SIEMENS

SIMATIC NET

S7-1500 - Industrial Ethernet CP 1545-1

Instructions de service

Avant-propos

Application et fonctions 1

LED, connecteurs 2

Montage, connexion, mise en service, utilisation 3

Configuration 4

Blocs de programme 5

Diagnostic et maintenance 6

Caractéristiques techniques 7

Homologations 8

Dessins cotés 9

Guide de la documentation A

Messages Syslog B

12/2019

C79000-G8977-C499-02

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

C79000-G8977-C499-02
℗ 12/2019 Sous réserve de modifications

Copyright © Siemens AG 2019.
Tous droits réservés

Avant-propos

ATTENTION

Pour éviter de vous blesser, lisez le manuel avant d'utiliser l'appareil.

Validité du document

Le document est valable pour le produit suivant :

- CP 1545-1
  Numéro d'article 6GK7545-1GX00-0XE0
  Version du matériel 1
  Version du firmware V1.0

  Processeur de communication pour la connexion de SIMATIC S7-1500 à Industrial Ethernet
  Fonctions de communication : TCP/IP, UDP, S7, client/serveur FTP, messagerie, connexion à des systèmes de Cloud via MQTT



Figure 1 S7-1500 avec CP 1545-1 (à droite)

Objet du document

Le document décrit l'utilisation et les propriétés de l'appareil. Il vous assiste lors de la configuration et montre des possibilités de maintenance et de diagnostic.

Connaissances requises

Pour monter, mettre en service et utiliser l'appareil, vous devez posséder des connaissances dans les domaines suivants :

- électrotechnique générale
- Technique d'automatisation / STEP 7 Professional

Désignations de produit et abréviations

Vous trouverez dans ce document les désignations et abréviations suivantes :

- **CP / appareil / module**

  Désignations du processeur de communication CP 1545-1

- **ES**

  Station d'ingénierie (STEP 7 Professional)

- **Station**

  Station SIMATIC S7

- **WBM**

  Abréviation du "Web Based Management", c.-à-d. les pages web de l'application pour données de configuration et de diagnostic.

Document sur Internet

L'édition courante de ce document est disponible sur les pages Internet du Siemens Industry Online Support :
Link: (https://support.industry.siemens.com/cs/ww/fr/ps/25625/man)

Documentation complémentaire

Vous trouverez un exemple d'application du CP à la page suivante :
Link: (https://support.industry.siemens.com/cs/ww/fr/ps/25625/ae)

Vous trouverez de la documentation complémentaire sur S7-1500 sous Guide de la documentation (Page 115).

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 prennent en charge la combinaison de touches <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 le libellé de la licence d'utilisation dans le document suivant qui se trouve sur le support de données fourni :

- OSS_CP15451_99.pdf

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)

Firmware

Le firmware est signé et crypté. Il s'ensuit que seul un firmware d'origine Siemens peut être chargé sur l'appareil.

Appareil défectueux

En cas de panne, veuillez retourner l'appareil à votre agence Siemens. Une réparation sur site n'est pas possible.

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)

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)

Formation, Service & Support

Vous trouverez des informations sur la formation, le service après-vente et l'assistance dans le document multilingue "DC_support_99.pdf" sur le site Internet du Siemens Industry Online Support :

Lien : (https://support.industry.siemens.com/cs/ww/fr/view/38652101)

Sommaire

Avant-propos 3

1 Application et fonctions 11

1.1 Application 11

1.2 Services de communication 11

1.3 Communication en nuage 12

1.4 Autres fonctions 14

1.5 Industrial Ethernet Security 15

1.6 Capacités fonctionnelles et caractéristiques de performance 16
1.6.1 Caractéristiques générales 16
1.6.2 Caractéristiques CloudConnect 17
1.6.3 Caractéristiques de la communication S7 17
1.6.4 Caractéristiques pour OUC et FETCH/WRITE 18
1.6.5 Caractéristiques pour le mode FTP / FTPS 19
1.6.6 Caractéristiques de sécurité des données - Règles de pare-feu 20

1.7 Configuration logicielle requise 20

1.8 Configuration matérielle requise (CPU) 20

2 LED, connecteurs 21

2.1 LED 21

2.2 Interface Gigabit 23

3 Montage, connexion, mise en service, utilisation 25

3.1 Notes importantes concernant la mise en œuvre de l'appareil 25
3.1.1 Consignes pour une mise en œuvre en atmosphère explosible 25
3.1.2 Consignes pour une mise en œuvre en atmosphère explosible selon ATEX / IECEx 26
3.1.3 Consignes pour une mise en œuvre en atmosphère explosible selon UL HazLoc et FM 27

3.2 Montage 29

3.3 Raccordement 31

3.4 Mise en service - Chargement des données de configuration 32

3.5 État de fonctionnement de la CPU : Effet sur le CP 33

4 Configuration 35

4.1 STEP 7 Professional 35

4.2 Recommandations de sécurité 35

4.3 Restriction des services de communication sur la CPU 39

4.4 Configuration IP 39
4.4.1 Particularités de la configuration IP 39

4.4.2 Redémarrage après détection d'une adresse IP double sur le réseau ... 40
4.4.3 Routage IP ... 40
4.4.4 Connexions programmées : Restriction des règles de pare-feu ... 41
4.5 Synchronisation d'horloge ... 41
4.6 Configuration DNS ... 42
4.7 Configuration du serveur FTP ... 42
4.7.1 Configuration de la fonction serveur FTP ... 42
4.7.2 Structure de la liste de configuration FTP ... 44
4.7.3 Accès via FTPS ... 45
4.8 SNMP ... 45
4.9 CloudConnect ... 46
4.9.1 Configuration de l'accès au cloud ... 46
4.9.1.1 Notes à propos de la structure des données et de la configuration ... 46
4.9.1.2 Règles de configuration ... 47
4.9.1.3 Présentation de la configuration ... 49
4.9.1.4 Groupe de paramètres "CloudConnect" ... 50
4.9.1.5 Onboarding dans MindConnect IoT Extension ... 53
4.9.1.6 Zones d'opérandes et variables ... 54
4.9.2 Configuration de rubriques, de groupes et de points de données ... 55
4.9.2.1 Configuration des rubriques et groupes ... 55
4.9.2.2 Configuration des points de données ... 55
4.9.2.3 Types de données ... 57
4.9.2.4 Déclenchement ... 57
4.9.2.5 Format des données utiles ... 61
4.9.2.6 Coupure de la connexion et mise en tampon des données ... 65
4.9.3 Dialogue des propriétés des rubriques ... 67
4.9.3.1 Quality of Service (QoS) ... 67
4.10 Security ... 67
4.10.1 Utilisateur de sécurité des données ... 68
4.10.2 Pare-feu ... 68
4.10.2.1 Ordre des pare-feux lors du contrôle des télégrammes entrants et sortants ... 68
4.10.2.2 Syntaxe correcte de l'adresse IP source (mode de pare-feu avancé) ... 68
4.10.2.3 HTTP et HTTPS via IPv6 ne fonctionne pas ... 68
4.10.3 Fonctions en ligne ... 69
4.10.3.1 Diagnostic de sécurité en ligne via le port 8448 ... 69
4.10.3.2 Paramètres pour le diagnostic de sécurité en ligne et le chargement sur la station tandis que le pare-feu est activé ... 69
4.10.4 Paramètres de journal - Filtrage des évènements système ... 70
4.10.5 Certificats ... 70
4.10.5.1 Certificats tiers ... 70
4.10.5.2 Gestionnaire de certificats ... 71
4.10.5.3 Manipulation de certificats ... 71
5 Blocs de programme ... 75
5.1 Blocs de programme pour la communication ... 75
5.2 Modification de l'adresse IP en cours de fonctionnement ... 79
5.3 Bloc pour la fonction de client FTP ... 80
5.3.1 FTP_CMD ... 80

5.3.2 Paramètres d'entrée de FTP_CMD....82
5.3.3 Blocs de tâche pour FTP_CMD....84
5.3.4 Paramètres de sortie et informations d'état de FTP_CMD....89
5.3.5 Structure du bloc de données (DB fichier) pour le mode client FTP....92
6 Diagnostic et maintenance....97
6.1 Possibilités de diagnostic....97
6.2 Etablir la connexion en ligne....98
6.3 Diagnostic via SNMP....99
6.4 Mise à jour du firmware....101
6.5 Echange de module sans PG....104
7 Caractéristiques techniques....105
7.1 Caractéristiques techniques....105
7.2 Brochage de l'interface Ethernet....106
7.3 Longueurs de câble admissibles - (Ethernet)....106
7.4 Longueurs de câble admissibles - Ethernet Gigabit....106
8 Homologations....107
9 Dessins cotés....113
A Guide de la documentation....115
B Messages Syslog....117
B.1 Structure des messages Syslog....117
B.2 Variables dans les messages Syslog....118
B.3 Messages....120
Index....121

Application et fonctions

1

1.1 Application

Application

Le CP est conçu pour fonctionner dans un automate programmable S7-1500. Le CP permet de connecter le S7-1500 à Industrial Ethernet et à un système de cloud.

En combinant diverses fonctions de sécurité telles que pare-feu et protocoles de cryptage de données, le CP protège le S7-1500, voire des cellules d'automatisation complètes, des intrusions. Il met en outre les communications entre la station S7 et les partenaires de communication à l'abri de l'espionnage et des manipulations.

1.2 Services de communication

Services de communication

Le CP prend en charge les services de communication suivants :

- **Open User Communication (OUC)**

  L'Open User Communication prend en charge, via le CP et des connexions de communication programmées ou configurées, les services de communication suivants :

  – Transport ISO (selon ISO/CEI 8073)

  – TCP (IPv4/IPv6) (selon RFC 793 et 8200)

    Avec son interface, le CP supporte, via des connexions TCPv4/v6, l'interface socket vers TCP/IP disponible sur la quasi totalité des systèmes terminaux.

  – ISO on TCP (selon RFC 1006)

  – UDP (selon RFC 768)

  – multicast via connexion UDP

    Le mode Multicast est possible grâce à un adressage IP approprié lors de la configuration de la connexion.

  – Envoi d'e-mails via SMTP (port 25) ou SMTPS (port 587) avec authentification par un serveur de messagerie.

  Concernant les blocs, voir chapitre Blocs de programme (Page 75).

- **MQTT**

  MQTT pour la connexion du S7-1500 à un système de cloud. Pour les fonctions de communication et systèmes de cloud, voir chapitre Communication en nuage (Page 12).

- **Communication S7**
  - Communication PG
  - Fonctions de conduite et de visualisation (communication IHM)
  - Echange de données via connexions S7
- **FTP/FTPS**

  Fonctions FTP (File Transfer Protocol) de gestion de fichiers et d'accès aux blocs de données sur la CPU
  - Serveur FTP

    Activable via la configuration
  - Client FTP

    Paramétrable par blocs de programme.

    Concernant les blocs, voir chapitre Blocs de programme (Page 75).
- **E-mail**

  Voir ci-dessus (OUC)
- **HTTP/HTTPS**
  - Serveur web de la CPU : Surveillance des données relatives au matériel et au process via HTTP/HTTPS.

    Si vous n'avez pas besoin de la fonctions vous pouvez la désactiver dans la configuration STEP 7 et bloquer le port 80 (groupe de paramètres "Accès au serveur Web").
- **FETCH/WRITE**

  Services FETCH/WRITE comme serveur (selon protocole S5) via connexions ISO-Transport, ISO on TCP et TCP.

  Le S7-1500 avec CP est ici toujours serveur (établissement de connexion passif).

  L'accès en lecture ou écriture (fonction de client avec établissement de connexion actif) est assuré par un automate SIMATIC S5 ou d'une autre marque / un PC.

Pour des informations détaillées sur la configuration des fonctions de communication, veuillez vous référer au système d'aide de STEP 7.

1.3 Communication en nuage

Protocoles pour la connexion au cloud

Pour la communication avec un cloud Broker ou cloud Server le CP prend en charge les protocoles suivants :

- MQTT

  Version 3.1 / 3.1.1 selon la norme OASIS

Systèmes de cloud et fonctions de communication

Le CP prend en charge la connexion à des systèmes de cloud qui supportent une fonctionnalité de broker avec le protocole MQTT.

La configuration de l'accès au cloud ("fournisseur de cloud") est adaptée à la communication avec les systèmes de cloud suivants :

- MindSphere (Siemens)

  Service : MindConnect IoT Extension :

  Fonction du CP :

  – Publisher
- Autre cloud

  Profil pour un autre système de cloud

  Fonction du CP :

  – Publisher

  – Subscriber

  Voir détails ci-dessous.

  Les systèmes de cloud possibles sont :

  – AWS (Amazon)

  Service : IoT Core :

  – Azure (Microsoft)

  Service : IoT Hub :

  – IBM Cloud (IBM)

  Service : Watson IoT Platform :

Fonctions du CP pour la communication avec le cloud

Le tableau ci-après récapitule les fonctions prises en charge avec divers fournisseurs de cloud au moment de la mise sous presse du présent manuel.

Renseignez-vous auprès de votre fournisseur de cloud sur les fonctions prises en charge.

Signification des symboles

- **+**: Pris en charge

Fonction	MindSphere (Siemens)	AWS (Amazon)	Azure (Microsoft)	IBM Cloud (IBM)
Fonction de Publisher du CP	+	+	+	+
Fonctions de Subscriber du CP				+
QoS = 2	+			
MQTT via TLS :	+	+	+	+

1.4 Autres fonctions

Synchronisation d'horloge via NTP (Network Time Protocol)

Le CP émet à intervalles réguliers des requêtes d'horodatage à un serveur NTP et synchronise sont horloge locale.

La date/heure est en outre retransmise aux modules CPU de la station S7 pour synchroniser ainsi les horloges sur l'ensemble de la station S7.

Le CP prend en charge NTP (secure) pour la transmission sécurisée de l'heure.

Adressage via l'adresse MAC prédéfinie d'usine

Il est possible d'accéder à un CP neuf, tel que livré, par l'interface choisie via l'adresse MAC prédéfinie en vue de lui attribuer une adresse IP. L'attribution d'une adresse en ligne s'effectue sous STEP 7.

Agent SNMP

Le CP prend en charge la requête de données via SNMP en version V1 (Simple Network Management Protocol). Il délivre alors le contenu d'objets MIB selon Standard MIB II et Automation System MIB.

Le CP prend en charge SNMPv3 si les fonctions de sécurité des données sont activées.

Configuration IP (IPv4 / IPv6)

- Le CP prend en charge l'utilisation d'adresses IP selon IPv4 et IPv6.
- Vous pouvez configurer la voie et la procédure par laquelle l'adresse IP, le masque de sous-réseau et l'adresse de la passerelle sont attribués au CP.
- La configuration IP et la configuration des connexions (IPv4) peuvent également être affectées au CP via le programme utilisateur, voir chapitre Blocs de programme (Page 75). Ne s'applique pas aux connexions S7.

Routage IP

Le CP prend en charge le routage IP statique (IPv4) vers d'autres CM/CP.

Voir détails au chapitre Routage IP (Page 40).

Adresse IPv6 - Domaine d'utilisation sur le CP

Une adresse IPv6 peut être utilisée pour les services de communication suivants :

- Accès FETCH/WRITE (le CP est serveur)
- Mode serveur FTP
- Mode client FTP avec adressage par bloc de programme
- Transfert d'e-mails avec adressage par bloc de programme

- TCP via blocs OUC avec les SDT suivants : TCON_QDN, TCON_QDN_SEC
- SNMP

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

Accès au serveur web de la CPU

L'interface de réseau local du CP donne accès au serveur web de la CPU. Le serveur web de la CPU permet de lire le données de module d'une station. L'"accès au serveur Web" est activable pour l'interface Ethernet dans la configuration.

Tenez compte de la documentation du serveur Web ; voir Guide de la documentation (Page 115)

Remarque

Accès au serveur Web via HTTPS

Le serveur web d'une station SIMATIC S7-1500 se trouve sur la CPU. C'est pourquoi le certificat SSL de la CPU est affiché lors d'un accès via HTTPS au serveur Web de la station via l'adresse IP du CP.

Mode d'adressage S5/S7 pour FETCH/WRITE

Le mode d'adressage est configurable pour l'accès FETCH/WRITE en mode d'adressage S7 ou S5. Le mode d'adressage indique comment déterminer la position de l'adresse de début lors d'un accès aux données. Le mode d'adressage S7 est applicable aux blocs de données (DB).

Veuillez tenir compte des informations complémentaires de l'aide en ligne de STEP 7.

1.5 Industrial Ethernet Security

Protection sans faille - Fonction d'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 à partir du réseau externe connecté au CP peut être protégée par la combinaison de diverses mesures de sécurité contre :

- l'espionnage de données (FTPS, HTTPS)
- la manipulation de données
- les intrusions

Il est possible d'exploiter des réseaux subordonnés sécurisés via des interfaces Ethernet/PROFINET additionnelles, réalisées au moyen de la CPU ou de CP complémentaires.

Fonctions de sécurité du CP pour la station S7-1500

L'utilisation du CP permet à la station S7-1500 de bénéficier des fonctions de sécurité 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 non IP selon IEEE 802.3 (Layer 2)
  - Limitation de la vitesse de transmission
  - Règles de pare-feu globales et personnalisées

  La fonction de sécurité du pare-feu peut s'étendre au fonctionnement d'un appareil, de plusieurs appareils ou de segments de réseau complets.
- Journalisation

  Des évènements peuvent être enregistrés, à des fins de surveillance, dans des fichiers journal que STEP 7 permet de lire ou d'envoyer automatiquement à un serveur Syslog.
- FTPS (mode explicite)

  Pour la transmission cryptée de fichiers
- NTP (secure)

  Pour la synchronisation d'horloge sécurisée
- SMTPS

  Pour la transmission sécurisée d'e-mails via le port 587
- SNMPv3

  Pour la transmission à l'abri des écoutes d'informations d'analyse de réseau

Veuillez prendre en compte les remarques au chapitre Recommandations de sécurité (Page 35).

1.6 Capacités fonctionnelles et caractéristiques de performance

1.6.1 Caractéristiques générales

Caractéristique	Signification / Valeurs
Nombre total de liaisons utilisables sans restrictions via Industrial Ethernet	118 La valeur s'applique au total des liaisons de type suivant : • liaisons S7 • liaisons pour services de communication ouverts • FTP (client FTP)

Remarque

Ressources de liaison de la CPU

Le nombre de ressources de liaison disponible varie selon le type de CPU. Le nombre de ressources de liaison détermine finalement le nombre de liaisons configurable. Des valeurs inférieures à celles indiquées pour le CP dans le présent chapitre sont donc possibles.

1.6.2 Caractéristiques CloudConnect

Nombre de connexions au Cloud

- **Nombre de sessions avec le brocker**

  1 session max.

Nombre der données du processus pour la connexion au Cloud

- **Variables dans la zone de données de la CPU S7**
  - 500 variables max.

Nombre de rubriques / groupes

- **Nombre de rubriques ou de groupes configurables**
  - 500 max.

1.6.3 Caractéristiques de la communication S7

La communication S7 propose la transmission de données via les protocoles transport ISO ou ISO-on-TCP.

Caractéristique	Signification / Valeurs
Nombre total de connexions S7 utilisables sans restrictions via Industrial Ethernet	118 max.
Interface de réseau local - longueur de bloc de données générée par le CP par unité de protocole (PDU = protocol data unit)	• Pour l'émission : 480 octets / PDU • Pour la réception : 480 octets / PDU
Nombre de connexions OP réservables *	4 max.
Nombre de connexions PG réservables *	4 max.
Nombre de connexions HTTP pour le web	4 max.

* La CPU réserve des ressources de connexion Tenez compte des valeurs indiquées également pour les connexions programmées.

Remarque

Valeurs maximales pour la station S7-1500

Des valeurs maximales s'appliquent à la station S7-1500 en fonction de la CPU utilisée. Tenez compte des indications dans la documentation correspondante.

1.6.4 Caractéristiques pour OUC et FETCH/WRITE

L'Open User Communication (OUC) donne accès à la communication via des connexions TCP, ISO-on-TCP, transport ISO et UDP.

Les caractéristiques suivantes sont significatives (OUC + FETCH/WRITE) :

Caractéristique	Signification / Valeurs
Nombre de connexions	Nombre de connexions configurées et programmées (transport ISO + ISO-on-TCP + TCP + UDP + FETCH/WRITE + e-mail) : • Au total 118 max. Dont max. : – Connexions TCP : 0...118 – Connexions ISO-on-TCP : 0...118 – Connexions transport ISO : 0...118 – Nombre total de connexions UDP (spécifiées et libres) : 0...118 – Connexion e-mail : 0...1 – Connexions pour FETCH/WRITE : 0...16
Longueur max. de données pour blocs de programme	Les blocs de programme permettent de transférer les longueurs de données utiles suivantes : • ISO-on-TCP, TCP, transport ISO : 1 à 64 Ko • UDP : 1 octet à 2 ko • E-mail – En-tête de tâche + données utiles : 1 à 256 octets – Pièce jointe au mail : jusqu'à 64 Ko
Interface réseau local - longueur d'enregistrement max. générée par le CP par unité de protocole (TPDU = transport protocol data unit)	• pour l'émission Transport ISO, ISO-on-TCP, TCP : 1452 octets / TPDU • pour la réception – Transport ISO : 512 octets / TPDU – ISO-on-TCP : 1452 octets / TPDU – TCP : 1452 octets / TPDU

Remarque

Ressources de connexion de la CPU

Le nombre de ressources de connexion disponibles varie selon le type de CPU. Le nombre de ressources de connexion détermine finalement le nombre de connexions configurables. Des valeurs inférieures à celles indiquées pour le CP dans le présent chapitre sont donc possibles.

Vous trouverez des informations détaillées sur les ressources de connexion dans la description fonctionnelle "Communication" ; voir chapitre Guide de la documentation (Page 115)

Restrictions pour UDP

- Restrictions UDP broadcast / multicast

  Pour éviter de surcharger le CP par de nombreux échanges de télégrammes broadcast/multicast, la réception de diffusions braodcast/multicast UDP est limitée sur le CP.

- Mise en tampon de télégrammes UDP

  Longueur du tampon de télégrammes : au moins 7360 octets

  En cas de débordement du tampon, les nouveaux télégrammes arrivants qui n'ont pas été relevés par le programme utilisateur, sont rejetés.

1.6.5 Caractéristiques pour le mode FTP / FTPS

Liaisons TCP pour FTP

Les actions FTP sont transmises par le CP via des liaisons TCP. Les caractéristiques suivantes s'appliquent :

- mode client FTP

  Vous pouvez exploiter au maximum 32 sessions FTP.

  Jusqu'à 2 liaisons TCP sont occupées par session FTP activée (1 liaison de contrôle et 1 liaison de données).

- Mode serveur FTP

  Vous pouvez exploiter au plus 16 sessions FTP simultanément.

  Jusqu'à 2 liaisons TCP sont occupées par session FTP activée (1 liaison de contrôle et 1 liaison de données).

Bloc de programme FTP_CMD pour mode client FTP

Utilisez pour la communication le bloc de programme FTP_CMD.

Le temps d'exécution des blocs dépend en mode FTP des temps de réponse du partenaire et de la longueur des données utiles. Il n'est donc pas possible de fournir ici une indication généralement valable.

1.6.6 Caractéristiques de sécurité des données - Règles de pare-feu

Règles de pare-feu (mode de pare-feu avancé)

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 14.90.120.0/16)
- Au maximum 128 règles avec limitation de la vitesse de transmission ("Limitation de largeur de bande")

1.7 Configuration logicielle requise

Logiciel de configuration et de fonctions en ligne

La configuration et l'utilisation du CP nécessitent l'emploi de l'outil d'ingénierie suivant :

- STEP 7 Professional V15.1

  + Update 3

  + Support Package 0284 (CP 1545-1 V1.0)

1.8 Configuration matérielle requise (CPU)

CPU compatibles

Le CP est utilisable avec les CPU suivantes :

- S7-1500

  Toutes les CPU configurables sous STEP 7 à partir de la version de firmware V2.0 des séries suivantes :

  – CPU standard (CPU 15xx)

  – CPU compactes (CPU 15xxC)

Modules de communication compatibles

Le CP 1545-1 peut être utilisé dans le châssis à côté d'un CP 1543-1 ou CM 1542-1.

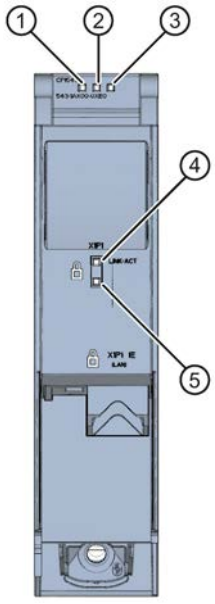
Le CP 1545-1 ne peut pas être utilisé comme rechange d'un CP 1543-1.

LED, connecteurs

2

2.1 LED

LED



① LED RUN
② LED ERROR
③ LED MAINT
④ LED LINK/ACT
⑤ LED de réserve

Figure 2-1 LED du CP 1545-1 (sans volet frontal)

Signification des symboles de LED

Signification des symboles de LED dans les tableaux suivants :

LED verte	LED rouge	LED jaune	Signification
☐	☐	☐	LED éteinte
■	■	■	LED allumée (lumière fixe)
☼	☼	☼	LED clignotante

Signification des LED témoins

Le CP dispose, pour signaler les états de fonctionnement et de diagnostic courants, des 3 LED suivantes. Le tableau suivant indique la signification des différentes combinaisons d'états des LED.

Tableau 2- 1 Signification des LED "RUN", "ERROR", "MAINT"

RUN (vert)	ERROR (rouge)	MAINT (jaune)	Signification
☐	☐	☐	Tension d'alimentation du CP trop faible ou manquante.
■	■	■	Test des LED au démarrage
■	■	☐	Démarrage du CP
■	☐	☐	Le CP est à l'état de fonctionnement MARCHE. Aucun défaut.
■	☼	☐	Présence d'un événement de diagnostic.
■	☐	■	Maintenance requise :
■	☐	☼	Chargement du programme utilisateur
☼	☐	☐	• Configuration de CP manquante ou incomplète. • Chargement du firmware en cours
☼	☼	☼	Défaut du module (clignotement synchrone des LED)

Signification des LED témoins de l'interface Ethernet X1 P1

La LED LINK/ACT (vert/jaune) affiche l'état et l'activité du port de l'interface Ethernet :

Tableau 2- 2 Signification de la LED "LINK/ACT"

LINK/ACT		Signification
☐ vert éteint	☐ jaune éteint	Pas de connexion à Ethernet Pas de connexion Ethernet entre CP et partenaire de communication Pas d'émission / de réception de données via Ethernet
☼ vert clignotant	☐ jaune éteint	"Test de clignotement des LED", voir Aide STEP 7 ("Diagnostic du matériel")
■ vert allumé	☐ jaune éteint	Connexion à Ethernet Connexion Ethernet établie entre CP et partenaire de communication
■ vert allumé	■ jaune vacillant	Émission / réception de données via Ethernet

2.2 Interface Gigabit

Interface Ethernet selon spécification Gigabit avec accès de sécurité

Le CP possède une interface Ethernet selon le standard Gigabit IEEE 802.3. Cette interface Ethernet prend en charge l'autocroisement, l'autonégociation et l'autodétection.

L'interface Ethernet permet d'établir des connexions sécurisées par un pare-feu à des réseaux externes. La fonction de protection proposée par le CP assure :

- la protection de la station S7-1500 dans laquelle fonctionne le CP ;
- la protection des réseaux d'entreprise subordonnés, connectés à d'autres interfaces de la station S7-1500.

Le brochage de l'embase femelle Sub-RJ45 est décrit au chapitre Brochage de l'interface Ethernet (Page 106).

Montage, connexion, mise en service, utilisation 3

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.

3.1 Notes importantes concernant la mise en œuvre de l'appareil

3.1.1 Consignes pour une mise en œuvre en atmosphère explosible

⚠ ATTENTION
DANGER D'EXPLOSION N'ouvrez pas l'appareil lorsqu'il est sous tension.

⚠ ATTENTION
DANGER D'EXPLOSION L'échange de composants remet en cause la conformité à Class I, Division 2 ou Zone 2.

⚠ 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
DANGER D'EXPLOSION Il est interdit d'effectuer des branchements ou débranchements de câbles sur l'appareil tant que ce dernier se trouve dans une atmosphère facilement inflammable ou combustible.

⚠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.

Remarque

Le montage mural est interdit dans les zones à atmosphère explosive.



⚠ATTENTION

Si un appareil est utilisé à une température ambiante supérieure à 50 °C à 60 °C, la température du boîtier de l'appareil peut dépasser 70 °C. Le lieu d'implantation de l'appareil doit par conséquent être situé dans une zone à accès restreint, réservé au personnel de maintenance ou à des utilisateurs informés de la raison de la restriction d'accès et des mesures de sécurités requises lorsque la température ambiante dépasse 60 °C.

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

⚠ATTENTION

Rail DIN symétrique

Dans le domaine d'application d'ATEX et IECex, seul le rail DIN symétrique Siemens 6ES5 710-8MA11 est autorisé pour le montage des modules.

⚠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).

⚠ATTENTION

Connexion LAN (Local Area Network)

Un réseau local ou un segment de réseau local et tous les appareils qui y sont connectés doivent être entièrement intégrés dans une distribution d'énergie basse tension d'un même bâtiment. Le réseau local est conçu pour "Environment A" selon IEEE802.3 ou "Environment 0" selon IEC TR 62102.

N'établissez jamais une connexion électrique directe à un réseau téléphonique (Telephone Network Voltage) ou à un WAN (Wide Area Network).

3.1.3 Consignes pour une mise en œuvre en atmosphère explosible selon UL HazLoc et FM

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

L'utilisation d'autres composants remet en cause la conformité de l'appareil.

⚠ATTENTION

L'échange de composants remet en cause la conformité à Division 2.

⚠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.

⚠ATTENTION

Ne débranchez pas les câbles sous tension de l'appareil si l'alimentation est en circuit ou si l'appareil se trouve dans un environnement facilement inflammable ou combustible.

⚠ATTENTION

Danger d'explosion

Ne débranchez pas les câbles sous tension de l'appareil si l'appareil se trouve dans un environnement facilement inflammable ou combustible.

⚠ATTENTION

Le montage mural hors d'une armoire électrique ou d'un boîtier n'est pas conforme aux spécifications de l'homologation FM.

⚠ATTENTION

Le montage mural n'est autorisé que si les spécifications du boîtier, les instructions de montage, les distances et les règles de sectionnement de l'armoire électrique ou du boîtier sont respectées. L'ouverture du capot de l'armoire électrique ou du boîtier doit nécessiter l'emploi d'un outil. Les câbles doivent être équipés d'une décharge de traction appropriée.

⚠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.

⚠ATTENTION

Si l'appareil est installé dans une armoire électrique, la température interne de l'armoire correspond à la température ambiante de l'appareil.

3.2 Montage

⚠ATTENTION

Matériels ouverts

Ces appareils sont des "matériels ouverts" (open equipment) selon la norme CEI 61010-2-201 ou UL 61010-2-201 / CSA C22.2 No. 61010-2-201. Afin de satisfaire aux dispositions en matière de sécurité en ce qui concerne la résistance mécanique, la tenue à la propagation des flammes, la stabilité et la protection contre les contacts directs, il faudra prévoir l'un des types de montage suivants :

- Montage dans une armoire électrique appropriée
- Montage dans un coffret approprié,
- Montage dans un local fermé, aménagé en conséquence

Montage

IMPORTANT

Montage et démontage de l'appareil uniquement hors tension !

Mettez la station hors tension avant de monter ou de démonter le module. Le montage ou démontage sous tension risque d'endommager les modules et de causer la perte de données.

IMPORTANT

Position de montage - Impact sur la plage de température

Tenez compte du fait que la plage de température admissible varie en fonction de la position de montage :

- Si le châssis (rail DIN symétrique) est monté à l'horizontale, les modules sont fixés en position verticale.
- Si le châssis (rail DIN symétrique) est monté à la verticale, les modules sont fixés en position horizontale.

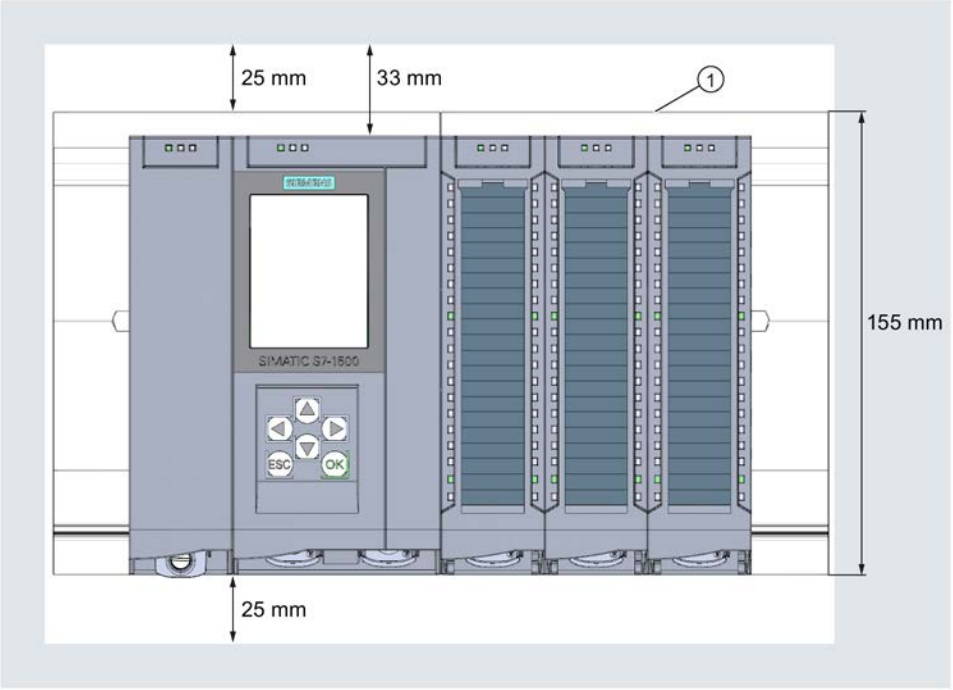
Les plages de température admissibles sont indiquées au chapitre Caractéristiques techniques (Page 105).

Espacement minimal

Montez le Module de sorte à ne pas obstruer les fentes d'aération en haut et en bas du module afin de permettre une bonne ventilation et d'empêcher une surchauffe.

Lors du montage horizontal du châssis, respectez les espacements minimaux suivant pour assurer la circulation de l'air :

- Au-dessus du module : au moins 33 mm
- Au-dessous du module : au moins 25 mm



Montage du châssis	Position de montage des modules
Montage horizontal du châssis	
Montage vertical du châssis	

ATTENTION

Lisez le manuel système "Automate programmable S7-1500"

Avant de procéder au montage, à la connexion et à la mise en service, lisez les sections correspondantes du manuel système "Automate programmable S7-1500", voir chapitre Guide de la documentation (Page 115).

Marche à suivre

Effectuez le montage et la connexion comme indiqué dans les descriptions relatives au montage de modules périphériques du manuel système "Automate programmable S7 1500", voir Guide de la documentation (Page 115).

3.3 Raccordement

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.

Connexion

ATTENTION

Lisez le manuel système "Automate programmable S7-1500"

Avant de procéder au montage, à la connexion et à la mise en service, lisez les sections correspondantes du manuel système "Automate programmable S7-1500", voir chapitre Guide de la documentation (Page 115).

Alimentation coupée

Veuillez vous assurer que l'alimentation est bien coupée durant le raccordement des appareils.

Marche à suivre

1. Connectez le CP au réseau Industrial Ethernet au moyen du connecteur femelle RJ-45 (sous le CP).

   Pour le brochage de l'interface Ethernet voir chapitre Brochage de l'interface Ethernet (Page 106).

2. Mettez la station S7 sous tension.
3. Refermez les volets des modules.

Les volets en face avant doivent rester fermés durant le fonctionnement.

3.4 Mise en service - Chargement des données de configuration

Condition : Configuration complète

La mise en service complète du CP présuppose que vous disposiez de toutes les données de projet STEP 7 de la station.

Charger

La mise en service se poursuit par le chargement des données de projet STEP 7.

Lors du chargement des données de configuration sur la CPU, le CP reçoit les données de configuration adéquates.

Les données de configuration peuvent être chargées sur la CPU via une carte mémoire ou une interface Ethernet/PROFINET de la station S7-1500. Pour charger la station via Ethernet, 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 de l'aide en ligne de STEP 7 :

- "Compilation et chargement des données de projet"
- "Utilisation des fonctions en ligne et des fonctions de diagnostic"

Établissement d'une connexion

Si vous utilisez le CP pour la communication avec le cloud et que toutes les connexions ont été configurées, le CP établit automatiquement la connexion au cloud.

3.5 État de fonctionnement de la CPU : Effet sur le CP

Basculement de la CPU : RUN → STOP

Vous avez la possibilité de basculer entre le mode de fonctionnement MARCHE et ARRÊT de la CPU à l'aide de STEP 7.

Remarque
LED RUN/STOP du CP

La LED RUN/STOP verte du CP reste allumée même si la CPU est à l'état ARRET.

À l'état ARRET de la CPU, le CP reste à l'état RUN. Le CP se comporte comme suit :

- les connexions établies (connexions transport ISO, ISO-on-TCP, TCP, UDP)
  - restent établies s'il s'agit de connexions programmées.
  - sont coupées s'il s'agit de connexions configurées.
- Les fonctions suivantes restent activées :
  - Configuration et diagnostic du CP

    Les connexions système pour la configuration, le diagnostic et le routage de canal PG restent établies.
  - Diagnostic Web
  - la fonction de routage S7
  - la synchronisation d'horloge

Configuration

4

4.1 STEP 7 Professional

Configuration sous STEP 7

La configuration du CP s'effectue sous STEP 7 Professional.

La version de STEP 7 requise est indiquée au chapitre Configuration logicielle requise (Page 20).

4.2 Recommandations de sécurité

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

Généralités

- Assurez-vous régulièrement que l'appareil est conforme aux présentes recommandations et aux éventuelles stratégies de sécurité internes.
- Procédez à une évaluation globale de la sécurité 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 ici des informations sur la sécurité de la communication industrielle :
    Lien : (https://new.siemens.com/global/en/products/automation/industrial-communication/industrial-ethernet/network-security.html)
  - 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 :
  Lien : (https://support.industry.siemens.com/cs/ww/fr/ps/25625/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, activez les fonctions de sécurité des données ou intercalez des systèmes de protection adéquats, un SCALANCE S avec pare-feu p. ex.

Fonctions de sécurité du produit

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

- Niveaux de protection

  Configurez l'accès à la CPU sous "Protection et sécurité".

- Fonction de sécurité de la communication
  - Activez les fonctions de sécurité 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. Exploitez la possibilité de "limitation de largeur de bande" offerte par le pare-feu pour restreindre les attaques par flooding ou déni de service.

    La fonctionnalité FETCH/WRITE offre la possibilité d'accéder à n'importe quelles données de vos API. N'utilisez donc pas la fonctionnalité FETCH/WRITE lorsque vous êtes connecté à des réseaux publics.
  - Utilisez les variantes de protocole sécurisées HTTPS, FTPS, NTP (secure) et SNMPv3.
  - Utilisez les blocs de programme pour la communication sécurisée OUC (Secure OUC).
  - Laissez désactivé l'accès au serveur Web de la CPU (configuration de la CPU).
- 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 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.
- Désactivez DHCP sur les interfaces vers des réseaux publics et Internet pour vous protéger contre l'usurpation d'adresse IP.

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.
- **Etat 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.
  - Ouvert lors de l'appel du bloc

    Le port n'est ouvert que si un bloc de programme adéquat est appelé.
- **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
DCP	93 (UDP)	Ouvert	Ouvert	non
Connexions S7 et connexions en ligne	102 (TCP)	Ouvert	Ouvert *	Non
Diagnostic de sécurité en ligne	8448 (TCP)	Fermé	Ouvert après configuration	non
HTTP	80 (TCP)	Fermé	Ouvert après configuration	non
HTTPS	443 (TCP)	Fermé	Ouvert après configuration	Oui
FTP	20 (TCP) 21 (TCP)	Fermé	Ouvert après configuration	Non
FTPS	989 (TCP) 990 (TCP)	Fermé	Ouvert après configuration	Oui
SNMP	161 (UDP)	Ouvert	Ouvert après configuration	Oui (sous SNMPv3)

***** Pour éviter l'ouverture du port 102 lors du diagnostic, voir chapitre Diagnostic de sécurité en ligne via le port 8448 (Page 69).

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 de :

- Port du broker
  - MQTT non sécurisé : 1883 (TCP)
  - MQTT via TLS : 8883 (TCP)

  Le numéro de port est paramétrable dans la configuration.
- DHCP / 67, 68 (UDP)
- DNS / 53 (UDP)
- NTP / 123 (UDP)
- SMTP / 25 (TCP) - ouvert dans le CP lors de l'appel du bloc (uniquement trafic sortant)
- SMTPS / 587 (TCP) - ouvert dans le CP lors de l'appel du bloc (uniquement trafic sortant)
- Syslog / 514 (UDP)

4.3 Restriction des services de communication sur la CPU

Services de communication sans connexions

La CPU peut être serveur d'une série de services de communication sans que des connexions aient été configurées pour la CPU. D'autres abonnés de communication peuvent accéder aux données de la CPU. La CPU locale n'a donc pas, en tant que serveur, la possibilité de contrôler les communications avec les clients.

L'autorisation de ces services de communication se configure avec le paramètre "mécanismes de connexion" du groupe de paramètres "Protection & Sécurité" de la CPU.

"Autoriser accès via communication PUT/GET par le partenaire à distance"

- Option activée

  L'accès côté client aux données de la CPU est autorisé.

- Option désactivée

  L'accès en lecture et en écriture aux données de la CPU n'est possible que pour les connexions de communication qui présupposent une configuration ou programmation aussi bien de la CPU locale que du partenaire de communication.

  Les connexions pour lesquelles la CPU locale est uniquement serveur (pas de configuration/programmé de la communication avec le partenaire), ne sont pas possibles.

  Les services de communication du CP se rapportent à une CPU ≥ V2.

  Si l'option est désactivée, les accès suivants ne sont pas possibles :

  – accès PUT/GET via le CP

  – accès FETCH/WRITE via le CP

  Si l'option est désactivée, l'accès suivant est possible :

  – accès PUT/GET FTP via le CP

4.4 Configuration IP

4.4.1 Particularités de la configuration IP

Liaisons S7 et OUC configurées non utilisables en cas d'adresse IP fournie par DHCP

Remarque

Si vous obtenez l'adresse IP par DHCP, les liaisons S7 et OUC éventuellement configurées ne seront pas opérationnelles. Motif : l'adresse IP configurée est remplacée, lors du fonctionnement, par l'adresse IP fournie par DHCP.

4.4.2 Redémarrage après détection d'une adresse IP double sur le réseau

Afin de vous éviter une difficile localisation d'erreurs sur le réseau, le CP détecte au démarrage les adresses doubles sur le réseau.

Comportement au démarrage du CP

Si, au démarrage, le CP détecte un adresse double, il passe à MARCHE mais n'est pas accessible via l'interface Ethernet. La LED ERROR clignote.

4.4.3 Routage IP

Routage IP via le bus interne

Le CP prend en charge le routage IP statique (IPv4) vers d'autres CM/CP :

- CP 1545-1
- CM 1542-1 V2.0
- CP 1543-1 V2.0

Vous pouvez utiliser le routage IP par exemple pour accéder au serveur Web de modules subordonnées.

Le débit binaire du routage IP est limité à 1 Mbit/s. Tenez compte à ce propos du nombre de modules participants et du trafic prévu via le bus interne.

Configuration

Vous pouvez activer le routage IP dans STEP 7 avec les paramètres suivants :
"Interface Ethernet > Adresses Ethernet > Routage IP entre modules de communication"

Veuillez noter :
Si vous utilisez plusieurs CP sur une station et voulez vous servir du routage IP, vous ne pouvez configurer un routeur que pour un seul CP de la station.

De plus, des règles de pare-feu IP, adaptables en mode de pare-feu avancé dans les paramètres de sécurité globaux, sont créées à l'activation de la fonction de sécurité des données.

4.4.4 Connexions programmées : Restriction des règles de pare-feu

Restrictions pour les connexions programmées et la configuration des fonctions de sécurité

Il est d'une manière générale possible de programmer des connexions de communication via le bloc de programme TCON et de configurer en même temps un pare-feu.

Remarque

Adresses IP des partenaires pas dans les règles de pare-feu

Lors de la configuration de connexions spécifiées (terminaisons actives) sous STEP 7, les adresses IP des partenaires ne sont pas automatiquement reprises dans la configuration du pare-feu.

4.5 Synchronisation d'horloge

Méthode

Le CP supporte la méthode de synchronisation d'horloge ci-après :

- Méthode NTP (NTP : Network Time Protocol)

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. Vous bénéficiez ainsi d'une différence aussi faible que possible entre l'heure interne et l'heure absolue.

Remarque

Particularité de la synchronisation d'horloge via NTP

Si l'option "Accepter la date/heure de serveurs NTP non synchronisés" n'est pas activée, le comportement est le suivant :

Si le CP reçoit un télégramme d'heure d'un serveur NTP de strate 16 non synchronisé, l'heure n'est pas synchronisée. Dans ce cas, le diagnostic n'affiche pas les serveurs NTP comme "NTP maître" mais simplement comme "accessibles".

Sécurité des données

Dans la configuration NTP avancée, vous pouvez créer et gérer des serveurs NTP additionnels.

Remarque

S'assurer d'une date/heure valide

Si vous utilisez les fonctions de sécurité des données, la validité de l'heure est d'une grande importance. Si l'heure n'est pas fournie par la station (CPU), nous vous recommandons de faire appel à la méthode NTP (secure).

Configuration

Pour plus de détails sur la configuration, veuillez vous référer au groupe de paramètres "Synchronisation d'horloge" de l'aide en ligne de STEP 7.

4.6 Configuration DNS

Serveur DNS

Un serveur DNS peut être nécessaire si le module même, un partenaire de communication ou un serveur FTP par exemple doivent être joignables via le nom d'hôte (FQDN). En cas de saisie de l'adresse d'un appareil sous forme de FQDN, vous devez configurer un serveur DNS. L'adresse IP de l'appareil est alors déterminée par le serveur DNS configuré.

Ne configurez pas plus de 3 serveurs DNS pour le CP. Le 4e serveur DNS n'est pas traité.

4.7 Configuration du serveur FTP

4.7.1 Configuration de la fonction serveur FTP

Configuration du CP

Configurez la fonction de serveur FTP du CP dans le groupe de paramètres suivant.

- Si les fonctions de sécurité sont désactivées : "Configuration du serveur FTP"
- Si les fonctions de sécurité sont activées : "Security > Configuration du serveur FTP"

Conditions requises dans la configuration de la CPU et programmation

Utilisez les paramètres suivants pour permettre l'accès via FTP :

- Dans la configuration de la CPU sous "Protection & sécurité > Mécanismes de connexion" :

  désactivez l'option "Accès via communication PUT/GET ...".

- Créez des blocs de données de type "Array-of-Byte" comme DB fichiers.

CP S7-1500 comme serveur FTP

La fonction décrite ici permet de transférer, à l'aide de commandes FTP, des données sous forme de fichiers (files) sur une station S7-1500 ou à partir d'une telle station. Vous pouvez utiliser pour ce faire les commandes FTP d'usage pour la lecture, l'écriture ou la gestion de fichiers.

Il est possible d'accéder aux données suivantes du S7-1500 :

- **Blocs de données de la CPU**

  Nom du répertoire :

  /cpu1 / DBx

  "DBx" est le nom du bloc de données correspondant, par exemple BD10.

- **Memory Card SIMATIC de la CPU**

  La fonction est prise en charge par les versions de firmware suivantes :

  – CPU : V2.0

  – CP 1543-1 : V2.0

  – CP 1545-1 : V1.0

  Nom du répertoire :

  /mmc_cpu1

  Il est possible d'accéder aux dossiers suivants de la Memory Card SIMATIC :

  – /DATALOGS

    Répertoire des fichiers journaux

  – /RECIPES

    Répertoire des fichiers de recettes

Remarque

Accès FTP à la Memory Card SIMATIC de la CPU : ARRÊT CPU possible

Veuillez noter que les cartes ont une capacité limitée. Lorsque l'espace mémoire de la Memory Card SIMATIC est épuisé suite à l'enregistrement d'un volume important de données, la CPU passe à l'état ARRÊT.

- Utilisez une carte avec une capacité de mémoire suffisante.
- Évitez d'enregistrer souvent des volumes importants de données via FTP sur la Memory Card SIMATIC.

Lecture/écriture via des DB de la CPU

Créez sur la CPU des DB appropriés pour le transfert FTP de données via des blocs de données. Ils sont appelés DB fichiers en raison de leur structure particulière.

Le CP utilisé comme serveur FTP vérifie, à la suite d'une instruction FTP, dans sa table d'allocation comment les blocs de données utilisés sur la CPU pour le transfert FTP doivent être reproduits sur des fichiers. L'affectation des blocs de données s'effectue dans la configuration STEP 7 du CP (configuration FTP).

Pour la structure du DB fichier voir chapitre Structure du bloc de données (DB fichier) pour le mode client FTP (Page 92).

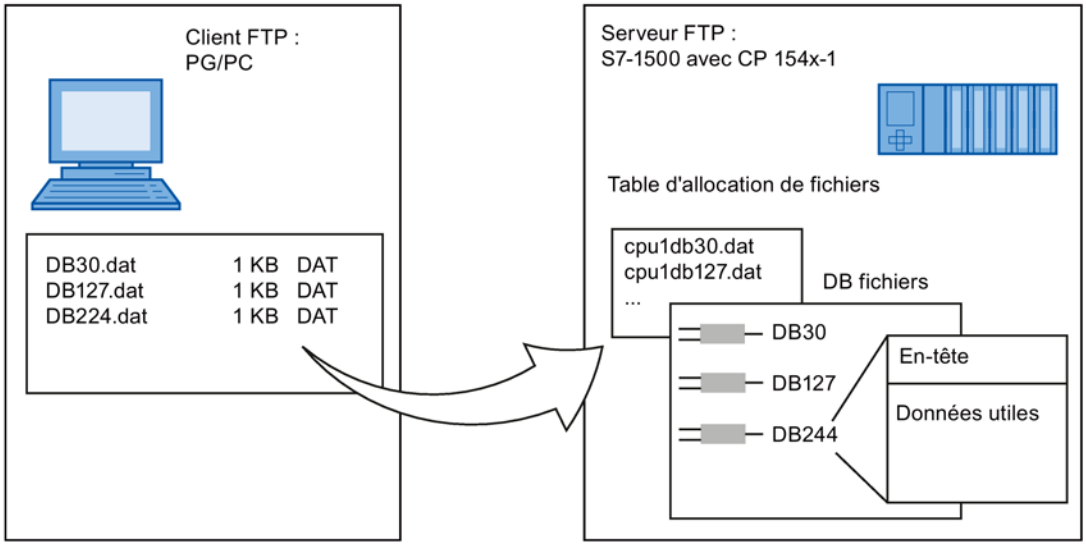


Figure 4-1 CPU S7 avec CP 154x-1 comme serveur FTP pour les données de CPU S7

4.7.2 Structure de la liste de configuration FTP

Affectation des DB sous STEP 7

Signification et syntaxe des cellules du tableau d'affectation des DB sous STEP 7 :

Titre de colonne	CPU	DB	Nom de fichier	Commentaire
Signification	Affectation de la CPU Sélectionnable dans une liste déroulante	N° du bloc de données (DB fichier) Sélectionnable dans une liste déroulante	Nom de fichier affecté au DB fichier Nom proposé automatiquement, entrée éditable.	Commentaire informel
Exemple	cpu1 [PLC_1]	20	cpu1_db20.dat	Valeurs de mesure Installation 1

Remarques sur la syntaxe

Syntaxe du nom de fichier d'un DB fichier :

- Le nom de fichier débute par "cpuX" (avec X=1 pour S7-1500).

  Remarque

  Respectez l'orthographe (écrire "cpu" en minuscules et pas d'espace en début de ligne). Sinon, les fichiers ne sont pas reconnus.

- Longueur : 64 caractères max. (y compris la mention "cpuX")

4.7.3 Accès via FTPS

Accès FTPS uniquement si les fonctions de sécurité sont activées

L'accès à la station S7-1500 en tant que serveur FTP via FTPS présuppose qu'un utilisateur possédant les droits requis ait été configuré dans le projet STEP 7. Il est par conséquent nécessaire que les fonctions de sécurité aient été activées sur le CP. Les paramètres de sécurité sont ainsi disponibles dans la gestion globale des utilisateurs.

4.8 SNMP

SNMP

Le CP prend en charge les versions suivantes de SNMP :

- **SNMPv1**

  Disponible si les fonctions de sécurité sont 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 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".

- **SNMPv3**

  Disponible uniquement en cas d'activation des fonctions de sécurité

Pour plus de détails, voir chapitre Diagnostic via SNMP (Page 99).

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.

4.9 CloudConnect

4.9.1 Configuration de l'accès au cloud

4.9.1.1 Notes à propos de la structure des données et de la configuration

Structures des données

Pour accéder aux données du processus pour la communication cloud, le CP accède à des variables de DB de la CPU. Les données référencées dans les variables de DB, sont configurées dans le CP via des points de données.

Les données sont structurées différemment selon le fournisseur de cloud pour la transmission au broker.

- Autre cloud (AWS / Azure / IBM Cloud)
  - Rubriques

    Une rubrique est le canal de transmission des valeurs d'un ou de plusieurs points de données.

    Vous pouvez créer plusieurs rubriques.

    Il n'est pas possible de configurer des groupes.
- Siemens MindSphere - MindConnect IoT Extension
  - Groupes

    Un groupe peut contenir un ou plusieurs points de données.

    Vous pouvez créer un ou plusieurs groupes.
  - Rubrique

    Tous les groupes sont affectés définitivement à la rubrique par défaut "s/us" de la MindConnect IoT Extension.

Noms de rubrique et de groupe

Configuration des noms de rubrique :

- Pour le fournisseur de cloud MindConnect IoT Extension, le nom de rubrique "s/us" est prédéfini.
- Pour tous les autres fournisseurs de cloud, les noms de rubrique sont configurables.

4.9.1.2 Règles de configuration

Règles de configuration

Observez les règles suivantes pour la configuration :

- Nom de rubrique

  Le nom de rubrique doit être unique au sein d'une application de cloud.

  Ceci s'applique à tous les Publishers et Subscribers associés.
- Nom du point de données

  Le nom du point de donnée doit être unique au sein d'une rubrique.

Remarque

Contrôle de cohérence de paramètres pour Publisher et Subscriber

Si le CP reçoit en cours de fonctionnement, en tant que Subscriber, des données d'un Publisher, le Subscriber vérifie, à chaque valeur reçue, les paramètres suivants livrés par le Publisher dans les données utiles.

- Nom de rubrique
- Nom du point de données
- Type de données

Si ces trois paramètres du Publisher sont identiques aux paramètres configurés dans le Subscriber et si le QualityCode des valeurs transmises est "GOOD", le Subscriber inscrit les données reçues dans le bloc de données de sa CPU.

Si un ou plusieurs de ces trois paramètres du Publisher ne sont pas identiques aux paramètres configurés dans le Subscriber, le Subscriber rejette les données.

Recommandations

Lors de la transmission de données dans un système à structure hiérarchique, il est généralement recommandé de nommer les composants en fonction de cette structure hiérarchique.

L'affectation et l'analyse ultérieures des données publiées est plus facile si les noms se réfèrent aux données du processus des stations.

Vous pouvez par exemple créer des niveaux hiérarchiques pour l'analyse ultérieure par les Subscribers en insérant des barres obliques (/).

- Exemples de noms de rubrique/groupe

  Vous souhaitez nommer un groupe ou une rubrique "Moteur5". Les données sont affectées à la station S7 "Station1".

  Il est utile dans cet exemple d'utiliser le nom de rubrique/groupe "Station1/Moteur5".

- Exemple pour un nom nom de point de données

  "Installation1/Parie de l'installation1/Unité1/DB1_Signal1"

Points de données et DB

Au sein d'une application de cloud, des Publishers peuvent publier des données destinées à plusieurs Subscribers. Des Subscribers peuvent s'abonner aux données de plusieurs Publishers

Pour améliorer la clarté des données tout en réduisant la possibilité de noms identiques, il est recommandé de procéder comme suit lors de la configuration.

- Bloc de données

  Créez dans une CPU des DB distincts uniquement pour la fonction Publisher et uniquement pour la fonction Subscriber.

- Nom de point de données / numéro de DB

  Utilisez le numéro du bloc de données (DB), auquel le point de données accède, comme élément du nom du point de données.

- Publisher
  - Créez dans la CPU affectée un DB distinct pour chaque Subscriber possible.
  - Si un Subscriber s'abonne aux données de plusieurs Publishers, configurez sur les CPU des divers Publishers un autre numéro de DB pour chaque DB destiné à ce Subscriber.

    Vous évitez ainsi que les variables de Publishers différents possèdent un nom de point de données identique lorsque les noms de point de données utilisent le numéro de DB comme élément constituant du nom.

- Subscriber

  Créez dans la CPU affectée un DB distinct pour chaque Publisher.

4.9.1.3 Présentation de la configuration

Configuration de l'accès au cloud - Vue d'ensemble

1. Créez les blocs de données et variables de DB requis pour l'accès de l'application du cloud à la mémoire image du processus dans la CPU locale.

   Les points de données des rubriques / groupes (voir ci-dessous) accèdent à ces variables de DB de la CPU, voir chapitre Zones d'opérandes et variables (Page 54).

2. Créez, dans les paramètres de sécurité généraux, un utilisateur avec le rôle "NET Administrator".
3. Activez pour le CP, dans le groupe de paramètres "Sécurité des données", l'option "Activer les fonctions de sécurité des données".
4. Activez pour la communication avec le cloud l'option "Activer CloudConnect".

   Sélectionnez le fournisseur de cloud :

   - Siemens MindSphere - MindConnect IoT Extension
   - Autre cloud

   Pour les fournisseurs de cloud supportés, voir chapitre Communication en nuage (Page 12).

   Configurez les autres paramètres, voir Groupe de paramètres "CloudConnect" (Page 50).

5. Si vous configurez une communication cryptée (MQTT via TLS) avec le broker, vous avez besoin au moins du certificat correspondant et éventuellement d'une clé du fournisseur de cloud.

   Procurez-vous ceux-ci auprès de votre fournisseur de cloud ou de son site Internet, et importez les fichiers dans le projet STEP 7 et sur le CP. Pour la marche à suivre, voir chapitre Certificats (Page 70).

6. Ouvrez ensuite le navigateur de projet :

   Station > Modules locaux > CP 1545-1 > Connexion au cloud

   Voir à ce propos chapitre Configuration des rubriques et groupes (Page 55).

   Créez un groupe et/ou une rubrique.

7. Ouvrez le groupe ou la rubrique, ajoutez des points de données et configurez-les.
8. Ouvrez la boîte de dialogue des propriétés de la rubrique / du groupe avec l'option de menu contextuel "Propriétés".
   - Configurez le nom et facultativement "Auteur" et "Commentaire" de la rubrique / du groupe.
   - Configurez pour les rubriques ("Autre cloud") les paramètres de QoS. Voir à ce propos chapitre Quality of Service (QoS) (Page 67).

4.9.1.4 Groupe de paramètres "CloudConnect"

Général

- **Activer CloudConnect**

  Active la communication avec un système de cloud via l'interface Ethernet du CP.

- **Fournisseur de cloud**

  Sélectionnez le fournisseur de cloud voulu :

  - Siemens MindSphere - MindConnect IoT Extension
  - Autre Cloud (Profil pour un autre système de Cloud)

- **Nom du module**

  Validité : Uniquement MindConnect IoT Extension

  Pour la signification voir Onboarding dans MindConnect IoT Extension (Page 53).

- **Cycle d'interrogation de la variable**

  Cycle (ms) d'interrogation des variables de DB de la CPU.

  Plage de valeurs : 100..4294967295 ms

  Remarque
  Nombre de données transmises

  La valeur du paramètre influence directement le volume de données transmis. Tenez compte à ce propos de la note du chapitre Déclenchement (Page 57).

  Perte de données

  Si vous configurez un cycle de balayage des variables très court et en même temps un grand nombre de points de données, il se peut qu'avec certains brokers les données publiées ne soient pas toutes lues dans le tampon d'entrée du serveur de cloud.

  Tenez également compte à ce propos de la fonction de la mémoire de télégrammes, voir chapitre Coupure de la connexion et mise en tampon des données (Page 65).

- **Rubriques horodatées**

  Lorsque l'option est activée, chaque valeur est horodatée à l'instant de sa publication.

Configuration du broker

- **MQTT / MQTT via TLS**

  Sélectionnez sinon l'une des variantes de protocole suivante :

  – MQTT (transmission non cryptée)

  – MQTT via TLS (transmission cryptée)

- **Version TLS minimale**

  Définit la version de TLS utilisée par le CP et le partenaire.

- **Certificat du broker**

  Le paramètres est uniquement activé si vous avez activé la transmission cryptée "MQTT via TLS". Vous avez dans ce cas besoin d'un certificat de votre fournisseur de cloud.

  Par défaut : "Automatique". Si "Automatique" est sélectionné, le certificat affecté est choisi parmi les certificats dignes de confiance.

  Procédez comme suit pour l'affectation manuelle du certificat.

  – Importez le certificat du partenaire :

    Paramètres de sécurité généraux > Gestionnaire de certificats > Certificats dignes de confiance > bouton droit de la souris

  – Affectez le certificat au CP :

    Sélectionnez le certificat dans la liste "Certificats dignes de confiance" sélectionner > bouton droit de la souris

    Le certificat figure sur le CP dans le groupe de paramètres "Sécurité des données > Gestionnaire de certificats" dans la liste "Certificats des appareils partenaires".

  – Sélectionnez à présent le certificat importé dans la zone de liste déroulante "Certificat du broker".

- **Adresse du broker**

  Adresse de serveur du broker (adresse IPv4 ou nom d'hôte)

- **Port du broker**

  Numéro de port du serveur du broker.

  – En cas de transmission non cryptée (MQTT), le port est par défaut 1883.

  – En cas de transmission cryptée (MQTT via TLS), le port est par défaut 8883.

- **ID de client**

  Entrez l'ID de client que votre opérateur de services vous a attribué ou que vous avez défini vous-même.

  255 caractères max. de la plage ASCII (hex) 0x20 .. 0x7F

- **Effacer session**

  Si cette option est activée, les informations de session sont supprimées lors de l'établissement de la connexion.

  Si cette option est désactivée, les informations de session sont conservées lors de l'établissement de la connexion.

  Remarque

  Recommandation : Activer "Effacer session"

  Il est recommandé d'activer ce paramètre.

  Si la valeur configurée pour QoS est > 0 et "Effacer session" est désactivé, il se peut que des situations confuses surviennent en cas de coupures de connexion en ce qui concerne les acquittements en suspens.

Surveillance du broker

- **Intervalle de keep alive**

  Temps de surveillance de la connexion au broker

  Si, après l'émission de données, il n'y a plus de donnée à transmettre ou si le CP ne reçoit pas de paquets du broker pendant le temps de surveillance, le CP envoie un paquet keep-alive (PINGREQ) au broker que celui-ci doit acquitter (PINGRESP).

  Tenez compte de l'influence du paramètre sur le comportement en cas de coupures de connexion, voir chapitre Coupure de la connexion et mise en tampon des données (Page 65).

  Après la mise en service, les modifications de la valeur ne sont appliquées qu'après une nouvelle commande "Charger dans l'appareil".

Authentification du broker

- **Activer l'authentification**

  Si cette option est activée, la connexion au broker est établie avec authentification. Utilisez dans la mesure du possible TLS pour la transmission du nom d'utilisateur et du mot de passe.

  Si cette option est désactivée, la connexion est établie anonymement.

- **Nom d'utilisateur**

  Saisissez le nom d'utilisateur qui vous a été fourni par votre opérateur de services ou que vous avez défini vous-même.

- **Mot de passe**

  Saisissez le mot de passe qui vous a été fourni par votre opérateur de services ou que vous avez défini vous-même.

4.9.1.5 Onboarding dans MindConnect IoT Extension

Paramètres de Device

Lors de la connexion au Siemens MindSphere - MindConnect IoT Extension deux paramètres sont utilisés, après l'établissement de la connexion entre le CP et MindConnect IoT Extension, pour l'identification de votre appareil au moment du processus de Onboarding.

- **Nom du module**

  Attribuez le nom dans le groupe de paramètres "Sécurité des données > CloudConnect > Général" du CP.

  Le CP est enregistré sous ce nom lors du processus de Onboarding.

  Le nom du module s'affiche dans MindConnect IoT Extension à l'emplacement suivant : Device > Device profile > "NAME"

- **Type de module**

  Ce paramètre n'est pas configurable et est défini par la chaîne de caractères suivante :

  – c8y_MQTTDevice

  Le paramètre est nécessaire dans MindConnect IoT Extension pour définir le type d'appareil.

  Le type de module s'affiche dans MindConnect IoT Extension à l'emplacement suivant : Device > Device profile > "Type"

Pour plus d'informations sur la configuration de IoT Extension voir sur Internet sous :
Lien : (https://support.industry.siemens.com/cs/ww/fr/ps/25625)

4.9.1.6 Zones d'opérandes et variables

Zones d'opérandes

Des variables des zones d'opérandes suivantes de la CPU peuvent être utilisées pour le transfert de données de la station S7 :

- Bloc de données (DB global)

  Tenez compte de ce qui suit lors de la configuration dans le dialogue des propriétés du DB :

  – Activez l'attribut "DB accessible à partir d'OPC UA".

Configuration des variables de DB

Tenez compte de ce qui suit lors de la configuration des variables de DB :

- Activez l'option "Joignable à partir de HMI/OPC UA".
- Activez l'option "Éditable à partir de HMI/OPC UA".

  Nécessaire pour l'accès en écriture

Pour les types de données utilisables pour la connexion au nuage voir chapitre Types de données (Page 57).

4.9.2 Configuration de rubriques, de groupes et de points de données

4.9.2.1 Configuration des rubriques et groupes

Configuration sous différents fournisseurs de cloud

Lors du choix du fournisseur de cloud vous optez pour la configuration de rubriques ou de groupes à des fins de transmission de données.

- MindConnect IoT Extension

  Vous pouvez créer plusieurs groupes.

  Un groupe peut contenir plusieurs points de données.

  Un groupe correspond dans IoT Extension à la caractéristique de structure "Series". Tous les groupes sont affectés définitivement à la rubrique par défaut "s/us".

  Sélectionnez la station dans le navigateur de projet et développez-la :

  > Station > Modules locaux > CP 1545-1 > Connexion au cloud > Groupes

  Cliquez sur "Ajouter un groupe" Un groupe de Publishers est créé.

- Autre cloud

  Vous pouvez créer plusieurs rubriques.

  Une rubrique peut contenir plusieurs points de données.

  Sélectionnez la station dans le navigateur de projet et développez-la :

  > Station > Modules locaux > CP 1545-1 > Connexion au cloud > Rubriques publiées / Rubriques abonnées

  Vérifiez avec le fournisseur de cloud quelle fonction (Publisher / Subscriber) est prise en charge, voir chapitre Communication en nuage (Page 12).

  Cliquez sur "Ajouter rubrique". Une rubrique est créée.

Pour la suite de la configuration des groupes et rubriques, voir chapitre Configuration des points de données (Page 55).

4.9.2.2 Configuration des points de données

Ajout de points de données à une rubrique / un groupe

Ouvrez un groupe / une rubrique par un double clic.

Cliquez dans les rubriques / dans le groupe sur le champ "Variable d'API" de la première ligne libre du tableau.

Dans le dialogue de sélection d'objets, choisissez la variable voulue d'un DB de la CPU. Pour les variable de DB voir Zones d'opérandes et variables (Page 54).

La variable de DB est reprise dans le tableau comme point de données, les propriétés et paramètres étant affichés au-dessous.

Le tableau récapitule tous les points de données configurés.

Configuration de points de données

- **Nom**

  Nom configuré du point de données.

- **Variable d'API**

  Nom configuré de la variable de DB

- **Type de données**

  Type de données configuré du point de données

  Pour les types de données supportés voir Types de données (Page 57).

- **Attribut**

  ⇒ Validité : MindConnect IoT Extension

  L'attribut et repris comme <ADDITIONAL_ATTRIBUTE> dans les données utiles, voir chapitre Format des données utiles (Page 61).

  Lors de la connexion à IoT Extension, l'attribut sert d'identifiant des unités physique des points de données respectifs. Les unités par défaut sont :

  – C = Température en degrés Celsius
  – P = Pression en bars
  – mm = Longueur en millimètres
  – km/h = Vitesse en km/h
  – m/s2 = Accélération en m/s^2
  – % = Taille en pour cent
  – %RH = Humidité relative de l'air en pour cent
  – A = Intensité en ampères
  – V = Tension en volts
  – W = Puissance en watts
  – kWh = Énergie en kilowattheures
  – VAh = Énergie apparente en voltampères heure
  – dBm = Niveau de puissance en décibels milliwatts (rapport logarithmique)
  – lux = Éclairement lumineux en lux (lm/m^2)

  Il est également possible d'indiquer d'autres unités composées du système SI, par exemple :

  m/h, m/s, m, km, mW, kW, mWh, mA, VArh

4.9.2.3 Types de données

Types de données supportés

Le tableau récapitule les types de données configurables.

Tableau 4- 1 Types de données utilisables pour l'accès au Cloud

Types de données S7 Type (bits / *octets*)	<DATAPOINT_TYPE> *
Bool (1)	BOOL
Byte (8)	UINT8
Char (8)	CHAR
USInt (8)	UINT8
Int (16)	INT16
UInt (16)	UINT16
Word (16)	UINT16
Real (32)	SINGLE_FLOAT
DWord (32)	UINT32
DInt (32)	INT32
UDInt (32)	UINT32
LReal (64)	DOUBLE_FLOAT
String (*2..256 Char*)	S7_STRING
Date_And_Time (*8*)	S7_DT
DTL (*12*)	S7_DTL

***** <DATAPOINT_TYPE> indique le type de données en cas de publication.

Pour la publication des données utiles et de la variable <DATAPOINT_TYPE> voir chapitre Format des données utiles (Page 61).

4.9.2.4 Déclenchement

Instant et nombre de données transmises

Conditions de transmission de données au cloud

Les conditions suivantes doivent être remplies pour la transmission d'une valeur :

- Le point de données est affecté dans la configuration à une rubrique.
- Au moins une condition de déclenchement est remplie.

Instant de la transmission

Le "Déclenchement" vous permet de définir pour chaque point de données l'instant auquel les valeurs des points de données sont transmises au broker.

Nombre de données transmises

Dès que la valeur d'un point de donnée est prête à être transmise, les données suivantes sont transmises ensemble au broker :

- Autre cloud

  Transmission des valeurs de tous les points de données d'une rubrique

- MindConnect IoT Extension

  Transmission des valeurs de tous les points de données d'une rubrique

Durée de la transmission (déclenchement de valeur)

Veuillez noter à propos des déclenchements de valeur, que les données d'une rubrique ou d'un groupe sont transmises aussi longtemps que la condition de déclenchement est remplie. Ceci influence le volume de données transmis.

Remarque

Transmission durant le "Cycle de balayage des variables"

Lorsque la condition de déclenchement d'un déclenchement de valeur est remplie, les données sont transmises au broker avec chaque cycle de balayage des variables.

Le "cycle de balayage des variables" se configure sur le CP dans le groupe de paramètres "Sécurité des données > CloudConnect > Général", voir chapitre Groupe de paramètres "CloudConnect" (Page 50).

Déclenchement

Les déclenchements définissent les conditions qui, lorsqu'elles sont remplies, déclenchent la transmission de la valeur enregistrées au cloud ou au broker.

Vous pouvez sélectionner jusqu'à deux types de déclenchement par variable :

- **Déclenchement temporel**
  - Cyclique
  - Instant (quotidien / hebdomadaire / mensuel)
- **Déclenchement de valeur**

  Les types de déclenchement suivants sont sélectionnables :
  - Différence (transmission en cas de différence)
  - Seuil BAS / Seuil HAUT
  - Dans plage / Hors plage

  Pour la signification, voir ci-dessous.

Vous pouvez combiner un déclenchement temporel et un déclenchement de valeur par variable. En cas de configuration de deux types de déclenchement ceux-ci sont égaux en droits.

Le transfert est déclenché dès que l'une des deux conditions de déclenchement est remplie.

Les types de déclenchement ne sont pas tous utilement combinables pour une variable. Les combinaisons de déclenchement suivantes sont supportées :

Combinaisons de déclenchement admissibles	
Déclenchement 1	**Déclenchement 2**
Cyclique	Déclenchement de valeur
Instant	-
Déclenchement de valeur	Cyclique

D'autres restrictions peuvent résulter des types de déclenchement supportés par les types de données respectifs, voir tableau ci-après.

Types de déclenchement

Déclenchement temporel

- Cyclique

  Transfert cyclique - configurable en millisecondes

  La valeur est transmise cycliquement.

- Quotidien

  La valeur est transmise une fois par jour à l'heure configurée.

- Hebdomadaire

  La valeur est transmise une fois par semaine.

- Mensuel

  La valeur est transmise une fois par mois.

  Veuillez noter :
  Si un mois compte moins de jours que la date (le 31 par ex.) indiquée dans la configuration, aucune valeur n'est transmise à la fin du mois.

Déclenchement de valeur

Tenez compte, pour tous les déclenchements de valeur, de la plage de valeurs du type de données du point de données considéré. La valeur de déclenchement est configurée en fonction de la plage de valeurs.

- Différence

  La valeur est transmise dès qu'elle diffère d'un montant configurable de la dernière valeur enregistrée sur la CPU.

  La transmission est déclenchée lorsque les conditions suivantes sont remplies :

  – Nouvelle valeur > (dernière valeur enregistrée + différence positive)
  – Nouvelle valeur < (dernière valeur enregistrée - différence positive)
  – Nouvelle valeur > (dernière valeur enregistrée - différence négative)
  – Nouvelle valeur < (dernière valeur enregistrée + différence négative)

- Seuil BAS

  La valeur est transmise dès qu'elle est inférieure à la valeur configurée.

  La transmission est déclenchée lorsque les conditions suivantes sont remplies :

  – Nouvelle valeur < Seuil BAS configuré
- Seuil HAUT

  La valeur est transmise dès qu'elle est supérieure à la valeur configurée.

  La transmission est déclenchée lorsque les conditions suivantes sont remplies :

  – Nouvelle valeur > Seuil HAUT configuré
- Dans plage

  La valeur est transmise dès qu'elle est située dans la plage configurée.

  La transmission est déclenchée lorsque les conditions suivantes sont remplies :

  – Limite inférieure de plage < Nouvelle valeur < Limite supérieure de plage
- Hors plage

  La valeur est transmise dès qu'elle est située hors de la plage configurée.

  La transmission est déclenchée lorsque les conditions suivantes sont remplies :

  – Limite inférieure de plage > Nouvelle valeur
  – Limite supérieure de plage < Nouvelle valeur

Les plages de valeurs des déclenchements de valeur sont fonction du type de données du point de données.

Type de données et types de déclenchement

Chaque type de données ne supporte pas tous les types de déclenchement. Le tableau récapitule les types de données configurables et indique, pour chaque type de données, les types de déclenchement supportés.

Signification des symboles

- **+**: Pris en charge
- **-**: non pris en charge

Tableau 4- 2 Types de données supportés par le déclenchement

Type de données S7 Type (bits / *octets*)	Déclenchements pris en charge	
	Déclenchement tempo-rel	Déclenchement de valeur
Bool (1)	+	x (uniquement la valeur 0)
Byte (8)	+	+
Char (8)	+	+
USInt (8)	+	+
Int (16)	+	+

Type de données S7 Type (bits / *octets*)	Déclenchements pris en charge	
	Déclenchement temporel	Déclenchement de valeur
UInt (16)	+	+
Word (16)	+	+
Real (32)	+	+
DWord (32)	+	+
DInt (32)	+	+
UDInt (32)	+	+
LReal (64)	+	+
String (*2..256 Char*)	+	-
Date_And_Time (*8*)	+	-
DTL (*12*)	+	-

Plages de valeurs des types de données

Des seuils sont configurés pour les types de déclenchement "Différence", "Seuil BAS", "Seuil HAUT", "Dans plage" et "Hors plage".

Les principaux types de données qui conviennent aux déclenchements sur seuil ont les plages de valeurs suivantes :

- USInt: 0...255
- Int: -32768...32767
- UInt: 0...65535
- DInt: -2147483648...+2147483647
- UDInt: 0...4294967295
- Real: 1.175495e-38...3.402823e+38

4.9.2.5 Format des données utiles

Format des données utiles

Divers systèmes de cloud utilisent différents formats lors de la transmission de données utiles. Selon le système de cloud connecté (paramètre "Fournisseur de cloud"), le CP émet les données utiles dans les formats suivants :

- MindConnect IoT Extension

  Format pour MindSphere / IoT Extension (Siemens)

- JSON

  Format pour Autre cloud

  Services de cloud qui attendent le format JSON pour le traitement de rubriques.

- XML

  (non utilisé)

Le CP utilise pour le formatage des données utiles le codage UTF-8.

Format des données utiles - MindConnect IoT Extension

```
<PUBLISH_TIMESTAMP><DATAPOINTS_BEGIN> SEPARATOR=\\n>200,<DATAPOINT_NAME>,<GROUP>,
<DATAPOINT_VALUE>,<ADDITIONAL_ATTRIBUTE>,<DATAPOINT_QUALITY_CODE><DATAPOINTS_END>
```

Format de données utiles - JSON PubSub (Autre cloud)

```
{ "Timestamp": "<PUBLISH_TIMESTAMP>", "DataItems": [
<DATAPOINTS_BEGIN> SEPARATOR=,\n>: { "Variable": "<DATAPOINT_NAME>",
"Type": "<DATAPOINT_TYPE>", "Value": "<DATAPOINT_VALUE>",
"QualityCode": "<DATAPOINT_QUALITY_CODE>" }
<DATAPOINTS_END> ] }
```

Composants de code

Le code pour le formatage des données utiles est constitué des composants listés ci-après.

La description ci-après des divers composant du code est structurée comme suit :

- **Composants de code**

  `<Syntaxe>`

  Signification

  – Exemples (pas pour tous les composants)

Composants de code : Syntaxe et signification

- **Horodatage**

  `<PUBLISH_TIMESTAMP>`

  Signification : Instant de la publication

  – Exemple :

    Syntaxe : "`<PUBLISH_TIMESTAMP>`"
    Produit la chaîne de caractères : "`2018-08-20T13:58:16.192313634+00:00`"

- **Début des données avec séparateur**

  `<DATAPOINTS_BEGIN>`

  Début d'un bloc de texte répété pour l'envoi de données.

  "`<DATAPOINTS_BEGIN>`" doit précéder "`<DATAPOINTS_END>`" (fin du bloc de texte, voir ci-dessous).

  "`SEPARATOR=`" est un séparateur, "\" est un caractère de masquage et le deuxième "\" est le caractère générique pour le séparateur "Backslash". La combinaison de caractères sépare les diverses données utiles par un backslash.

  – Exemple de transmission de données :

    Syntaxe "`<DATAPOINTS_BEGIN> SEPARATOR=\\n>200,<DATAPOINT_NAME>,<GROUP>, <DATAPOINT_VALUE>,<DATAPOINTS_END>`"

    Produit : Chaîne de caractères avec backslash comme séparateur des valeurs et à la suite de la dernière valeur envoyée.

- **200**

  `<200>`

  Code de fonction (MindConnect IoT Extension)

- **Point de données / Variable**

  `<DATAPOINT_NAME>`

  Nom du point de données

- **Groupe**

  `<GROUP>`

  Nom de groupe

- **Valeur**

  `<DATAPOINT_VALUE>`

  Valeur du point de données

- **Attribut**

  `<ADDITIONAL_ATTRIBUTE>`

  Attribut (MindConnect IoT Extension)

- **Type de données**

  `<DATAPOINT_TYPE>`

  Type de données du point de données émis par l'appareil

  Pour l'émission des types de données voir chapitre Zones d'opérandes et variables (Page 54).

- **QualityCode**

  `<DATAPOINT_QUALITY_CODE>`

  État de qualité de la valeur

  Pour sa signification, voir ci-dessous

- **Fin des données**

  `<DATAPOINTS_END>`

  Fin de la transmission de données

Exemple de données utiles transmises (JSON PubSub)

Vous trouverez ci-après un exemple de données utiles transmises d'une rubrique.

La rubrique contient trois variables d'une station S7 pour les points de données "DP1", "DP2" et "DP3".

La valeur de la clé "DataItems" est un tableau avec les objets des trois variables.

```
{ "Timestamp": "2019-05-03T09:13:46.000000000+00:00",
"DataItems": [ { "Variable":"DP1", "Type":"BOOL", "Value":"0",
"QualityCode":"GOOD" }, { "Variable":"DP2", "Type":"DOUBLE_FLOAT",
"Value":"0.496043966059748", "QualityCode":"GOOD" },
{ "Variable":"DP3", "Type":"S7_STRING", "Value":"Abcd99vE",
"QualityCode":"GOOD" } ] }
```

QualityCode

Transmission et QualityCode

La transmission des données utiles s'accompagne aussi de la transmission de l'état de qualité "QualityCode" d'un point de données. Cet état caractérise la validité de la valeur.

L'état est défini par le CP comme Publisher et possède les valeurs suivantes :

- GOOD

  La valeur est valide.

- BAD

  La valeur de la variable n'est pas valide ou pas actuelle. Causes possibles :

  – CPU à l'ARRÊT

  – Valeur pas actuelle

  – Erreur à la lecture de la variable.

La transmission est influencée comme suit par la valeur de l'état :

- Publisher → Cloud

  La publication de messages du CP comme Publisher n'est pas impactée par la valeur de l'état.

- Cloud → Subscriber

  La réception de messages par le CP comme Subscriber n'est pas impactée par la valeur de l'état.

  En cas de réception d'un message à l'état "BAD" la valeur n'est cependant pas inscrite par le CP comme Subscriber dans la CPU.

4.9.2.6 Coupure de la connexion et mise en tampon des données

Comportement du CP en cas de coupures de connexion

Les coupures de connexion induisent le comportement suivant :

- **Coupure de la connexion entre CP et CPU (CPU à l'ARRÊT)**
  - Durant la coupure de la connexion :

    Le CP émet des messages avec des chaines de caractères vides pour les valeurs et le QualityCode "BAD".
  - Après rétablissement de la connexion :

    Si la condition de déclenchement est remplie, le CP publie des messages avec des valeurs actuelles et le QualityCode "GOOD".
- **Coupure de la connexion entre CP et cloud - débranchement du câble sur le CP**
  - Durant la coupure de la connexion :

    Le CP ne publie pas de message.
  - Après rétablissement de la connexion :

    Pour le comportement, voir Section suivante.
- **Coupure de la connexion entre CP et cloud - serveur de cloud inaccessible**

  Pour le comportement, voir Section suivante.

Comportement en cas de coupure de la connexion en fonction de la valeur de QoS-

Le comportement du CP en cas de coupure de la connexion au serveur de cloud dépend de la valeur de QoS configurée.

- QoS = 0
  - Durant la coupure de la connexion :

    Le CP publie des messages avec les valeurs actuelles.

    Après chaque envoi d'un message, le CP déclenche l'"intervalle de keep alive" pour la surveillance de la connexion au broker. Si le CP ne reçoit pas de paquet du broker durant ce temps de surveillance, il envoie un paquet PINGREQ au broker.

    Si le CP ne reçoit pas de paquet PINGRESP du broker, il coupe la connexion après un temps égal à 1,5 fois la valeur de l'intervalle de keep alive. Le CP essaie ensuite de rétablir la connexion.

    Le CP ne met pas de message publié en tampon.
  - Après rétablissement de la connexion :

    Le CP publie des messages avec les valeurs actuelles.
- QoS = 1 / 2
  - Durant la coupure de la connexion :

    Le CP publie des messages avec des valeurs actuelles et attend à chaque message l'acquittement du broker. Le CP ne supprime les messages publiés de son tampon qu'après leur acquittement par le broker.

    Selon la valeur de QoS utilisée par le broker, ce dernier envoie les acquittements suivants :

    - QoS = 1 : PUBACK

    - QoS = 2 : PUBREC + PUBREL

    Si le CP ne reçoit pas d'acquittement du broker pour aucun des messages envoyés dernièrement (16 max.), il ne publie plus de nouveaux messages.

    Si le CP ne reçoit pas de paquet du broker durant le temps de surveillance (Intervalle de keep alive), il envoie un paquet PINGREQ au broker. Si le CP ne reçoit pas de paquet PINGRESP du broker, il coupe la connexion après un temps égal à 1,5 fois la valeur de l'intervalle de keep alive. Le CP essaie ensuite de rétablir la connexion.
  - Après rétablissement de la connexion :

    Après rétablissement de la connexion, le CP attend les acquittements manquants.

    Après réception des acquittements, le CP publie d'abord les messages de la mémoire de télégrammes et ensuite les nouveaux messages entrants.

Mise en tampon de données dans la mémoire de télégrammes

Le CP enregistre les messages reçus qui n'ont pas encore été publiés dans sa mémoire de télégrammes. Cette dernière a une capacité de 3500 messages.

Le tampon de télégrammes procède dans l'ordre chronologique, c.-à-d. que les données les plus anciennes sont transmise les premières (principe FIFO). Lorsque la capacité maximale est épuisée, les messages les plus anciens sont écrasés.

4.9.3 Dialogue des propriétés des rubriques

4.9.3.1 Quality of Service (QoS)

Propriétés d'une rubrique - Quality of Service (QoS)

Le paramètre devient accessible si vous ouvrez le CP dans le volet de navigation, sous les modules locaux, puis ouvrez dans le menu contextuel le dialogue des propriétés d'une rubrique.

- **Quality of Service (QoS) requise**

  Vous définissez ici le comportement de transmission voulu (Quality of Service) de cette rubrique.

  La valeur configurée doit si possible être satisfaite par le broker. Observez la réaction du broker que vous utilisez lorsqu'il ne fournit pas le niveau de QoS requis. Certains brokers choisissent dans ce cas le niveau qui se rapproche le plus du niveau requis. D'autres brokers émettent un message de défaut.

  – QoS 0

    Transfert au plus une fois

    Le CP transmet la rubrique une fois au broker. Le CP n'attend pas d'accusé de réception.

    Si la rubrique n'est pas reçue par le broker, elle est perdue.

  – QoS 1

    Transfert au moins une fois

    Le CP transmet la rubrique au broker tant qu'il n'a pas reçu du broker de paquet PUBACK comme accusé de réception.

  – QoS 2

    Transfert une seule fois

    Le CP transmet la rubrique au broker et attend de recevoir du broker l'accusé de réception en deux étapes requis par la spécification.

    Cette variante, qui constitue le plus haut niveau de qualité, implique cependant un temps de gestion maximum tant du côté du client que du côté du serveur.

4.10 Security

Une vue d'ensemble de l'étendue et de l'application des fonctions de sécurité des données du CP est fournie au chapitre Industrial Ethernet Security (Page 15).

Concernant la capacité fonctionnelle des fonctions de sécurité des données, voir chapitre Caractéristiques de sécurité des données - Règles de pare-feu (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 68).

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 Pare-feu

4.10.2.1 Ordre des pare-feux lors du contrôle des télégrammes entrants et sortants

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.

Voir aussi

Connexions programmées : Restriction des règles de pare-feu (Page 41)

4.10.2.2 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.

4.10.2.3 HTTP et HTTPS via IPv6 ne fonctionne pas

La communication HTTP et HTTPS via le protocole IPv6 sur le serveur web de la station ne fonctionne pas.

Si le pare-feu est activé, les cases cochées "Autoriser HTTP" et "Autoriser HTTPS" dans l'entrée "Pare-feu" > "Règles IPv6 prédéfinies" des paramètres de sécurité locaux, sont sans fonction.

4.10.3 Fonctions en ligne

4.10.3.1 Diagnostic de sécurité en ligne via le port 8448

Diagnostic de sécurité des données via le port 8448

Condition : Accès au serveur Web du CP via HTTPS activé.

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.

4.10.3.2 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

Procédez comme suit lorsque les fonctions de sécurité des données sont activées :

1. Dans les paramètres de sécurité généraux (voir navigation de projet), 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".
4. Sélectionnez ensuite le CP sur la station S7.
5. Activez le mode pare-feu avancé dans les paramètres de sécurité locaux du CP, dans le groupe de paramètres "Sécurité des données > Pare-feu".
6. Ouvrez le groupe de paramètres "Règles IP".

7. Dans le tableau, ajoutez une nouvelle règle IP pour les services qui viennent d'être créés, comme suit :
   – Action : Allow ; "Externe -> vers station" avec le service global créé "Echo Request"
   – Action : Allow ; "De station -> vers externe" avec le service global créé "Echo Reply"
8. Pour la règle IP d'Echo Request, entrez sous "Adresse IP source" l'adresse IP de la station d'ingénierie. Vous ne permettez ainsi qu'aux télégrammes ICMP (ping) issus de votre station d'ingénierie de passer le pare-feu.

4.10.4 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.

4.10.5 Certificats

4.10.5.1 Certificats tiers

Certificats de fournisseurs de cloud

Pour la communication cryptée entre la station S7 et le broker (MQTT via TLS), vous avez besoin du certificat CA racine du broker et éventuellement de certificats d'appareil ou d'une clé privée.

Les exigences varient selon les fournisseurs de cloud.

Procurez-vous les fichiers requis auprès de votre fournisseur de cloud ou téléchargez-les de son site Internet.

Vous trouverez des informations sur les fichiers requis et les pages Internet pertinentes dans l'exemple d'application du CP. Vous trouverez ce document sur le site du Siemens Industry Online Support.
Link: (https://support.industry.siemens.com/cs/ww/fr/ps/25625/ae)

4.10.5.2 Gestionnaire de certificats

Affectation de certificats

Si vous utilisez pour le CP la communication avec authentification, vous devez importer les certificats des partenaires de communication dans le projet STEP 7 et les charger avec les données de configuration sur le CP.

1. Importez les certificats tiers de tous les partenaires de communication via le gestionnaire de certificats dans les paramètres de sécurité généraux.
2. Affectez ensuite au CP les certificats de tous ses partenaires de communication, 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 71).

4.10.5.3 Manipulation de certificats

Certificats pour l'authentification

Si vous avez configuré pour le CP une 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 est établi pour chaque application du CP qui exige un certificat. Il est affiché dans STEP 7 sous "Paramètres de sécurité généraux > Gestionnaire de certificats > Certificats d'appareils". En plus d'informations complémentaires, vous y trouverez l'utilisation des certificats (service/application).

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.

Pour que le CP, 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 CP, 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 CP > 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 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 CP, il faut qu'il soit affiché dans le groupe de paramètres "Sécurité des données" du CP.

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

Procédez pour l'importation comme suit :

1. Dans le projet STEP 7, sélectionnez le CP.
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 CP.

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 CP.

L'exportation du certificat du CP 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 CP 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 CP 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 (SAN)" des données de configuration de 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.

Blocs de programme

5

5.1 Blocs de programme pour la communication

Utilisation des blocs de programme

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

La communication via blocs de programme n'est pas configurée. Les blocs de programme paramétrables sont disponibles comme interface pour votre programme utilisateur STEP 7.

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

Recommandation : Utilisez si possible la version actuelle d'un bloc.

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.

Blocs de programme pris en charge pour l'Open User Communication (OUC)

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

Les blocs suivants sont disponibles :

- **TSEND_C / TRCV_C**

  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 des blocs pour l'établissement / coupure de la connexion et des blocs distincts pour l'émission / la réception de données :

- **TCON / TDISCON**

  Connexion / déconnexion

- **TUSEND / TURCV**

  Emission ou réception de données via UDP

- **TSEND / TRCV**

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

- **TMAIL_C**

  Envoi d'e-mails

  Pour pouvoir transmettre des e-mails cryptés, 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**

  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 79).

Remarque

Conditions dans la configuration 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.

Bloc pour le client FTP du CP

Vous trouverez le bloc de programme sous STEP 7 dans la Task Card "Instructions > Communication > Processeur de communication > SIMATIC NET CP".

- **FTP_CMD**

  Bloc pour la fonction de client FTP

  Configuration de connexions FTP et transfert de fichiers depuis/vers un serveur FTP

  Tenez compte de la description du chapitre Bloc pour la fonction de client FTP (Page 80).

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.

Utilisation des SDT

- **TCON_IP_v4**

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

- **TADDR_Param**

  Pour la transmission de données 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)

Pour la transmission sécurisée des données :

- **TCON_IP_V4_SEC**

  Pour la transmission sécurisée des données via TCP ou UDP

- **TCON_QDN_SEC**

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

- **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

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 réussie 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.

Blocs de programme - Récapitulatif

Les blocs de programme (instructions) suivants sont disponibles pour le CP.

Tableau 5- 1 Blocs de l'Open User Communication

Protocole	Blocs de programme (instruction)	Types de donnée système
TCP	• TSEND_C/TRCV_C ou • TCON/TDISCON + TSEND/TRCV	• TCON_IP_v4 • TCON_QDN • TCON_Configured • TCON_IP_V4_SEC • TCON_QDN_SEC
ISO-on-TCP		• TCON_IP_RFC
ISO		• TCON_Configured
UDP	• TCON/TDISCON + TUSEND/TURCV	• TCON_IP_v4 • TADDR_Param • TADDR_SEND_QDN • TADDR_RCV_IP
E-mail	• TMAIL_C	• TMAIL_V4 • TMAIL_V6 • TMAIL_FQDN • TMAIL_V6_SEC • TMAIL_QDN_SEC

Tableau 5- 2 Bloc pour les services de communication du CP

Protocole	Blocs de programme (instruction)	Types de donnée système
FTP	• FTP_CMD	• FTP_CONNECT_IPV4 • FTP_CONNECT_IPV6 • FTP_CONNECT_NAME • FTP_FILENAME • FTP_FILENAME_PART

Tableau 5- 3 Bloc pour la configuration de l'interface Ethernet ou d'un serveur NTP/DNS

Fonction	Blocs de programme (instruction)	Types de donnée système
Configuration de l'interface Ethernet	• T_CONFIG	• IF_CONF_V4 • IF_CONF_V6 • IF_CONF_NTP • IF_CONF_DNS • IF_CONF_MAC

5.2 Modification de l'adresse IP en cours de fonctionnement

Modification de paramètres d'adresse 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

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).

Vous pouvez utiliser les blocs de programme et types de données système suivants :

- T_CONFIG

  En relation avec SDT :

  – IF_CONF_V4
  – IF_CONF_V6
  – IF_CONF_MAC
  – IF_CONF_DNS
  – IF_CONF_NTP

  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".

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

Conditions requises dans la configuration 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.

5.3 Bloc pour la fonction de client FTP

5.3.1 FTP_CMD

FTP_CMD

Vous trouverez le bloc dans STEP 7 si Main [OB1] est ouvert dans la Task Card "Instructions" sous "Communication > Processeur de communication > SIMATIC NET CP".

L'instruction FTP_CMD permet d'établir des liaisons FTP et de transmettre des fichiers depuis et vers un serveur FTP.

Il est possible de transférer les données via FTP ou FTPS (connexions SSL sécurisées).

Remarque

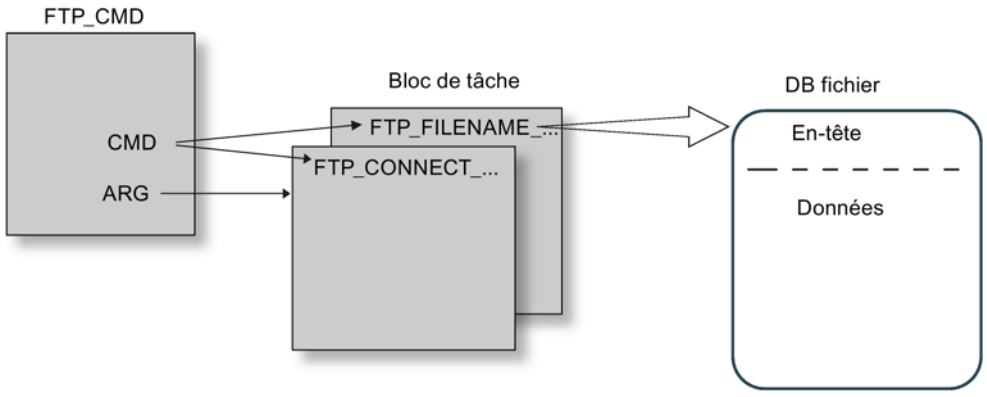
FTPS : Synchronisation de certificats

FTPS exige la synchronisation des certificats entre serveur FTP et client FTP. Si le serveur FTP est configuré hors du projet STEP 7 du client FTP, l'importation du certificat du serveur FTP s'impose. Dans le gestionnaire de certificats, importez le certificat du serveur FTP comme certificat digne de confiance.

Mode de fonctionnement

L'instruction FTP_CMD renvoie à un bloc de tâche (ARG) dans lequel la commande FTP est spécifiée. Selon le type de commande FTP (CMD), ce bloc de tâche utilise pour le paramétrage différentes structures de données. Des types de données appropriés (UDT) sont disponibles pour ces différentes structures.

La figure ci-dessous présente la structure d'appel :



Blocs de tâche

Les blocs de tâche utilisent les structures de données suivantes :

- Établissement d'une liaison

  L'établissement d'une liaison s'effectue à l'aide de diverses structures de données pour les modes d'accès suivants :

  – FTP_CONNECT_IPV4 : établissement de connexion avec adresses IP selon IPv4

  – FTP_CONNECT_IPV6 : établissement de connexion avec adresses IP selon IPv6

  – FTP_CONNECT_NAME : établissement de connexion avec nom de serveur (DNS)

- Transfert de données

  Il existe diverses structures de données pour le transfert de données :

  – FTP_FILENAME : structure de données par l'accès à un fichier complet

  – FTP_FILENAME_PART : structure de données pour l'accès en lecture à une zone de données

Transfert de données dans le DB fichier

Le transfert de données s'effectue dans des blocs de données qui se compose d'un en-tête pour les données de la tâche et d'une zone pour les données utiles. Le bloc de données est spécifié dans le tampon de tâches.

Vous trouverez un exemple de DB fichier dans le système d'information STEP 7.

5.3.2 Paramètres d'entrée de FTP_CMD

Explication des paramètres d'entrée

L'instruction FTP_CMD accepte les paramètres d'entrée suivants :

Tableau 5- 4 Paramètres formels de l'instruction FTP_CMD - paramètres d'entrée

Paramètre	Déclaration	Type de données	Zone de mémoire	Signification / remarque
REQ	Input	BOOL	E, A, M, DB, L	Lance la tâche d'émission sur front montant.
ID *	INPUT	INT	1, 2 ... 64	Les tâches FTP sont exécutées via des connexions FTP. Ce paramètre identifie la connexion utilisée.
CMD *	INPUT	BYTE	Voir aussi le tableau "Commandes".	Commande FTP qui doit être exécutée lors de l'appel de l'instruction. Vous trouverez les plages de valeurs pour les types de commande FTP à la suite de ce tableau. La commande FTP figurant ici doit être spécifiée de manière identique dans le bloc de tâche (paramètre ARG). Quand une commande n'est pas supportée par le firmware du CP, un message d'erreur le signale avec STATUS = $8F6B_H$.
ARG *	INPUT	VARIANT	Voir aussi le tableau "Commandes".	Bloc de tâche Renvoie à la zone de données avec les paramètres d'exécution correspondant à la commande FTP. Des types de données spécifiques (UD) sont utilisée en fonction de la commande FTP. Les UDT sont indiqués ci-après. L'emploi du type de données ANY n'est pas licite pour l'indicateur à spécifier !

***** Les valeurs des paramètres d'entrée "ID" et "CMD" écrasent la valeur du paramètre d'entrée "ARG".

Commandes FTP dans le paramètre "CMD"

Le tableau suivant donne la signification des commandes du paramètre "CMD" et indique les UDT à utiliser pour les divers blocs de tâche.

Tableau 5- 5 Types de commande

CMD (type de commande)	Blocs de tâche pertinents / UDT	Signification / maniement
0 (NOOP)	*	Le FB appelé n'exécute aucune action. Avec cette valeur du paramètre, les indications d'état sont les suivantes : DONE=1; ERROR=0; STATUS=0
1 (CONNECT)	FTP_CONNECT_IPV4 FTP_CONNECT_IPV6 FTP_CONNECT_NAME	Etablissement de connexion FTP Par cette commande, le client FTP établit une connexion FTP à un serveur FTP (port 21). Cette connexion est disponible pour toutes les autres commandes FTP sous l'ID de connexion attribuée ici. Des données sont alors échangées avec le serveur FTP spécifié pour cet utilisateur.
2 (STORE)	FTP_FILENAME	Avec cet appel de fonction, un bloc de données (DB de fichier) est transmis du client FTP (CPU S7) au serveur FTP. Attention : si le fichier (DB de fichier) existe déjà sur le serveur FTP, il sera écrasé.
3 (RETRIEVE)	FTP_FILENAME	Avec cet appel de fonction, un fichier est transmis du serveur FTP au client FTP (CPU S7). Attention : si le bloc de données (DB de fichier) sur le client FTP contient déjà un fichier, il sera écrasé.
4 (DELETE)	FTP_FILENAME	Avec cet appel de fonction, vous supprimez un fichier sur le serveur FTP.
5 (QUIT)	*	Avec cet appel de fonction, vous coupez la connexion FTP spécifiée dans "ID".
6 (APPEND)	FTP_FILENAME	De manière analogue à "STORE", la commande "APPEND" (ajouter) stocke un fichier sur le serveur FTP. Mais avec "APPEND", le fichier existant sur le serveur FTP n'est pas écrasé, le nouveau contenu à mémoriser s'y ajoute. Si le fichier n'existe pas sur le serveur FTP, il est créé.
7 (RETR_PART)	FTP_FILENAME_PART	Avec la commande "RETR_PART" (lire une partie), vous pouvez demander un extrait d'un fichier se trouvant sur le serveur FTP. Avec les fichiers très volumineux, ceci vous permet de restreindre la lecture à la partie dont vous avez besoin. Pour cela, vous devez connaître la structure du fichier. Indiquez l'extrait souhaité à l'aide des deux paramètres "OFFSET" et "LEN" du FB 40.

***** Pour les types de commande 0 (NOOP) et 5 (QUIT) il faut indiquer un bloc de tâche (UDT) quelconque. Celui-ci n'est pas traité.

5.3.3 Blocs de tâche pour FTP_CMD

Signification

Le bloc de tâche est attribué à l'instruction FTP_CMD via le paramètre ARG. La structure dépend du type de commande FTP. Dans la mesure où vous utilisez les types de données spécifiés (UDT), l'instruction détecte le type du bloc de tâche. Les types de données (UDT) sont indiqués ci-après en fonction des blocs de tâche suivants :

- établissement de connexion FTP avec adresse IP selon IPv4
- établissement de connexion FTP avec adresse IP selon IPv6
- établissement de connexion FTP avec nom de serveur
- accès en écriture et lecture et autres commandes FTP
- commande FTP RETR_PART

Bloc de tâche pour établissement de connexion FTP avec adresse IP selon IPv4

L'établissement de connexion FTP avec adresse IP selon IPv4 s'effectue avec la structure de données suivante.

Tableau 5- 6 FTP_CONNECT_IPV4

Paramètre	Type	Plage de valeurs	Signification / remarque
InterfaceID	HW_ANY		Adresse de début du module Lors de l'appel d'une instruction, vous fournissez l'adresse de début du module CP dans le paramètre LADDR. L'adresse de début du CP est indiquée dans la configuration du CP sous : "Propriétés>Adresses>Entrées"
ID	CONN_OUC	1, 2...64	Les tâches FTP sont exécutées via des connexions FTP. Ce paramètre identifie la connexion utilisée.
ConnectionType	BYTE	0	Type de connexion "FTP"
ActiveEstablishment	BOOL	TRUE	TRUE = établissement actif d'une connexion
FTPCmd	BYTE	1	Commande FTP "CONNECT" Commande FTP qui est exécutée lors de l'appel de l'instruction. Vous trouverez les plages de valeurs pour les types de commande au chapitre Paramètres d'entrée de FTP_CMD (Page 82). Nota : La commande FTP figurant ici doit être spécifiée de manière identique dans le paramètre d'entrée CMD.
CertIndex	BYTE	0 = FTP 1 = FTPS	Choisissez l'un des types de protocoles FTP ou FTPS. Note à propos de FTPS : Si le serveur FTP est configuré hors du projet STEP 7 du client FTP, l'importation du certificat du serveur FTP s'impose.
UserName	STRING[32]	'benutzer'	Nom d'utilisateur pour la connexion au serveur FTP.

Paramètre	Type	Plage de valeurs	Signification / remarque
Password	STRING[32]	'passwort'	Mot de passe pour la connexion au serveur FTP.
FTPserverIPaddr	IP_V4	ADDR(1) ... ADDR(4)	Adresse IP du serveur FTP sous forme d'Array[1..4] of Byte, 1 octets spécifiant un bloc de l'adresse. Exemple : ADDR(1) spécifient le premier bloc de l'adresse (le premier octet de l'adresse).

Bloc de tâche pour établissement de connexion FTP avec adresse IP selon IPv6

L'établissement de connexion FTP avec adresse IP selon IPv6 s'effectue avec la structure de données suivante.

Tableau 5- 7 FTP_CONNECT_IPV6

Paramètre	Type	Plage de valeurs	Signification / remarque
InterfaceID	HW_ANY		Adresse de début du module Lors de l'appel d'une instruction, vous fournissez l'adresse de début du module CP dans le paramètre LADDR. L'adresse de début du CP est indiquée dans la configuration du CP sous : "Propriétés>Adresses>Entrées"
ID	CONN_OUC	1, 2...64	Les tâches FTP sont exécutées via des connexions FTP. Ce paramètre identifie la connexion utilisée.
ConnectionType	BYTE	0	Type de connexion "FTP"
ActiveEstablishment	BOOL	TRUE	TRUE = établissement actif d'une connexion
FTPCmd	BYTE	1	Commande FTP "CONNECT" Commande FTP qui est exécutée lors de l'appel de l'instruction. Vous trouverez les plages de valeurs pour les types de commande au chapitre Paramètres d'entrée de FTP_CMD (Page 82). Nota : La commande FTP figurant ici doit être spécifiée de manière identique dans le paramètre d'entrée CMD.
CertIndex	BYTE	0 = FTP 1 = FTPS	Choisissez l'un des types de protocoles FTP ou FTPS. Note à propos de FTPS : Si le serveur FTP est configuré hors du projet STEP 7 du client FTP, l'importation du certificat du serveur FTP s'impose.
UserName	STRING[32]	'utilisateur'	Nom d'utilisateur pour la connexion au serveur FTP.
Password	STRING[32]	'mot_de_passe'	Mot de passe pour la connexion au serveur FTP.
FTPserverIPaddr	IP_V6	ADDR(1) ... ADDR(16)	Adresse IP du serveur FTP sous forme d'Array[1..16] of Byte, 2 octets spécifiant un bloc de l'adresse. Exemple : ADDR(1) + ADDR(2) spécifient le premier bloc de l'adresse.

Bloc de tâche pour établissement de connexion FTP avec nom de serveur

L'établissement de connexion FTP avec mention d'un nom de serveur s'effectue avec la structure de données suivante. Le nom de serveur est attribué via DNS à une adresse IP.

Tableau 5- 8 FTP_CONNECT_NAME

Paramètre	Type	Plage de valeurs	Signification / remarque
InterfaceID	HW_ANY		Adresse de début du module Lors de l'appel d'une instruction, vous fournissez l'adresse de début du module CP dans le paramètre LADDR. L'adresse de début du CP est indiquée dans la configuration du CP sous : "Propriétés>Adresses>Entrées"
ID	CONN_OUC	1, 2...64	Les tâches FTP sont exécutées via des connexions FTP. Ce paramètre identifie la connexion utilisée.
ConnectionType	BYTE	0	Type de connexion "FTP"
ActiveEstablishment	BOOL	TRUE	TRUE = établissement actif d'une connexion
FTPcmd	BYTE	1	Commande FTP "CONNECT" Commande FTP qui est exécutée lors de l'appel de l'instruction. Vous trouverez les plages de valeurs pour les types de commande au chapitre Paramètres d'entrée de FTP_CMD (Page 82). Nota : La commande FTP figurant ici doit être spécifiée de manière identique dans le paramètre d'entrée CMD.
CertIndex	BYTE	0 = FTP 1 = FTPS	Choisissez l'un des types de protocoles FTP ou FTPS. Note à propos de FTPS : Si le serveur FTP est configuré hors du projet STEP 7 du client FTP, l'importation du certificat du serveur FTP s'impose.
UserName	STRING[32]	'benutzer'	Nom d'utilisateur pour la connexion au serveur FTP.
Password	STRING[32]	'passwort'	Mot de passe pour la connexion au serveur FTP.
FTPserverName	STRING[254]		Adresse IP du serveur FTP.

Bloc de tâche pour accès en écriture et lecture et autres commandes FTP

La structure de données ci-après est utilisée pour les commandes FTP store, retrieve, delete et append.

Tableau 5- 9 FTP_FILENAME

Paramètre	Type	Plage de valeurs	Signification / remarque
InterfaceID	HW_ANY		Adresse de début du module Lors de l'appel d'une instruction, vous fournissez l'adresse de début du module CP dans le paramètre LADDR. L'adresse de début du CP est indiquée dans la configuration du CP sous : "Propriétés>Adresses>Entrées"
ID	CONN_OUC	1, 2...64	Les tâches FTP sont exécutées via des connexions FTP. Ce paramètre identifie la connexion utilisée.

Paramètre	Type	Plage de valeurs	Signification / remarque
ConnectionType	BYTE	0	Type de connexion "FTP"
ActiveEstablishment	BOOL	TRUE	TRUE = établissement actif d'une connexion
FTPcmd	BYTE	2, 3, 4, 6	Commande FTP "STORE / RETRIEVE / DELETE / APPEND" Commande FTP qui est exécutée lors de l'appel de l'instruction. Vous trouverez les plages de valeurs pour les types de commande au chapitre Paramètres d'entrée de FTP_CMD (Page 82). Nota : La commande FTP figurant ici doit être spécifiée de manière identique dans le paramètre d'entrée CMD.
CertIndex	BYTE	0 = FTP 1 = FTPS	Choisissez l'un des types de protocoles FTP ou FTPS. Note à propos de FTPS : Si le serveur FTP est configuré hors du projet STEP 7 du client FTP, l'importation du certificat du serveur FTP s'impose.
DataBlockNumber	UINT		Le bloc de données indiqué ici contient le DB fichier à lire ou à écrire.
LenFilename	UINT	0...1000	Le paramètre "LenFilename" indiquant la longueur totale du nom de fichier n'est pas traité. L'indication de longueur prise en compte est par contre celle figurant dans la chaine de caractères du paramètre "Filename".
Filename	ARRAY[0..3] OF STRING[254]		Nom du fichier source ou cible. Les quatre chaines de caractères sont concaténées et transférées comme chaine complète sur le serveur.

Bloc de tâche pour la commande FTP RETR_PART

La structure de données suivante est utilisée pour la commande FTP RETR_PART.

Tableau 5- 10 FTP_FILENAME_PART

Paramètre	Type	Plage de valeurs	Signification / remarque
InterfaceID	HW_ANY		Adresse de début du module Lors de l'appel d'une instruction, vous fournissez l'adresse de début du module CP dans le paramètre LADDR. L'adresse de début du CP est indiquée dans la configuration du CP sous : "Propriétés>Adresses>Entrées"
ID	CONN_OUC	1, 2...64	Les tâches FTP sont exécutées via des connexions FTP. Ce paramètre identifie la connexion utilisée.
ConnectionType	BYTE	0	Type de connexion "FTP"
ActiveEstablishment	BOOL	TRUE	TRUE = établissement actif d'une connexion

Paramètre	Type	Plage de valeurs	Signification / remarque
FTPcmd	BYTE	7	Commande FTP "RETR_PART" Commande FTP qui est exécutée lors de l'appel de l'instruction. Vous trouverez les plages de valeurs pour les types de commande au chapitre Paramètres d'entrée de FTP_CMD (Page 82). La commande FTP figurant ici doit être spécifiée de manière identique dans le paramètre d'entrée CMD.
CertIndex	BYTE	0 = FTP 1 = FTPS	Choisissez l'un des types de protocoles FTP ou FTPS. Note à propos de FTPS : Si le serveur FTP est configuré hors du projet STEP 7 du client FTP, l'importation du certificat du serveur FTP s'impose.
Offset	DWORD		décalage en octets à partir duquel le fichier est à lire.
Length	DWORD		longueur partielle, nombre d'octets lus à partir de la valeur indiquée par "OFFSET". Particularités : • Avec "DW#16#FFFFFFFF", c'est le reste disponible du fichier qui est lu. Résultat OK (DONE = 1, STATUS = 0) si aucune autre erreur ne survient. • Quand OFFSET > longueur du fichier d'origine : longueur du fichier cible (ACT_LENGTH dans le DB fichier) : 0 octet dans la CPU. Résultat OK (DONE = 1, STATUS = 0) si aucune autre erreur ne survient. • Quand OFFSET + LEN > longueur du fichier d'origine (et LEN ≠ 0xFFFFFFFF) : longueur du fichier cible (ACT_LENGTH dans le DB fichier) : octets disponibles à partir de "OFFSET". Résultat OK (DONE = 1, STATUS = 0) si aucune autre erreur ne survient.
DataBlockNumber	UINT		Le bloc de données indiqué ici contient le DB fichier à lire ou à écrire.
LenFilename	UINT	0...1000	Le paramètre "LenFilename" indiquant la longueur totale du nom de fichier n'est pas traité. L'indication de longueur prise en compte est par contre celle figurant dans la chaine de caractères du paramètre "Filename".
Filename	ARRAY[0..3] OF STRING[254]		Nom du fichier source ou cible. Les quatre chaines de caractères sont concaténées et transférées comme chaine complète sur le serveur.

Fourniture des paramètres pour les types de commande NOOP et QUIT

Affectez également une référence au bloc de tâche à l'instruction FTP_CMD pour les types de commande ci-après :

CMD = 0 (NOOP)

CMD = 5 (QUIT)

Le contenu du bloc de tâche n'est pas exploité lors de l'exécution de ces types de commande, le type (UDT) du bloc de tâche indiqué est donc sans importance.

Remarque

Comportement en l'absence de référence au bloc de tâche FTP

En l'absence de référence, la commande n'est pas exécutée. L'instruction demeure apparemment en phase d'exécution sans envoi de message à l'interface du programme utilisateur.

5.3.4 Paramètres de sortie et informations d'état de FTP_CMD

Paramètres BUSY, DONE et ERROR

Vous contrôlez l'état d'exécution au moyen des paramètres BUSY, DONE, ERROR et STATUS. Le paramètre BUSY indique l'état du traitement. Avec le paramètre DONE, vous vérifiez si une tâche s'est exécutée correctement. Le paramètre ERROR est à 1 si des erreurs se sont produites pendant l'exécution de "FTP_CMD". Les informations d'erreur sont transmises par le paramètre STATUS.

Le tableau suivant montre la relation entre les paramètres BUSY, DONE et ERROR :

BUSY	DONE	ERROR	Description
1	-	-	La tâche est en cours d'exécution.
0	1	0	La tâche a été exécutée correctement.
0	0	1	La tâche s'est terminée avec une erreur. La cause de l'erreur est indiquée dans le paramètre STATUS.
0	0	0	Aucune nouvelle tâche n'a été affectée.

Exploiter les indications d'état

Remarque

Analyse

- Analyse si BUSY = 0

  N'analysez pas l'affichage d'état avant que BUSY = 0.
- État $8Fxx_H$

  Pour les entrées à l'état $8Fxx_H$, veuillez consulter également le manuel de référence STEP 7 Fonctions système et fonctions standard. Vous y trouverez des informations au chapitre "Evaluation d'erreur avec le paramètre de sortie RET_VAL".

Tableau 5- 11 FTP_CMD : signification du paramètre STATUS en collaboration avec DONE et ERROR

DONE	ERROR	STATUS	Signification
0	0	0000_H	Il n'y a pas de tâche en cours.
1	0	0000_H	La tâche s'est terminée sans erreur.
0	0	7001_H	La tâche a été lancée pour la première fois
0	0	7002_H	La tâche est encore en cours.
0	1	$80C4_H$	Erreur de communication (survient temporairement ; une répétition dans le programme utilisateur est donc judicieuse).
0	1	8183_H	La configuration ne correspond pas aux paramètres de la tâche.
0	1	8401_H	Erreur inconnue Causes possibles : • Un timeout a été détecté sur la connexion. • Le serveur FTP a coupé la connexion. Remède : Réémettre les commandes QUIT et CONNECT pour rétablir la connexion.
0	1	8402_H	La connexion est à l'état erroné. Il se peut que le timeout de la connexion soit dépassé ou que le serveur FTP ait coupé la connexion. Remède : Réémettre les commandes QUIT et CONNECT pour rétablir la connexion.
0	1	8403_H	La connexion a échoué.
0	1	8404_H	Accès au serveur FTP impossible.
0	1	8405_H	La transmission a échoué.
0	1	8406_H	Timeout de l'opération en cours
0	1	8407_H	Impossible de trouver le fichier sur le serveur FTP.
0	1	8408_H	Transmission impossible.
0	1	8409_H	Impossible d'aller chercher le fichier.
0	1	8410_H	L'activation du port TCP pour la connexion de données a échoué.
0	1	8411_H	L'indication d'offset n'est pas compatible.
0	1	8412_H	Erreur lors du changement d'indication de répertoire
0	1	8413_H	Erreur à la réception de données
0	1	8414_H	Erreur à l'émission de données
0	1	8415_H	L'indication de CMD (type de commande a été rejetée par le client.
0	1	8416_H	La connexion a été coupée par le serveur FTP.
0	1	8418_H	Erreur dans les données utiles. Causes possibles : • Le nom de fichier est vide. • La longueur de données est "0". • etc.
0	1	8419_H	Aucune Socket-Ressource n'est disponible pour l'ouverture d'une connexion de données.
0	1	8420_H	Aucune Socket-Ressource n'est disponible pour l'ouverture d'une connexion de commande.
0	1	8421_H	Erreur à l'ouverture en lecture du DB de fichier
0	1	8422_H	Erreur à l'ouverture en écriture du DB de fichier

DONE	ERROR	STATUS	Signification
0	1	8423_H	Echec d'établissement d'une connexion au serveur FTP.
0	1	8424_H	Erreur interne
0	1	8425_H	Erreur de format du nom de domaine
0	1	8426_H	Nombre excessif de requêtes DNS.
0	1	8427_H	Le serveur DNS indiqué n'a pas trouvé de correspondance pour le nom de domaine spécifié.
0	1	8428_H	Aucune ressource de connexion n'est disponible.
0	1	8429_H	ID de canal inconnu
0	1	8430_H	Le DB fichier est trop court.
0	1	8431_H	Erreur d'écriture dans le DB fichier.
0	1	8432_H	Erreur de lecture du DB fichier.
0	1	8433_H	Erreur d'accès au DB fichier.
0	1	8434_H	L'action a été abandonnée.
0	1	8435_H	Le canal est réinitialisé.
0	1	8436_H	Réponse du serveur inattendue.
0	1	8437_H	Impossible de vérifier le certificat.
0	1	8438_H	Une erreur inconnue est survenue.
0	1	8439_H	La commande FTP provoque une erreur. La cause se trouve sur le serveur FTP (commande REST).
0	1	8440_H	Le serveur FTP ne prend pas en charge le protocole SSL requis.
0	1	8446_H	Après l'envoi du mot de passe FTP au serveur FTP celui-ci a retourné un code inattendu.
0	1	8451_H	Une erreur a été signalée après la tentative de passer du mode de transmission binaire à ASCII.
0	1	8455_H	Une requête d'enregistrement sur CM/CP a échoué.
0	1	8460_H	Un problème est survenu lors de la transaction SSL/TLS.
0	1	8469_H	Erreur d'interface Impossible d'utiliser l'interface de sortie. Remède : Spécifiez l'interface à utiliser pour les connexions sortantes.
0	1	8475_H	Le certificat SSL ou le SSH md5 fingerprint a été estimé non digne de confiance.
0	1	8476_H	Le serveur FTP n'a rien reçu. Dans l'état actuel, il s'agit probablement d'un comportement erroné.
0	1	8477_H	Le "crypto engine" (module cryptographique) spécifié est introuvable.
0	1	8478_H	L'opération a échoué, spécifiez que le "crypto engine" SSL (module cryptographique) est le module par défaut.
0	1	8480_H	Un problème est survenu en rapport avec le certificat du client FTP.
0	1	8481_H	Le chiffre indiqué n'est pas utilisable.
0	1	8482_H	Le serveur FTP utilise un codage qui n'est pas pris en charge.
0	1	8484_H	La taille maximale de fichier a été dépassée.
0	1	8485_H	Le DB de fichier a été modifié durant l'émission ou n'a pas été correctement créé.

DONE	ERROR	STATUS	Signification
0	1	8489_H	Les données n'ont pas pu être émises. La capacité mémoire disponible sur le serveur est insuffisante.
0	1	8492_H	Le fichier existe déjà. Le fichier n'est pas écrasé.
0	1	8496_H	Un problème est survenu à la lecteur du certificat CA SSL.
0	1	8497_H	Une erreur inattendue est survenue lors de la session SSH.
0	1	8498_H	Impossible d'établir la connexion SSL.
0	1	8499_H	Le socket n'est pas prêt à émettre/recevoir. Attendez qu'il soit prêt, puis essayez à nouveau.
0	1	8501_H	La vérification du certificat SSL du serveur FTP a échoué.
0	1	8507_H	Un timeout est survenu durant la session FTP active lors de l'attente du serveur FTP dans le cadre de l'établissement de la connexion.
0	1	$8F54_H$	Le bit "EXIST" de l'en-tête du DB fichier n'est pas à 1.
0	1	$8F55_H$	Bit d'état d'en-tête : Locked
0	1	$8F56_H$	Le bit NEW dans l'en-tête du DB fichier n'a pas été remis à zéro.
0	1	$8F6B_H$	Causes possibles : • Valeur erronée du paramètre CMD Il peut prendre les valeurs 0 à 15. • Une commande du FB 40 n'est pas supportée. Cause possible : Firmware incorrect du CP Remède : mise à jour du firmware (avec les anciens CP, utiliser les fonctions FC 40 à FC 44 au lieu du FB 40).
0	1	$8F7F_H$	Erreur interne, par ex. référence ANY illicite.

5.3.5 Structure du bloc de données (DB fichier) pour le mode client FTP

Mode de fonctionnement

Vous devez créer des blocs de données sur la CPU de votre station S7 pour la transmission de données via FTP (DB fichiers). Ces blocs de données doivent être conformes à une structure définie afin qu'ils puissent être manipulés par les services FTP au même titre que des fichiers transmissibles. Ils se composent des sections suivantes

- Section 1 : En-tête de DB fichier (structure invariable avec une longueur de 20 octets)
- Section 2 : Données utiles sous forme de "Array [..] of Byte" ou de "Array [..] of Char" (longueur et structure variables)

Cohérence des données

Veillez à ne pas accéder plusieurs fois simultanément au même DB fichier.

Création d'un DB fichier

1. Créez un bloc de données dans STEP 7.
2. Ouvrez l'éditeur de blocs.
3. Sélectionnez, dans l'éditeur de bloc, la ligne que vous utiliserez comme ligne de début du DB fichier.
4. Saisissez au clavier le type "FILE_DB_HEADER" dans la colonne "Type de données".

   La structure de données qui est alors créée possède la structure d'en-tête requise par le DB fichier.
5. Mettez le paramètre "WRITEACCESS" à "true" pour permettre l'accès.
6. Spécifiez la valeur de longueur des données utiles dans le paramètre "MAX_LENGTH".
7. Créez au-dessous un champ de données de type "Array [..] of Byte" ou "Array [..] of Char" pour les données utiles à transférer.

   La taille du champ doit correspondre à l'entrée sous "MAX_LENGTH" de l'en-tête.

En-tête de DB fichier pour mode client FTP

L'en-tête de DB fichier décrit ici est identique à l'en-tête de DB fichier décrit pour le mode serveur FTP.

Paramètre	Type	Valeur / Signification	Alimentation
EXIST	BOOL	Le bit EXIST indique la présence ou non de données valides dans la zone de données utiles. La commande FTP retrieve traite le contrat uniquement si EXIST=1. • 0 : Le DB fichier ne contient pas de données utiles valides (Fichier inexistant). • 1 : Le DB de fichier contient des données utiles valides (Fichier existant).	La commande FTP DELETE met EXIST à 0. La commande FTP STORE met EXIST à 1.
LOCKED	BOOL	Le bit LOCKED sert à interdire l'accès au DB fichier. • 0 : L'accès au DB fichier est possible. • 1 : L'accès au DB fichier est bloqué.	Les commandes FTP "STORE"et "RETRIEVE" mettent LOCKED à 1 durant le traitement si le bit était auparavant à 0. Le programme utilisateur de la CPU S7 peut également mettre LOCKED à 1 ou à 0 durant l'accès en écriture à des fins de garantie de cohérence. On obtient ainsi un verrouillage mutuel entre programme utilisateur et traitement FTP pour assurer la cohérence. Marche à suivre recommandée dans le programme utilisateur : 1. Interroger le bit LOCKED (si = 0) 2. Mettre le bit WRITEACCESS à 0 3. Interroger le bit LOCKED (si = 0) 4. Mettre le bit LOCKED à 1 5. Ecrire les données 6. Mettre le bit LOCKED à 0
NEW	BOOL	Le bit NEW indique si le données ont été modifiées depuis la dernière opération de lecture. • 0 : Le contenu du DB fichier est resté inchangé depuis la dernière opération d'écriture. Le programme utilisateur de la CPU S7 a enregistré la dernière modification. • 1 : Le programme utilisateur de la CPU S7 n'a pas encore enregistré la dernière opération d'écriture.	L'instruction FTP "RETRIEVE" met NEW=1 après traitement. Le programme utilisateur sur la CPU S7 doit, après lecture des données, remettre NEW=0 pour autoriser une nouvelle commande "RETRIEVE".

Paramètre	Type	Valeur / Signification	Alimentation
WRITEACCESS	BOOL	• 0 : Le programme utilisateur possède le droit d'écriture pour les DB fichiers de la CPU S7. • 1 : Le programme utilisateur ne possède pas le droit d'écriture pour les DB fichiers de la CPU S7.	Le bit est mis à une valeur d'initialisation lors de la configuration du DB. Recommandation : Si possible, ne modifiez pas ce bit ! Une adaptation à des cas particuliers est possible durant le fonctionnement.
ACT_LENGTH	DINT	Longueur actuelle de la zone de données utiles. Le contenu de ce champ n'est valide que si EXIST = 1.	La longueur actuelle est mise à jour après toute opération d'écriture.
MAX_LENGTH	DINT	Longueur maximale de la zone de données utiles (longueur totale du DB moins 20 octets d'en-tête).	Il convient de définir la longueur maximale lors de la configuration du DB. La valeur peut également être modifiée durant le fonctionnement par le programme utilisateur.
FTP_REPLY_CODE	INT	Nombre non signé (16 bits) qui contient le dernier code Reply de FTP sous forme de valeur binaire. Le contenu de ce champ n'est valide que si EXIST = 1.	Est mis à jour par l'exécuteur du protocole FTP lors du traitement de commandes FTP du serveur.
DATE_TIME	DATE_AND_TIME	Date et heure de la dernière modification du fichier. Le contenu de ce champ n'est valide que si EXIST = 1.	La date/heure actuelle est mise à jour après toute opération d'écriture. Si la fonction "Retransmission de la date/heure" est utilisée, cette entrée correspond à la date/heure retransmise. Si la fonction "Retransmission de la date/heure" n'est pas utilisée, l'entrée est la date/heure relative. La référence est dans ce cas le moment du démarrage du CP (valeur d'initialisation : 01.01.1994 00:00h).

Diagnostic et maintenance

6

6.1 Possibilités de diagnostic

Les possibilités de diagnostic sont les suivantes :

LED du module

Vous trouverez des informations sur les indications fournies par les LED au chapitre LED (Page 21).

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

Si votre station d'ingénierie est connectée au module via Ethernet, vous obtenez des informations sur l'état de connexion de la station d'ingénierie au module.

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

À partir d'une station d'ingénierie, sur laquelle est enregistré le projet STEP 7, vous pouvez à l'aide des fonctions en ligne lire diverses informations de diagnostic du module et exécuter des fonctions de maintenance.

Pour plus de détails sur les fonctions de diagnostic de STEP 7, veuillez vous référer au système d'information STEP 7.

Diagnostic

Vous obtenez ici des informations statiques sur le module sélectionné :

- Général

  Informations générales sur le module
- État de diagnostic

  Informations sur l'état du diagnostic
- Interface Ethernet

  Informations d'adresse et statistiques
- Heure

  Indication de l'heure courante du module et de la source d'horodatage
- Sécurité des données

  Indications d'état et entrées de journal

Fonctions

Vous pouvez exécuter ici les fonctions suivantes :

- Mise à jour du firmware

  Pour la description, voir chapitre Mise à jour du firmware (Page 101).
- Affectation d'une adresse IP
- Attribution d'un nom d'appareil PROFINET
- Enregistrer les données de maintenance

STEP 7 : Connexion en ligne

Le menu contextuel "Etablir la connexion en ligne" permet d'établir une connexion au module.

Pour la marche à suivre, voir chapitre Etablir la connexion en ligne (Page 98).

Serveur Web

Vous pouvez accéder aux pages Web de la CPU à partir d'un PC via HTTP/HTTPS. Celles-ci fournissent diverses informations.

Concernant l'accès et les contenus, voir Guide de la documentation (Page 115).

SNMP

Pour plus de détails sur les fonctions prises en charge, veuillez vous référer au chapitre Diagnostic via SNMP (Page 99).

6.2 Etablir la connexion en ligne

Fonctions en ligne

Le CP propose avec STEP 7 sur la station d'ingénierie (ES) diverses fonctions de diagnostic et de maintenance. Il faut pour cela que l'ES et le CP se trouvent dans le même sous-réseau.

Établissement d'une connexion via Ethernet

Marche à suivre :

1. Connectez l'ES au réseau.
2. Ouvrez le projet STEP 7 voulu sur l'ES.
3. Sélectionnez le CP.
4. Activez les fonctions en ligne avec l'icône "Etablir la connexion en ligne".

5. Sélectionnez l'entrée "PN/IE"dans la zone de liste déroulante "Type d'interface PG/PC" de la boîte de dialogue "Etablir la connexion en ligne".
6. Sélectionnez l'interface de l'ES dans la zone de liste déroulante "Interface PG/PC".

   L'icône  à droite de la zone de liste déroulante permet de contrôler les paramètres de l'interface.
7. Sélectionnez l'interface de la station dans la zone de liste déroulante "Connecter à l'interface/au sous-réseau".
8. Cliquez sur "Lancer la recherche"

   Si une connexion est possible, la station est affichée.
9. Sélectionnez la station dans le tableau des appareils de destination.

   Le chemin via le CP et celui via la CPU sont tous deux possibles.
10. Cliquez sur "Connecter"

Coupure de la connexion en ligne

Coupez la connexion en ligne en fin de session à l'aide du bouton "Déconnexion".

Voir aussi

Fonctions en ligne (Page 69)

6.3 Diagnostic via SNMP

Condition

La condition d'utilisation de SNMP est l'activation de la fonction dans la configuration.

SNMP (Simple Network Management Protocol)

SNMP est un protocole de diagnostic et de gestion de réseau 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).

Pour plus de détails sur SNMP et sur la Siemens Automation MIB, voir le manuel "Diagnostic et configuration avec SNMP" que vous trouverez sur Internet :
Lien : (https://support.industry.siemens.com/cs/ww/fr/ps/15392/man).

Fonctionnalités du CP

Le CP prend en charge les versions suivantes de SNMP :

- SNMPv1
- SNMPv3 (si les fonctions de Security sont activées)

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

MIB prises en charge sous SNMPv1

Le CP prend en charge les MIBs suivantes :

- **MIB II (selon RFC1213)**

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

  – System
  – Interfaces
  – IP
  – ICMP
  – TCP
  – UDP
  – SNMP

- **LLDP MIB**
- **Siemens Automation MIB**

  Tenez compte des droits d'écriture sur les objets MIB, voir chapitre suivant (SNMPv3).

Objets MIB pris en charge sous SNMPv3

Si SNMPv3 est activé, le CP délivre le contenu des objets MIB suivants :

- **MIB II (selon RFC1213)**

  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 (IPv4/IPv6)
  – 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**
- **Siemens Automation MIB**

  Veuillez noter que les accès en écriture ne sont autorisés que pour les objets MIB suivants du groupe "System" :

  – sysContact
  – sysLocation
  – sysName

    Tout sysName activé est transmis comme nom d'hôte au serveur DHCP via l'option DHCP 12 à des fins d'enregistrement auprès d'un serveur DNS.

  Pour tous les autres objets MIB et groupes, seul un accès en lecture est autorisé pour des raisons de sécurité.

Droits d'accès via nom de communauté (SNMPv1)

Le CP utilise les community strings suivants pour gérer les droits d'accès aux agents SNMP :

Tableau 6- 1 Droits d'accès de l'agent SNMP

Mode d'accès	Community String *)
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 généralement connues "public" et "private".

6.4 Mise à jour du firmware

Nouvelles versions de firmware du CP

Dès qu'il existe une nouvelle version de firmware pour le CP, elle est mise à disposition sur le site Internet Siemens Industry Online Support :

Lien : (https://support.industry.siemens.com/cs/ww/fr/ps/25625/dl)

Les fichiers de firmware ont le format de fichier *.upd.

Enregistrez le fichier de firmware sur votre PC.

Pour charger un fichier de firmware sur le CP, vous disposez des moyens suivants :

- Fonctions en ligne de STEP 7 via Ethernet
- Chargement du firmware à partir d'une carte SD sur la CPU

Remarque
Carte SD uniquement pour fichier de firmware

Vous avez besoin d'une carte mémoire SD SIMATIC pour le fichier de firmware, par exemple (numéros d'article) :

- 6AV6671-8XB10-0AX1
- 6AV2181-8XP00-0AX0
- 6AV2181-8AQ10-0AX0

La carte de mise à jour du firmware ne doit pas contenir d'autres données. Vous ne pouvez pas utiliser une carte SD contenant des données de configuration.

Remarque
Durée de la mise à jour du firmware

Le chargement du nouveau fichier de firmware peut durer plusieurs minutes.

Attendez toujours que les LED signalent l'achèvement de la mise à jour (voir ci-dessous).

Chargement du firmware avec les fonctions en ligne de STEP 7 via Ethernet

Conditions :

- La CPU de la station est joignable via Ethernet.
- La station d'ingénierie et la CPU se trouvent dans le même sous-réseau.
- Le nouveau fichier de firmware est enregistré sur la station d'ingénierie.
- La station d'ingénierie est connectée au réseau.
- Le projet STEP 7 voulu est ouvert sur la station d'ingénierie.

Marche à suivre :

1. Sélectionnez la station que vous voulez mettre à jour avec un nouveau firmware.
2. Activez les fonctions en ligne avec l'icône "Connexion en ligne".
3. Dans le dialogue "Connexion en ligne", sélectionnez dans la zone de liste déroulante "Type d'interface PG/PC" l'interface Ethernet.
4. Sélectionnez la CPU de la station.
5. Cliquez sur "Démarrer la recherche" pour rechercher le module sur le réseau et définir le chemin de connexion.

   Lorsque le module est trouvé, il est affiché dans le tableau.

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

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

7. Choisissez la CPU dans la vue de réseau et sélectionnez le menu contextuel "En ligne & diagnostic" (bouton droit de la souris).
8. Sélectionnez dans la navigation de la vue En ligne & diagnostic l'entrée "Fonctions > Mise à jour de firmware".
9. Recherchez avec le bouton "Parcourir" (groupe de paramètres "Chargeur de firmware") le nouveau fichier de firmware dans le système de fichiers de la station d'ingénierie.
10. Démarrez le chargement du firmware avec le bouton "Démarrer la mise à jour" lorsque le champ de sortie "État" affiche la version correcte du firmware signé.

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

Chargement du firmware via la carte SD

Vous trouverez des informations détaillées sur l'utilisation d'une carte SD dans le manuel système du S7-1500, voir Guide de la documentation (Page 115).

Conditions :

- Vous avez copié le nouveau fichier de firmware de votre PC sur la carte SD à l'aide d'un lecteur de cartes approprié.
- En option : Vous avez réalisé un fichier de sauvegarde du fichier de firmware utilisé actuellement.

Marche à suivre :

1. Basculez le sélecteur de mode CPU sur ARRÊT.

   Veuillez vous assurer qu'à l'état ARRÊT aucune fonction d'écriture (fonctions en ligne ou de test) n'est activée.

2. Retirez la SIMATIC Memory Card contenant les données de configuration de son logement sur la CPU.
3. Enfichez la carte SD avec le fichier de firmware dans le logement de carte de la CPU.

   La mise à jour du firmware démarre peu de temps après l'enfichage de la carte. Le visuel affiche : "STOP - FW UPDATE"

   Si des erreurs surviennent, les messages correspondants s'affichent.

   Lorsque la mise à jour de firmware est achevée, le visuel affiche une page de résultats.

   Le succès de la mise à jour est signalé par le schéma de signalisation suivant des LED de la CPU :

   – RUN allumée en jaune

   – MAINT clignote en jaune

4. Retirez la carte SD et enfichez à nouveau la SIMATIC Memory Card.
5. Basculez le sélecteur de mode CPU sur MARCHE.

   La CPU utilise au démarrage le nouveau firmware.

Concernant le schéma de signalisation des LED du CP durant le redémarrage, voir chapitre LED (Page 21).

6.5 Echange de module sans PG

Données de configuration lors d'un échange de module

Les données de configuration du CP sont gérées sur la CPU. L'échange de ce module par un module du même type (référence identique) peut par conséquent s'effectuer sans PG.

Remarque

Recopie de l'adresse MAC configurée

Veuillez noter,qu' en cas de sélection du protocole ISO, l'adresse MAC préalablement définie dans la configuration est transférée de la CPU sur le module CP.

Echange de module en cas d'attribution d'adresse par DHCP (IPv4)

L'une des options de la configuration IP du CP est l'attribution de l'adresse IP par un serveur DHCP.

Remarque

Recommandation : Configuration de l'ID de client

Notez, lors de l'échange de modules, que l'adresse MAC par défaut du nouveau module est différente de celle du module précédent.

Si l'adresse MAC par défaut du nouveau module est transmise au serveur DHCP, ce dernier retournera une adresse IP différente ou pas d'adresse IP du tout.

Lors de la définition de la configuration IP, procédez donc de préférence comme suit :

- Spécifiez toujours un ID client et configurez votre serveur DHCP en conséquence. Ceci permet de s'assurer, qu'après un échange de module, le CP obtient toujours du serveur DHCP la même adresse IP.

Si vous avez configuré une nouvelle adresse MAC au lieu d'utiliser l'adresse MAC par défaut, le CP transmet toujours au serveur DHCP l'adresse MAC configurée. Le CP obtient dans ce cas la même adresse IP que le module précédent.

Caractéristiques techniques 7

7.1 Caractéristiques techniques

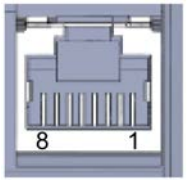
Caractéristiques techniques - CP 1545-1		
Numéro d'article :	6GK7545-1GX00-0XE0	
Connexion au réseau Industrial Ethernet		
Nombre	1 interface Gigabit (X1 P1)	
Exécution	connecteur femelle RJ45, séparation galvanique	
Propriétés		
• Norme	• 1000BASE-T, IEEE 802.3ab	
• Vitesses de transmission	• 10 / 100 / 1000 Mbit/s	
• Autres caractéristiques	• semi-duplex/duplex intégral, autocroisement, autonégociation	
Alimentation		
Exécution	Via bus interne S7-1500 (15 V)	
Autres caractéristiques techniques		
Consommation typique)	300 mA via bus interne S7-1500	
Puissance dissipée (typique)	4,5 W	
Isolation	contrôlée sous :	DC 780 V (type test)
Catégorie de surtension selon CEI / EN 60664-1	Catégorie II	
Conditions ambiantes admissibles		
Température ambiante	Pendant l'exploitation, le châssis étant monté horizontalement	0 °C ... +60 °C
	Pendant l'exploitation, le châssis étant monté verticalement	0 °C ... +40 °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
Contamination atmosphérique admissible	Contrôle de gaz toxique selon ISA-S71.04 severity level G1, G2, G3	
	• SO_2	• < 0,5 ppm
	• H_2S	• < 0,1 ppm
Forme, dimensions et poids		
Format du module	module compact S7-1500, simple largeur	
Degré de protection	IP20	
Poids	320 g	
Dimensions (L x H x P)	35 x 147 x 129 mm	
Type de fixation	Montage sur profilé support S7-1500	

Pour plus de caractéristiques, voir chapitre Application et fonctions (Page 11) de même que dans le manuel système S7-1500, voir Guide de la documentation (Page 115).

7.2 Brochage de l'interface Ethernet

Brochage des interfaces Ethernet Gigabit

Le tableau suivant indique le brochage de l'interface X1.

Vue du connecteur femelle RJ45	Broche	Nom de signal	Brochage
	1	D1+	D1+ bidirectionnelle
	2	D1-	D1- bidirectionnelle
	3	D2+	D2+ bidirectionnelle
	4	D3+	D3+ bidirectionnelle
	5	D3-	D3- bidirectionnelle
	6	D2-	D2- bidirectionnelle
	7	D4+	D4+ bidirectionnelle
	8	D4-	D4- bidirectionnelle

7.3 Longueurs de câble admissibles - (Ethernet)

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

Voir Siemens Mall : (https://mall.industry.siemens.com)

7.4 Longueurs de câble admissibles - Ethernet Gigabit

Longueurs de câble admissibles - Ethernet Gigabit	Combinaisons alternatives
0 ... 60 m	• Max. 60 m IE FC TP Flexible Cable GP 4x2 + 10 m TP Cord RJ45/RJ45 4x2 via IE FC RJ45 Modular Outlet Insert 1GE
0 ... 100 m	• max. 90 m IE FC TP Standard Cable GP 4x2 + 10 m TP Cord RJ45/RJ45 4x2 via IE FC RJ45 Modular Outlet Insert 1GE

Voir Siemens Mall : (https://mall.industry.siemens.com)

Homologations

8

Homologations accordées

Remarque

Homologations accordées sur la plaque signalétique de l'appareil

Les homologations mentionnées - à l'exception des certificats pour la construction navale - 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. Les homologations pour la construction navales constituent une exception.

Certificats pour la construction navale et homologations nationales

Les certificats établis pour les appareils destinés à la construction navale et les homologations nationales spécifiques sur le site Internet du Siemens Industry Online Support :
Link: (https://support.industry.siemens.com/cs/ww/fr/ps/15340/cert)

Déclaration de conformité de l'UE

Le produit 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.

- **2014/30/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 CE est fournie à toutes les autorités compétentes par :

Siemens Aktiengesellschaft
Digital Industries
BP 48 48
90026 Nuernberg
Deutschland

Vous trouverez également la déclaration de conformité UE sur Internet à l'adresse suivante :
Link: (https://support.industry.siemens.com/cs/ww/fr/ps/25625/cert)

Les versions de norme en vigueur sont indiquées dans la déclaration de conformité UE et les certificats.

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/25625/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 26).

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'

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 26).

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)

CEM

Le produit satisfait jusqu'au 19/04/2016 aux exigences de la directive 2014/30/UE "Compatibilité électromagnétique" (directive CEM).

Normes appliquées :

- EN 61000-6-4

  Compatibilité électromagnétique (CEM) - Partie 6-4 : normes générique - Norme sur l'émission pour les environnements industriels
- EN 61000-6-2

  Compatibilité électromagnétique (CEM) - Partie 6-2 : normes générique - Immunité pour les environnements industriels

RoHS

Le produit est conforme aux exigences de la directive 2011/65/UE relative à la limitation de l'utilisation de certaines substances dangereuses dans les équipements électriques et électroniques.

Norme appliquée :

- EN 50581

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)

Report / UL file: E 85972 (NRAG, NRAG7)

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 T3...T6
- Cl. 1, Zone 2, GP. IIC T3...T6

Ta : Voir classe de température sur la plaque signalétique du CP

Report / UL file: E223122 (NRAG, NRAG7)

Conformez-vous 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 UL HazLoc et FM (Page 27).

Remarque

For devices with C-PLUG memory: The C-PLUG memory module may only be inserted or removed when the power is off.

FM



Factory Mutual Approval Standards:

- Class 3600
- Class 3611
- Class 3810
- ANSI/ISA 61010-1

Report Number 3049847

Class I, Division 2, Group A, B, C, D, T4

Class I, Zone 2, Group IIC, T4

Pour les classes de température, consultez la plaque signalétique du module.

Australie - RCM



Le produit remplit les exigences des normes selon AS/NZS 2064 (classe A).

MSIP 요구사항 - For Korea only



A급 기기(업무용 방송통신기자재)

이 기기는 업무용(A급) 전자파 적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정 외의 지역에서 사용하는것을 목적으로 합니다.

Veuillez noter que cet appareil est conforme, en matière de perturbations radioélectriques, à la classe de valeurs limites A. Cet appareil est utilisables dans tous les secteurs, excepté dans l'environnement résidentiel

Marquage pour l'Union douanière eurasienne



EAC (Eurasian Conformity)

Communauté économique eurasiatique de Russie, Biélorussie, Arménie, Kazakhstan et Kirghisistan

Déclaration de conformité aux règles techniques de l'union douanière (TR ZU)

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/25625/cert)

Dessins cotés

9

Toutes les dimensions des dessins cotés sont indiquées en millimètres.

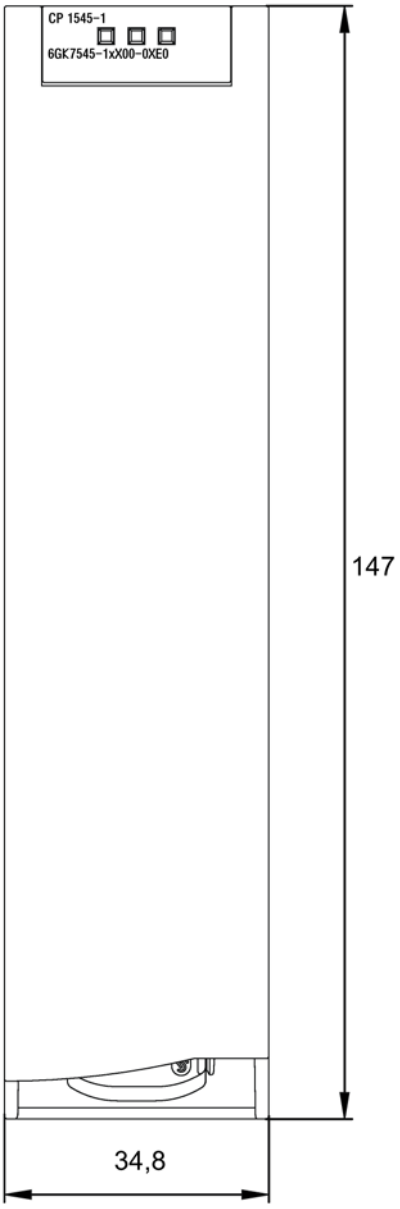


Figure 9-1 Vue de face

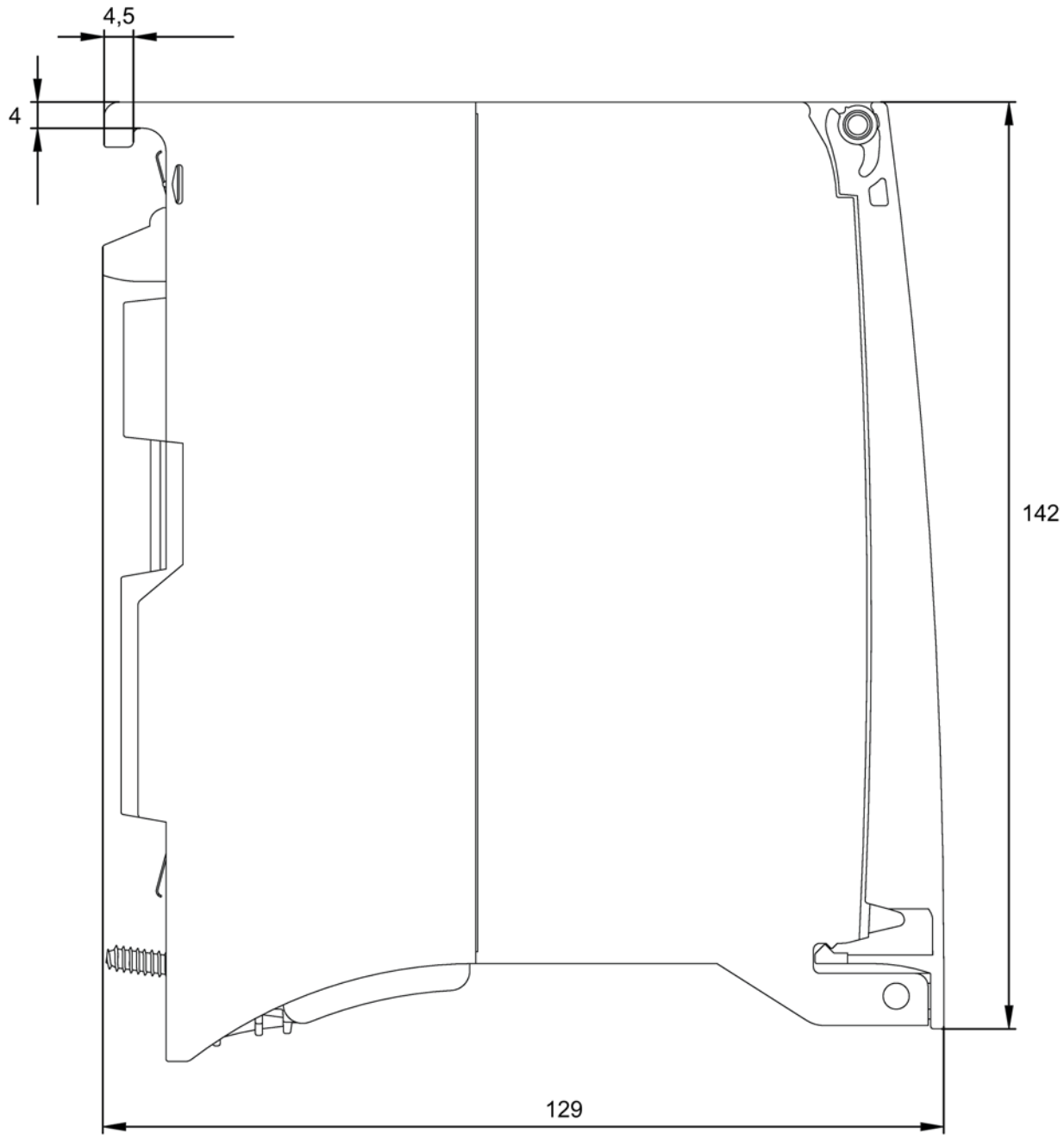


Figure 9-2 Vue de côté

Guide de la documentation

A

Documentation du S7-1500

La documentation des produits SIMATIC est de conception modulaire et traite des sujets touchant à votre système d'automatisation.

La documentation complète relative au système S7-1500 est constituée du manuel système, des descriptions fonctionnelles et des manuels ou instructions de service.

En outre, le système d'information de STEP 7 (aide en ligne) vous aidera à configurer et à programmer votre système d'automatisation.

Le tableau suivant indique les autres documents complétant le présent manuel du CP et disponibles sur Internet.

Tableau A- 1 Récapitulatif de la documentation du S7-1500

Sujet	Documentation	Principaux thèmes
Description du système	Manuel système Système d'automatisation S7-1500 (https://support.industry.siemens.com/cs/ww/fr/view/59191792)	• Planification de l'utilisation • Montage • Raccordement • Mise en service
Diagnostic système	Description fonctionnelle Diagnostic système (https://support.industry.siemens.com/cs/ww/fr/view/59192926)	• Présentation • Analyse du diagnostic matériel/logiciel
Communication	Description fonctionnelle Communication (https://support.industry.siemens.com/cs/ww/fr/view/59192925)	• Présentation
	Description fonctionnelle Serveur Internet (https://support.industry.siemens.com/cs/ww/fr/view/59193560)	• Fonction • Utilisation
	SIMATIC NET - Industrial Ethernet / PROFINET - • Industrial Ethernet Link: (https://support.industry.siemens.com/cs/ww/de/view/27069465) • Composants de réseau passifs Link: (https://support.industry.siemens.com/cs/ww/en/view/84922825)	• Réseaux Ethernet • Configuration de réseaux • Composants de réseau

Sujet	Documentation	Principaux thèmes
Montage immune aux perturbations des automates	Description fonctionnelle Montage immune aux perturbations des automates (https://support.industry.siemens.com/cs/ww/fr/view/59193566)	• Notions fondamentales • Compatibilité électromagnétique • Protection contre la foudre • Choix du boîtier
Temps de cycle et de réaction	Description fonctionnelle Temps de cycle et de réaction (https://support.industry.siemens.com/cs/ww/fr/view/59193558)	• Notions fondamentales • Calculs

Messages Syslog

B

Le produit émet des messages Syslog conformément à RFC 5424. La structure des messages repose sur la norme CEI 62443-3-3.

Vous trouverez une description détaillée des messages ci-après.

B.1 Structure des messages Syslog.

Les messages Syslog journalisent les changements d'état d'appareils sous forme d'information d'état. Les messages Syslog selon RFC 5424 ou 5426 sont émis par des appareils et transmis à un serveur via le port UDP (par défaut : 514). Le serveur Syslog collecte les informations des appareils et renseigne sur les évènements.

Le protocole Syslog prescrit un ordre et une structure définis des paramètres possibles. Les messages Syslog selon RFC5424 possèdent la structure suivante :

Partie / Paramètre	Signification
HEADER	
PRI	Priorité du message Syslog, répartie en : • Severity (gravité) Valeurs possibles : – 0 Emergency – 1 Alert – 2 Critical – 3 Error – 4 Warning – 5 Notice – 6 Information – 7 Debug • Facility (origine) Valeurs possibles, par ex. : sous-système, service, utilisateur
VERSION	Numéro de version de la spécification Syslog
TIMESTAMP	Horodatage de l'appareil en date/heure locale, y compris le fuseau horaire et éventuellement la correction requise pour l'heure d'été/hiver. Format : YYYY-MM-DDThh:mm:ss.msmsmsms+xx:yy Exemple : 2010-01-01T02:03:15.0003+02:00

Partie / Paramètre	Signification
HOSTNAME	nom d'hôte identifiant l'appareil source ou bien : • FQDN • Adresse·IPv4 selon RFC 1035 : Octets en notation décimales : XXX.XXX.XXX.XXX • Adresse·IPv6 selon RFC4291 Section 2.2 • Nom d'hôte Les indications manquantes sont remplacées par "-". Sur le produit : Le nom d'hôte configuré ou l'adresse IPv4 configurée
APP-NAME	Appareil ou application dont est issu le message. Les indications manquantes sont remplacées par "-". Sur le produit : "-"
PROCID	L'ID de process sert par ex. à identifier clairement les divers processus lors d'analyses et de la localisation de pannes. Les indications manquantes sont remplacées par "-". Sur le produit : "-"
MSGID	ID d'identification du message. Les indications manquantes sont remplacées par "-". Sur le produit : "-"
STRUCTURED-DATA	
timeQuality	L'élément de données structuré "timeQuality" renseigne sur la date/heure système avec les deux paramètres "tzKnown" et "isSynced". Exemple : [timeQuality tzKnown="0" isSynced="0"] • tzKnown Le paramètre indique si le fuseau horaire est connu ou non sur l'appareil source. – 1 = connu – 0 = inconnu • isSynced Le paramètre indique si l'appareil source est synchronisé ou non à une horloge fiable, via NTP par ex. – 1 = synchronisé – 0 = non synchronisé
MSG	
MESSAGE	Texte du message sous forme de chaine de caractères ASCII (anglais)

Pour plus d'informations sur la structure des messages Syslog et sur la signification des paramètres, voir les RFC :

https://tools.ietf.org/html/rfc5424

https://tools.ietf.org/html/rfc5426

B.2 Variables dans les messages Syslog

Les variables sont représentées au chapitre "Messages Syslog", dans le champ "Texte du message" entre accolades {variable}.

Les messages émis peuvent contenir les variables suivantes :

Variable	Description	Format	Valeurs possibles ou exemple
{IP address}	Adresse·IPv4 selon RFC1035 Adresse·IPv6 selon RFC4291 Section 2.2	%d.%d.%d.%d XXX.XXX.XXX.XXX	192.168.1.105 2001:DB8::8:800:200C:417A
{FQHN}	Fully Qualified Host Name: Nom d'hôte entier indiqué ; indication sous forme de domaine (FQDN) ou d'adresse IP.	FQDN : host1.com IPv4 : %d.%d.%d.%d	serveur1 192.168.1.105
{Src port} {Dest port}	Numéro de port (décimal)	%d	0 ... 65535
{Src mac} {Dest mac}	Adresse MAC source/de destination	%02x:%02x:%02x;%02x:%02x:%02x	00:0C:29:2F:09:B3
{Protocol}	Protocole de couche 4 utilisé ou service qui a généré l'évènement.	%s	UDP | TCP | WBM | Telnet | SSH | Console | PNIO | PB | OPC | TFTP | SFTP
{Group}	Nom d'identification du groupe (chaîne de caractères sans espace)	%s	Service informatique
{User name}	Chaine de caractères (sans espaces) qui identifie l'utilisateur authentifié par son nom.	%s	<Nom>
{Local interface}	Nom symbolique de l'interface locale	%s	Console
{Action user name} ou {Destination user name}	Identifie l'utilisateur de destination par son nom. Il ne s'agit pas de l'utilisateur authentifié	%s	<Prénom>.<Nom>
{Role}	Nom symbolique du rôle	%s	Administrateur
{Time minute} {Timeout}	Nombre de minutes	%d	44
{Time second}	Nombre de secondes	%d	44
{Failed login count}	Nombre d'échecs de connexion	%d	10
{Max sessions}	Nombre maximal de sessions	%d	10
{Trigger pin}	Chaine de caractères (sans espaces) pour un PIN d'E/S qui déclenche l'évènement	%s	DI1
{Firewall rule}	Chaine de caractères (avec espaces) pour un jeu de règles de pare-feu	%s	Rule1
{Subject}	Chaine de caractères (avec espaces) pour l'objet du certificat. Est utilisée comme élément de l'authentification par certificat qui doit également contenir des caractères Unicode.	%s pour code UTF8 : %S	Objet
{Config detail}	Chaine de caractères (avec espaces) pour l'identification d'une partie de la configuration	%s	OpenVPN
{Connection name}	Nom d'une connexion VPN		Connexion_1

Variable	Description	Format	Valeurs possibles ou exemple
{Firewall accept}	Action de pare-feu exécutée (paquet accepté)		ACCEPT
{Firewall action reject}	Action de pare-feu exécutée (paquet rejeté)		REJECT DROP
{Length}	Longueur du paquet de réseau (en octets)	%d	52
{Network interface}	Nom symbolique d'une interface de réseau	%s	vlan 1

B.3 Messages

Le produit émet les messages SYSLOG suivants, triés par classes.

B.3.1 Non-repudiation

B.3.1.1 15.1_SE_CONFIG_CHANGE_(protocol)_(configuration)

Texte du message	{Protocol}: User {User name} has changed configuration.
Exemple	Console: User admin has changed configuration.
Signification	L'utilisateur a modifié les données de configuration en chargeant de nouvelles données de configuration.
Severity	Info
Facility	local0
Norme	CEI 62443-3-3 Reference: SR 2.12

Index

A

Abréviations, 4
Adresse IP
    via DHCP, 39
Adresse IP - Modification programmée, 79
Adresse IPv6
    Utilisation, 14
Adresse MAC, 14

B

Blocs de programme - max. Longueur de données, 18

C

CEM - Compatibilité électromagnétique, 107
Client FTP
    Capacités fonctionnelles, 19
Communication IHM, 12
Communication PG, 12
Communication S7, 12
Configuration IP
    IPv4 / IPv6, 14
Connexion de communication programmée, 41
Connexion e-mail, 18
Connexions de PG
    Nombre, 17
Connexions FETCH/WRITE, 18
Connexions ISO-on-TCP, 18
Connexions OP
    Nombre, 17
Connexions pour web
    Nombre, 17
Connexions programmées
    Nombre, 17
Connexions S7
    Nombre utilisable sans restrictions, 17
Connexions TCP, 18
Connexions transport ISO, 18
Connexions UDP, 18
Consignes de sécurité, 25

D

Déconnexion, 64
Désignation du produit, 4
DHCP, 104
Diagnostic de sécurité des données, 69
Diagnostic en ligne, 97
Double adressage sur le réseau, 40

E

Élimination, 5
E-mail, 11
État de fonctionnement de la CPU, 33

F

FETCH/WRITE, 12, 39
    Mode d'adressage S5/S7, 15
Fonctions en ligne, 98
Formation, 6
FTP, 39
    Comportement en l'absence de référence au bloc de tâche FTP, 89
FTP (client FTP), 16
FTP_CMD, 80
    Temps d'exécution du bloc, 19
FTPS, 16
FTPS - Security, 45

G

Gestion des données - Données de configuration, 104
Glossaire, 6
Glossaire SIMATIC NET, 6

I

Instruction
    FTP_CMD, 79
    T_CONFIG, 79
    TCON, TSEND/TRCV, 78
    TDISCON, 78
    TMAIL_C, 78

TSEND_C/TRCV_C, 78
TUSEND/TURCV, 78
Instructions (OUC), 75
Interface Ethernet, 23
Configuration via T_CONFIG, 79
ISO-on-TCP (RFC 1006), 11
ISO-Transport (RFC 8073), 11

J

Journalisation, 16

L

Liaisons S7, 16
Liaisons TCP pour FTP, 19
Logiciel
Version, 3

M

MIB, 99
Mise en tampon de données, 66
Mise en tampon de télégrammes UDP, 19
Multicast (UDP), 11

N

Notes particulières
Recommandation pour le réglage de la date/heure, 41
S'assurer d'une date/heure valide, 42
NTP, 14
NTP (secure), 16, 42
Numéros d'article, 3

O

Open User Communication (OUC), 11
OUC (Open User Communication), 75

P

Pare-feu, 16
Pièce de rechange, 20
Port 8448, 69
PUT/GET, 39

Q

QoS, 66
QualityCode, 64

R

Recyclage, 5
Références croisées (PDF), 4
Ressources de liaison de la CPU, 17
Routage IP, 40
RUN → STOP, 33

S

Serveur de journalisation, 73
Serveur DNS - Modification programmée, 79
Serveur FTP
Capacités fonctionnelles, 19
Serveur NTP, 42
Serveur NTP - Modification programmée, 79
Serveur web, 15
Service & Support, 6
SMTPS, 16
SNMP, 45, 99
SNMPv3, 16
Spécification Gigabit, 23
Synchronisation d'horloge, 14

T

TCP (RFC 793), 11
Transmission de données (cloud), 57
Types de donnée système
FTP_..., 79
TCON_..., 78
TMail_..., 78

U

UDP
Restrictions, 19
UDP (RFC 768), 11

V

Version de STEP 7 -, 20
Version du matériel, 3