemplo sencillo muestra los pasos explicados hasta ahora para configurar la vigilancia.

Supuestos

- Se supervisa el nivel de un recipiente. En caso de rebase por exceso del nivel máximo debe enviarse una alarma al personal de mantenimiento en forma de SMS.
- El personal de mantenimiento está formado por dos trabajadores, "User-1" y "User-2".
- El medidor de nivel está conectado a la entrada digital n.º 1 del LOGO! BM:

Si se rebasa por exceso el valor límite, el medidor de nivel pone la entrada digital n.º 1 a "1".

Procedimiento

Requisitos: el CMR y el BM deben estar conectados entre sí mediante un cable Ethernet.

1. En la ficha "LOGO! BM", introduzca la dirección IP del BM en el campo de entrada "IP address of LOGO! BM".
2. Para que el CMR establezca una conexión con el BM, active la casilla de verificación "Active".

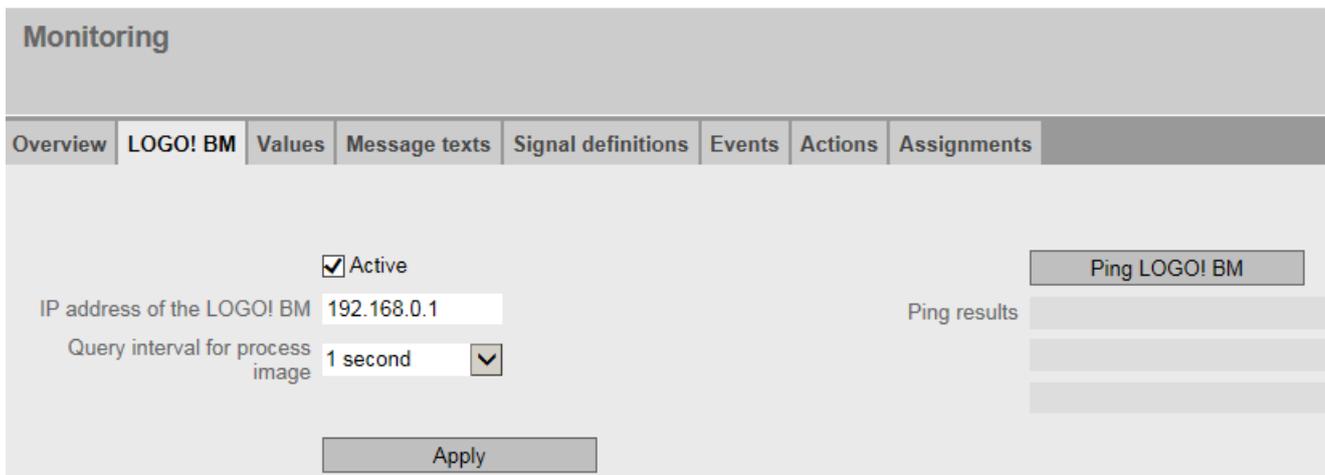


Figura 5-5 Monitoring – ficha "LOGO! BM": establecer una conexión con el BM

3. En la ficha "Users" introduzca los dos usuarios User 1 y User 2 con las propiedades siguientes:

User		Recipient groups					
NOTE: Maximum number of users: 20.							
	Name	Description	Login	Phone number	E-mail address	Allow receipt of SMS messages	Phone number of this user
1	User 2		JS	0721-12345678-2	user2@siemens.com	Yes	Yes
2	User 0		admin	0721-12345678-0	user0@siemens.com	Yes	Yes
3	User 1		SK	0721-12345678-1	user1@siemens.com	Yes	Yes

Add Delete

Change user

Name

Description

Phone number

Allow receipt of SMS messages

Phone number of this user can be changed using SMS

E-mail address

Change login data

Login

Password

Figura 5-6 Users / groups – ficha "Users": configurar usuarios

User 1

- User 1 es el instalador que tiene el nombre de usuario "SK".
- User 1 tiene autorización para recibir SMS del CMR con su número de teléfono 0721-12345678-1.
- El número de teléfono de User 1 puede modificarse mediante el comando de SMS "CHANGEUSER": p. ej., en caso de suplencia por vacaciones por un compañero con otro número de teléfono.

User 2

- User 2 es el encargado que tiene el nombre de usuario "JS".
- User 2 tiene autorización para recibir SMS del CMR con su número de teléfono 0721-12345678-2.
- El número de teléfono de User 2 también puede modificarse mediante el comando de SMS "CHANGEUSER":

User Recipient groups

NOTE:
Maximum number of users: 20.

	Name	Description	Login	Phone number	E-mail address	Allow receipt of SMS messages	Phone number of this user
1	User 2		JS	0721-12345678-2	user2@siemens.com	Yes	Yes
2	User 0		admin	0721-12345678-0	user0@siemens.com	Yes	Yes
3	User 1		SK	0721-12345678-1	user1@siemens.com	Yes	Yes

Add Delete

Change user

Name

Description

Phone number

Allow receipt of SMS messages

Phone number of this user can be changed using SMS

E-mail address

Change login data

Login

Password

Figura 5-7 Users / groups: ficha "Users": configurar usuarios

4. Asigne los dos trabajadores al grupo destinatario "Maintenance". El grupo forma parte de la unidad organizativa "Service" (parámetro "Description"):

User	Recipient groups																
NOTE: Maximum number of recipient groups: 10. Maximum number of users per recipient group: 10.																	
	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr style="background-color: #cccccc;"> <th style="width: 5%;">#</th> <th style="width: 45%;">Name</th> <th style="width: 20%;">Group type</th> <th style="width: 30%;">Description</th> </tr> </thead> <tbody> <tr style="background-color: #e6f2ff;"> <td>1</td> <td>Maintenance</td> <td>SMS</td> <td>Service</td> </tr> <tr> <td>2</td> <td>IT support</td> <td>E-mail</td> <td>IT</td> </tr> <tr> <td>3</td> <td>All (SMS)</td> <td>SMS</td> <td></td> </tr> </tbody> </table>	#	Name	Group type	Description	1	Maintenance	SMS	Service	2	IT support	E-mail	IT	3	All (SMS)	SMS	
#	Name	Group type	Description														
1	Maintenance	SMS	Service														
2	IT support	E-mail	IT														
3	All (SMS)	SMS															
<div style="display: flex; justify-content: space-around; margin-top: 10px;"> Add Delete </div>																	
Change group																	
Name <input style="width: 150px;" type="text" value="Maintenance"/> Description <input style="width: 150px;" type="text" value="Service"/> Group type <input style="width: 100px;" type="text" value="SMS"/> <input style="width: 20px; height: 20px; border: 1px solid gray;" type="button" value="v"/>																	
<input checked="" type="checkbox"/> User 2 (0721-12345678-2 / user2@siemens.com) <input type="checkbox"/> User 0 (0721-12345678-0 / user0@siemens.com) <input checked="" type="checkbox"/> User 1 (0721-12345678-1 / user1@siemens.com)																	

Figura 5-8 Users / groups: ficha "Recipient groups": asignar un grupo de destinatarios

- 5. En la ficha "Message texts", introduzca el texto "Overflow 1" para el texto "Alarm1" en el campo de entrada "Content":

Overview | LOGO! BM | Values | **Message texts** | Signal definitions | Events | Actions | Assignments

NOTE:
Maximum number of message texts: 20.

	Name	Content
1	Alarm1	Overflow 1

Add Delete

Change text

Name Alarm1

Content
Overflow 1

Number of characters 10

Apply

NOTE:
SMS message texts including up to 16 placeholders for process and system variables with formatting instructions.

Figura 5-9 Monitoring: ficha "Message texts": configurar el texto del SMS de alarma

6. Cree la señal asignando la entrada digital 1 del BM al nombre de señal "LOGO_DI1" como origen de la señal:

Overview	LOGO! BM	Values	Message texts	Signal definitions	Events	Actions	Assignments
NOTE: Maximum number of signal definitions: 32.							
	Name		Signal definition				
1	LOGO_DI1		LOGO! BM / 1 - digital input / 1				

Change signal definition

Name

Signal source ▼

Signal type ▼

Number ▼

Figura 5-10 Monitoring – ficha "Signals": crear una señal

7. Cree el evento que debe vincularse a la señal:

Overview | LOGO! BM | Values | Message texts | Signal definitions | **Events** | Actions | Assignments

NOTE:
Maximum number of events: 32.

	Name	Event definition
1	LOGO! event1	LOGO_DI1 Changes to 1

Add Delete

Change event

Name LOGO! event1

Signal name LOGO_DI1 ▼

Event Changes to 1 ▼

Figura 5-11 Monitoring: ficha "Events": crear un evento

- Configure una acción que deba ejecutarse cuando se produzca el evento creado arriba. La acción debe ser enviar un SMS de alarma:

Overview	LOGO! BM	Values	Message texts	Signal definitions	Events	Actions	Assignments
NOTE: Maximum number of transmission actions: 32.							
	Name	Action definition					
1	Service SMS 1	Send SMS message / Maintenance / Alarm1					

Change action

Name	Service SMS 1
Destination	Send SMS message <input type="button" value="v"/>
Recipient group	Maintenance <input type="button" value="v"/>
Message text	Alarm1 <input type="button" value="v"/>

Figura 5-12 Monitoring: ficha "Actions": configurar una acción

- Finalmente, vincule el evento a la acción prevista:

Overview LOGO! BM Values Message texts Signal definitions Events Actions **Assignments**

NOTE:
Maximum number of assignments: 32.

	Active	Name	Event	Action
1	Yes	Alarm1 - Service SMS	LOGO! event1	Service SMS 1

Add Delete

Change assignment

Name: Alarm1 - Service SMS

Activate assignment

If:

Event: LOGO! event1

Signal name: LOGO_DI1

Signal definition: LOGO! BM / I - digital input / 1

Event definition: LOGO_DI1 Changes to 1

Then:

Action: Service SMS 1

Action definition: Send SMS message / Maintenance / Alarm1

Figura 5-13 Monitoring: ficha "Assignments": definir una asignación

Resultado

El resultado de la vigilancia es el siguiente:

Si el encóder de valor límite del medidor de nivel pone a 1 la entrada digital "I1" del LOGO! BM, el CMR envía un SMS con el texto "Overflow 1" a los dos trabajadores de mantenimiento "User 1" y "User 2".

Diagnóstico y mantenimiento

6.1 Posibilidades de diagnóstico

Están disponibles las siguientes posibilidades de diagnóstico.

LEDs del módulo

Encontrará información sobre los indicadores LED en el capítulo LED para la indicación del funcionamiento (Página 32).

Encontrará imágenes de errores concretas en el capítulo Fallos y causas posibles (Página 145).

Web Based Management (WBM)

Para ello es necesario conectar el PC al CMR localmente o a través de la red de telefonía móvil.

En el área del WBM "Diagnóstico" encontrará los avisos de diagnóstico y las posibilidades de ajuste para enviar mensajes cuando se produzcan errores (véase más abajo).

Encontrará información sobre el estado del CMR en las páginas siguientes del WBM:

- Encontrará información general sobre el estado del CMR en la página inicial del WBM.
- Encontrará los avisos de diagnóstico en la página de diagnóstico del WBM, consulte el capítulo Diagnostics buffer (Página 81).

Avisos de diagnóstico en el búfer de diagnóstico

Cuando se producen algunos eventos importantes, el CMR escribe avisos de diagnóstico en el búfer de diagnóstico.

Se documentan, p. ej.:

- Avisos de servicio como arranque o cambio de la configuración
- Establecimiento e interrupción de la conexión con el BM
- Establecimiento e interrupción de la conexión a la red de telefonía móvil
- Establecimiento e interrupción de la conexión móvil de datos
- Advertencias a la hora de leer la configuración de la tarjeta SD o del PC
- Sincronización horaria

Los avisos de diagnóstico se clasifican en 4 categorías, consulte el capítulo Diagnostics buffer (Página 81).

Es posible leer o transferir los avisos de diagnóstico mediante los mecanismos siguientes:

- Lectura del búfer de diagnóstico a través del WBM
- Transferencia mediante SMS o correo electrónico de avisos de diagnóstico referidos a errores

Los errores pueden enviarse como mensajes (SMS o correo electrónico). Encontrará la descripción en el capítulo Notifications (Página 82).

SMS de diagnóstico

Además de poder configurar la transferencia del búfer de diagnóstico, el CMR puede enviar SMS de diagnóstico estándar cuando se solicite. El CMR envía un SMS de diagnóstico a un teléfono con un número autorizado cuando recibe de dicho teléfono un SMS con el texto siguiente:

DIAG?

Encontrará el contenido del SMS de diagnóstico del CMR en el capítulo SMS de diagnóstico (Página 142).

6.2 SMS de diagnóstico

Comando SMS "DIAG?"

El SMS de respuesta a una solicitud de diagnóstico (comando SMS "DIAG?") proporciona información con la siguiente estructura:

Información	Contenido del SMS
Nombre del módulo del CMR	Nombre From: DEVICE-
Fecha y hora del módulo	<YYYY-MM-DD> <hh:mm:ss>
Tipo y versión de firmware	<Nombre del CMR> <Versión de firmware>
Estado de la red de telefonía móvil	<ul style="list-style-type: none"> • not registered (no registrado en la red / no conectado) • registered (registrado en la red / conectado) • not configured (no configurado) • searching network (búsqueda de red) • denied (registro rechazado) • unknown (desconocido) • roaming (buscando) • invalid (datos de acceso no válidos)
Conectado desde (solo con registered / roaming)	Attached for (ddd:hh:mm:ss) <ddd>:<hh>:<mm>:<ss>
Estado del servicio de datos	Encontrará las entradas posibles en "Estado de la red de telefonía móvil" más arriba.
Tiempo de conexión	Attached for (ddd:hh:mm:ss) <ddd>:<hh>:<mm>:<ss>
Nombre de la red / del operador	Network: <nombre de la red>

Información	Contenido del SMS
Dirección IP	IP: xxx.xxx.xxx.xxx Si no existe dirección IP: IP: -
Intensidad de señal	Signal Quality: <ul style="list-style-type: none">• invalid• good• medium• weak• no signal
Intensidad de campo de señales (CSQ/dBm)	(CSQ:xx / -xxdBm) Encontrará el significado de los valores en el capítulo WAN (Página 92).

Comando SMS "DIAG? Response"

Si no es posible enviar la información con un SMS, sigue un segundo SMS que empieza por "DIAG? Response".

Un SMS de respuesta de este tipo puede tener el siguiente aspecto:

Ejemplo de dos SMS de respuesta:

1.er SMS

- From: logo.cmr
- 2016-10-05 14:14:45
- LOGO! CMR2020 V2
- GSM: registered
- Attached for (ddd:hh:mm:ss): 000:00:03:36

2.º SMS

- DIAG? Response
- GPRS: registered
- Attached for (ddd:hh:mm:ss): 000:00:03:36
- Network: <operador>.com
- IP: 77.25.26.11
- Signal Quality: good (CSQ:29/-55dBm)

6.3 Detección de errores de e-mails

Indicaciones relativas a e-mails en las entradas del búfer de diagnóstico

En caso de errores en la transmisión de e-mails se genera una entrada en el búfer de diagnóstico.

La entrada en el búfer de diagnóstico puede contener los siguientes datos:

- Código de error interno; los códigos de error correspondientes se explican en la página siguiente: Enlace: (<https://curl.haxx.se/libcurl/c/libcurl-errors.html>)
- Última respuesta del servidor
- número de intentos

Última respuesta del servidor

Los códigos de error de los servidores de correo electrónico significan lo siguiente:

Tabla 6- 1 SMTP (correo electrónico)

Código	Significado
421	Servicio no disponible. Deshaciendo la conexión. (con frecuencia insuficiencia de recursos del operador del servicio)
450	Acción no ejecutada: bandeja de entrada no disponible / no accesible. Vuélvalo a intentar más adelante.
451	Acción interrumpida - Error en la ejecución.
452	Acción interrumpida - No hay suficiente memoria en el sistema.
500	Error de sintaxis: comando desconocido.
501	Error de sintaxis Compruebe los datos de configuración.
502	Comando no implementado
503	Secuencia de comandos incorrecta
504	Parámetro desconocido o no implementado
521	El dominio no acepta el correo electrónico.
530	Acceso denegado Para el acceso vía STARTTLS es necesario el cifrado.
535	Autenticación SMTP incompleta Compruebe en la configuración "Servicios > Correo electrónico": <ul style="list-style-type: none"> • "Nombre de usuario" y "Contraseña" • Seguridad de la conexión
550	Error de sintaxis - Dirección de correo electrónico del destinatario o dominio desconocidos. Compruebe en la configuración "Usuarios / Grupos > Grupos": <ul style="list-style-type: none"> • Dirección de correo electrónico del destinatario
551	Bandeja de entrada no local Intente una transmisión.
552	Acción interrumpida - Error en la asignación de memoria. No ha sido posible transferir el correo electrónico porque el tamaño del correo electrónico es mayor que el máximo ajustado por el administrador.
553	Acción no ejecutada - Nombre de bandeja de entrada no permitido (sintaxis incorrecta). Consulte error 535.

Código	Significado
554	Ha fallado la transferencia - No hay servicio SMTP disponible.
5xx	Otro mensaje de error del servidor de correo electrónico El estado se corresponde con el número de error de tres cifras del protocolo SMTP.

6.4 Fallos y causas posibles

Fallo	Significado	Solución
LED de error encendido en rojo	<ul style="list-style-type: none"> No hay conexión con el BM PIN incorrecto No hay tarjeta SIM con la interfaz de telefonía móvil activada <p>Infórmese sobre otras causas de fallo posibles a través de los eventos documentados en el búfer de diagnóstico.</p>	<ul style="list-style-type: none"> Comprobar la conexión/realizar un test de PING Desbloquear la tarjeta SIM Insertar la tarjeta SIM
LED de error intermitente en rojo	<ul style="list-style-type: none"> Dirección IP duplicada 	<ul style="list-style-type: none"> Corregir la dirección IP
Ninguna indicación LED	<ul style="list-style-type: none"> Alimentación demasiado débil El CMR se encuentra apagado 	<ul style="list-style-type: none"> Corregir la alimentación de acuerdo con los Datos técnicos (Página 153)
No es posible la localización	<ul style="list-style-type: none"> Mala recepción GPS Antena no insertada o no colocada correctamente 	<ul style="list-style-type: none"> Por lo general, la recepción GPS solo es posible al aire libre, no en recintos cerrados. Comprobar la conexión
Sincronización horaria mediante NTP inexistente o defectuosa	<ul style="list-style-type: none"> Mala cobertura de telefonía móvil Configuración incorrecta en el WBM Interfaz de telefonía móvil desactivada Nombre del servidor NTP o dirección IP erróneos 	<ul style="list-style-type: none"> Corregir la orientación de la antena Activar la interfaz de telefonía móvil en el WBM Comprobar la configuración de la conexión de datos móviles en el WBM
No se reciben SMS	<ul style="list-style-type: none"> Recepción de SMS desactivada Mala cobertura de telefonía móvil Usuario no registrado o no autorizado 	<ul style="list-style-type: none"> Activar la recepción de SMS en el WBM Comprobar los derechos del usuario en el WBM y corregirlos si es necesario Comprobar la posición de la antena de telefonía móvil
Sin conexión a la red de telefonía móvil	<ul style="list-style-type: none"> Introducción de un PIN erróneo por tercera vez Interfaz de telefonía móvil desactivada en el WBM 	<ul style="list-style-type: none"> Consulte el capítulo Insertar la tarjeta SIM e introducir el PIN (Página 48), desbloquear la tarjeta SIM Activar la interfaz de telefonía móvil en el WBM

Fallo	Significado	Solución
Monitoring no funciona	<ul style="list-style-type: none"> No se reciben los mensajes SMS esperados configurados en el WBM 	Comprobar en el WBM: <ul style="list-style-type: none"> ¿Están activas las asignaciones (Assignments)? ¿Están conectadas correctamente las entradas/salidas? Solo si se vigilan objetos del BM: <ul style="list-style-type: none"> ¿Está conectado el BM?
Se ha recibido un SMS que contiene un comodín entre 2 signos de exclamación	<ul style="list-style-type: none"> Un nombre de señal indicado en el WBM no existe o se ha escrito incorrectamente. El nombre de señal erróneo o inexistente se representa en los textos de mensajes del siguiente modo: [CMR_I1] se convierte en !CMR_I1! 	<ul style="list-style-type: none"> Corregir el comodín en el WBM

6.5 Cargar firmware

Versiones de firmware nuevas

Cuando haya una nueva versión de firmware para el módulo, esta aparecerá en las páginas web de Siemens Industry Online Support, en:

Enlace: (<https://support.industry.siemens.com/cs/ww/es/ps/15383/dl>)

Guarde el archivo de firmware en el PC de configuración.

Carga de archivos de firmware nuevos

Un archivo de firmware nuevo se carga desde el PC de configuración en el CMR a través del WBM.

Encontrará la descripción del modo de establecer la conexión del PC de configuración al CMR en el capítulo Establecer la conexión con el CMR (Página 68).

Encontrará la descripción de cómo cargar un archivo de firmware en el CMR a través del WBM en el capítulo Firmware (Página 85).

6.6 Restablecer la configuración de fábrica

Restablecer la configuración de fábrica: Repercusión

Nota**Se borran los datos del CMR**

Con las funciones aquí descritas para restablecer la configuración de fábrica se borran todos los datos de configuración del CMR.

Nota**Ya no se puede acceder al CMR a través de VPN**

Al restablecer la configuración de fábrica se borra la configuración VPN, y ya no se puede acceder al CMR a través de OpenVPN.

- **Datos borrados**

Al restablecer la configuración de fábrica se borran los datos siguientes:

- Una dirección IP configurada por el usuario para la interfaz LAN

Se restablece la dirección IP predeterminada de fábrica: 192.168.0.3.

- Todos los restantes datos de configuración de la memoria del CMR
- Datos de configuración de una tarjeta SD que esté insertada Se borran los archivos "default.cfg" y "user.cfg" de la tarjeta SD.

- **Datos no borrados**

Al restablecer la configuración de fábrica no se borran los datos siguientes:

- Dirección MAC de la interfaz LAN

Ejecutar la función "Reset to factory settings"

Para restablecer la configuración de fábrica hay disponibles dos procedimientos:

- **Restablecer desde el WBM**

Encontrará la descripción de este procedimiento en el capítulo Operating status (Página 86).

- **Restablecer mediante el pulsador "SET"**

Consulte el número de veces y el tiempo que hay que accionar el pulsador en el capítulo El pulsador "SET" (Página 35).

Sobre la respuesta de los LEDs mientras se restablece la configuración de fábrica, consulte el capítulo LED para la indicación del funcionamiento (Página 32).

Respuesta tras restablecer la configuración de fábrica

Tras el restablecimiento, la RTU arranca automáticamente. El resto de reacciones depende de si se utiliza o no una tarjeta SD opcional:

- **Arranque sin tarjeta SD**

- Si no se utiliza una tarjeta SD, el CMR permanece sin datos de configuración.
- Se puede acceder localmente al CMR mediante la siguiente dirección IP predeterminada de fábrica 192.168.0.3.
- El CMR arranca sin datos de configuración.

En general se aplican los ajustes predeterminados en la primera puesta en marcha, consulte el capítulo Establecer la conexión de configuración (Página 69).

- **Arranque con tarjeta SD**

Si hay una tarjeta SD insertada, el CMR busca en ella el archivo de configuración "default.cfg", que se había borrado durante el restablecimiento de la configuración de fábrica.

No se utiliza ningún archivo de configuración "user.cfg" guardado por el cliente en la tarjeta SD.

Si se desconecta el CMR tras restablecer la configuración de fábrica y, con la tarjeta SD insertada, se arranca con un archivo de configuración "default.cfg", el CMR utilizará el archivo de configuración "default.cfg". Consulte también el capítulo Configuration (Página 83).

6.7 Sustitución del CMR

Cambio del CMR

Para sustituir el CMR en caso de repuesto puede utilizarse también la tarjeta SD para transferir al nuevo dispositivo los datos de configuración del CMR antiguo guardados en la tarjeta. En la tarjeta SD que esté insertada se guardan todos los cambios de los datos de configuración.

 ADVERTENCIA
--

Consulte las consignas de seguridad
--

Antes de cambiar el CMR lea las consignas de seguridad del capítulo Indicaciones importantes sobre el uso del dispositivo (Página 39).
--

Asegúrese de que está desconectada la alimentación de tensión mientras se realizan los trabajos.
--

Para sustituir el CMR proceda como se describe en el capítulo Montar el dispositivo (Página 42).

Recuerde que al sustituir el CMR deberá transferir la tarjeta SIM del dispositivo antiguo al nuevo.

Transferencia de los datos de configuración al nuevo CMR

El procedimiento para transferir los datos de configuración al CMR depende de si en el CMR se utiliza o no una tarjeta SD:

- **Sustitución de dispositivo sin tarjeta SD**

Si no se utiliza una tarjeta SD, antes de sustituir el dispositivo deben transferirse los datos de configuración del PC de configuración al nuevo CMR.

Al crear los datos de configuración desde el WBM del CMR es posible guardar los datos de configuración en el PC de configuración.

- **Sustitución de dispositivo con tarjeta SD**

Si en el CMR antiguo se ha utilizado una tarjeta SD, después de desconectar la alimentación de tensión debe extraerse la tarjeta del CMR antiguo e insertarse en el CMR nuevo antes de realizar la conexión y el montaje.

Al rearrancar, el CMR lee los datos de configuración de la tarjeta SD.

Encontrará información sobre cómo guardar, cargar y editar archivos de configuración en el capítulo Configuration (Página 83).

Croquis acotados

7

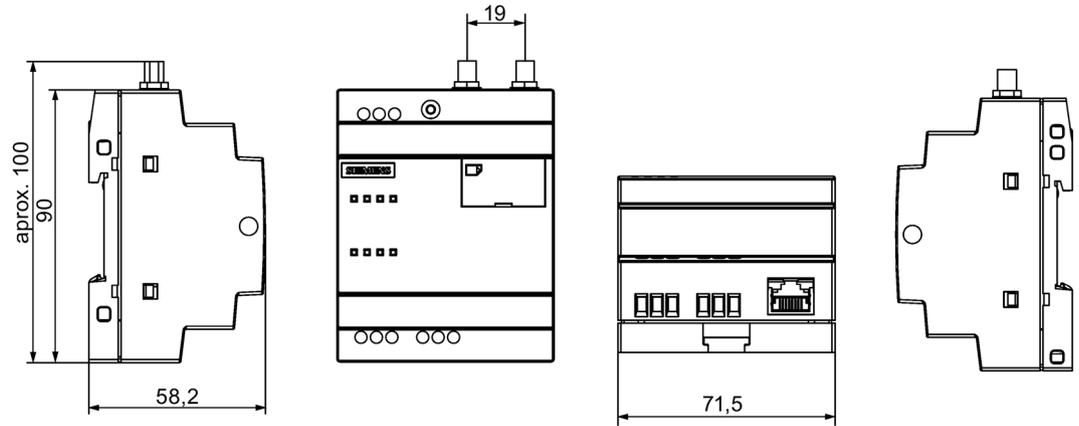


Figura 7-1 Todas las dimensiones en mm

Datos técnicos

Datos técnicos - LOGO! CMR2020 / LOGO! CMR2040

Referencias

LOGO! CMR2020 6GK7 142-7BX00-0AX0

LOGO! CMR2040 6GK7 142-7EX00-0AX0

Conexión a Industrial Ethernet

Interfaz X1P1 para aplicaciones locales

- | | |
|----------------------------|--|
| • Número | • 1 |
| • Ejecución | • Conector hembra RJ45 |
| • Propiedades | • 10/100-Base-T, Ethernet IEEE 802, Autocrossover, Autonegotiation |
| • Velocidad de transmisión | • 10/100 Mbits/s |
-

Longitudes de línea admisibles (Ethernet)

(Combinaciones alternativas por rango de longitud) *

- | | |
|-------------|--|
| 0 ... 55 m | <ul style="list-style-type: none"> • Máx. 55 m IE TP Torsion Cable con IE FC RJ45 Plug 180 • Máx. 45 m IE TP Torsion Cable con IE FC RJ45 + 10 m TP Cord mediante IE FC RJ45 Outlet |
| 0 ... 85 m | <ul style="list-style-type: none"> • Máx. 85 m IE FC TP Marine/Trailing/Flexible/FRNC/Festoon/Food Cable con IE FC RJ45 Plug 180 • Máx. 75 m IE FC TP Marine/Trailing/Flexible/FRNC/Festoon/Food Cable + 10 m TP Cord mediante IE FC RJ45 Outlet |
| 0 ... 100 m | <ul style="list-style-type: none"> • Máx. 100 m IE FC TP Standard Cable con IE FC RJ45 Plug 180 • Máx. 90 m IE FC TP Standard Cable + 10 m TP Cord mediante IE FC RJ45 Outlet |
-

Datos eléctricos

Alimentación

- | | |
|----------------|---|
| • Alimentación | • 12 ... 24 V DC nominal |
| • Tolerancia | • -15 ... +20 % |
| • Ejecución | • Regleta de bornes de 3 polos, sin aislamiento galvánico |
-

Consumo de corriente

- | | |
|----------------------|---|
| • A 12 V | • Máx. 850 mA (incluidos 2 x 300 mA para salidas digitales) |
| • A 24 V | • Máx. 725 mA (incluidos 2 x 300 mA para salidas digitales) |
| • I _{Burst} | • 1050 mA (incluidos 2 x 300 mA para salidas digitales) |
-

Potencia activa disipada

Máximo 3 W

Datos técnicos - LOGO! CMR2020 / LOGO! CMR2040

Entradas digitales (I1, I2)

- Número
 - Ejecución
 - Rango de tensión admisible
 - Tensión en estado ON
 - Tensión en estado OFF
 - Consumo de corriente
- 2
 - Bloque de bornes de 3 polos, sin aislamiento galvánico
 - 12 ... 24 V (nominal)
 - > 8,5 V
 - < 5 V
 - I = 5,5 mA (máximo)
-

Salidas digitales (Q1, Q2)

- Número
 - Ejecución
 - Tensión de salida
 - Capacidad de carga
- 2
 - Bloque de bornes de 3 polos, transistor, sin aislamiento galvánico
 - Tensión de alimentación
 - Máx. 0,3 A
-

Interfaz de telefonía móvil (XR02)

Conexión de antena

- Número
 - Ejecución
 - Impedancia nominal
- 1
 - Conector SMA
 - 50 Ω
-

Bandas de frecuencia

- LOGO! CMR2020
 - LOGO! CMR2040
- GSM
GSM 850 MHz, EGSM 900 MHz, DCS 1800 MHz, PCS 1900 MHz
 - GSM
EGSM 900 MHz, DCS 1800 MHz
 - UMTS
Banda I (2100 MHz), banda V (850 MHz), banda VIII (900 MHz)
 - LTE
Banda III (1800 MHz), banda VII (2600 MHz), banda XX (800 MHz)
-

Propiedades y velocidad de transferencia (máxima)

- LOGO! CMR2020
- GPRS
 - Clase multislots 10
 - Clase de terminal B
 - Esquema de codificación: 1 ... 4
 - Downlink: 80 kbits/s
 - Uplink: 40 kbits/s
-

Datos técnicos - LOGO! CMR2020 / LOGO! CMR2040

- LOGO! CMR2040
 - LTE
 - Downlink: 100 Mbits/s
 - Uplink: 50 Mbits/s
 - HSPA+
 - Downlink: 42 Mbits/s
 - Uplink: 5,76 Mbits/s
 - EDGE
 - Clase multislot 33
 - Clase de terminal B
 - Esquema de codificación: 1 ... 9
 - Downlink: 296 kbits/s
 - Uplink: 236,8 kbits/s

Interfaz GPS (XR01)

- Número
 - 1
 - Ejecución
 - Conector SMA
 - Impedancia nominal
 - 50 Ω
-
- Alimentación
- 3,8 V (nominal)
 - A 5 mA: 3,575 V
 - A 10 mA: 3,35 V
 - A 15 mA: 3,125 V
-
- Consumo de corriente
- Máx. 15 mA
-
- Ejecución
- Estándar GPS de 32 canales
-
- Bandas de frecuencia
- L1 (GPS)
 - L1, FDMA (Glonass)

Condiciones ambientales admisibles

- Temperatura ambiente
- Durante el funcionamiento
 - -20 °C ... +70 °C
 - Durante el almacenamiento
 - -40 °C ... +85 °C
-
- Humedad relativa del aire a 25 °C
- 0 ... 95%, sin condensación

Forma, medidas y peso

- Forma
- Diseño compacto, para montaje en perfil DIN simétrico
-
- Grado de protección
- IP20
-
- Peso
- 160 g
-
- Dimensiones (an x al x p)
- 71,5 x 90 x 58,2 mm (sin conectores hembra de antena)
-
- Material
- Plástico

* Consulte los detalles en el catálogo IK PI, sistema de cableado.

Encontrará más funciones y datos característicos en el capítulo Aplicación y funciones (Página 13).

Homologaciones

Homologaciones concedidas

Nota

Homologaciones otorgadas en la placa de características del dispositivo

Las homologaciones indicadas solo se consideran otorgadas si el producto está provisto de la correspondiente identificación. Las identificaciones de la placa de modelo indican cuál de las siguientes homologaciones se ha otorgado para su producto.

Declaración de conformidad UE



El producto cumple los requisitos y los objetivos en materia de seguridad de las directivas de la UE siguientes y, además, cumple las normas europeas armonizadas (EN) de autómatas programables que se mencionan en los documentos oficiales de la UE.

- **2014/34/UE (directiva de protección frente a explosiones ATEX)**

Directiva del Parlamento Europeo y del Consejo, de 26 de febrero de 2014, relativa a la aproximación de las legislaciones de los Estados miembros sobre los aparatos y sistemas de protección para uso en atmósferas potencialmente explosivas; boletín oficial de la UE L96, 29/03/2014, pág. 309-356

- **2014/53/UE (directiva de equipos radioeléctricos)**

Directiva del Parlamento Europeo y del Consejo, de 16 de abril de 2014, relativa a la armonización de las legislaciones de los Estados miembros sobre la comercialización de equipos radioeléctricos, y por la que se deroga la Directiva 1999/5/CE

- **2011/65/UE (directiva RoHS)**

Directiva del Parlamento Europeo y del Consejo, de 8 de junio de 2011, sobre restricciones a la utilización de determinadas sustancias peligrosas en aparatos eléctricos y electrónicos

La declaración de conformidad UE se encuentra a disposición de todas las autoridades competentes en:

Siemens Aktiengesellschaft
Process Industries and Drives
Process Automation
DE-76181 Karlsruhe
Alemania

Encontrará la declaración de conformidad UE correspondiente a estos productos en la dirección de Internet:

Enlace: (<https://support.industry.siemens.com/cs/ww/es/ps/15383>)

> Tipo de certificado: "Declaración de conformidad CE"

A continuación se enumeran las normas armonizadas que son relevantes para el producto de acuerdo con las directivas citadas anteriormente.

Norma	LOGO! CMR2020	LOGO! CMR2040
EN 60079-0	x	x
EN 60079-15	x	x
EN 50581	x	x
EN 60950-1	x	x
EN 62311	x	x
EN 301 489-1	x	x
EN 301 489-3	x	x
EN 301 489-7	x	x
EN 301 489-24	-	x
EN 61000-6-1	x	x
EN 61000-6-2	x	x
EN 61000-6-3	x	x
EN 61000-6-4	x	x
EN 300 440-2	x	x
EN 301 511	x	x
EN 301 908-1	-	x
EN 301 908-2	-	x
EN 301 908-13	-	x

Las redacciones actualizadas de las normas pueden consultarse en la versión actualmente vigente de la declaración de conformidad UE.

IECEX

El producto cumple los requisitos de protección contra explosión según IECEX.

Clasificación IECEx:

- Ex nA IIC T4 Gc

Certificado: IECEx DEK 14.0025X

Normas aplicadas:

- EN 60079-0 - Áreas potencialmente explosivas - Parte 0: Recursos - Requisitos generales
- EN 60079-15 - Áreas potencialmente explosivas - Parte 15: Protección del dispositivo por modo de protección 'n'

- Ex ec IIC T4 Gc

Certificado: IECEx DEK 18.0018X

Normas aplicadas:

- EN 60079-0 - Áreas potencialmente explosivas - Parte 0: Recursos - Requisitos generales
- EN 60079-7 - Áreas potencialmente explosivas - Parte 7: Protección del dispositivo por seguridad aumentada "e"

Las versiones actuales de las normas pueden consultarse en el certificado IECEx, que encontrará en Internet en la dirección siguiente:

Enlace: (<https://support.industry.siemens.com/cs/es/es/ps/15383/cert>)

Deben cumplirse las siguientes condiciones para el uso seguro del producto conforme al capítulo Notas sobre el uso en áreas Ex según ATEX / IECEx (Página 41).

Tenga también en cuenta las indicaciones del documento "Use of subassemblies/modules in a Zone 2 Hazardous Area", que encontrará en Internet en la dirección siguiente:

Enlace: (<https://support.industry.siemens.com/cs/ww/es/view/78381013>)

ATEX



El producto cumple los requisitos de la Directiva Comunitaria 2014/34/UE "Aparatos y sistemas de protección para uso en atmósferas potencialmente explosivas".

Homologación ATEX:

- II 3 G Ex nA IIC T4 Gc

Type Examination Certificate: KEMA 07 ATEX 0145X

Normas aplicadas:

- EN 60079-0 - Áreas potencialmente explosivas - Parte 0: Recursos - Requisitos generales
- EN 60079-15 - Áreas potencialmente explosivas - Parte 15: Protección del dispositivo por modo de protección 'n'

- II 3 G Ex ec IIC T4 Gc

Type Examination Certificate: DEKRA 18 ATEX 0026X

Normas aplicadas:

- EN 60079-0 - Áreas potencialmente explosivas - Parte 0: Recursos - Requisitos generales
- EN 60079-7 - Áreas potencialmente explosivas - Parte 7: Protección del dispositivo por seguridad aumentada "e"

Las redacciones actualizadas de las normas pueden consultarse en la declaración de conformidad UE, véase más arriba.

Deben cumplirse las siguientes condiciones para el uso seguro del producto conforme al capítulo Notas sobre el uso en áreas Ex según ATEX / IECEx (Página 41).

Tenga también en cuenta las indicaciones del documento "Use of subassemblies/modules in a Zone 2 Hazardous Area", que encontrará en:

- En SIMATIC NET Manual Collection en "Todos los documentos" > "Use of subassemblies/modules in a Zone 2 Hazardous Area"
- La siguiente dirección de Internet:
Enlace: (<https://support.industry.siemens.com/cs/ww/es/view/78381013>)

Directiva de equipos radioeléctricos

El CM cumple los requisitos de la Directiva Comunitaria 2014/53/UE (equipos radioeléctricos) conforme a los requisitos de los arts. 3 (1) a, 3 (1) b y 3 (2).

Art. 3 (1) a - Salud y seguridad

Normas armonizadas:

- EN 60950-1+A1+A2+A11+A12

Equipos de tecnología de la información - Seguridad - Parte 1: Requisitos generales

- EN 62311

Evaluación de los equipos eléctricos y electrónicos respecto de las restricciones relativas a la exposición de las personas a los campos electromagnéticos (0 Hz ... 300 GHz)

Art. 3 (1) b - CEM

Normas armonizadas:

- ETSI EN 301 489-1
Compatibilidad electromagnética y espectro de radiofrecuencia (ERM) - Norma de compatibilidad electromagnética para equipos y servicios de radiocomunicaciones - Parte 1: Requisitos técnicos comunes
- ETSI EN 301 489-3
Compatibilidad electromagnética y espectro de radiofrecuencia (ERM) - Norma de compatibilidad electromagnética (CEM) para equipos y servicios de radiocomunicaciones - Parte 3: Condiciones específicas para los dispositivos de corto alcance (SRD) para el uso en frecuencias entre 9 kHz y 246 GHz
- ETSI EN 301 489-7
Compatibilidad electromagnética y espectro de radiofrecuencia (ERM) - Norma de compatibilidad electromagnética para equipos y servicios de radiocomunicaciones - Parte 7: Condiciones específicas para los equipos de radiocomunicaciones móvil y portátil y los equipos auxiliares de sistemas de telecomunicaciones radio celulares digitales (GSM y DCS)
- ETSI EN 301 489-24
Compatibilidad electromagnética y espectro de radiofrecuencia (ERM) - Norma de compatibilidad electromagnética para equipos y servicios de radiocomunicaciones - Parte 24: Condiciones específicas para IMT-2000 CDMA emisión directa (UTRA) para equipos radio móviles y portátiles (UE) y equipos auxiliares
- EN 61000-6-1
Compatibilidad electromagnética (CEM) - Parte 6-1: Normas genéricas - Inmunidad en entornos residenciales, industriales y de industria ligera
- EN 61000-6-2+AC
Compatibilidad electromagnética (CEM) - Parte 6-2: Normas genéricas - Inmunidad en entornos industriales
- EN 61000-6-3+A1+AC
Compatibilidad electromagnética (CEM) - Parte 6-3: Normas genéricas - Norma de emisión en entornos residenciales, comerciales y de industria ligera
- EN 61000-6-4+A1
Compatibilidad electromagnética (CEM) - Parte 6-4: Normas genéricas - Norma de emisión en entornos industriales

Art. 3 (2) - Medidas para el uso eficiente del espectro de frecuencias

Normas armonizadas:

- ETSI EN 300 440-2
Compatibilidad electromagnética y espectro de radiofrecuencia (ERM) - Equipos radioeléctricos de corto alcance - Dispositivos para el uso en el rango de frecuencia entre 1 GHz y 40 GHz. Parte 2: Norma armonizada que incluye los requisitos esenciales conforme al artículo 3.2 de la directiva R&TTE.
- ETSI EN 301 511
Sistema global de comunicación móvil (GSM). Norma armonizada para teléfonos móviles en la banda de GSM 900 y GSM 1800 que incluye los requisitos esenciales conforme al artículo 3.2 de la directiva R&TTE.
- ETSI EN 301 908-1
Redes celulares IMT - norma armonizada que incluye los requisitos esenciales conforme al artículo 3.2 de la directiva R&TTE. Parte 1: Introducción y requisitos comunes
- ETSI EN 301 908-2
Redes celulares IMT. Norma armonizada que incluye los requisitos esenciales conforme al artículo 3.2 de la directiva R&TTE. Parte 2: Equipo de usuario (UE) para CDMA con espectro ensanchado de secuencia directa (UTRA FDD).
- ETSI EN 301 908-13
IMT cellular networks. Harmonized standard covering the essential requirements of article 3.2 of the R&TTE directive. Part 13: Evolved Universal Terrestrial Radio Access (E-UTRA) User Equipment (UE)

Ganancia máxima de la antena

Los usuarios e instaladores deben tener acceso a las indicaciones de instalación que deben observarse para antenas y a las condiciones para el funcionamiento de la instalación emisora con el fin de cumplir con la exposición HF admisible.

Tenga en cuenta al respecto los datos técnicos de la antena, consulte el anexo Antenas (Página 165).

Directiva RoHS

El producto cumple los requisitos de la directiva europea 2011/65/CE sobre restricciones a la utilización de determinadas sustancias peligrosas en aparatos eléctricos y electrónicos.

Norma aplicada:

- EN 50581

cULus



- UL 60950-1 (Information Technology Equipment - Safety - Part 1: General Requirements)
- CSA C22.2 No. 60950-1-07 (Information Technology Equipment - Safety - Part 1: General Requirements)

- UL 61010-1 (Safety Requirements for Electrical Equipment for Measurement, Control, and Laboratory Use - Part 1: General Requirements)
- UL 61010-2-201 (Part 2-201: Particular Requirements for Control Equipment)
- CAN/CSA C22.2 No. 61010-1-12 (Safety Requirements for Electrical Equipment for Measurement, Control, and Laboratory Use - Part 1: General Requirements)
- CAN/CSA-IEC 61010-2-201 (Part 2-201: Particular Requirements for Control Equipment)

cULus HAZ.LOC.



Underwriters Laboratories, Inc., Certificate / Report No. E240480

- ISA 12.12.01 (Nonincendive Electrical Equipment for Use in Class I and II, Division 2 and Class III, Divisions 1 and 2 Hazardous (Classified) Locations)
- CSA C22.2 No. 213 (Hazardous Location)

APPROVED for Use in:

- Cl. 1, Div. 2, GP. A, B, C, D T4; Ta = -20 °C...+70 °C
- Cl. 1, Zone 2, GP. IIC T4; Ta = -20 °C...+70 °C

Certificación FM



Factory Mutual Research (FM):

Norma de certificación clase número 3600 y 3611

Homologado para el uso en:

Class I, Division 2, Group A, B, C, D, Temperature Class T4, Ta = 70 °C

Class I, Zone 2, Group IIC, Temperature Class T4, Ta = 70 °C

Homologaciones radioeléctricas nacionales

Para el uso del aparato en determinados países deben preverse homologaciones radioeléctricas, el marcado acordado debe encontrarse en la placa de características y deben observarse indicaciones especiales para el país en cuestión.

Homologaciones nacionales de telefonía móvil para dispositivos SIMATIC NET

Encontrará una relación de las homologaciones nacionales de telefonía móvil para dispositivos SIMATIC NET aquí:

Enlace: (www.siemens.com/mobilenetwork-approvals)

Puede consultar información complementaria sobre las homologaciones nacionales de telefonía móvil para dispositivos SIMATIC NET en Siemens Industry Online Support:

Enlace: (<http://www.siemens.de/automation/support-request>)

Homologaciones actuales

Los productos SIMATIC NET se entregan periódicamente a autoridades y oficinas de homologación para proceder a su homologación para los mercados y las aplicaciones que correspondan.

Póngase en contacto con su representante de Siemens si necesita una lista de las homologaciones actuales para los diferentes aparatos o infórmese en las páginas de Internet de Siemens Industry Online Support:

Enlace: (<https://support.industry.siemens.com/cs/ww/es/ps/15383/cert>)

Accesorios

A.1 Antenas

Se ofrecen las siguientes antenas de montaje en interior o exterior:

Antenas



Figura A-1 Antena GPRS/LTE, ANT794-4MR, antena de varilla

Referencia	Explicación
6NH9 860-1AA00	Antena omnidireccional para GSM (2G), UMTS (3G) y LTE (4G); omnidireccional, resistente a la intemperie para interior y exterior; cable de conexión de 5 m fijado a la antena; conector SMA; incl. escuadra de montaje, tornillos y tacos.

Si desea información más detallada, consulte el manual del equipo. La encontrará en Internet, en las páginas de Siemens Industry Online Support, en la dirección siguiente:

Enlace: (<https://support.industry.siemens.com/cs/ww/es/view/23119005>)



Figura A-2 Antena LTE, ANT896-4MA, antena de varilla

Referencia	Explicación
6GK5896-4MA00-0AA3	Antena IRC ANT 896-4MA para GSM (2G), UMTS (3G) y LTE (4G); omnidireccional, girable radialmente, con articulación adicional; ganancia de la antena: 2 dBi; incl. conector SMA; IP54, -40 ... +85 °C; para montaje directo con sistema de conexión SMA; volumen de suministro: 1 x ANT896-4MA



Figura A-3 Antena LTE, ANT896-4ME, antena cilíndrica

Referencia	Explicación
6GK5896-4ME00-0AA0	Antena cilíndrica ANT 896-4ME para GSM (2G), UMTS (3G) y LTE (4G); omnidireccional, incl. conector N hembra: 3 dBi; IP66, -40 ... +70 °C; montaje en armario eléctrico; volumen de suministro: 1 x ANT896-4ME



Figura A-4 Antena GPS, ANT895-6ML, antena plana

Referencia	Explicación
6GK5895-6ML00-0AA0	Antena ANT 895-6ML, antena GPS activa incluido el cable de conexión (0,3 m) y el conector hembra N; 3 dBic @ 90°; IP67, -40 ... +85 °C, montaje con fijación mediante imanes o tornillos

A.2 Cable de antena

Cable de antena

Nota

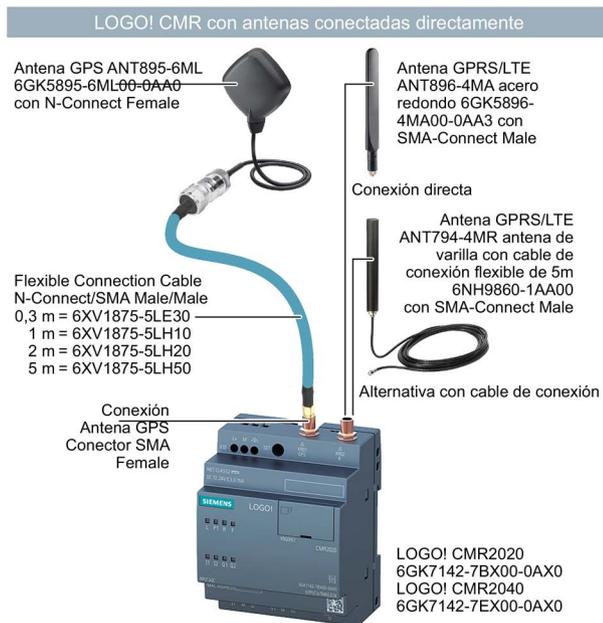
Longitud máxima del cable de antena

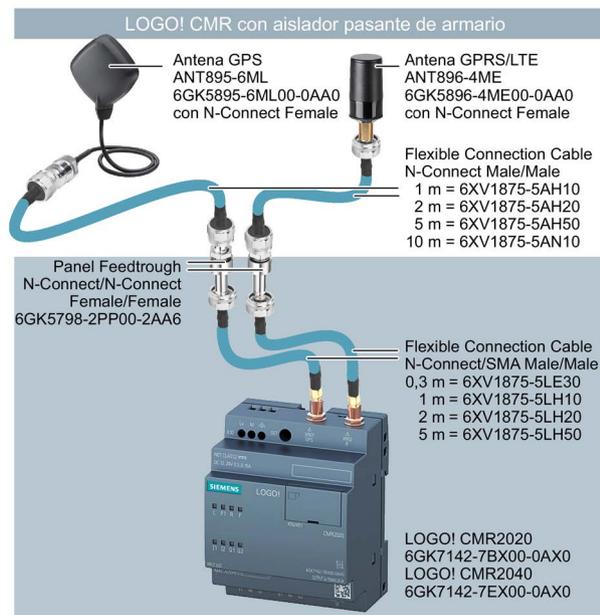
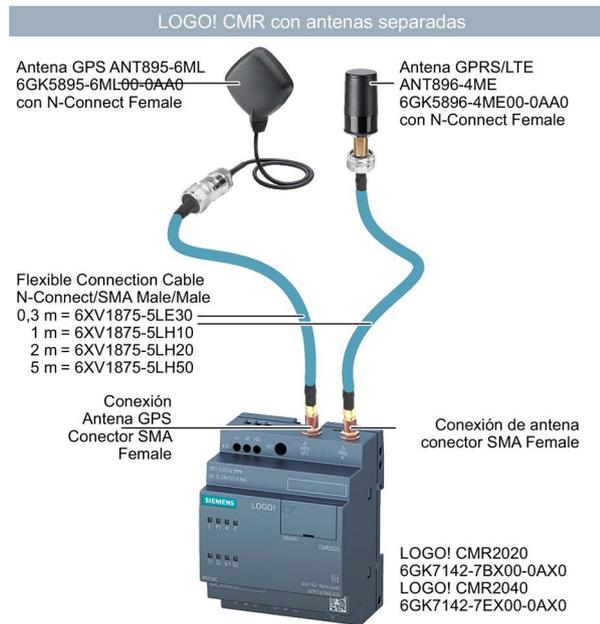
La longitud máxima admisible del cable de antena es de 15 m.

Tabla A- 1 Cables de conexión de antena

Referencia	Longitudes de cables	Explicación
6XV1875-5LE30	0,3 m	 <p>Cable de conexión flexible SIMATIC NET N-Connect/SM Male/Male preconfeccionado</p>
6XV1875-5LH10	1 m	
6XV1875-5LH20	2 m	
6XV1875-5LH50	5 m	
6XV1875-5AH10	1 m	 <p>Cable de conexión flexible SIMATIC NET N-Connect/N-Connect Male/Male preconfeccionado</p>
6XV1875-5AH20	2 m	
6XV1875-5AH50	5 m	
6XV1875-5AN10	10 m	

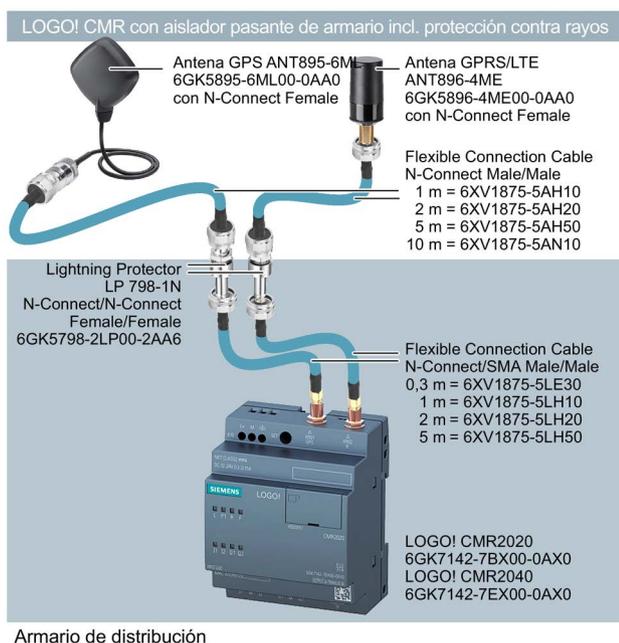
A continuación encontrará propuestas de conexiones de antenas del CMR para diferentes variantes de configuración.





Armario de distribución

A.3 Aislador pasante de armario / acoplamiento de antena



A.3 Aislador pasante de armario / acoplamiento de antena

Aislador pasante de armario

Aislador pasante de armario / pieza de acoplamiento



Referencia	Explicación
6GK5798-2PP00-2AA6	Pasatapas para armario para espesores de pared de 4,5 mm como máximo; también puede utilizarse como pieza de acoplamiento entre dos cables de conexión de antena, conexión hembra/hembra N-Connect/N-Connect; apto entre 0 y 11 GHz, IP68

A.4 Protección contra sobretensiones

Protección contra sobretensiones

Elemento de protección contra rayos



Referencia	Explicación
6GK5798-2LP00-2AA6	Elemento de protección contra rayos LP798-1N, para las antenas ANT790 y ANT890; para conexiones N-Connect, conexión hembra/hembra N-Connect/N-Connect; apto entre 0 y 6 GHz, IP68; también apto para alimentación DC a través del cable de antena

A.5 Tarjeta SD

Tarjetas SD compatibles

Para guardar archivos de configuración existe la posibilidad opcional de utilizar una tarjeta SD.

El slot para tarjetas y el CMR son compatibles con los formatos de tarjeta siguientes:

- **Tarjeta microSD**
 - Formato 15 x 11 mm
 - Especificaciones:
 - SD 1.0, 1 GB, FAT32
 - SD 1.1, 2 GB, FAT32
 - SDHC, hasta 32 GB, FAT32

Encontrará detalles sobre la utilización de la tarjeta SD en el capítulo Tarjeta SD (Página 76).

Nota

Rango de temperatura de la tarjeta SD

Al utilizar una tarjeta SD asegúrese de que es adecuada para el rango de temperatura en el que se utiliza el CMR.

Información complementaria sobre SMS

B.1 Comportamiento del CMR al recibir o responder SMS

Lista de todos los caracteres permitidos/no permitidos

Encontrará una lista de todos los caracteres permitidos y no permitidos en el capítulo Caracteres permitidos y longitudes de strings (Página 64).

Comprobar el número del remitente

Al recibir un SMS, el CMR comprueba en primer lugar si el remitente está registrado en el CMR con su número de teléfono y si dispone de derechos para enviar un SMS al CMR (consulte los ajustes en el capítulo Users (Página 112)):

- El CMR solo acepta mensajes de números de remitentes autorizados.
- También existe la posibilidad de crear grupos de números de teléfono utilizando el carácter "***"; consulte el capítulo Users (Página 112).

Comprobar las palabras clave y la contraseña del mensaje SMS

Nota

- La contraseña debe estar separada de la palabra clave por un punto y coma (;).
 - Los accesos de lectura no deben contener ninguna contraseña.
 - Los accesos de escritura pueden incluir una contraseña (entrada de contraseña desactivable).
-

Requisitos:

- El número del remitente del SMS se ha cotejado con los números de teléfono configurados de los usuarios autorizados.
- Se han rechazado todos los mensajes procedentes de números de teléfono no autorizados.

Para consultas y accesos de escritura, se aplican las siguientes convenciones:

- Las palabras clave siempre deben indicarse en mayúsculas.
- En los accesos de escritura se suprime el carácter "?" después de la palabra clave. Debe anteponer una contraseña:
 - Acceso de escritura: <contraseña>;<palabra clave>=<parámetro>
 - Acceso de lectura: <palabra clave>?<posib. parámetro>

El CMR comprueba si hay palabras clave en el texto del SMS o, en caso de comandos SMS de escritura, primero comprueba si está la contraseña indicada en la configuración:

- Si el SMS no contiene ninguna palabra clave o ninguna contraseña, o si la contraseña es errónea, se realiza una entrada en el búfer de diagnóstico.
 - Si el SMS procede de un número de teléfono autorizado, siempre se envía un SMS de respuesta.
 - Excepción: Si el SMS procede de un número de teléfono no autorizado o la opción "Allow receipt of SMS messages" está desactivada, se rechaza el SMS.

Configuración de la contraseña en SMS con acceso de escritura

Nota

Sin punto y coma en la contraseña

- La contraseña no debe tener punto y coma (;).
 - La contraseña debe estar separada de la palabra clave por un punto y coma.
-

En los mensajes de SMS con acceso de escritura puede haber una contraseña al principio. Configure dicha contraseña mediante el WBM.

La contraseña sirve para autorizar al usuario e impide la manipulación de los valores del LOGO! BM o del LOGO! CMR.

Responder SMS

Los SMS de usuarios autorizados pueden ser respondidos por el CMR (configurable). En los accesos de escritura, esta respuesta consiste en una confirmación del proceso de escritura, ya sea positiva o negativa.

Nota

Prevención de un bucle de SMS con CMR acoplados

Para que no se forme un bucle de SMS en caso de que haya varios CMR acoplados a través de la red de telefonía móvil, las tramas de confirmación se reciben pero no se responden.

El número de peticiones de envío de SMS/tiempo está limitado

El CMR guarda un número limitado de peticiones de envío de SMS en una cola de espera de peticiones.

El envío de un SMS puede tardar varios segundos debido al retardo en la transmisión en la red de telefonía móvil.

Compruebe bien los puntos siguientes para que se envíen SMS en la hora deseada:

- Adapte la longitud del intervalo de tiempo en correspondencia para volúmenes de datos grandes que deban enviarse cíclicamente, p. ej. PA-SMS (SMS de vigilancia).
- Asegúrese de que haya suficiente tiempo entre diferentes acciones que envíen PI SMS.

Si, p. ej., un mensaje PI SMS solicitado por SMS se ha enviado de forma incompleta, repita el SMS de petición.

Avisos de error de SMS

Encontrará una lista de posibles avisos de error en Avisos de error de SMS (Página 175).

B.2 Avisos de error de SMS

Aviso	Causas posibles
OK	El comando SMS se ha ejecutado correctamente.
Invalid Command	No se ha podido reconocer la palabra clave del SMS. Comprobar el uso de mayúsculas y minúsculas así como la sintaxis
Invalid Parameter	Parámetro de transferencia incorrecto; contraseña incorrecta.
No Success	Los valores no han podido ajustarse o leerse.
Try Again	Se está reconfigurando el CMR. No es posible procesar la petición.
No connection to LOGO! BM	<ul style="list-style-type: none"> • LOGO! BM no está activado o se ha ajustado una dirección IP errónea • Se ha extraído el cable entre LOGO! BM y LOGO! CMR
No GPS Signal	<ul style="list-style-type: none"> • GPS no configurado • No es posible recibir la señal GPS porque no se ha establecido ninguna conexión visual con el satélite GPS.
Not supported by LOGO! BM	Esta versión del dispositivo no soporta la activación de bits en la VM del Logo! BM. Para utilizar una variable VM de tipo BIT se necesita al menos un LOGO! BM con la versión de hardware FS:04 y la versión de firmware V1.81.01.

B.3 Sintaxis de todos los comandos SMS

Sintaxis de los comandos SMS y posibles respuestas

¿Qué información se desea obtener?	Ejemplo
Leer datos de diagnóstico del CMR	DIAG?
Leer la posición GPS del CMR	GPSPOSITION?
Leer la imagen de proceso (PI)	MONITOR?
Leer el estado del BM	STATUS?
Leer el valor actual	LOGO?VM125,WORD

¿Qué deseo modificar?	Ejemplo
Ajustar el estado del BM	Contraseña;STATUS=RUN
Escribir el valor actual	Contraseña;LOGO=VM125,1,WORD
Ajustar la salida digital del CMR	Contraseña;OUTPUT=O1,1
Modificar el número de teléfono de un usuario	Contraseña;CHANGEUSER="Joe","01721234567"
Configurar la dirección de un servidor NTP	Contraseña;NTPSERVER="217.13.75.19"
Consultar un código de servicio al operador de telefonía móvil	Contraseña;SERVICECODE="*100#"

B.4 Comandos SMS

En las tablas siguientes se describen todas las estructuras de SMS posibles para los comandos SMS y se ilustran con ejemplos.

Nota

Para cada SMS enviado al CMR solo es posible 1 comando SMS.

Nota

Uso de tarjetas SIM de prepago

Si usa una tarjeta SIM de prepago, puede consultar su saldo actual a través del código de servicio correspondiente de su proveedor.

Si su saldo se ha agotado, el CMR no envía ninguna advertencia automática.

Leer datos de diagnóstico del CMR	
Función	Petición de datos de diagnóstico del CMR
Acceso	Lectura, no se necesita contraseña

Leer datos de diagnóstico del CMR	
Estructura y palabra clave	DIAG?
Valores de retorno	Datos de diagnóstico o mensaje de error: Avisos de error de SMS (Página 175) Estructura de los datos de diagnóstico:SMS de diagnóstico (Página 142)
Ejemplo	SMS enviado: DIAG? SMS de respuesta: SMS de diagnóstico (Página 142)

Leer la posición GPS del CMR			
Función	Solicitar la posición GPS actual. La posición GPS actual se lee y se devuelve al remitente.		
Acceso	Lectura, no se necesita contraseña		
Estructura y palabra clave	GPSPOSITION?		
Valores de retorno	Coordenadas GPS o mensaje de error: Avisos de error de SMS (Página 175) Estructura del SMS: Posición GPS: ddd:mm:ss.hs N/S ddd:mm:ss.hs W/E Alt mmmm		
Ejemplo	SMS enviado: GPSPOSITION? SMS de respuesta: Posición GPS: 49:0:50.4 N 8:24:15.48 E Alt 0350		
Explicación para leer los datos de transferencia	ddd	degree	Grados
	mm	minutes	Minutos
	ss.hs	seconds	Segundos
	N/S	North/South	Longitud
	W/E	West/East	Latitud
	Alt mmmm	Altitude	Altitud sobre el nivel del mar en metros

Leer la imagen de proceso	
Función	Lectura de la imagen de proceso del BM y del estado de las dos entradas y salidas del CMR.
Acceso	Lectura, no se necesita contraseña
Estructura y palabra clave	MONITOR?
Valores de retorno	Memoria imagen de proceso o mensaje de error: Avisos de error de SMS (Página 175) Estructura de la memoria imagen de proceso: SMS de respuesta del comando "MONITOR?" (Página 181)
Ejemplo	SMS enviado: MONITOR? SMS de respuesta: SMS de respuesta del comando "MONITOR?" (Página 181)

Leer el estado del BM	
Función	Consulta del estado del BM
Acceso	Lectura, no se necesita contraseña
Estructura y palabra clave	STATUS?

Leer el estado del BM	
Valores de retorno	RUN, STOP o mensaje de error: Avisos de error de SMS (Página 175)
Ejemplo	SMS enviado: STATUS? SMS de respuesta: STATUS:RUN

Ajustar el estado del BM	
Función	Ajustar el estado del BM a RUN o STOP
Acceso	De escritura, contraseña (si está configurada)
Estructura y palabra clave	<Contraseña>;STATUS=<estado de LOGO>
Valores de retorno	OK (opcional) o mensaje de error: Avisos de error de SMS (Página 175)
Ejemplo	SMS de envío: Contraseña;STATUS=RUN SMS de respuesta: STATUS=RUN:OK

Configurar la dirección de un servidor NTP	
Función	Configurar la dirección de un servidor NTP. Solo si se ha elegido NTP como método de sincronización horaria, puede configurarse la dirección de un servidor NTP. <Dirección> puede ser la dirección IP en formato 123.123.123.123 o el nombre del servidor NTP en formato URL, p. ej., http://www.ntpservname.de.
Acceso	De escritura, contraseña (si está configurada)
Estructura y palabra clave	<Contraseña>;NTPSERVER="<Dirección>"
Valores de retorno	OK (opcional) o mensaje de error: Avisos de error de SMS (Página 175)
Ejemplo	Ejemplo 1: SMS de envío: Contraseña;NTPSERVER="http://www.ntpservname.de" SMS de respuesta: NTPSERVER="http://www.ntpservname.de":OK Ejemplo 2: SMS de envío: Contraseña;NTPSERVER="217.13.75.19" SMS de respuesta: NTPSERVER="217.13.75.19":OK

Nota

Acceso directo a la memoria de variables del BM

Por razones de seguridad, solo se puede acceder a la dirección de la VM en modo de lectura y escritura mediante SMS si la dirección se ha creado previamente como señal mediante el WBM.

Los comandos "Establecer o leer valor en la memoria de variables del BM" acceden directamente a la memoria de variables del BM.

Cuando utilice estos comandos tenga en cuenta las indicaciones del capítulo Sinopsis (Página 51).

Leer el valor actual de la memoria de variables del BM: leer "valores actuales"	
Función	<p>Leer el valor actual de la memoria de variables del BM.</p> <p>La dirección se obtiene de la memoria de variables del BM. El valor <tipo de datos> es BIT, BYTE, WORD o DWORD.</p> <p>Solo pueden leerse y escribirse los primeros 128 bytes de la memoria de variables del BM.</p> <p>Direcciones iniciales de los tipos de datos:</p> <ul style="list-style-type: none"> • BIT / BYTE: 0 ... 127 • WORD: 0 ... 126 • DWORD: 0 ... 124 <p>Puede leerse cualquier valor de la memoria de variables del BM. Si se conoce a fondo el programa de conmutación LOGO!, esto puede ser útil, p. ej., para fines de diagnóstico.</p>
Acceso	Lectura, no se necesita contraseña
Estructura y palabra clave	<ul style="list-style-type: none"> • LOGO?VM<Dirección>,<Tipo de datos> • LOGO?<Signal name>
Valores de retorno	<p>Valor actual o mensaje de error: Avisos de error de SMS (Página 175)</p> <ul style="list-style-type: none"> • Estructura del valor de retorno de la memoria de variables: VM<dirección>:<valor>(<tipo de datos>) • Estructura del valor de retorno de una señal: <nombre de señal>:<valor> <p>Salida: salida del valor de retorno en formato decimal</p>
Ejemplo	<p>SMS enviado: LOGO?VM125,WORD</p> <p>SMS de respuesta: VM125:1(WORD)</p>

Ajustar el valor en la memoria de variables del BM: escribir "valores actuales"	
Función	<p>Ajustar valores de un componente en la memoria de variables del BM, p. ej., entradas, salidas o marcas.</p> <p>La dirección del componente se obtiene de la memoria de variables del BM.</p> <p>Solo pueden leerse y escribirse los primeros 128 bytes de la memoria de variables del BM.</p> <p>Direcciones iniciales de los tipos de datos:</p> <ul style="list-style-type: none"> • BIT, BYTE: 0 ... 127 • WORD: 0 ... 126 • DWORD: 0 ... 124 <p>Al ajustar un valor en la memoria de variables del BM, puede modificarse la secuencia de un programa de conmutación LOGO!.</p> <p>Utilice este comando solo si conoce a fondo el programa de conmutación.</p> <p>El CMR procesa todos los valores como valores con signo.</p>
Acceso	De escritura, contraseña (si está configurada)
Estructura y palabra clave	<ul style="list-style-type: none"> • <Contraseña>;LOGO=VM<Dirección>,<Valor>,<Tipo de datos> • <contraseña>;LOGO=VM<dirección>,<nombre de constante> • <contraseña>;LOGO=<nombre de señal>,<valor> • <contraseña>;LOGO=<nombre de señal>,<nombre de constante>

B.4 Comandos SMS

Ajustar el valor en la memoria de variables del BM: escribir "valores actuales"	
Valores de retorno	Confirmación (opcional) o mensaje de error: Avisos de error de SMS (Página 175)
Ejemplo	SMS de envío: Contraseña;LOGO=VM125,1,WORD SMS de respuesta: LOGO=VM125,1,WORD: OK

Ajustar la salida digital del CMR	
Función	Ajuste de la salida digital 1 o 2 del CMR a un valor: 1 o 0.
Acceso	De escritura, contraseña (si está configurada)
Estructura y palabra clave	<ul style="list-style-type: none"> • <Contraseña>;OUTPUT=O<1/2>,<1/0> • <contraseña>;OUTPUT=<nombre de señal>,<1/0> • <contraseña>;OUTPUT=<nombre de señal>,<nombre de constante>
Valores de retorno	OK (opcional) o mensaje de error: Avisos de error de SMS (Página 175)
Ejemplo	SMS de envío: Contraseña;OUTPUT=O1,1 SMS de respuesta: OUTPUT=O1,1:OK

Modificación del número de teléfono de un usuario	
Función	Modificación del número de teléfono de un usuario claramente especificado mediante el nombre de usuario. Para el usuario seleccionado debe registrarse para ello la autorización correspondiente en la ficha Users de Users / groups en el WBM; consulte el capítulo Users (Página 112).
Acceso	De escritura, contraseña (si está configurada), la autorización debe estar configurada en el WBM
Estructura y palabra clave	<contraseña>;CHANGEUSER="User name","número de teléfono" Utilice para este comando el nombre de usuario que ha introducido para iniciar sesión en el WBM.
Valores de retorno	OK (opcional) o mensaje de error: Avisos de error de SMS (Página 175)
Ejemplo	SMS de envío: Contraseña;CHANGEUSER="Joe","01751234567" SMS de respuesta: CHANGEUSER="Joe","01751234567":OK

Consultas al operador de telefonía móvil a través del código de servicio	
Función	Consulta de un código de servicio al operador de telefonía móvil, p. ej., "**100#". El texto transmitido por el operador de telefonía móvil se devuelve sin cambios como respuesta en un SMS. Si utiliza una tarjeta SIM de prepago y desea consultar su saldo actual, puede utilizar el código de servicio para hacerlo. Sin embargo, no pueden usarse todos los códigos de servicio posibles para realizar consultas.
Acceso	De escritura, contraseña (si está configurada)
Estructura y palabra clave	<Contraseña>;SERVICECODE="Código"
Valores de retorno	Respuesta original del operador de telefonía móvil o aviso de error
Ejemplo	SMS de envío: Contraseña;SERVICECODE="**100#" SMS de respuesta: *100#: Texto original del operador de telefonía móvil o mensaje de error

B.5 SMS de respuesta del comando "MONITOR?"

Imagen de proceso

La imagen de proceso muestra los estados actuales y los valores del CMR y del BM con sus módulos de ampliación.

El número de elementos de periferia disponibles realmente en la instalación depende de los módulos de ampliación utilizados.

Encabezado del SMS		Bloques de valores
Nombre del módulo del CMR		From: logo.cmr
Fecha y hora del módulo		<YYYY-MM-DD> <hh:mm:ss>

CMR		Bloques de valores
Entradas digitales	Entradas	I1, I2
Salidas digitales	Salidas	Q1, Q2

BM		Bloques de valores
Estado de programa	Estado de programa	PS
Estado de comunicación	Estado de conexión BM-CMR	CS
Entradas digitales	Entradas	I1 ... I24
Salidas digitales	Salidas	Q1 ... Q20
Marcas digitales		M1 ... M64
Entradas de registros de desplazamiento		S1.1 ... S4.8
Teclas de flecha		▶ ◀ ▼ ▲
Teclas de función		F1 ... F4
Entradas analógicas		AI1 ... AI8
Salidas analógicas		AQ1 ... AQ8
Marcas analógicas		AM1 ... AM64

Estructura del SMS de respuesta de la memoria imagen de proceso (PA-SMS)

Nota

Máximo 7 mensajes SMS

El SMS de respuesta abarca un total máximo de 7 mensajes SMS. El número de mensajes SMS depende de las señales vigiladas.

Significado de "*" en las tablas

"*" corresponde a dígitos en blanco en la estructura del SMS de respuesta.

Representación de valores digitales, registros de desplazamiento

- Un dígito, con su estado lógico (0 o 1).
- Ocho valores por fila, modo de contaje de derecha a izquierda.

Representación de valores analógicos

- Valores analógicos en función de la representación interna (máx. 6 caracteres) de los valores analógicos del LOGO! BM.
- Los valores se representan con 6 cifras y ceros a la izquierda. En cada fila se muestra un valor analógico.

Representación de valores y bloques de valores no utilizados

- Los valores no utilizados se representan con "x".
- Si en las demás filas de un bloque de valores no hay más valores utilizados a continuación, dichas filas no se muestran.
Consulte el siguiente "Ejemplo de SMS de respuesta" en el bloque de valores "BM I:".
- Un bloque de valores no utilizado se suprime por completo en la representación, incluido su nombre.

Representación de las teclas de manejo

- 4 valores por fila

El SMS de respuesta del CMR a una consulta de la imagen de proceso tiene preparada la siguiente estructura:

Tabla B- 1 SMS de respuesta: Estructura

Contenido del SMS	Información
Encabezado del SMS	
From: lo-go.cmr	Nombre del módulo del CMR
2016-10-05 14:14:45	Fecha y hora del módulo
CMR I: denominación del bloque de valores para entradas del CMR	
*****xx	Entradas del CMR 1 y 2, valores de derecha (I1) a izquierda (I2)
CMR Q: denominación del bloque de valores para salidas del CMR	
*****xx	Salidas del CMR 1 y 2, valores de derecha (Q1) a izquierda (Q2)
BM PS/CS: estado del programa y de la comunicación del BM	
*****1	PS CS PS = 1: BM en RUN PS = 0: BM en STOP CS = 1: conexión con el CMR CS = 0: ninguna conexión con el CMR
BM I: denominación del bloque de valores para entradas digitales del LOGO! BM	
xxxxxxxx	Entradas 8 ... 1, valores de derecha (I1) a izquierda (I8)
xxxxxxxx	Entradas 16 ... 9
xxxxxxxx	Entradas 24 ... 17
BM Q: denominación del bloque de valores para salidas digitales del LOGO! BM	
xxxxxxxx	Salidas 8 ... 1, valores de derecha (Q1) a izquierda (Q8)
xxxxxxxx	Salidas 16 ... 9
***xxxx	Salidas 20 ... 17
BM M: denominación del bloque de valores para marcas digitales del LOGO! BM	
xxxxxxxx	Marcas 8 ... 1, valores de derecha (M1) a izquierda (M8)
xxxxxxxx	Marcas 16 ... 9
xxxxxxxx	Marcas 24 ... 17
xxxxxxxx	Marcas 32 ... 25
xxxxxxxx	Marcas 40 ... 33
xxxxxxxx	Marcas 48 ... 41
xxxxxxxx	Marcas 56 ... 49
xxxxxxxx	Marcas 64 ... 57
BM S: denominación del bloque de valores para registros de desplazamiento del LOGO! BM	
xxxxxxxx	Entradas de registros de desplazamiento S1.8 ... S1.1
xxxxxxxx	Entradas de registros de desplazamiento S2.8 ... S2.1
xxxxxxxx	Entradas de registros de desplazamiento S3.8 ... S3.1
xxxxxxxx	Entradas de registros de desplazamiento S4.8 ... S4.1
BM C: denominación del bloque de valores para teclas de flecha del LOGO! BM	

Contenido del SMS	Información
xxxx	Teclas 4 ... 1 con los símbolos ▶ ◀ ▼ ▲
BM F: denominación del bloque de valores para teclas de función del LOGO! BM	
xxxx	Teclas de función F4 ... F1, F1 a la derecha
BM AI: denominación del bloque de valores para entradas analógicas del LOGO! BM	
xxxxxx	Entrada analógica 1
xxxxxx	Entrada analógica 2
xxxxxx	Entrada analógica 3
xxxxxx	Entrada analógica 4
xxxxxx	Entrada analógica 5
xxxxxx	Entrada analógica 6
xxxxxx	Entrada analógica 7
xxxxxx	Entrada analógica 8
BM AQ: denominación del bloque de valores para salidas analógicas del LOGO! BM	
xxxxxx	Salida analógica 1
xxxxxx	...
xxxxxx	...
xxxxxx	Salida analógica 8
BM AM: denominación del bloque de valores para marcas analógicas del LOGO! BM	
xxxxxx	Marca analógica 1
xxxxxx	...
xxxxxx	...
xxxxxx	Marca analógica 64

Ejemplo de SMS de respuesta

- En el CMR se utilizan la entrada 1 y la salida 2.
- En el programa de conmutación del BM se vigilan además I1, I2 e I6, así como Q1, Q3, Q9 y Q17, y la entrada analógica 2.

Supuesto

- BM en RUN, CMR conectado con el BM
- CMR: I1 = 1, Q2 = 1
- BM: I1 = 0, I2 = 1, I6 = 0, Q1 = 1, Q3 = 0, Q9 = 1, Q17 = 0, AI2 = 3,5 V

Tabla B- 2 SMS de respuesta

Contenido	Descripción
Encabezado del SMS	
From: DEVICE- nombre	Nombre del módulo del CMR
2016-10-05 14:14:45	Fecha y hora del módulo
CMR I:	
*****x1	* = 6 espacios en blanco al principio
CMR Q:	
*****1x	* = 6 espacios en blanco al principio
BM PS/CS:	
*****11	BM en RUN, CMR conectado con el BM
BM I:	
xx0xxx10	Entradas 9 ... 24 del bloque de valores no utilizadas y no mostradas
BM Q:	
xxxxx0x1	
xxxxxxx1	
****xxx0	* = 4 espacios en blanco al principio
BM AI:	Bloques de valores BM M, BM S, BM C y BM F no utilizados y no mostrados
xxxxxx	
00350	Ningún valor más en este bloque de valores ni en los bloques de valores siguientes; por lo tanto, ninguna indicación en el SMS.

Ejemplo con LOGO! BM

- El rango de tensión de la entrada analógica es de 0 a 10 V:
Este rango se representa con valores en 1 000 pasos.
- Una tensión en la entrada analógica de 3,5 V tiene un valor de 350 [00350]:
Tensión de entrada en V * 100 = valor interno de LOGO!
- Los valores se representan con 6 cifras y ceros a la izquierda. En cada fila se muestra un valor analógico.
- Los valores no utilizados se representan con x.
Los valores que no pueden leerse se representan con "e".
- Las demás filas de un bloque de valores se omiten por completo si en ellas ya no hay a continuación ningún valor utilizado.

Bibliografía

Cómo encontrar la documentación Siemens

- **Referencias / Catálogos**

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

Encontrará los catálogos en la página web del Siemens Industry Mall:

Enlace: (<https://mall.industry.siemens.com>)

También puede solicitar catálogos e información adicional a la subsidiaria o sucursal correspondiente de Siemens.

- **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 seleccione el tipo de artículo "Manual".

C.1 /1/

SIMATIC NET
LOGO! CMR2020 / CMR2040
Instrucciones de servicio
Siemens AG

Enlace: (<https://support.industry.siemens.com/cs/ww/es/ps/15383/man>)

C.2 /2/

LOGO!
Manual de sistema
Siemens AG
Edición actual en la siguiente página web:

Enlace: (<https://support.industry.siemens.com/cs/ww/es/ps/13617/man>)

Índice alfabético

A

Abreviatura, 4
Acceso al LOGO! BM, 53
Actualización de valores mostrados, 74
Alimentación, 20
 Externa, 40
Antenas
 Orientar de forma óptima, 97
Archivo de configuración - editar, 85
Archivos - Formatos, 77
Avisos de diagnóstico, 141

B

Bandas de frecuencia, 45
Bornes con tornillos
 Alimentación, 46
Búfer de diagnóstico, 141

C

Cambio de dispositivo, 37, 84
Cargar el programa del BM, 25
Causa del fallo, 145
Condiciones de la licencia de Open Source Software, 60
Conexión con el BM, 118
Configuración
 Mediante la interfaz local, 69
 Reutilizar en otro CMR, 89
Configurar el navegador web, 69
Consignas de seguridad para el uso de los equipos, 39
Contacto, 7
Contraseña
 En SMS, 174
Contrato de telefonía móvil - Recomendaciones, 20
Correos electrónicos - Intentos de transmisión, 93

D

Desbloquear la tarjeta SIM, 49

E

Eliminación, 6
Entradas, 44
Enviar valores de proceso (SMS/correo electrónico), 121
Estrategia de reserva LTE, 14

F

Formación, 7

G

Glosario, 6
Glosario de SIMATIC NET, 6
Guardar configuración, 63

H

Homologaciones radioeléctricas, 163

I

Imagen de proceso, 181
Intensidad de señal, 46
Interfaz X1P1, 43
Internet - conexión directa, 91

M

Memoria, 76
Montaje en riel de perfil de sombrero, 42
Montaje mural, 43

N

Navegadores web, 68
Navegadores web soportados, 68
Nombres de archivo, 77

O

OpenVPN
 Versión, 18

P

Página inicial
 Llamar, 69
 Ninguna indicación, 70
 Visualización, 70
Parámetros de acceso, 94
Pulsador SET
 Funciones, 35

R

Rearranque completo, 87
Reciclado, 6
Referencia, 3
Referencias cruzadas (PDF), 4
Registro (generación de informes), 89
Reset to factory settings, 87
Router, 91

S

Salidas, 44
Signal strength, 73
Sincronización horaria, 78
SMSC
 Cambiar número, 96
Support, 7

T

Tarjeta SIM
 Desbloqueo, 95
Tarjeta SIM - Recomendaciones, 20

V

Versión de firmware, 3
Versión de hardware, 3

W

WBM - Web Based Management, 60