SIEMENS

SIMATIC NET

S7-1200 - TeleControl CP 1243-1

Instructions de service

12/2019

C79000-G8977-C365-05

Mentions légales

Signalétique d'avertissement

Ce manuel donne des consignes que vous devez respecter pour votre propre sécurité et pour éviter des dommages matériels. Les avertissements servant à votre sécurité personnelle sont accompagnés d'un triangle de danger, les avertissements concernant uniquement des dommages matériels sont dépourvus de ce triangle. Les avertissements sont représentés ci-après par ordre décroissant de niveau de risque.

⚠DANGER
signifie que la non-application des mesures de sécurité appropriées **entraîne** la mort ou des blessures graves.

⚠ATTENTION
signifie que la non-application des mesures de sécurité appropriées **peut entraîner** la mort ou des blessures graves.

⚠PRUDENCE
signifie que la non-application des mesures de sécurité appropriées peut entraîner des blessures légères.

IMPORTANT
signifie que la non-application des mesures de sécurité appropriées peut entraîner un dommage matériel.

En présence de plusieurs niveaux de risque, c'est toujours l'avertissement correspondant au niveau le plus élevé qui est reproduit. Si un avertissement avec triangle de danger prévient des risques de dommages corporels, le même avertissement peut aussi contenir un avis de mise en garde contre des dommages matériels.

Personnes qualifiées

L'appareil/le système décrit dans cette documentation ne doit être manipulé que par du **personnel qualifié** pour chaque tâche spécifique. La documentation relative à cette tâche doit être observée, en particulier les consignes de sécurité et avertissements. Les personnes qualifiées sont, en raison de leur formation et de leur expérience, en mesure de reconnaître les risques liés au maniement de ce produit / système et de les éviter.

Utilisation des produits Siemens conforme à leur destination

Tenez compte des points suivants:

⚠ATTENTION
Les produits Siemens ne doivent être utilisés que pour les cas d'application prévus dans le catalogue et dans la documentation technique correspondante. S'ils sont utilisés en liaison avec des produits et composants d'autres marques, ceux-ci doivent être recommandés ou agréés par Siemens. Le fonctionnement correct et sûr des produits suppose un transport, un entreposage, une mise en place, un montage, une mise en service, une utilisation et une maintenance dans les règles de l'art. Il faut respecter les conditions d'environnement admissibles ainsi que les indications dans les documentations afférentes.

Marques de fabrique

Toutes les désignations repérées par ® sont des marques déposées de Siemens AG. Les autres désignations dans ce document peuvent être des marques dont l'utilisation par des tiers à leurs propres fins peut enfreindre les droits de leurs propriétaires respectifs.

Exclusion de responsabilité

Nous avons vérifié la conformité du contenu du présent document avec le matériel et le logiciel qui y sont décrits. Ne pouvant toutefois exclure toute divergence, nous ne pouvons pas nous porter garants de la conformité intégrale. Si l'usage de ce manuel devait révéler des erreurs, nous en tiendrons compte et apporterons les corrections nécessaires dès la prochaine édition.

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
ALLEMAGNE

Numéro de commande du document: C79000-G8977-C365-05
℗ 01/2020 Sous réserve de modifications

Avant-propos

Validité du manuel

Le présent document contient des informations sur le produit Telecontrol suivant :

- **CP 1243-1**
  Numéro d'article 6GK7 243-1BX30-0XE0
  Version de matériel 2
  Version de firmware V3.2

  Le CP 1243-1 est le processeur de communication permettant de connecter un S7-1200 SIMATIC, via l'infrastructure publique (DSL p. ex.), à des systèmes de poste de conduite. Pour les protocoles Telecontrol pris en charge, voir chapitre Propriétés du CP (Page 13).

  Grâce à la technologie VPN et au pare-feu, le CP assure un accès sécurisé au S7-1200.

  Le CP peut en outre être utilisé comme interface Ethernet additionnelle de la CPU pour la communication S7.

Figure 1 CP 1243-1

Derrière le volet supérieur du boîtier du module, un "X" est imprimé à droite du numéro d'article pour désigner le numéro de version. Si la mention imprimée est par exemple "X 2 3 4" le "X" signale qu'il s'agit de la version 1 du matériel.

La version de firmware du CP à la livraison figure derrière le volet supérieur du boîtier à gauche sous le champ de LED.

L'adresse MAC figure derrière le volet inférieur du boîtier.

Désignations de produit et abréviations

- **CP / module**

  Ces abréviations sont utilisées ci-après en lieu et place de la désignation complète du produit CP 1243-1.

- **TCSB**

  Cette abréviation est utilisée ci-après pour le logiciel "TeleControl Server Basic" version V3.

- **STEP 7**

  Cette abréviation est utilisée ci-après pour l'outil de configuration STEP 7 Basic / Professional.

- **ES**

  PC sur lequel se trouve le projet STEP 7

Objet du manuel

Ce manuel décrit les propriétés du module et vous aide à monter l'appareil et à le mettre en service.

Le manuel fournit en outre des informations sur l'utilisation et le diagnostic de l'appareil.

Configuration

Les étapes de la configuration sont présentées sous forme de récapitulatif.

- **CP sans communication Telecontrol**

  Pour ces applications, les étapes de configuration significatives sont décrites dans le présent manuel.

- **CP avec communication Telecontrol**

  La description complète de la configuration et du diagnostic pour ces applications figure dans le manuel de configuration correspondant /4/ (Page 108).

Tenez compte des indications de la section "Structure de la documentation".

Nouveau dans cette édition

- Nouvelle version de firmware V3.2, avec entre autres les améliorations fonctionnelles suivantes :
  - Augmentation du nombre de point de données
  - Extension des fonctions Telecontrol, voir configuration de point de données
  - Prise en charge de blocs OUC supplémentaires
- Nouvelle homologation ATEX/IECEx
- Nouvelle structure de la documentation

Édition du manuel remplacée

Édition 02/2018

Structure de la documentation

La documentation du CP se compose des manuels et contenus suivants :

- **Instructions de service**
  - Application et fonctions (sans Telecontrol)
  - Configuration requise (CPU, logiciel de configuration, etc.)
  - Description du matériel
  - Montage, connexion, mise en service, utilisation
  - Configuration

    Le chapitre "Configuration" décrit uniquement la configuration des fonctions liées à Telecontrol.

    Si vous utilisez des fonctions Telecontrol, lisez le Manuel de configuration correspondant.
  - Diagnostic, maintenance
  - Caractéristiques techniques, homologations, accessoires
- **Manuel de configuration TeleControl Basic**

  Configuration et diagnostic sous STEP 7 Professional (TIA Portal)

  Valable pour tous les modules de communication SIMATIC NET qui supportent le protocole TeleControl Basic.

- **Manuel de configuration DNP3**

  Configuration et diagnostic sous STEP 7 Professional (TIA Portal)

  Valable pour tous les modules de communication SIMATIC NET qui supportent le protocole DNP3.

- **Manuel de configuration CEI 60870-5**

  Configuration et diagnostic sous STEP 7 Professional (TIA Portal)

  Valable pour tous les modules de communication SIMATIC NET qui supportent le protocole CEI 60870-5-101/104.

Vous trouverez les liens Internet des manuels en annexe Bibliographie (Page 107).

Édition actuelle du manuel sur Internet

L'édition actuelle de ce manuel se trouve sur les sites Internet du Siemens Industry Online Support :

Link: (https://support.industry.siemens.com/cs/ww/fr/ps/15922/man)

Connaissances requises

Pour monter, mettre en service et utiliser le CP, vous devez posséder des connaissances dans les domaines suivants :

- technique d'automatisation
- installation du système SIMATIC S7-1200
- SIMATIC STEP 7 Basic / Professional

Références croisées

Ce manuel contient de nombreuses références renvoyant à d'autres chapitres.

Pour retourner à la page de départ, après avoir consulté une référence croisée, certaines visionneuses de PDF supportent la commande <Alt>+<flèche vers la gauche>.

Licence d'utilisation

Remarque

Logiciels Open Source

Le produit contient des logiciels Open Source. Lisez attentivement la licence d'utilisation des logiciels Open Source avant d'utiliser le produit.

Vous trouverez la licence d'utilisation sur le support de données fourni.

- OSS_CP1243x_99.pdf

Firmware

Le firmware est signé et crypté. Ceci permet de s'assurer que seul du firmware d'origine Siemens sera chargé sur l'appareil.

Notes relatives à la sécurité des données

Siemens commercialise des produits et solutions comprenant des fonctions de sécurité industrielle qui contribuent à une exploitation sûre des installations, systèmes, machines et réseaux.

Pour garantir la sécurité des installations, systèmes, machines et réseaux contre les cybermenaces, il est nécessaire d'implémenter (et de préserver) un concept de sécurité industrielle global et moderne. Les produits et solutions Siemens constituent une partie d'un tel concept.

Il incombe aux clients d'empêcher tout accès non autorisé à leurs installations, systèmes, machines et réseaux. Ces systèmes, machines et composants doivent uniquement être connectés au réseau d'entreprise ou à Internet dans la mesure où cela est nécessaire et seulement si des mesures de protection correspondantes (p. ex. des pare-feux et/ou la segmentation du réseau) ont été prises.

Pour plus d'informations sur les mesures de protection pouvant être mises en œuvre dans le domaine de la sûreté industrielle, rendez-vous sur :
Link: (http://www.siemens.com/industrialsecurity)

Les produits et solutions Siemens font l'objet de développements continus pour être encore plus sûrs. Siemens vous recommande donc vivement d'effectuer des actualisations dès que les mises à jour correspondantes sont disponibles et de ne toujours utiliser que les versions de produit actuelles. L'utilisation de versions obsolètes ou qui ne sont plus prises en charge peut augmenter le risque de cybermenaces.

Afin d'être informé des mises à jour produit dès qu'elles surviennent, abonnez-vous au flux RSS Siemens Industrial Security sous :
Link: (http://www.siemens.com/industrialsecurity)

Glossaire SIMATIC NET

De nombreux termes techniques figurant dans cette documentation sont expliqués dans le glossaire SIMATIC NET.

Le glossaire SIMATIC NET se trouve à l'adresse Internet suivante :

Lien : (https://support.industry.siemens.com/cs/ww/fr/view/50305045)

Recyclage et élimination

Le produit ne contient que peu de polluants, est recyclable et conforme aux exigences de la directive DEEE 2012/19/UE relative aux "Déchets d'équipements électriques et électroniques".

N'éliminer pas le produit dans des décharges publiques. Pour un recyclage respectueux de l'environnement de vos appareils usagés, veuillez vous adresser à une société agréée de recyclage de déchets électroniques ou à votre interlocuteur Siemens.

Tenez compte des règlements locaux.

Vous trouverez des informations sur la restitution de produits sur le site du Siemens Industry Online Support :
Link: (https://support.industry.siemens.com/cs/ww/fr/view/109479891)

Formation, Service & Support

Vous trouverez des informations sur Formation, Service & Support dans le document multilingue "DC_support_99.pdf" qui figure sur le support de données fourni contenant la documentation.

Sommaire

Application et fonctions

1

1.1 Propriétés du CP

Application

Le CP est conçu pour fonctionner dans un automate programmable S7-1200.

Le CP permet de connecter le S7–1200 à Industrial Ethernet et via Internet aux systèmes de poste de conduite suivants :

- Serveur Telecontrol (application serveur OPC TCSB V3)
- Poste de conduite central DNP3
- Poste de conduite central IEC

Le CP peut en outre être utilisé comme extension de l'interface Ethernet de la CPU. Dans cette fonction il permet de s'isoler du réseau.

En combinant diverses fonctions de sécurité telles que pare-feu et protocoles de cryptage des données, le CP protège la station ou des cellules d'automatisation complètes contre les intrusions. Il met en outre les communications entre la station et les partenaires de communication à l'abri de l'espionnage et des manipulations.

1.2 Services de communication

Communication Telecontrol

Les applications suivantes sont supportées :

- **Communication avec un poste de commande central**

  Le CP est le processeur de communication du SIMATIC S7-1200 pour la connexion aux systèmes de poste de conduite précités. Le CP peut communiquer avec des postes de conduite redondants.

  Le protocole Telecontrol approprié est activé sur le CP pour chaque système de conduite ("Mode de communication"). Les protocoles servent à la transmission de données basée IP pour applications Telecontrol.

  Les fonctions de sécurité des données utilisables sont indiquées au chapitre Fonctions de sécurité des données (Page 18).

- **Communication transversale / directe entre stations**

  Avec les trois protocoles Telecontrol, le CP permet de communiquer avec d'autres stations S7.

Messages / e-mails

En cas d'évènements particuliers, le CP peut envoyer des messages par e-mail.

La fonction se configure dans la communication Telecontrol sous STEP 7. Il n'est pas nécessaire d'utiliser des blocs de programme.

Les conditions et fonctions sont décrites au chapitre Configuration de la messagerie (Page 60).

Communication via SINEMA Remote Connect

Supportée à partir du firmware version V3.1. Voir chapitre Communication via SINEMA RC (Page 15).

Communication S7 et communication PG/OP

La lecture / l'écriture de données sur une CPU est possible si la communication S7 a été activée dans la configuration du CP.

Le CP prend en charge les fonctions suivantes :

- **PUT/GET**

  Le CP prend en charge la fonction comme client et serveur pour l'échange de données avec des stations distantes (S7-300/400/1200/1500)

  Pour plus de détails sur les blocs de programme voir le système d'information de STEP 7.

- **Fonctions PG**
- **Fonctions de conduite et de visualisation (IHM)**
- **Routage S7**

  À partir du firmware du CP V2.1 avec CPU ≥ V4.2

Le CP a besoin, pour la communication S7, d'une adresse IP statique.

Communication via Open User Communication (OUC)

Grâce à l'interface Ethernet et aux blocs de programme de l'Open User Communication sur la CPU, le CP dispose des options de communication suivantes :

- communication avec des stations SIMATIC
- envoi d'e-mails

  À la différence du service correspondant de la communication Telecontrol (voir ci-dessus), la transmission de SMS/e-mails via OUC nécessite l'emploi du bloc de programme TMAIL_C, voir chapitre Blocs de programme pour OUC (Page 83).

1.3 Communication via SINEMA RC

Communication via SINEMA Remote Connect (SINEMA RC)

L'application "SINEMA RC Server" constitue un système de gestion cohérent via Internet des connexions de réseaux distribués. Il permet également d'accéder en toute sécurité à des stations subordonnés. La communication entre le serveur SINEMA RC et les abonnés distants passe par des tunnels VPN en prenant en compte les droits d'accès définis.

SINEMA RC utilise OpenVPN pour le cryptage des données. Le centre de communication est le serveur SINEMA RC par lequel passent les communications entre les abonnés et qui gère la configuration du système de communication.

Les routeurs SCALANCE M que vous pouvez utiliser pour la connexion, supportent également OpenVPN et le couplage à SINEMA Remote Connect.

Concernant la version de firmware requise du CP pour la communication via SINEMA RC voir chapitre Services de communication (Page 13).

Groupes de paramètres

La configuration de la communication via SINEMA RC et de la communication Telecontrol via SINEMA RC s'effectue dans deux groupes de paramètres :

- Communication via SINEMA RC

  > "Security > VPN"

- Communication Telecontrol via SINEMA RC :

  > "Modes de communication"

  Pour la configuration, voir les manuels de configuration Telecontrol /4/ (Page 108).

Applications

De la combinaison des paramètres de la communication Telecontrol et de SINEMA RC découlent les possibilités d'application suivantes :

Cas d'application :

- (1) Pas de Telecontrol et pas de SINEMA RC (CP uniquement pour la séparation des réseaux)
- (2) CP uniquement pour la télémaintenance via SINEMA RC
- (3) Communication uniquement pour la communication Telecontrol
- (4) Le CP utilise la communication Telecontrol, mais SINEMA RC uniquement pour la télémaintenance.
- (5) Le CP utilise SINEMA RC pour la communication Telecontrol et la télémaintenance.

Le tableau récapitule les cas d'application et les paramétrages correspondants.

- "Activé" signifie que le paramètre est activé.
- "Désactivé" signifie que le paramètre est désactivé.

Tableau 1- 1 Cas d'application et paramètres à activer

Cas d'application	Paramétrages (paramètre abrégé) *		
	SRC	TC	TC-SRC
(1)	Désactivé	Désactivé	Désactivé
(2)	Activé	Désactivé	Désactivé
(3)	Désactivé	Activé	Désactivé
(4)	Activé	Activé	Désactivé
(5)	Activé	Activé	Activé

***** Signification des abréviations de paramètre :

SRC - Security > VPN (activé) > "Type de connexion VPN":
"Configuration OpenVPN automatique via SINEMA Remote Connect Server"

TC - Modes de communication > Communication Telecontrol activée

TC-SRC - Modes de communication >
"Activer la communication Telecontrol via SINEMA Remote Connect"

1.4 Autres services et propriétés

Autres services et propriétés

- **Configuration IP - IPv4 et IPv6**
  - IPv4 / IPv6

    Le CP prend en charge les adresses IP selon IPv4 et IPv6.

    Une adresse IPv6 peut être utilisée en plus d'une adresse IPv4 dans les réseau IPv6.
  - Attribution d'adresse

    L'adresse IP, le masque de sous-réseau et l'adresse d'une passerelle peuvent être définis manuellement dans la configuration.

    L'adresse IP peut sinon être également obtenue d'un serveur DHCP ou par un autre moyen hors de la configuration.
- **Synchronisation d'horloge**

  Le CP prend en charge diverses méthodes de synchronisation d'horloge : Pour plus d'informations, voir chapitre Synchronisation d'horloge (Page 47).

- **Fonctions en ligne**

  La station d'ingénierie vous permet, grâce aux fonctions en ligne de STEP 7, d'accéder à la station via le CP.

  Les fonctions en ligne suivantes sont disponibles :

  – chargement de données de projet ou de programme d'un projet STEP 7 sur la station
  – lecture de données de diagnostic sur la station
  – chargement de fichiers de firmware sur le CP

  Vous trouverez des informations sur les fonctions en ligne au chapitre Possibilités de diagnostic (Page 89).

- **SNMP**

  Le CP prend en charge, en tant qu'agent SNMP, la requête de données via SNMP (Simple Network Management Protocol).

  Pour plus d'informations, reportez-vous au chapitre SNMP (Page 94).

Autres propriétés du mode Telecontrol

- **Configuration de points de données**

  Du fait de la configuration de points de données sous STEP 7, il n'est pas nécessaire de programmer des blocs de programme pour la transmission des données de process. Les divers points de données sont traités à l'identique par le système.

- **Tampon d'émission**

  Le CP enregistre les valeurs de points de données qui sont configurés comme évènement, dans le tampon d'émission.

  L'enregistrement des données n'est pas rémanent. Lors d'une coupure de la tension elles sont perdues.

- **Transfert de données de process sur évènement**

  Le CP transfère les données du tampon d'émission au partenaire de communication individuellement (spontanément) ou groupées. Le transfert peut être déclenché par divers évènements.

- **Prétraitement de valeurs analogiques**

  Le CP peut traiter des valeurs analogiques selon diverses méthodes.

1.5 Fonctions de sécurité des données

Industrial Ethernet Security

Industrial Ethernet Security permet de sécuriser des appareils, des cellules d'automatisation ou des segments d'un réseau Ethernet. La transmission de données via le CP peut être protégée par la combinaison de diverses mesures de sécurité contre les attaques suivantes :

- l'espionnage de données
- la manipulation de données
- les intrusions

Il est possible d'exploiter des réseaux subordonnés sécurisés via des interfaces Ethernet/PROFINET additionnelles de la CPU.

Les fonctions de sécurité des données sont utilisables indépendamment de la communication Telecontrol.

Fonctions de sécurité des données des protocoles Telecontrol

- **TeleControl Basic**
  - **Communication Telecontrol cryptée**

    En tant que fonction de sécurité des données intégrée (non configurable), le protocole crypte les données lors du transfert.

    L'intervalle d'échange de clés entre le CP et le serveur Telecontrol se configure sous STEP 7 dans le groupe de paramètres "Interface Ethernet (X1) > Options avancées > Paramètres de transmission".
  - **Mot de passe Telecontrol**

    Pour l'authentification du CP auprès du serveur Telecontrol
- **DNP3**

  Les fonctions de sécurité des données spécifiques DNP3 sont utilisables.
- **CEI 60870-5**

  Il n'existe pas de fonctions de sécurité des données spécifiques pour le protocole CEI.

Autres fonctions de sécurité des données configurables du CP

L'utilisation du CP comme module de sécurité permet à la station S7-1200 de bénéficier des fonctions de sécurité des données suivantes au niveau de l'interface vers le réseau externe :

- **Pare-feu**
  - Pare-feu IP avec Stateful Packet Inspection (couches 3 et 4)
  - Pare-feu également pour trames Ethernet "non IP" selon IEEE 802.3 (couche 2)
  - Limitation de la vitesse de transmission pour restreindre les attaques de type flooding ou DoS ("Définition de règles de filtrage de paquets IP")
  - Règles de pare-feu globales
- **VPN**

  Les options suivantes sont également praticables :
  - Communication sécurisée par tunnel IPsec

    La communication VPN permet d'établir des tunnels IPSec sécurisés pour la communication avec un ou plusieurs modules de sécurité. Le CP peut être configuré avec d'autres modules pour former des groupes VPN. Des tunnels IPsec sont alors établis entre tous les modules de sécurité d'un groupe VPN.
  - Télémaintenance via SINEMA Remote Connect

    La création d'un groupe VPN pour la communication via un serveur SINEMA RC n'est ni nécessaire ni possible. Le serveur SINEMA RC gère la communication entre les abonnés et les mécanismes de sécurité des données (OpenVPN).
- **Journalisation**

  Des évènements peuvent être enregistrés, à des fins de surveillance, dans des fichiers journal que l'outil de configuration permet de lire ou d'envoyer automatiquement à un serveur Syslog.
- **STARTTLS / SMTPS**

  Pour la transmission sécurisée d'e-mails
- **NTP (secure)**

  Pour la transmission sécurisée lors de la synchronisation d'horloge
- **SNMPv3**

  Pour la transmission à l'abri des écoutes d'informations d'analyse de réseau
- **Protection des appareils et segments de réseau**

  La fonction de sécurité du pare-feu peut s'étendre à un appareil, à plusieurs appareils ou à des segments de réseau complets.

Remarque

Installations critiques sur le plan de la sécurité - Recommandation

Exploitez les possibilités suivantes :

- Utilisez, dans les installations devant répondre à de sévères critères de sécurité, les protocoles sécurisés NTP (secure), HTTPS et SNMPv3.
- En cas de connexion à des réseaux publics, activez le pare-feu. Evaluez le pour et le contre des services par lesquels vous voulez permettre l'accès à la station via les réseaux publics. Exploitez la possibilité de "limitation de largeur de bande" offerte par le pare-feu pour restreindre les attaques par flooding ou déni de service.

Voir chapitre Recommandations de sécurité (Page 41).

Concernant la configuration des fonctions de sécurité des données, voir chapitre Security (Page 57).

Pour plus de détails sur la fonctionnalité et la configuration des fonctions de sécurité des données, voir le système d'information STEP 7.

1.6 Capacités fonctionnelles et caractéristiques de performance

Nombre de CM/CP par station

Vous pouvez embrocher et configurer par station S7-1200 jusqu'à trois CM/CP dont aux maximum trois CP 1243-1.

Ressources de connexion

- **Connexions S7 et connexions TCP / UDP / ISO-on-TCP**

  Nombre total de connexions via Industrial Ethernet : 14 au maximum
  dont :

  – S7 : 14 au maximum (y compris les connexions de routage S7)

  – TCP/IP : 14 max.

  – ISO-on-TCP : 14 max.

  – UDP : 14 max.

En complément :

- **Connexions Telecontrol**

  Le CP peut se connecter avec divers protocoles Telecontrol aux types de partenaire suivants :

  TeleControl Basic

  – à un serveur Telecontrol (TCSB) simple ou redondant

  – Communication transversale en plus

    La communication transversale entre les CP de deux stations transite toujours par le serveur Telecontrol. Elle se configure dans le groupe de paramètres "Stations partenaires" > "Partenaire de la communication transversale".

    Capacités fonctionnelles pour la communication transversale : Au total 15 max., dont :

    - envoi à des partenaires : Max. 3 (paramètre "Tampon d'émission" activé)

    - réception des partenaires : Max. 15 (paramètre "Tampon d'émission" activé)

  DNP3 / CEI 60870-5

  – Communication simultanée avec au maximum 4 partenaires

    Un partenaire est un maitre simple ou redondant ou une station (Communication directe).

    La communication directe entre stations se configure via les connexions Telecontrol.

- **Connexions en ligne**

  2 ressources pour 1 connexion en ligne à une station d'ingénierie (STEP 7)

- **Connexions PG et IHM (OP)**

  Au total 4 max., dont :

  – Ressources pour connexions PG : 1 max.

  – Ressources pour connexions IHM : 3 max.

Nombre de points de données pour la configuration de points de données

Nombre maximal de points de données configurables

- TeleControl Basic: 200
- DNP3 : 500
- CEI : 500

Données utiles

Les données à transmettre par le CP sont affectées dans la configuration STEP 7 à différents points de données.

Le volume de données utiles par point de données dépend du type de données du point de données en question (voir Types de points de données).

Mémoire de télégrammes (tampon d'émission)

Le CP possède une mémoire de télégrammes (tampon d'émission) pour les valeurs de points de données configurés comme évènement et qui doivent être transmises au partenaire de communication.

La taille maximale du tampon d'émission est de 64000 évènements, répartis à parts égales sur tous les partenaires de communication configurés. La taille du tampon de télégrammes est paramétrable sous STEP 7 (groupe de paramètres "Communication avec la CPU").

Avec le protocole TeleControl Basic, le tampon d'émission peut également être utilisé pour la communication transversale avec jusqu'à trois partenaires. La configuration s'effectue dans le groupe de paramètres "Partenaire".

Messages (e-mail)

- L'envoi d'au maximum 10 messages (e-mails) peut être configuré dans l'éditeur de messages.
- Envoi d'e-mails avec le bloc de programme TMAIL_C

Tunnel IPSec (VPN)

Il est possible d'établir jusqu'à 8 tunnels IPSec pour la communication sécurisée avec d'autres modules de sécurité.

Règles de pare-feu

Le nombre maximal de règles de pare-feu en mode de pare-feu avancé est de 256.

Les règles de pare-feu se répartissent en :

- Au maximum 226 règles à adresses individuelles
- Au maximum 30 règles à plage d'adresses ou adresses de réseau (p. ex. 140.90.120.1 - 140.90.120.20 ou 140.90.120.0/16)
- Au maximum 128 règles avec limitation de la vitesse de transmission ("Limitation de largeur de bande")

1.7 Exemples de configuration

Pour les exemples de configuration des applications Telecontrol, voir les manuels de configuration /4/ (Page 108).

Configuration avec CP assurant une coupure sûre du réseau

L'exemple suivant montre une configuration avec CP 1243-1 protégeant la station et la cellule d'automatisation subordonnée.

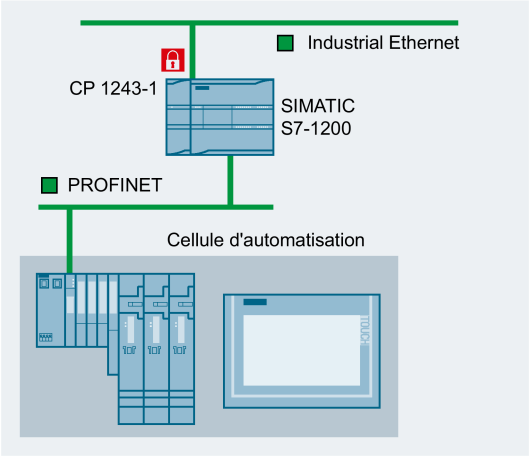


Figure 1-1 Communication sécurisée avec CP 1243-1

Configuration avec envoi d'e-mails

L'exemple suivant montre une configuration avec envoi d'e-mails. La communication Telecontrol du CP est désactivée.

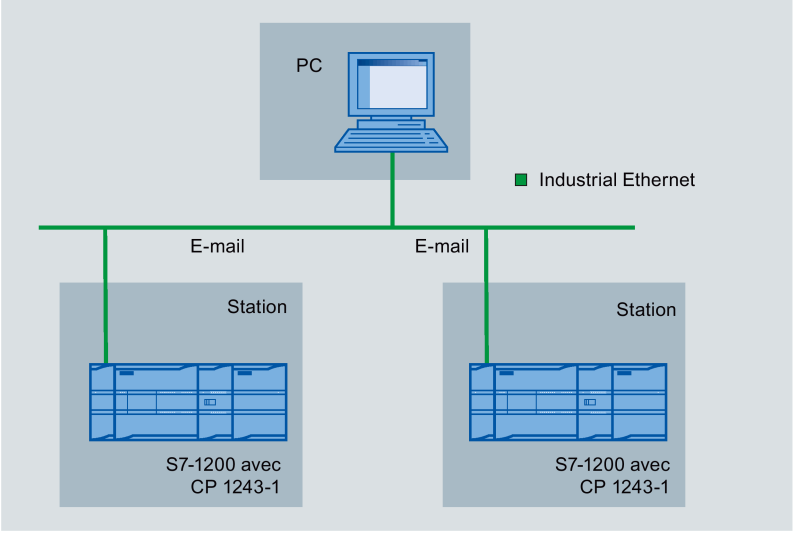


Figure 1-2 Envoi d'e-mails :

Télémaintenance avec SINEMA RC

La figure suivante montre la connexion de diverses stations avec CP de sécurité des données à une station d'ingénierie via SINEMA Remote Connect - Server.

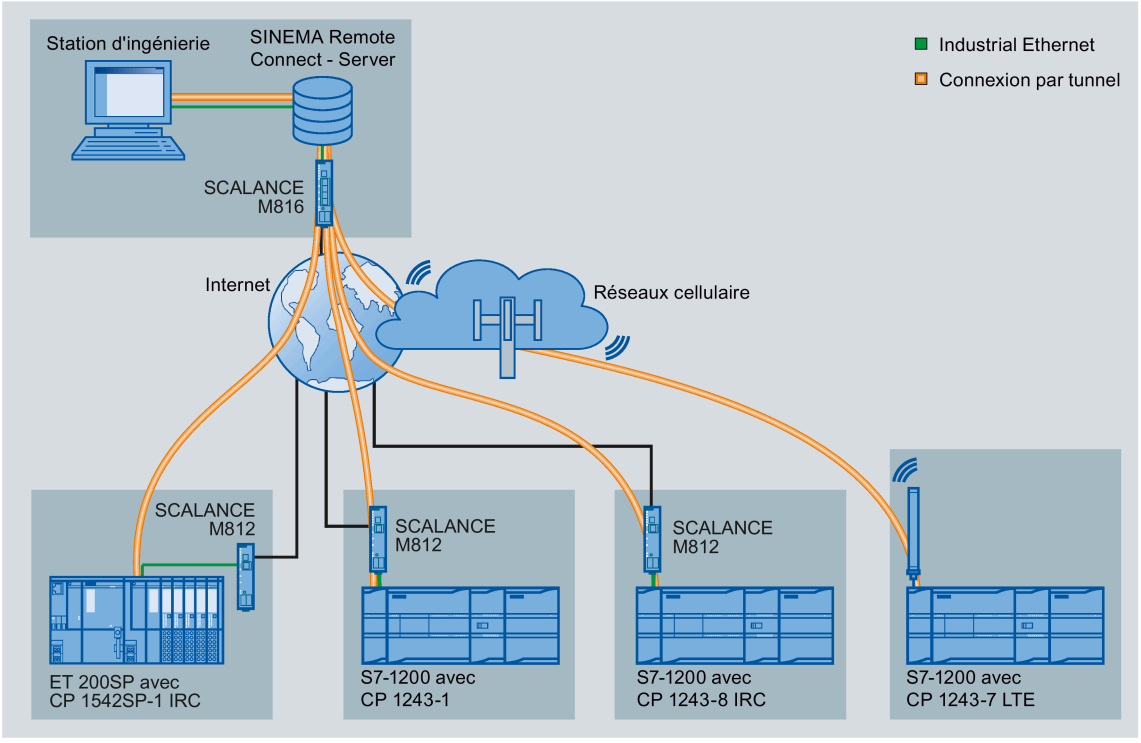


Figure 1-3 Connexion de stations à une station d'ingénierie via SINEMA RC

1.8 Conditions de mise en œuvre

1.8.1 Configuration matérielle requise

CPU 1200

Le CP est utilisable avec :

- CPU avec firmware V3 ou suivantes
- La totalité des fonctions du CP n'est disponible qu'avec une CPU à partir de V4.4.

1.8.2 Configuration logicielle requise

Logiciel de configuration et de fonctions en ligne

Pour pouvoir utiliser toutes les fonctions, la configuration du module doit être réalisée avec l'outil de configuration suivant :

- STEP 7 Basic V16

LED et connexions

2

2.1 Ouverture des volets du boîtier

Position des voyants et des connecteurs électriques

Les LED informant en détail sur les états de fonctionnement du module se trouvent derrière le volet supérieur du module.

Le connecteur Ethernet se trouve derrière le volet inférieur du module.

Ouverture des volets du boîtier

Vous ouvrez le volet supérieur ou inférieur du boîtier en le faisant basculer, vers le bas ou le haut, comme indiqué sur la figure par des flèches. Les volets se terminent par un rebord facilitant l'ouverture.

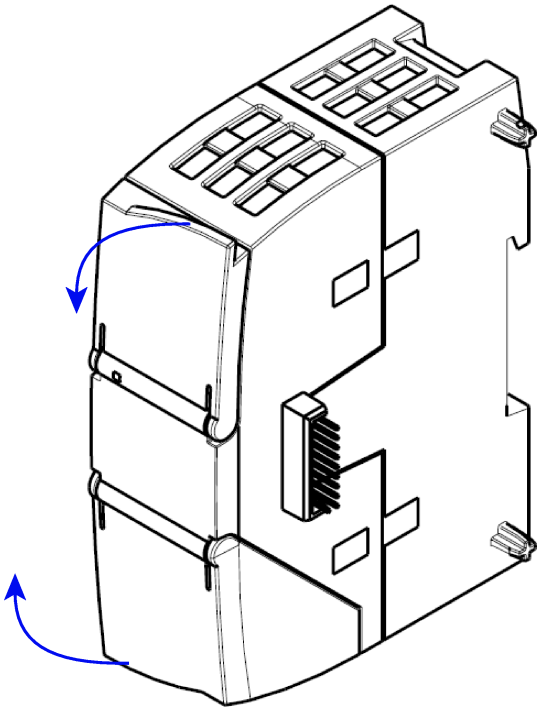


Figure 2-1 Ouverture des volets du boîtier

2.2 LED

LED du module

Le module possède diverses LED de visualisation d'état :

- **LED en face avant**

  La LED "DIAG", toujours visible, signale les états de base du module.

- **LED sous le volet supérieur**

  Les LED sous le volet supérieur précisent les informations d'état du module.

Tableau 2- 1 LED en face avant

LED / couleurs	Désignation	Signification
(rouge / vert)	DIAG	État de base du module

Tableau 2- 2 LED sous le volet supérieur

LED (couleur)	Désignation	Signification
(vert)	LINK	État de la connexion à Industrial Ethernet
(vert)	CONNECT	État des connexions au partenaire de communication
(vert)	VPN	État de la configuration VPN ou SINEMA Remote Connect
(vert)	SERVICE	État d'une connexion pour fonctions en ligne

Couleurs des LED et représentation des états de LED

Signification des symboles de LED dans les tableaux suivants :

Tableau 2- 3 Signification des symboles de LED

Symbole	○	● ●	☼ ☼ ●	-
État de la LED	Eteinte	Allumée (en permanence)	Clignotante	Sans signification

Remarque

Couleur des LED au démarrage du module

Au démarrage du module toutes les LED s'allument brièvement. Les LED polychromes visualisent une couleur mixte. A cet instant, la couleur des LED n'est pas clairement définissable.

Visualisation des états de base du CP (LED "DIAG")

Tableau 2- 4 Visualisation des états de base du CP

DIAG (rouge / vert)	**Signification** **(en cas de plusieurs points : signification alternative)**
États de base du CP	
○	• Hors tension • Défaut au démarrage
● vert	Marche (RUN) sans erreur grave
☼ clignotement vert	• Pas de connexion au partenaire • Firmware chargé avec succès
☼ clignotement rouge	• Démarrage en cours • Défaut du module • Données de projet STEP 7 non valides
● clignotement vert-rouge	Erreur de chargement du firmware

Visualisation des états de fonctionnement et de communication

Les LED visualisent l'état de fonctionnement et de communication du module selon le schéma suivant :

Tableau 2- 5 Visualisation des états de fonctionnement et de communication

DIAG (rouge / vert)	-	LINK (vert)	CONNECT (vert)	VPN (vert)	SERVICE (vert)	Signification (en cas de plusieurs points : signification alternative)
Démarrage du module (STOP → RUN) ou états d'erreur						
○		○	○	○	○	Hors tension
● rouge		●	●	●	●	Démarrage - phase 1
☼ clignotement rouge		-	○	○	○	Démarrage - phase 2
● vert		-	-	-	-	Marche (RUN) sans erreur grave
○			●	●	●	Défaut au démarrage
● rouge		-	☼	-	-	Données de projet STEP 7 non valides
☼ clignotement rouge		-	○	-	-	Données de projet STEP 7 manquantes
☼ clignotement rouge		●	☼	-	-	Erreur de bus de fond de panier
Connexion à Industrial Ethernet						
-		●	-	-	-	Connexion à Industrial Ethernet disponible
● vert		☼	-	-	-	• Etablissement de la connexion à Industrial Ethernet. • Obtention de l'adresse IP.
-		○	-	-	-	Pas de connexion à Industrial Ethernet

DIAG (rouge / vert)	-	LINK (vert)	CONNECT (vert)	VPN (vert)	SERVICE (vert)	Signification (en cas de plusieurs points : signification alternative)
Connexion aux partenaires de communication						
vert		vert	vert	-	-	Connexion établie à au moins un partenaire
vert		vert	clignotement vert	-	-	Partenaire accessible, CPU à l'état STOP
clignotement vert		vert	○	-	-	Partenaire non joignable
Connexion pour fonctions en ligne						
vert		vert	-	-	vert	Connexion pour fonctions en ligne établie
vert		vert	-	-	clignotement vert	Tentative d'établissement d'une connexion pour fonctions en ligne
vert		-	-	-	○	Pas de connexion à la station d'ingénierie
Connexion VPN / SINEMA Remote Connect						
vert		vert	-	vert	-	Connexion VPN / SINEMA Remote Connect établie
vert clignotant		vert	-	vert clignotant	-	Tentative d'établissement d'une connexion VPN / SINEMA Remote Connect configurée
-		-	-	○	-	Aucune connexion VPN / SINEMA Remote Connect configurée sur le CP ou actuellement établie
Chargement du firmware						
rouge / vert		clignotement vert	clignotement vert	clignotement vert	clignotement vert	Chargement du firmware en cours. La LED DIAG clignote rouge et vert.
clignotement vert		clignotement vert	clignotement vert	clignotement vert	clignotement vert	Le firmware a été chargé avec succès.
clignotement rouge		clignotement vert	clignotement vert	clignotement vert	clignotement vert	Erreur de chargement du firmware

2.3 Connexions électriques

2.3.1 Alimentation

Alimentation

Le CP est alimenté par le bus de fond de panier. Il n'a pas besoin d'alimentation distincte.

2.3.2 Interface Ethernet X1P1

Interface Ethernet

Le connecteur Ethernet se trouve derrière le volet inférieur du module. L'interface est un connecteur RJ45 femelle selon IEEE 802.3.

Pour le brochage et les autres caractéristiques de l'interface Ethernet voir chapitre Caractéristiques techniques (Page 99).

Montage, connexion, mise en service

3

3.1 Note importante concernant la mise en œuvre des appareils

Consignes de sécurité pour la mise en œuvre des appareils

Respectez les consignes de sécurité ci-après lors de l'installation et de l'exploitation de l'appareil ainsi que pour les travaux qui y sont liés tels que montage, connexion et échange de l'appareil.

Coupe-circuit de surtension

IMPORTANT
Protection de l'alimentation externe Si le module ou la station est alimenté par des câbles d'alimentation longs ou des réseaux de grande envergure, il se peut que les lignes d'alimentation soient parasitées par le couplage de fortes impulsions électromagnétiques telles que produites par la foudre ou par la commutation de charges importantes. La connexion à l'alimentation externe n'est pas protégée contre les fortes impulsions électromagnétiques. Il faut pour ce faire un module parasurtenseur externe. Les spécifications de la norme EN61000-4-5, à savoir essai de surtension sur les câbles d'alimentation électrique, ne sont satisfaites qu'en cas d'utilisation d'un parasurtenseur approprié. On pourra utiliser à cet effet le parasurtenseur Dehn Blitzductor BVT AVD 24, nº d'article 918 422 ou équivalent. Constructeur : DEHN+SOEHNE GmbH+Co.KG, Hans-Dehn-Str.1, Postfach 1640, D-92306 Neumarkt

3.1.1 Consignes pour une mise en œuvre en atmosphère explosible

⚠ATTENTION

DANGER D'EXPLOSION

N'OUVREZ PAS L'APPAREIL TANT QU'IL EST SOUS TENSION.

⚠ATTENTION

L'utilisation de l'appareil n'est permise que dans un environnement de classe de pollution 1 ou 2 (cf. CEI 60664-1).

⚠ATTENTION

Cet appareil est conçu pour fonctionner à une très basse tension de sécurité (Safety Extra-Low Voltage, SELV) fournie par une alimentation électrique à puissance limitée (Limited Power Source, LPS).

C'est pourquoi on ne doit connecter aux bornes d'alimentation que des très basses tensions de sécurité (TBTS) à puissance limitée (Limited Power Source, LPS) selon CEI 60950-1 / EN 60950-1 / VDE 0805-1 ou n'utiliser qu'un bloc d'alimentation de l'appareil conforme à NEC Class 2 de la norme National Electrical Code (r) (ANSI / NFPA 70).

Si l'appareil est connecté à une alimentation électrique redondante (deux alimentations séparées), les deux alimentations doivent être conformes.

⚠ATTENTION

DANGER D'EXPLOSION

IL EST INTERDIT, DANS UN ENVIRONNEMENT FACILEMENT INFLAMMABLE OU COMBUSTIBLE, DE CONNECTER DES CÂBLES À L'APPAREIL OU DE LES DÉCONNECTER.

⚠ATTENTION

DANGER D'EXPLOSION

L'ÉCHANGE DE COMPOSANTS PEUT PORTER PRÉJUDICE À LA CONFORMITÉ À CLASS I, DIVISION 2 OU ZONE 2.

⚠ATTENTION

En cas d'utilisation en atmosphère explosible selon Class I, Division 2 ou Class 1, Zone 2, l'appareil doit être incorporé à une armoire électrique ou à un boîtier.

3.1.2 Consignes pour une mise en œuvre en atmosphère explosible selon ATEX / IECEx

⚠ATTENTION

Spécifications de l'armoire électrique

Pour être conforme à la directive 2014/34 (ATEX 114) de l'UE et aux conditions de l'IECEx, le boîtier ou l'armoire électrique doit satisfaire pour le moins aux exigences IP 54 (de la norme EN 60529) selon EN 60079-7.

⚠ATTENTION

Conducteur

Si la température régnant au niveau du câble ou du connecteur du boîtier est supérieure à 70 °C ou si la température au niveau de l'embranchement des conducteurs du câble est supérieure à 80 °C, des dispositions particulières doivent être prises. Si l'appareil est utilisé à une température ambiante supérieure à 50 °C, vous devrez utiliser des câbles agréés pour une température de service d'au moins 80 °C.

⚠ATTENTION

Prenez les mesures qui s'imposent pour empêcher des surtensions transitoires supérieures à 40% de la tension nominale. Cette condition est remplie si vous alimentez les appareils exclusivement en TBTS (très basse tension de sécurité).

3.1.3 Consignes pour une mise en œuvre en atmosphère explosible conformément à UL HazLoc

⚠ATTENTION

DANGER D'EXPLOSION

Ne déconnectez pas l'appareil d'un câble sous tension avant de vous être assuré qu'il n'existe pas d'atmosphère explosible dans les environs.

Cet appareil est uniquement conçu pour une utilisation dans un environnement conforme à Class I, Division 2, Groups A, B, C et D et dans des atmosphères non explosibles.

Cet appareil est uniquement conçu pour une utilisation dans un environnement conforme à Class I, Zone 2, Group IIC et dans des atmosphères non explosibles.

3.1.4 Consignes pour une mise en œuvre en atmosphère explosible conformément à FM

⚠ATTENTION

DANGER D'EXPLOSION

Le branchement ou débranchement de câbles électriques conducteurs n'est autorisé que si l'alimentation est coupée ou que si l'appareil se trouve dans une zone exempte de concentrations de gaz inflammables.

Cet appareil est uniquement conçu pour une utilisation dans un environnement conforme à Class I, Division 2, Groups A, B, C et D et dans des atmosphères non explosibles.

Cet appareil est uniquement conçu pour une utilisation dans un environnement conforme à Class I, Zone 2, Group IIC et dans des atmosphères non explosibles.

⚠ATTENTION

DANGER D'EXPLOSION

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

3.2 Montage, connexion et mise en service

Préparatifs du montage et de la mise en service

⚠PRUDENCE

Lisez le manuel système "Automate programmable S7-1200"

Avant de procéder au montage, à la connexion et à la mise en service, lisez les sections correspondantes du manuel système "Automate programmable S7-1200", voir références bibliographique en annexe.

Effectuez le montage et la connexion comme indiqué dans les descriptions du manuel système "Automate programmable S7-1200 ".

Débrochage/Embrochage du module

IMPORTANT
Mise hors tension de la station en cas de débrochage/embrochage du module
Coupez toujours l'alimentation de la station avant de débrocher ou d'embrocher le module.

Dimensions pour le montage

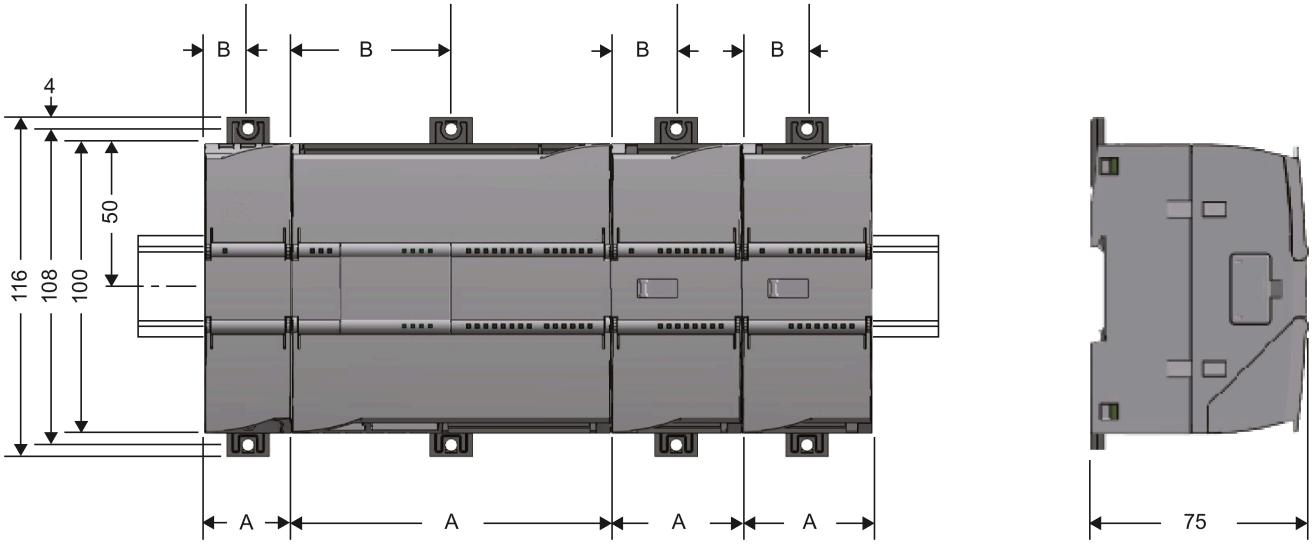


Figure 3-1 Cotes d'encastrement du S7-1200

Tableau 3- 1 Dimensions pour le montage (mm)

Appareils S7-1200		Largeur A	Largeur B *
CPU (exemples)	CPU 1211C, CPU 1212C	90 mm	45 mm
	CPU 1214C	110 mm	55 mm
Interfaces de communication (exemples)	CM 1241, CM 1243-5, CM 1242-5	30 mm	15 mm
	CP 1242-7, CP 1243-1, CP 1243-7, CP 1243-8 IRC	30 mm	15 mm

* Largeur B : Distance entre le bord du boîtier et le centre du trou du clip de rail symétrique

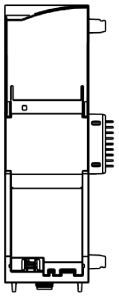
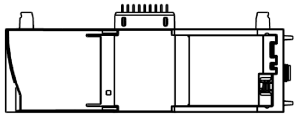
Vous trouverez les cotes détaillées du module au chapitre Dessins cotés (Page 105).

Clips pour rail symétrique, montage en tableau

Les CPU, SM, CM et CP peuvent être montés sur rail symétrique DIN (35 mm) en armoire électrique. Utilisez les clips extractibles de rail symétrique pour fixer l'appareil sur le rail symétrique. Ces clips s'enclenchent également en position tirée afin de permettre le montage sur tableau de commande. Le diamètre intérieur du trou pour les clips de rail symétrique est de 4,3 mm.

Position de montage

IMPORTANT
Position de montage Veillez lors du montage à ne pas obstruer les fentes d'aération en haut et en bas du module afin de permettre une bonne ventilation. Ménagez un espace libre de 25 mm au-dessus et au-dessous de l'appareil pour permettre à l'air de circuler et protéger l'appareil contre la surchauffe. Tenez compte des plages de température admissibles en fonction de la position de montage. Les plages de température admissibles sont indiquées au chapitre Caractéristiques techniques du CP 1243-1 (Page 99).

Position de montage / plage de température admissible	Position de montage
Montage horizontal du châssis	
Montage vertical du châssis :	

Condition requise : Configuration avant mise en service

La mise en service complète du module présuppose que vous disposiez de toutes les données du projet STEP 7 (voir ci-dessous, étape 5).

Montage, connexion et mise en service du module

Remarque

Connexion uniquement lorsque l'appareil est hors tension

Mettez les équipements hors tension avant d'effectuer le câblage du S7-1200.

Tableau 3- 2 Marche à suivre pour le montage et la connexion

Etape	Exécution	Notes et explications
1	Posez le CM sur le rail symétrique et raccordez-le au module voisin à sa droite.	Utilisez un rail symétrique DIN de 35 mm. Les emplacements admissibles se trouvent à gauche de la CPU.
2	Fixez le rail symétrique.	
3	Connectez le câble Ethernet au CP.	Vous trouverez le brochage de l'interface au chapitre Caractéristiques techniques (Page 99).
4	Mettez sous tension.	
5	La mise en service se poursuit par le chargement des données de projet STEP 7.	Les données de projet STEP 7 du CP sont chargées pendant le chargement de la station. Pour charger la station, connectez la station d'ingénierie, sur laquelle se trouve les données de projet, à l'interface Ethernet de la CPU. Pour plus de détails concernant le chargement, veuillez vous référer aux chapitres ci-après du système d'information STEP 7 : • "Chargement des données de projet" • "Utilisation des fonctions en ligne et des fonctions de diagnostic"
6	Refermez les volets du module et laissez-les fermés durant le fonctionnement.	

Réglage manuel de l'heure lors de la mise en service

Remarque

Synchronisation d'horloge en mode sécurité des données / SINEMA RC

En cas d'utilisation des fonctions de sécurité des données, SINEMA Remote Connect par exemple, le CP a besoin de l'heure actuelle pour l'authentification auprès du serveur SINEMA RC.

Le module se procure cette heure auprès de la CPU ou d'un serveur NTP avant le premier établissement d'une connexion.

Recommandation :

Lors de la mise en service, réglez au moins une fois l'heure de la CPU manuellement à l'aide des fonctions en ligne de STEP 7. Ceci est notamment nécessaire si vous avez configuré pour la synchronisation d'horloge l'option "Heure du partenaire". Vous avez ainsi l'assurance qu'au démarrage la CPU possède une heure valide et que le CP est en mesure d'échanger les certificats requis avec le partenaire ou le serveur SINEMA RC.

3.3 Note relative à l'utilisation

IMPORTANT
Fermeture des volets en face avant Pour assurer le bon fonctionnement du module, maintenez les volets de face avant fermés durant son fonctionnement.

Configuration

4

4.1 Recommandations de sécurité

Conformez-vous aux recommandations de sécurité des données ci-après pour empêcher toute intrusion dans le système.

Si la communication Telecontrol est activée, conformez-vous également aux instructions du manuel de configuration correspondant.

Généralités

- Assurez-vous régulièrement que l'appareil est conforme aux présentes recommandations et aux éventuelles stratégies de sécurité des données internes.
- Procédez à une évaluation globale de la sécurité des données de votre installation. Mettez en place un concept de protection cellulaire avec des produits appropriés.
- Ne connectez pas l'appareil directement à Internet. Exploitez l'appareil au sein d'une zone protégée du réseau.
- Informez-vous régulièrement sur les nouveautés sur les sites Internet Siemens.
  - Vous trouverez ici des informations sur Industrial Security :
    Lien : (http://www.siemens.com/industrialsecurity)
  - Vous trouverez un choix de documents sur la sécurité des réseaux ici :
    Lien : (https://support.industry.siemens.com/cs/ww/fr/view/92651441).
- Veillez à ce que le firmware soit à jour. Informez-vous régulièrement sur les mises à jour de sécurité et appliquez-les.

  Vous trouverez à l'adresse suivante des informations sur les nouveaux produits et les nouvelles versions de firmware :
  Link: (https://support.industry.siemens.com/cs/ww/fr/ps/21764/dl)

Accès physique

Limitez l'accès physique à l'appareil au seul personnel qualifié.

Connexion au réseau

Ne connectez pas le CP directement à Internet. Si vous souhaitez connecter le CP à Internet, intercalez des systèmes de protection adéquats, un SCALANCE S avec pare-feu p. ex ou utilisez le CP.

Fonctions de sécurité des données du produit

Utilisez les possibilités des paramétrages de sécurité des données dans la configuration du produit. En font notamment partie :

- Niveaux de protection

  Configurez un niveau de protection de la CPU.

  Vous trouverez des instructions à ce sujet dans le système d'information de STEP 7.

- Fonction de sécurité des données de la communication
  - Activez les fonctions de sécurité des données du CP et configurez le pare-feu.

    En cas de connexion à des réseaux publics, activez le pare-feu. Évaluez le pour et le contre des services par lesquels vous voulez permettre l'accès à la station via les réseaux publics. La limitation de la "Vitesse de transmission" via les règles de filtre de paquets IP du pare-feu permet de restreindre les attaques par flooding et déni de service.
  - Utilisez les variantes de protocole sécurisées NTP (secure) et SNMPv3.
  - Utilisez les fonctions de sécurité des données des protocoles Telecontrol.
  - Laissez l'accès au serveur Web de la CPU désactivé.
- Protection des mots de passe d'accès aux blocs de programme

  Protégez l'accès aux mots de passe enregistrés dans des blocs de données pour les blocs de programme. Vous trouverez des informations sur la marche à suivre dans le système d'information de STEP 7 sous le mot-clé "Protection de savoir-faire".
- Fonctions de journalisation

  Activez la fonction via la configuration de sécurité des données et vérifiez régulièrement dans les évènements journalisés qu'il n'y a pas d'intrusion.

Mots de passe

- Définissez des règles d'utilisation des appareils et d'attribution de mots de passe.
- Actualisez régulièrement les mots de passe pour accroître la sécurité.
- Utilisez exclusivement des mots de passe à force élevée. Evitez d'utiliser des mots de passe faibles tels que "motdepasse1", "123456789" ou équivalents.
- Veuillez vous assurer que tous les mots de passe sont protégés et inaccessibles à toute personne non autorisée.

  Voir aussi la section précédente.
- N'utilisez pas le même mot de passe pour différents utilisateurs et systèmes.

Protocoles

Protocoles sûrs et peu sûrs

- Activez uniquement les protocoles nécessaires à la mise en œuvre du système.
- Utilisez des protocoles sûrs si l'appareil n'est pas sécurisé par des mesures de protection physiques.
  - Le protocole NTP offre avec NTP (secure) une alternative sûre si vous n'utilisez pas la communication Telecontrol.
  - Le protocole HTTP offre, avec HTTPS, une alternative sûre lors de l'accès au serveur Web (configuration sous la CPU).

Tableau : Signification des titres de colonne et entrées :

Le tableau ci-après vous donne un aperçu des ports ouverts de cet appareil.

- **Protocole / fonction**

  Protocoles pris en charge par l'appareil.
- **Numéro de port (protocole)**

  Numéro de port affecté au protocole.
- **Paramètre par défaut du port**
  - Ouvert

    Le port est ouvert en début de configuration.
  - Fermé

    Le port est fermé en début de configuration.
- **État du port**
  - Ouvert

    Le port est toujours ouvert et ne peut pas être fermé.
  - Ouvert après configuration

    Le port est ouvert, s'il a été configuré.
  - Ouvert (connexion, si configurée)

    Le port est ouvert par défaut. Après configuration du port, le partenaire de communication doit se connecter.
  - Fermé après configuration

    Le port est fermé car le CP est toujours client pour ce service.
- **Authentification**

  Indique si le protocole authentifie le partenaire de communication durant l'accès.

Protocole / fonction	Numéro de port (protocole)	Paramètre par défaut du port	État du port	Authentification
DNP3	20000 (TCP/UDP)	Fermé	Ouvert après configuration	Oui, si Secure Authentication est activée.
CEI	2404 (TCP)	Fermé	Ouvert après configuration	Non
Connexions S7 et connexions en ligne	102 (TCP)	Fermé	Ouvert après configuration *	Non
Diagnostic de sécurité des données en ligne (si pris en charge)	102 (TCP)	Ouvert	Ouvert après configuration *	Non
Communication via SINEMA RC (si prise en charge)	443 (TCP)	Fermé	Ouvert après configuration	Oui
HTTP	80 (TCP)	Fermé	Ouvert après configuration	Oui
HTTPS	443 (TCP)	Fermé	Ouvert après configuration	Oui
SNMP (si pris en charge)	161 (UDP)	Ouvert	Ouvert après configuration	Oui (sous SNMPv3)
Syslog	514 (UDP)	Fermé	Ouvert après configuration	Non

***** Certains opérateurs de service reprochent à l'ouverture du port 102 de constituer une faille de sécurité.
Pour éviter l'ouverture du port 102 lors du diagnostic en ligne, voir chapitre Diagnostic de sécurité en ligne via le port 8448 (Page 93).

Ports des partenaires de communication et des routeurs

N'oubliez pas d'autoriser, sur les partenaires de communication et les routeurs intercalés, les ports client requis dans les pare-feux respectifs.

Il peut s'agir, si pris en charge ou utilisés, de :

- TeleControl Basic / 55097 (TCP)
- DNS / 53 (UDP)
- DHCP / 67, 68 (UDP)
- NTP / 123 (UDP)
- SMTP / 25 (TCP)
- STARTTLS / 587 (TCP)
- SSL/TLS / 465 (TCP)
- SINEMA RC Configuration automatique / 443 (TCP) - paramétrable
- SINEMA RC et OpenVPN / 1194 (UDP) - paramétrables sous SINEMA RC
- IPSec / 500 (TCP)
- Syslog / 514 (UDP)

4.2 Configuration sous STEP 7

Configuration sous STEP 7

La configuration des modules et réseaux s'effectue sous SIMATIC STEP 7. Vous trouverez la version requise au chapitre Configuration logicielle requise (Page 25).

Vous pouvez configurer au maximum trois CM/CP par station.

La description ci-après vaut pour les applications sans communication Telecontrol.

Configuration de la communication Telecontrol

La description de la configuration de la communication Telecontrol figure dans les manuels de configuration /4/ (Page 108).

Récapitulatif des étapes de configuration sous STEP 7

Pour la configuration, procédez comme suit :

1. Créez un projet STEP 7.
2. Créez les stations SIMATIC requises avec les modules et CP nécessaires.
3. Créez un réseau Ethernet.
4. Connectez les stations au sous-réseau Ethernet.
5. Configurez les CP, y compris les messages (e-mails).
6. Créez, si vous le souhaitez, les blocs de programme pour la communication S7 et l'Open User Communication, puis paramétrez-les.
7. Enregistrez et compilez le projet.
8. Chargez les données de projet sur les stations

   La fonction "Charger sur l'appareil" charge sur la CPU voulue les données de projet STEP 7 y compris les données de configuration des CP.

Pour plus d'informations sur la configuration du CP , veuillez vous référer au système d'information STEP 7 ainsi qu'aux chapitres ci-après.

Chargement et enregistrement des données de configuration

Lors du chargement de la station, les données de projet de la station, y compris les données de configuration du CP sont enregistrées sur la CPU.

Vous trouverez des informations sur le chargement de la station dans le système d'information STEP 7.

4.3 Types de communication

Groupe de paramètres "Modes de communication"

Ce groupe de paramètres permet d'activer les services de communication du CP.

Pour minimiser le risque d'intrusion dans la station, vous devez activer individuellement les services de communication à utiliser par le CP. Vous pouvez activer toutes les options, mais vous devez activer au moins une option.

Il n'est pas nécessaire d'activer l'Open User Communication, car vous devez pour ce faire créer activement les blocs de programme requis. Un accès involontaire au CP est donc exclu.

- **Activer la communication Telecontrol**

  Active sur le CP la communication Telecontrol.

  Le choix du protocole Telecontrol s'effectue dans la zone de liste déroulante "Type de protocole".

  – TeleControl Basic

  – DNP3

  – CEI 60870-5

  Veuillez noter qu'en cas de modification ultérieure du protocole Telecontrol tous les paramètres spécifiques protocole seront supprimés. En font partie notamment les informations de points de données et de partenaires.

  Pour plus d'informations, voir les manuels de configuration /4/ (Page 108).

- **Activer la communication Telecontrol via SINEMA Remote Connect**

  Pour plus d'informations, voir les manuels de configuration /4/ (Page 108).

  Pour la télémaintenance via SINEMA Remote Connect, voir chapitre SINEMA Remote Connect (Page 68).

- **Activer les fonctions en ligne**

  Autorise sur le CP l'accès à la CPU pour les fonctions en ligne (diagnostic, chargement des données de projet, etc.). Lorsque la fonction est activée, la station d'ingénierie peut accéder à la CPU via le CP.

  Si cette option est désactivée, les fonctions en ligne ne permettent pas d'accéder à la CPU via le CP: Le diagnostic en ligne de la CPU avec connexion directe à l'interface de la CPU reste cependant possible.

- **Activer la communication S7**

  Active dans le CP les fonctions de la communication S7 avec la CPU de la station et le routage S7.

  Si vous configurez des connexions S7 à la station en question, qui transitent via le module de communication, vous devez activer cette option sur le module de communication.

4.4 Synchronisation d'horloge

Remarque

Synchronisation d'horloge en cas d'utilisation de SINEMA RC.

Si le CP obtient l'heure de la CPU et si vous utilisez SINEMA Remote Connect durant la mise en service, réglez l'heure de la CPU manuellement, voir note du chapitre Montage, connexion et mise en service (Page 36).

Remarque

Synchronisation d'horloge du CP

Les applications exigeant une synchronisation d'horloge imposent une synchronisation de l'horloge du CP à intervalles réguliers. Si vous ne synchronisez pas régulièrement l'horloge du CP, il se peut que l'heure du CP dérive de quelques secondes par jour.

Les fonctions de sécurité des données étant activées, activez la synchronisation d'horloge.

Remarque

Recommandation pour le réglage de la date/heure

Il est recommandé de procéder à une synchronisation avec une horloge externe toutes les 10 secondes. Ceci permet de maintenir l'écart de l'heure interne par rapport à l'heure UTC aussi faible de possible.

Synchronisation d'horloge sur S7--1200

En cas d'utilisation d'une source de l'heure externe, la station S7-1200 peut obtenir l'heure actuelle aussi bien via la CPU que via un CP.

Remarque

Recommandation : synchronisation d'horloge par 1 module seulement

Veillez à ce que la synchronisation d'horloge de la station par une source externe ne soit assurée que par un seul module de la station pour que l'heure au sein de la station soit cohérente.

Si la CPU obtient l'heure du CP, désactivez la synchronisation d'horloge de la CPU.

Sur un CP S7-1200, l'heure n'est pas retransmise au sous-réseau.

Groupes de paramètres pour la synchronisation d'horloge

Vous pouvez configurer la synchronisation d'horloge dans les groupes de paramètres suivants :

- **Interface Ethernet**

  La configuration s'effectue ici en respectant les conditions suivantes :

  – la communication Telecontrol est désactivée

  – les fonctions de sécurité des données sont désactivées.

- **Security**

  Procédez ici à la configuration si les fonctions de sécurité des données sont activées.

Méthodes de synchronisation selon l'utilisation du CP

Selon l'utilisation de la communication Telecontrol ou des fonctions de sécurité des données, vous pouvez sélectionner les méthodes de synchronisation suivantes :

- **Communication Telecontrol activée, fonctions de sécurité des données désactivées**
  - NTP
  - Heure de la CPU
- **Communication Telecontrol désactivée, fonctions de sécurité des données activées**
  - NTP
  - NTP (secure)
  - Heure de la CPU
- **Communication Telecontrol et fonctions de sécurité des données activées**
  - Heure du partenaire
  - NTP
  - NTP (secure)
  - Heure de la CPU

Méthode de synchronisation du CP

Le CP prend en charge les méthodes de synchronisation d'horloge suivantes :

- **NTP**

  L'heure est fournie par un serveur NTP connecté au réseau.

  Cette méthode peut également être utilisée si la communication Telecontrol est activée.

  Sur les CP à firmware V3 ou suivantes, l'adresse du serveur NTP peut également être entrée sous forme d'URL, par ex. <ntp.server.com>. Il faut pour ce faire un serveur DNS.

- **NTP (secure)**

  La méthode sécurisée NTP (secure) est également utilisable si les fonctions de sécurité des données sont activées. Elle utilise l'authentification par clés symétriques. Il existe plusieurs algorithmes de hachage pour effectuer le contrôle d'intégrité.

  Dans les paramètres de sécurité globaux, vous pouvez créer et gérer des serveurs NTP de type NTP (secure).

  Les serveurs à utiliser doivent être définis sur le CP.

- **Heure de la CPU**

  Les CPU V4.2 et suivantes peuvent synchroniser tous les CM/CP de la station durant un cycle de synchronisation de 10 secondes.

  Paramètres de la CPU :
  L'option "La CPU synchronise les modules de l'appareil" permet de spécifier la synchronisation de tous les CP Telecontrol à firmware ≥ V2.1.77 de la station avec l'horloge de la CPU selon un cycle de 10 secondes.

- **Pas de synchronisation d'horloge configurée**

  Si aucune synchronisation d'horloge n'a été configurée sur le CP, l'heure du CP peut être synchronisée si la condition suivante est remplie :

  Si l'option "La CPU synchronise les modules de l'appareil" est activée sous "Interface PROFINET > Synchronisation d'horloge" sur la CPU, tous les CM/CP de la station sont synchronisés avec l'horloge de la CPU.

- **Heure du partenaire**

  Si la communication Telecontrol est activée : Le CP adopte l'heure du partenaire de communication.

  Vous trouverez la description dans le Manuel de configuration /4/ (Page 108).

Retransmission de l'heure du CP à la CPU

Remarque

Retransmission de l'heure à la CPU

Selon la version de firmware des modules concernés, l'heure du CP est retransmise de différentes manières à la CPU :

- Retransmission de l'heure du CP à la CPU via une variable d'API
- Retransmission de l'heure du CP à la CPU via le bus interne

La retransmission de l'heure du CP à la CPU dépend de la version de firmware du CP et de la CPU. Tenez compte du comportement suivant.

- **Firmware du CP < V3**

  Avec cette version de firmware, l'heure du CP peut être transmise facultativement à la CPU via une variable d'API. Si cette variable d'API est lue cycliquement par la CPU, la CPU adopte l'heure du CP.

  Dans le groupe de paramètres "Communication avec la CPU", vous pouvez spécifier la mise à disposition de la CPU de l'heure courante du CP via une variable d'API. Concernant les variables d'API, voir le groupe de paramètres "Communication avec la CPU" du CP.

- **Firmware du CP ≥ V3.0 et firmware de la CPU ≥ V4.2**

  Si les deux modules possèdent sur une station l'une des versions de firmware précitées, l'heure du CP peut être retransmise automatiquement à la CPU.

  Condition requise : Sur la CPU, sous "Interface PROFINET > Synchronisation d'horloge", l'option "La CPU synchronise les modules de l'appareil" est activée.

  Tous les modules intelligents de la station sont alors synchronisés avec l'horloge de la CPU.

  La CPU adoptant automatiquement l'heure du CP, vous n'avez plus besoin de l'option de retransmission via la variable d'API.

4.5 Interface Ethernet

4.5.1 Adresses Ethernet

Adresses Ethernet

Les groupes de paramètres suivants permettent de mettre l'interface Ethernet en réseau et de configurer les paramètres d'adresse IP.

Dans les groupes de paramètres sous Options avancées > Port [Xn P1], configurez l'interconnexion des ports et les propriétés de transmission.

Pour plus d'informations, voir le système d'information STEP 7.

4.5.2 IPv6

Configuration manuelle d'adresses IPv6

Si vous configurez en supplément des adresses IPv6 (option "Configuration manuelle"), veuillez vous assurer que les deux adresses IPv6 appartiennent à des sous-réseaux distincts.

Vous trouverez des informations sur la configuration dans le système d'information de STEP 7.

Partenaires de communication et IPv6

Remarque

Communication Internet via IPv6

Si vous voulez utiliser des adresses IPv6 et connecter le CP à Internet, veuillez vous assurer que le routeur connecté à Internet et les fournisseurs des services Internet utilisés (la messagerie par ex.) prennent également en charge les adresses IPv6.

Communication OUC via IPv6

Si vous utilisez des blocs de l'Open User Communication utilisation und si vous activez IPv6, veuillez vous assurer que les partenaires de communication supportent également IPv6. Lors de requêtes adressées à des serveurs DNS, les adresses IPv6 retournées sont utilisées en priorité par rapport aux adresses IPv4.

4.5.3 Identification du CP

Le groupe de paramètres n'est disponible que si la communication Telecontrol est activée. Pour plus d'informations, voir les manuels de configuration /4/ (Page 108).

4.5.4 Synchronisation d'horloge

Synchronisation d'horloge

Pour la synchronisation d'horloge, veuillez lire le chapitre de niveau supérieure Synchronisation d'horloge (Page 47).

4.5.5 Options avancées

Surveillance de connexion TCP

Le paramétrage effectué ici s'applique à toutes les connexions TCP configurées du CP.

- **Temps de surveillance de connexion TCP**

  Fonction : Si aucun trafic de données n'a lieu durant le temps de surveillance de connexion TCP, le module de communication envoie un télégramme keep alive au partenaire de communication et attend sa réponse avant écoulement du temps de surveillance keep alive TCP.

  Paramétrage par défaut : 180 s. Plage admissible : 1...65535 s

- **Temps de surveillance keep alive TCP**

  Après avoir envoyé un télégramme keep alive, le module de communication attend une réponse du partenaire de communication avant écoulement du temps de surveillance keep alive. Si le module ne reçoit pas de réponse durant le temps configuré, il coupe la connexion, puis tente de la rétablir.

  Paramétrage par défaut : 10 s. Plage admissible : 1...65535 s

Paramètres de transmission

Les paramètres spécifiques protocole ne sont visibles que si la communication Telecontrol est activée. Pour plus d'informations, voir les manuels de configuration /4/ (Page 108).

4.5.6 Accès au serveur Web

Accès au serveur Web de la CPU

Le serveur Web du S7-1200 se trouve sur la CPU. Le CP donne accès au serveur Web de la CPU.

Vous pouvez accéder à partir d'un PC au serveur Web de la station via le réseau local.

Vous trouverez des informations sur le serveur Web dans le manuel /1/ (Page 107).

Pour les particularités de l'accès aux serveurs Web en cas d'utilisation du protocole TeleControl Basic, voir le manuel de configuration /4/ (Page 108)

Pour plus d'informations sur le serveur Web du S7-1200 voir le manuel /1/ (Page 107).

4.6 Stations partenaires

Le groupe de paramètres n'est affiché que si la communication Telecontrol est activée.

4.7 Configuration DNS

Serveur DNS

Un serveur DNS peut être nécessaire si le module même ou le module NTP, un partenaire de communication ou un serveur de messagerie par exemple doit être joignable via un nom d'hôte (FQDN).

Si vous voulez adresser un partenaire de communication par FQDN, configurez un serveur DNS. L'adresse IP (IPv4/IPv6) du partenaire de communication est alors déterminée par le serveur DNS configuré.

En cas d'utilisation d'adresses IPv6, veillez à configurer le serveur DNS en conséquence.

4.8 Communication avec la CPU

4.8.1 Communication avec la CPU

Communication avec la CPU

Les 4 premiers paramètres sont uniquement significatifs pour la communication Telecontrol.

Bit de chien de garde

- **Surveillance du CP**

  Le bit de chien de garde sert au CP à contrôler la connexion à la CPU.

  Le CP transmet le bit toutes les 5 secondes à la CPU et le remet à zéro au cours du prochain cycle de balayage de la CPU. En cas de dérangement de la connexion, le bit n'est pas transmis. Le dérangement de la connexion est ainsi signalé à la CPU.

  La variable d'API du bit de chien de garde doit être traitée par le programme utilisateur.

Heure du CP

- **Heure du CP à la CPU**

  La fonction permet à la CPU de lire l'heure du CP. C'est ainsi que le CP peut synchroniser l'horloge de la CPU.

  Déroulement :

  – La CPU met l'entrée "variable de déclenchement d'horodatage" (BOOL) à 1 via le programme utilisateur.

  – Le CP inscrit alors son heure dans la "variable d'horodatage du CP" (DTL) et remet la valeur de la "variable de déclenchement d'horodatage" à 0.

  – Le programme utilisateur lit la "variable d'horodatage du CP" pour régler l'heure de la CPU.

  Recommandation :
  N'activez la "Variable de déclenchement d'horodatage" pas plus d'une fois par seconde pour éviter de surcharger inutilement le bus interne par une communication excessive.

Remarque

Conformez-vous aux instructions du chapitre Synchronisation d'horloge (Page 47).

4.8.2 Diagnostic CP

Les fonctions sont supportées par un CP à version de firmware à partir de V3.

Diagnostic CP

Le groupe de paramètres "Diagnostic CP" permet de fournir à la CPU des données du diagnostic avancé du CP à l'aide de variables d'API.

Vous pouvez afficher les états des variables d'API à l'aide du serveur Web de la CPU.

- **Activer diagnostic CP avancé**

  Activez l'option pour utiliser le diagnostic avancé du CP.

  Si l'option est activée, il faut configurer au moins la "Variable de déclenchement de diagnostic".

  Les variables d'API ci-après des diverses données de diagnostic peuvent être activées sélectivement.

- **Variable de déclenchement de diagnostic**

  Si la variable d'API (BOOL) du programme utilisateur de la CPU est mise à 1, le CP actualise les valeurs des variables d'API suivantes pour le diagnostic avancé.

  Après écriture des valeurs actuelles dans les variables d'API suivantes, le CP met la "Variable de déclenchement de diagnostic" à 0 et signale ainsi à la CPU que les valeurs actualisées de variables d'API peuvent être lues.

  Remarque
  Mise à 1 rapide de la variable de déclenchement de diagnostic

  Ne pas activer les déclencheurs plus souvent qu'une fois par seconde.

Selon le type de CP et les fonctions prises en charge, vous pouvez configurer des variables d'API pour les données de diagnostic suivantes :

- **Avertissement de débordement de la mémoire de télégrammes**

  - Uniquement significatif pour la communication Telecontrol -

- **Mémoire de télégrammes utilisée**

  - Uniquement significatif pour la communication Telecontrol -

- **Adresse IP momentanée**

  Variable d'API (type de données String) pour l'adresse IP momentanée de l'interface du CP.

- **Date de connexion réussie à TCSB**

  - Uniquement significatif pour la communication Telecontrol -

- **Date d'échec de connexion à TCSB**

  - Uniquement significatif pour la communication Telecontrol -

- **État du TeleService**

  - Uniquement significatif pour la communication Telecontrol -

- **État VPN-IPsec**

  La variable d'API (BOOL) indique si un tunnel VPN-IPsec est établi :

  – 0 = aucun tunnel établi

  – 1 = tunnel établi

- **Connexion à SINEMA Remote Connect**

  La variable d'API (BOOL) indique si un tunnel OpenVPN est établi vers SINEMA RC :

  – 0 = aucun tunnel établi

  – 1 = tunnel établi

4.9 SNMP

SNMP

Le CP prend en charge les versions suivantes de SNMP :

- **SNMPv1**

  Disponible si les fonctions de sécurité de données sont activées ou désactivées.

  Veuillez noter que dans ce cas, il est possible d'accéder au module aussi bien en lecture qu'en écriture. Il n'est pas possible d'effectuer dans ce cas d'autres paramétrages.

  La configuration des Community-Strings est uniquement possible si les fonctions de sécurité sont activées.

  Le CP utilise par défaut les Community Strings suivants pour l'authentification de l'accès via SNMPv1 à ses agents SNMP :

Accès à un agent SNMP sur le CP	Community-String d'authentification pour SNMPv1 *)
Accès en lecture	public
Accès en lecture et écriture	private

*) Veillez à effectuer les entrées en minuscules !

Remarque

Sécurité de l'accès

Modifiez, pour des raisons de sécurité, les chaînes de caractères par défaut et généralement connues "public" et "private".

Si les fonctions de sécurité des donnnées sont activées, les Community-Strings sont configurables.

- **SNMPv3**

  Disponible uniquement en cas d'activation des fonctions de sécurité

  Pour la configuration de SNMPv3, voir chapitre SNMP (Page 62).

Configuration

- **"Activer SNMP"**

  Si l'option est activée, la communication via SNMPv1 est autorisée sur le CP.

  Si l'option est désactivée, le CP ne répond aux requêtes de clients SNMP, ni via SNMPv1, ni via SNMPv3.

4.10 Security

La possibilité de configurer les différentes options dépend du protocole Telecontrol utilisé.

Une vue d'ensemble de l'étendue et de l'application des fonctions de sécurité des données du CP est fournie au chapitre Fonctions de sécurité des données (Page 18).

Concernant la capacité fonctionnelle des fonctions de sécurité des données, voir chapitre Capacités fonctionnelles et caractéristiques de performance (Page 20).

Pour pouvoir configurer les fonctions de sécurité des données, créez au moins un utilisateur de sécurité des données, voir chapitre Utilisateur de sécurité des données (Page 57).

4.10.1 Utilisateur de sécurité des données

Créer un utilisateur de sécurité des données

Pour pouvoir configurer des fonctions de sécurité des données, vous devez posséder des droits de configuration appropriés. Pour ce faire, vous devez créez au moins un utilisateur de sécurité de données possédant les droits requis.

Naviguez jusqu'aux paramètres de sécurité des données généraux > "Utilisateurs et rôles" > onglet "Utilisateur".

1. Créez un utilisateur et configurez les paramètres.
2. Attribuez à cet utilisateur dans la zone en-dessous "Utilisateurs et rôles affectés" le rôle "NET Standard" ou "NET Administrateur".

Cet utilisateur pourra, après connexion au projet STEP 7, effectuer les paramétrages requis.

Connectez-vous également à l'avenir, lors de travaux sur les paramètres de sécurité des données, avec cet utilisateur.

4.10.2 Vue d'ensemble des paramètres

Groupes de paramètres

Lorsque les fonctions de sécurité du CP sont activées, vous trouvez ici les groupes de paramètres suivants pour la configuration du CP :

- **Identification du CP**

  Uniquement pour protocole TeleControl Basic

  Configurez ici les paramètres suivants concernant l'authentification du CP auprès du serveur Telecontrol. Vous trouverez plus de détails sur les paramètres ci-après.

- **Options de sécurité DNP3**

  Uniquement pour protocole DNP3

  Vous configurez ici des fonctions de sécurité spécifique protocole. Vous trouverez plus de détails sur les paramètres ci-après.

- **Pare-feu**

  Voir chapitre Pare-feu (Page 58).

- **Synchronisation d'horloge**

  Pour la synchronisation d'horloge, veuillez lire le chapitre de niveau supérieure Synchronisation d'horloge (Page 47).

- **Configuration e-mail**

  Voir chapitre Configuration de la messagerie (Page 60).

- **Paramètres de journal**

  Vous configurez ici les paramètres de journalisation des évènements touchant à la sécurité des données.

  Voir chapitre Paramètres de journal - Filtrage des évènements système (Page 61).

- **SNMP**

  Vous configurez ici les paramètres de l'agent SNMP sur le CP.

  Voir chapitre SNMP (Page 62).

- **Gestionnaire de certificats**

  Voir chapitre Gestionnaire de certificats (Page 71).

Dans les paramètres de sécurité généraux de STEP 7 vous trouverez entre autres les groupes de paramètres suivants :

- **Groupes VPN**

  Vous configurez ici la communication VPN, voir chapitre VPN (Page 63).

- **Gestion des utilisateurs**

  Configurez ici les utilisateurs, rôles et droits.

4.10.3 Pare-feu

4.10.3.1 Contrôle anticipé de télégrammes par le pare-feu MAC

Chaque télégramme entrant ou sortant passe d'abord par le pare-feu MAC (couche 2). Si le télégramme est déjà rejeté à ce niveau, il n'est plus contrôlé par le pare-feu IP (couche 3). Certaines règles de pare-feu MAC peuvent ainsi limiter ou bloquer la communication IP.

4.10.3.2 Syntaxe correcte de l'adresse IP source (mode de pare-feu avancé)

Si vous spécifiez, dans les paramètres de pare-feu avancés du CP, une plage d'adresses pour l'adresse IP source, veillez à utiliser la syntaxe correcte :

- séparez les deux adresses IP uniquement par un trait d'union.

  Correct : 192.168.10.0-192.168.10.255

- N'entrez pas d'autres caractères entre les deux adresses IP.

  Faux : 192.168.10.0 - 192.168.10.255

Si la plage n'est pas correctement entrée, la règle de pare-feu n'est pas appliquée.

4.10.3.3 Paramètres de pare-feu pour liaisons configurées via tunnel VPN

Règles IP de pare-feu en mode de pare-feu avancé

Si vous créez des liaisons configurées par tunnel VPN entre CP et un partenaire de communication, adaptez les paramètres locaux de pare-feu du CP :

Sélectionnez pour les liaisons, pour les deux sens de communication du tunnel VPN, l'action "Allow*" en mode de pare-feu avancé ("Security > Pare-feu > Règles IP").

Voir à ce propos le chapitre Paramètres pour le diagnostic de sécurité en ligne et le chargement sur la station tandis que le pare-feu est activé (Page 59).

4.10.3.4 Paramètres pour le diagnostic de sécurité en ligne et le chargement sur la station tandis que le pare-feu est activé

Paramétrage du pare-feu pour les fonctions en ligne

Si les fonctions de sécurité des données sont activées, procédez comme suit :

Fonctions de sécurité des données générales :

1. Sélectionnez l'entrée "Pare-feu > Services > Définir des services pour les règles IP".
2. Sélectionnez l'onglet "ICMP".
3. Ajoutez respectivement une entrée de type "Echo Reply" et "Echo Request".

Fonctions de sécurité des données locales du CP :

Sélectionnez ensuite le CP sur la station S7.

1. Activez le mode pare-feu avancé dans les paramètres de sécurité locaux du CP, dans le groupe de paramètres "Sécurité des données > Pare-feu".
2. Ouvrez le groupe de paramètres "Règles IP".

3. Dans le tableau, ajoutez une nouvelle règle IP pour les services qui viennent d'être créés, comme suit :
   – Action : Accept ; De : Externe ; Vers : Station ; Service > Service ICMPv4/6 > Echo Request (le service global créé auparavant)
   – Action : Accept ; De : Station ; Vers : Externe ; Service > Service ICMPv4/6 > Echo Reply (le service global créé auparavant)
4. Pour la règle IP du service "Echo Request", entrez sous "Adresse IP source" l'adresse IP de la station d'ingénierie.

Ces règles permettent à la station d'ingénierie d'accéder au CP uniquement avec des paquets ICMP (ping) à travers le pare-feu.

Remarque

Chargement d'autres services pour le diagnostic de sécurité des données en ligne

Si vous voulez utiliser les fonctions "Diagnostic de sécurité des données en ligne" ou "Charger dans l'appareil", créez des règles supplémentaires ou désactivez les services "Echo Request" / "Echo Reply".

4.10.4 Configuration de la messagerie

Configuration de la messagerie sous STEP 7

Lorsque surviennent des évènements particuliers, ARRÊT CPU par ex., le CP peut envoyer des e-mails . Ceci n'est pas lié à l'utilisation de la communication Telecontrol.

En cas d'utilisation de la communication Telecontrol, des évènements supplémentaires configurables dans la mémoire image de la CPU peuvent déclencher l'envoi d'e-mails. Des données de process peuvent être envoyées en même temps que l'e-mail.

L'éditeur de messages (entrée "Messages") permet de configurer les e-mails, voir chapitre Messages (Page 75).

Conditions requises pour l'envoi d'e-mails

Tenez compte des prérequis de la configuration du CP pour la transmission d'e-mails :

- Les fonctions de sécurité sont activées.
- L'heure du CP est synchronisée.

Vous avez besoin pour la configuration des données du serveur SMTP et du compte utilisateur :

- adresse du serveur, numéro de port, nom d'utilisateur, mot de passe, adresse e-mail de l'expéditeur (CP)
- En cas de transmission cryptée : Certificat de serveur

Configuration de la messagerie

Avec le paramétrage par défaut du port SMTP 25, le module transmet des e-mails non cryptés.

Si votre opérateur de service de messagerie prend uniquement en charge la transmission cryptée, utilisez les options suivantes :

- N° de port 587

  Si vous utilisez STARTTLS, le module envoie des e-mails cryptés au serveur SMTP de votre opérateur de service de messagerie.

  Recommandation : Si votre opérateur de messagerie offre les deux possibilités (STARTTLS / SSL/TLS) utilisez de préférence STARTTLS avec le port 587.

- N° de port 465

  Si vous utilisez SSL/TLS (SMTPS), le module envoie des e-mails cryptés au serveur SMTP de votre opérateur de service de messagerie.

Renseignez-vous auprès de votre opérateur de service de messagerie sur l'option prise en charge.

Importation de certificat en cas de transmission cryptée

Pour pouvoir utiliser la transmission cryptée, vous devez charger le certificat de votre compte e-mail dans le gestionnaire de certificats de STEP 7. Le certificat vous est fourni par votre opérateur de messagerie.

Utilisez le certificat en exécutant les opérations suivantes :

1. Enregistrez le certificat fourni par votre opérateur de messagerie dans le système de fichiers de la station d'ingénierie.
2. Importez le certificat dans votre projet STEP 7 par "Paramètres de sécurité généraux > Gestionnaire de certificats".
3. Utilisez le certificat importé pour tous les modules qui exploitent des e-mails cryptés, via le tableau "Gestionnaire de certificats" dans le groupe de paramètres locaux "Security".

Pour la marche à suivre, voir chapitre Manipulation de certificats (Page 72).

4.10.5 Paramètres de journal - Filtrage des évènements système

Problèmes de communication en cas de valeur excessive paramétrée pour les évènements système

Si la valeur spécifiée pour le filtrage des évènements système est trop élevée, il se peut que vous ne puissiez pas utiliser les capacités fonctionnelles maximales de la communication. Le nombre élevé de messages d'erreur émis retarde ou bloque éventuellement le traitement des liaisons de communication.

Dans "Sécurité (Security) > Paramètres de journal > Configurer évènements système", sélectionnez pour le paramètre "Niveau :" la valeur "3 (Error)", pour assurer l'établissement sûr des liaisons de communication.

4.10.6 SNMP

SNMP

Les caractéristiques du CP concernant SNMP sont indiquées au chapitre SNMP (Page 94).

Si les fonctions de sécurité sont activées, vous disposez des options et possibilités de paramétrage suivantes.

SNMP

- **"Activer SNMP"**

  Si l'option est activée, la communication via SNMP est autorisée sur l'appareil. SNMPv1 est activé par défaut.

  Si l'option est désactivée, aucune réponse n'est fournie aux requêtes de clients SNMP, ni via SNMPv1, ni via SNMPv3.

- **"Utiliser SNMPv1"**

  Active l'utilisation de SNMPv1 pour le CP. Pour la configuration des Community-Strings requis, voir ci-dessous (SNMPv1).

- **"Utiliser SNMPv3"**

  Active l'utilisation de SNMPv3 pour le CP. Pour la configuration des algorithmes requis, voir ci-dessous (SNMPv3).

SNMPv1

Les Community-Strings doivent être transmis via SNMPv1 avec les requêtes adressées au CP.

- **"Lecture du Community String en cours"**

  La chaîne de caractères est requise pour l'accès en lecture.

  Laissez la chaîne "public" prédéfinie ou configurez une nouvelle chaîne.

- **"Autorise accès en écriture"**

  L'activation de cette option autorise l'accès en écriture au CP et le Community-String associé devient éditable.

- **"Écriture du Community String en cours"**

  La chaîne de caractères est requise pour l'accès en écriture et peut également être utilisée pour un accès en lecture.

  Laissez la chaîne "private" prédéfinie ou configurez une nouvelle chaîne.

Conformez-vous à la syntaxe en minuscules du Community-String prédéfini !

Remarque

Sécurité de l'accès

Modifiez, pour des raisons de sécurité, les chaînes de caractères généralement connues "public" et "private".

SNMPv3

Les algorithmes doivent être configurés via SNMPv3 pour l'accès crypté au CP.

- **"Algorithme d'authentification"**

  Sélectionnez la procédure d'authentification à utiliser dans la zone de liste déroulante.

- **"Algorithme de cryptage"**

  Sélectionnez la procédure de cryptage à utiliser dans la zone de liste déroulante.

  Tenez compte des informations sur la sécurité des algorithmes disponibles, fournies dans l'aide en ligne.

Gestion des utilisateurs

Dans la gestion des utilisateurs que vous trouverez dans les paramètres de sécurité généraux, attribuez le rôle voulu aux divers utilisateurs.

Dans les propriétés des rôles figure la liste des droits de chaque rôle, notamment par exemple les différents types d'accès via SNMP. Pour les nouveaux rôles, vous pouvez configurer librement divers droits.

Vous trouverez des informations sur les utilisateurs, rôles et stratégies de mot de passe dans le système d'information de STEP 7.

4.10.7 VPN

4.10.7.1 VPN (Virtual Private Network)

VPN - IPsec

Virtual Private Network (VPN) est une technologie de transport sûr de données confidentielles via des réseaux IP publics, via Internet p. ex. VPN permet de créer et d'exploiter une connexion sécurisée (tunnel IPsec) entre deux systèmes informatiques ou réseaux sécurisés via un réseau non fiable.

Le tunnel IPsec retransmet toutes les données, même celles de protocoles de couches de plus haut niveau (HTTP, FTP, etc.).

Le trafic de données de deux composants de réseau est transporté sans restrictions à travers un autre réseau. Des réseaux complets peuvent ainsi être interconnectés à travers un réseau voisin ou intercalé.

Propriétés

- VPN constitue un réseau partiel logique encapsulé dans un réseau voisin (associé). VPN utilise les mécanismes d'adressage habituel du réseau associé, mais transporte des télégrammes de réseau particuliers et fonctionne ainsi indépendamment du reste de ce réseau.
- VPN permet aux partenaires VPN qui s'y trouvent, de communiquer avec le réseau associé.
- VPN qui repose sur une technologie de tunnelisation, est configurable.
- La communication à l'abri des écoutes et manipulations entre partenaires VPN est assurée par l'emploi de mots de passe, de clés publiques ou de certificats numériques (authentification).

Domaines d'application/de mise en œuvre

- Interconnexion sécurisée de réseaux locaux via Internet (connexion "site to site").
- Accès sécurisé à un réseau d'entreprise (connexion "end to site")
- Accès sécurisé à un serveur (connexion "end to end")
- Communication entre deux serveurs, non accessibles à des tiers (connexion "end to end" ou "host to host").
- Sécurité des informations dans les installations interconnectées en réseau dans le domaine de l'automatisation
- Sécurisation de systèmes d'ordinateurs y compris de la communication de données associée au sein d'un réseau d'automatisation ou de l'accès à distance via Internet
- Accès à distance sécurisé d'un PC/d'une console de programmation aux automates et réseaux protégés par des modules de sécurité via des réseaux publics.

Concept de protection de cellule

Industrial Ethernet Security permet de sécuriser des appareils ou des segments d'un réseau Ethernet :

- L'accès à des appareils et segments de réseau, protégés par des modules de sécurité, est autorisé.
- Permet d'établir des connexions sécurisées via des structures de réseau non fiables.

En combinant diverses fonctions de sécurité telles que pare-feu, routeur NAT/NAPT et VPN via tunnel IPsec, les modules de sécurité protègent contre :

- l'espionnage de données
- la manipulation de données
- les intrusions

4.10.7.2 Création de tunnels VPN entre stations pour la communication S7

Conditions

Pour créer un tunnel VPN destiné à la communication S7 entre deux stations S7 ou entre une station S7 et une station d'ingénierie avec un CP de sécurité des données (un CP 1628 p. ex.), les conditions suivantes doivent être remplies :

- Les deux stations ont été configurées.
- Les CP des deux stations doivent prendre en charge les fonctions de sécurité des données.
- Les interfaces Ethernet des deux stations font partie du même sous-réseau.

Remarque

Communication également possible via un routeur IP

Les deux stations peuvent également communiquer via un routeur IP. Cette voie de communication nécessite cependant des paramétrages supplémentaires.

Marche à suivre

Pour créer un tunnel VPN, vous devez exécuter les opérations suivantes :

1. Créer un utilisateur de sécurité des données

   Si l'utilisateur de sécurité des données a déjà été créé : Connectez-vous sous ce nom d'utilisateur.
2. Option "Activer les fonctions de sécurité des données"
3. Créer un groupe VPN et y affecter les modules de sécurité
4. Configurer les propriétés du groupe VPN
5. Configurer les propriétés VPN locales des deux CP

Vous trouverez la description détaillée des opérations dans les sections ci-après du présent chapitre.

Sélectionnez "Activer les fonctions de sécurité des données"

Après vous être connecté, cochez sur les deux CP la case "Activer les fonctions de sécurité des données des données".

Vous disposez à présent des fonctions de sécurité des données pour les deux CP.

Créer un groupe VPN et y affecter les modules de sécurité

1. Dans les paramètres de sécurité des données généraux, sélectionnez l'entrée "Pare-feu" > "Groupes VPN" > "Ajouter un nouveau groupe VPN".
2. Double-cliquez sur l'entrée "Ajouter un nouveau groupe VPN" pour créer un groupe VPN.

   Résultat : Un nouveau groupe VPN est affiché sous l'entrée sélectionnée.
3. double-cliquez dans les paramètres de sécurité des données généraux sur l'entrée "Groupes VPN" > "Affecter module à un groupe VPN".
4. Affectez au groupe VPN les modules de sécurité entre lesquels des tunnels VPN seront établis.

Remarque

Date et heure courantes du CP pour connexions VPN

En général, l'établissement d'une connexion VPN et l'acceptation des certificats échangés qui y est liée, présuppose la date et l'heure courantes des deux stations.

L'établissement d'une connexion VPN à une station d'ingénierie qui est en même temps serveur Telecontrol (TCSB installé), se déroule, avec la synchronisation d'horloge du CP, comme suit :

Sur la station d'ingénierie (avec TCSB), vous voulez que le CP établisse une connexion VPN. Même si le CP ne possède pas encore l'heure courante, la connexion VPN est établie. Les certificats utilisés sont jugés valides et la communication sécurisée fonctionne.

Après établissement de la connexion, le CP synchronise son horloge avec le PC car le serveur Telecontrol est, lorsque la communication Telecontrol est activée, l'horloge maître.

Configuration des propriétés du groupe VPN

1. Effectuez un double-clic sur le groupe VPN créé.

   Résultat : Les propriétés du groupe VPN sont affichées sous "Authentification".
2. Attribuez un nom au groupe VPN. Configurez dans les propriétés les paramètres du groupe VPN.

   Ces propriétés définissent les paramètres par défaut du groupe VPN que vous pouvez modifier à volonté.

Remarque

Définition des propriétés VPN des CP

Définissez les propriétés VPN des CP dans le groupe de paramètres "Security" > "Pare-feu" > "VPN" de chaque module.

Résultat

Vous avez défini un tunnel VPN. Le pare-feu du CP est automatiquement activé : La case "Activer pare-feu" est cochée automatiquement lors de la création d'un groupe VPN. Vous ne pouvez pas supprimer la coche de la case.

Chargez la configuration matérielle sur tous les modules appartenant au groupe VPN.

4.10.7.3 Communication par tunnel VPN avec SOFTNET Security Client (station d'ingénierie)

La configuration d'une communication par tunnel VPN entre un SOFTNET Security Client et le CP s'effectue comme décrit au chapitre Création de tunnels VPN entre stations pour la communication S7 (Page 65).

La communication par tunnel VPN ne fonctionne que si l'abonné interne est désactivé

Dans certaines conditions, l'établissement d'une communication par tunnel VPN entre SOFTNET Security Client et CP ne fonctionne pas.

SOFTNET Security Client tente d'établir simultanément une communication par tunnel VPN avec un abonné interne subordonné. Cette tentative d'établissement d'une communication avec un abonné inexistant empêche l'établissement de la communication voulue avec le CP.

Pour que l'établissement de la communication par tunnel VPN avec le CP fonctionne, désactivez l'abonné interne.

N'utilisez la procédure ci-après de désactivation de l'abonné que si le problème décrit se pose.

Désactivez l'abonné dans la liste de tunnels du SOFTNET Security Client :

1. Supprimez la coche de la case "Enable active learning".

   L'abonné subordonné disparaît dans un premier temps de la liste de tunnels.
2. Sélectionnez la connexion voulue au CP dans la liste de tunnels.
3. Dans le menu contextuel qui s'ouvre avec le bouton droit de la souris, sélectionnez "Enable all members".

   L'abonné subordonné réapparaît temporairement dans la liste de tunnels.
4. Sélectionnez l'abonné subordonné dans la liste de tunnels.
5. Dans le menu contextuel qui s'ouvre avec le bouton droit de la souris, sélectionnez "Delete entry".

Résultat : L'abonné subordonné est définitivement désactivé. L'établissement d'une communication par tunnel VPN fonctionne.

4.10.7.4 Mise en place de la communication par tunnel VPN entre CP et SCALANCE M

Créez un tunnel VPN entre CP et le routeur SCALANCE M selon la marche à suivre décrite pour les stations.

La communication par tunnel VPN n'est établie que si vous avez coché la case "Perfect Forward Secrecy" dans les paramètres de sécurité généraux du groupe VPN créé ("Groupes VPN > Authentification").

Si la case n'est pas cochée, le CP refuse d'établir la liaison.

4.10.7.5 CP abonné passif de liaisons VPN

Paramétrer sur abonné passif l'autorisation d'établir une liaison VPN

Si le CP est connecté à un autre abonné VPN via une passerelle et si le CP est un abonné passif, paramétrez l'option "Responder" pour la permission d'établir une liaison VPN.

C'est le cas pour la configuration typique suivante :

abonné VPN (actif) ⇔ passerelle (adresse IP dyn.) ⇔ Internet ⇔ passerelle (adresse IP fixe) ⇔ CP (passif)

Configurez pour le CP, abonné passif, la permission d'établir une liaison VPN comme suit :

1. Sous STEP 7, sélectionnez l'affichage d'appareils et de réseau.
2. Sélectionnez le CP.
3. Ouvrez le groupe de paramètres "VPN" dans les paramètres de sécurité locaux.
4. Remplacez, pour chaque liaison VPN au CP qui est abonné VPN passif, le paramètre par défaut "Initiator/Responder" par le paramètre "Responder".

4.10.7.6 SYSLOG

Utilisation de SYSLOG uniquement avec 1 connexion VPN

Si vous voulez utiliser SYSLOG au niveau 7 (debug) via des connexions VPN, ce n'est possible que si une seule connexion VPN est configurée.

4.10.7.7 SINEMA Remote Connect

Télémaintenance avc SINEMA Remote Connect (SINEMA RC)

L'application "SINEMA Remote Connect" (SINEMA RC) est mise à disposition à des fins de télémaintenance.

SINEMA RC utilise OpenVPN pour le cryptage des données. Le centre de communication est le serveur SINEMA RC par lequel passent les communications entre les abonnés et qui gère la configuration du système de communication.

Étapes préparées

Exécutez les étapes suivantes avant de commencer à configurer le couplage de SINEMA RC au module sous STEP 7. Elles sont indispensables pour assurer la cohérence du projet STEP 7.

- Configuration de SINEMA Remote Connect Server

  Réalisez la configuration requise du SINEMA RC Server (pas sous STEP 7). Le module de communication et son partenaire de communication doivent être configurés sur le serveur SINEMA RC.

- Exportation du certificat CA (facultatif)

  Si vous voulez utiliser le certificat du serveur comme méthode d'authentification du module de communication lors de l'établissement d'une connexion, exportez le certificat CA du SINEMA RC Server.

  Importez ensuite le certificat CA du SINEMA RC Server sur la station d'ingénierie.

  Vous pouvez sinon utiliser comme autre méthode d'authentification du module de communication, l'empreinte digitale du certificat du serveur. La durée de validité de l'empreinte digitale peut être inférieure à celle du certificat.

  Veuillez noter qu'en cas d'échange de module, vous devrez importer à nouveau le certificat.

Configuration de SINEMA Remote Connect

Importation du propre certificat

1. Naviguez sur le CP jusqu'au groupe de paramètres "Sécurité des données > Gestionnaire de certificats > Certificats des appareils partenaires".
2. Ouvrez la boîte de dialogue pour la sélection du certificat par un double clic sur la première ligne vide du tableau.
3. Sélectionnez le certificat CA de SINEMA RC Server.

Naviguez ensuite jusqu'au groupe de paramètres "Security > VPN".

VPN > Général

1. Activez VPN
2. Sélectionnez comme "Type de connexion VPN" l'option "Configuration OpenVPN automatique via SINEMA Remote Connect Server" si vous voulez utiliser la communication via SINEMA Remote Connect.

   Si vous sélectionnez "Internet Key Exchange (IKE) ..." vous pouvez utiliser la communication via tunnel IPsec.

SINEMA Remote Connect Server

Entrez l'adresse et le numéro de port du serveur.

Vérification de serveur

Sélectionnez ici la méthode d'authentification du module de communication lors de l'établissement d'une connexion.

- Certificat CA

  Choisissez sous "Certificat CA" le certificat CA préalablement importé et affecté dans le gestionnaire de certificats local du SINEMA RC Server.

  Le module vérifie d'une manière générale le certificat CA du serveur et sa durée de validité. Les deux options ne sont pas modifiables.

- Empreinte digitale

  Si vous choisissez cette méthode d'authentification, entrez l'empreinte digitale du certificat de serveur de SINEMA RC Server.

Authentification

- ID d'appareil

  Entrez l'ID d'appareil généré pour le module sous SINEMA RC.

- Mot de passe d'appareil

  Entrez le mot de passe d'appareil du module configuré sous SINEMA RC.

  Nombre max. de caractères : 127

Paramètres facultatifs

L'établissement d'une connexion se configure dans le groupe de paramètres "Security > VPN > Paramètres facultatifs" à l'aide du paramètre "Type de connexion"

- **Intervalle d'actualisation**

  Ce paramètre permet de définir l'intervalle d'interrogation par le CP de la configuration du serveur SINEMA RC.

  Veuillez noter qu'en cas de paramétrage de 0 (zéro) le CP ne pourra éventuellement plus établir de connexion au serveur SINEMA RC après une modification de la configuration du serveur SINEMA RC.

- **"Type de connexion"**

  Les deux options du paramètre influencent comme suit l'établissement d'une connexion :

  – Auto

    Le module établit une connexion au SINEMA RC. La connexion OpenVPN est maintenue jusqu'à la modification des paramètres de connexion par le serveur SINEMA Remote Connect. En cas de coupure de la connexion, le CP rétablit automatiquement la connexion.

    Si le serveur SINEMA Remote Connect modifie les paramètres de connexion, le CP lit les nouvelles données de connexion dès que l'intervalle d'actualisation configuré ci-dessus est écoulé.

– Variable d'API pour déclenchement

  Cette option est prévue pour une communication sporadique du module via le serveur SINEMA RC.

  Vous pouvez utiliser cette option si vous voulez établir des connexions temporaires entre le module et un PC. Les connexions temporaires sont établies par une variable d'API et sont utilisables par exemple à des fins de dépannage.

Remarque

Déconnexion

En cas d'ARRÊT de la CPU, par mise à jour du firmware ou par "Charger dans l'appareil" par exemple, la connexion OpenVPN est coupée.

Ces fonctions ne sont utilisables que si l'option "Auto" est activée.

- **Variable d'API pour établissement de connexion**

  Si l'option "Variable d'API pour déclenchement" a été sélectionnée, le module établit une connexion lorsque la variable d'API (bool) est mise à 1. En fonctionnement, la variable d'API peut être mise à 1 selon les besoins, par exemple par un panneau IHM.

  Lors de la remise à 0 de la variable d'API, la connexion est coupée.

4.10.8 Gestionnaire de certificats

Affectation de certificats

Si vous utilisez une communication avec authentification pour le module, par exemple SSL/TLS pour la transmission sécurisée d'e-mails, l'emploi de certificats s'impose. Vous devez importer des certificats de partenaires de communication autres que Siemens dans le projet STEP 7 et les charger avec les données de configuration sur le module :

1. Importez les certificats du partenaire de communication via le gestionnaire de certificats dans les paramètres de sécurité généraux.
2. Affectez ensuite au module les certificats importés, au choix :
   – via le tableau "Certificats dignes de confiance et autorités de certification racine" des paramètres de sécurité généraux
   – via le tableau "Certificats des appareils partenaires" du gestionnaire local de certificats du module (sécurité des données)

     Ajoutez également à ce tableau les certificats des partenaires de communication dont les certificats ont été générés dans le même projet STEP 7.

La marche à suivre est décrite au chapitre Manipulation de certificats (Page 72).

Pour plus d'informations, veuillez vous référer au système d'information STEP 7.

4.10.9 Manipulation de certificats

Certificats pour l'authentification

Si vous avez configuré, pour le module de communication, la communication sécurisée avec authentification, l'établissement de la communication nécessitera l'utilisation de certificats locaux et de certificats du partenaire de communication.

Des certificats sont attribués à tous les abonnés d'un projet STEP 7 si les fonctions de sécurité sont activées. Le projet STEP 7 est dans ce cas l'autorité de certification.

Remarque

Pas de certificat si les fonctions de sécurité sont désactivées

Si vous avez désactivé dans le projet STEP 7 les fonctions de sécurités du CP, aucun certificat n'est généré pour le CP.

Un certificat SSL est créé pour le CP pour la transmission sécurisée d'e-mails via SSL/TLS. Il est affiché dans STEP 7 sous "Paramètres de sécurité généraux > Gestionnaire de certificats > Certificats d'appareils". Le tableau "Certificats d'appareils" affiche l'émetteur, la validité, l'utilisation d'un certificat (service/application) et l'utilisation d'une clé. Vous pourrez faire afficher de plus amples informations sur le certificat si vous sélectionnez le certificat dans le tableau et choisissez l'option "Afficher" du menu contextuel. Vous voyez également dans le tableau tous les autres certificats générés sous STEP 7 ou importés.

Pour que le module, dont les fonctions de sécurité sont activées, puisse communiquer avec des partenaires autres que Siemens, il faut que les certificats appropriés des partenaires soient échangés lors de la communication. Pour la fourniture de certificats tiers au module, procédez comme suit :

1. Importation de certificats tiers de partenaires de communication

   ⇒ Paramètres de sécurité généraux du projet (Gestionnaire de certificats)

2. Affectation de certificats, alternative :

   – Paramètres de sécurité généraux > Gestionnaire de certificats > "Certificats dignes de confiance"

   – Paramètres de sécurité locaux du module > Gestionnaire de certificats > "Certificats des appareils partenaires"

Ces étapes sont décrites dans les sections ci-après.

Importation de certificats tiers de partenaires de communication

Importez les certificats des partenaires de communication de constructeurs tiers via le gestionnaire de certificats dans les paramètres de sécurité généraux du projet STEP 7. Procédez pour ce faire comme suit :

1. Enregistrez le certificat tiers dans le système de fichiers du PC de la station d'ingénierie connectée.
2. Dans le projet STEP 7, ouvrez le Gestionnaire de certificats global :

   Paramètres de sécurité généraux > Gestionnaire de certificats
3. Ouvrez l'onglet "Certificats dignes de confiance et autorités de certification racine"
4. Cliquez sur une ligne du tableau et sélectionnez le menu contextuel "Importer".
5. Importer à l'aide du dialogue qui s'ouvre le certificat du système de fichiers de la station d'ingénierie dans le projet STEP 7.

Affectation de certificats dans les paramètres de sécurité généraux.

Importez les certificat du partenaire via : Paramètres de sécurité généraux > Gestionnaire de certificats > Certificats dignes de confiance > bouton droit de la souris. Affectez le certificat au CP (sélectionner certificat > bouton droit de la souris).

1. Ouvrez l'onglet "Certificats dignes de confiance et autorités de certification racine"
2. Sélectionnez le certificat voulu.
3. Dans le menu contextuel (bouton droit de la souris), sélectionnez "Affecter".
4. Sélectionnez, dans le dialogue qui s'ouvre, le module voulu.

   Après l'affectation, le certificat d'apparait dans le gestionnaire de certificats local du module dans le tableau "Certificats des appareils partenaires".

Affectation locale de certificats

Afin de pouvoir utiliser un certificat importé pour le module, il faut que le certificat soit affiché dans le groupe de paramètres "Sécurité des données" du module. Procédez pour ce faire comme suit :

1. Dans le projet STEP 7, sélectionnez le module.
2. Naviguez jusqu'au groupe de paramètres "Security > Gestionnaire de certificats".
3. Double-cliquez dans le tableau sur la ligne contenant l'entrée "<Ajouter nouveau>".

   Le tableau "Gestionnaire de certificats" des Paramètres de sécurité généraux s'affiche.
4. Sélectionnez dans le tableau le certificat tiers voulu puis cliquez pour l'appliquer sur la coche verte sous le tableau.

   Le certificat sélectionné s'affiche dans le tableau local du module.

Ce n'est qu'à partir de maintenant que le certificat est utilisé pour le module.

Ajoutez également à ce tableau les certificats des partenaires de communication dont les certificats ont été générés dans le même projet STEP 7.

Exportation de certificats pour des applications d'autres constructeurs (serveur de journalisation par ex.)

Pour la communication avec des applications d'autres constructeurs, l'application tierce a généralement également besoin du certificat du module.

L'exportation du certificat du module pour des partenaires de communication d'un autre constructeur s'effectue de manière analogue à l'importation (voir ci-dessus). Procédez pour ce faire comme suit :

1. Dans le projet STEP 7, ouvrez le Gestionnaire de certificats global :

   Paramètres de sécurité généraux > Gestionnaire de certificats
2. Ouvrez l'onglet "Certificats d'appareils".
3. Cliquez dans le tableau sur la ligne qui contient le certificat voulu puis sélectionnez le menu contextuel "Importer".
4. Enregistrez le certificat dans le système de fichiers du PC de la station d'ingénierie connectée.

Vous pouvez à présent transférer le certificat du module dans le système du constructeur tiers.

Certificats pour serveur de journalisation

Si vous utilisez un serveur de journalisation dans votre système, exportez le certificat SSL pour authentifier le module auprès du serveur.

Modification du certificat : Nom de propriétaire de certificat alternatif

STEP 7 reprend les propriétés "Nom DNS", "Adresse IP" et "URI" du paramètre "Nom de propriétaire de certificat alternatif" (Windows : "Nom de demandeur alternatif") des données de configuration STEP 7.

Vous pouvez modifier ces paramètres d'un certificat dans le gestionnaire de certificats des paramètres de sécurité généraux. Sélectionnez pour ce faire le certificat voulu dans le tableau des certificats d'appareils et ouvrez le menu contextuel "Renouveler". Les propriétés du paramètre "Nom de propriétaire de certificat alternatif", modifiées sous STEP 7, ne sont pas reprises dans le projet STEP 7.

4.11 Points de données

Vous trouverez la description des paramètres spécifiques Telecontrol dans les manuels de configuration, voir /4/ (Page 108).

4.12 Messages

Configuration d'e-mails

En cas d'évènements importants, le CP peut émettre des messages. Vous pouvez configurer des e-mails. Le destinataire peut être un PC connecté à Internet ou une station S7.

Les messages se configurent dans l'éditeur de messages du CP. Vous le trouverez soit :

- dans le menu contextuel du CP
- par navigation dans le projet : Répertoire de la station > modules locaux > CP

Les caractères autorisés dans les textes de message et autres paramètres sont indiqués au chapitre Jeu de caractères pour messages (Page 81).

Vue d'ensemble de la configuration et informations nécessaires

Il n'est plus nécessaire d'activer la communication Telecontrol (groupe de paramètres "Modes de communication") pour transmettre des messages. Vous pouvez envoyer des messages au CP sans utiliser la communication Telecontrol.

Informations requises pour l'utilisation d'e-mails :

- Données d'accès du serveur SMTP : adresse, numéro de port, nom d'utilisateur, mot de passe
- En cas d'utilisation de STARTTLS ou SSL/TLS : certificat de l'opérateur de messagerie
- Adresses e-mail des destinataires

La configuration s'effectue dans les groupes de paramètres suivants :

- Activation des fonctions de sécurité

  Pour pouvoir utiliser des e-mails, activez les fonctions de sécurité du CP, groupe de paramètres "Security".

- Configuration du service / protocole :

  "Configuration e-mail", voir chapitre Configuration de la messagerie (Page 60).

- En cas d'utilisation de STARTTLS ou SSL/TLS :
  - Importation du certificat de l'opérateur de messagerie :

    "Paramètres de sécurité généraux"
  - Utilisation du certificat importé pour le CP :

    Groupe de paramètres "Security" > "Gestionnaire de certificats"

Configuration dans l'éditeur de messages

La configuration des messages s'effectue sous STEP 7 dans l'éditeur de points de données et de messages. Vous pouvez ouvrir l'éditeur soit :

- par sélection du module de communication

  dans le menu contextuel "Ouvrir l'éditeur de points de données et de messages"

- par navigation dans le projet :

  Projet > Répertoire de la station en question > Modules locaux > Module de communication voulu

  Un double clic sur l'entrée ouvre l'éditeur de points de données et de messages.

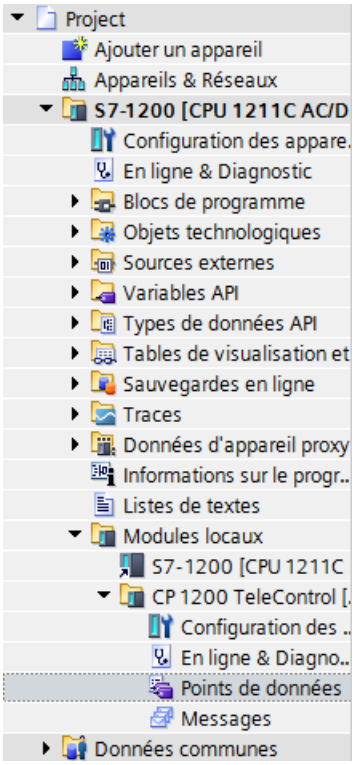


Figure 4-1 Ouverture de l'éditeur de messages par navigation dans le projet

Après l'ouverture de l'éditeur, vous pourrez basculer à l'aide des deux entrées en haut à droite au-dessus du tableau entre l'éditeur de points de données et l'éditeur de messages.

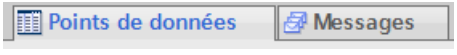


Figure 4-2 Basculement entre les deux éditeurs

L'éditeur de points de données est uniquement significatif pour la communication Telecontrol.

Création d'objets

Créez un nouvel objet (message) par un double clic sur la première ligne du tableau qui contient l'entrée grisée "<Ajouter objet>".

Vous pouvez adapter le nom par défaut selon vos besoins mais il doit être unique au sein du module.

Organisation des colonnes et lignes, affichage/masquage de colonnes

Comme dans beaucoup d'autres programmes, vous pouvez également réorganiser les colonnes et le tableau selon vos besoins :

- Réorganisation des colonnes

  Si vous cliquez sur un en-tête de colonne avec le bouton gauche de la souris et le maintenez enfoncé, vous pouvez déplacer la colonne.

- Tri d'objets

  Si vous cliquez brièvement avec le bouton gauche de la souris sur un en-tête de colonne, vous pouvez trier les objets du tableau dans l'ordre croissant ou décroissant des entrées de la colonne. L'ordre du tri est indiqué par une flèche dans l'en-tête de la colonne.

  Après un tri dans l'ordre décroissant, vous pouvez désactiver le tri en cliquant à nouveau sur l'en-tête de la colonne.

- Adaptation de la largeur de colonne

  Cette fonction s'obtient par les actions suivantes :

  – En ouvrant le menu contextuel par un clic du bouton droit de la souris sur un en-tête de colonne.

    "Optimiser la largeur", "Optimiser la largeur de toutes les colonnes"

  – Si vous amenez le point à proximité de la limite d'un en-tête de colonne, le symbole suivant s'affiche :

    Effectuez alors un double clic sur l'en-tête de colonne. La largeur de la colonne est alors ajustée à l'entrée la plus large de la colonne en question.

- Affichage/masquage de colonnes

  Cette fonction figure dans le menu contextuel qui s'ouvre lorsque vous cliquez avec le bouton droit de la souris sur un en-tête de colonne.

Copie de messages

Vous pouvez copier et coller des messages. Cliquez avec le bouton droit de la souris dans la ligne d'un objet du tableau pour accéder aux fonctions précitées dans le menu contextuel :

- Couper
- Copier
- Coller

  Vous pouvez coller des objets coupés ou copiés dans le tableau ou dans la première ligne libre sous le tableau.

  Vous pouvez également coller des objets coupés ou copiés dans les tableaux d'autres modules de communication du même type et utilisant le même protocole Telecontrol.
- Supprimer

Maintenez la touche <Ctrl> enfoncée pour sélectionner plusieurs lignes non contiguës

Maintenez la touche <Maj> enfoncée pour sélectionner le début et la fin d'une zone continue.

Onglet de configuration des messages

Sélectionner un message dans le tableau "Messages". Configurez les paramètres du message sélectionné dans les onglets figurant sous le tableau.

"Paramètres de message"

Vous configurez ici le numéro d'appel c.-à-d. le destinataire, l'objet (e-mail) et le texte du message.

"Déclenchement"

Le groupe de paramètres "Déclenchement" permet de configurer le déclenchement de l'envoi du message ainsi que d'autres paramètres.

- **Déclenchement d'e-mail**

  Définit l'évènement qui déclenche l'envoi du message :

  – **Utiliser des variables d'API**

    Le signal de déclenchement de l'envoi d'un e-mail est la transition de front (0 → 1) du bit de déclenchement "Variable d'API pour déclenchement", positionné par le programme utilisateur. Si nécessaire, il est possible de configurer un bit de déclenchement distinct pour chaque message. Concernant le bit de déclenchement, voir ci-dessous.

    Remise à zéro du bit de déclenchement :
    Si la zone de mémoire du bit de déclenchement se trouve dans la zone de mémento ou dans un bloc de données, le bit de déclenchement est remis à zéro par l'envoi du message.
    Dans tous les autres cas, le bit de déclenchement doit être mis à zéro par le programme utilisateur.

    Remarque
    Mise à 1 rapide de la variable de déclenchement de diagnostic

    Ne pas activer les déclencheurs plus souvent qu'une fois par seconde.

  – **La CPU passe à ARRET**

  – **La CPU passe à MARCHE**

  – **Connexion VPN établie**

    Déclenche l'envoi du message lorsque la connexion VPN est établie ou rétablie.

  – **Connexion VPN coupée**

    Déclenche l'envoi du message lorsque la connexion VPN au partenaire est coupée.

  – **Connexion SINEMA RC établie**

    Déclenche l'envoi du message lorsque la connexion Open VPN est établie ou rétablie.

  – **Connexion SINEMA RC coupée**

    Déclenche l'envoi du message lorsque la connexion OpenVPN au partenaire est coupée.

- **Variable d'API pour déclenchement**

  Variable d'API pour le déclenchement "Utiliser des variables d'API"

- **Activer identificateur d'état de traitement**

  Si cette option est activée, l'état qui informe sur l'état de traitement du message envoyé, est émis après chaque tentative d'envoi.

  L'état est inscrit dans la "Variable d'API d'état de traitement". En cas de problèmes de notification des messages, vous pouvez vérifier l'état à l'aide du serveur Web de la CPU en y faisant afficher la valeur de la variable d'API.

  Pour la signification des états indiqués en hexadécimal, voir chapitre État de traitement d'e-mails (Page 95).

- **Variable d'API d'état de traitement**

  Variable d'API de type DWORD pour l'état de traitement

- **Enable Value Tag**

  Si vous activez l'option, le CP inscrit dans le message à l'emplacement des caractères génériques $$ une valeur issue de la mémoire de la CPU. Entrez pour ce faire dans le texte du message les caractères génériques "$$" à l'emplacement de la valeur à transférer.

  Sélectionnez une variable d'API dont la valeur sera intégrée au message. La valeur est inscrite dans le texte du message à l'emplacement des caractères génériques $$.

  $$ servant de caractères génériques des valeurs de points de données supportent les types de données :
  Bool, Byte, Char, Int, UInt, Word, DWord, UDInt, DInt, Real, String,
  Tableaux des types de données précités

- **Variable d'API pour la valeur**

  Variable d'API dans laquelle est inscrite la valeur à joindre.

4.13 Jeu de caractères pour messages

Jeu de caractères pour textes de message

Le jeu de caractères ASCII suivant (valeur hexadécimale et nom du caractère) est pris en charge pour les textes :

- 0x0A

  LF (saut de ligne)

- 0x0D

  CR (retour de chariot)

- 0x20

  Espace

- 0x21 ... 0x5A

  ! " # $ % & ' ( ) * + , - . / 0 1 2 3 4 5 6 7 8 9 : ; < = > ? @ A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

- 0x5F

  £

- 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

Blocs de programme (OUC) 5

5.1 Blocs de programme pour OUC

Utilisation des blocs de programme pour l'Open User Communication (OUC)

Les instructions figurant ci-dessous (blocs de programme) sont utilisables pour la communication directe entre stations S7.

À la différence des autres types de communication, il n'est pas nécessaire d'activer l'Open User Communication dans la configuration du CP, car les blocs de programme requis doivent être créés activement. Pour plus de détails sur les blocs de programme voir le système d'information de STEP 7.

Remarque

Différentes versions de bloc de programme

Veillez à ne pas utiliser sous STEP 7 différentes versions d'un bloc de programme dans une station.

Conditions pour Secure OUC

Condition d'utilisation de la transmission sécurisée via Secure OUC :

- STEP 7 : À partir de V16
- Firmware de la CPU : À partir de V4.4
- Firmware du CP : À partir de V3.2

Blocs de programme pris en charge pour OUC

Les instructions ci-après, dans la version minimale spécifiée, sont disponibles pour la programmation de l'Open User Communication :

- **TSEND_C V3.0 / TRCV_C V3.0**

  Blocs compacts pour :

  – l'établissement/la coupure de connexions et l'émission de données

  – l'établissement/la coupure de connexions et la réception de données

Utilisez alternativement :

- **TCON V4.0 / TDISCON V2.1**

  Connexion / déconnexion

- **TUSEND V4.0 / TURCV V4.0**

  Emission ou réception de données via UDP

- **TSEND V4.0 / TRCV V4.0**

  Emission ou réception de données via TCP ou ISO-on-TCP

- **TMAIL_C V4.0**

  Envoi d'e-mails

  Pour pouvoir transmettre des e-mails cryptés avec ce bloc, le CP doit posséder l'heure exacte. Configurez la synchronisation d'horloge.

Pour modifier les données de configuration du CP en cours de fonctionnement :

- **T_CONFIG V1.0**

  Configuration programmée des paramètres IP

  Conformez-vous aux instructions concernant T_CONFIG et les SDT "IF_CONF_..." du chapitre Modification de l'adresse IP en cours de fonctionnement (Page 86).

Remarque

Pas de retour d'information du CP

"T_CONFIG" ne prend pas en charge les retours d'information du CP à la CPU. Les erreurs d'appel de bloc ou de paramètres d'adresse ne sont pas signalées. Que le paramètre d'adresse ait été activé ou non, le bloc signale "BUSY" ou "DONE".

Vous trouverez les blocs de programme sous STEP 7 dans la Task Card "Instructions > Communication > Open User Communication".

Description des connexions dans les types de données système (SDT)

Les blocs mentionnés ci-dessus utilisent, pour la description des connexions, le paramètre CONNECT. TMAIL_C utilise le paramètre MAIL_ADDR_PARAM.

La description de connexion est enregistrée dans un bloc de données dont la structure est définie par un type de données système (SDT).

Création d'un SDT pour les blocs de données

Créez le SDT requis pour chaque description de connexion sous forme de bloc de données (Global DB).

Pour générer le type de SDT, ne sélectionnez pas une entrée de la zone de liste déroulante "Type de données" dans la table de déclaration du bloc mais entrez manuellement par exemple le nom "TCON_IP_V4" dans le champ "Type de données".

Le SDT voulu est alors créé avec ses paramètres.

SDT utilisables

- **TCON_IP_V4**

  Pour la transmission de télégrammes via TCP ou UDP

- **TCON_QDN**

  Pour la communication TCP ou UDP via le de nom de domaine entièrement qualifié (FQDN) (IPv4 / IPv6)

- **TCON_IP_RFC**

  Pour la transmission de télégrammes via ISO-on-TCP (communication directe entre deux stations S7)

- **TADDR_Param**

  Pour la transmission de télégrammes via UDP

- **TMail_V4**

  Pour la transmission d'e-mails avec adressage du serveur de messagerie avec une adresse IPv4

- **TMail_V6**

  Pour la transmission d'e-mails avec adressage du serveur de messagerie avec une adresse IPv6

- **TMail_FQDN**

  Pour la transmission d'e-mails avec adressage du serveur de messagerie par son nom (FQDN)

- **TCON_IP_V4_SEC**

  Pour la transmission sécurisée des données via TCP

- **TCON_QDN_SEC**

  Pour la transmission sécurisée de données via le nom d'hôte

- **TMail_V4_SEC**

  Pour la transmission sécurisée d'e-mails avec adressage du serveur de messagerie avec une adresse IPv4

- **TMail_V6_SEC**

  Pour la transmission sécurisée d'e-mails avec adressage du serveur de messagerie avec une adresse IPv6

- **TMail_QDN_SEC**

  Pour la transmission sécurisée d'e-mails avec adressage du serveur de messagerie avec les noms d'hôte

Note concernant TMail_Vx_SEC / TMail_QDN_SEC :
Pour ces SDT, le certificat du serveur de messagerie est contrôlé mais pas l'ID du certificat "TLSServerCertRef" (référence interne STEP 7).

Les SDT et leurs paramètres sont décrits dans le système d'information de STEP 7 sous leur nom respectif.

Connexion et déconnexion

Le bloc de programme TCON permet d'établir des connexions. Veuillez noter qu'il faut appeler un bloc de programme TCON particulier pour chaque connexion.

Il faut établir une connexion particulière pour chaque partenaire de communication, même si les blocs de données transmis sont identiques.

Après transmission des données, la connexion peut être coupée. La connexion est coupée par l'appel de TDISCON.

Remarque

Déconnexion

Si une connexion est coupée par le partenaire de communication ou par une perturbation du réseau, la connexion doit tout de même être coupée par l'appel de TDISCON. Tenez-en compte lors de la programmation.

5.2 Modification de l'adresse IP en cours de fonctionnement

Modification de l'adresse IP en cours de fonctionnement

Vous pouvez modifier par programmation les paramètres d'adresse suivants du CP :

- Adresse IP
- Masque de sous-réseau
- Adresse de routeur

Remarque

Modification des paramètres IP en cas d'adresse IP dynamique

Tenez compte des conséquences d'une modification programmée des paramètres IP au cas où le CP obtient une adresse IP dynamique du routeur connecté : le cas échéant les partenaires de communication ne pourront plus accéder au CP.

Conditions - Version de firmware

Les conditions pour la modification programmée des paramètres IP sont :

- firmware du CP ≥ V2.1.7x

  et

- firmware de la CPU ≥ V4.2

Conditions - Blocs de programme / Versions STEP 7

La modification programmée des paramètres IP est prise en charge par des blocs de programme : Les blocs de programme accèdent aux données d'adresse qui sont enregistrées dans le type de données système (SDT) approprié.

Outre les paramètres d'adresse du CP, vous pouvez également modifier par programmation avec T_CONFIG les paramètres d'adresse de serveurs DNS (IF_CONF_DNS) et de serveurs NTP (IF_CONF_NTP).

Selon la version de STEP 7, vous pouvez utiliser les blocs de programme et types de données système suivants :

- **STEP 7 Basic ≥ V14**

  T_CONFIG

  en relation avec :

  – IF_CONF_V4

  – IF_CONF_NTP

  – IF_CONF_V6

  – IF_CONF_DNS

  Les paramètres d'adresse ne peuvent être configurés que temporairement sur le CP. Dans chaque SDT "IF_CONF_...", il faut activer le paramètre "Mode" = 2.

  Remarque

  Pas de retour d'information du CP

  "T_CONFIG" ne prend pas en charge les retours d'information du CP à la CPU. Les erreurs d'appel de bloc ou de paramètres d'adresse ne sont pas signalées. Que le paramètre d'adresse ait été activé ou non, le bloc signale "BUSY" ou "DONE".

- **STEP 7 Basic ≤ V14**

  TC_CONFIG

  en relation avec :

  – IF_CONF_V4

Vous trouverez des d'informations plus détaillées sur la programmation des blocs et du SDT dans le système d'information STEP 7.

Conditions - Programmation du CP

Pour pouvoir modifier les paramètres IP par programmation, il faut avoir activé l'option "Autoriser adaptation de l'adresse IP directement sur l'appareil" dans la configuration de l'adresse IP de l'interface Ethernet du CP.

Diagnostic et maintenance

6

6.1 Possibilités de diagnostic

Vous disposez des options de diagnostic ci-après.

LED du module

Vous trouverez des informations sur les indications fournies par les LED au chapitre LED (Page 28).

STEP 7 : L'onglet "Diagnostic" dans la fenêtre d'inspection

Il fournit les informations suivantes sur l'état en ligne du module sélectionné :

STEP 7 Basic : Fonctions de diagnostic via le menu "En ligne" > "En ligne & diagnostic".

Vous pouvez lire les informations de diagnostic sur le CP via les fonctions en ligne à partir d'une station d'ingénierie sur laquelle est enregistré le projet du CP.

Si vous voulez exploiter le diagnostic en ligne avec la station via le CP, vous devez au préalable activer le type de communication "Activer les fonctions en ligne", voir chapitre Types de communication (Page 46).

Groupe "Diagnostic"

Les pages de diagnostic sont réparties en groupes comme suit :

- **Général**

  Ce groupe affiche des informations générales sur le module.

- **État de diagnostic**

  Ce groupe affiche des informations d'état du module du point de vue de la CPU.

  – Évènements spécifiques appareil

    Ce groupe affiche des informations sur des évènements internes du module.

- **Interface Ethernet**

  Informations d'adresse et statistiques

- **Industrial Remote Communication**

  Le groupe comprend les pages de diagnostic suivantes :

  – Partenaire

    Informations sur l'adressage du partenaire, statistiques de connexion, données de configuration du partenaire et autres informations de diagnostic

  – Liste de point de données

    Informations diverses sur les points de données telles que données de configuration, valeur, état de la connexion, etc.

  – Diagnostic de protocole

    Le bouton "Activer la fonction Protocol-Trace" recopie durant quelques secondes les télégrammes reçus et envoyés par le module.

    L'option "Désactiver la fonction Protocol-Trace" arrête la journalisation et les données sont transférées dans un fichier journal.

    L'option "Enregistrer" permet d'enregistrer le fichier journal sur la station d'ingénierie et de l'analyser.

- **Heure**

  Informations sur l'heure de l'appareil

- **Security**

  Le groupe comprend les pages de diagnostic suivantes :

  – État

    Cette page de diagnostic affiche les principaux paramètres de sécurité des données, l'heure et les données de configuration.

  – Journal système

    Sur cette page de diagnostic, vous pouvez, à condition qu'une connexion ait été établie à un module SCALANCE S, démarrer la journalisation des entrées système. Vous pouvez enregistrer les entrées.

  – Journal de sécurité

    Sur cette page de diagnostic, vous pouvez démarrer l'enregistrement des données de journal du module. Vous pouvez enregistrer les entrées.

  – État de communication

    Cette page de diagnostic affiche les états des modules de sécurité des données connus du groupe VPN, leurs nœuds d'extrémité et les propriétés du tunnel.

  – SINEMA RC - Configuration VPN automatique

    Cette page de diagnostic affiche l'état de la configuration OpenVPN automatique et des connexions OpenVPN.

Groupe "Fonctions"

- **Mise à jour du firmware**

  Pour la description, voir chapitre Chargement du firmware (Page 97).

- **Affecter une adresse IP**
- **Attribuer un nom d'appareil PROFINET**
- **Enregistrer les données de maintenance**

  Cette fonction permet de journaliser des processus internes du module au cas ou vous ne seriez pas en mesure de remédier vous-même à un comportement inattendu ou indésirable du module.

  Le bouton "Enregistrer les données de maintenance" crée le fichier journal. Les données sont enregistrées dans une fichier au format "*.dmp" exploitable par l'assistance technique Siemens.

E-mail de diagnostic

Dans le cas d'évènements configurés, tels que l'ARRÊT de la CPU, le CP peut envoyer un e-mail de diagnostic. Pour la configuration, voir "Messages".

État du partenaire

En cas d'utilisation de la communication Telecontrol, le CP peut signaler à la CPU l'état de la connexion au partenaire de communication via une variable. Vous pouvez afficher l'état de la variable via le serveur Web de la CPU. La variable se configure dans le groupe de paramètres suivant :

- TeleControl Basic : "Stations partenaires"
- DNP3 / CEI : "Communication avec la CPU"

Diagnostic CP

Le CP peut enregistrer des données de diagnostic étendues dans des variables d'API. Vous pouvez afficher les états des variables d'API à l'aide du serveur Web de la CPU.

Pour la configuration, voir chapitre Diagnostic CP (Page 54).

Serveur Web de la CPU

Le CP vous permet d'accéder au serveur Web de la CPU et aux informations qui y sont disponibles. Concernant l'accès, voir chapitre Accès au serveur Web (Page 52).

SNMP

Pour les fonctions, voir chapitre SNMP (Page 94).

6.2 Serveur Web S7-1200 : Établissement d'une connexion

Établissement d'une connexion au serveur Web

Procédez comme suit pour vous connecter à partir d'un PC au serveur Web de la CPU.

Conditions requises dans la configuration de la CPU

1. Ouvrez le projet voulu sur la station d'ingénierie.
2. Sélectionnez sous STEP 7 la CPU de la station concernée.
3. Sélectionnez l'entrée "Serveur Web".
4. Dans le groupe de paramètres "Général" activez l'option "Activer le serveur Web sur ce module".
5. Dans le cas d'une CPU version V4.0 et suivantes, créez dans la gestion des utilisateurs un utilisateur possédant les droits requis.

La marche à suivre pour établir une liaison au serveur Web varie selon que, dans le groupe de paramètres "Général", l'option "Autoriser uniquement l'accès via HTTPS" est activée ou désactivée :

- **Connexion via HTTP**

  Marche à suivre si l'option "Autoriser uniquement l'accès via HTTPS" est désactivée

- **Connexion via HTTPS**

  Marche à suivre si l'option "Autoriser uniquement l'accès via HTTPS" est activée

Ces deux variantes sont décrites dans les sections ci-après.

Les conditions requises pour accéder au serveur Web de la CPU (navigateurs agréés) et la description de la marche à suivre se trouvent dans le système d'information STEP 7 sous le mot clé "Informations utiles sur le serveur Web".

Connexion via HTTP

1. Connectez le PC à la CPU via l'interface Ethernet.
2. Entrez l'adresse de la CPU dans le champ d'adresse de votre navigateur Web : http://<Adresse IP>
3. Appuyez sur la touche d'entrée <Entrée>

   La page d'accueil du serveur Web s'ouvre.
4. Cliquez sur l'entrée "Télécharger certificat" en haut à droite dans la fenêtre.

   La boîte de dialogue "Certificat" s'ouvre.
5. Chargez le certificat sur votre PC en cliquant sur le bouton "Installer certificat..."

   Le certificat est chargé sur votre PC.

   Vous trouverez des informations sur le chargement du certificat dans l'aide de votre navigateur et dans le système d'information STEP 7 sous les mots clé "HTTPS" et "Accès par HTTPS (S7-1200)

6. Lorsque la connexion est passée en mode sécurisé HTTPS ("https://<Adresse IP>/..." dans le champ d'adresse du serveur Web), vous pouvez continuer comme décrit dans la section ci-après.

   Si vous coupez la connexion au serveur Web, vous pourrez vous connecter la prochaine fois au serveur Web via HTTP sans charger de certificat.

Connexion via HTTPS

1. Connectez le PC à la CPU via l'interface Ethernet.
2. Entrez l'adresse de la CPU dans le champ d'adresse de votre navigateur Web : https://<Adresse IP>
3. Appuyez sur la touche d'entrée <Entrée>

   La page d'accueil du serveur Web s'ouvre.
4. Connectez-vous en tant qu'utilisateur avec les droits requis sur la page d'accueil du serveur Web.

   Utilisez les identifiants configurés dans la gestion des utilisateurs du serveur Web de la CPU.
5. Après vous être connecté, sélectionnez, dans le navigateur l'entrée "Etat du module"
6. Sélectionnez le CP dans la liste des modules.

   Les contenus spécifiques CP s'affichent.

6.3 Diagnostic de sécurité en ligne via le port 8448

Diagnostic de sécurité des données via le port 8448

Conditions :

- L'accès au serveur Web de la station via HTTPS a été activé.
- Si le pare-feu est activé, l'accès doit avoir été autorisé.

Si vous voulez exécuter un diagnostic de sécurité des données sous STEP 7 Professional, procédez comme suit :

1. Sélectionnez le CP sous STEP 7.
2. Ouvrez le menu contextuel "En ligne & diagnostic".
3. Dans le groupe de paramètres "Security", cliquez sur le bouton "Établir la connexion en ligne".

Vous exécutez ainsi le diagnostic de sécurité via le port 8448.

Voir aussi

Paramètres pour le diagnostic de sécurité en ligne et le chargement sur la station tandis que le pare-feu est activé (Page 59)

6.4 SNMP

SNMP (Simple Network Management Protocol)

SNMP est un protocole pour la gestion et le diagnostic de réseaux et d'abonnés de réseau. Pour la transmission de données, SNMP se sert du protocole sans connexion UDP.

Les informations sur les propriétés des appareils compatibles SNMP sont enregistrées dans des fichiers MIB (MIB = Management Information Base).

Fonctionnalités du CP en tant qu'agent SNMP

Le CP prend en charge la requête de données via SNMP dans les versions suivantes :

- SNMPv1 (standard)
- SNMPv3 (Security)

Il délivre alors le contenu d'objets MIB de la MIB II standard selon RFC1213.

- **MIB II**

  Le CP prend en charge les groupes suivants d'objets MIB :

  – System

  – Interfaces

    L'objet MIB "Interfaces" fournit des informations d'état via les interfaces du CP.

  – IP

  – ICMP

  – TCP

  – UDP

  – SNMP

  Les groupes suivants de la MIB II standard ne sont pas pris en charge :

  – Adress Translation (AT)

  – EGP

  – Transmission

- **LLDP MIB**

Les traps ne sont pas pris en charge par le CP.

Vous trouverez des informations complémentaires sur les fichiers MIB et SNMP dans le manuel /5/ (Page 108).

Configuration

Pour la configuration, voir :

- Si les fonctions de sécurité sont désactivées (SNMPv1) : SNMP (Page 56)
- Si les fonctions de sécurité sont activées (SNMPv1 / SNMPv3) : SNMP (Page 62)

6.5 État de traitement d'e-mails

Configuration de l'état de traitement d'e-mails

Les identifications d'état s'appliquent aux e-mails qui ont été configurés dans l'éditeur de messages du CP. L'émission d'identificateurs d'état est autorisée par l'option "Activer identificateur d'état de traitement". L'identificateur d'état est inscrit dans la "Variable d'API d'état de traitement" sur la CPU.

Pour la configuration, voir chapitre Configuration de la messagerie (Page 60).

Émission de l'état de traitement d'e-mails

L'état de traitement est retourné, après remise d'un message à envoyer, par le CP même ou par les serveurs du service.

En cas de problèmes de notification de messages, vous pouvez vérifier l'état à l'aide du serveur Web de la CPU.

État de traitement d'e-mails

Les identificateurs d'états livrés par la "Variable d'API d'état de traitement" signifient :

Tableau 6- 1 Signification de l'identificateur d'état émis au format hexadécimal

État	Signification
0000	Transmission terminée sans erreur
82xx	Autre message d'erreur du serveur de messagerie Mis à part le "8" qui précède, le message correspond au code d'erreur à trois chiffres du protocole SMTP.
8401	Aucun canal disponible. Cause possible : Il existe déjà une liaison e-mail via le CP. Il n'est pas possible d'établir une seconde liaison en parallèle.
8403	Impossible d'établir une liaison TCP/IP au serveur SMTP.
8405	Le serveur SMTP à rejeté la requête de connexion.
8406	Une erreur SSL interne ou un problème de structure de certificat a été détecté sur le client SMTP.
8407	La requête d'utilisation de SSL a été rejetée.
8408	Le client n'a pas trouvé d'interface pour l'établissement d'une liaison TCP/IP au serveur de messagerie.
8409	Cette liaison ne permet pas d'écrire. Cause possible : Le partenaire de communication à réinitialisé ou coupé la liaison.
8410	Cette liaison ne permet pas de lire. Cause possible : Le partenaire de communication a coupé la liaison ou la liaison a été interrompue.
8411	L'envoi de l'e-mail a échoué. Cause : L'espace mémoire était insuffisant pour exécuter l'émission.
8412	Le serveur DNS configuré n'a pas pu résoudre le nom de domaine indiqué.
8413	En raison d'une erreur interne du sous-système DNS, il n'a pas été possible de résoudre le nom de domaine.

État	Signification
8414	Le nom de domaine entré est une chaîne de caractères vide.
8415	Une erreur interne s'est produite dans le module cURL. L'exécution a été abandonnée.
8416	Une erreur interne s'est produite dans le module SMTP. L'exécution a été abandonnée.
8417	Requête à SMTP sur un canal déjà utilisé ou ID de canal non valide. L'exécution a été abandonnée.
8418	L'envoi de l'e-mail a été abandonné. Cause possible : Dépassement du temps d'exécution.
8419	Le canal a été interrompu et n'est pas utilisable tant que la liaison n'est pas coupée.
8420	La chaîne de certificats du serveur n'a pas pu être vérifiée avec le certificat racine du CP.
8421	Une erreur interne est survenue. L'exécution a été suspendue.
8450	L'action n'a pas été exécutée : boîte à lettre non disponible / non joignable. Réessayez plus tard.
84xx	Autre message d'erreur du serveur de messagerie Mis à part le "8" qui précède, le message correspond au code d'erreur à trois chiffres du protocole SMTP.
8500	Erreur de syntaxe : commande inconnue. Inclus également l'erreur de chaîne de commande trop longue. Ceci peut être dû au fait que le serveur de messagerie ne prend pas en charge la procédure d'authentification LOGIN. Essayez d'envoyer des e-mails sans authentification (sans nom d'utilisateur).
8501	Erreur de syntaxe. Vérifiez les données de configuration suivantes : Configuration de messages > Données d'e-mail (Content) : • Adresse de destinataire ("A" ou "Cc").
8502	Erreur de syntaxe. Vérifiez les données de configuration suivantes : Configuration de messages > Données d'e-mail (Content) : • Adresse e-mail (expéditeur)
8535	Authentification SMTP incomplète. Vérifiez dans la configuration du CP les paramètres "Nom d'utilisateur" et "Mot de passe".
8550	Le serveur SMTP n'est pas joignable. Vous ne possédez par de droits d'accès. Vérifiez les données de configuration suivantes : • Configuration du CP > Configuration de la messagerie : – Nom d'utilisateur – Mot de passe – Adresse e-mail (expéditeur) • Configuration de messages > Données d'e-mail (Content) : – Adresse de destinataire ("A" ou "Cc").
8554	La transmission a échoué
85xx	Autre message d'erreur du serveur de messagerie Mis à part le "8" qui précède, le message correspond au code d'erreur à trois chiffres du protocole SMTP.

6.6 Chargement du firmware

Nouvelles versions de firmware du CP

Dès qu'il existe une nouvelle version de firmware pour le module, elle est mise à disposition sur le site Internet Siemens Industry Online Support à l'adresse suivante :
Link: (https://support.industry.siemens.com/cs/ww/fr/ps/15922/dl)

Veuillez noter que les versions de firmware V3 et suivantes ne sont pas chargeables sur des CP de version 1.

Pour charger un nouveau fichier de firmware sur le CP, vous disposez de trois options :

- enregistrer le fichier de firmware sur la carte mémoire de la CPU

  Vous trouverez une description de la marche à suivre pour le chargement sur la carte mémoire de la CPU, sur le site Internet de l'Industry Online Support Siemens.
- charger le firmware avec les fonctions en ligne de STEP 7 via WAN

Remarque

Conséquences pour la mémoire rémanente de la CPU

- Si vous utilisez une carte SIMATIC Memory Card pour installer le fichier de firmware, la mémoire rémanente est préservée.
- Si vous utilisez les fonctions en ligne pour installer le fichier de firmware, le contenu de la mémoire rémanente est perdu.

Le chargement du firmware est visualisé par le clignotement des LED du CP, voir LED (Page 28).

Charger le firmware avec les fonctions en ligne de STEP 7 via WAN

Conditions :

- Le CP est accessible via son adresse IP.
- La station d'ingénierie et le CP se trouve dans le même sous réseau.
- Le nouveau fichier de firmware est enregistré sur la station d'ingénierie.

Marche à suivre :

1. Connectez la station d'ingénierie au réseau.
2. Ouvrez le projet STEP 7 voulu sur la station d'ingénierie.
3. Sélectionnez le CP ou la CPU de la station dont le CP doit être mis à jour par un nouveau firmware.
4. Activez les fonctions en ligne avec l'icône "Liaison en ligne".
5. Dans le dialogue "Liaison en ligne", sélectionnez dans la zone de liste déroulante "Type d'interface PG/PC" l'interface Ethernet "PN/IE".

6. Sélectionnez l'emplacement du CP ou de la CPU.

   Les voies sont possibles.

7. Connectez-vous avec le bouton "Connecter".

L'assistant "Liaison en ligne" vous guide à travers les étapes suivantes.

Vous trouverez dans le système d'information de STEP 7 une aide plus détaillée sur les fonctions en ligne.

6.7 Echange de module

Echange de module

⚠ PRUDENCE

Lisez le manuel système "Automate programmable S7-1200"

Avant de procéder au montage, à la connexion et à la mise en service, lisez les sections correspondantes du manuel système "Automate programmable S7-1200" (voir références bibliographique en annexe).

Effectuez le montage et la connexion comme indiqué dans les descriptions du manuel système "Automate programmable S7-1200 ".

Veuillez vous assurer que l'alimentation est bien coupée durant le montage/démontage des appareils.

Les données de projet STEP -7 du CP sont enregistrées sur la CPU locale. Ceci simplifie l'échange du CP dans la mesure où il n'est pas nécessaire de charger à nouveau les données de projet sur la station.

Au redémarrage de la station, le nouveau CP lit les données de projet sur la CPU.

Exception :
Les données de la configuration SINEMA RC et le certificat du serveur SINEMA RC sont enregistrés sur le CP. Elles ne peuvent pas être lues par la CPU.

Caractéristiques techniques 7

7.1 Caractéristiques techniques du CP 1243-1

Tableau 7- 1 Caractéristiques techniques du CP 1243-1

Caractéristiques techniques		
Numéro d'article :	6GK7 243-1BX30-0XE0	
Connexion au réseau Industrial Ethernet		
Nombre	1	
Exécution	Connecteur femelle RJ45	
Propriétés	100BASE-TX, IEEE 802.3-2005, semi-duplex/duplex intégral, autocroisement, autonégociation, séparation galvanique	
Vitesse de transmission	10 / 100 Mbit/s	
Longueurs de câble admissibles (Ethernet)	**(combinaisons alternatives par plage de longueurs) ***	
0 ... 55 m	• max. 55 m IE TP Torsion Cable avec IE FC RJ45 Plug 180 • max. 45 m IE TP Torsion Cable avec IE FC RJ45 + 10 m TP Cord via IE FC RJ45 Outlet	
0 ... 85 m	• max. 85 m IE FC TP Marine/Trailing/Flexible/FRNC/Festoon/Food Cable avec IE FC RJ45 Plug 180 • max. 75 m IE FC TP Marine/Trailing/Flexible/FRNC/Festoon/Food Cable + 10 m TP Cord via IE FC RJ45 Outlet	
0 ... 100 m	• max. 100 m IE FC TP Standard Cable avec IE FC RJ45 Plug 180 • max. 90 m IE FC TP Standard Cable + 10 m TP Cord via IE FC RJ45 Outlet	
Caractéristiques électriques		
Alimentation	au niveau du bus interne du S7-1200	DC 5 V
Consommation typique)	au niveau du bus interne du S7-1200	250 mA
Puissance dissipée (typique)	au niveau du bus interne du S7-1200	1,25 W
Conditions ambiantes admissibles		
Température ambiante	Pendant l'exploitation, le châssis étant monté horizontalement	-20 °C à +70 °C
	Pendant l'exploitation, le châssis étant monté verticalement	-20 °C à +60 °C
	Pendant le stockage	-40 °C ... +70 °C
	Pendant le transport	-40 °C ... +70 °C
Humidité relative de l'air	En fonctionnement	≤ 95 % à 25 °C, sans condensation

Caractéristiques techniques	
Forme, dimensions et poids	
Format du module	module compact S7-1200, simple largeur
Degré de protection	IP20
Poids	122 g
Dimensions (L x H x P)	30 x 110 x 75 mm
Possibilités de montage	Rail DIN symétrique Tableau de commande
Fonctions produit **	

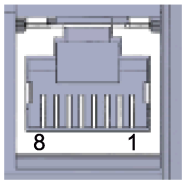
***** Pour plus de détails, voir catalogue IK PI, Technique de câblage
****** Vous trouverez d'autres propriétés et caractéristiques de performances au chapitre Application et fonctions (Page 13).

7.2 Brochage de l'interface Ethernet

Brochage de l'interface Ethernet

Le tableau suivant indique le brochage de l'interface Ethernet. Le brochage est conforme à la norme Ethernet 802.3-2005 en version 100BASE-TX.

Tableau 7- 2 Brochage de l'interface Ethernet

Vue du connecteur femelle RJ45	Broche	Nom de signal	Brochage
	1	TD	Transmit Data +
	2	TD_N	Transmit Data -
	3	RD	Receive Data +
	4	GND	Ground
	5	GND	Ground
	6	RD_N	Receive Data -
	7	GND	Ground
	8	GND	Ground

Homologations

A

Homologations accordées

Remarque

Homologations accordées sur la plaque signalétique de l'appareil

Les homologations mentionnées ne sont valables que si le marquage approprié a été apposé sur le produit. Pour savoir quelles homologations ont été attribuées au produit, veuillez vous référer aux marquages de la plaque signalétique.

Le CP possède les homologations suivantes et est conforme aux normes ci-après :

Déclaration de conformité de l'UE

CE

Le CP est conforme aux exigences et objectifs de sécurité des directives suivantes de l'UE ainsi qu'aux normes européennes harmonisées (EN) pour automates programmables qui ont été publiées dans les journaux officiels de l'UE.

- **2014/34/EU (Directive ATEX de protection contre l'explosion)**

  Directive du Parlement européen et du Conseil du 26 février 2014 concernant le rapprochement des législations des États membres pour les appareils et les systèmes de protection destinés à être utilisés en atmosphères explosibles ; journal officiel de l'UE L96, 29/03/2014, p. 309-356

- **2014/30/UE (CEM)**

  Directive CEM du Parlement européen et du Conseil du 26 février 2014 relative au rapprochement des législations des États membres concernant la compatibilité électromagnétique ; journal officiel de l'UE L96, 29/03/2014, p. 79-106

- **2011/65/UE (RoHS)**

  Directive du Parlement européen et du Conseil du 8 juin 2011 relative à la limitation de l'utilisation de certaines substances dangereuses dans les équipements électriques et électroniques

La déclaration de conformité UE est fournie à toutes les autorités compétentes par :

Siemens Aktiengesellschaft
Digital Industries
BP 48 48
90026 Nuremberg
Allemagne

La déclaration de conformité UE de ce produit se trouve sur Internet à l'adresse suivante :

Link: (https://support.industry.siemens.com/cs/ww/fr/ps/15922/cert) > "Déclaration de conformité de l'UE"

IECEx

Le produit satisfait aux exigences de protection en atmosphère explosible selon CEI Ex.

Classification IECEx :

- Ex ec IIC T4 Gc

  Certificat : IECEx DEK 18.0019X

  Normes appliquées :

  – EN 60079-0 - Explosive atmospheres - Part 0: Equipment - General requirements

  – EN 60079-7 - Explosive Atmospheres - Part 7: Equipment protection by increased safety 'e'

Les éditions en vigueur des normes peuvent être consultées dans le certificat IECEx qui est disponible sur Internet à l'adresse suivante :
Link: (https://support.industry.siemens.com/cs/ww/fr/ps/15922/cert)

Il convient de se conformer aux conditions d'une mise en œuvre du produit en toute sécurité telles que spécifiées au chapitre Consignes pour une mise en œuvre en atmosphère explosible selon ATEX / IECEx (Page 35).

Tenez également compte des indications du document "Use of subassemblies/modules in a Zone 2 Hazardous Area" que vous trouverez sur Internet à l'adresse suivante :
Lien : (https://support.industry.siemens.com/cs/ww/fr/view/78381013)

ATEX

Le produit satisfait à toutes les exigences de la directive de l'UE 2014/34/UE sur les "Appareils et systèmes de protection destinés à être utilisés en atmosphères explosibles".

Homologation ATEX :

- II 3 G Ex ec IIC T4 Gc

  Type Examination Certificate: DEKRA 18 ATEX 0027X

  Normes appliquées :

  – EN 60079-0 - Explosive atmospheres - Part 0: Equipment - General requirements

  – EN 60079-7 - Explosive Atmospheres - Part 7: Equipment protection by increased safety 'e'

⚠ ATTENTION

Respect des directives de montage

Le produits répond aux spécifications si vous tenez compte des points suivants lors de l'installation et de l'exploitation :

- des instructions du chapitre Note importante concernant la mise en œuvre des appareils (Page 33)
- des règles d'installation du document /1/ (Page 107)

Les versions de norme en vigueur sont indiquées dans la déclaration de conformité UE, voir ci-dessus.

Il convient de se conformer aux conditions d'une mise en oeuvre du produit en toute sécurité telles que spécifiées au chapitre Consignes pour une mise en œuvre en atmosphère explosible selon ATEX / IECEx (Page 35).

Tenez également compte des indications du document "Use of subassemblies/modules in a Zone 2 Hazardous Area" que vous trouverez ici :

- Dans SIMATIC NET Manual Collection sous
  "Tous les documents" >"Use of subassemblies/modules in a Zone 2 Hazardous Area"
- Sur Internet à l'adresse suivante :
  Lien : (https://support.industry.siemens.com/cs/ww/fr/view/78381013)

c(UL)us

Normes appliquées :

- Underwriters Laboratories, Inc.: UL 61010-1 (Safety Requirements for Electrical Equipment for Measurement, Control, and Laboratory Use - Part 1: General Requirements)
- IEC/UL 61010-2-201 (Safety requirements for electrical equipment for measurement, control and laboratory use. Particular requirements for control equipment)
- Canadian Standards Association: CSA C22.2 No. 142 (Process Control Equipment)

File Number: E223122

cULus Hazardous (Classified) Locations

Underwriters Laboratories, Inc.: cULus IND. CONT. EQ. FOR HAZ. LOC.

Normes appliquées :

- ANSI ISA 12.12.01
- CSA C22.2 No. 213-M1987

APPROVED for Use in:

- Cl. 1, Div. 2, GP. A, B, C, D T4A; Ta = -20 °C...60 °C
- Cl. 1, Zone 2, GP. IIC T4; Ta = -20 °C...60 °C

Report / UL file: E223122 (NRAG.E223122)

Conformez-vous aux conditions d'une mise en oeuvre du CP en toute sécurité telles que spécifiées au chapitre Consignes pour une mise en œuvre en atmosphère explosible conformément à UL HazLoc (Page 35).

FM

Factory Mutual Approval Standard Class Number 3600, 3611, 3810, ANSI/ISA-61010-1

Equipment rating:
Class I, Division 2, Group A, B, C, D, Temperature Class T4A, Ta = 60 °C
Class I, Zone 2, Group IIC, Temperature Class T4, Ta = 60 °C

Report Number: 3049779, 3049925

Conformez-vous aux conditions d'une mise en oeuvre du CP en toute sécurité telles que spécifiées au chapitre Consignes pour une mise en œuvre en atmosphère explosible conformément à FM (Page 36).

Australie - RCM

Le CP remplit les exigences des normes selon AS/NZS 2064 (classe A).

EAC (Eurasian Conformity)

Union douanière de Russie, Biélorussie et Kazakhstan

Déclaration de conformité aux règles techniques de l'union douanière (TR CU)

Homologations actuelles

Les produits SIMATIC NET sont régulièrement présentés aux autorités compétentes en vue de leur homologation en fonction de marchés et d'applications définis.

Veuillez contacter votre agence Siemens pour obtenir une liste à jour des homologations des divers appareils ou renseignez-vous sur les sites Internet du Siemens Industry Online Support.

Link: (https://support.industry.siemens.com/cs/ww/fr/ps/15922/cert)

Dessins cotés

B

Remarque

Toutes les dimensions des dessins du CP sont indiquées en millimètres.

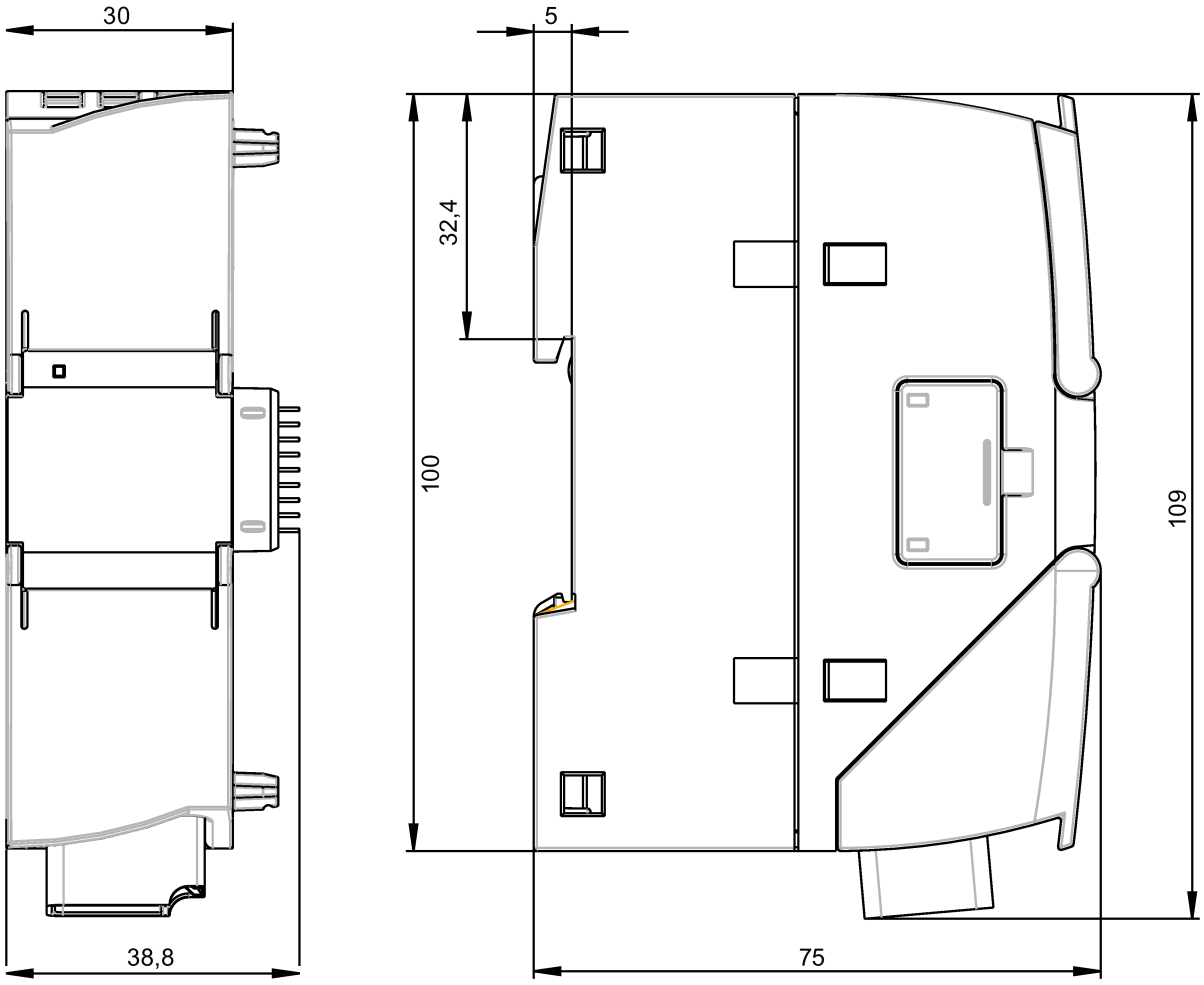


Figure B-1 Vue de face et du côté gauche

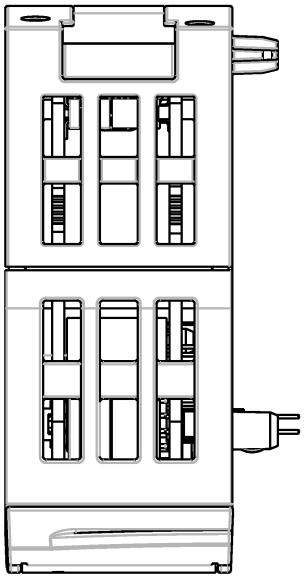


Figure B-2 Vue de dessus

Bibliographie

C

Comment trouver la documentation Siemens

- Références

  Les références des produits Siemens en question ici figurent dans les catalogues suivants :

  – SIMATIC NET - Communication industrielle / Identification industrielle, catalogue IK PI

  – SIMATIC - Produits pour Totally Integrated Automation et Micro Automation, catalogue ST 70

  Vous pouvez vous procurer ces catalogues ainsi que des informations complémentaires auprès des agences Siemens. Vous trouverez également les informations produit sur le site Siemens Industry Mall à l'adresse suivante :

  Lien : (https://mall.industry.siemens.com)

- Manuels sur Internet

  Les manuels SIMATIC NET se trouvent également sur les pages Internet du Siemens Industry Online Support :

  Lien : (https://support.industry.siemens.com/cs/ww/fr/ps/15247/man)

  Naviguez dans l'arborescence des produits jusqu'au produit voulu et procédez au paramétrage suivant :

  Type d'article "Manuels"

- Manuels sur supports de données

  Les manuels des produits SIMATIC NET se trouvent aussi sur le support de données joint à de nombreux produits SIMATIC NET.

/1/

SIMATIC
Automate programmable S7-1200
Manuel système
Siemens AG
Lien : (https://support.industry.siemens.com/cs/ww/fr/ps/13683/man)

/2/

SIMATIC NET
CP 1243-1
Instructions de service
Siemens AG
Link: (https://support.industry.siemens.com/cs/ww/fr/view/103948898)

/3/

SIMATIC NET
TeleControl Server Basic (version V3)
Instructions de service
Siemens AG
Lien : (https://support.industry.siemens.com/cs/ww/fr/ps/15918/man)

/4/

SIMATIC NET - TeleControl
Siemens AG
Manuels de configuration pour les protocoles :
- TeleControl Basic
- SINAUT ST7
- DNP3
- CEI 60870-5
Lien : (https://support.industry.siemens.com/cs/ww/fr/ps/21764/man)

/5/

SIMATIC NET
Diagnostic et configuration avec SNMP
Manuel de diagnostic
SIEMENS AG
Link: (https://support.industry.siemens.com/cs/ww/fr/ps/15392/man)

Index

S

T

V