DOC023.91.90143

Transmetteur sc1000 Communications avancées

MANUEL

12/2018, Edition 3

Table des matières

Chapitre 1 Caractéristiques techniques

Les caractéristiques techniques peuvent être modifiées sans préavis.

Module d'affichage du contrôleur sc1000	
Modem *GSM/*GPRS	Le module d'affichage sc1000 avec modem GSM/GPRS intégré transfère les données, les SMS et les services GPRS aux réseaux GSM. Le contrôleur SC1000 supports les bandes de fréquence GSM: 850 / 900 / 1800 / 1900 MHz
	Supporte le GPRS multislot classe 10 et les schémas de codage GPRS: CS-1, CS-2, CS-3 et CS-4.
Serveur Modbus TCP	Le serveur Modbus TCP atteste une "conformité classe 0" avec la prise en charge des codes de fonction suivantes : Read Multiple Registers (CF 03) Write Multiple Registers (CF 16) D'autres codes de fonction sont également pris en charge, notamment : Read/Write Multiple Registers (CF 23) Read Device Information (CF 43/14)
Port Ethernet	Ethernet RJ45, 10 Mo/s
Garantie	
Garantie	1 an

* **Etats-Unis**

Le transmetteur contenu dans ce produit est un dispositif "Quad-mode" pouvant fonctionner dans les bandes de fréquence 850 / 900 / 1800 / 1900 MHz. L'usage de cet appareil en tant que GSM à 900 / 1800 MHz n'est pas autorisé aux États-Unis et au Canada.
L'usage de ce transmetteur est autorisé dans des emplacements fixes ou mobiles.
Les antennes employées doivent être placées à une distance minimum de 20 cm (7,9 po) de toute personne et strictement loin de toute autre antenne de transmission.
L'utilisateur n'est pas autorisé à utiliser une antenne autre que celle fournie par le fabricant ni excédant une puissance de 2,89 dbi pour le GSM 1900 et de 1,33 dbi pour le GSM 850 Mhz.

ID FCC :	QIPMC55i
IC # :	7830A-MC55i
CE via Organisme notifié no. :	CE 0681

* **EUROPE**

ATTENTION

- Ne pas faire fonctionner l'appareil dans les hôpitaux et/ou près d'instruments médicaux tels que les stimulateurs cardiaques ou les prothèses auditives.
- Ne pas utiliser l'appareil dans des lieux dangereux.
- Ne pas faire fonctionner l'appareil en présence de gaz combustibles, de vapeurs ou de poussière.
- Ne pas faire fonctionner l'appareil à proximité de zones ayant un niveau de combustibilité élevé tels que les stations d'essence, les dépôts de carburant, les usines chimiques et les travaux de minage.
- L'appareil peut provoquer des perturbations à proximité des téléviseurs, de radios ou d'ordinateurs.
- Ne pas soumettre l'appareil à des vibrations ou à de forts impacts.
- L'utilisation des services GSM (messages SMS, communication de données, GPRS, etc.) est susceptible d'engager des coûts additionnels chez un fournisseur de services. L'utilisateur est entièrement responsable de tous les dommages et des coûts encourus.
- Ne pas utiliser ou installer cet équipement autrement qu'indiqué dans le présent manuel. Une utilisation inappropriée annulera la garantie.
- Toute modification de l'équipement est inacceptable et entraîne la perte de l'autorisation de fonctionnement
- Outre les mesures de sécurité, respecter toutes les réglementations en vigueur dans le pays d'exploitation de l'équipement.

Chapitre 2 Généralités

2.1 Consignes de sécurité

Veuillez lire entièrement le présent manuel avant d'installer le logiciel. Des informations supplémentaires concernant le transmetteur sc1000 sont données dans le manuel relatif au transmetteur sc1000.

2.2 Présentation du produit

Remarque

La sécurité du réseau et du point d'accès relève de la responsabilité du client utilisant l'appareil sans fil. Le fabricant ne peut être tenu pour responsable des dommages, y compris mais sans s'y limiter, indirects, particuliers, fortuits ou accessoires occasionnés en raison d'une brèche dans la sécurité du réseau ou d'une violation de la sécurité du réseau.

Le transmetteur sc1000 est conçu pour gérer les communications avec d'autres utilisateurs via Internet. Il est doté d'un port Ethernet (connexion câblée) et d'un modem GSM//GPRS (connexion radio) faisant fonction d'interface.

La connexion câblée via le port Ethernet (port de service) est établie à l'aide d'un câble LAN. Au besoin, en cas d'installation à l'extérieur, il est possible d'utiliser le kit pour port Ethernet extérieur sc1000 (en option) afin d'offrir plus de protection au port même. Les transmetteurs sc1000 sont souvent installés dans des zones mal adaptées pour les connexions réseau/Internet câblées. Les réseaux de communication mobile constituent, dans ce cas, un bon moyen de collecter les données et de commander à distance le sc1000. Cette solution "M2M" (M2M = machine-to-machine) permet d'intégrer le transmetteur sc1000 dans un réseau informatique local via un réseau de communications mobiles GPRS.

Un tunnel VPN assurera la sécurité des communications entre le sc1000 et le réseau informatique.

Après avoir établi la connexion LAN ou GPRS, aucune autre opération n'est requise sur le transmetteur sc1000.

La configuration se fait via un navigateur web sur ordinateur. Il est également possible de télécharger des journaux de données ou des mises à jour de logiciels par le même moyen.

Le module logiciel Modbus TCP (en option) active le transmetteur sc1000 de manière à s'intégrer directement dans les systèmes PLC (PLC = programmable logic controller, automate programmable). Les systèmes PLC enregistrent les données mesurées par le sc1000 pour les traiter ultérieurement.

Remarque : *Les logiciels non fournis par le fabricant ne sont pas pris en charge. Pour plus d'informations, contactez le fournisseur.*

Chapitre 3 Installation

3.1 Spécifications relatives à l'utilisateur

Seul un personnel spécialisé et opportunément formé est autorisé à installer et faire fonctionner l'ordinateur et le transmetteur sc1000. Les utilisateurs doivent être familiarisés avec la technologie réseau et des ordinateurs.

3.2 Spécifications générales liées à la maintenance à distance

Toute condition spécifiée doit être remplie afin de pouvoir effectuer la maintenance à distance du sc1000 ou d'accéder via navigateur au transmetteur, autrement le système risque de subir des dommages.

3.2.1 Spécifications relatives au transmetteur sc1000

Toutes les informations et les instructions relatives à la sécurité indiquées dans le manuel du transmetteur sc1000 doivent être respectées.

Spécifications supplémentaires :

Attribution du mot de passe au navigateur
Il est nécessaire d'attribuer un mot de passe au navigateur avant de configurer la connexion Ethernet//GPRS afin d'assurer que l'accès au transmetteur via navigateur est possible.

CONFIG. SYSTÈME
ACCÈS NAVIGATEUR
MOT DE PASSE

1. Sélectionnez **CONFIG. SYSTÈME>ACCÈS NAVIGATEUR>MOT DE PASSE** dans le menu principal du transmetteur.
2. Attribuez un mot de passe au navigateur.

Evaluation de la disponibilité du GPRS sur le lieu
Le GPRS doit être disponible sur le lieu d'installation du transmetteur sc1000 pour que celui-ci soit accessible via GPRS.

Remarque : *La disponibilité du GPRS doit être assurée à l'emplacement du transmetteur.*

Installation du logiciel Modbus TCP
En cas de recours l'assistance Modbus TCP, le logiciel doit posséder une licence et un code d'activation.

3. Pour activer une licence d'essai ou permanente, saisissez **CONFIG. SYSTÈME>GESTION LICENCES**.

3.2.2 Spécifications relatives à l'ordinateur

L'ordinateur à connecter au transmetteur sc1000 doit être en mesure d'établir une connexion Internet pratique.

Les spécifications suivantes doivent être respectées :

- Les droits d'administration doivent être attribués au compte utilisateur possédant l'accès à l'ordinateur
- Un navigateur web doit être installé
- Une connexion Internet doit être disponible.

3.2.3 Contenu de la livraison

La livraison inclut les composants suivants :

- Logiciel client VPN personnalisé pour le transmetteur sc1000
- Manuel

Remarque : *Contactez immédiatement le fabricant ou le représentant responsable si l'un des composants susmentionnés est défectueux ou absent.*

3.3 Aperçu général des possibilités de connexion

Plusieurs types de connexion sont possibles entre le transmetteur sc1000 et un ordinateur. Des exemples de types de connexions mentionnées ci-dessous sont illustrés dans les Figure 1 et Figure 2 :

- Connexion Ethernet
- Connexion GPRS

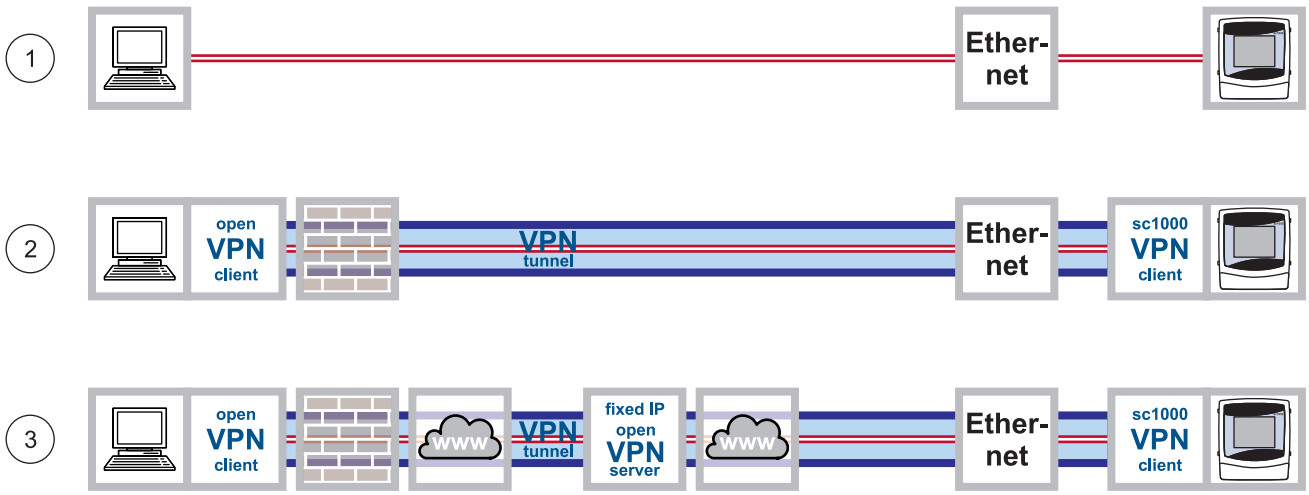

Figure 1 Aperçu des connexions Ethernet alternatives

1	Connexion Ethernet de base
2	Connexion Ethernet avec tunnel VPN sécurisé
3	Connexion Ethernet via serveur VPN-IP fixe

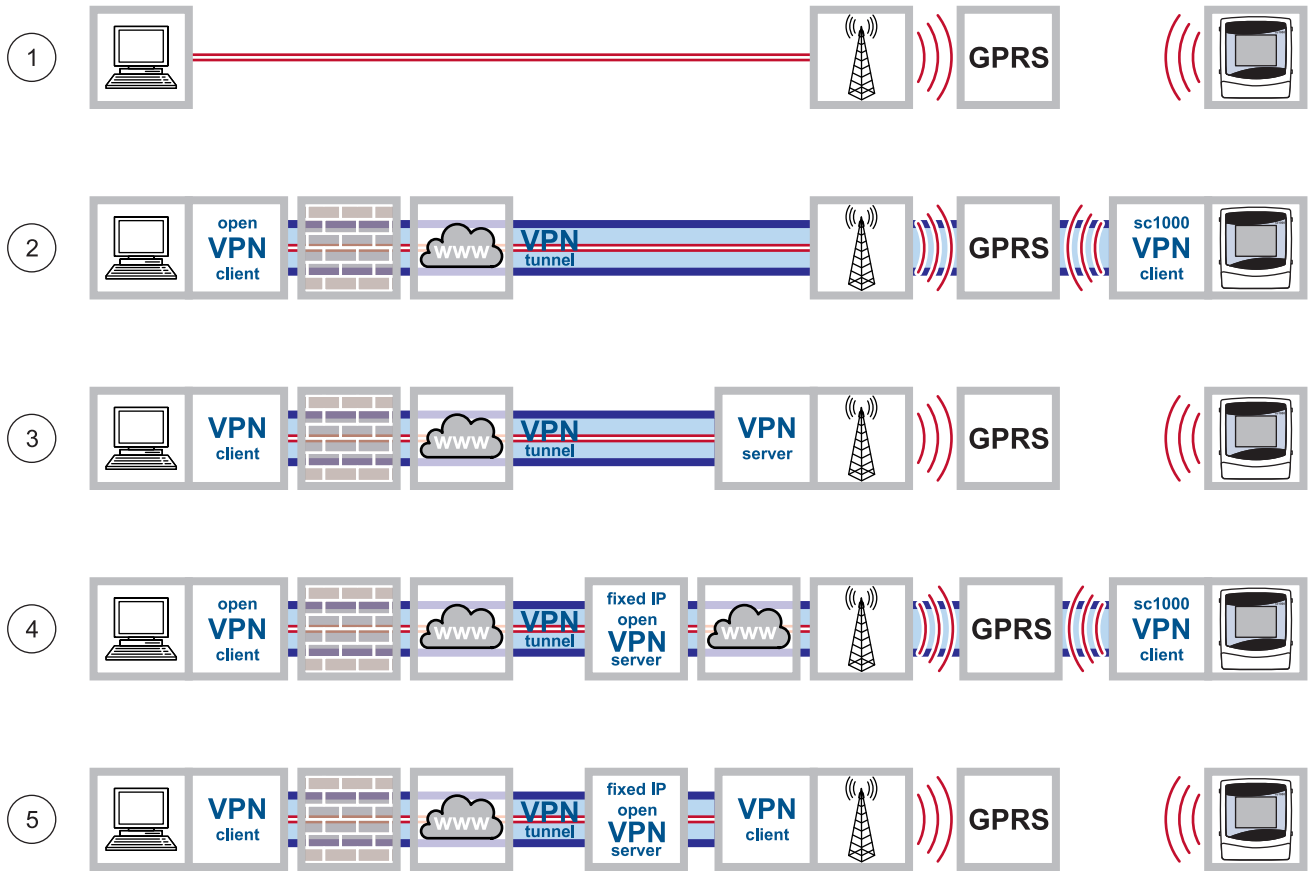

Figure 2 Aperçu des connexions GPRS alternatives

1	Connexion GPRS sans tunnel VPN (possible uniquement si un compte CDA (Corporate Data Access) est configuré avec l'opérateur du réseau mobile)
2	Connexion GPRS avec tunnel VPN sécurisé
3	Connexion GPRS via serveur VPN de l'opérateur du réseau mobile
4	Connexion GPRS via serveur VPN-IP fixe
5	Connexion GPRS via service IP fixe et serveur VPN de l'opérateur du réseau mobile

3.4 Établissement d'une connexion Ethernet

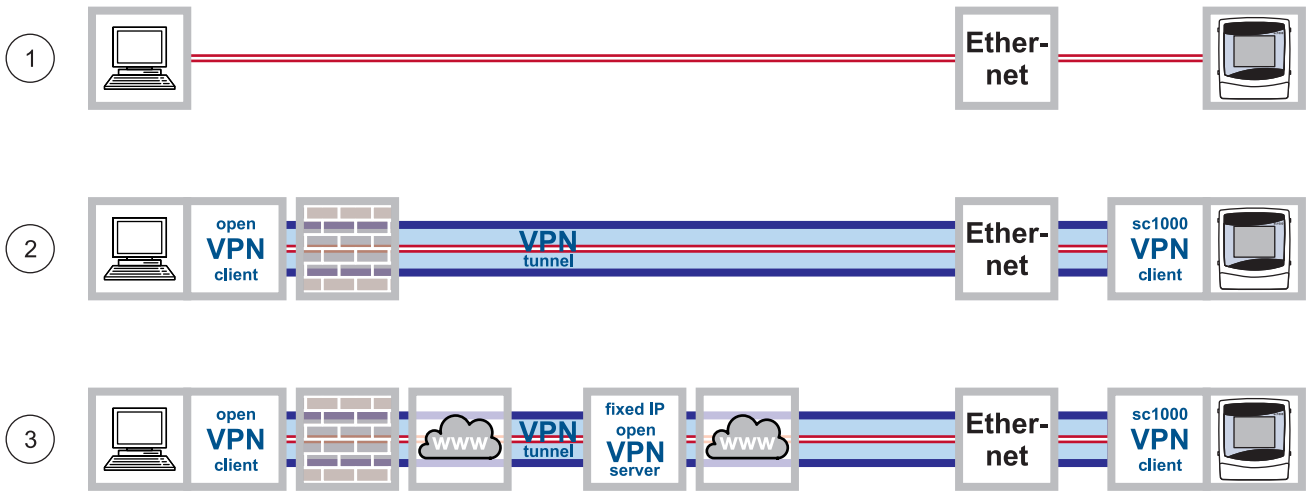

Figure 3 Connexions Ethernet

1	Connexion Ethernet de base
2	Connexion Ethernet avec tunnel VPN sécurisé
3	Connexion Ethernet avec serveur VPN-IP fixe

La connexion Ethernet est la connexion câblée entre un ordinateur et le port Ethernet du transmetteur sc1000. Ce port Ethernet, situé sur le module d'affichage, constitue une connexion Ethernet 10 à Mo/s.

Une connexion directe entre l'ordinateur et le transmetteur sc1000 se réalise comme suit :

Via connexion Ethernet de base
(Figure 3, point 1)

Portée de l'application : le transmetteur sc1000 est placé au sein d'un réseau d'entreprise ou est utilisé à des fins de test.

Via connexion Ethernet avec tunnel VPN sécurisé
(Figure 3, point 2)

Portée de l'application : le transmetteur sc1000 se situe hors du réseau d'entreprise.

Via connexion Ethernet avec serveur VPN-IP fixe
(Figure 3, point 3)

Portée de l'application : le transmetteur sc1000 est accessible de partout via Internet à l'aide d'une adresse IP fixe.

3.4.1 Établissement d'une connexion Ethernet de base

Figure 4 Connexion Ethernet de base

Si le transmetteur sc1000 est placé au sein d'un réseau d'entreprise ou est utilisé à des fins de test, une connexion Ethernet sans VPN entre l'ordinateur et le transmetteur est recommandable (Figure 4).

1. Connectez l'ordinateur au réseau d'entreprise à l'aide d'un câble Ethernet. Assurez-vous que la connexion Internet fonctionne parfaitement. Ouvrez plusieurs pages sur Internet afin de tester la connexion.
2. Connectez le transmetteur sc1000 au réseau en raccordant le câble Ethernet au port Ethernet RJ45 (Figure 5).

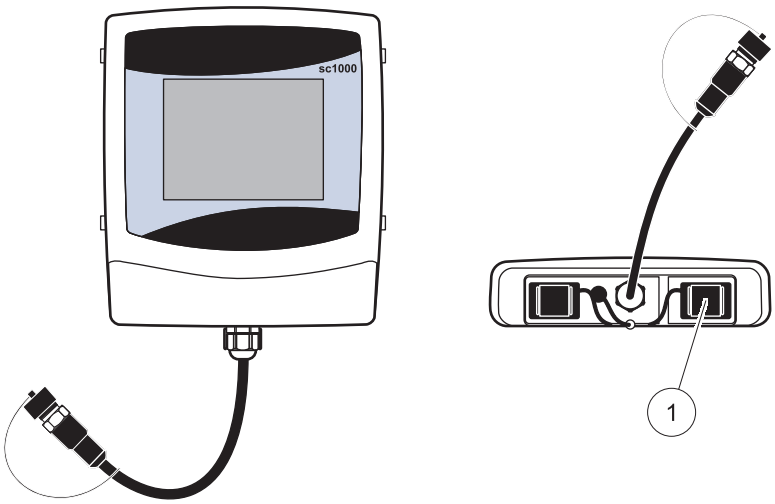

Figure 5 Port Ethernet sur le module d'affichage du transmetteur sc1000

1	Port Ethernet (utilisé en tant que port de sortie) sur le module d'affichage

3. Sélectionnez **CONFIG. SYSTÈME>ACCÈS NAVIGATEUR** dans le menu principal du transmetteur sc1000 pour configurer les paramètres de réseau.
4. En cas de configuration manuelle du réseau, adressez-vous au département informatique afin d'obtenir les paramètres suivants :
   - ADRESSE IP
   - MASQUE DE RÉSEAU
   - DNS IP
   - PASSERELLE

CONFIG. SYSTÈME
ACCÈS NAVIGATEUR
ADRESSE IP
MASQUE DE RÉSEAU
DNS IP
PASSERELLE
DHCP

5. En cas de configuration automatique, définissez le DHCP comme suit :
   - DHCP: ACTIF
6. Ouvrez un navigateur web sur l'ordinateur. Saisissez l'adresse IP du transmetteur dans la barre d'adresse (voir le point 3.). La page de connexion du transmetteur sc1000 s'affiche (Figure 6).
7. Saisissez le mot de passe du navigateur (voir (Figure 6 et Chapitre 3.4.1, page 13).

Remarque : *Le mot de passe de navigateur est fondamental pour les accès au transmetteur via navigateur web.*

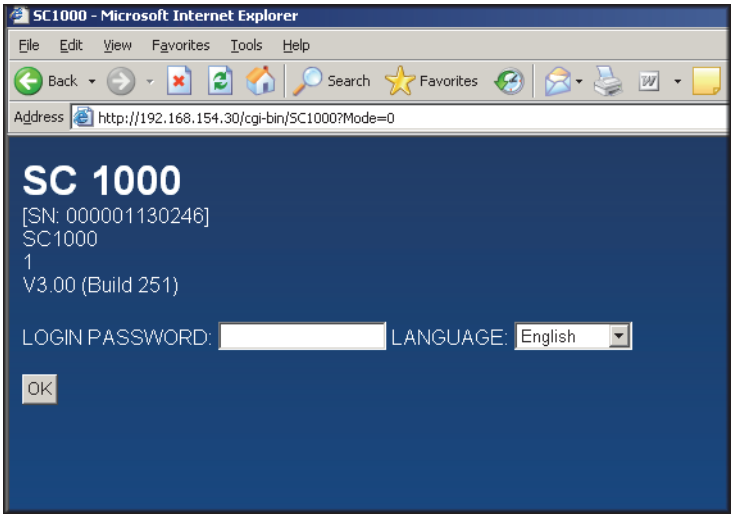

Figure 6 Page d'accueil du transmetteur sc1000

La connexion Ethernet entre l'ordinateur et le transmetteur sc1000 est à présent établie.

3.4.2 Établissement d'une connexion Ethernet avec tunnel VPN sécurisé

Figure 7 Connexion Ethernet avec tunnel VPN sécurisé

Si le transmetteur se trouve hors du réseau d'entreprise, une connexion Ethernet avec tunnel VPN est obligatoire (Figure 7). Les informations concernant la configuration d'un tunnel VPN sont fournies au Chapitre 3.5, page 15.

3.5 Installation d'un tunnel VPN

Si le transmetteur se trouve **hors du réseau d'entreprise**, l'installation d'un réseau privé virtuel (VPN) est requise entre le transmetteur sc1000 et l'ordinateur. Le VPN permet d'établir une communication sur canal sécurisé (tunnel) entre l'ordinateur et le transmetteur, et protégé contre les accès non autorisés.

Windows 2000 et Windows XP offrent tous deux un serveur VPN incorporé. Cette solution, cependant, permet d'activer une seule connexion à la fois entre le transmetteur et l'ordinateur. Pour pouvoir activer plusieurs connexions simultanément, il est nécessaire de disposer d'un serveur VPN autonome.

Le serveur VPN peut être offert par le biais d'un fournisseur de services réseau mobile/Internet ou par le département informatique, en fonction de la conception du VPN. La conception doit être complètement définie avant de commencer l'installation.

3.5.1 Spécifications relatives au transmetteur sc1000

Le transmetteur sc1000 nécessite un logiciel VPN spécifique fourni par le fabricant. L'installation du logiciel VPN sur le transmetteur sc1000 peut être faite à l'aide de plusieurs outils :

- Une carte mémoire SD
- Un navigateur web
- Un transfert de données FTP de Windows Explorer

3.5.2 Spécifications relatives à l'ordinateur

Le logiciel gratuit VPN "Open VPN" doit être installé sur l'ordinateur (voir le Chapitre 3.5.4, page 17).

3.5.3 Transmetteur sc1000 : Installation du client VPN à l'aide d'une carte mémoire SD

Le module d'affichage du transmetteur sc1000 est doté d'un logement pour cartes SD. Une des fonctions de la carte SD consiste à mettre à jour le logiciel du transmetteur. Des informations supplémentaires concernant l'utilisation de cartes mémoire SD sont données dans le manuel relatif au transmetteur sc.

Une carte mémoire SD contenant le logiciel client VPN personnalisé pour le transmetteur sc1000 est disponible à l'achat auprès du fabricant (voir le Chapitre 5, page 45).

Remarque : *Pour l'installation, utilisez uniquement des cartes SD avec une capacité de mémoire maximum de 1 Go.*

1. Sur la carte mémoire SD, créez les répertoires suivants (s'ils n'ont pas déjà été créés) :
   - DEV_SETTINGS
   - SC1000
   - UPDATE
2. Copiez dans le répertoire UPDATE de la carte mémoire SD les fichiers suivants :

Du fabricant :

- Logiciel client VPN personnalisé
  (s'il n'est pas déjà installé sur la carte mémoire SD, contactez l'assistance du fabricant)

Fournis par le fournisseur de service VPN :

- Fichier de configuration (fichier avec extension ".ovn")
- Certificat (fichier avec extension ".crt")
- Fichier clé (fichier avec extension ".key")

3. Démarrez le transmetteur sc1000.
4. Retirez le couvercle du logement de la carte SD sur le module d'affichage du transmetteur sc1000 (Figure 8).

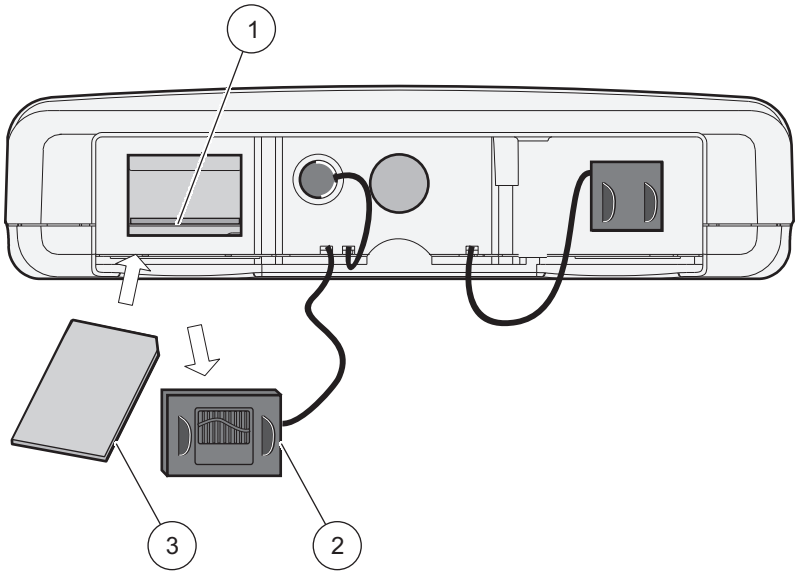

Figure 8 Dans la partie inférieure du module d'affichage

1	Logement de la carte SD	**3**	Carte mémoire SD
2	Couvercle du logement de la carte SD		

5. Insérez la carte mémoire SD dans son logement situé sur le transmetteur.
6. Remontez le couvercle du logement de la carte SD.

CONFIG. SYSTÈME
CARTE MÉMOIRE
MISE À JOUR DU LOGICIEL

7. Démarrez l'installation du client VPN en sélectionnant les options du menu, **CONFIG. SYSTÈME>CARTE MÉMOIRE> MISE À JOUR DU LOGICIEL**.

Le transmetteur sc1000 installe et configure automatiquement le logiciel VPN, après quoi il nécessite d'être redémarré.

8. Afin de valider la configuration du VPN, sélectionnez **CONFIG. SYSTÈME>ACCÈS NAVIGATEUR>VPN**.

3.5.4 Transmetteur sc1000 : Installation du client VPN à l'aide d'un navigateur web

Remarque : *Le navigateur web installé sur l'ordinateur doit inclure la prise en charge du transfert de données via FTP. Seul le navigateur Microsoft Internet Explorer 7 inclut la prise en charge partielle du protocole FTP.*

1. Assurez-vous que la connexion Ethernet entre le transmetteur sc1000 et l'ordinateur fonctionne parfaitement.
2. Assurez-vous que navigateur web utilisé inclut la prise en charge le protocole FTP.
3. Ouvrez le navigateur web sur l'ordinateur et saisissez l'adresse IP du transmetteur dans la barre d'adresse (Figure 9).
4. La page de connexion du transmetteur s'affiche.

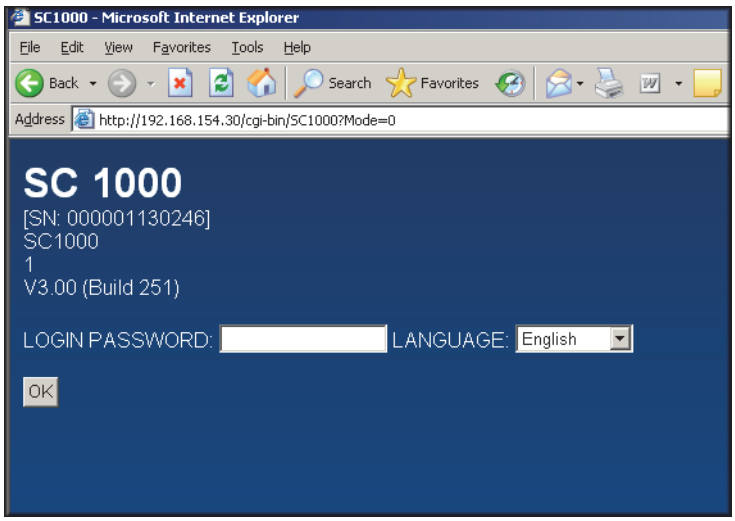

Figure 9 Page d'accueil du transmetteur sc1000

CONFIG. SYSTÈME
ACCÈS NAVIGATEUR
ADRESSE IP

L'adresse IP du transmetteur sc1000 se trouve sous **CONFIG. SYSTÈME>ACCÈS NAVIGATEUR>ADRESSE IP**.

5. Saisissez le mot de passe du navigateur (voir (3.4.1, page 13).

   Remarque : *Le mot de passe de navigateur est fondamental pour les accès au transmetteur via navigateur web.*

6. Appuyez sur le bouton **MISE À JOUR**du volet NAVIGATION (Figure 10).

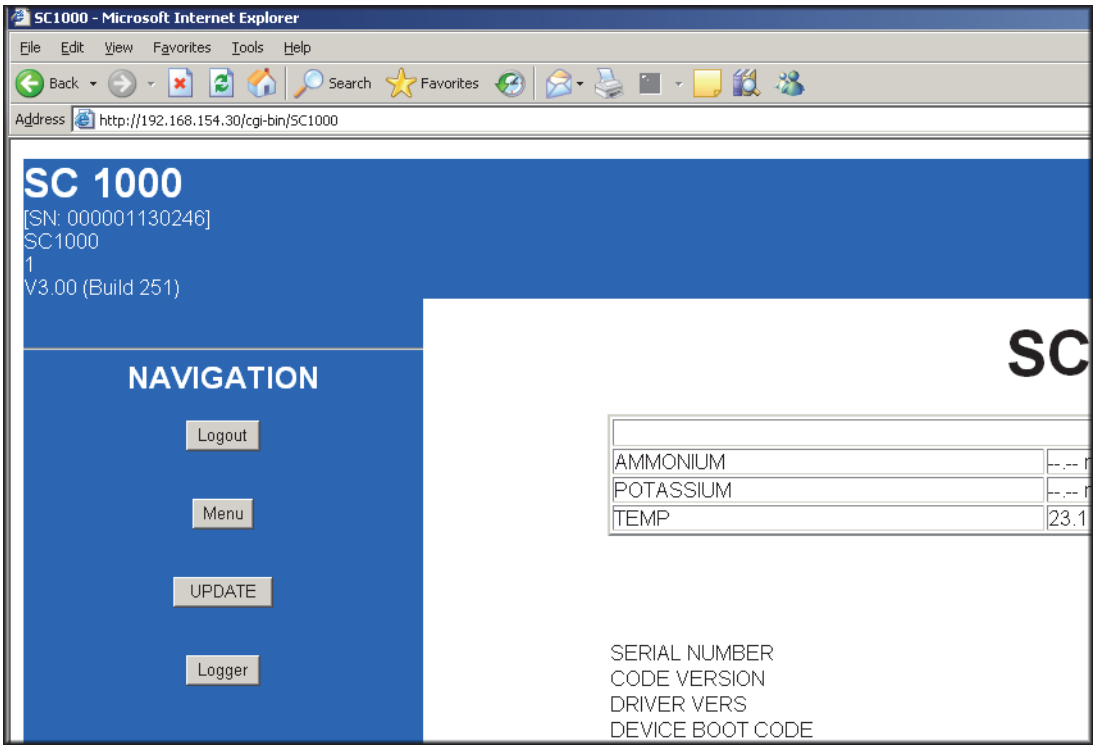

Figure 10 **BOUTON** Mise à jour

7. Cliquez sur le lien **MISE À JOUR DU MODULE D'AFFICHAGE** (Figure 11).

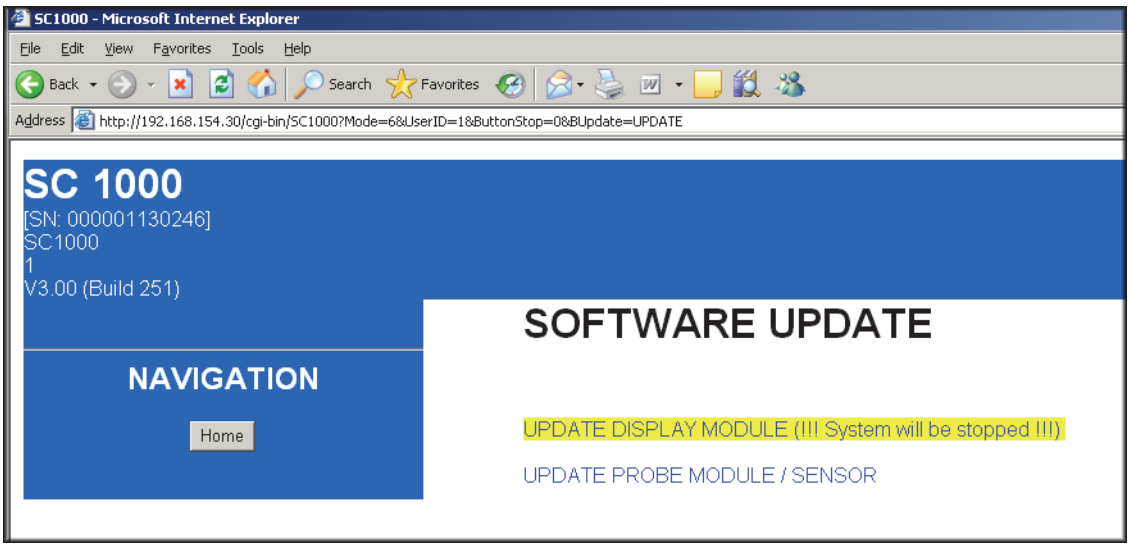

Figure 11 Lien de mise à jour du module d'affichage

8. L'écran "Télécharger les fichiers sur sc1000" s'affiche et l'interface du gestionnaire de fichiers (Microsoft Windows Explorer) est intégré dans la fenêtre du navigateur.

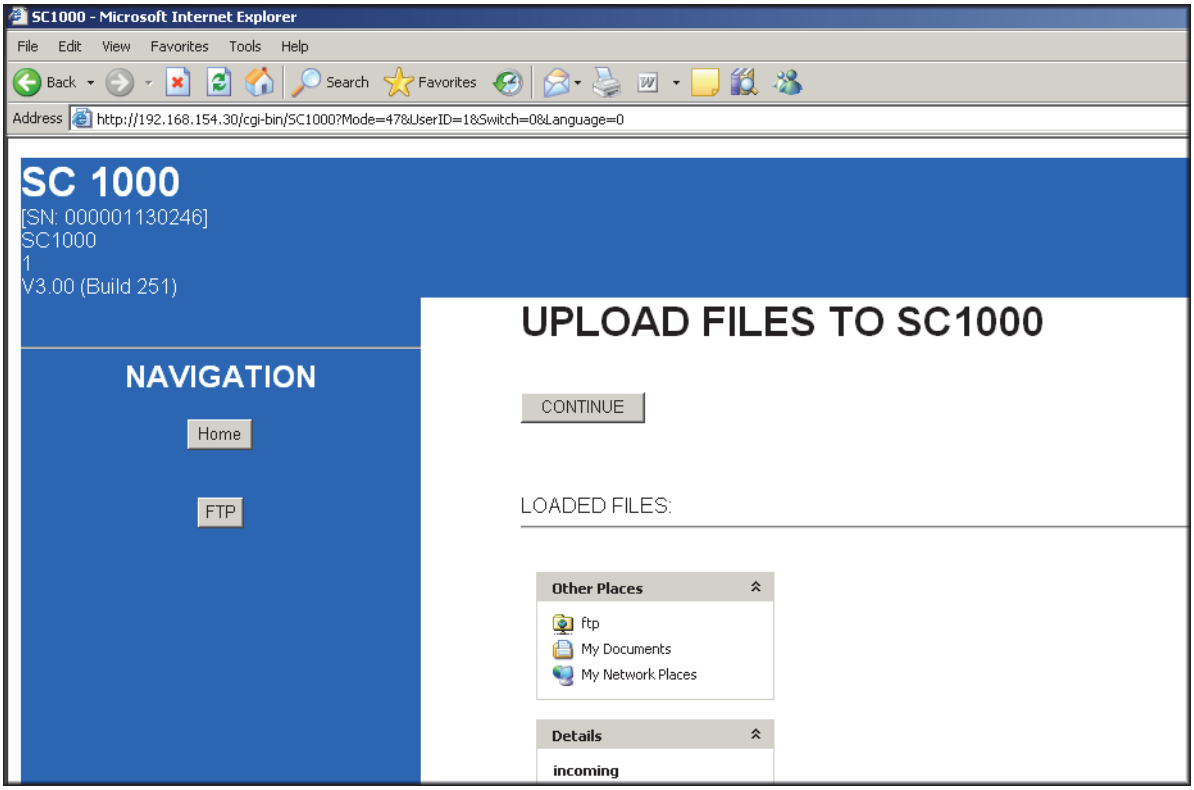

Figure 12 Télécharger les fichiers sur le transmetteur sc1000

9. Cliquez sur **ftp** sous le volet FICHIERS TELECHARGES de la fenêtre du navigateur.
10. Ouvrez le gestionnaire de fichiers (Microsoft Windows Explorer) et sélectionnez les fichiers indiqués ci-dessous. Ces fichiers doivent être stockés sur le disque dur , sur le réseau ou sur une porteuse de données mobile :

Du fabricant :

- Logiciel client VPN personnalisé

Du fournisseur de service VPN :

- Fichier de configuration (fichier avec extension ".ovn")
- Certificat (fichier avec extension ".crt")
- Fichier clé (fichier avec extension ".key")

11. Copiez et collez les fichiers dans le répertoire **incoming**du navigateur web (Figure 13).

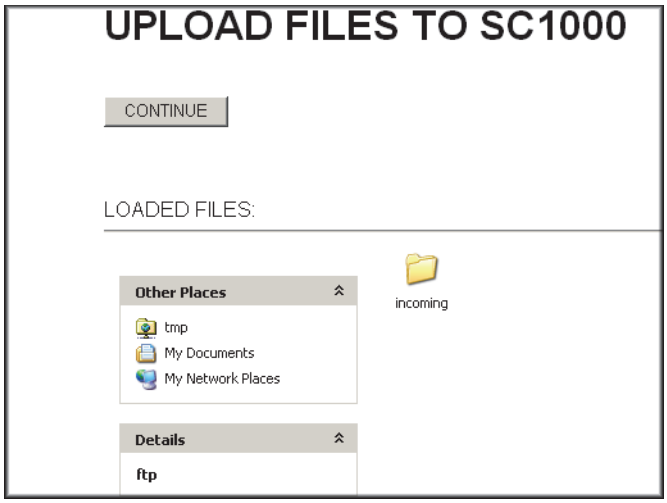

Figure 13 Transfert des fichiers

12. Appuyez sur le bouton **CONTINUER**.
13. Confirmez la mise à jour sur l'écran du transmetteur sc1000.

    Dès lors, le transmetteur installe et configure automatiquement le logiciel, puis il doit être redémarré.

3.5.5 Transmetteur sc1000 : Installation du client VPN via FTP de Windows Explorer

Si le navigateur web ne prend pas en charge le protocole FTP, vous pouvez également effectuer le transfert de données via FTP dans Windows Explorer.

1. Fermez le navigateur web (s'il est encore ouvert).
2. Ouvrez Windows Explorer.
3. Saisissez l'adresse FTP indiquée ci-dessous dans la barre d'adresse de Windows Explorer :

   ftp://*<adresse du transmetteur sc1000>*/tmp/incoming

   Exemple : ftp://192.168.154.30/tmp/incoming
4. Appuyez sur la touche **ENTREE** pour confirmer la connexion FTP.
5. Ouvrez le gestionnaire de fichiers (ex.. Microsoft Windows Explorer) et sélectionnez les fichiers suivants : Ces fichiers doivent être stockés sur le disque dur , sur le réseau ou sur une porteuse de données mobile :

Du fabricant :

- Logiciel client VPN personnalisé

Du fournisseur de service VPN :

- Fichier de configuration (fichier avec extension ".ovn")
- Certificat (fichier avec extension ".crt")
- Fichier clé (fichier avec extension ".key")

6. Copiez les fichiers sélectionnés dans le répertoire FTP :
*<adresse IP du transmetteur sc1000>***tmp****incoming** (Figure 14).

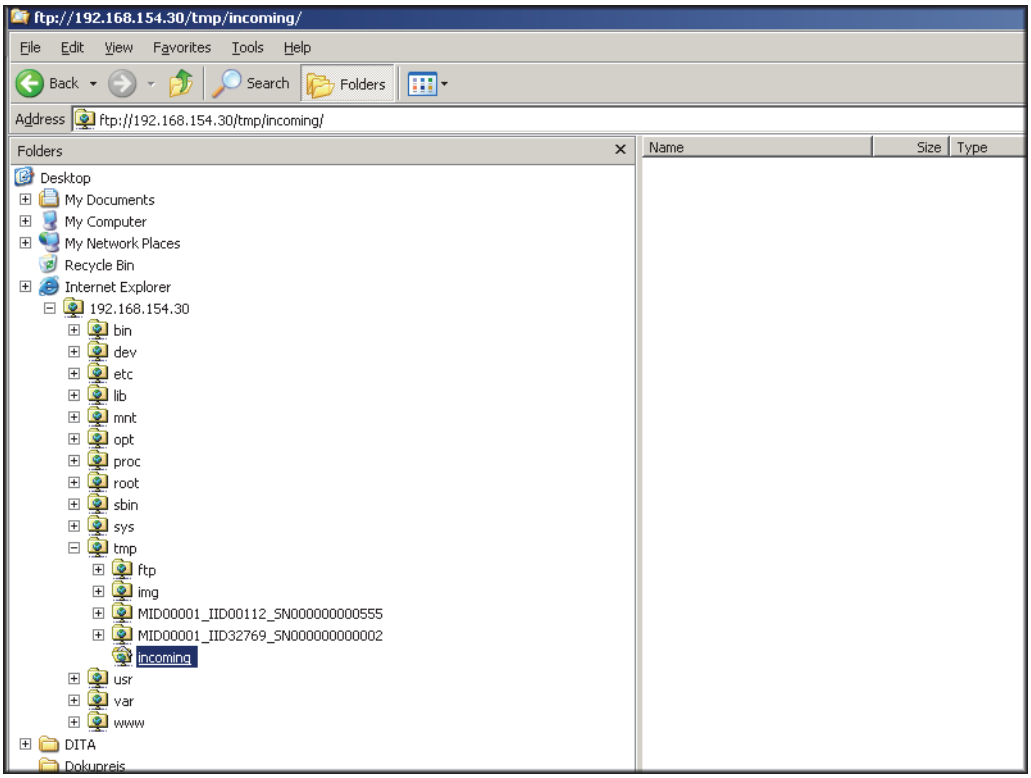

Figure 14 Transfert de données FTP dans Microsoft Windows Explorer

7. Ouvrez le navigateur web sur l'ordinateur et saisissez l'adresse IP du transmetteur dans la barre d'adresse.

   La page de connexion du transmetteur s'affiche.

8. Saisissez le mot de passe du navigateur.
9. Appuyez sur le bouton **UPDATE**.
10. Cliquez sur le lien **MISE À JOUR DU MODULE D'AFFICHAGE** .
11. Confirmez la mise à jour sur l'écran du transmetteur sc1000.

Dès lors, le transmetteur installe et configure automatiquement le logiciel, puis il doit être redémarré.

3.5.6 Transmetteur sc1000 : Vérification de l'installation de VPN

1. Ouvrez le navigateur web sur l'ordinateur et saisissez l'adresse IP du transmetteur dans la barre d'adresse.
2. Saisissez le mot de passe du navigateur (voir (3.4.1, page 13)).

CONFIG. SYSTÈME
ACCÈS NAVIGATEUR
VPN
VPN

3. Sur l'écran **CONFIG. SYSTÈME>ACCÈS NAVIGATEUR>VPN**, assurez-vous que la balise **VPN**est définie sur **LAN**.
4. Sur l'écran **CONFIG. SYSTÈME>ACCÈS NAVIGATEUR**, assurez-vous que la balise **VPN**est définie sur **CONNEXION**.

CONFIG. SYSTÈME
ACCÈS NAVIGATEUR
VPN
FICHIER CONFIG

5. Sur l'écran **CONFIG. SYSTÈME>ACCÈS NAVIGATEUR>FICHIER CONFIG**, assurez-vous qu'aucune balise n'est mise en évidence en rouge.

   Les balises affichées en rouge indiquent des erreurs (voir le Chapitre 4, page 41).

   Les balises affichées en gris clair indiquent que les informations correspondantes sont déjà inclues dans la configuration et qu'elles peuvent être ignorées.
6. Saisissez le **NOM UTILISATEUR** et le **MOT DE PASSE**sur l'écran **CONFIG. SYSTÈME>ACCÈS NAVIGATEUR>VPN**, si le fournisseur de service VPN vous le demande. Ces détails doivent être fournis par le fournisseur de service VPN.

3.5.7 Ordinateur : Installation du client VPN

Pour communiquer avec le transmetteur sc1000 via tunnel VPN, vous devez installer un client VPN sur l'ordinateur également.

Remarque importante : *S'il est nécessaire d'installer un client VPN sur le transmetteur sc1000 pour établir une connexion, le client OpenVPN doit être installé sur l'ordinateur. OpenVPN est une solution VPN gratuite, prise en charge par plusieurs systèmes d'exploitation. Ce logiciel peut être téléchargé à partir du site web : http://www.openvpn.net.*

1. Installez OpenVPN sur l'ordinateur (en suivant les instructions fournies avec le logiciel).

   L'icône OpenVPN s'affiche dans la barre des tâches du bureau au terme de l'installation (Figure 15).

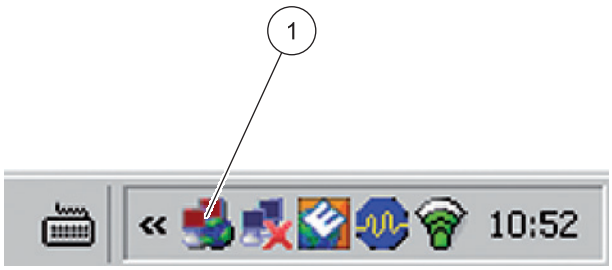

Figure 15 Icône OpenVPN dans la barre des tâches

1	Icône OpenVPN

2. Copiez dans le répertoire OpenVPN les fichiers suivants :

Du fabricant :

- Logiciel client VPN personnalisé

Du fournisseur de service VPN :

- Fichier de configuration (fichier avec extension ".ovn")
- Certificat (fichier avec extension ".crt")
- Fichier clé (fichier avec extension ".key")

3. Démarrez OpenVPN.

3.5.8 Établissement d'une connexion VPN entre le transmetteur sc1000 et l'ordinateur

1. Démarrez OpenVPN sur l'ordinateur.
2. Saisissez le nom d'utilisateur et le mot de passe (Figure 16). Ces données sont fournies par le fournisseur de service VPN.

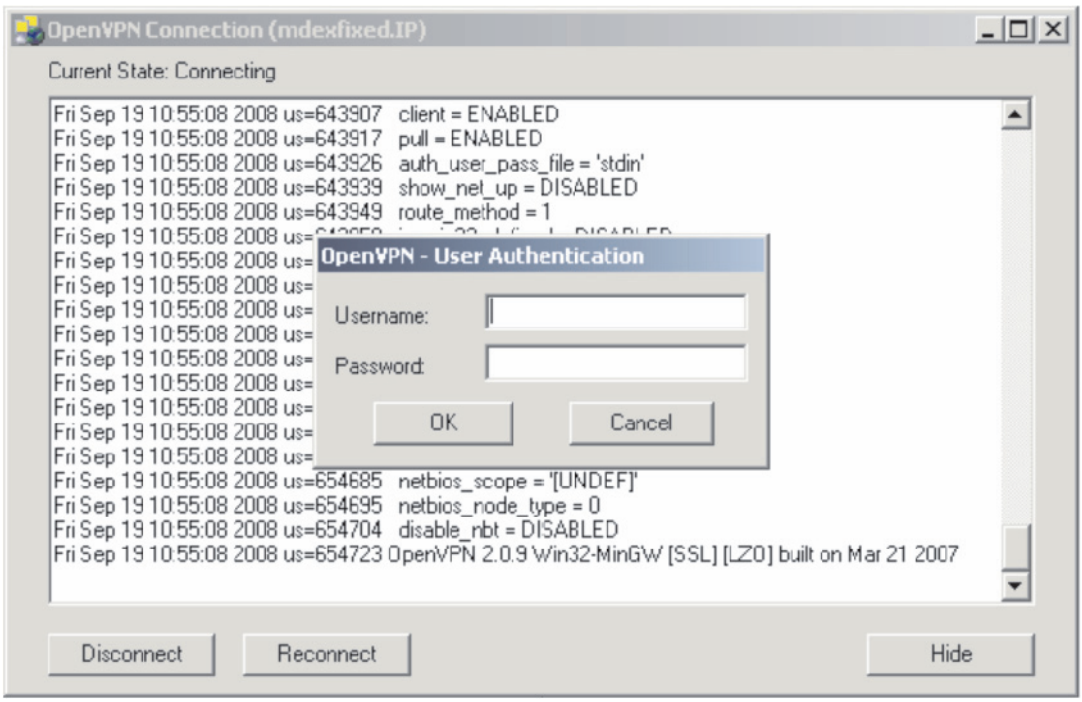

Figure 16 Établissement de la connexion dans OpenVPN

3. Saisissez l'adresse IP du transmetteur (fournie par le fournisseur de service VPN) dans le navigateur web de l'ordinateur (Figure 17).

   Remarque : *Pour trouver l'adresse IP, sélectionnez* ***CONFIG. SYSTÈME>ACCÈS NAVIGATEUR>VPN>ADRESSE IP*** *dans le menu du transmetteur.*

Remarque : *Le logiciel OpenVPN installé sur l'ordinateur n'est pas fourni par le fabricant. Pour plus d'informations, contactez le fournisseur de service VPN.*

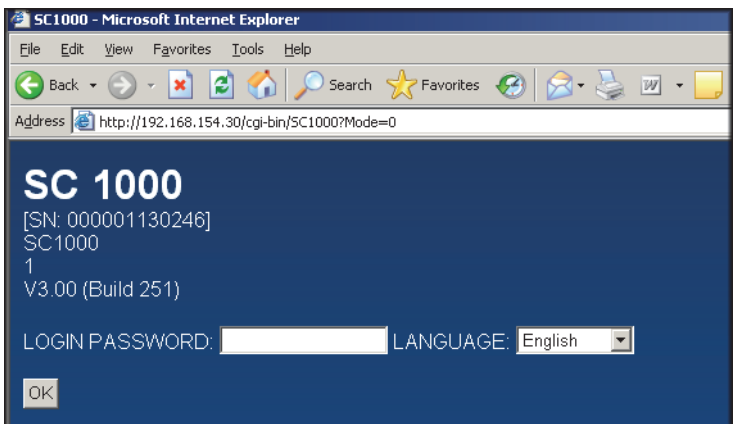

Figure 17 Page d'accueil du transmetteur sc1000

4. Saisissez le mot de passe du navigateur (voir (Chapitre 3.4.1, page 13)).

L'ordinateur e le transmetteur sc1000 sont désormais connectés via un tunnel sécurisé VPN.

3.6 Établissement d'une connexion GPRS

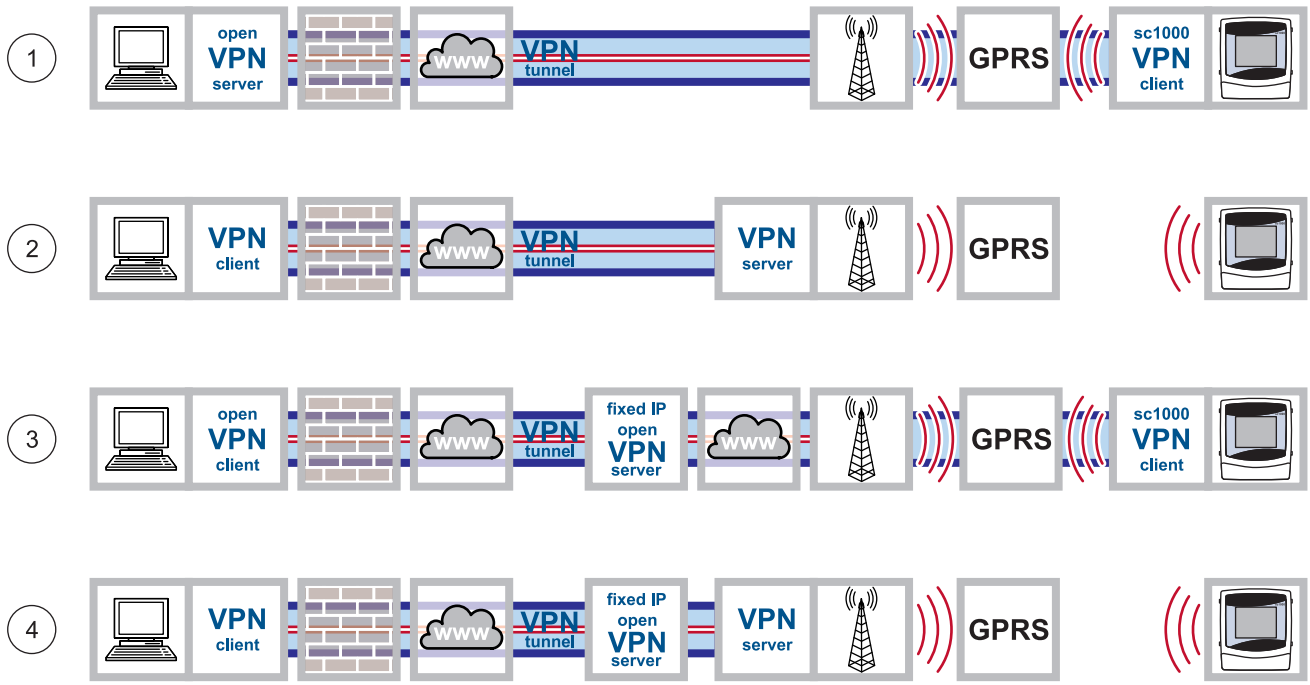

Figure 18 Connexions GPRS

1	Connexion GPRS avec tunnel VPN sécurisé
2	Connexion GPRS via serveur VPN de l'opérateur du réseau mobile
3	Connexion GPRS via serveur VPN-IP fixe (possible uniquement si un compte CDA (Corporate Data Access) est configuré avec l'opérateur du réseau mobile)
4	Connexion GPRS via service IP fixe et serveur VPN de l'opérateur du réseau mobile

Le GPRS est un service de communication données orientée paquet fondé sur la norme de téléphonie mobile GSM. Le GPRS permet aux utilisateurs de transférer des données en déplacement. Ce type de transfert de données consiste à convertir des lots individuels de données en petits paquets, lesquels seront envoyés successivement. Ces paquets seront reconstruits ensuite lors de leur réception.

Lorsque le GPRS est activé sur le transmetteur sc1000, une connexion permanente est établie en apparence avec le récepteur (\qtoujours\q en fonctionnement). Toutefois, le canal radio n'est pas ouvert jusqu'à ce que les données ne soient effectivement transférées. La facturation du service GPRS tient compte du volume de données envoyées, non pas du temps de connexion.

Une adresse IP dynamique et temporaire est attribuée à la station mobile (par ex., le transmetteur sc1000) afin d'identifier de manière unique la station. Du point de vue de l'utilisateur, l'accès au dispositif se fait via cette adresse IP, comme usuellement sur Internet.

Le GPRS munit le transmetteur sc1000 d'une connexion Internet lui permettant de communiquer avec d'autres utilisateurs d'Internet.

L'adresse IP attribuée au transmetteur lors de l'utilisation du GPRS n'est pas accessible directement de l'internet. Par conséquent, les requêtes transmises par un appareil GPRS (le transmetteur sc1000, dans ce cas) ne peuvent être acheminées que par le réseau Internet. Uniquement à ce moment là, l'opérateur de réseau autorise le routage de la réponse depuis l'Internet vers le dispositif GPRS.

Toutes les connexions GPRS sont gérées via un opérateur de réseau mobile. Les types de connexion GPRS détaillées dans ce manuel (Figure 18) sont les suivants :

- Connexion GPRS avec tunnel VPN sécurisé
  (Figure 18, point 1)
- Connexion GPRS via serveur VPN de l'opérateur du réseau mobile (possible uniquement si un compte CDA (Corporate Data Access) est configuré avec le susdit opérateur)
  (Figure 18, point 2)
- Connexion GPRS via serveur VPN avec IP fixe
  (Figure 18, point 3)
- Connexion GPRS via service IP fixe et serveur VPN de l'opérateur du réseau mobile
  (Figure 18, point 4)

3.6.1 Spécifications matérielles relatives au transmetteur sc1000

Le transmetteur sc1000 doit être équipé pour les communications données mobile :

- Un modem GSM//GPRS doit être installé.
- Une antenne doit être connectée.
- Une carte SIM GPRS doit être installée.
  Si tel est le cas, la carte SIM doit être configurée selon les spécifications de l'opérateur de réseau mobile (PIN modifié).

  Remarque : *Un contrat doit être stipulé avec l'opérateur du réseau mobile spécifiant le volume de données approprié.*

3.6.2 Paramètres logiciels du transmetteur sc1000

- Attribuez un mot de passe de navigateur via les options du menu **CONFIG. SYSTÈME>ACCÈS NAVIGATEUR>MOT DE PASSE**.
- Saisissez le PIN spécifié par l'opérateur de réseau mobile via les options du menu **CONFIG. SYSTÈME>MODULE GSM>PIN**.

CONFIG. SYSTÈME
MODULE GSM
NUMERO D'ACCÈS
APN
GPRS
NOM UTILISATEUR
MOT DE PASSE

- Dans le menu **CONFIG. SYSTÈME>MODULE GSM>GPRS**
  - Vérifiez si le **NUMERO D'ACCÈS** est identique au numéro spécifié par l'opérateur du réseau mobile
  - Saisissez l'**APN** (Access Point Name, fourni par l'opérateur du réseau mobile)
  - Saisissez le **NOM UTILISATEUR**et le **MOT DE PASSE** (fournis par l'opérateur du réseau mobile)
  - Définissez la balise **GPRS**sur **ACTIF**.
  -

Le transmetteur sc1000 est à présent prêt pour les communications GPRS.

3.6.3 Connexion GPRS sans tunnel VPN

Figure 19 Connexion GPRS sans tunnel VPN

Une connexion GPRS sans tunnel VPN est possible uniquement si un compte CDA a été configuré avec l'opérateur du réseau mobile. Si tel est le cas, seuls les paramètres logiciels doivent être configurés sur le transmetteur sc1000 (Chapitre 3.6.2, page 26) ; la configuration du réseau VPN en lui-même est du ressort de l'administration CDA.

En absence d'un compte CDA, seule la connexion Internet est possible. Ce type de connexion permet d'envoyer les courriels mais ne permet pas l'accès au transmetteur.

3.6.4 Établissement d'une connexion GPRS avec tunnel VPN sécurisé

Figure 20 Établissement d'une connexion GPRS avec tunnel VPN sécurisé

1. Installez le client VPN sur l'ordinateur et sur le transmetteur comme indiqué au Chapitre 3.5, page 15.
2. Sur le transmetteur sc1000, accédez à l'écran **CONFIG. SYSTÈME>ACCÈS NAVIGATEUR>VPN>VPN**, puis définissez la balise VPN sur **GPRS**.
3. Sous **CONFIG. SYSTÈME>ACCÈS NAVIGATEUR>VPN**, vérifiez les conditions suivantes
   - La balise **STATUT** est définie sur **CONNEXION**
   - L'adresse IP et affichée dans la balise **ADRESSE IP**

   Remarque : *L'adresse IP est importante et elle a dû être spécifiée par le fournisseur de service VPN. Cette adresse a déjà été définie lors de la mise ne place de la connexion standard VPN Ethernet.*

Vérification de la connexion
La connexion GPRS avec tunnel VPN sécurisé est active si les conditions suivantes sont remplies :

- La balise **CONNEXION GPRS** est affichée sous **STATUT** dans le menu **CONFIG. SYSTÈME>MODULE GSM>GPRS**.
- Une **adresse IP**a été attribuée dans le menu **CONFIG. SYSTÈME>MODULE GSM>GPRS**. Cette adresse IP doit être attribuée, toutefois elle n'est plus importante dorénavant.

3.7 Établissement d'une connexion GPRS via serveur VPN-IP fixe

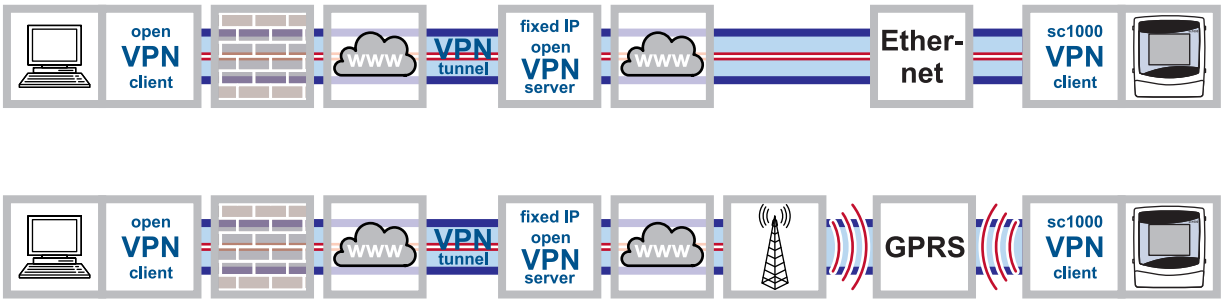

Figure 21 Établissement d'une connexion GPRS via serveur VPN-IP fixe

La connexion d'un transmetteur sc1000 au sein d'un réseau d'entreprise via tunnel VPN présente des problèmes. Par conséquent un service IP externe fixe faisant fonction de serveur VPN et d'interface vers l'opérateur du réseau mobile constitue une alternative acceptable.

Si tel est le cas, l'accès au transmetteur sc1000 se fait via l'Internet à l'aide de l'adresse fixe qui lui est attribuée. Cette adresse ne change pas.

Une telle connexion IP fixe peut utiliser le protocole Ethernet ou le GPRS (Figure 21). Les coûts encourus par l'utilisation du réseau mobile/ GPRS sont calculés en fonction du volume des données transmises et de la fréquence à laquelle elles sont transmises.

3.8 Connexion GPRS via serveur VPN de l'opérateur du réseau mobile

Figure 22 Connexion GPRS via serveur VPN de l'opérateur du réseau mobile

Le service CDA (Corporate Data Access) est utilisé pour le transfert de données chiffrées entre les appareils et le centre de commande via le GPRS. Le réseau d'entreprise est connecté au réseau mobile dans l'un des deux modes : via la location d'une ligne qui garantit une largeur de bande fixe et un haut niveau de sécurité, ou via l'Internet. La connexion entre le réseau d'entreprise te l'opérateur de réseau mobile est établie via un tunnel VPN sécurisé

L'APN (Access Point Name), le nom d'utilisateur et le mot de passe sont requis à chaque connexion entre le transmetteur sc1000 et l'ordinateur. Les utilisateurs sont identifiés par l'opérateur du réseau mobile.

CONFIG. SYSTÈME
MODULE GSM
NUMERO D'ACCÈS
APN
GPRS
NOM UTILISATEUR
MOT DE PASSE

- Dans le menu **CONFIG. SYSTÈME>MODULE GSM>GPRS**
  - Vérifiez si le **NUMERO D'ACCÈS** est identique au numéro spécifié par l'opérateur du réseau mobile
  - Saisissez l'**APN** (Access Point Name, fourni par l'opérateur du réseau mobile)
  - Saisissez le **NOM UTILISATEUR**et le **MOT DE PASSE** (fournis par l'opérateur du réseau mobile)
  - Définissez la balise **GPRS** sur **ACTIF**

Il est possible également d'obtenir un point d'accès privé (APN) au sein du réseau. Si vous choisissez cette option, seules les machines possédant un profil de carte SIM spécifique peuvent se connecter au réseau via ce point d'accès. L'opérateur du réseau mobile précise les conditions requises liées à la configuration d'un point d'accès privé.

3.9 Connexion GPRS via le service IP fixe et le serveur VPN de l'opérateur du réseau mobile

Figure 23 Connexion GPRS via le service IP fixe et le serveur VPN de l'opérateur du réseau mobile

La connexion à un réseau privé d'entreprise présente parfois des problèmes. C'est pour cette raison que les fournisseurs de service IP fixe offrent usuellement ce service.

L'opérateur du réseau mobile connecte l'utilisateur au fournisseur du service IP fixe via un tunnel privé VPN. Dans ce cas, le transmetteur sc1000 ne nécessite pas de son propre client VPN. L'utilisateur nécessite que le logiciel client VPN soit installé sur son ordinateur afin de se connecter au fournisseur du service IP fixe.

3.10 Expansion Modbus TCP en option

Le Modbus TCP est un protocole standard pour les communications industrielles. Par le biais du protocole Modbus TCP, les ordinateurs peuvent se connecter aux systèmes de commande et mesures, lesquels utilisent le protocole TCP/IP pour la transmission des données. Cette forme de transmission de données est dénommée M2M (M2M= machine-to-machine).

Remarque : *Il n'est pas nécessaire d'installer une carte Modbus dans le transmetteur sc1000 pour utiliser le module logiciel Modbus TCP.*

Le module logiciel Modbus TCP permet d'intégrer le transmetteur sc1000 directement dans les systèmes PLC (automates programmables). Les systèmes PLC enregistrent les données mesurées par le sc1000 pour les traiter ultérieurement. L'analyse des données reçues et les actions qui en découlent sont programmées par le système PLC.

3.10.1 Spécifications relatives au logiciel Modbus TCP

L'utilisation du logiciel Modbus TCP dans le transmetteur nécessite une activation ou une licence.

3.10.2 Paramètres logiciels du transmetteur sc1000

La configuration du logiciel Modbus TCP est effectuée dans les menus suivants du transmetteur sc1000 :

CONFIG. SYSTÈME MODBUS TCP	
MODBUS TCP	Détermine si le protocole TCP Modbus est activé (ACTIF) ou non (INACTIF).
PORT TCP	Détermine le port TCP.
TÉLÉGRAMME	Configure un esclave basé sur les compilations des données individuelles des divers appareils.
ADRESSE MODBUS	Valeur par défaut : 0 Détermine l'adresse (de 1 à 247) de l'esclave Modbus configuré dans le menu TÉLÉGRAMME.
ESCLAVES VIRTUELS	Valeur par défaut : DÉSACTIVÉS Les esclaves virtuels peuvent être ajoutés. Ceux-ci sont des copies des appareils effectifs et sont configurés dans le menu TÉLÉGRAMME. Les adresses Modbus de ces esclaves sont directement affichées à droite de l'adresse d'esclave configuré. L'adresse Modbus du premier appareil configuré est directement affichée à droite de l'adresse de l'esclave configuré, l'adresse du deuxième appareil est affichée à droite de celui-ci, et ainsi de suite. ACTIVÉ : la copie de l'esclave est activée. DÉSACTIVÉ : la copie de l'esclave est désactivée.
DATA ORDER	Valeur par défaut : NORMALE Détermine la séquence d'octets permettant de transférer les valeurs en virgule flottante. Une valeur en virgule flottante comprend 4 octets. Remarquez que cette configuration affecte uniquement les données de l'esclave configuré. PERMUTÉ : Échange la première paire d'octets avec la dernière. NORMAL : Les paires ne sont pas permutées. Une fausse configuration dans ce menu peut entraîner des légères déviations des valeurs en virgule flottante (décalé d'un registre).
SIMULATION	Permet de simuler deux valeurs en virgule flottante ainsi que des erreurs ou des statuts en se substituant à un instrument. La première valeur en virgule flottante suit une rampe limitée par un MINIMUM et un MAXIMUM définis dans les menus correspondants.
SIMULATION	Valeur par défaut : NON Active la simulation (OUI) ou la désactive (NON).
DURÉE	Valeur par défaut : 10 minutes Détermine le temps que la première valeur en virgule flottante emploie pour passer du MINIMUM au MAXIMUM.
MAXIMUM	Valeur par défaut : 100 Limite supérieure pour la première valeur de la virgule flottante.
MINIMUM	Valeur par défaut : 50 Limite inférieure pour la première valeur de la virgule flottante.
ERREURS	Valeur par défaut : 0 La valeur saisie dans ce menu est définie comme étant la valeur du premier registre simulé.
STATUT	Valeur par défaut : 0 La valeur saisie dans ce menu est définie comme étant la valeur du second registre simulé.
BASCULER	Change la direction de la rampe simulée.
STATUT	Contient les informations sur le transfert de données.

3.10.3 Configuration du logiciel Modbus TCP sur le transmetteur sc1000

CONFIG. SYSTÈME
MODBUS TCP
MODBUS TCP
PORT TCP
TÉLÉGRAMME
ADRESSE MODBUS
ESCLAVES VIRTUELS
SIMULATION
STATUT

1. Définissez la balise **MODBUS TCP** sur **ACTIF** dans le menu **CONFIG. SYSTÈME>MODBUS TCP**.
2. Définissez la balise **PORT TCP** sur **502**dans le menu **CONFIG. SYSTÈME>MODBUS TCP**.

   Remarque : *Il peut s'avérer nécessaire de sélectionner un port alternatif en fonction de la configuration du pare-feu d'entreprise. Le responsable du département d'informatique fournira les informations appropriées à ce sujet.*
3. Créez le télégramme sur l'écran de configuration **CONFIG. SYSTÈME>MODBUS TCP>TÉLÉGRAMME**(voir le manuel du transmetteur sc1000 ou Chapitre 3.10.4, page 33).

   Remarque : *Le télégramme définit les points données que le transmetteur transfère et dans quelle séquence. Les données ainsi que leur nom dépendent de la sonde.*
4. Veillez à saisir l'adresse du télégramme dans le menu **CONFIG. SYSTÈME>MODBUS TCP>ADRESSE MODBUS** (valeur par défaut = 1).

   Remarque : *Les appareils présents aux adresses successives ne répondent que si la balise des esclaves virtuels dans le menu* ***CONFIG. SYSTÈME>MODBUS TCP>ESCLAVES VIRTUELS*** *est définie sur* ***ACTIF****.*
5. Saisissez les valeurs dans le menu **CONFIG. SYSTÈME>MODBUS TCP>SIMULATION** pour activer le transfert des données à tester.
6. Définissez la balise dans le menu **CONFIG. SYSTÈME>MODBUS TCP>SIMULATION>SIMULATION** sur **ACTIF** pour tester le transfert de données.

Les informations concernant le transfert de données sont affichées dans le menu **CONFIG. SYSTÈME>MODBUS TCP>STATUT** (voir aussi le Tableau 4, page 41).

Figure 24 Menu du statut Modbus TCP

Après avoir défini toutes les valeurs, vous pouvez requérir les valeurs transférées dans le télégramme et les traiter à partir de n'importe quel client Modbus TCP.

Un maximum de 5 clients Modbus TCP peuvent être connectés au serveur simultanément. Si un client supplémentaire tente d'établir une connexion, celle-ci sera acceptée mais une connexion préalablement existante sera perdue. Dans ce cas, le système interrompt la connexion restée inutilisée le plus longtemps.

3.10.4 Configuration du télégramme Modbus

CONFIG. SYSTÈME
MODBUS TCP
TÉLÉGRAMME

1. Sélectionnez **CONFIG. SYSTÈME>MODBUS TCP>TÉLÉGRAMME**.
2. L'écran de configuration s'affiche (Figure 25).

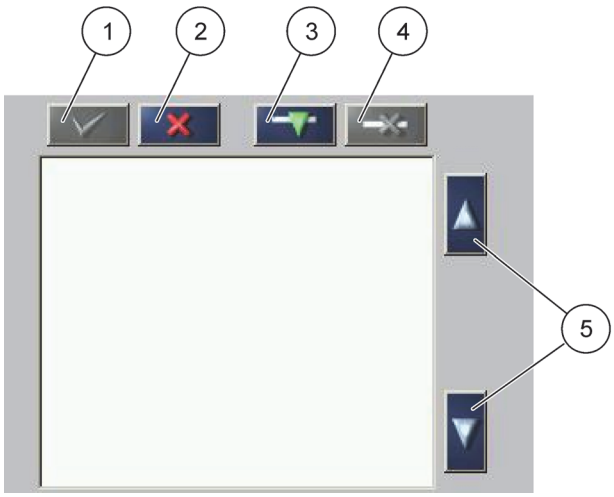

Figure 25 Écran de configuration

1	**LE BOUTON** ENTRER : enregistre la configuration et revient au menu du bus de terrain	**4**	**LE BOUTON** SUPPRIMER : élimine un dispositif / une balise du télégramme
2	**LE BOUTON** ANNULER : revient au menu du bus de terrain sans enregistrer	**5**	**LES FLÈCHES** HAUT/BAS : déplace l'appareil / la balise vers le haut et le bas
3	**LA BOUTON** AJOUTER : ajoute un appareil / une balise au télégramme		

3. Appuyez sur **AJOUTER**, puis sélectionnez une sonde / un appareil. La fenêtre de sélection d'appareil s'affiche (Figure 26).

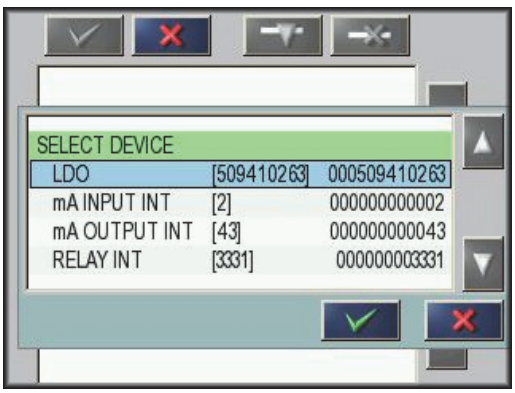

Figure 26 Fenêtre de sélection d'appareil

4. Sélectionnez une sonde / un appareil et appuyez sur le bouton**ENTRER**. La sonde / l'appareil (numéro de série inclus) est ajouté (e) à la boîte du télégramme (Figure 27).

Figure 27 Liste des appareils

5. Sélectionnez une balise (erreur ou statut, par exemple) et appuyez sur le bouton **AJOUTER**. La fenêtre de sélection des balises s'affiche avec toutes les balises disponibles pour la sonde/l'appareil (Figure 28). Les registres d'erreur et de statut sont identiques pour tous les appareils (Tableau 2) et (Tableau 3).

Figure 28 Fenêtre de sélection des balises

6. Sélectionnez une balise et appuyez sur le bouton**ENTRER**. La nouvelle balise est ajoutée au télégramme. Sélectionnez une balise et appuyez sur les boutons **HAUT** et **BAS** pour modifier la position de la balise (Figure 29et Tableau 1).

Figure 29 Liste du télégramme avec une nouvelle balise

7. Répétez ces étapes pour ajouter d'autres sondes / appareils et balises.
8. Appuyez le bouton**ENTRER** pour enregistrer la configuration.

Tableau 1 Liste de télégrammes—description des colonnes

Colonne	Description
1	Position des données dans l'esclave Profibus configuré (en mots de 2 octets)
	Modbus: Emplacement des données sur l'esclave Modbus configuré Cet esclave contient les registres de stockage à partir de 40001. Exemple : "0" indique Registre 40001 et "11" indique registre 40012.
2	Nom de la balise pour identifier les données configurées.
3	Type de données flot=valeur en virgule flottante int = valeurs entières sel = valeur entière issue d'une énumération ou d'une liste de sélection
4	État des données r = donnée en lecture seule r/w = lecture/écriture

Tableau 2 Registre d'erreur

Bit	Erreur	Description
0	Calibration error (Erreur d'étalonnage)	Détection d'un étalonnage défectueux
1	Electronic settings error (Erreur de réglage électronique)	Étalonnage/réglages électroniques défectueux
2	Erreur de nettoyage	Détection d'erreur dans le cycle de nettoyage
3	Erreur de module de mesure	Détection d'erreur dans le module de mesure
4	System initialization (Initialisation du système)	Détection d''incohérences au niveau des paramètres, restaurer les paramètres d'usine
5	Erreur de hardware	Détection de matériel défectueux
6	Erreur de communication interne	Détection d'erreur de communication interne
7	Erreur d'humidité	Détection d'humidité excessive
8	Excessive temperature (Température excessive)	Détection de température excessive
9		
10	Sample feed warning (Alerte sur échantillon en entrée)	Détection d'erreur sur l'échantillon en entrée
11	Alerte d'étalonnage douteux	Précision de l'étalonnage précédent inadéquate
12	Alerte de mesure douteuse	Précision de la mesure précédente inadéquate ou hors de la plage admise
13	Alerte de sécurité	Détection d'erreur sur l'équipement de sécurité
14	Alerte de réactif	Alerte de réactif, détection du niveau de remplissage < min par exemple
15	Service request warning (Alerte de requête de service)	Détection d'une requête de service

Tableau 3 Registre de statut

Bit	Statut 1	Description
0	Calibration activated (Étalonnage activé)	Étalonnage en cours, valeur de la mesure non mise à jour
1	Cleaning activated (Nettoyage activé)	Nettoyage en cours, valeur de la mesure non mise à jour
2	Service mode activated (Mode service activé)	Appareil en mode "Service", valeur de la mesure non mise à jour
3	General error message (Message d'erreur générale)	Erreur générale détectée, lire le texte d'erreur pour plus de détails
4	Measurement value channel 0, poor quality (Mesure du canal 0, mauvaise qualité)	La précision de la mesure ne respecte pas les limites spécifiées
5	Measurement value channel 0, range short-fall (Mesure du canal 0, inférieure à la plage)	La valeur de la mesure est inférieure à la plage spécifiée
6	Measurement value channel 0, range exceeded (Mesure du canal 0, supérieure à la plage)	La valeur de la mesure excède la plage spécifiée
7	Measurement value channel 1, poor quality (Mesure du canal 1, mauvaise qualité)	La précision de la mesure ne respecte pas les limites spécifiées
8	Measurement value channel 1, range short-fall (Mesure du canal 1, inférieure à la plage)	La valeur de la mesure est inférieure à la plage spécifiée
9	Measurement value channel 1, range exceeded (Mesure du canal 1, supérieure à la plage)	La valeur de la mesure excède la plage spécifiée
10	Measurement value channel 2, poor quality (Mesure du canal 2, mauvaise qualité)	La précision de la mesure ne respecte pas les limites spécifiées
11	Measurement value channel 2, range short-fall (Mesure du canal 2, inférieure à la plage)	La valeur de la mesure est inférieure à la plage spécifiée
12	Measurement value channel 2, range exceeded (Mesure du canal 2, supérieure à la plage)	La valeur de la mesure excède la plage spécifiée
13	Measurement value channel 3, poor quality (Mesure du canal 3, mauvaise qualité)	La précision de la mesure ne respecte pas les limites spécifiées
14	Measurement value channel 3, range short-fall (Mesure du canal 3, inférieure à la plage)	La valeur de la mesure est inférieure à la plage spécifiée
15	Measurement value channel 3, range exceeded (Mesure du canal 3, supérieure à la plage)	La valeur de la mesure excède la plage spécifiée

3.10.5 Exemple de configuration du système à l'aide d'Unity Pro

Remarque : *Le logiciel d'Unity Pro de Schneider Electric est le logiciel commun d'exploitation, de débogage et de programmation IEC 61131-3 pour les systèmes Modicon M340™, Premium™ et Quantum™. Pour plus de détails, veuillez contacter l'assistance locale de Schneider Electric.*

Les Figure 30 à Figure 32 montrent comment effectuer la configuration d'un système à l'aide du logiciel Unity Pro pour PLC.

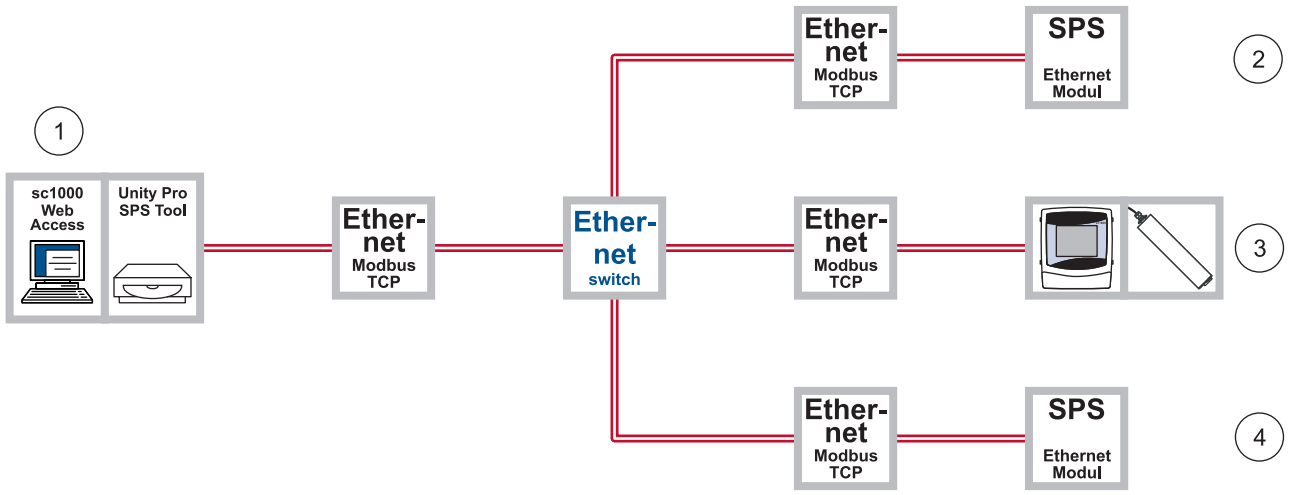

Figure 30 Présentation de la configuration système avec Unity Pro

1	Station technique avec sc1000 WebAccess	**3**	Transmetteur sc1000 avec sonde
2	Par ex., Telemecanique TSX Premium P57 4634M	**4**	Par ex., Telemecanique Modicon Quantum CPU 65160

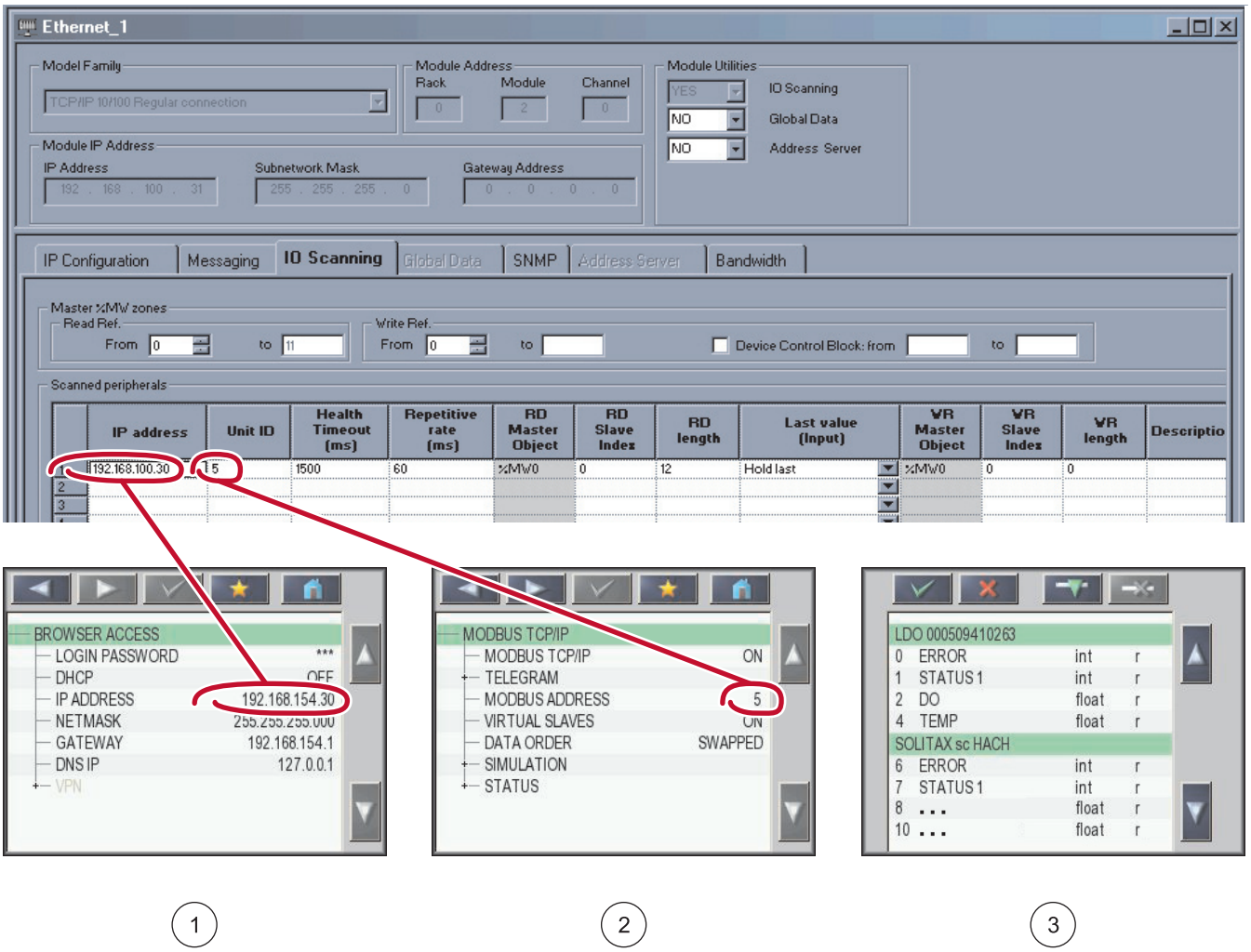

Figure 31 Connexion du transmetteur sc1000 à l'aide de Unity Pro
(La langue des options de menu dépend des paramètres de langue)

1	Adresse IP	**3**	Contenu du télégramme
2	Adresse Modbus		

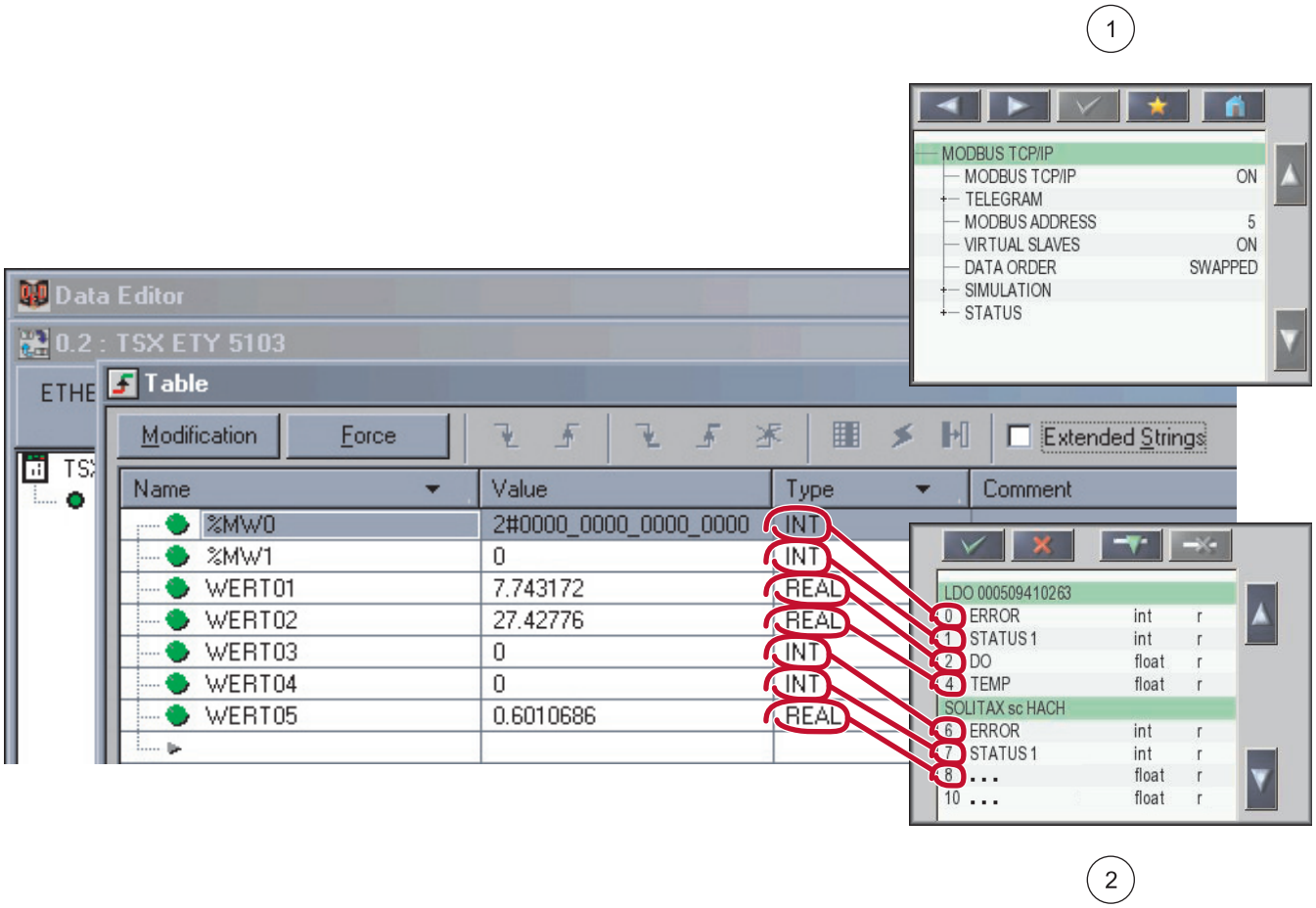

Figure 32 Configuration du système à l'aide de Unity Pro

1	Ordre des données permuté	**2**	Telemecanique TSX Premium P57 4634M démarre avec écart 0 Telemecanique Modicon Quantum CPU 65160 avec écart 1

Chapitre 4 Messages d’erreur

4.1 GSM/GPRS

Voir les messages d'erreur du GSM dans le manuel du transmetteur sc1000.

Aucun message de statut n'est donné pour le GPRS.

4.2 Tunnel VPN

CONFIG. SYSTÈME
ACCÈS NAVIGATEUR
VPN

Plusieurs messages de statut sont relatifs à l'établissement de la connexion avec le tunnel VPN. Ceux-ci sont affichés sous **CONFIG. SYSTÈME>ACCÈS NAVIGATEUR**>**VPN**:

- INACTIF : le client VPN est désactivé
- LIAISON : le client VPN tente d'établir une connexion avec le serveur.
- CONNEXION : la connexion avec le serveur a été établie.
- INTERRUPTION : la connexion avec le serveur a été interrompue. Ce statut s'affiche quand la connexion Internet s'interrompt, le câble Ethernet est débranché ou la connexion GPRS n'est plus active. La connexion se rétablit automatiquement après avoir résolu l'erreur de communication.

4.3 Modbus TCP

CONFIG. SYSTÈME
MODBUS TCP
STATUT

Lorsqu'une erreur se produit, le serveur Modbus TCP transmet les codes d'exception correspondants au client concerné (Tableau 4).

Le dernier code d'exception transmis à chaque client s'affiche dans le menu **CONFIG. SYSTÈME>MODBUS TCP>STATUT**.

Tableau 4 Codes d'exception Modbus conformes aux spécifications Modbus

Code d'exception	Désignation
01	Fonction illicite
02	Adresse données incorrecte
03	Valeur données incorrecte
04	Longueur de la réponse illicite
05	Accusé de réception
06	Appareil esclave occupé
07	Accusé de réception négatif
08	Erreur de parité au niveau de la mémoire
10	Chemin de la passerelle non disponible
11	Échec de réponse relative à l'appareil cible de la passerelle

4.4 Notification par messagerie électronique en cas de messages d'erreur ou d'alertes

En cas d'erreur, un message électronique contenant la description de l'erreur est transmis à un ou plusieurs destinataires. Il est possible de créer un maximum de quatre jeux de configuration pour les notifications par messagerie électronique.

Chaque jeu de configuration contient les informations suivantes (non exhaustives) :

- L'adresse de messagerie du destinataire.
- Des erreurs, alertes et événements sélectionnés associés aux sondes connectées déclenchant la notification.

La possibilité de bénéficier des notifications par messagerie électronique nécessite qu'une connexion active soit établie entre le transmetteur sc1000 et l'ordinateur (GPRS ou Ethernet). Un compte de messagerie électronique doit également être configuré avec un fournisseur de messagerie électronique. Ce fournisseur doit être équipé de serveur SMTP (serveur de courrier sortant) pour la prise en charge des messages à transmettre.

4.4.1 Paramètres logiciels du transmetteur sc1000

La fonction de notification par messagerie électronique est configurée dans les menus suivants du transmetteur sc1000 :

CONFIG. SYSTÈME	
MESSAGE	
MESSAGE 1-4	
ADRESSE MESSAGERIE	Indique l'adresse de messagerie électronique à laquelle les notifications seront envoyées. Plusieurs adresses de messagerie peuvent être indiquées. Celles-ci doivent être séparées par un espace.
LANGUE	Sélectionne la langue du MESSAGE
LONGUEUR MAX. (0–100)	Indique le nombre maximum de messages de notification transmissibles par le sc1000 dans un délai de 24 heures. Le cycle de 24 heures commence selon la valeur saisie dans DÉMARRAGE.
RÉPÉTITION (0–24 h)	Indique le temps au bout duquel la transmission du message à l'adresse de messagerie spécifiée est répétée en cas d'absence d'accusé de réception des messages d'erreur.
DÉMARRAGE	Indique le temps de démarrage de la fonction de répétition. Par exemple : RÉPÉTITION = 6 h, DÉMARRAGE = 02:00: les messages non confirmés sont retransmis à 02:00, 08:00, 14:00, 20:00.
INHIBITION	Par défaut : INACTIF ACTIF : si la même erreur se produit plus d'une fois, le message de notification n'est transmis que pour la première instance.
CONFIGURATION	Indique les appareils sous surveillance et les types de message d'erreur / d'alerte transmis par messagerie électronique.
AJOUTER	Permet d'ajouter des appareils à la liste de configuration. Tous les appareils connectés sont affichés, y compris le transmetteur sc1000. Les appareils grisés figurent déjà dans la liste et ne sont pas sélectionnables.
SUPPRIMER	Supprime des appareils de la liste de configuration. Tous les appareils configurés sont affichés.
NOM D'APPAREIL 1-n	Permet de compiler individuellement les messages associés à un appareil. Les menus ERREURS et ALERTES contiennent toutes les erreurs / alertes relatives à l'appareil sélectionné. 1 = Un message est transmis à la survenance d'une erreur / alerte 0 = Un message n'est pas transmis à la survenance d'une erreur / alerte SÉLECTIONNER TOUT : Active (1) ou désactive (2) toutes les options de menu en une fois.

CONFIG. SYSTÈME	
EXPÉDITEUR	Adresse de messagerie du transmetteur sc1000. Permet d'indiquer l'expéditeur.
SERVEUR SMTP	Serveur de courrier sortant du fournisseur. Le nom du serveur est indiqué par le fournisseur du service de messagerie.
NOM D'UTILISATEUR	Nom d'utilisateur pour se connecter au serveur SMTP. Celui-ci est indiqué par le fournisseur du service de messagerie.
MOT DE PASSE	Serveur SMTP du fournisseur du service de messagerie. Le mot de passe est indiqué par le fournisseur du service de messagerie.

4.4.2 Format du message électronique

Le Tableau 5 et le Tableau 6 illustrent le format du message :

Tableau 5 Format du message électronique

Date	Heure locale	Compteur d'événements
Texte de l'alerte/erreur	ID d'erreur ou d'alerte	
Nom de l'appareil	Numéro de série de l'appareil	

Tableau 6 Exemple de format de message

2008-18-12	18:07:32	(1)
Erreur de communication	<E32>	
LDO	[405410120]	

Chapitre 5 Pièces et accessoires de rechange

Description	Cat. Nº
Carte SD, 1 Go	LZY520
Module d'affichage HACH avec modem GSM	LXV402.99.01002
Kit port Ethernet extérieur	LZY553
Câble Ethernet RJ45	LZX998
Module logiciel TCP Modbus, code licence	LZY598

Chapitre 6 Glossaire

Tableau 7 Glossaire

Terme	Explication
APN	(Access Point Name) Nom du point d'accès ; autorise l'accès à un réseau externe de données de paquets.
DHCP	(Dynamic Host Configuration Protocol) Protocole DHCP; active une connexion automatique entre un ordinateur et un réseau existant.
DNS	(Domain Name System) Système de noms de domaine
Ethernet	Couche de communication réseau physique, conformément à la norme IEEE 802.3.
Serveur IP fixe	Serveur qui affecte et gère les adresses IP fixes aux périphériques terminaux.
FTP	(File Tranfer Protocol) Protocole FTP
Passerelle	Système gérant la communication entre réseaux utilisant des protocoles différents.
GPRS	(General Packet Radio Service) Norme pour téléphonie mobile large bande, orientée paquet permettant l'envoi de données et de mail via téléphones cellulaires et ordinateurs.
GSM	(Global System for Mobile Communications) Norme pour téléphonie mobile de deuxième génération (2G).
M2M	Service machine-to-machine
Modbus TCP/IP	Protocole Modbus intégré dans le protocole TCP/IP.
PLC	(Programmable logic controller) Automate programmable
VPN	Logiciel conçu pour la connexion de périphériques fonctionnant au sein d'un réseau voisin au réseau propre, même si ces réseaux ne sont pas compatibles. Le réseau auquel sont connectés les périphériques est appelé réseau affecté.
Client VPN	Logiciel permettant au périphérique d'un réseau d'accéder à un réseau VPN secondaire, lequel offre une simulation virtuelle de la configuration du réseau affecté.
Tunnel VPN	Chiffrement supplémentaire des paquets du réseau d'origine au sein du protocole VPN afin d'éviter que les paquets ne soient interceptés et manipulés.

HACH COMPANY World Headquarters
P.O. Box 389, Loveland, CO 80539-0389 U.S.A.
Tel. (970) 669-3050
(800) 227-4224 (U.S.A. only)
Fax (970) 669-2932
orders@hach.com
www.hach.com

HACH LANGE GMBH
Willstätterstraße 11
D-40549 Düsseldorf, Germany
Tel. +49 (0) 2 11 52 88-320
Fax +49 (0) 2 11 52 88-210
info-de@hach.com
www.de.hach.com

HACH LANGE Sàrl
6, route de Compois
1222 Vésenaz
SWITZERLAND
Tel. +41 22 594 6400
Fax +41 22 594 6499

12/2018, Edition 3