DOC023.72.90143

sc1000 Controller
Enhanced Communications

HANDBUCH

12/2018, Edition 3

Inhaltsverzeichnis

Kapitel 1 Technische Daten

Änderungen vorbehalten.

sc1000 Controller Display Modul	
*GSM/*GPRS Modem	Das sc1000 Displaymodul mit integriertem GSM/GPRS Modem überträgt Daten, SMS und GPRS-Dienste in GSM Netze. Der sc1000 Controller unterstützt die GSM-Frequenzbänder: 850 / 900 / 1800 / 1900 MHz
	Unterstützt GPRS Multislot-Klasse 10 und GPRS Kodierungs-Schemas: CS-1, CS-2, CS-3 und CS-4.
Modbus TCP Server	Der Modbus TCP Server hat die "Conformance class 0". Diese Klasse unterstützt die folgenden Function Codes: Read Multiple Registers (FC 3) Write Multiple Registers (FC 16) Zusätzlich werden noch folgende Function Codes unterstützt: Read/Write Multiple Registers (FC 23) Read Device Information (FC 43/14)
Ethernet-Port	Ethernet RJ45, 10 MB/s
Garantie	
Garantie	2 Jahre

* **USA**

Der in diesem Produkt enthaltene Transmitter ist ein "Quad-Band"-Gerät, das im 850 / 900 / 1800 / 1900 MHz-Band betrieben werden kann. Die Verwendung dieses Geräts ist nicht für den Betrieb im GSM Band 900 / 1800 MHz in den USA und Kanada zugelassen.
Dieser Transmitter ist für den Einsatz an festen oder mobilen Standorten zugelassen.
Mit diesem Produkt verwendete Antennen müssen im Betrieb mindestens 20 cm (7,9 in) von allen Personen entfernt sein und dürfen nicht mit anderen Sendeantenne zusammengeschaltet sein.
Der Nutzer ist nicht berechtigt, andere Antennen als die des Herstellers, mit mehr als 2,89 dbi für GSM 1900 und 1,33 dbi für GSM 850 Mhz, zu verwenden.

FCC ID:	QIPMC55i
IC #:	7830A-MC55i
CE per Notified Body#:	CE 0681

* **EUROPA**

VORSICHT

- Das Gerät darf nicht in Krankenhäusern und/oder in der Nähe von medizinischen Geräten (z. B. Herzschrittmacher oder Hörgeräte) betrieben werden.
- Das Gerät darf nicht in gefährlichen Umgebungen verwendet werden.
- Das Gerät darf nicht in der Nähe von brennbaren Gasen, Dämpfen oder Stäuben betrieben werden.
- Das Gerät darf nicht in der Nähe von brandgefährdeten Bereichen (z. B. Tankstellen, Brennstofflagerstätten, Chemiewerke und Sprengstätten) betrieben werden.
- Das Gerät kann Störungen verursachen, wenn es sich in der Nähe von Fernsehgeräten, Radios oder Computern befindet.
- Das Gerät darf weder starken Vibrationen noch Stößen ausgesetzt werden.
- Die Nutzung von GSM-Diensten (z. B. SMS-Nachrichten, Datenkommunikation und GPRS) kann zu zusätzlichen Kosten durch den Service-Provider führen. Der Benutzer ist allein verantwortlich für hierdurch entstehende Schäden und Kosten.
- Bei nicht bestimmungsgemäßer Verwendung übernimmt der Hersteller keine Garantie.
- Eine Änderung des Geräts ist unzulässig und führt zum Verlust der Betriebsgenehmigung.
- Zusätzlich zu diesen Hinweisen sind alle Richtlinien des Landes zu befolgen, in dem das Gerät in Betrieb genommen wird.

Kapitel 2 Allgemeine Informationen

2.1 Sicherheitshinweise

Lesen Sie das Handbuch sorgfältig und vollständig bevor Sie Software installieren. Weitere Informationen über den sc1000 Controller sind im Handbuch zum sc1000 Controller enthalten.

2.2 Produktüberblick

Hinweis

Die Sicherheit von Netzwerk und Zugangspunkt liegt in der Verantwortung des Kunden, der das drahtlose Gerät verwendet. Der Hersteller ist nicht haftbar für Schäden, die durch einen Eingriff oder eine Verletzung der Netzwerksicherheit verursacht wurden, einschließlich aber nicht nur begrenzt auf indirekte, spezielle, zufällige oder Folgeschäden.

Der sc1000 Controller kann über eine Internetverbindung mit anderen Internetteilnehmern kommunizieren. Die Kommunikationsschnittstelle am sc1000 ist entweder der Ethernet Port (kabelgebunden) oder das GSM/GPRS Modem (kabellos).

Die kabelgebundene Verbindung über den Ethernet Port (früher Service Port) erfolgt über ein LAN-Kabel. Bei Bedarf wird der Ethernet Port am sc1000 Controller im Außenbereich durch das optionale sc1000 Outdoor Ethernet Port Kit zusätzlich geschützt. sc1000 Controller sind auch oft an Orten installiert, die für einen kabelgebundenen Anschluss an ein Netzwerk oder an das Internet ungeeignet sind. Um Daten zu sammeln und den sc1000 Controller aus der Ferne zu steuern, bieten sich Mobilfunknetze an. Diese sogenannte M2M-Lösung (M2M=Machine to Machine) bindet den sc1000 Controller über ein GPRS-Mobilfunknetz in ein lokales IT-Netz ein.

Die sichere Kommunikation zwischen sc1000 Controller und IT-Netz wird durch einen VPN-Tunnel realisiert.

Ist die LAN- oder GPRS-Verbindung eingerichtet, sind keine weiteren Bedienschritte am sc1000 Controller notwendig.

Konfiguriert wird der sc1000 Controller über einen Internet-Browser an einem Computer. Über den Internet-Browser können desweiteren Datenprotokolle heruntergeladen und Softwareaktualisierungen hochgeladen werden.

Das optionale Modbus TCP Softwaremodul erlaubt die direkte Integration des sc1000 Controllers in SPS-Systeme (SPS=Speicherprogrammierbare Steuerung). SPS-Systeme erfassen die vom sc1000 Controller gemessenen Daten und verarbeiten diese Daten weiter.

Hinweis:

Kapitel 3 Installation

3.1 Benutzeranforderungen

Sämtliche Installationen und Arbeiten am Computer und am sc1000 Controller dürfen nur von geschultem Fachpersonal vorgenommen werden. Benutzer müssen über fundierte Kenntnisse der Netzwerktechnik und der Computertechnik verfügen.

3.2 Allgemeine Voraussetzungen für die Fernwartung

Alle jeweils genannten Voraussetzungen müssen erfüllt sein, da sonst Fernwartung und/oder Browser-Zugriff auf den sc1000 Controller nicht möglich sind und Schäden am System auftreten können.

3.2.1 Voraussetzungen am sc1000 Controller

Alle im Handbuch des sc1000 Controller genannten Sicherheitshinweise und Anweisungen müssen unbedingt eingehalten werden.

Weitere Voraussetzungen sind:

Browser-Passwort vergeben
Damit der Zugriff auf den sc1000 Controller mit einem Internet-Browser funktioniert, ist die Vergabe eines Browser-Passwort vor dem Einrichten der Ethernet-/GPRS-Verbindung notwendig.

SYSTEM SETUP
BROWSER ZUGANG
PASSWORT

1. Im Hauptmenü des sc1000 Controllers **SYSTEM SETUP>BROWSER ZUGANG> PASSWORT** wählen.
2. Ein Browser-Passwort vergeben.

GPRS-Verfügbarkeit am Standort prüfen
Soll über GPRS auf den sc1000 Controller zugegriffen werden, muss GPRS am Standort des sc1000 Controllers verfügbar sein.

Hinweis: *GPRS-Verfügbarkeit am Standort des sc1000 Controllers muss gewährleistet sein.*

Modbus TCP-Softwaremodul installieren
Wird die Modbus TCP-Unterstützung genutzt, muss zusätzlich das Modbus TCP-Softwaremodul mit Freischaltcode lizenziert werden.

3.2.2 Voraussetzungen am Computer

Der Computer, der mit dem sc1000 Controller verbunden werden soll, muss eine funktionierende Internetverbindung aufbauen können.

Es müssen folgende Voraussetzungen am Computer erfüllt sein:

- Das Benutzerkonto, mit dem sich der Benutzer am Computer anmeldet, muss über Administratorrechte verfügen
- Ein Internet-Browser muss installiert sein
- Zugang zum Internet muss vorhanden sein

3.2.3 Lieferumfang

Zum Lieferumfang gehören folgende Komponenten:

- Speziell an den sc1000 Controller angepasste VPN-Client-Software
- Handbuch

Hinweis: *Sollte eines der aufgelisteten Teile fehlen oder defekt sein, wenden Sie sich bitte sofort an den Hersteller oder die zuständige Vertretung.*

3.3 Überblick über die verschiedenen Verbindungsmöglichkeiten

Es gibt mehrere Wege, eine Verbindung zwischen dem sc1000 Controller und einem Computer herzustellen. Exemplarisch vorgestellt werden hier (Abbildung 1 und Abbildung 2):

- Verbindungen über Ethernet
- Verbindungen über GPRS

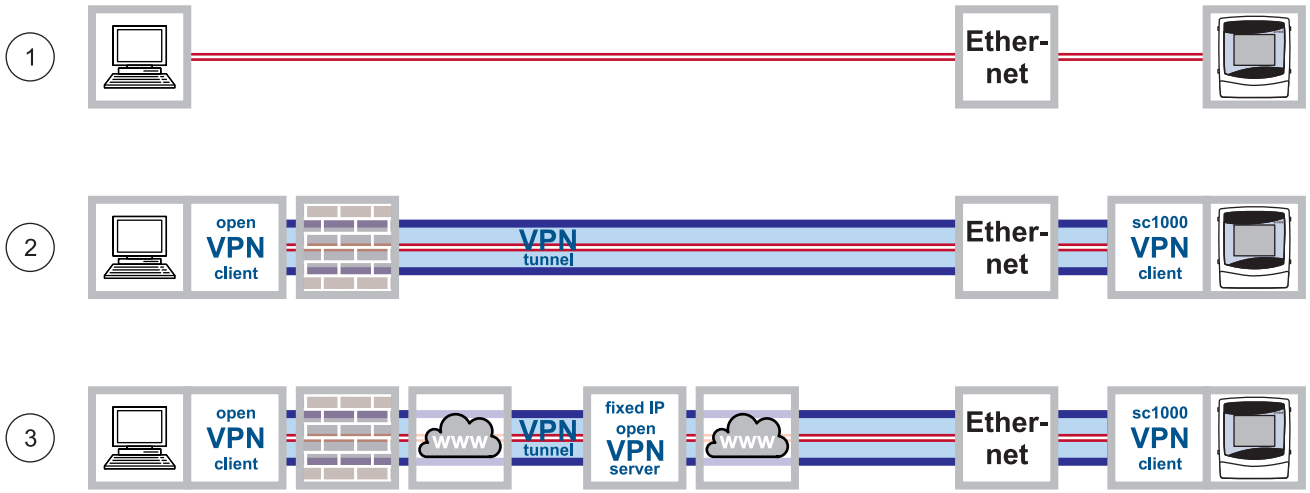

Abbildung 1 Übersicht über die Ethernet-Verbindungsmöglichkeiten

1	Einfache Ethernet-Verbindung
2	Ethernet-Verbindung mit einem sicheren VPN-Tunnel
3	Ethernet-Verbindung über einen Fixed-IP VPN-Server

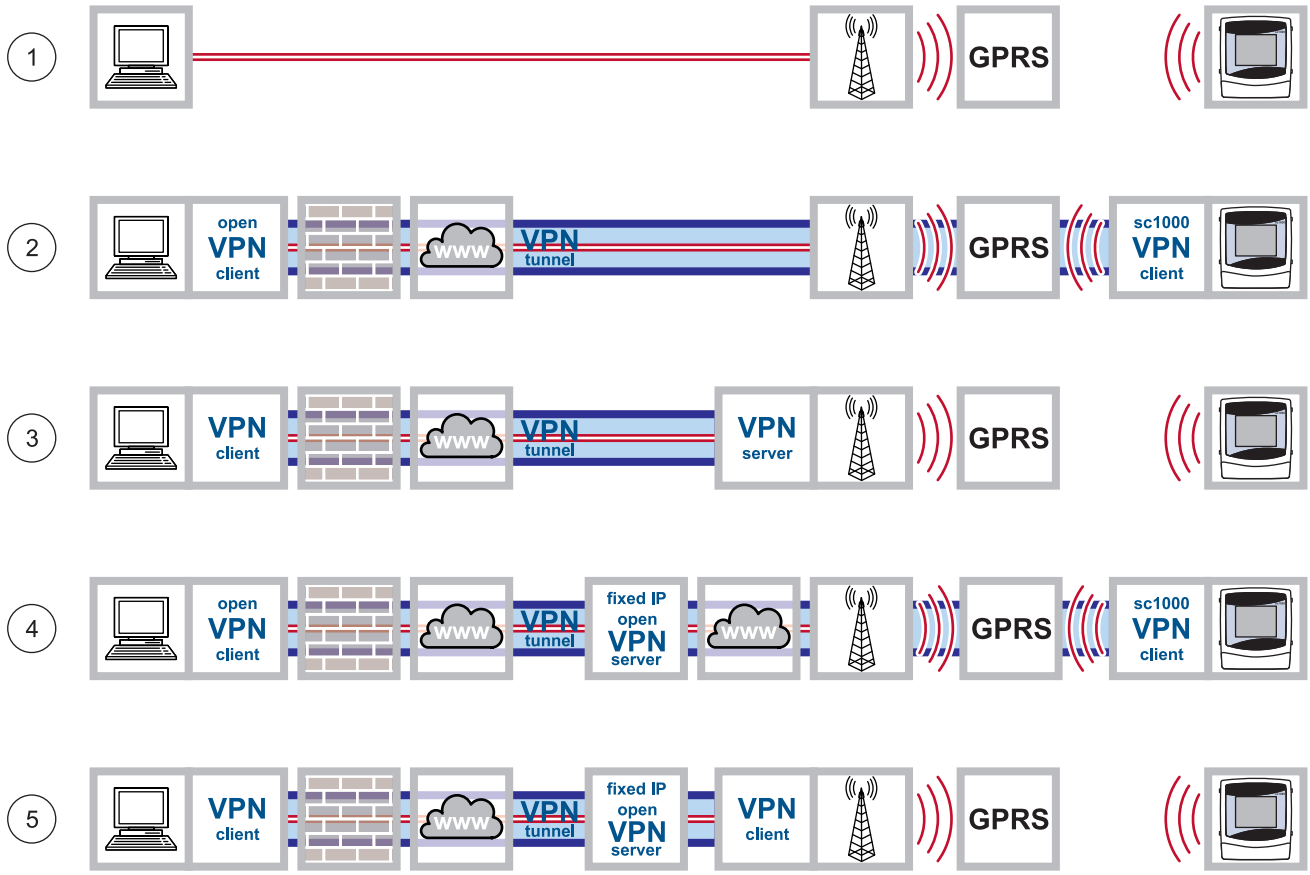

Abbildung 2 Übersicht über die GPRS-Verbindungsmöglichkeiten

1	GPRS-Verbindung ohne VPN-Tunnel (nur möglich, wenn ein CDA-Konto beim Mobilfunkanbieter vorhanden ist)
2	GPRS-Verbindung mit einem sicheren VPN-Tunnel
3	GPRS-Verbindung über einen VPN-Server des Mobilfunkanbieters
4	GPRS-Verbindung über einen Fixed-IP VPN-Server
5	GPRS-Verbindung über Fixed IP-Dienst und VPN-Server des Mobilfunkanbieters

3.4 Ethernet-Verbindung herstellen

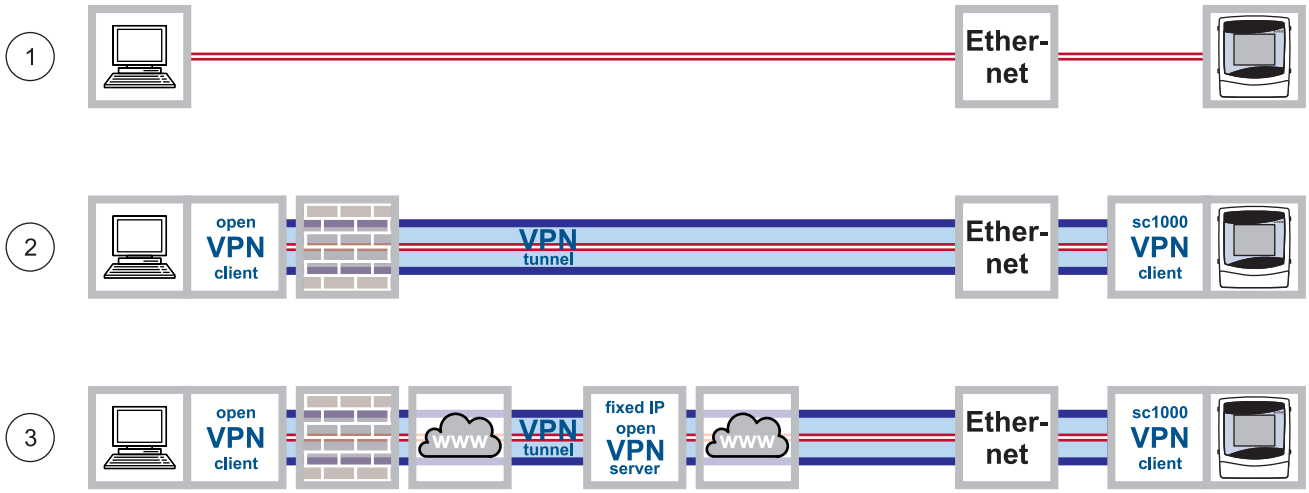

Abbildung 3 Ethernet-Verbindungen

1	Einfache Ethernet-Verbindung
2	Ethernet-Verbindung mit einem sicheren VPN-Tunnel
3	Ethernet-Verbindung mit einen Fixed-IP VPN-Server

Die Ethernet-Verbindung ist die kabelgebundene Verbindung zwischen einem Computer und dem Ethernet Port des sc1000 Controllers. Der Ethernet Port des sc1000 Controllers ist ein 10 MB/s Ethernet-Anschluss am Display Modul.

Eine direkte Verbindung zwischen Computer und sc1000 Controller wird folgendermaßen hergestellt:

Über eine einfache Ethernet-Verbindung
(Abbildung 3, Punkt 1)

Anwendungsbereich: Der sc1000 Controller ist in das Firmennetzwerk eingebunden oder zu Testzwecken.

Über eine Ethernet-Verbindung mit einem sicheren VPN-Tunnel
(Abbildung 3, Punkt 2)

Anwendungsbereich: Der sc1000 Controller befindet sich außerhalb des Firmennetzwerks.

Über eine Ethernet-Verbindung mit einen Fixed-IP VPN-Server
(Abbildung 3, Punkt 3)

Anwendungsbereich: Der sc1000 Controller ist über das Internet von jedem Standort mit einer festen IP-Adresse ansprechbar.

3.4.1 Einfache Ethernet-Verbindung herstellen

Abbildung 4 Einfache Ethernet-Verbindung

Wenn sich der sc1000 Controller innerhalb des Firmennetzwerks befindet oder zu Testzwecken, ist eine einfache Ethernet-Verbindung ohne VPN zwischen beiden Geräten sinnvoll (Abbildung 4).

1. Den Computer mit dem Firmennetzwerk über ein Ethernet-Kabel verbinden und sicherstellen, dass die Internet-Verbindung fehlerfrei funktioniert. Zum Test verschiedene Internetseiten aufrufen.
2. Den sc1000 Controller über ein Ethernet-Kabel am Ethernet Port mit dem Netzwerk verbinden (Abbildung 5).

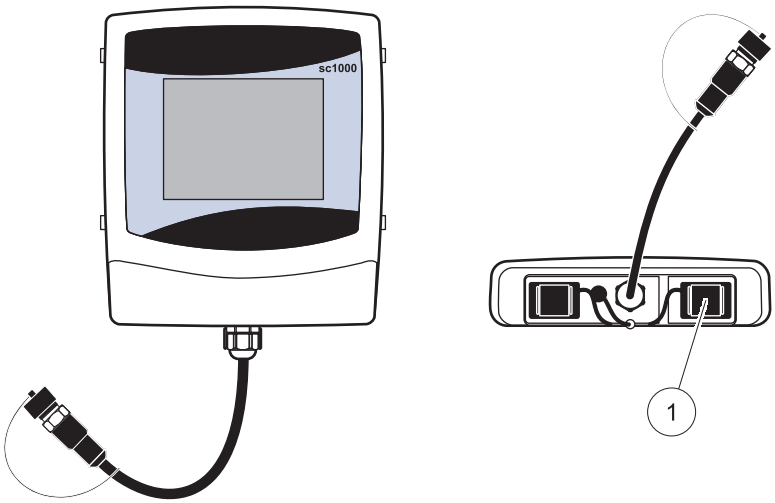

Abbildung 5 Ethernet Port am Display Modul des sc1000 Controllers

1	Ethernet Port (früher Service Port) am Display Modul

3. Im Hauptmenü des sc1000 Controllers **SYSTEM SETUP>BROWSER ZUGANG** wählen, um die Netzwerkeinstellungen zu setzen.
4. Für eine manuelle Konfiguration der Netzwerkeinstellungen folgende Einstellungen von der IT-Abteilung erfragen:
   - IP-ADRESSE
   - NETMASK
   - DNS-IP
   - GATEWAY
5. Für eine automatische Konfiguration folgende Einstellung setzen:
   - DHCP: EIN

SYSTEM SETUP
BROWSER ZUGANG
IP-ADRESSE
NETMASK
DNS-IP
GATEWAY
DHCP

6. Am Computer einen Internet-Browser starten. In der Adresszeile die IP-Adresse des sc1000 eintragen (siehe Punkt 3.). Es erscheint das Anmeldefenster des sc1000 Controllers (Abbildung 6).
7. Das Browser-Passwort eingeben (siehe Abbildung 6 und Kapitel 3.4.1, Seite 13).

Hinweis: *Ein Browser-Passwort ist zwingend erforderlich für den Internet-Browser Zugriff auf den sc1000 Controller.*

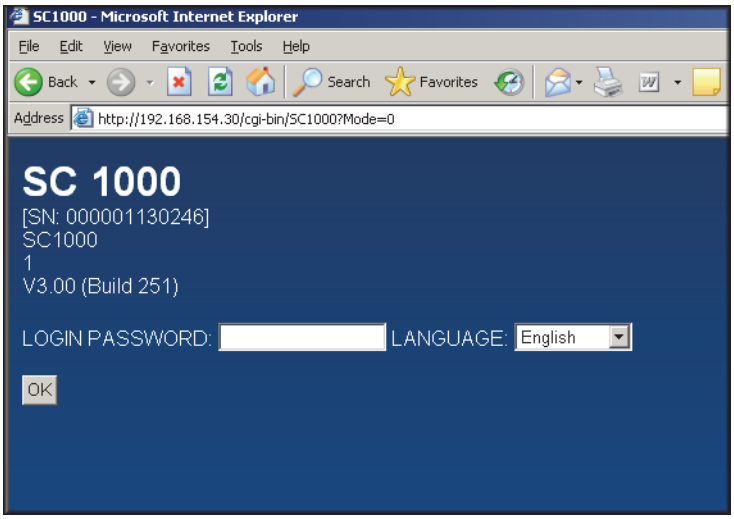

Abbildung 6 Anmeldefenster des sc1000 Controllers

Die Ethernet-Verbindung zwischen Ihrem Computer und dem sc1000 Controller ist hergestellt.

3.4.2 Ethernet-Verbindung mit einem sicheren VPN-Tunnel herstellen

Abbildung 7 Ethernet-Verbindung mit einem sicheren VPN-Tunnel

Die Ethernet-Verbindung mit einem VPN-Tunnel ist notwendig, wenn sich der sc1000 Controller außerhalb des Firmennetzes befindet (Abbildung 7). Wie der VPN-Tunnel eingerichtet wird, steht in Kapitel 3.5, Seite 15.

3.5 VPN-Tunnel installieren

Wenn sich der sc1000 Controller **außerhalb des Firmennetzwerks** befindet, muss zwischen Computer und sc1000 Controller ein Virtual Private Network (VPN) installiert werden. Das VPN sorgt dafür, dass Computer und sc1000 in einem vor nichtautorisierten Personen/Zugriffen geschützten Kanal (Tunnel) kommunizieren können.

Windows 2000 sowie Windows XP bieten bereits einen eingebauten VPN-Server. Dieser erlaubt aber immer nur eine einzige Verbindung zwischen einem sc1000 Controller und dem Computer. Für mehrere Verbindungen gleichzeitig, benötigt man einen eigenständigen VPN-Server.

Je nach Konzeption der VPN-Verbindung stellt ein Mobilfunk- oder Internet-Anbieter oder die IT-Abteilung einen VPN-Server zur Verfügung. Das Konzept muss vor der Installation sorgfältig geplant werden.

3.5.1 Voraussetzungen am sc1000 Controller

Der sc1000 Controller benötigt ein spezielles VPN-Softwarepaket, das beim Hersteller bezogen werden muss. Es gibt mehrere Möglichkeiten, das VPN-Softwarepaket am sc1000 Controller zu installieren:

- mit einer SD-Speicherkarte
- über den Internet-Browser
- über den Windows Explorer/FTP-Datentransfer

3.5.2 Voraussetzungen am Computer

Am Computer muss die kostenlose VPN-Software OpenVPN installiert sein (siehe Kapitel 3.5.4, Seite 17).

3.5.3 Am sc1000 Controller: VPN-Client mit einer SD-Speicherkarte installieren

Das Displaymodul des sc1000 Controllers besitzt einen eingebauten Steckplatz für eine SD-Speicherkarte. Die SD-Speicherkarte wird u. a. dazu genutzt, um die sc1000 Controller Software zu aktualisieren. Weitere Informationen zum EInsatz der SD-Speicherkarte stehen im sc1000 Controller Handbuch.

Eine SD-Speicherkarte, die die speziell angepasste VPN-Client-Software für den sc1000 Controller bereits enthält, kann beim Hersteller bezogen werden (siehe Kapitel 5, Seite 45).

Hinweis: *Zur Installation nur SD-Speicherkarten mit einer maximalen Speichergröße von 1 Gigabyte verwenden.*

1. Auf der SD-Speicherkarte folgende Verzeichnisse anlegen (wenn noch nicht vorhanden):
   - DEV_SETTINGS
   - SC1000
   - UPDATE
2. Folgende Dateien auf die SD-Speicherkarte in das Verzeichnis UPDATE kopieren:

Vom Hersteller:

- Speziell angepasste VPN-Client-Software
  (wenn noch nicht auf der SD-Karte vorhanden)

Vom Anbieter des VPN-Servers:

- Konfigurationsdatei (z. B. Datei mit der Erweiterung .ovn)
- Zertifikat (z. B. Datei mit der Erweiterung .crt)
- Schlüsseldatei (z. B. Datei mit der Erweiterung .key)

3. sc1000 Controller starten.
4. Abdeckung des SD-Kartenschachts am Displaymodul des sc1000 Controllers entfernen (Abbildung 8).

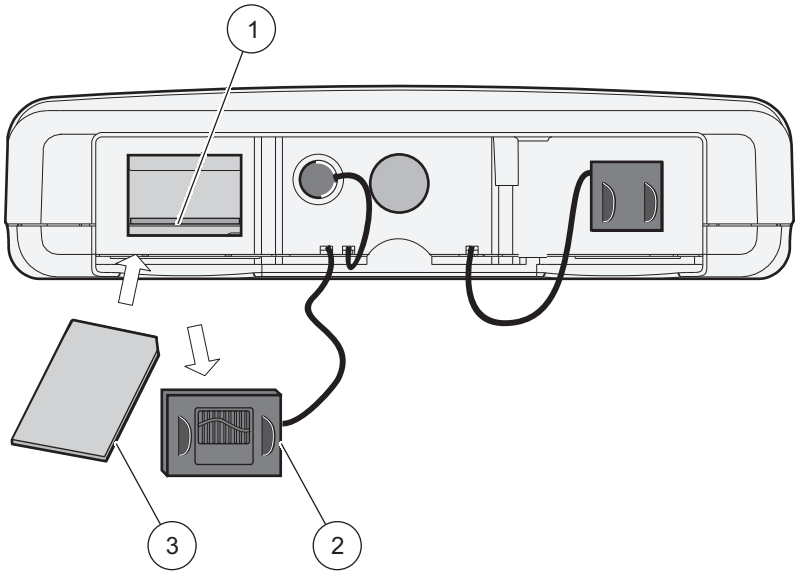

Abbildung 8 Unterseite des Display Moduls

1	SD-Kartenschacht	**3**	SD-Speicherkarte
2	Abdeckung des SD-Kartenschachts		

5. Die SD-Speicherkarte in den SD-Kartenschacht des sc1000 Controllers stecken.
6. Abdeckung des SD-Kartenschachts montieren.

SYSTEM SETUP
SPEICHERKARTE
SOFTWARE AKTUALISIERUNG

7. Installation des VPN-Clients über **SYSTEM SETUP>SD KARTE> SOFTWARE AKTUALISIERUNG** starten.

Der sc1000 Controller installiert und konfiguriert selbstständig die VPN-Software und muss anschließend neu gestartet werden.

3.5.4 Am sc1000 Controller: VPN-Client über Internet-Browser installieren

Hinweis: *Der Internet-Browser am Computer muss das FTP-Protokoll unterstützen. Microsoft Internet Explorer 7 unterstützt das FTP-Protokoll nur bedingt.*

1. Sicherstellen, dass die Ethernet-Verbindung zwischen dem sc1000 Controller und dem Computer funktioniert.
2. Sicherstellen, dass der benutzte Internet-Browser das FTP-Protokoll unterstützt.
3. Den Internet-Browser des Computers starten und die IP-Adresse des sc1000 Controllers in der Adresszeile des Internet-Browser eingeben (Abbildung 9).
4. Das Anmeldefenster des sc1000 Controllers erscheint.

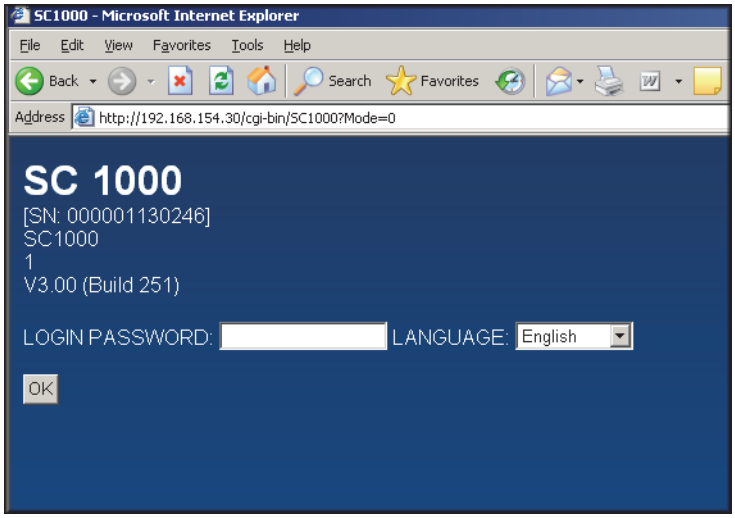

Abbildung 9 Anmeldefenster des sc1000 Controllers

SYSTEM SETUP
BROWSER ZUGANG
IP ADRESSE

Die IP-Adresse des sc1000 Controllers ist zu finden unter **SYSTEM SETUP>BROWSER ZUGANG>IP ADRESSE**.

5. Das Browser-Passwort eingeben (siehe 3.4.1, Seite 13).

   Hinweis: *Ein Browser-Passwort ist zwingend erforderlich für den Internet-Browser Zugriff auf den sc1000 Controller.*

6. Unter NAVIGATION auf die Schaltfläche **UPDATE** klicken (Abbildung 10).

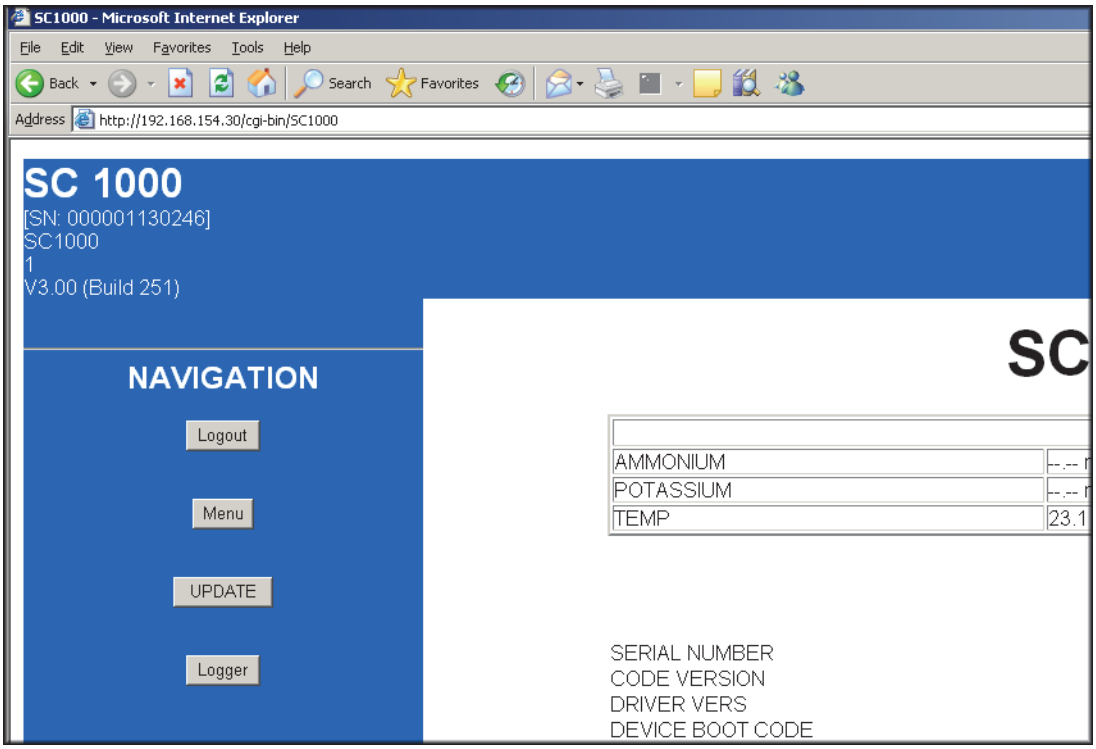

Abbildung 10 Schaltfläche **UPDATE**

7. Auf den Link **UPDATE DISPLAY-MODUL** klicken (Abbildung 11).

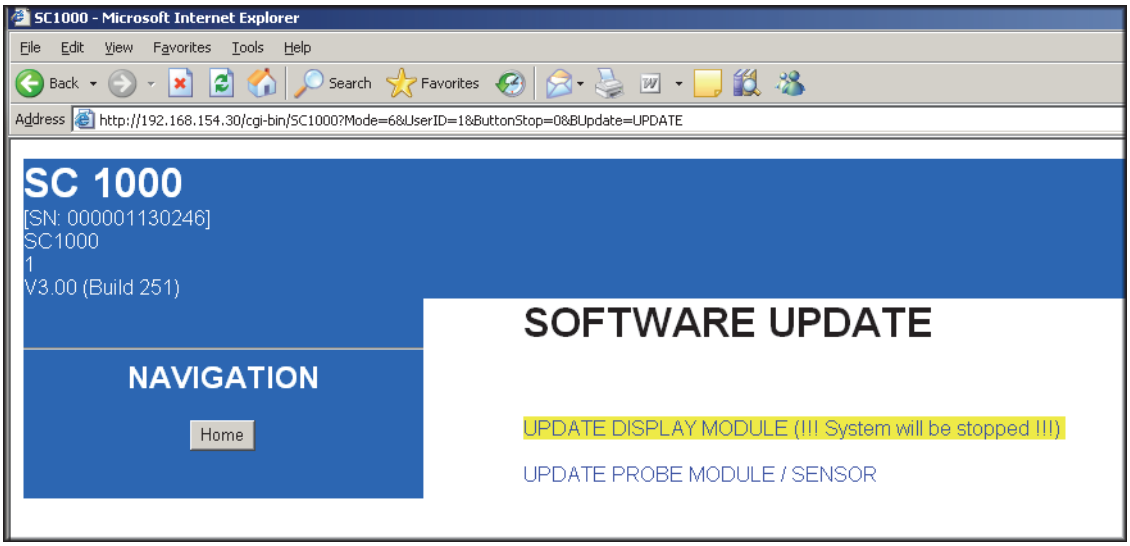

Abbildung 11 Link Update Display-Modul

8. Es erscheint das Fenster Dateien in sc1000 laden und die Dateimanager-Oberfläche (z.B. Microsoft Windows Explorer) wird in das Browser-Fenster eingebunden.

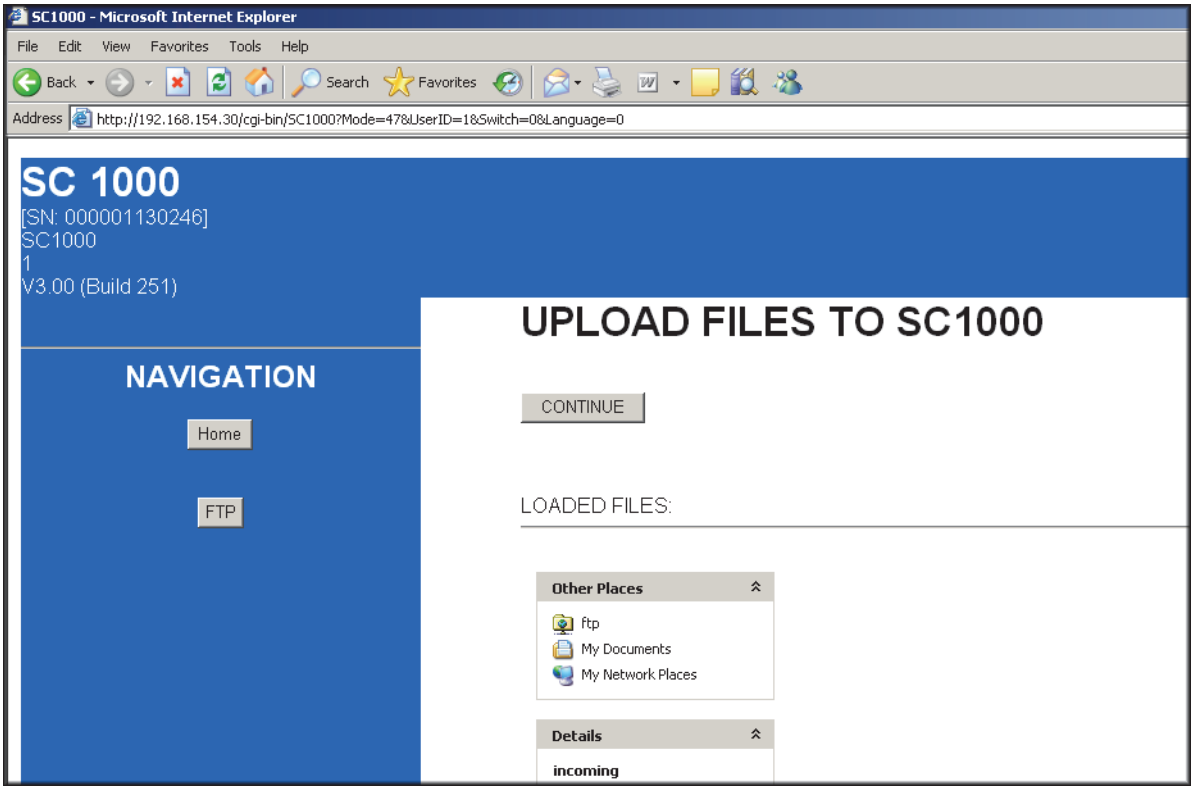

Abbildung 12 Dateien in den sc1000 Controller laden

9. Im Browser-Fenster unter GELADENE DATEIEN auf **ftp** klicken.
10. Dateimanager (z. B. Microsoft Windows Explorer) starten und folgende Dateien auswählen. Die Dateien müssen sich auf der Festplatte, im Netzwerk oder auf einem mobilen Datenträger befinden:

Vom Hersteller:

- Speziell angepasste VPN-Client-Software

Vom Anbieter des VPN-Servers:

- Konfigurationsdatei (z. B. Datei mit der Erweiterung .ovn)
- Zertifikat (z. B. Datei mit der Erweiterung .crt)
- Schlüsseldatei (z. B. Datei mit der Erweiterung .key)

11. Die Dateien kopieren und in das Verzeichnis **incoming** im Internet Browser einfügen (Abbildung 13).

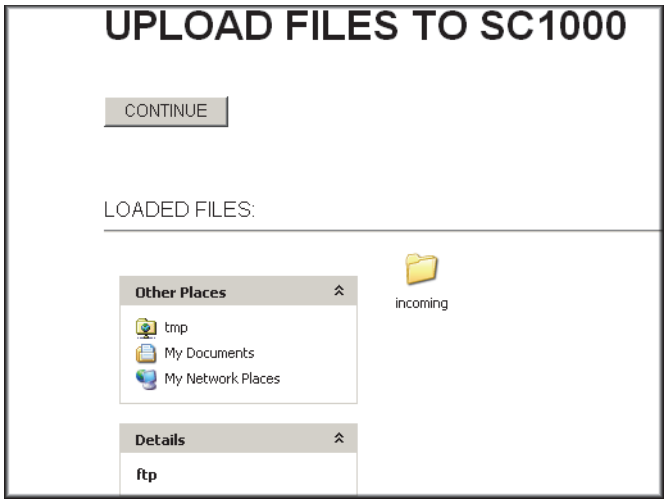

Abbildung 13 Dateie übertragen

12. Auf die Schaltfläche **WEITER** drücken
13. Das Update im Fenster des sc1000 Controllers bestätigen.

    Der sc1000 Controller installiert und konfiguriert jetzt selbstständig die Software und muss neu gestartet werden.

3.5.5 Am sc1000 Controller: VPN-Client über den Windows Explorer/FTP installieren

Wenn der Internet-Browser das FTP-Protokoll nicht unterstützt, bietet sich als Alternative der Datentransfer per FTP über den Windows Explorer an.

1. Internet-Browser schließen (wenn nicht bereits geschlossen).
2. Windows Explorer starten.
3. In die Adresszeile des Windows Explorers folgende FTP-Adresse eintragen:

   ftp://<*IP-Adresse sc1000 Controllers*>/tmp/incoming

   Beispiel: ftp://192.168.154.30/tmp/incoming
4. FTP-Verbindung mit der **EINGABE**-Taste bestätigen.
5. Dateimanager (z. B. Microsoft Windows Explorer) starten und folgende Dateien auswählen. Die Dateien müssen sich auf der Festplatte, im Netzwerk oder auf einem mobilen Datenträger befinden:

Vom Hersteller:

- Speziell angepasste VPN-Client-Software

Vom Anbieter des VPN-Servers:

- Konfigurationsdatei (z. B. Datei mit der Erweiterung .ovn)
- Zertifikat (z. B. Datei mit der Erweiterung .crt)
- Schlüsseldatei (z. B. Datei mit der Erweiterung .key)

6. Ausgewählte Dateien in das FTP-Verzeichnis <*IP-Adresse sc1000 Controller*>**\tmp\incoming** kopieren (Abbildung 14).

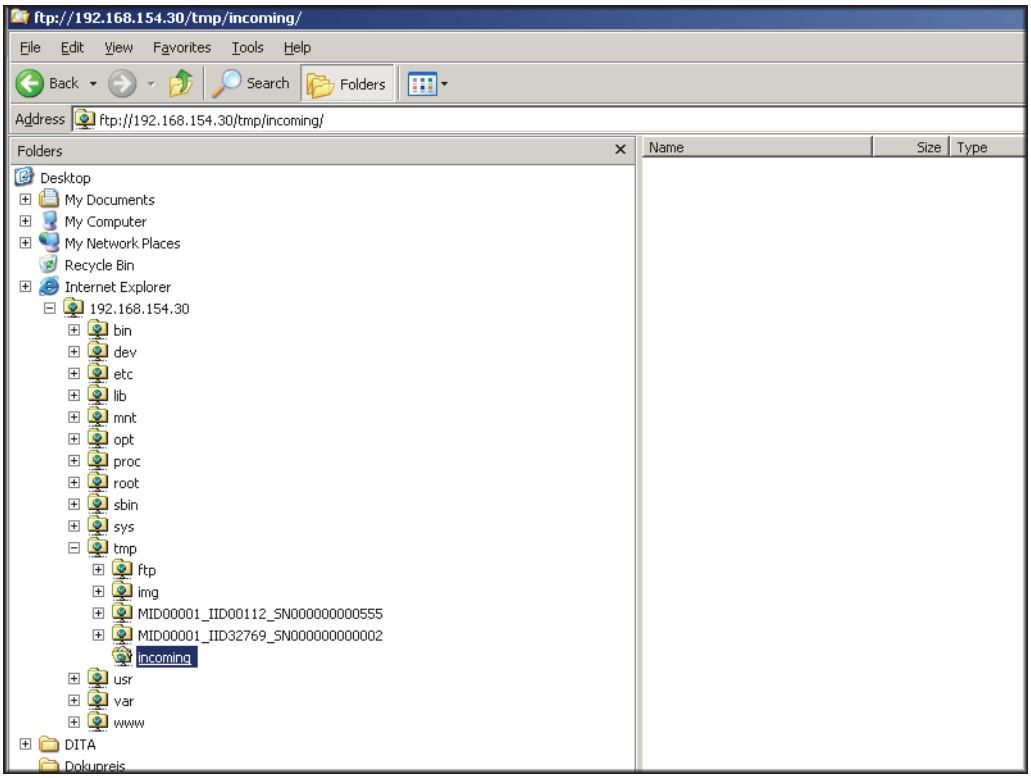

Abbildung 14 FTP-Datentransfer über Microsoft Windows Explorer

7. Den Internet-Browser des Computers starten und die IP-Adresse des sc1000 Controllers in der Adresszeile des Internet-Browsers eingeben.

   Das Anmeldefenster des sc1000 Controllers erscheint.

8. Das Browser-Passwort eingeben.

9. Auf die Schaltfläche **UPDATE** klicken.

10. Auf den Link **UPDATE DISPLAY MODUL** klicken.

11. Das Update im Fenster des sc1000 Controllers bestätigen.

Der sc1000 Controller installiert und konfiguriert jetzt selbstständig die Software und muss neu gestartet werden.

3.5.6 Am sc1000 Controller: VPN-Installation überprüfen

1. Den Internet-Browser des Computers starten und die IP-Adresse des sc1000 Controllers in die Adresszeile eingeben.
2. Das Browser-Passwort eingeben (siehe 3.4.1, Seite 13).

SYSTEM SETUP
BROWSER ZUGANG
VPN
VPN

3. Sicherstellen, dass im Fenster **SYSTEM SETUP>BROWSER ZUGANG>VPN** der Eintrag **VPN** auf **LAN** steht.
4. Sicherstellen, dass im Fenster **SYSTEM SETUP>BROWSER ZUGANG** der Eintrag **VPN** auf **VERBINDUNG** steht.

SYSTEM SETUP
BROWSER ZUGANG
VPN
KONFIG DATEI

5. Sicherstellen, dass im Fenster **SYSTEM SETUP>BROWSER ZUGANG> VPN>KONFIG DATEI** kein Eintrag rot markiert ist.

   Rote Einträge markieren Fehler (siehe Kapitel 4, Seite 41).

   Hellgraue Einträge markieren Informationen, die schon in der Konfiguration vorliegen und ignoriert werden können.
6. Wenn vom Anbieter des VPN-Servers gefordert, **USERNAME** und **PASSWORT** im Fenster **SYSTEM SETUP>BROWSER ZUGANG>VPN** eintragen. Beides muss vom Anbieter des VPN-Servers geliefert werden.

3.5.7 Am Computer: VPN-Client installieren

Um mit dem sc1000 Controller über einen VPN-Tunnel zu kommunizieren, muss auch am Computer ein VPN-Client vorhanden sein.

Wichtiger Hinweis: *Wird auf dem sc1000 Controller ein VPN-Client für den Verbindungsaufbau benötigt, ist auf Computerseite OpenVPN als VPN-Client zwingend erforderlich. OpenVPN ist eine kostenlose VPN-Lösung und unterstützt mehrere Betriebssysteme. OpenVPN steht unter http://www.openvpn.net zum Download bereit.*

1. OpenVPN auf dem Computer installieren (wie in der Installationsanleitung der Software beschrieben).

   Nach der Installation erscheint in der Task-Leiste des Desktops das OpenVPN-Symbol (Abbildung 15).

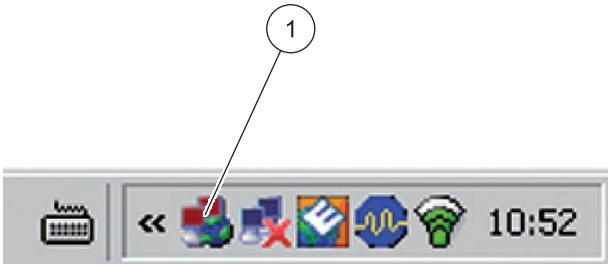

Abbildung 15 OpenVPN-Symbol in der Taskleiste

1	OpenVPN-Symbol

2. Folgende Dateien in das OpenVPN-Verzeichnis kopieren:

Vom Hersteller:

- Speziell angepasste VPN-Client-Software

Vom Anbieter des VPN-Servers:

- Konfigurationsdatei (z. B. Datei mit der Erweiterung .ovn)
- Zertifikat (z. B. Datei mit der Erweiterung .crt)
- Schlüsseldatei (z. B. Datei mit der Erweiterung .key)

3. OpenVPN starten.

3.5.8 VPN-Verbindung zwischen sc1000 Controller und Computer herstellen

1. Auf dem Computer OpenVPN starten.
2. Usernamen und Passwort eingeben (Abbildung 16). Beides stellt der Anbieter des VPN-Servers zur Verfügung.

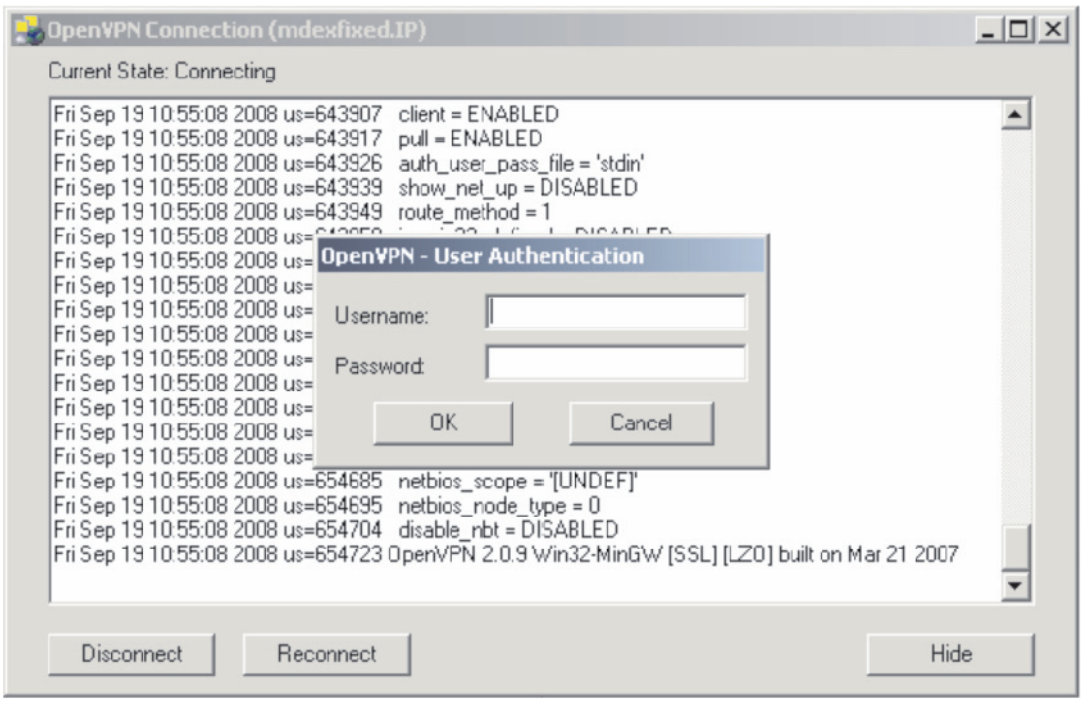

Abbildung 16 OpenVPN-Verbindungsaufbau

3. Im Internet-Browser des Computers die IP-Adresse (vom Anbieter des VPN-Servers) des sc1000 Controllers eingeben (Abbildung 17).

   Hinweis: *Die IP-Adresse ist im Menü* ***SYSTEM SETUP>BROWSER ZUGANG> VPN>IP ADRESSE*** *des sc1000 Controllers zu finden.*

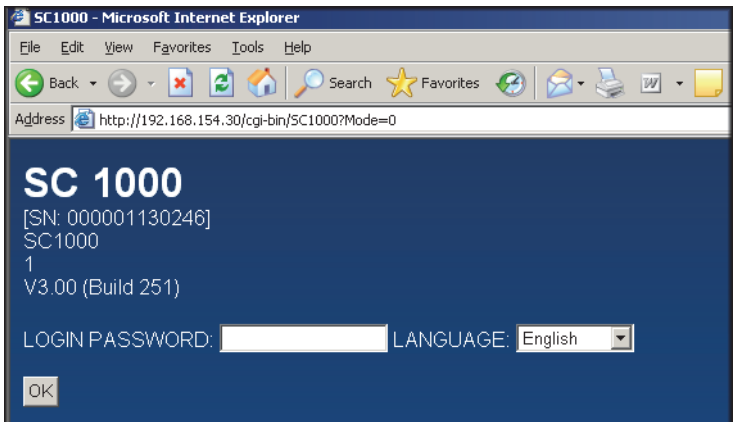

Abbildung 17 Anmeldefenster des sc1000 Controllers

4. Das Browser-Passwort eingeben (siehe Kapitel 3.4.1, Seite 13).

Computer und sc1000 Controller sind nun über einen sicheren VPN-Tunnel verbunden.

3.6 GPRS-Verbindung herstellen

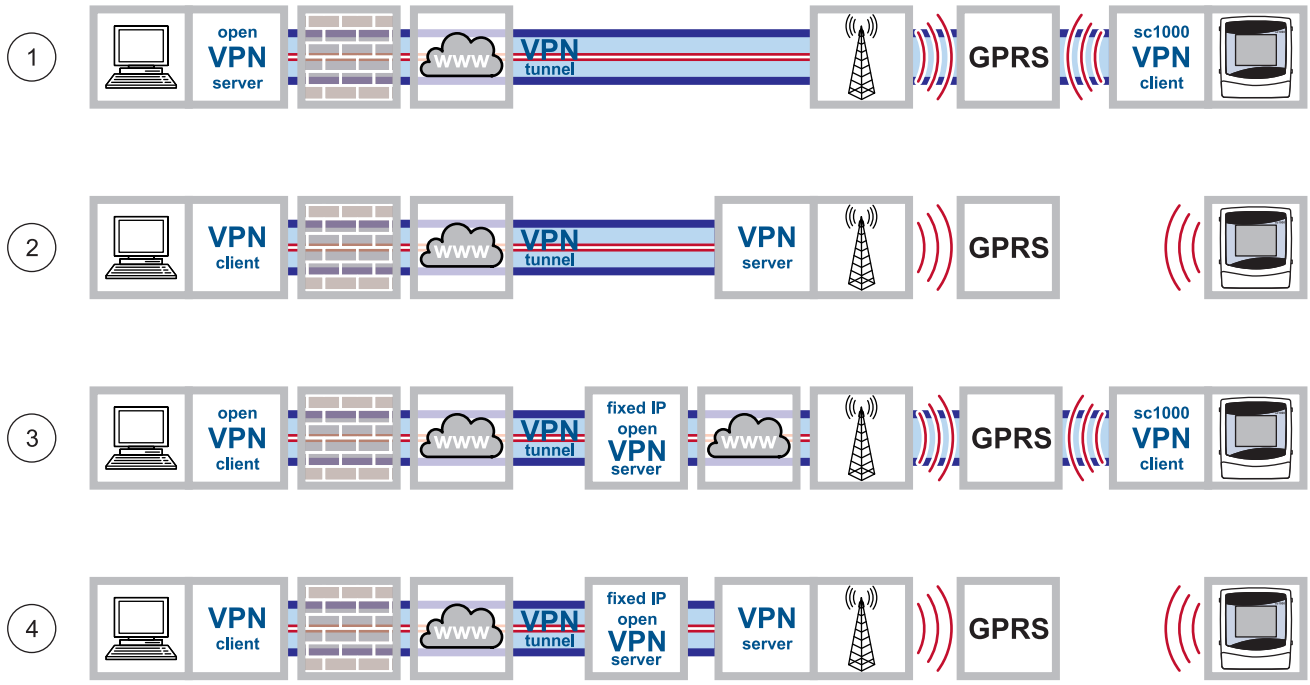

Abbildung 18 GPRS-Verbindungen

1	GPRS-Verbindung mit einem sicheren VPN-Tunnel
2	GPRS-Verbindung über einen VPN-Server des Mobilfunkanbieters
3	GPRS-Verbindung über einen Fixed-IP VPN-Server (nur möglich, wenn ein CDA-Konto beim Mobilfunkanbieter vorhanden ist)
4	GPRS-Verbindung über Fixed IP-Dienst und VPN-Server des Mobilfunkanbieters

GPRS ist ein paketorientierter Datendienst und basiert auf dem bekannten GSM-Mobilfunkstandard. GPRS bietet die Möglichkeit, Daten mobil zu übermitteln. Bei dieser Form der Datenübertragung werden die einzelnen Dateninformationen in kleine Datenpakete umgewandelt, versendet und beim Empfänger wieder zusammengesetzt.

Wenn GPRS im sc1000 Controller aktiviert ist, besteht eine scheinbar dauerhafte Verbindung zur Gegenstelle (Always-on-Betrieb). Ein Funkkanal wird allerdings erst dann geöffnet, wenn wirklich Daten übermittelt werden. Bei der Nutzung des GPRS-Dienstes zahlt der Nutzer nicht für die Dauer der aufgebauten Verbindung, sondern nur für die gesendeten Datenmengen.

Der Mobilstation (z. B. dem sc1000 Controller) wird eine temporäre, dynamische IP-Adresse zugeordnet, die sie eindeutig identifiziert. Aus der Sicht des Teilnehmers erfolgt die Adressierung, wie im Internet üblich, über diese IP-Adresse.

GPRS erlaubt dem sc1000 Controller eine Internetverbindung aufzubauen, über die eine Kommunikation mit anderen Internetteilnehmern möglich ist.

Die bei GPRS zugewiesene IP-Adresse ist üblicherweise nicht vom Internet heraus direkt ansprechbar. Dies hat zur Folge, dass ein GPRS Gerät (z. B. der sc1000 Controller) nur Anfragen ins Internet senden kann. Nur dann lässt der Netzbetreiber die Richtung vom Internet zum GPRS-Gerät für die Antwort der Anfrage zu.

Alle GPRS-Verbindungen werden über einen Mobilfunkanbieter abgewickelt. Hier werden diese GPRS-Verbindungen beschrieben (Abbildung 18):

- GPRS-Verbindung mit einem sicheren VPN-Tunnel (Abbildung 18, Punkt 1)
- GPRS-Verbindung über einen VPN-Server des Mobilfunkanbieters (nur möglich, wenn ein CDA-Konto beim Mobilfunkanbieter vorhanden ist) (Abbildung 18, Punkt 2)
- GPRS-Verbindung über einen Fixed-IP VPN-Server (Abbildung 18, Punkt 3)
- GPRS-Verbindung über einen Fixed IP-Dienst und VPN-Server des Mobilfunkanbieters (Abbildung 18, Punkt 4)

3.6.1 Hardware-Voraussetzungen am sc1000 Controller

Der sc1000 Controller muss für den Funkbetrieb vorbereitet sein:

- Ein GSM/GPRS Modem muss installiert sein.
- Eine Antenne muss angeschlossen sein.
- Eine für GPRS freigeschaltete SIM-Karte muss eingebaut sein.
  Die SIM-Karte muss gegebenenfalls nach den Angaben des Mobilfunkanbieters konfiguriert worden sein (z. B. PIN ändern).

  Hinweis: *Es sollte ein passender Datenvolumenvertrag mit einem Mobilfunkanbieter abgeschlossen sein.*

3.6.2 Softwareeinstellungen am sc1000 Controller

- Im Menü **SYSTEM SETUP>BROWSER ZUGANG>PASSWORT** ein Browser-Passwort vergeben.
- Im Menü **SYSTEM SETUP>GSM MODUL>PIN** die vom Mobilfunkanbieter genannte PIN eingeben.

SYSTEM SETUP
GSM MODUL
EINWAHLNUMMER
APN
GPRS
USERNAME
PASSWORT

- Im Menü **SYSTEM SETUP>GSM MODUL>GPRS**
  - prüfen, ob die **EINWAHLNUMMER** mit der vom Mobilfunkanbieter genannten identisch ist
  - den **APN** (Access Point Name) eingeben (kommt vom Mobilfunkanbieter)
  - **USERNAME** und **PASSWORT** eingeben (kommt vom Mobilfunkanbieter)
  - den Eintrag **GPRS** auf **EIN** stellen.

Der sc1000 Controller ist nun GPRS-fähig.

3.6.3 GPRS-Verbindung ohne VPN-Tunnel herstellen

Abbildung 19 GPRS-Verbindung ohne VPN-Tunnel herstellen

Eine GPRS-Verbindung ohne VPN-Tunnel ist nur möglich, wenn ein CDA-Konto (CDA=Corporate Data Access) bei einem Mobilfunkanbieter vorhanden ist. In diesem Fall müssen nur die Softwareeinstellungen am sc1000 Controller gesetzt werden (Kapitel 3.6.2, Seite 26), die VPN-Konfiguration ist in diesem Fall Bestandteil der CDA-Administration.

Ohne CDA-Konto besteht nur eine Verbindung zum Internet. Es können E-Mails versendet werden, der Zugriff auf den sc1000 Controller ist mit dieser Verbindung nicht möglich.

3.6.4 GPRS-Verbindung mit einem sicheren VPN-Tunnel herstellen

Abbildung 20 GPRS-Verbindung mit einem sicheren VPN-Tunnel herstellen

1. VPN-Client an Computer und sc1000 Controller installieren, wie im in Kapitel 3.5, Seite 15 beschrieben.
2. Am sc1000 Controller den Eintrag **SYSTEM SETUP>BROWSER ZUGANG>VPN>VPN** auf **GPRS** stellen.
3. Prüfen, ob unter **SYSTEM SETUP>BROWSER ZUGANG>VPN**
   - der Eintrag **STATUS** auf **VERBINDUNG** steht
   - im Eintrag **IP ADRESSE** eine IP-Adresse angezeigt wird

   Hinweis: *Diese IP-Adresse ist wichtig und wurde vom Anbieter des VPN-Servers genannt. Diese Adresse wurde schon eingestellt als die normale VPN-Ethernet-Verbindung aufgebaut wurde.*

Verbindungsaufbau prüfen
Die GPRS-Verbindung mit einem VPN-Tunnel ist aufgebaut, wenn

- im Menü **SYSTEM SETUP>GSM MODUL>GPRS** unter **STATUS** der Eintrag **GPRS-Verbindung** steht
- im Menü **SYSTEM SETUP>GSM MODUL>GPRS** eine **IP-Adresse** zugewiesen wurde. Diese IP-Adresse ist für den weiteren Verlauf nicht relevant, sie muss nur vorhanden sein

3.7 Verbindung über einen Fixed IP-Dienst herstellen

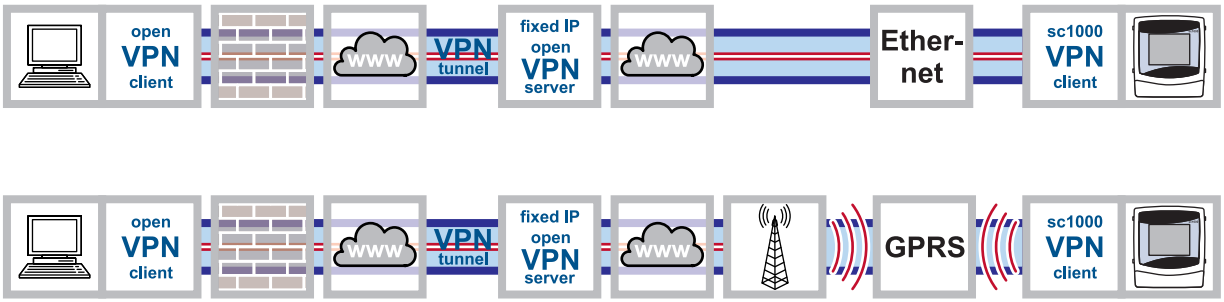

Abbildung 21 GPRS-Verbindung über einen Fixed IP-Dienst herstellen

Die Anbindung des sc1000 Controllers über einen VPN-Tunnel innerhalb des eigenen Firmennetzes kann problematisch sein. Deshalb bietet sich ein externer Fixed IP-Dienst an, der die Rolle als VPN-Server und Schnittstelle zum Mobilfunkanbieter übernimmt.

Wird ein Fixed IP-Dienst genutzt, erhält der sc1000 Controller eine eigene, feste IP-Adresse. Der sc1000 Controller ist dann über das Internet unter immer derselben IP-Adresse zu erreichen.

Eine solche Fixed IP-Verbindung kann über das Ethernet oder GPRS hergestellt werden (Abbildung 21). Die anfallenden GPRS-/Mobilfunk-Kosten hängen von der Datenmenge und der Übertragungshäufigkeit ab.

3.8 GPRS-Verbindung über VPN-Server des Mobilfunkanbieters herstellen

Abbildung 22 GPRS-Verbindung über VPN-Server des Mobilfunkanbieters herstellen

Der CDA-Dienst (Corporate Data Access-Dienst) vom Mobilfunk-Anbieter überträgt Daten zwischen Maschinen und der Zentrale verschlüsselt über GPRS. Das Firmennetz wird an das Mobilfunknetz entweder über eine Mietleitung, die eine feste Bandbreite und eine hohe Sicherheit garantiert, oder über das Internet angebunden. Zwischen dem Firmennetz und dem Mobilfunk-Anbieter wird eine Verbindung durch einen gesicherten VPN-Tunnel hergestellt.

Bei jedem Verbindungsaufbau zwischen sc1000 Controller und Computer werden der APN (Access-Point-Name), der Benutzername und das Passwort abgefragt. Die Teilnehmeridentifizierung erfolgt durch den Mobilfunk-Anbieter.

SYSTEM SETUP
GSM MODUL
EINWAHLNUMMER
APN
GPRS
USERNAME
PASSWORT

- Im Menü **SYSTEM SETUP>GSM MODUL>GPRS**
  - prüfen, ob die **EINWAHLNUMMER** mit der vom Mobilfunkanbieter genannten identisch ist
  - den **APN** (Access Point Name) eingeben (kommt vom Mobilfunkanbieter)
  - **USERNAME** und **PASSWORT** eingeben (kommt vom Mobilfunkanbieter)
  - den Eintrag **GPRS** auf **EIN** stellen

Außerdem besteht die Möglichkeit, einen eigenen Zugangspunkt (APN) im Netz zu erhalten. So können sich lediglich die Maschinen mit einem speziellen SIM-Karten-Profil über diesen Zugangspunkt im Netz einbuchen. Die Voraussetzungen für die Einrichtung eines eigenen Zugangspunktes teilt der Mobilfunk-Anbieter mit.

3.9 GPRS-Verbindung über Fixed IP-Dienst und VPN-Server des Mobilfunkanbieters herstellen

Abbildung 23 GPRS-Verbindung über Fixed IP-Dienst und VPN-Server des Mobilfunkanbieters herstellen

Die Anbindung an das eigene Firmennetz ist oft problematisch. Deshalb bieten auch Fixed-IP Anbieter in der Regel diesen Dienst an.

Der Mobilfunk-Anbieter verbindet den Teilnehmer über einen eigenen VPN Tunnel mit dem Fixed-IP Anbieter. Der sc1000 Controller benötigt in diesem Fall keinen eigenen VPN-Client. Der Benutzer benötigt auf seinem PC eine VPN-Client-Software, um sich mit dem Fixed-IP Anbieter zu verbinden.

3.10 Optionale Erweiterung Modbus TCP

Modbus TCP ist ein Standard für die industrielle Kommunikation. Mit Modbus TCP können Computer mit Mess- und Regelsystemen verbunden werden, die das TCP/IP-Protokoll zur Datenübermittlung verwenden. Diese Datenübermittlung wird als M2M-Kommunikation (M2M=Machine to Machine) bezeichnet.

Hinweis: *Um das Modbus TCP Softwaremodul nutzen zu können, muss KEINE Modbus-Karte im sc1000 Controller installiert sein.*

Das Modbus TCP-Softwaremodul erlaubt die direkte Integration des sc1000 Controllers in SPS-Systeme (SPS=Speicherprogrammierbare Steuerung). SPS-Systeme erfassen die vom sc1000 Controller gemessenen Daten und verarbeiten diese Daten weiter. Die Analyse der erhaltenen Daten und die daraus resultierenden Aktionen sind im SPS-System programmiert.

3.10.1 Voraussetzungen für Modbus TCP

Das Modbus TCP-Softwaremodul muss im sc1000 Controller freigeschaltet/lizenziert sein.

3.10.2 Software-Einstellungen am sc1000 Controller

Das Modbus TCP-Softwaremodul wird in diesen sc1000 Controller Menüs konfiguriert:

SYSTEM SETUP MODBUS TCP	
MODBUS TCP	Bestimmt, ob Modbus TCP aktviert ist (EIN) oder nicht (AUS)
TCP PORT	Bestimmt den TCP Port
TELEGRAMM	Richtet einen Slave ein, der auf einzelnen Datenzusammenstellungen von verschiedenen Geräten basiert.
MODBUS ADRESSE	Standardwert: 0 Setzt die Adresse (1 bis 247) des Modbus Slaves, der im TELEGRAMM Menü konfiguriert wurde, fest.
VIRTUELLE SLAVES	Standardwert: DEAKTIVIERT Virtuelle Slaves können hinzugefügt werden. Diese Slaves sind eine Kopie der tatsächlichen Geräte, diese werden im TELEGRAMM Menü konfiguriert. Die Modbus-Adressen dieser Slaves stehen direkt rechts von der Adresse des konfigurierten Slaves. Das erste konfigurierte Gerät hat die Modbus-Adresse direkt rechts neben der Adresse des konfigurierten Slaves, das zweite Geräte hat die übernächste Adresse usw. AKTIVIERT: Slave-Kopie ist aktiviert. DEAKTIVIERT: Slave-Kopie ist nicht aktiviert.
DATA ORDER	Standardwert: NORMAL Setzt die Reihenfolge der Bytes für die Übertragung der Gleitpunktwerte fest. Ein Gleitpunktwert besteht aus 4 Bytes. Beachten, dass diese Einstellung nur die Daten des konfigurierten Slaves betrifft. VERTAUSCHT: Tauscht das erste Bytepaar mit dem letzten Paar. NORMAL: Die Paare werden nicht getauscht. Eine falsche Einstellung in diesem Menü kann zu leichten Abweichungen der Gleitpunktwerte in Form von Verschiebung um ein Register führen.
SIMULATION	Simuliert zwei Gleitpunktwerte und Fehler/Status als Ersatz für ein Instrument. Der erste Gleitpunktwert durchläuft eine Rampe zwischen den Begrenzungen, die in den Menüs MINIMUM und MAXIMUM gesetzt wurden.
SIMULATION	Standardwert: NEIN Schaltet die Simulation ein (JA) oder aus (NEIN).
DAUER	Standardwert: 10 Minuten Bestimmt die Zeit, die der erste Gleitpunktwert benötigt, um durch den gesamten Bereich zwischen MINIMUM und MAXIMUM zu laufen.
MAXIMUM	Standardwert: 100 Obergrenze für den ersten Gleitpunktwert.
MINIMUM	Standardwert: 50 Untergrenze für den ersten Gleitpunktwert.
FEHLER	Standardwert: 0 Der in dieses Menü eingegebene Wert wird in das erste simulierte Register gesetzt.
STATUS	Standardwert: 0 Der in dieses Menü eingegebene Wert wird in das zweite simulierte Register gesetzt.
UMSCHALTEN	Ändert die Richtung der simulierten Rampenanwendung.
STATUS	Enthält Informationen zur Datenübertragung.

3.10.3 Modbus TCP-Softwaremodul am sc1000 Controller konfigurieren

SYSTEM SETUP
MODBUS TCP
MODBUS TCP
TCP PORT
TELEGRAMM
MODBUS ADRESSE
VIRTUELLE SLAVES
SIMULATION
STATUS

1. Im Menü **SYSTEM SETUP>MODBUS TCP** den Eintrag **MODBUS TCP** auf **EIN** setzen.
2. Im Menü **SYSTEM SETUP>MODBUS TCP** den Eintrag **TCP PORT** auf **502** setzen.

   Hinweis: *Bei bestimmten Einstellungen der firmeneigenen Firewall kann die Wahl eines anderen Ports notwendig sein. Informationen darüber liefert die zuständige IT-Abteilung.*

3. Im Konfigurationsfenster **SYSTEM SETUP>MODBUS TCP>TELEGRAMM** das Telegramm erstellen (siehe Handbuch des sc1000 Controller bzw. Kapitel 3.10.4, Seite 33).

   Hinweis: *Das Telegramm legt fest, welche Datenpunkte in welcher Reihenfolge vom sc1000 Controller übertragen werden. Die Datenpunkte bzw. Namen sind sondenabhängig.*

4. Sicherstellen, dass unter **SYSTEM SETUP>MODBUS TCP>MODBUS ADRESSE** die Telegrammadresse eingetragen ist (Standard=1).

   Hinweis: *Die Geräte unter den Folgeadressen antworten nur, wenn* ***SYSTEM SETUP>MODBUS TCP>VIRTUELLE SLAVES*** *auf* ***EIN*** *gestellt ist.*

5. Im Menü **SYSTEM SETUP>MODBUS TCP>SIMULATION** Werte eintragen, um die Datenübertragung testen zu können.
6. Das Menü **SYSTEM SETUP>MODBUS TCP>SIMULATION>SIMULATION** auf **EIN** stellen, um die Datenübertragung zu testen.

Im Menü **SYSTEM SETUP>MODBUS TCP>STATUS** stehen Informationen zur Datenübertragung (siehe auch Tabelle 4, Seite 41).

Abbildung 24 Modbus TCP Menü Status

Sind alle Werte eingestellt, können die vom Telegramm übertragenen Werte mit jedem beliebigen Modbus TCP Client abgefragt und weiterverarbeitet werden.

Es können maximal 5 Modbus TCP Clients gleichzeitig mit dem Server verbunden sein. Versucht ein weiterer Modbus TCP Client eine Verbindung aufzubauen, wird diese Verbindung zwar akzeptiert, allerdings wird dafür eine bestehende Verbindung getrennt. Getrennt wird die Verbindung, deren letzter Datentransfer am längsten zurückliegt.

3.10.4 Modbus-Telegramm konfigurieren

SYSTEM SETUP
MODBUS TCP
TELEGRAMM

1. **SYSTEM SETUP>MODBUS TCP>TELEGRAMM** wählen.
2. Der Konfigurationsbildschirm wird angezeigt (Abbildung 25).

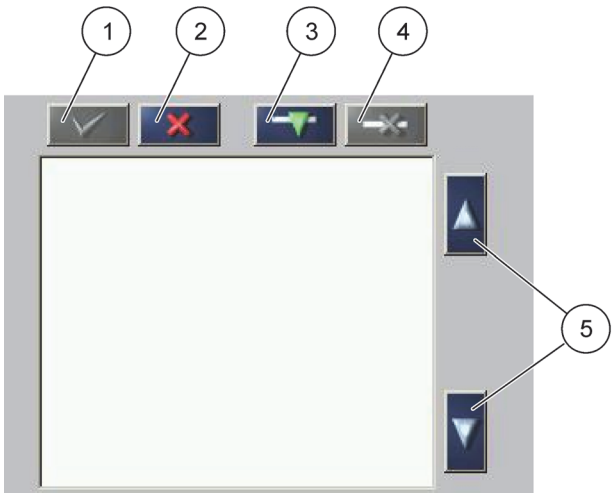

Abbildung 25 Konfigurationsfenster

1	**ENTER**—Sichert die Konfiguration und kehrt zum FELDBUS Menü zurück	**4**	**LÖSCHEN**—Entfernt ein Gerät bzw. einen Eintrag aus dem Telegramm
2	**ABBRECHEN**—Kehrt ohne zu speichern zum FELDBUS Menü zurück	**5**	**AUF/AB** Pfeile—Bewegen die Geräte/Einträge aufwärts bzw. abwärts
3	**EINFÜGEN**—Fügt dem Telegramm ein neues Gerät bzw. einen Eintrag hinzu		

3. **EINFÜGEN** drücken und eine Sonde/ein Gerät wählen. Es wird das Fenster mit der Geräteauswahl angezeigt (Abbildung 26).

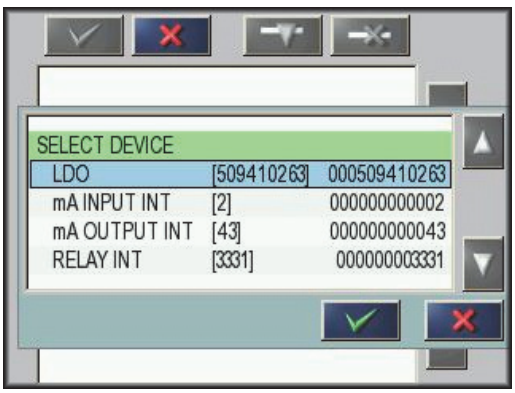

Abbildung 26 Geräteauswahl

4. Sonde/Gerät wählen und **ENTER**-Taste drücken. Die Sonde/das Gerät (inklusive Seriennummer) wird zur Telegrammbox hinzugefügt (Abbildung 27).

Abbildung 27 Geräteliste

5. Einen Eintrag auswählen (zum Beispiel Fehler oder Status) und **EINFÜGEN** drücken. Die Auswahlbox der Einträge mit allen für die Sonde/das Gerät verfügbaren Einträgen wird angezeigt (Abbildung 28) Fehler- und Statusregister sind für alle Sonden/Geräte identisch (Tabelle 2 und Tabelle 3).

Abbildung 28 Eintrag wählen

6. Eintrag wählen und **ENTER** drücken. Der neue Eintrag wird dem Telegramm hinzugefügt. Eintrag auswählen und die **AUF**- und **AB**-Tasten drücken, um die Position des Eintrags zu verändern (Abbildung 29 und Tabelle 1).

Abbildung 29 Telegrammliste mit neuem Eintrag

7. Schritte wiederholen, um weitere Sonden/Geräte und Einträge hinzuzufügen.
8. **ENTER** drücken, um die Konfiguration zu speichern.

Tabelle 1 Telegrammliste—Beschreibung der Spalten

Spalte	Beschreibung
1	Datenposition im konfigurierten Profibus Slave (in 2 Byte Worten)
	Modbus: Datenposition im konfigurierten Modbus Slave Dieser Slave enthält Bestandsregister, die bei 40001 beginnen. Beispiel: „0“ bedeutet Register 40001 und „11“ bedeutet Register 40012.
2	Der Name des Eintrags dient zur Identifizierung der konfigurierten Daten.
3	Datentyp float=Gleitpunktwert int=ganze Zahlen sel=ganze Zahl, als Resultat einer Aufzählungs- oder Auswahlliste
4	Status der Daten r=Daten sind schreibgeschützt (nur lesen) r/w=lesen und schreiben

Tabelle 2 Fehlerregister

Bit	Fehler	Erklärung
0	Kalibrierfehler	Fehlerhafte Kalibrierung erkannt
1	Elektronik-Einstellfehler	Fehlerhafte Einstellung bzw. Kalibrierung der Elektronik
2	Reinigungsfehler	Fehler im Reinigungszyklus erkannt
3	Messmodulfehler	Fehler im Messmodul erkannt
4	System Initialisierung	Inkonsistente Einstellungen erkannt, Rücksetzen auf Werkseinstellung
5	Hardwarefehler	Fehlerhafte Hardware erkannt
6	Interner Kommunikationsfehler	Interner Kommunikationsfehler erkannt
7	Feuchtigkeitsfehler	Feuchtigkeit erkannt
8	Übertemperatur	Temperaturüberschreitung erkannt
9		
10	Warnung Probenzuführung	Fehler im Bereich Probenzuführung erkannt
11	Warnung Kalibrierung fragwürdig	Letzte Kalibrierung von ungenügender Genauigkeit
12	Warnung Messwert fragwürdig	Letzte Messung von ungenügender Genauigkeit bzw. Bereichsverletzung
13	Sicherheitswarnung	Fehler im Bereich der Sicherheitseinrichtungen erkannt
14	Reagenzienwarnung	Warnung Reagenz z. B. Füllstand < min erkannt
15	Warnung Serviceanforderung	Anforderung für Serviceeingiff erkannt

Tabelle 3 Statusregister

Bit	Status1	Erklärung
0	Kalibrierung aktiviert	Kalibriervorgang läuft, Messwert nicht aktuell
1	Reinigung aktiviert	Reinigungsvorgang läuft, Messwert nicht aktuell
2	Servicemode aktiviert	Gerät in Betriebsart „Service“, Messwert nicht aktuell
3	Summenfehlermeldung	Allgemeiner Fehler erkannt, für Details siehe Fehlerwort
4	Messwert Kanal 0, Qualität schlecht	Messgenauigkeit außerhalb der Spezifikation
5	Messwert Kanal 0, Bereichsunterschreitung	Messwert unterhalb des spezifizierten Messbereichs
6	Messwert Kanal 0, Bereichsüberschreitung	Messwert oberhalb des spezifizierten Messbereiches
7	Messwert Kanal 1, Qualität schlecht	Messgenauigkeit außerhalb der Spezifikation
8	Messwert Kanal 1, Bereichsunterschreitung	Messwert unterhalb des spezifizierten Messbereiches
9	Messwert Kanal 1, Bereichsüberschreitung	Messwert oberhalb des spezifizierten Messbereiches
10	Messwert Kanal 2, Qualität schlecht	Messgenauigkeit außerhalb der Spezifikation
11	Messwert Kanal 2, Bereichsunterschreitung	Messwert unterhalb des spezifizierten Messbereiches
12	Messwert Kanal 2, Bereichsüberschreitung	Messwert oberhalb des spezifizierten Messbereiches
13	Messwert Kanal 3, Qualität schlecht	Messgenauigkeit außerhalb der Spezifikation
14	Messwert Kanal 3, Bereichsunterschreitung	Messwert unterhalb des spezifizierten Messbereiches
15	Messwert Kanal 3, Bereichsüberschreitung	Messwert oberhalb des spezifizierten Messbereiches

3.10.5 Systemkonfiguration mit Unity Pro

Abbildung 30 bis Abbildung 32 zeigen beispielhaft, wie ein System mit der SPS-Systemsoftware Unity Pro konfiguriert werden kann

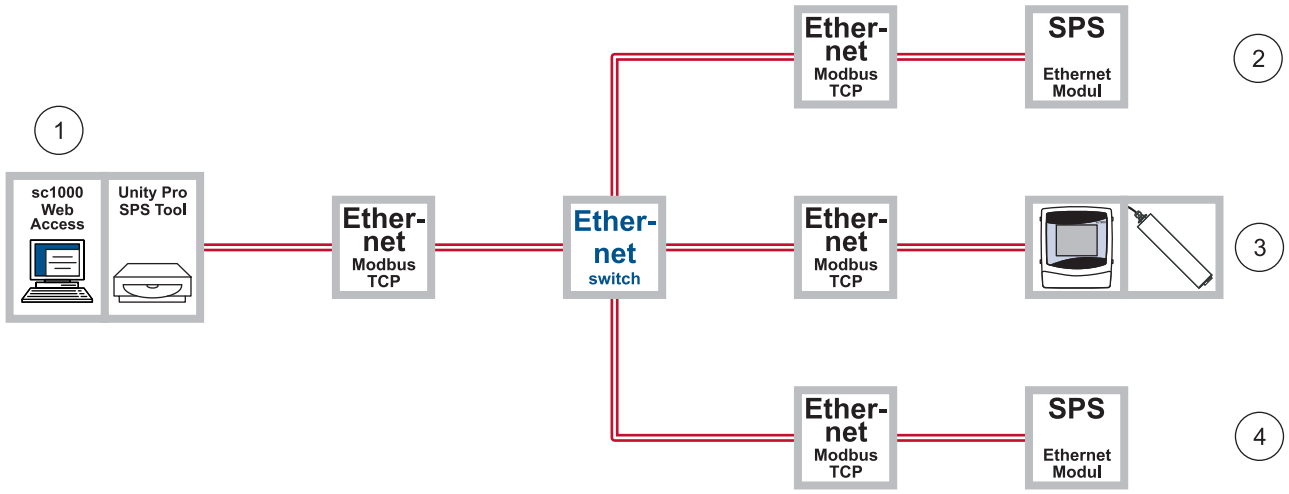

Abbildung 30 Überblick Systemkonfiguration mit Unity Pro

1	Engineering station mit sc1000 WebAccess	**3**	sc1000 Controller mit Sonde
2	z. B. Telemecanique TSX Premium P57 4634M	**4**	z. B. Telemecanique Modicon Quantum CPU 65160

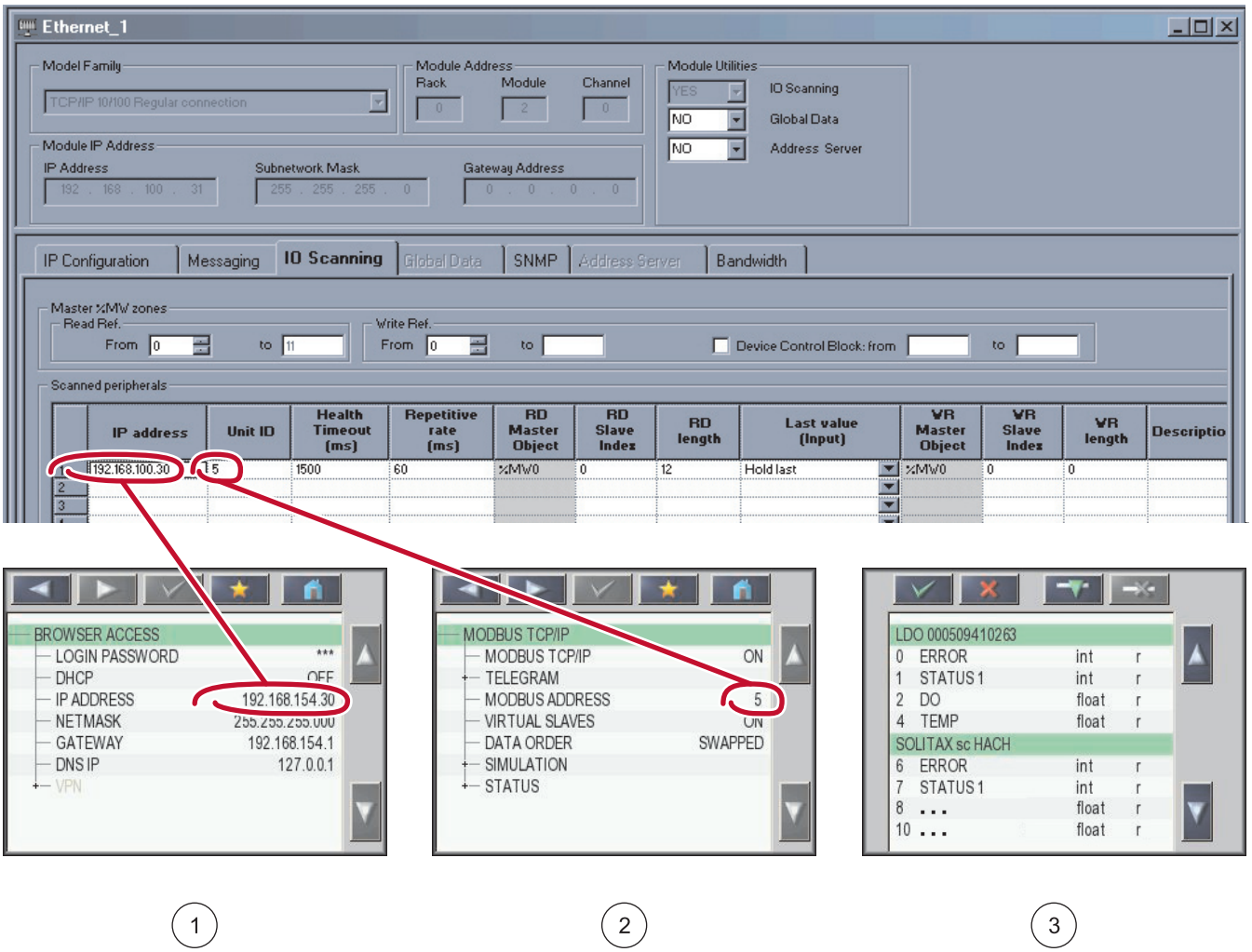

Abbildung 31 Verbindung sc1000 Controller mit Unity Pro
(Die Sprache der Menüeinträge ist abhängig von den Spracheinstellungen)

1	IP-Adresse	**3**	Inhalt des Telegramms
2	Modbus-Adresse		

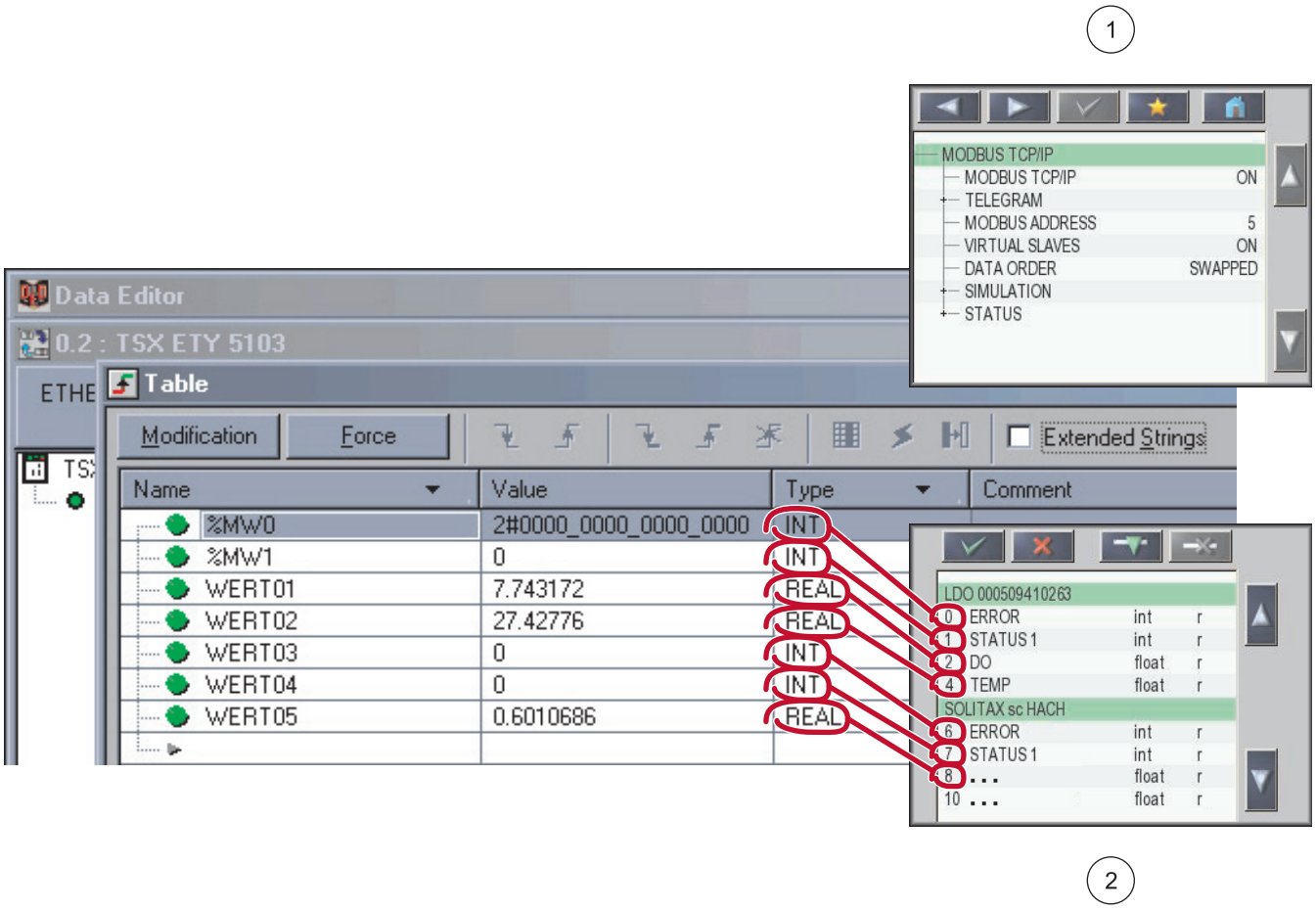

Abbildung 32 Systemkonfiguration mit Unity Pro

1	Data Order vertauscht (Swapped)	**2**	Telemecanique TSX Premium P57 4634M startet bei Offset 0 Telemecanique Modicon Quantum CPU 65160 bei Offset 1

Kapitel 4 Fehlermeldungen

4.1 GSM/GPRS

Siehe Fehlermeldungen für GSM im Handbuch zum sc1000 Controller.

GPRS hat keine speziellen Statusmeldungen.

4.2 VPN-Tunnel

SYSTEM SETUP
BROWSER ZUGANG
VPN

Für den Verbindungsaufbau des VPN-Tunnels gibt es mehrere Statusmeldungen. Diese werden angezeigt unter **SYSTEM SETUP>BROWSER ZUGANG>VPN**:

- AUS: Der OpenVPN Client ist deaktiviert.
- VERB. AUFBAU: Der OpenVPN Client versucht eine Verbindung zum Server herzustellen.
- VERBINDUNG: Die Verbindung zum Server wurde hergestellt.
- UNTERBROCHEN: Die Verbindung zum Server ist unterbrochen. Dieser Status tritt ein, wenn die Verbindung zum Internet gestört ist, z. B. das Ethernetkabel entfernt oder die GPRS Verbindung getrennt wurde. Nach Behebung des Kommunikationsfehlers wird die Verbindung automatisch wiederhergestellt.

4.3 Modbus TCP

SYSTEM SETUP
MODBUS TCP
STATUS

Im Falle eines Fehlers liefert der Modbus TCP Server entsprechende Exception Codes an den anfragenden Client zurück (Tabelle 4).

Der zuletzt aufgetretene Exception Code für jeden verbundenen Client wird im Menü **SYSTEM SETUP>MODBUS TCP>STATUS** angezeigt.

Tabelle 4 Modbus Exception Codes gemäß Modbus Spezifikation

Exception Code	Bezeichnung
01	Illegal Function
02	Illegal Data Address
03	Illegal Data Value
04	Illegal Response Length
05	Acknowledge
06	Slave Device Busy
07	Negative Acknowledge
08	Memory Parity Error
10	Gateway Path Unavailable
11	Gateway Target Device Failed to Respond

4.4 Benachrichtigung mit einer E-Mail bei Fehlermeldungen/Warnungen

Beim Auftreten eines Fehlers kann eine E-Mail mit der Fehlerbeschreibung an einen oder mehrere Empfänger verschickt werden. Für die Benachrichtigung mit einer E-Mail können bis zu vier Konfigurationssets erstellt werden.

Jedes Konfigurationsset enthält unter anderem folgendes:

- Die E-Mail-Adresse des Empfängers.
- Ausgewählte Fehler, Warnungen und Ereignisse angeschlossener Sonden, die eine E-Mail-Benachrichtigung auslösen.

Um die E-Mail Benachrichtigungen zu nutzen, muss eine Verbindung zwischen sc1000 Controller und einem Computer bestehen (über GPRS oder Ethernet) und ein E-Mail-Konto bei einem E-Mail-Anbieter vorhanden sein. Der Anbieter muss das Versenden von E-Mails über einen SMTP-Server (Postausgangsserver) unterstützen.

4.4.1 Software-Einstellungen am sc1000 Controller

Die E-Mail-Benachrichtigung wird in diesen sc1000 Controller Menüs konfiguriert:

SYSTEM SETUP		
EMAIL		
EMAIL 1-4		
	E-MAIL ADRESSE	Setzt E-Mail-Adresse für Benachrichtigungen. Es können mehrere Adressen angegeben werden. Diese müssen durch ein Leerzeichen getrennt sein.
	SPRACHE	Wählt eine Sprache für die E-MAIL
	E-MAIL LIMIT (0 - 100)	Gibt die maximale Anzahl von e-mail Benachrichtigung an, die der SC1000 innerhalb von 24 Stunden versenden darf. Der 24 Stunden Zyklus startet zur eingegebenen STARTZEIT
	WIEDER-HOLUNG (0-24h)	Gibt ein Intervall an, in dem nicht bestätigte Fehlermeldungen wiederholt an die E-MAIL ADRESSE versendet werden.
	STARTZEIT	Gibt die Startzeit für die WIEDERHOLUNG an. Beispiel: WIEDERHOLUNG=6 h, STARTZEIT=2:00 Uhr: Nicht bestätigte Meldungen werden um 2:00 Uhr, 8:00 Uhr, 14:00 Uhr, 20:00 Uhr wiederholt verschickt.
	UNTER-DRÜCKEN	Standard: AUS EIN: Bei wiederholtem Auftreten desselben Fehlers wird nur beim ersten Mal eine E-Mail verschickt.
	KONFIGURIEREN	Bestimmt, welche Geräte überwacht und welche Fehlermeldungen/Warnungen per E-Mail verschickt werden.
		HINZUFÜGEN	Fügt Geräte zur Konfigurationsliste hinzu. Es werden alle angeschlossen Geräte einschließlich des sc1000 Controllers angezeigt. Bereits hinzugefügte Geräte sind grau unterlegt und können nicht ausgewählt werden.
		ENTFERNEN	Entfernt Geräte aus der Konfigurationsliste. Es werden alle konfigurierten Geräte angezeigt.
		GERÄTENAME 1-n	Erstellt einzelne Nachrichten für ein Gerät. Die Menüs FEHLER und WARNUNGEN enthalten alle Fehler/Warnungen des gewählten Geräts. 1=Eine E-Mail wird bei Fehler/Warnung versendet. 0=Keine E-Mail wird bei Fehler/Warnung versendet. ALLE WÄHLEN: Aktiviert (1) oder deaktiviert (2) alle Menüpunkte auf einmal.
	ABSENDER		E-Mail-Adresse des sc1000 Controllers. Dient als Absenderangabe.
	SMTP SERVER		Postausgangsserver des E-Mail-Anbieters. Den Servernamen stellt der E-Mail-Anbieter zur Verfügung.
	BENUTZERNAME		Benutzername zum Anmelden an den SMTP Server des E-Mail-Anbieters. Den Benutzernamen stellt der E-Mail-Anbieter zur Verfügung.
	PASSWORT		SMTP Server des E-Mail-Anbieters. Das Passwort stellt der E-Mail-Anbieter zur Verfügung.

4.4.2 E-Mail-Format

Tabelle 5 und Tabelle 6 zeigen das Format, in der die E-Mail erscheint:

Tabelle 5 E-Mail-Format

Datum	Ortszeit	Ereigniszähler
Warnung-/Fehlertext	Warnung/Fehler ID Nummer	
Gerätename	Seriennummer des Geräts	

Tabelle 6 E-Mail-Format Beispiel

2008-12-18	18:07:32	(1)
Communication Error	<E32>	
LDO	[405410120]	

Kapitel 5 Ersatzteile und Zubehör

Beschreibung	Kat.-Nr.
SD-Karte 1 GB	LZY520
Display-Modul HACH-LANGE mit GSM-Modem	LXV402.99.01001
Outdoor Ethernet Port Kit	LZY553
Ethernet-Kabel RJ45	LZX998
Modbus TCP-Softwaremodul, Lizenzschlüssel	LZY598

Kapitel 6 Glossar

Tabelle 7 Glossar

Begriff	Erklärung
APN	Access Point Name; Ermöglicht den Zugang zu einem externen Paket-Datennetz.
DHCP	Dynamic Host Configuration Protocol; Ermöglicht die automatische Einbindung eines neuen Computers in ein bestehendes Netzwerk.
DNS	Domain Name System
Ethernet	Physikalischer Layer für Netzwerkkommunikation, der IEEE-Norm 802.3 folgend.
fixed IP-Server	Server, der Endgeräten eine feste IP-Adresse zuweist und verwaltet.
FTP	File Transfer Protokoll
Gateway	Über Gateways können Netzwerke, die auf unterschiedlichen Protokollen basieren, miteinander kommunizieren.
GPRS	General Packet Radio Service; paketorientierter Übertragungsdienst, der das Verschicken von Daten und Emails über Mobiltelefone und Computer ermöglicht.
GSM	Global System for Mobile Communications; Mobilfunkstandard der zweiten Generation (2G).
M2M	Machine to Machine
Modbus TCP/IP	Modbus Protokoll, das in das TCP/IP Protokoll eingebunden ist.
SPS	Speicherprogrammierbare Steuerung
VPN	Software um Geräte eines benachbarten Netzes an das eigene Netz einzubinden, ohne dass die Netzwerke zueinander kompatibel sein müssen. Das Netz, in das Geräte eingebunden werden, wird zugeordnetes Netz genannt.
VPN-Client	Software, die einem Gerät in einem Netz den Zugriff auf das zusätzliche VPN-Netz ermöglicht, also die Beschaffenheit des zugeordneten Netzes virtuell nachbildet.
VPN-Tunnel	Zusätzliche Verschlüsselung der ursprünglichen Netzwerkpakete innerhalb des VPN-Protokolls. Dadurch ist die Verbindung abhör- und manipulationssicher.

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, Ausgabe 3