Industrial Remote Communication: Data Communication via GPRS with S7-1200 and CP 1242-7

S7-1200 Set 31

Process data exchange between several remote stations with or without Telecontrol Server Basic

Applications & Tools

Answers for industry.

SIEMENS

Warranty and Liability

Note

The application examples are not binding and do not claim to be complete regarding configuration, equipment and any eventuality. The application examples do not represent customer-specific solutions. They are only intended to provide support for typical applications. You are responsible for ensuring that the described products are used correctly. These application examples do not relieve you of your responsibility to use sound practices in application, installation, operation and maintenance. When using these application examples, you recognize that we will not be liable for any damage/claims beyond the liability clause described. We reserve the right to make changes to these application examples at any time without prior notice. If there are any deviations between the recommendations provided in this application example and other Siemens publications (e.g. catalogs), the contents of the other documents shall have priority.

We do not accept any liability for the information contained in this document.

Any claims against us – based on whatever legal reason – resulting from the use of the examples, information, programs, engineering and performance data etc., described in this application example shall be excluded. Such an exclusion shall not apply in the case of mandatory liability, e.g. under the German Product Liability Act ("Produkthaftungsgesetz"), in case of intent, gross negligence, or injury of life, body or health, guarantee for the quality of a product, fraudulent concealment of a deficiency or violation of fundamental contractual obligations ("wesentliche Vertragspflichten"). The damages for a breach of a substantial contractual obligation are, however, limited to the foreseeable damage, typical for the type of contract, except in the event of intent or gross negligence or injury to life, body or health. The above provisions do not imply a change in the burden of proof to your detriment.

It is not permissible to transfer or copy these application examples or excerpts thereof without express authorization from Siemens Industry Sector.

Caution

The functions and solutions described in this article confine themselves to the realization of the automation task predominantly. Please take into account furthermore that corresponding protective measures have to be taken up in the context of Industrial Security when connecting your equipment to other parts of the plant, the enterprise network or the Internet. Further information can be found under the Item-ID 50203404.

http://support.automation.siemens.com/WW/view/en/50203404

Table of Contents

1 Task

Overview

This application example covers the following main points:

- Exchange of process values between remote stations
- Transfer of process values between remote stations[1] via a central station[2]
- Direct transfer of process values between remote stations, i.e. machine-to-machine (M2M), without using a central station

This task definition is further broken down into several variants which differ with regard to the transmission protocol used (WDC, ISO-ON-TCP) and the hardware installed in the remote stations (SIMATIC S7-1200, SIMATIC S7-300, …).

The basic technical challenge of how to enable communication between two or more remote stations is described on the basis of three variants. Each variant is explained in greater detail with the help of a specific application example, including a description of the selection and decision criteria relevant to finding the best solution. Finally, the individual variants are compared with regard to their technical differences.

There are separate start-up programs for each variant.

1.1 Variant 1 "M2M telecontrol"

Introduction

The functions and features of this application example are explained by the example of an elevated water tank.

Overview of the automation task

The filling level of an elevated water tank (remote station 1) shall be transmitted to a pump station (remote station 2). On the basis of this information, the pumps shall be turned on and off correspondingly.

For the purpose of remote control and remote visualization, the two remote stations are already connected to a control center (central station) on which the software 'Telecontrol Server Basic' is installed. Communication between the remote stations and the central station is described in scenario 1 (see \1\).

This new automation task, however, requires an additional communication feature for the exchange of process values between the two remote stations.

---

[1] A remote station (RS), in this context, is a distant automation station equipped with a SIMATIC S7-1200 CPU and a CP 1242-7 , or a SIMATIC S7-300 CPU and a SCALANCE M873-0 router.
[2] The term central station (CS) refers to a PC or IPC with the connection management software Telecontrol Server Basic installed.

Figure 1-1 Example of an automation task, variant 1
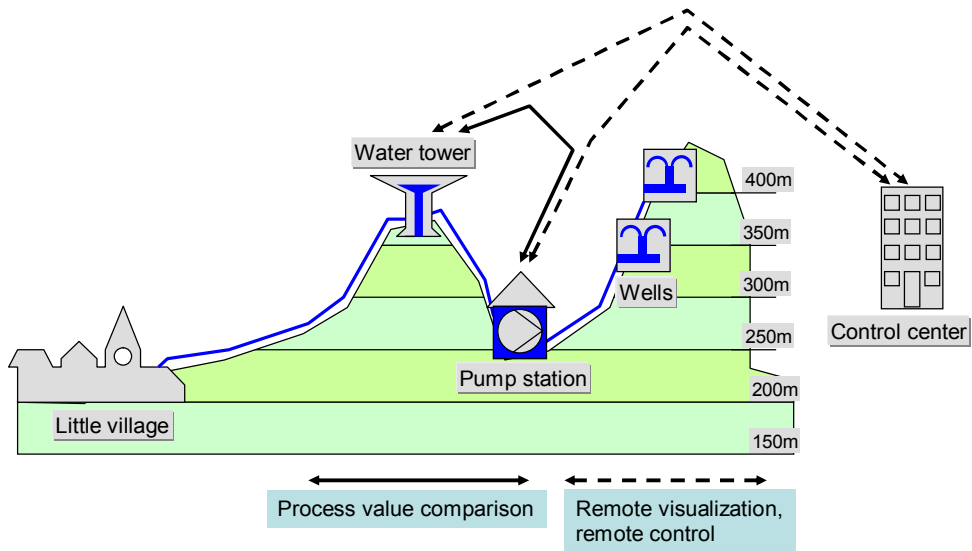
Description of the automation task

The automated plants shall communicate over a wireless connection. This leads to the following requirements:

- Wireless data transmission via GPRS

- A central station platform is already available in the form of a standard PC or ICP.

- The comparison of process values received from the automated plants focuses on the currentness of these values, not on their congruity or completeness.

- The time elapsed since the last process value comparison shall be measured, so as to generate an alarm, if the defined period has been exceeded and to ensure suitable reaction in the plant.

The selected task results in the following cases of communication:

Table 1-1

Direction	Initiator	Function
Water tower → Pump station	Water tower	The filling level measured in the water tower will be transmitted to the pump station.
Water tower ← Pump station	Pump station	The pump will be turned on or off, depending on the filling level measured in the water tower. The pump status will be transmitted to the water tower.

1.2 Variant 2 "M2M with S7-1200 directly via GPRS"

Introduction

The functions and features of this application example, variant 2 – are explained by the example of an I/O-connection between the wind turbines and the switching station of a wind farm.

Overview of the automation task

The power supplier and operator of a wind farm shall be able to adjust the output of his wind farm to the current consumption situation in the electricity grid. This shall be effected by means of an I/O connection between several wind turbines and a switching station.

Please note that the two remote stations shall not be connected to a control center for remote visualization or remote control.

The switching station would usually have a fixed-line connection to the control center, although this will not be considered in this application example.

Figure 1-2 Example of an automation task, variant 2
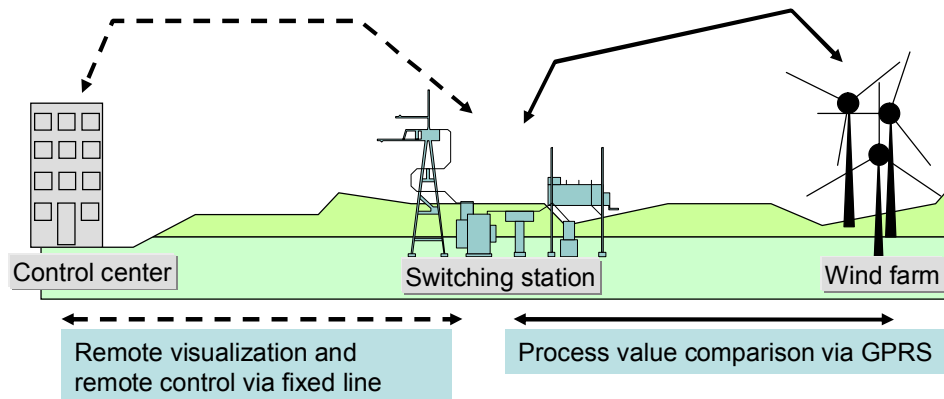
Description of the automation task

The automated plants shall communicate over a wireless connection. This leads to the following requirements:

- Wireless data transmission via GPRS

- The comparison of process values received from the automated plants focuses on the currentness of these values, not on their congruity or completeness.

The selected task results in the following cases of communication:

Table 1-2

Direction	Initiator	Function
Wind farm → switching station	Wind farm	The process information from the wind turbines is received via digital inputs and then transmitted to the switching station.
Wind farm ← switching station	Switching station	The control information from the switching station is received via digital inputs and then transmitted to the wind turbines.

1.3 Variant 3 "M2M with S7-1200 and S7-300 directly via GPRS"

Introduction

The functions and features of this application example variant 3 are explained by the example of automated oil production fields.

Overview of the automation task

Each of several oil production fields is provided with 25 to 30 SIMATIC S7-1200 controllers. These S7-1200 units are used to control the pumps independently of each other (on/off) and to transmit the filling levels to a higher-level SIMATIC S7-300 controller.

This higher-level SIMATIC S7-300 controller issues global release commands for oil production to the lower-level S7-1200 units installed in the oil production fields. Communication between a number of *n* S7-1200 controllers with the higher-level S7-300 controller shall be realized over a wireless connection.

Please note that the two remote stations shall not be connected to a control center for remote visualization or remote control.

Figure 1-3 Example of an automation task, variant 3
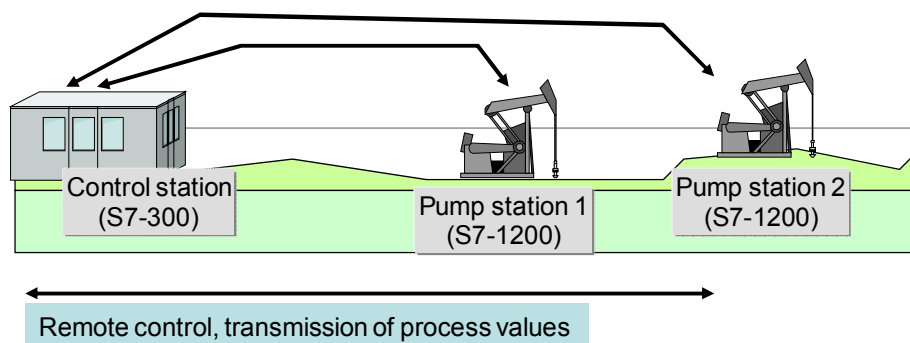
In this application example, only *two* S7-1200 controllers are illustrated in place of any number of *n* remote stations.

Description of the automation task

The automated plants shall communicate with the control station over a wireless connection. This leads to the following requirements:

- Wireless data transmission via GPRS

- The comparison of process values and remote control between the automated plants and the control station focus on the currency of these values, not on their congruity or completeness.

- The time elapsed since the last process value comparison shall be measured, so as to generate an alarm, if the defined period has been exceeded and to ensure suitable reaction in the plant.

1.4 Analysis and comparison of the automation tasks

Although the automation tasks of all variants require the exchange of process data between at least two remote stations, there are some further decisive parameters when it comes to selecting the best automation solution.

1.4.1 Direct communication or communication via a control center

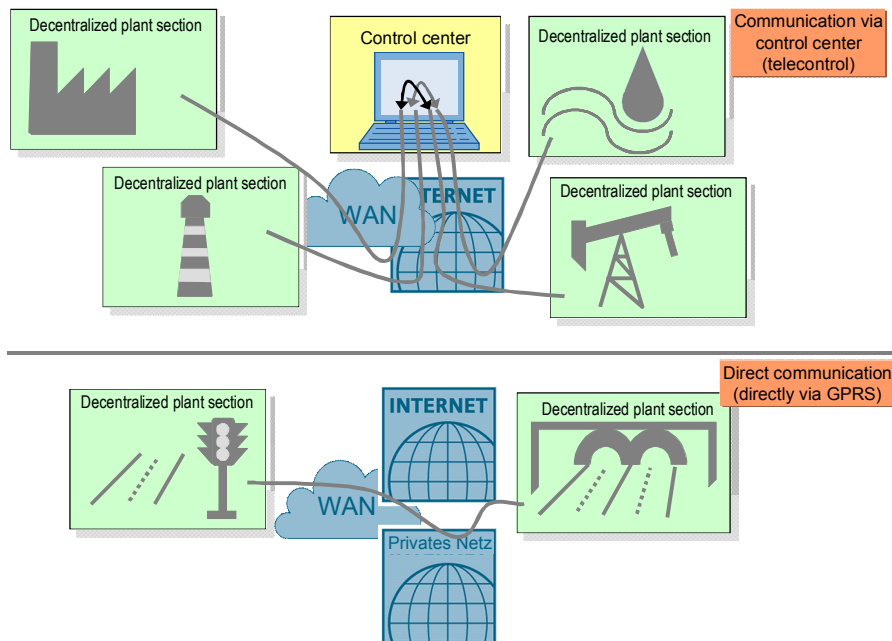In principle, there always arises the question whether the exchange of process data between the remote stations shall be accompanied by the exchange of process data with a control center for the purpose of visualization and control of distributed plant sections.

Figure 1-4 M2M communication with and without central station

A central control station is available

If a central station concept is already available, it may be reasonable to integrate it as a participant in the WAN structure, so as to enable cross-communication of all other stations. Since the central control station is provided with a static IP address or can be otherwise clearly identified in the Internet, the other WAN participants no longer need this special feature to be accessible via Internet/WAN.

This requirement is fulfilled in the application example "variant 1".

Cross-communication without central control station

If remote visualization or remote control is not necessary, the costs for a central station can be saved. In this case, some special requirements for the Internet access of the distributed plant sections must be fulfilled, so as to enable direct communication via WAN (Internet or private networks).

The WAN participant must, in any case, be provided with a static IP address. Without a central control station, cross-communication via DynDNS is not possible.

This static IP address is

1. either a public IP address which can be accessed via the Internet. In this case, M2M communication is effected over the WAN/Internet.

2. or a private IP address which cannot be accessed via the Internet and, consequently, can neither send own queries via the Internet.
In this case, the provider must ensure that all IP addresses of the distributed plant sections are located in the same private address area and can communicate with each other. As a result, M2M communication is effected over the WAN/private network.

The allocation of public IP addresses for this M2M communication should be used only in exceptional cases (e.g. if the distributed plant sections must be accessible over the Internet). Since the products used for this application do not have a VPN tunnel with adequate encryption options, this type of communication would not be sufficiently secured against manipulation by third parties. Furthermore, reliable cost controlling with hourly reports can be realized only via WAN/private networks.

The remaining variants 2 and 3 are based on M2M communication without a central control station and use the private static IP addresses of a private network.

1.4.2 Protocol selection

WDC

The WDC protocol is used for data transmission via the CP 1242-7, if communication shall be effected over the central control station with the Telecontrol Server Basic software.

Variant 1 is based on M2M communication with the WDC protocol.

ISO-on-TCP or UDP

For the products used in this application example you can select either an ISO-on-TCP or a UDP protocol.

Table 1-3 Protocols, advantages and disadvantages

Protocol	Advantage	Disadvantage
UDP	• Faster data transmission rate • Smaller telegrams	• No acknowledgement mechanism (unidirectional) • Insecure (no data protection possible)
ISO-on-TCP	• With acknowledgement mechanism	• Larger telegrams • Slower data transmission rate

Due to the missing security mechanisms for data transmission with the UDP protocol (and because decentralized plant sections based on S7-1200 can only send UDP telegrams, so that only streaming applications could be covered), the following descriptions only refer to the ISO-on-TCP protocol.

M2M communication of the remaining variants 2 and 3 is realized with the ISO-on-TCP protocol.

1.4.3 Homogenous, decentralized plant sections or mixed structure

One further fundamental question is whether all decentralized plant sections are based on SIMATIC S7-1200 controllers, or if the network also includes WAN participants with SIMATIC S7-300 controllers or Windows-based devices.

Figure 1-5 Only S7-1200 or mixed structure
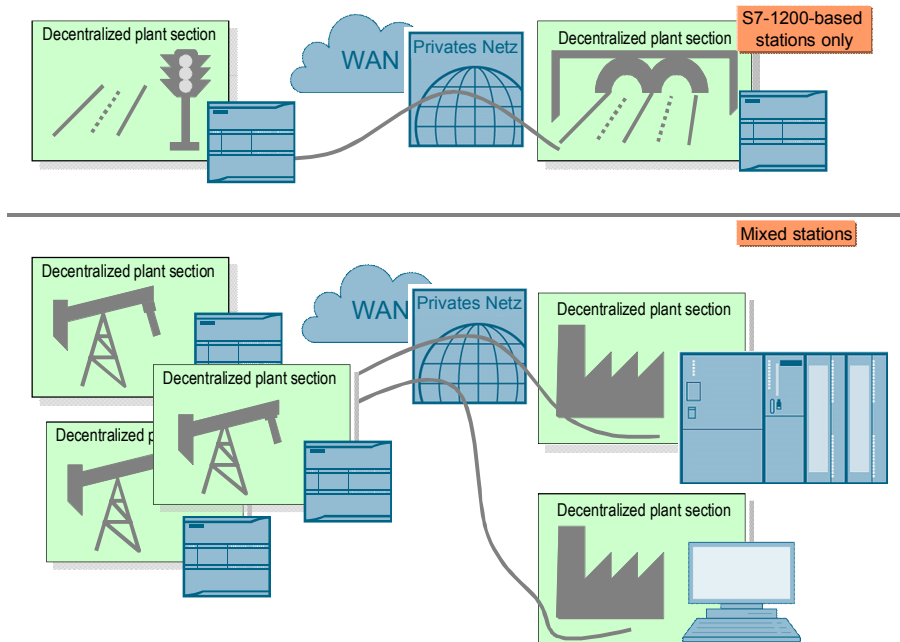
Cross-communication with S7-1200-based plant sections only

Decentralized plant sections based on SIMATIC S7-1200 use port 30000 for transmission with the ISO-on-TCP protocol. In a homogeneous system in which all decentralized plant sections are based on SIMATIC S7-1200 controllers, M2M communication can be effected without restrictions.

This configuration is represented in the application example "variant 2".

Cross-communication with remote stations based on S7-1200 and S7-300 or with Windows-based devices

Communication processors of the SIMATIC S7-300 series or protocol implementations for Windows-based devices use Port 102 for transmission with the ISO-on-TCP protocol. Please note that in a mixed structure with decentralized, SIMATIC S7-1200-based plant sections there must always be one device that translates the incoming and outgoing data traffic for the relevant port.

This configuration is represented in the application example "variant 3".

1.4.4   Summary

The graphic below again illustrates all platforms and <u>conceivable</u> communication configurations, as well as those which are actually discussed in <u>this application description</u>.

Figure 1-6 Conceivable and actually applied system configurations
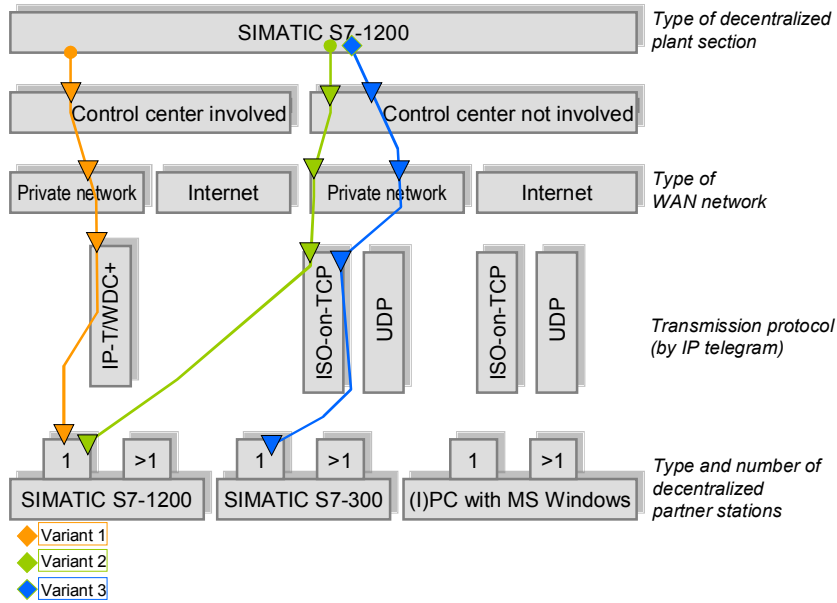
2 Solution

2.1 Variant "M2M telecontrol"

2.1.1 Overview of the general solution

Remote station 1 and remote station 2

The configuration of both remote stations is identical.

A GSM/GPRS modem type **CP 1242-7 (2)** is connected to the **SIMATIC S7-1200 controller 1214C (3)** via the bus interface.

The GSM/GPRS modem is equipped with a **SIM card (5)**, and connection to the air interface is realized with a quad band GSM/GPRS **antenna type ANT 794-4MR (4)**.

All components are supplied with power by a **SIMATIC PM 1207 power module (1)**.

Figure 2-1 Configuration scheme – remote station
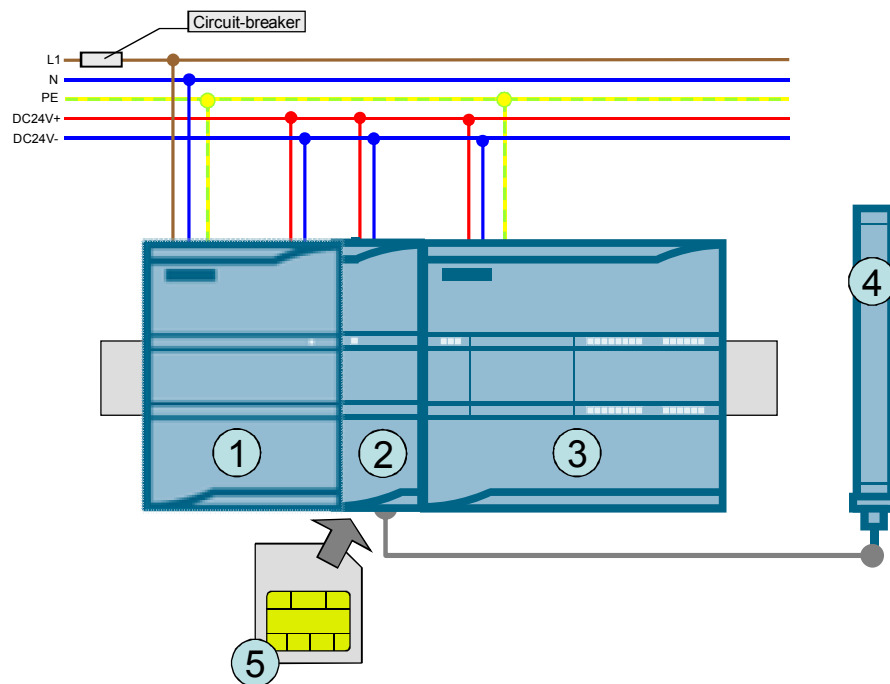
Central station

The central station consists of a **PC (2)** with the software **Telecontrol Server Basic (3)**. The PC is connected to the Internet via a **router (4)**.

Figure 2-2 Configuration scheme – central station
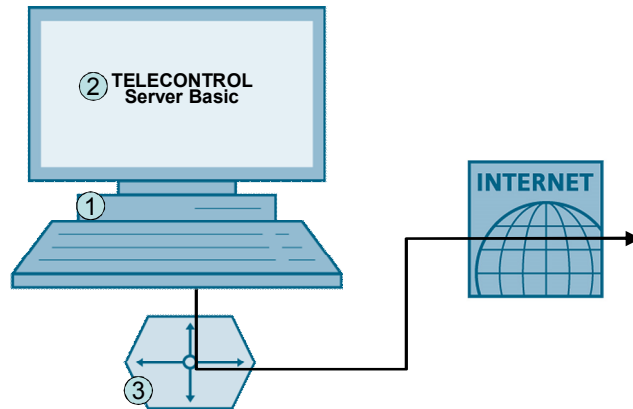
Overview of the communication landscape

The graphic below shows the IP addresses relevant to this variant and which must be known when starting up the system.

Figure 2-3
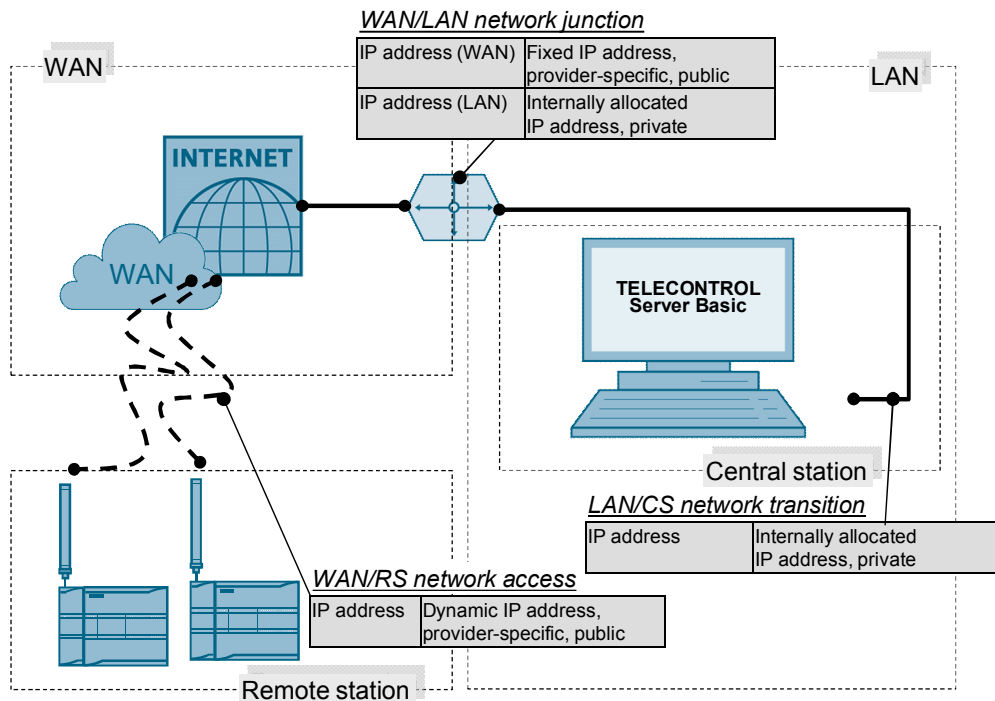
2.1.2 Hardware and software components used

Remote stations – hardware components

Table 2-1 Variant 1, RS HW components

Component	Qty.	Order number	Note
SIMATIC S7-1200, PM 1207	2	6EP1332-1SH71	2.5A
SIMATIC S7-1200, CPU 1214C	2	6ES7214-1AE30-0XB0	DC/DC/DC, FW 2.2.0 or higher, or another type of CPU
SIMATIC CP 1242-7	2	6GK7242-7KX30-0XE0	FW 1.3.0 or higher
SINAUT ANT 794-4MR, rod antenna	2	6NH9860-1AA00	As an alternative: flat antenna ANT794-3M (6NH9870-1AA00)
Ethernet line	1	6XV1870-3QH20	For configuration purposes (2 meters of this type or similar cable)
Circuit breaker	2	5SX2116-6	1 pole B, 16A
Standard mounting rail	2	6ES5 710-8MA11	35 mm
SIM card	2	Available at your mobile service provider	Please check if special M2M tariffs with included data volumes are available.

Remote stations – standard software components

Table 2-2 Variant 1, RS SW components

Component	Qty.	Order number	Note
STEP 7 Basic V11	1	6ES7822-0AA01-0YA0	Service Pack 2 or higher
Hardware Support Package for CP 1242-7		Internet link \9\	Necessary only for STEP 7 V11

Central station – hardware components

Table 2-3 Variant 1, CS HW components

Component	Qty.	Order number	Note
PC	1		
Router (with integrated DSL modem)	1	Specialist dealer	With port forwarding

Note The system requirements for the PC are described in chapter 2.1 of the Telecontrol Server Basic operating instructions. (Internet link **Fehler! Verweisquelle konnte nicht gefunden werden.**)

Central station – standard software components

Table 2-4 Variant 1, CS SW components

Component	Qty.	Order number	Note
Telecontrol Server Basic	1	6NH9910-0AA20-0AA0	8 stations; as an alternative: 64, 256, 1000 or 5000 stations
As an option: SIMATIC OPC-Scout	1	On the SIMATIC NET CD	To test the OPC interface of Telecontrol Server Basic.

SIM card and contract

The central control station used in this variant is available as a fixed access point for the exchange of process data for all other WAN participants. Cross-communication of the two station types "pump station" and "water tower" are also routed via the central control station. The SIM cards or the relevant mobile service contracts for these remote stations must have a public IP address (i.e. they must be accessible via the Internet). There are no further requirements.

Note	The public IP addresses are required, since the providers usually offer a fixed phone line only with public IP addresses. Consequently, the remote stations must also have public IP addresses. If your provider offers private IP addresses for fixed line and mobile services, the use of private IP addresses may be considered also for this variant.

Sample files and projects

The following list shows all files and projects used in scenario 2. Only the marked rows are relevant to this variant.

Table 2-5 Project files, variant 1

No.	Component	Note

1.	58099765_Set31 _**Var1**_CODE_V10.zip
	This file consists of:
	• 58099765_Set31_Var1_STEP7_V10
	   The STEP 7 TIA V11 project for the two remote stations
	• Smsc.sqlite im Ordner 58099765_Set31 _TCSB_V10
	   The Configuration file of Telecontrol Server Basic	

2.2 Variant "M2M with S7-1200 directly via GPRS"

2.2.1 Overview of the general solution

Remote station 1 and remote station 2

The configuration of both remote stations is identical. With this variant no central station is required.

A GSM/GPRS modem type **CP 1242-7 (2)** is connected to the **SIMATIC S7-1200 controller 1214C (3)** via the bus interface.

The GSM/GPRS modem is equipped with a **SIM card (5)**, and connection to the air interface is realized with a quad band GSM/GPRS **antenna type ANT 794-4MR (4)**.

All components are supplied with power by a **SIMATIC PM 1207 power module (1)**.

Figure 2-4 Configuration scheme – remote station
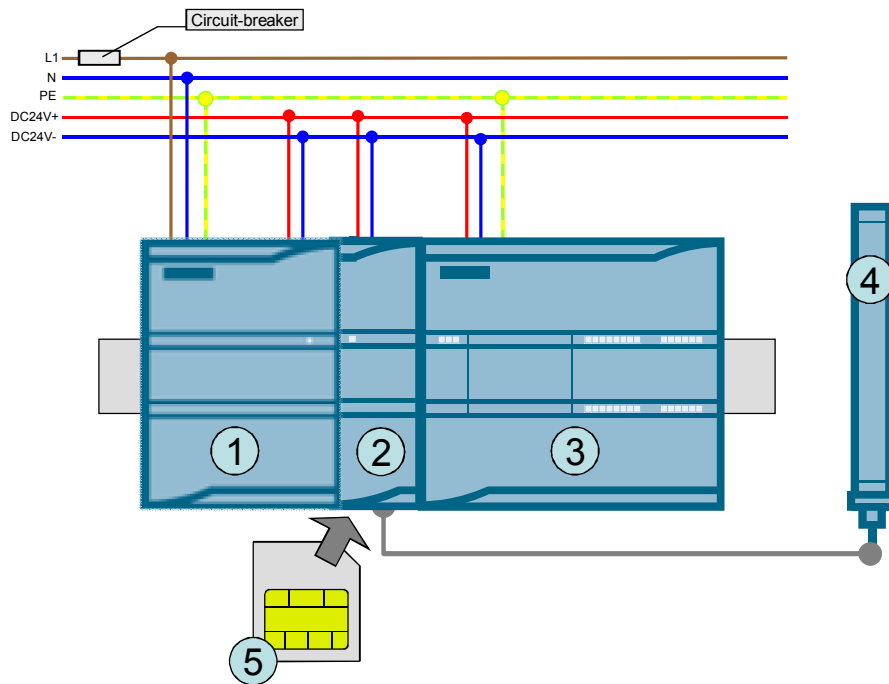
Overview of the communication landscape

The graphic below shows the IP addresses relevant to this variant and which must be known when starting up the system.

Figure 2-5

IP address	Static IP address, provider-specific, private

2.2.2 Hardware and software components used

Remote stations – hardware components

Table 2-6 Variant 2, RS HW components

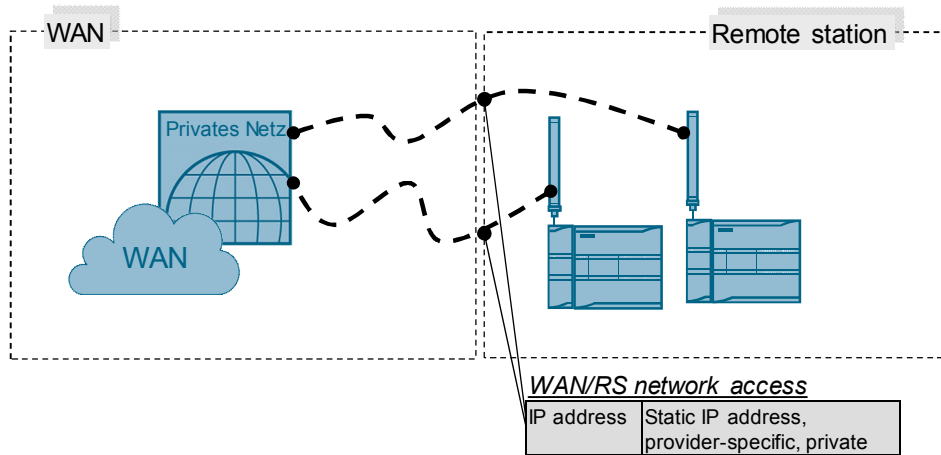| Component	Qty.	Order number	Note
SIMATIC S7-1200, PM 1207	2	6EP1332-1SH71	2.5A
SIMATIC S7-1200, CPU 1214C	2	6ES7214-1AE30-0XB0	DC/DC/DC, FW 2.2.0 or higher, or another type of CPU
SIMATIC CP 1242-7	2	6GK7242-7KX30-0XE0	FW 1.3.0 or higher
SINAUT ANT 794-4MR, rod antenna	2	6NH9860-1AA00	As an alternative: flat antenna ANT794-3M (6NH9870-1AA00)
Ethernet line	1	6XV1870-3QH20	For configuration purposes (2 meters of this type or similar cable)
Circuit-breaker	2	5SX2116-6	1 pole B, 16A
Standard mounting rail	2	6ES5 710-8MA11	35 mm
SIM card	2	Available at your mobile service provider	Please check if special M2M tariffs with included data volumes are available.

Remote stations – standard software components

Table 2-7 Variant 2, RS SW components

Component	Qty.	Order number	Note
STEP 7 Basic V11	1	6ES7822-0AA01-0YA0	Service Pack 2 or higher
Hardware Support Package for CP 1242-7	Internet link \9\		Necessary only for STEP 7 V11

SIM card and contract

This variant does not use a central station which might serve as a fixed access point for the exchange of process data for all other WAN participants. For this reason, the SIM cards or contracts with your mobile service provider for these remote stations must include the following features:

- **Static IP address allocation**: Static IP address allocation means, that a specific participant with a SIM card will always receive the same IP address when establishing a connection. The identification of this terminal is effected

  - a) either by a unique user name and user password for each SIM card

  - b) or by one and the same user name and user password for several SIM cards, but with phone number identification.

  Variant b) is specially suitable for a large number of terminals (with regard to access data) which can then be configured in the same way.

- **Either public IP addresses**: The public IP addresses must be actually visible in the Internet (RIPE allocation criterion, no "quasi public" IP addresses via NAT in the provider network). The visibility of the addresses in the Internet must not be restricted, e.g. by the exclusive use of a tunnel.

- **Or private IP addresses**: <u>Private IP addresses may be used, if the provider can guarantee mutual accessibility across the whole network.</u> This is usually realized with the help of a customer-specific APN.

In this variant, SIM cards with static and private IP addresses are used. This offers better protection during cross-communication against tapping or manipulation by third persons.

Sample files and projects

The following list shows all files and projects used in scenario 2. Only the marked rows are relevant to this variant.

Table 2-8 Project files, variant 2

No.	Component	Note
1.	58099765_Set31_**Var2**_CODE_V10.zip	STEP 7 V11 project for the two remote stations

2.3 Variant "M2M with S7-1200 and S7-300 directly via GPRS"

2.3.1 Overview of the general solution

Remote station 1 and remote station 2

A GSM/GPRS modem **CP 1242-7 (2)** is connected to a **SIMATIC S7-1200 controller 1214C (3)** via the bus interface.

The GSM/GPRS modem is equipped with a **SIM card (5)**, and connection to the air interface is realized with a quad band GSM/GPRS **antenna type ANT 794-4MR (4)**.

All components are supplied with power by a **SIMATIC PM 1207 power module (1)**.

Figure 2-6 Configuration scheme – remote station 1

2 Solution
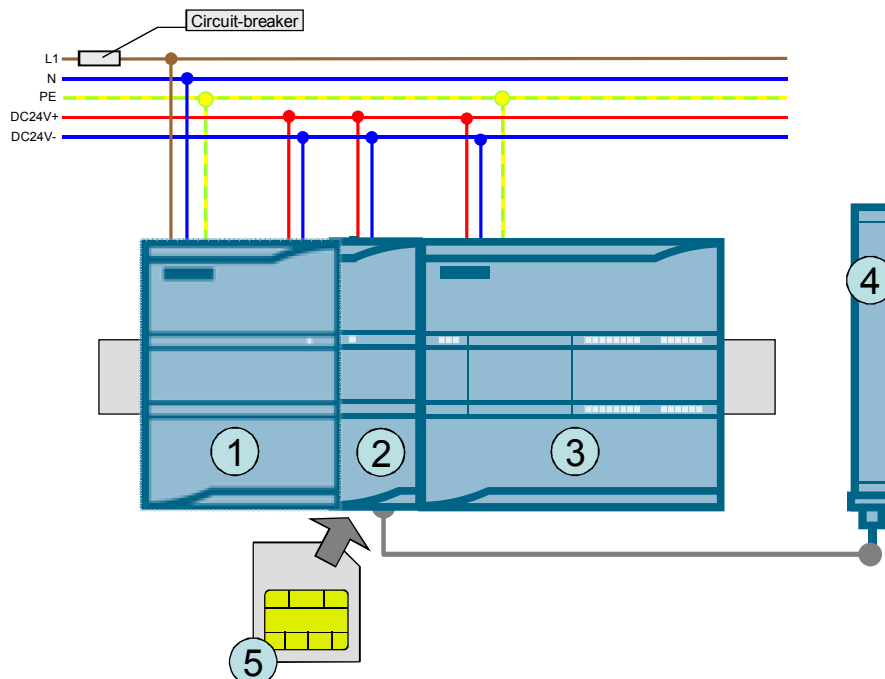
Control station

An UMTS/GSM modem **SCALANCE M873-0 (2)** is connected to a SIMATIC S7-300 controller **315-2 PN/DP (4)**.

The UMTS/GSM modem is equipped with a **SIM card (5)**, and connection to the air interface is realized with a quad band **antenna type ANT 794-4MR (1)**.

All components are supplied with power by a **SIMATIC PS307 Power Module (3)**.

The S7-300 controller is provided with a SIMATIC micro memory card.

Figure 2-7 Configuration scheme – remote station 2

Overview of the communication landscape

The graphic below shows the IP addresses relevant for this variant and which must be known when starting up the system.

Figure 2-8

WAN/RS network access	
IP address	Static IP address, provider-specific, private
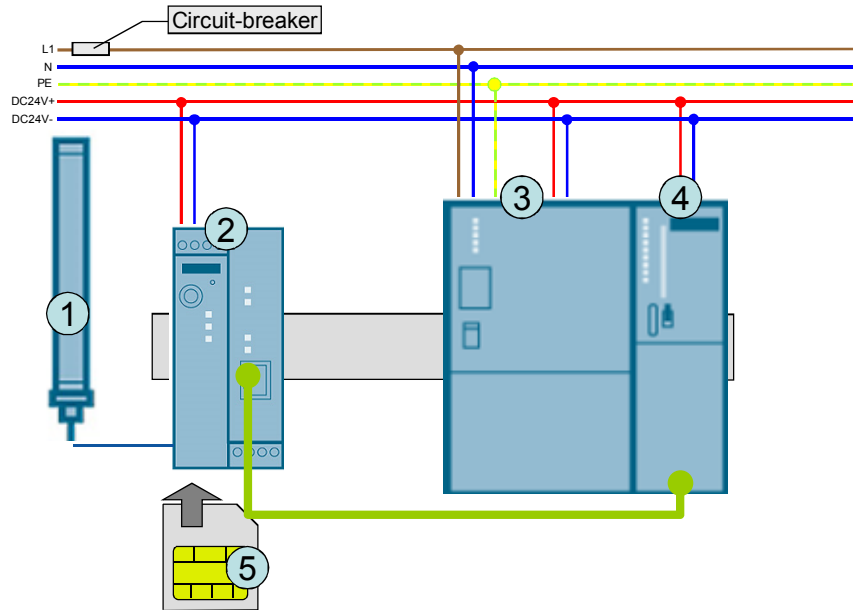
Copyright © Siemens AG 2012 All rights reserved

20

Telecontrol with S7-1200
V1.0, Entry ID: 58099765
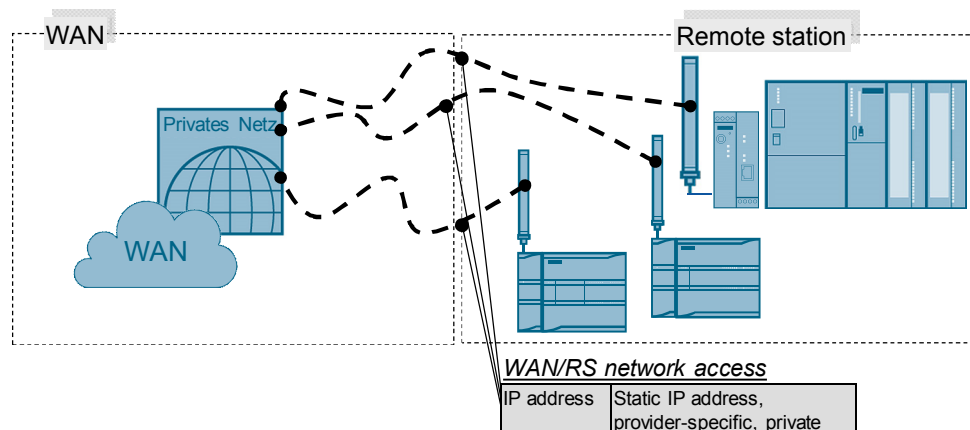
2.3.2 Hardware and software components used

Remote station 1 and remote station 2 – hardware components

Table 2-9 Variant 3, RS1 RS2 HW components

Component	Qty.	Order number	Note
SIMATIC S7-1200, PM 1207	2	6EP1332-1SH71	2.5A
SIMATIC S7-1200, CPU 1214C	2	6ES7214-1AE30-0XB0	DC/DC/DC, FW 2.2.0 or higher, or another type of CPU
SIMATIC CP 1242-7	2	6GK7242-7KX30-0XE0	FW 1.3.0 or higher
SINAUT ANT 794-4MR, rod antenna	2	6NH9860-1AA00	As an alternative: flat antenna ANT794-3M (6NH9870-1AA00)
Ethernet line	1	6XV1870-3QH20	For configuration purposes (2 meters of this type or similar cable)
Circuit-breaker	2	5SX2116-6	1 pole B, 16A
Standard mounting rail	2	6ES5 710-8MA11	35mm
SIM card	2	Available at your mobile service provider	Please check if special M2M tariffs with included data volumes are available.

Control station – hardware components

Table 2-10 Variant 3, S7-300 HW components

Component	Qty.	Order number	Note
SIMATIC S7-300, PS307	1	6ES7307-1BA01-0AA0	2A
SIMATIC S7-300 CPU 315-2 PN/DP	1	6ES7315-2EH14-0AB0	Or another type of CPU with integrated Profinet interface and TCP/IP-support
SIMATIC MMC 64KB	1	6ES7953-8LF20-0AA0	
SCALANCE M873-0	1	6GK5873-0AA10-1AA2	
SINAUT ANT 794-4MR, rod antenna	1	6NH9860-1AA00	As an alternative: flat antenna ANT794-3M (6NH9870-1AA00)
Ethernet line	3	6XV1870-3QH20	2 meters • 1x for configuration • 2x for network connection
Circuit-breaker	1	5SX2116-6	1 pole B, 16A
Standard mounting rail	1	6ES5 710-8MA11	35 mm
SIM card	1	Available at your mobile service provider	Please check if special M2M tariffs with included data volumes are available.

2 Solution

Remote stations 1 and 2 – standard software components

Table 2-11 Variant 3, RS12 SW components

Component	Qty.	Order number	Note
STEP 7 Professional V11	1	6ES7822-1AA01-0YC5	Service Pack 2 or higher
Hardware Support Package for CP 1242-7	Internet link \9\		Necessary only for STEP 7 V11

SIM card and contract

This variant does not use a central station which might serve as a fixed access point for the exchange of process data for all other WAN participants. For this reason, the SIM cards or contracts with your mobile service provider for these remote stations must include the following features:

- **Static IP address allocation**: Static IP address allocation means, that a specific participant with a specific terminal will always receive the same IP address when establishing a connection. The identification of this terminal is effected
  - a) either by a unique user name and user password for each SIM card
  - b) or by one and the same user name and user password for several SIM cards, but with phone number identification.

Variant b) is specially suitable for a large number of terminals (with regard to access data) which can then be configured in the same way.

- **Either public IP addresses**: The public IP addresses must be actually visible in the Internet (RIPE allocation criterion, no "quasi public" IP addresses via NAT in the provider network). The visibility of the addresses in the Internet must not be restricted, e.g. by the exclusive use of a tunnel.

- **Or private IP addresses**: Private IP addresses may be used, if the provider can guarantee mutual accessibility across the whole network. This is usually realized with the help of a customer-specific APN.

In this scenario, SIM cards with static and private IP addresses are used. This offers better protection during cross-communication against tapping or manipulation by third persons. For the SIM card of the SIMATIC S7-300 station, a higher data volume was agreed upon with the provider.

Sample files and projects

The following list shows all files and projects used in scenario 2. Only the marked rows are relevant to this variant.

Table 2-12 Project files, variant 3

No.	Component	Note

1.	58099765_Set31_ **Var3**_CODE_V10.zip
	This file consists of:
	• 58099765_Set31_ Var3_STEP7_V10
	  The STEP 7 TIA V11 project for the S7-1200-based remote station and the S7-300-based control station.
	• 58099765_Set31_SCALANCE_M873_V10.tgz
	  The configuration file for SCALANCE M873-0	

3 Basics on Data Transmission with CP1242-7 and Telecontrol Server Basic

Introduction

The following chapter describes some procedures which are important to understand the main mechanisms in connection with the S7-1200 system, CP 1242-7 and Telecontrol Server Basic.

3.1 Definition of connection-specific features

Introduction

This chapter explains how the different connection types are defined and how to establish a connection with Telecontrol Server Basic.

Overview of the connection characteristics

The function of the remote control system is defined by the following characteristics:

Table 3-1

Parameters	Possible parameter values	Notes
Operating mode	• Telecontrol • GPRS direct	Defined directly in the device configuration and Telecontrol Server Basic. Hereinafter referred to as **main connection**.
Connecting mode	• Permanent • Temporary	
Connection type	• Telecontrol connection • UDP • ISOonTCP • SMS • Teleservice	Programmed in the user program with the help of library blocks. Hereinafter referred to as **sub-connection**. One connection is always reserved for the connection type Teleservice and does not need to be programmed separately.
Connection parameter	Active/passive connection buildup, connection ID, information about the partner station	

Definition of the main connection

The main connection is defined by the selection of the corresponding parameters in the device configuration for the CP 1242-7. In this application example (scenario 2), the following operating mode is selected as connecting mode for the main connection of the remote station:

Table 3-2

Var 1 "M2M telecontrol"	Var 2: "M2M with S7-1200 directly via GPRS" Var 3: "M2M with S7-1200 and S-7300 directly via GPRS"
Operating mode: Telecontrol	Operating mode: GPRS direct
Connecting mode: Permanent	Connecting mode: Temporary
Explanation: Connection of the CP 1242-7 must always be set up via a Telecontrol server	Explanation: Connection of the CP 1242-7 is always set up directly to the partner station and is

Var 1 "M2M telecontrol"	Var 2: "M2M with S7-1200 directly via GPRS" Var 3: "M2M with S7-1200 and S-7300 directly via GPRS"
(central station) and the GPRS connection is maintained permanently.	established or terminated as required.

These parameters are described in detail in document \6\ chapter 4.1.

Definition of the sub-connection

There are several **connection types** available for the sub-connection which, however, are already determined by the selection of the main connection.

The desired connection type is programmed directly in the user program with the help of library blocks.

In this application example, the following sub-connections have been selected:

Table 3-3

Var 1 "M2M telecontrol"	Var 2: "M2M with S7-1200 directly via GPRS" Var 3: "M2M with S7-1200 and S7-300 directly via GPRS"
Connection type: Telecontrol connection	Connection type: ISOonTCP

The selection of different connection types (SDTs) is described in more detail in document \6\ chapters 1.5 and 5.4.7.

**Summary of selected main and sub-connections for all variants**

Table 3-4

Connection	Variant 1 "M2M telecontrol"	Variant 2 "M2M with S7-1200 directly via GPRS"	Variant 3 "M2M with S7-1200 and S7-300 directly via GPRS"
Main connection	Telecontrol	GPRS direct	GPRS direct
Sub-connection	Telecontrol connection	ISOonTCP	ISOonTCP

3.2 Establishing a connection

As soon as a **main connection** with the partner station has been established (depending on the selected variant, either via a central station or directly to the remote station), process data can be transmitted in both directions by means of **sub-connections**.

Depending on the type of main connection, five or four different sub-connections can be used simultaneously.

Figure 3-1 Number of connections available in parallel
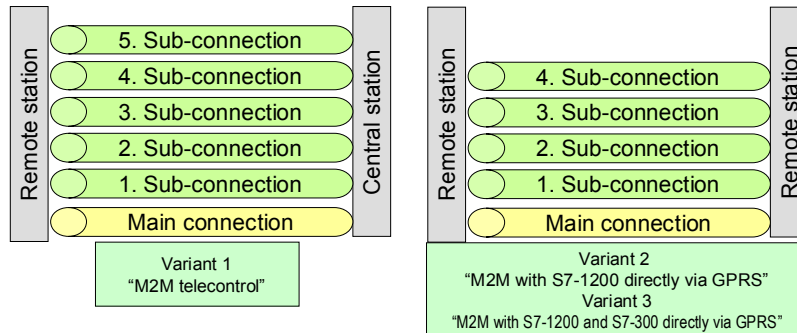
The main connection is pre-requisite for all other sub-connections.

The different sub-connections are built up on demand and, depending on the relevant **type of connection**, they represent a connection

- directly to the central station (telecontrol connection), or
- to another remote station which can be accessed via the central station (telecontrol connection, UDP[send only]), or
- directly to another remote station, without using the central station (ISOonTCP, UDP[send only]), or
- to another device (SMS).

Connection types in this example

In this application example, the following connection types have been selected as sub-connections for the exchange of process data with a partner station.

Figure 3-2
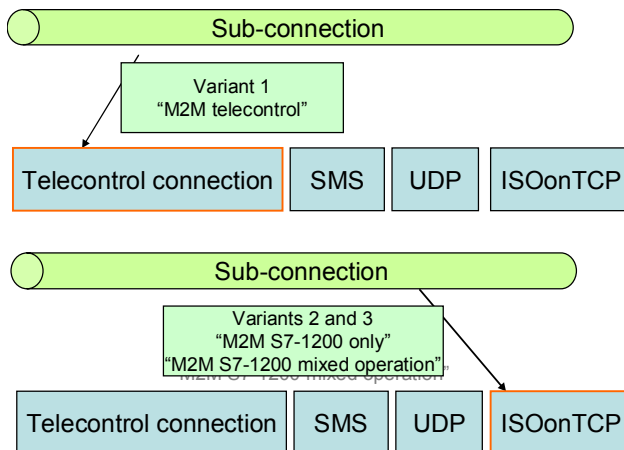
## 3.3 Overview of the GPRS communication platform

Overview

The descriptions below explain the whole system with all parameters required for communication between remote stations and a central station or between several remote stations.

3.3.1 Connection buildup

Variant 1 "M2M telecontrol"

In variant 1, the CP 1242-7 uses a WAN participant as a central access point and for the management of connections to other remote stations.

Figure 3-3
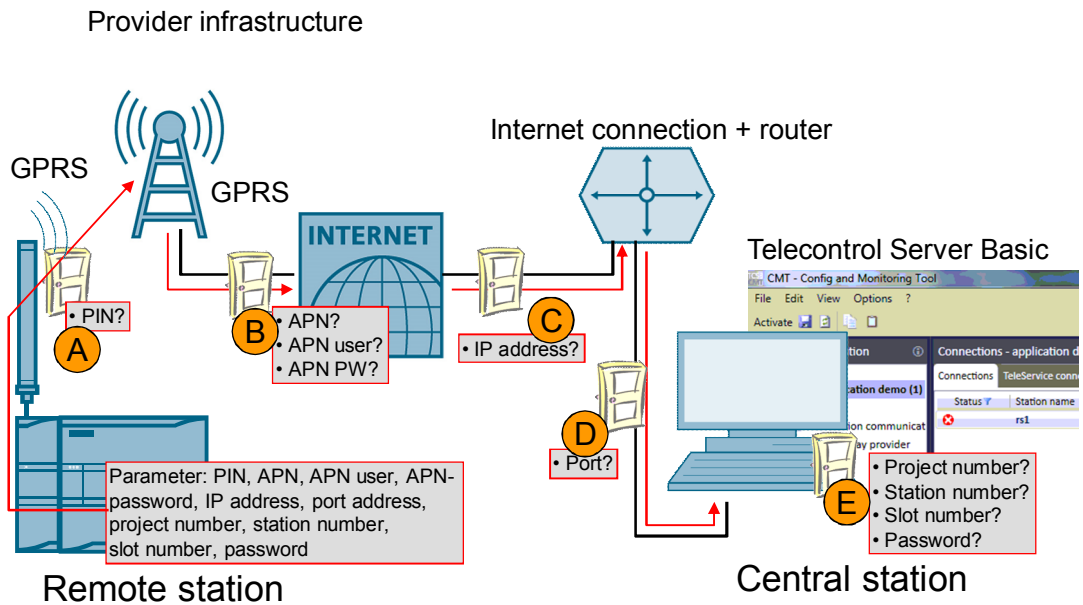
Connection buildup between remote station and central station

Table 3-5 Explanation of connection buildup, Variant 1

Digit	Description
(A)	The CP 1242-7 automatically logs into the provider's GSM network, provided, the **PIN number** of the inserted SIM card has been identified as valid.
(B)	The CP automatically logs into the GPRS access point of the mobile service provider with the help of the **APN address**, the **APN user name** and the **APN user password**. Then an IP address from the provider's address range is allocated to the CP. The modem is now accessible via the Internet and can send IP-based queries to other participants in the Internet.
(C)	The modem sends a request for connection to the central station. This requires the **static IP address** of the Internet connection used for access to the central station. As an option, this can also be effected with a combination of **DNS name server** (in the form of an IP address) and **host address** (in the form of a URL).
(D)	As soon as the connection request has been received by the router of the local IT network of the central station, it will be forwarded to the central station PC/IPC with the relevant **port number**.
(E)	The Telecontrol Server Basic software compares the connection request of the CP with the data defined during configuration. A remote station is always identified by the **project**, **station** and **slot number** (these three numbers form a six-digit identification number). In addition, a **password** for remote station authentication is required. If the connection request is evaluated as valid, Telecontrol Server Basic will update the entry in the internal routing table related to this remote station and the

Digit	Description
	corresponding IP address of the CP. A connection for the transmission of TCP/IP packages is now established. The telecontrol system described above uses this TCP/IP connection for data transmission in both directions using a separate log.

Note

- **Project number** and **station number** must be defined in Telecontrol Server Basic and stored in the remote station.
- The **slot number** is defined by the hardware setup of the remote station (slot number) and must be stored in Telecontrol Server Basic.

Variant 2 "M2M with S7-1200 directly via GPRS"

Variant 2 establishes and maintains an ISO-on-TCP connection directly to a WAN participant with a static, private IP address.
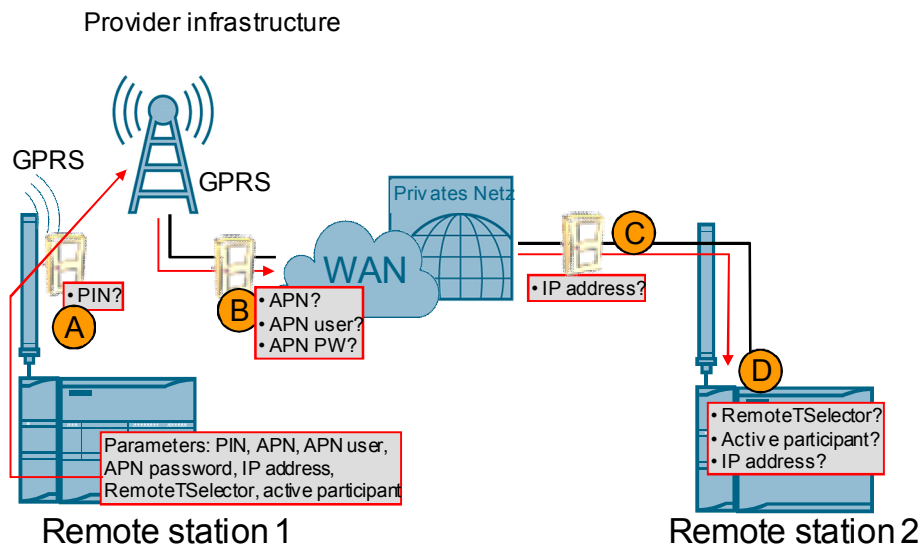
Figure 3-4

Table 3-6 Explanation of connection buildup, variant 2

Digit	Description
(A)	The CP 1242-7 automatically logs into the provider's GSM network, provided, the **PIN number** of the inserted SIM card has been identified as valid.
(B)	The CP automatically logs into the GPRS access point of the mobile service provider with the help of the **APN address**, the **APN user name** and the **APN user password**. Then an IP address from the provider's address range is allocated to the CP. For this station always the same IP address is used. The modem can now be accessed by participants from the same private network and can send IP-based queries to other participants within this network.
(C)	The modem sends a request for connection to the partner station (after having started connection buildup via the TC blocks). The partner station must also be logged into the private network. To do so, the **static IP address** of remote station 2 is required.

Digit	Description
(D)	Remote station 2 checks the connection request from remote station 1 by comparison with the parameters stored in the TC blocks. • Check of the **IP address** • The **RemoteTSelector** included in the transmission from remote station 1 must match with the LocalTSelector parameter of remote station 2. • Remote station 1 is configured as active connection partner. Accordingly, remote station 2 must be defied as a **passive** participant. This will also be checked. If the request for connection is evaluated as valid, an acknowledgement will be sent to remote station 1. The ISO-On-TCP connection is now established and ready for the transmission of process data. Connection buildup is always effected via port 30000. For the subsequent process data communication other ports will be used.

Variant 3 "M2M with S7-1200 and S7-300 directly via GPRS"

Variant 3 establishes and maintains an ISO-on-TCP connection directly to a WAN participant with a static, private IP address. In addition, a further device is used for the port management during the ISO-on-TCP connection buildup.
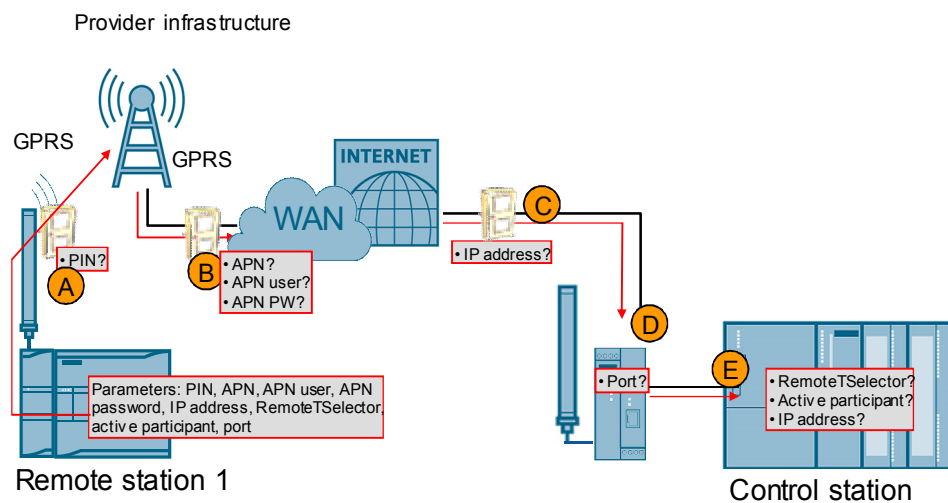
Figure 3-5 Explanation of connection buildup, variant 3

Table 3-7 Explanation of connection buildup, Variant 3

Digit	Description
(A)	The CP 1242-7 automatically logs into the provider's GSM network, provided, the **PIN number** of the inserted SIM card has been identified as valid.
(B)	The CP automatically logs into the GPRS access point of the mobile service provider with the help of the **APN address**, the **APN user name** and the **APN user password**. Then an IP address from the provider's address range is allocated to the CP. This IP address for this station is always the same. The modem can now be accessed by participants from the same private network and can send IP-based queries to other participants within this network.
(C)	The modem sends a request for connection to the partner station (after having started connection buildup via the TC blocks). The partner station with the SCALANCE M873-0 must also be logged into the private network. To do so, the **static IP address** of remote station 2 is required.
(D)	The connection request for ISO-on-TCP communication is effected via **port**

Digit	Description
	30000. The SCALANCE M873-0 requires this information to forward the telegram to the internal IP address of the S7-300 station and to switch over to port 201.
(E)	The control station checks the request for connection from remote station 1 by comparison with the parameters stored in the TC blocks. • The **RemoteTSelector** included in the transmission from remote station 1 must match with the LocalTSelector parameter of the central station. • Remote station 1 is configured as active connection partner. Accordingly, remote station 2 must be defied as a **passive** participant. This will also be checked. If the request for connection is evaluated as valid, an acknowledgement will be sent to remote station 1. The ISO-On-TCP connection is now established and ready for the transmission of process data. SCALANCE M873-0 has changed the port for connection buildup from 30000 to 201. Acknowledgement to remote station 1 is again set to port 30000. The subsequent process data communication will be handled via other ports with no specific settings in the SCALANCE M873-0.

Note   The S7-300 controller does not check the IP address of remote station 1, as it does in variant 2. All connection requests with matching RemoteTSelector and LocalTSelector will be accepted.

3.3.2   Connection management for variant 3

Variants 1 and 2 maintain permanent connections to the partner station. The connection management of variant 3 "M2M with S7-1200 and S7-300 directly via GPRS" is more complex, since the connections remain active only as long as process values are transmitted.

Apart from the parameters for connection buildup described in the above table, the connection management must be configured in the remote station and control station with the help of CON and DISCON blocks.

One connection for each remote station

Each connection to the partner station is maintained permanently.

The S7-300 controller used in this example (Table 2-10) allows up to eight connections for IE communication (here: ISO-on-TCP connections) in parallel. When using an S7-300 controller with a CPU319-3 PN/DP and the maximum number of inserted Ethernet ECs, up to 182 connections can be realized.

Advantage:

• Easy configuration/programming, if only the internal Profinet interface is used.
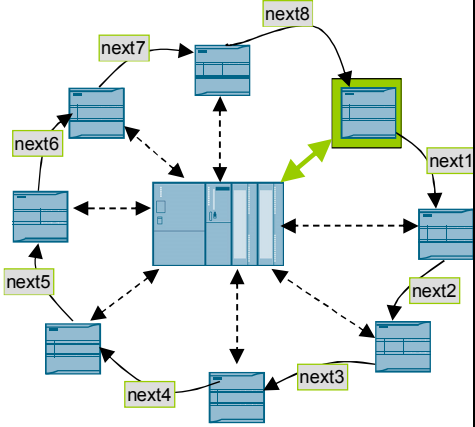• Fastest way to exchange process data between remote station and control station.

Disadvantage:

• In large systems this variant is more expensive.
• The ISO-on-TCP KeepAlive function causes additional data traffic at 30-second intervals.
• The use of the internal Profinet interface in combination with additional LAN CP interfaces (combination of TCON, TCON and AG_SEND, AG_RECEIVE) requires more configuration/programming efforts.

One connection shared by several or all remote stations

Only one connection is used and for the transmission and receipt of process values the remote stations log into the control station one after another. The following procedures can be used to determine which station is next in line:

Table 3-8

Description	Comment
Token <u></u> A token is passed on between the remote stations and determines the remote station which is next to exchange process data with the control station. To do so, the remote station is configured for three connections: • to the preceding remote station • to the control station • to the next remote station The connections used to pass on the token between the remote stations are maintained permanently. Advantage: • Access synchronization is possible also in large systems without causing unforeseeable delays.	 Disadvantage: • Requires great implementation efforts (especially the token management, if some remote stations within the systems fail) • Failure of one remote station will cause considerable delay in the system flow.
Time slots Each remote station is authorized to establish a connection to the control station at any time, and to exchange process data, if connection buildup was successful. If either connection buildup has failed, or if connection buildup has been successful, but the exchange of process data is completed, the next attempt to connect will start after a defined waiting period. Advantage: • Easy to configure/program • Can be easily expanded	The waiting period can be defined as follows: • The waiting period is defined by a fixed time reserved for this remote station to attempt connection . To do so, the clocks of all remote stations should be synchronized with the control station. • The waiting period is defined by a fixed interval (e.g. every 5 minutes). If two remote stations request for connection at the same time, the second one will be rejected. Disadvantage: • Overlapping connection attempts will lead to delays in the system flow. • Not recommended for large systems

Clustering of several remote stations per connection

A segmentation should be configured for all variants.

Example: In the operating mode "GPRS directly", the CP 1242-7 enables four parallel ISO-on-TCP connections. Assuming a number of 16 remote stations, four sub-connections can be configured, so that four remote stations are to be managed for each sub-connection.

3.4 Transmission of process data via a sub-connection

For each sub-connection, there are several options for the control of process data transfer. Having an understanding of the differences is essential, so as to find the best variant for the individual automation task.

Send / Receive block

STEP 7 V11 offers a series of blocks for the control of process data traffic, which are included in the "Hardware Support Package" for the CP 1242-7. The "TC_SEND" command is used to send, and the "TC_RECV" command is used to receive process data via the corresponding sub-connection.

Figure 3-6 Calling "TC_SEND" and "TC_RECV" to control the transfer of process data
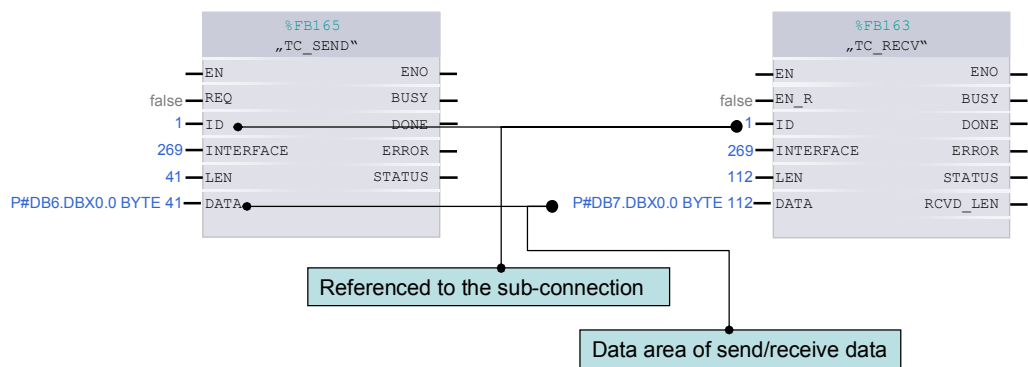
Note   These blocks are handled similar to the Open User Communication in S7-1200 (TSEND, TRECV).
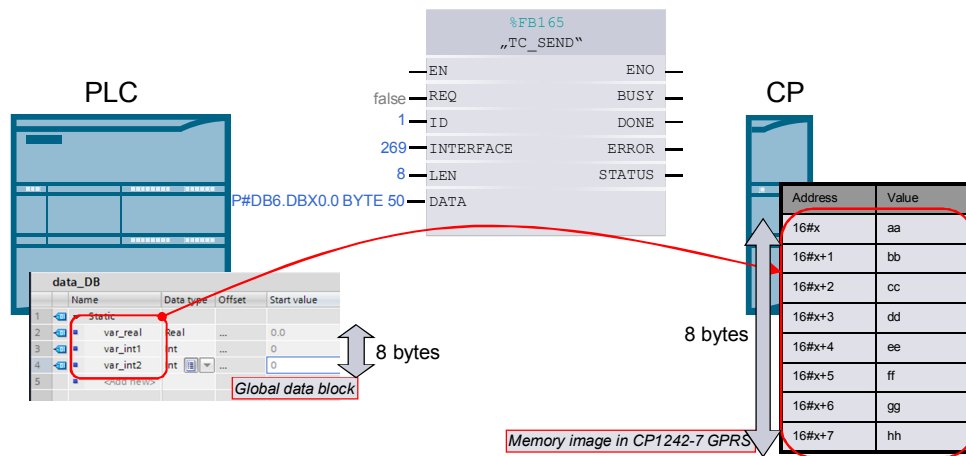
3.4.1 Sending process data with TC_SEND

PLC memory area and CP memory image

The library block "TC_SEND" sends process values from a global data block of the PLC to the memory image of the CP1242-7.

Note   Both TC_SEND and TC_RECV require a separate global data block.

Figure 3-7

The size of the defined PLC memory area for this sending process also determines the CP memory image to be transmitted to the partner station.

Parameter LEN of the library block "TC_SEND"

The parameter "LEN" indicates the size of the data area to be transmitted from the global data block. In this case, the length of the pointer at the parameter "DATA" is irrelevant.

Parameter DATA of the library block "TC_SEND"

The area transmitted from the global data block always starts with byte 0, irrespective of the start value indicated by the pointer.

Note	• It is not possible to write to data areas in the memory image of the CP1242-7 only partially.
	• The global data block for "TC_SEND" and the global data blocks of the process values in the user program should be separated. This facilitates the handling of modification in the data structure at a later point.

Memory organization in the global data block and in the CP's memory image

During the transmission of process values, the data type information gets lost. Consequently, the partner station must interpret the transmitted data area anew.

The parameterized block access for the global data block must always be defined as "standard compatible with S7-300/400".

3.4.2 Receiving process data with TC_RECV

PLC memory area and CP image

The library block "TC_RECV" receives the process values from the memory image of the CP1242-7 and transmits them to a global data block.

Note	Both TC_SEND and TC_RECV require a separate global data block.

Mechanism in general

During the send routine, the size of the CP image to be transmitted is defined by the PLC memory area for the "TC_SEND" library block.

During the receive routine, the partner station (in this application: another remote station) defines the number of process values to be transmitted. Those will be stored in the CP image without restrictions. How many of these process values shall be transmitted from this CP-Image to the PLC memory area is defined in the library block.

Parameter LEN of the library block "TC_RECV"

The parameter "LEN" indicates the size of the data area to be transmitted from the CP 1242-7. In this case, the length of the pointer at the parameter "DATA" is irrelevant.

Parameter DATA of the library block "TC_RECV"

The data area transmitted by the CP 1242-7 always starts with byte 0 of the global data block, irrespective of the start value indicated by the pointer.

Note	It is not possible to influence the memory area of incoming process values.

Parameter RCVD_LEN of the library block "TC_RECV"

If the data area from the partner station and received at the CP1242-7 is larger than or equals the parameter LEN of the library block "TC_RECV", the value of the parameter "LEN" will be output.

If the data area received is smaller than the parameter LEN of the library block "TC_RECV", the actually received size of the data area will be output.

Notice	It is not possible to identify which incoming process values were or were not changed by the partner station. For this reason, it is necessary to check the incoming process values for value changes.

Mechanism by example

The variables "real1", "int1" and "dword" from PLC1 correspond exactly to the variables from PLC2. The memory image cannot be shifted. The declaration of variables and the internal memory area of the data block between TC_Send and TC_Recv at the partner station need not match exactly. The DB may vary.

Figure 3-8 Recv by the example of "PLC 2 sending to PLC 1"
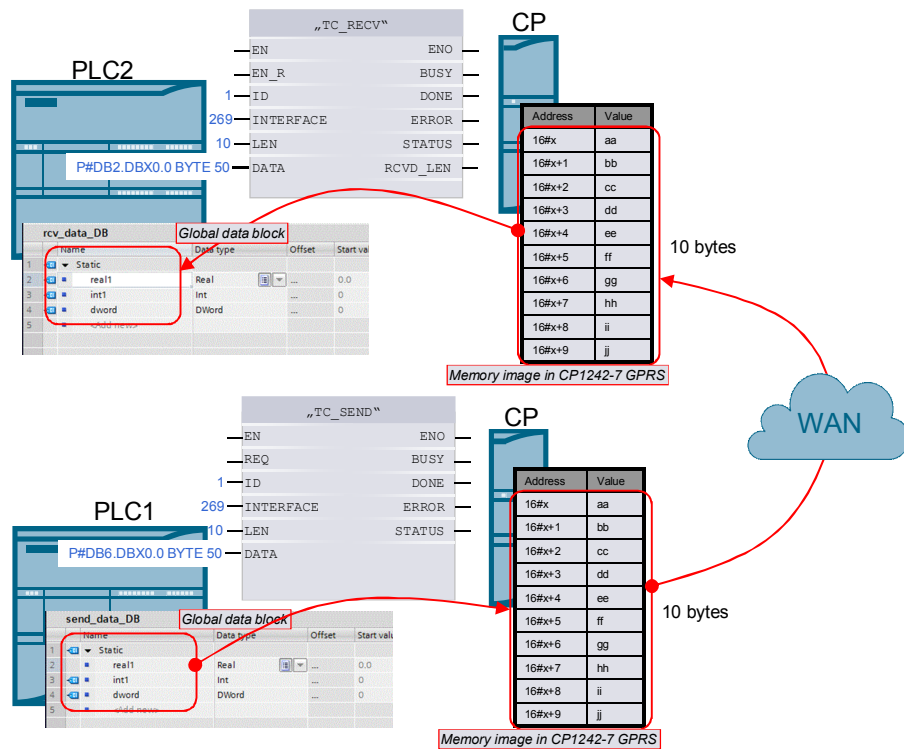
4 Functional Mechanisms of the Application

In this chapter we present the solution elements and their programmed implementation which result from the requirements implied in the individual application examples.

Overview of the process data transfer control

The table below shows an overview of all possible types for the control of process data transfer in these variants.

Table 4-1 Mechanisms for the control of process data transfer

No.	Variant	Direction	Initiator	Trigger type	Description
1.	M2M telecontrol	RS1 → RS2	RS1	cyclic	RS 1 and RS 2 send process values to each other at cyclic intervals using a permanently established connection.
2.	M2M telecontrol	RS1 ← RS2	RS2	cyclic	
3.	M2M with S7-1200 directly via GPRS	RS1 → RS2	RS1	cyclic	RS 1 and RS 2 send process values to each other at cyclic intervals using a permanently established connection.
4.	M2M with S7-1200 directly via GPRS	RS1 ← RS2	RS2	cyclic	
5.	M2M with S7-1200 and S7-300 directly via GPRS	RS n → CS (control station)	RS n	cyclic	RS 1 and RS 2 alternately build up connection to the CS for the transmission of process values.
6.	M2M with S7-1200 and S7-300 directly via GPRS	RS n ← CS (control station)	CS	event	Immediately after the receipt of process values from RS 1 or RS 2, the CS sends own control values to the remote station currently connected.

## 4.1 Control of process data transfer in variant 1 "M2M telecontrol"

4.1.1 Control of connection establishment / termination

Program overview

The user programs of all variants are identical with regard to the number and calling structure for functions and data blocks. The DB numbers may vary.

Calling the library blocks TC_SEND and TC_RECV, as well as the control of connection establishment and termination with TC_CON und TC_DISCON is realized in the function block "Z_call_telecontrol_blocks".

Figure 4-1
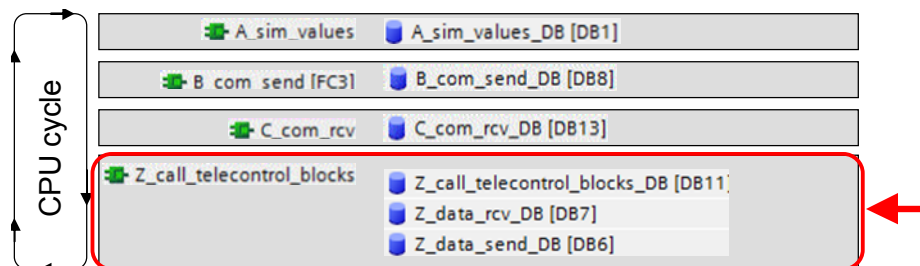
Connection management

Using the functions TC_CON and TC_DISCON is the easiest way to implement the connection management for variant 1 "M2M telecontrol". If correctly defined in the device configuration, the CP will ensure that the main connection to Telecontrol Server Basic will be maintained.

This is prerequisite to the sub-connection controlled with TC_CON and TC_DISCON, which also needs to be established successfully only once. This implies that only a connection resource will be reserved internally in the PLC, not a handshake or similar procedure with the partner station or Telecontrol Server Basic.

After successful establishment of a sub-connection, connection management will be effected without requiring further intervention until the PLC is started up anew.

The "connect_state" variable in the startup code is used to signal a properly functioning or failing connection to the partner station for other TC mechanisms. The status of "connect_state" is controlled as follows:

Figure 4-2
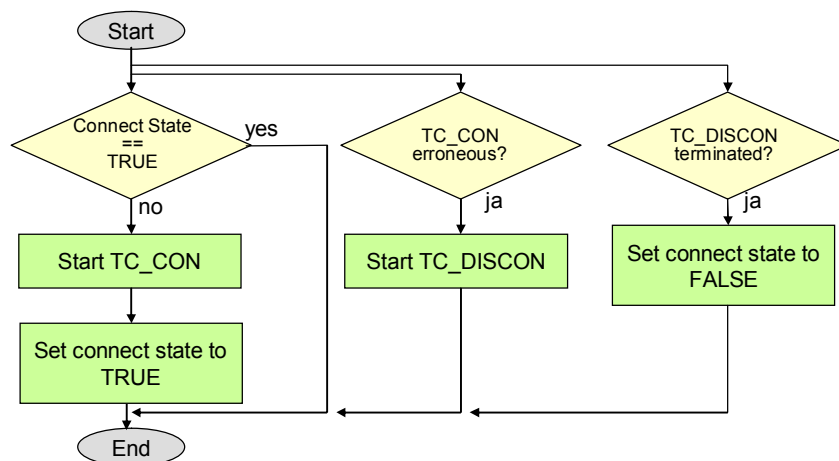
The functions "TC_SEND" and "TC_RECV" will be used only, if the status of "connect_state" is TRUE.

Note   The CP1242-7 reliably ensures an appropriate GPRS connection to the Telecontrol Server Basic. It is not reasonable to intervene in the connection management on user program level through any types of analyses, since the output parameters "done" and "error" at TC_SEND and TC_RECV (in "telecontrol" operating mode) only signal the transmission of user data to the CP, but not an successful or unsuccessful data transmission to the partner station or the Telecontrol Server Basic.
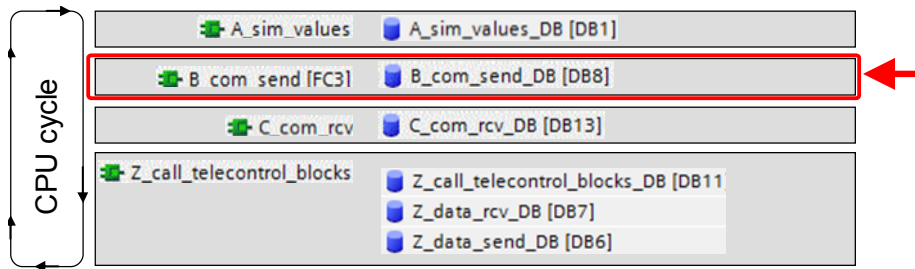
4.1.2   Cyclic transmission of process values to the partner station

Program overview

In all variants, data transmission is effected at cyclic intervals and not initiated spontaneously by a specific event.

In variant 1 "M2M telecontrol", this cyclic transmission is performed over a permanently established main connection and sub-connection.
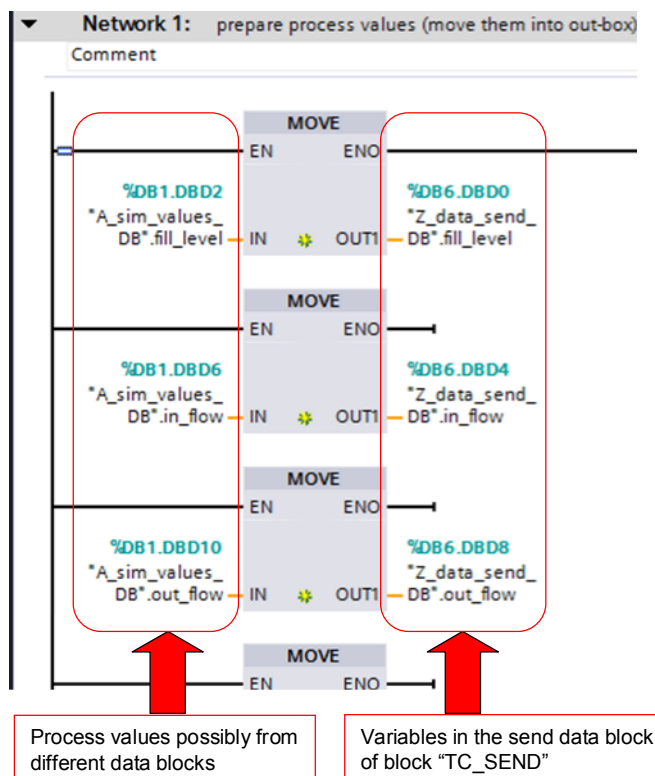
Figure 4-3

Note	The blocks for the CP1242-7 required for data transmission are TC_CON, TC_DISCON, TC_SEND and TC_RECV. With S7-300, the blocks TCON, TDISCON, TSEND and TRCV are used.

**Storing the process values in the send block**

Figure 4-4

This procedure is performed in each cycle and it is identical for all variants. The (simulated) values from the plant are stored in the send block which is accessed by the block TC_SEND.

Operating the time switch and starting the send function

In all variants, the time switch is implemented with the help of a flag in the S7-1200 CPU.

Figure 4-5
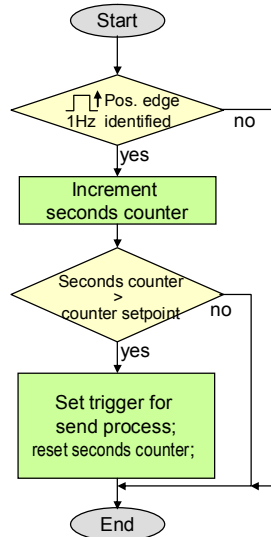
In variant 1 "M2M telecontrol" this routine is used for direct access to TC_SEND. The connection with the partner station remains permanently active.

4.1.3 Receiving process values from the partner station

Program overview

The receipt of process values from the partner station is realized in function block "C_com_rcv". It is identical for all variants.

Figure 4-6
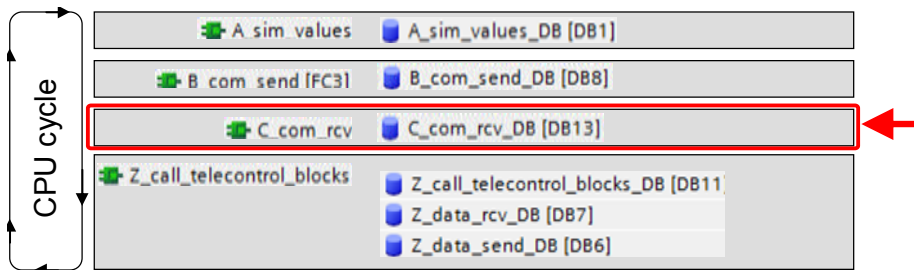
Identify the receipt of new process values and copy them from the receive data block

Figure 4-7

Data block at the receive data block "TC_RECV"	Variables in the data block for further use in the process
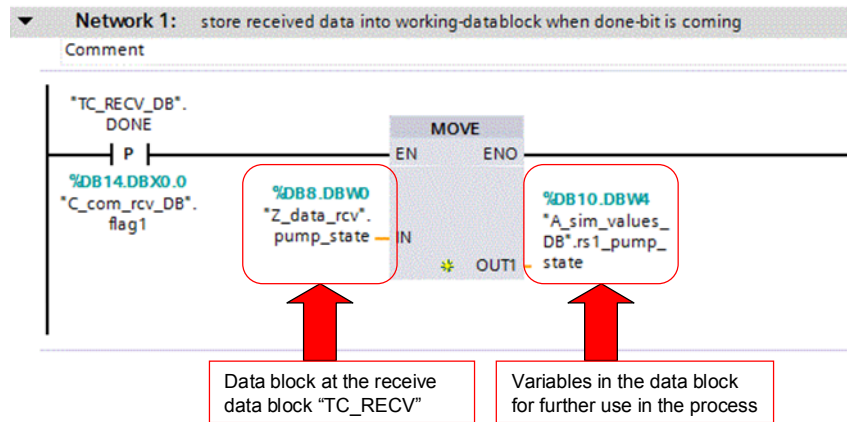
In all variants, the receipt of process data from the partner station is identified by means of the "done" output of the blocks TC_RECV or TRCV.

## 4.2 Control of process data transfer in variant 2 "M2M with S7-1200 directly via GPRS"

4.2.1 Control of connection establishment / termination

Program overview

The user programs of all variants are identical with regard to the number and calling structure for functions and data blocks. The DB numbers may vary.

Calling the library blocks TC_SEND and TC_RECV, as well as the control of connection establishment and termination with TC_CON und TC_DISCON is realized in the function block "Z_call_telecontrol_blocks".

Figure 4-8
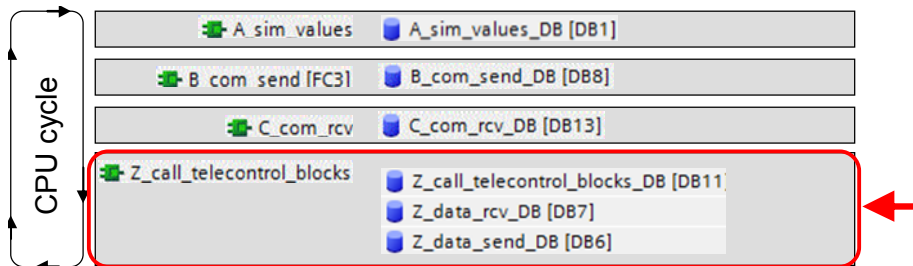
Connection management

In variant 2 "M2M with S7-1200 directly via GPRS", the connection management uses the functions TC_CON and TC_DISCON to establish an ISO-on-TCP connection to the partner station.

After successful connection buildup, the faultless exchange of data must be checked continuously. If sending attempts fail or if there is no communication over a certain period of time, connection must be terminated and established anew.

The "connect_state" variable in the start-up code is used to signal a properly functioning or erroneous connection to the partner station for further TC mechanisms. The status of the "connect_state" is controlled as follows:

Figure 4-9
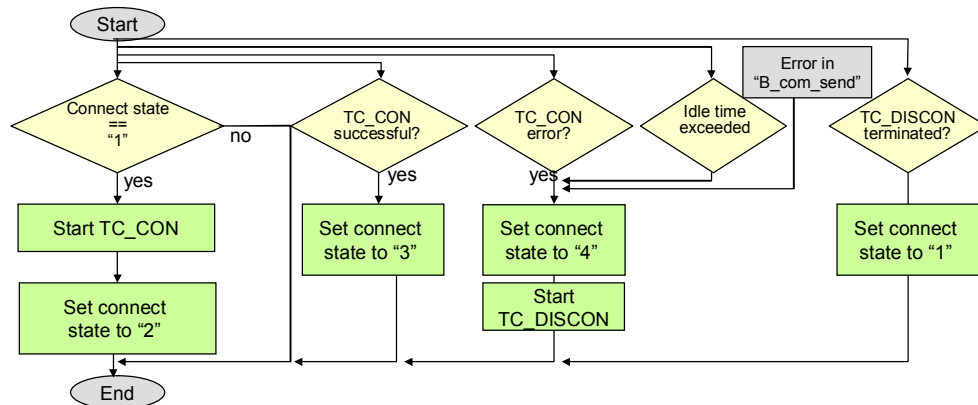
The functions "TC_SEND" and "TC_RECV" will be used only, if the value of "connect_state" shows three.

## 4.2.2 Cyclic transmission of process values to the partner station

Program overview

In all variants, data transmission is effected at cyclic intervals and not initiated spontaneously by a specific event.

In variants 1 "M2M telecontrol" and variant 2 "M2M with S7-1200 directly via GPRS", this cyclic transmission is performed via a permanently established main connection and sub-connection.

In variant 3 "M2M with S7-1200 and S7-300 directly via GPRS", the connections to the control station are established and terminated at fixed intervals. When a connection has been established, the process values are transmitted in both directions. This is also referred to as a cyclic data transmission.
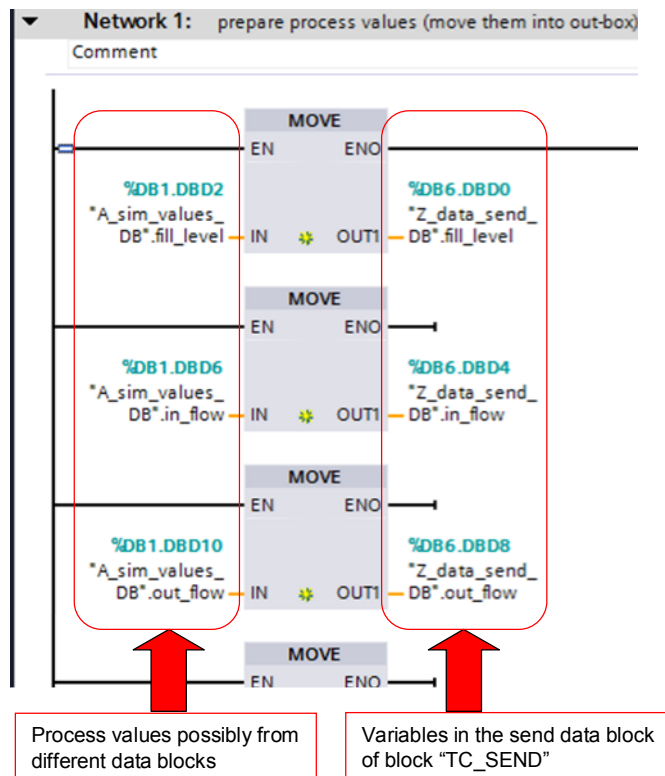
Figure 4-10
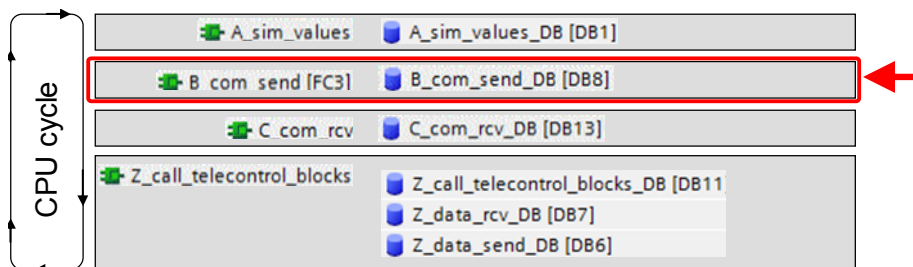
| Note | The blocks for the CP1242-7 required for data transmission are TC_CON, TC_DISCON, TC_SEND and TC_RECV. With S7-300, the blocks TCON, TDISCON, TSEND and TRCV are used. |

## Storing the process values in the send block

Figure 4-11

This procedure is performed in each cycle and it is identical for all variants. The (simulated) values from the plant are stored in the send block which is accessed by the block TC_SEND.

Operating the time switch and starting the send function

In all variants, the time switch is implemented with the help of a flag in the S7-1200 CPU.
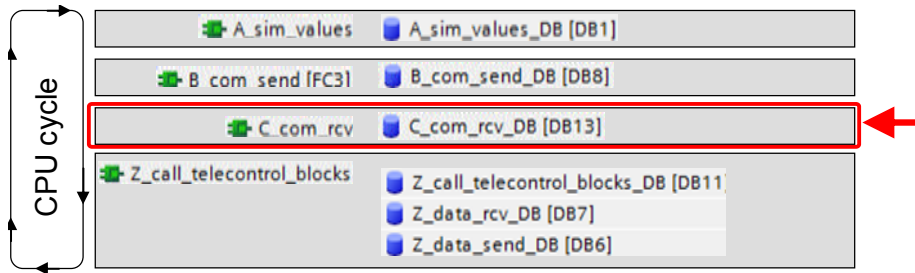
Figure 4-12
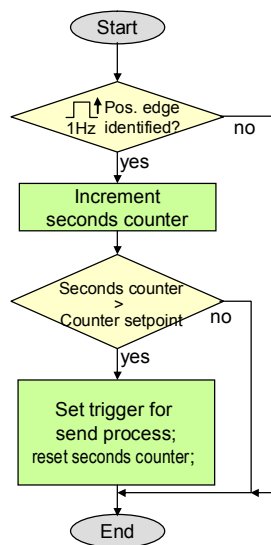
In variant 1 "M2M telecontrol" and variant 2 "M2M with S7-1200 directly via GPRS" this routine is used for a direct access to TC_SEND. The connection with the partner station remains permanently active.

4.2.3 Receiving process values from the partner station
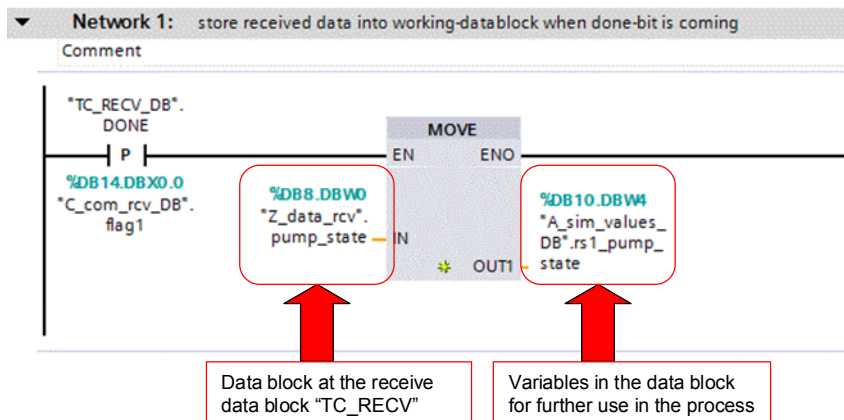
Program overview

The receipt of process values from the partner station is realized in function block "C_com_rcv". It is identical for all variants.

Figure 4-13

Identify the receipt of new process values and copy them from the receive data block

Figure 4-14

In all variants, the receipt of process data from the partner station is identified by the "done" output of the blocks TC_RECV or TRCV.

4.3 Control of process data transfer in variant 3 "M2M with S7-1200 and S7-300 directly via GPRS"

4.3.1 Control of connection establishment / termination

Program overview

The user programs of all variants are identical with regard to the number and calling structure for functions and data blocks. The DB numbers may vary.

Calling the library blocks TC_SEND and TC_RECV, as well as the control of connection establishment and termination with TC_CON und TC_DISCON is realized in the function block "Z_call_telecontrol_blocks".

Figure 4-15
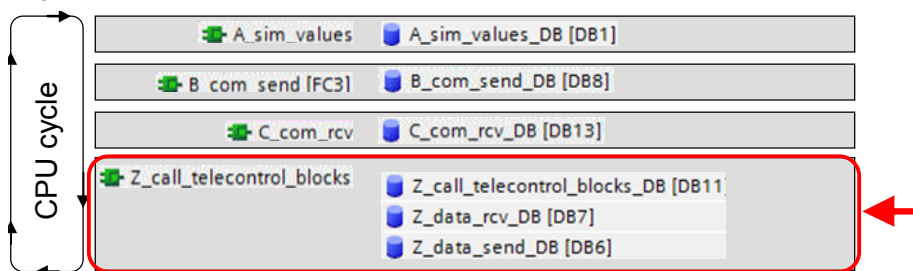
Connection management in variant 3

In variant 3 "M2M with S7-1200 and S7-300 directly via GPRS", the connection management uses the functions TC_CON and TC_DISCON (S7-1200) and TC_CON and TC_DISCON (S7-300) to establish an ISO-on-TCP connection to the partner station.

After successful connection buildup, the process values are transmitted before the connection is terminated again, so that the next remote station can build up a connection to the control station.

The "connect_state" variable in the start-up code is used in the remote stations and in the control station to inform the send and receive routines about a properly functioning or faulty connection to the partner station. The status of "connect_state" in the remote stations (active partner) is controlled as follows:

Figure 4-16
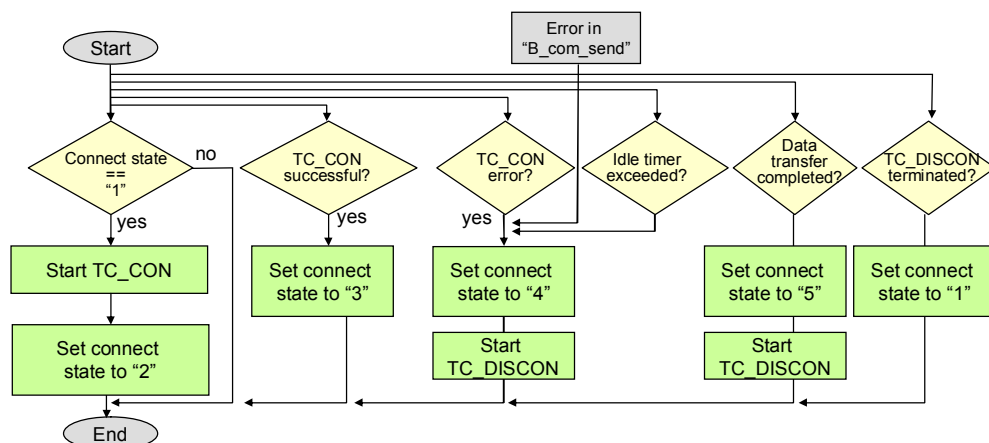
The functions "TC_SEND" and "TC_RECV" will be used only, if the value of the "connect_state" shows 3.

After successful or unsuccessful termination of data transmission, the next connection buildup will start after a waiting period of 15 seconds. During this period, the remote station can establish a connection to the control station.

4.3.2 Cyclic transmission of process values to the partner station

Program overview

In all variants, data transmission is effected at cyclic intervals and not initiated spontaneously by a specific event.

In variant 3 "M2M with S7-1200 and S7-300 directly via GPRS", the connections to the control station are established and terminated at fixed intervals. When a connection has been established, the process values are transmitted in both directions. This is also referred to as a cyclic data transmission.
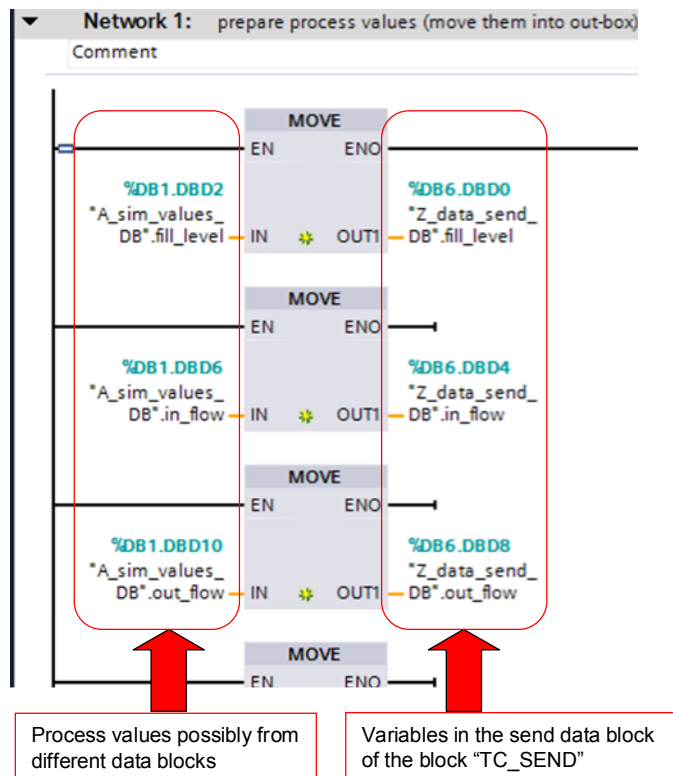
Figure 4-17
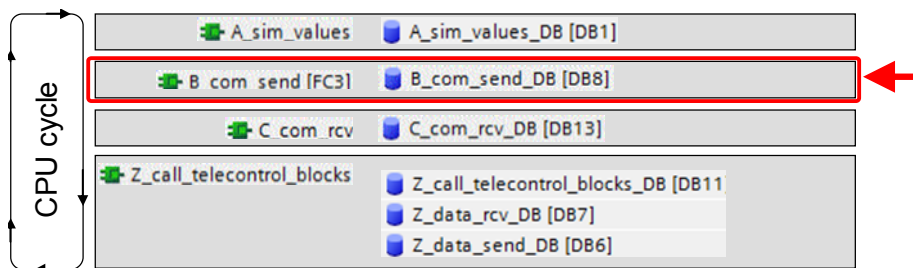
Note	The blocks for the CP1242-7 required for data transmission are TC_CON, TC_DISCON, TC_SEND and TC_RECV. With S7-300, the blocks TCON, TDISCON, TSEND and TRCV are used.

Storing the process values in the send block

Figure 4-18

|	
Process values possibly from different data blocks	Variables in the send data block of the block "TC_SEND"

This procedure is performed in each cycle and it is identical for all variants. The (simulated) values from the plant are stored in the send block which is accessed by the block TC_SEND.

Starting the send process

In variant 3 "M2M with S7-1200 and S7-300 directly via GPRS", the cyclic behavior is realized by the connection management (connection buildup at 15-second intervals, see chapter 4.3.1).

The send routine identifies an established connection and with the help of TC_SEND, the send mechanism will be immediately initiated. Since the connection between remote station and control station does not remain permanently active, a seconds counter for timeout monitoring is implemented.

Figure 4-19
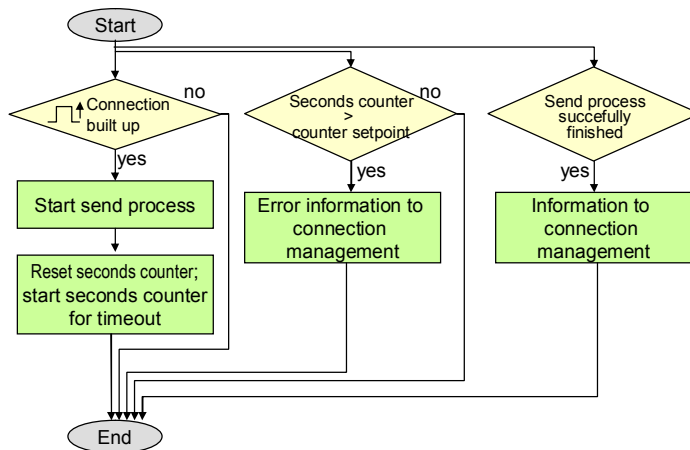
As described above, the control station does not require an active connection buildup. The control station waits until any remote station establishes a connection and until transmission from this remote station is completed. The end of transmission is signaled by the TRCV in the control station. Then the process values from the control station are sent to the remote station currently connected.
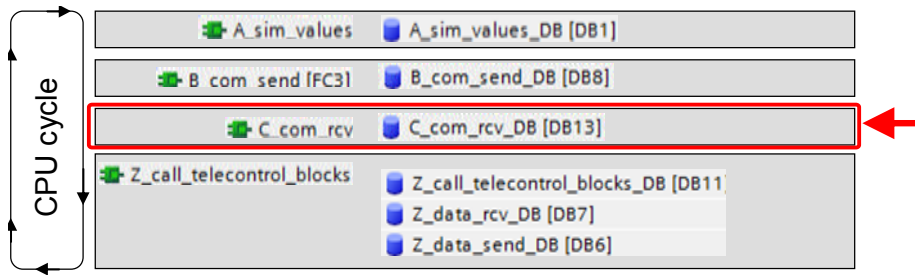
Figure 4-20
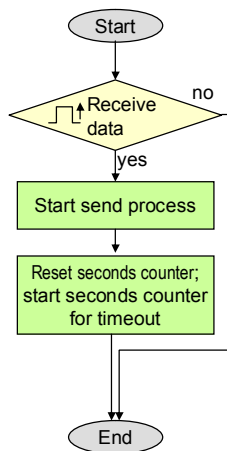
3. Send process and reset trigger

The send process is started by calling "TSEND" in the S7-300 using the function "Z_connect_and_disconnect". „Z_connect_and_disconnect". The trigger for the send function is also reset here.

4.3.3 Receiving process values from the partner station
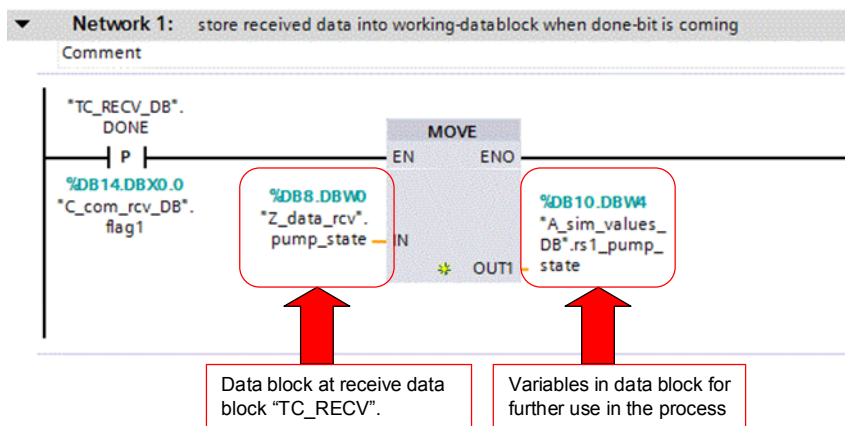
Program overview

The receipt of process values from the partner station is realized in function block "C_com_rcv". It is identical for all variants.

Figure 4-21

Identify the receipt of new process values and copy them from the receive data block

Figure 4-22

In all variants, the receipt of process data from the partner station is identified by the "done" output of the blocks TC_RECV or TRCV.

5 Starting up the Application

5.1 Hardware installation and wiring

Hardware installation

Table 5-1

No.	Action	Notes
1	Install all required components on the DIN rails.	See components list • Variant "M2M telecontrol" chapter 2.1.2 • Variant "M2M with S7-1200 directly via GPRS" chapter 2.2.2 • Variant "M2M with S7-1200 and S7-300 directly via GPRS" chapter 2.3.2
2	Wire and connect all components required for the remote station, the control station and central station as described. Activate the power supply for the SIMATIC PM 1207 only after completion of the above steps.	See wiring schemes: • Variant "M2M telecontrol" • Variant 2 "M2M with S7-1200 directly via GPRS" • Variant 3 "M2M with S7-1200 and S7-300 directly via GPRS"

CAUTION	**Take note of proper ground connection of the components.**

Note	Insert the SIM card in the CP 1242-7 only after having loaded the correctly configured startup code into the controller. Otherwise, the SIM card will be locked because the PIN number is wrong. If this happens, insert the SIM card into a mobile phone and enter the PUK number (super PIN) manually to unlock the SIM card again.

5.2 Configuration instructions

Network parameters

The following table lists all components and the associated network-relevant parameters and, if available, the parameter values in the startup projects.

The devices should be set to these IP addresses, so as to ensure trouble-free configuration when following the instructions in this chapter.

Table 5-2

Component	Designation	Variant	Parameter	Value
CPU S7-1200	Remote station 1	1,2,3	Internal IP address	192.168.0.1
CP 1242-7			External IP address	Specific to the provider; must be known for parameter assignment in variants 1 and 2, but not in variant 3.
CPU S7-1200	Remote station 2	1,2	Internal IP address	192.168.0.2

Component	Designation	Variant	Parameter	Value
CP 1242-7			External IP address	Specific to the provider; must be known for parameter assignment in variants 1 and 2, but not in variant 3.
SCALANCE M873-0	Control station	3	Internal IP address	192.168.0.4
SCALANCE M873-0			External IP address	Specific to the provider; must be known for parameter assignment
CPU S7-300			Internal IP address	192.168.0.3
Router/ DSL-modem	Central Station	1	Internal IP address	192.168.0.5
PC/IPC			Internal IP address	192.168.0.6
KTP1000 (simulated in the TIA portal)	HMI	1,2,3	Internal IP address	192.168.0.10
Programming unit	PG	1,2,3	Internal IP address	192.168.0.100

If not explicitly specified otherwise by the GPRS provider, the subnet mask is 255.255.255.0.

Note The provider-specific "external" IP addresses must be requested from the relevant provider or they are listed in the corresponding contract, respectively. Often online platforms for SIM card management are available.

Note The "internal" IP addresses of the above-listed devices can be changed as follows:

- S7-1200: With the S7-1200 tool, the IP address of the CPU can be changed quite easily (see link \10\). As an alternative, you may use the TIA portal and proceed as described in the S7-1200 system manual (see document \7\ chapter 5.6.4 pp).
- SCALANCE M873-0: The IP address of the UMTS modem when delivered is 192.168.1.1. Go directly to the relevant web site and change the IP address with the help of your browser (user name: admin, password: scalance)
- S7-300: With the Primary Setup tool, the IP address of the CPU can be changed quite easily (see link \11\). As an alternative, you may use the TIA portal and proceed as described in the S7-1200 system manual (see document \7\ chapter 5.6.4 pp).

5.2.1 Configuration of the central station

This chapter refers only to variant 1, "M2M telecontrol".

Note If you do not wish to overwrite your existing "Smsc.sqlite" configuration file with the configuration file supplied here, you have to create a station in Telecontrol Server Basic with the following properties:
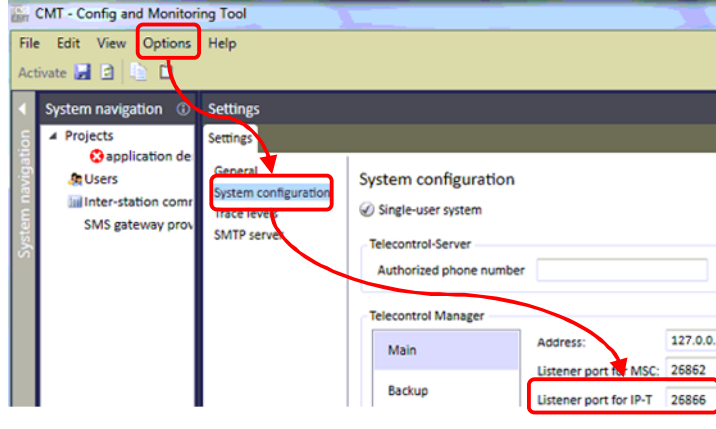
- Project number: 1 (the project name is not relevant)
- Station number: 1 (the station name is not relevant)
- Telecontrol password: "GEHEIM123"

This is the only way to make sure that all further startup data provided here will function properly.

Table 5-3

No.	Action	Notes
1	Install all software components on your central station PC.	• Telecontrol Server Basic • As an option: SIMATIC OPC Scout
2	Establish an Internet connection on your PC. Allocate the network addresses to all network participants as stated in Table 5-2.	• It is assumed that the router is already connected to the internet. • Check the internet connection of your central station with the help of an internet browser and by calling up any internet page.
3	• Enable port forwarding at the router for port 26866 to the IP address of the PC/IPCs. • If you have activated a firewall on your central station PC/IPC, define an exception for port 26866.	
4	If opened beforehand, the Telecontrol Manager of the Telecontrol Server Basic software must be closed now. Click the relevant icon in the Windows info area and select "Exit".	
5	Copy the file "Snmc.sqlite" (see file Table 2-5 , project file no. 2) into the working directory of Telecontrol Server Basic. Please note, that any previous configurations in Telecontrol Server Basic may get lost! Please also see the "Note" at the end of the table.	**Storage path** C:\ProgramData\Siemens\Automation\TCS Basic\Data Please note that the "ProgramData" folder is hidden. **Wrong storage path** The installation directory C:\Programs\...\...) also includes a file named "Smsc.sqlite". This file must not be overwritten.
6	Select "Start > Programs > Siemens Automation > SIMATIC > TCS Basic > Config and Monitoring Tool" to open the "Config and Monitoring Tool". Click the "Activate" button to enable configuration.	The station "rs1" in the project "application demo" must now show a white "x" on a red background.
7	Select "Start > Programs > Siemens Automation > SIMATIC > TCS Basic > Telecontrol Manager" to start the Telecontrol Manager anew.	
8	Check the settings for station "rs1" in the "Database" info window (see the "Note" at the end of this table). 	
9	Check the IP-T port settings in the "Config and Monitoring Tool". It must show 26866.	

No.	Action	Notes

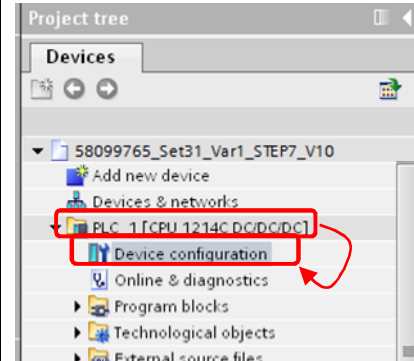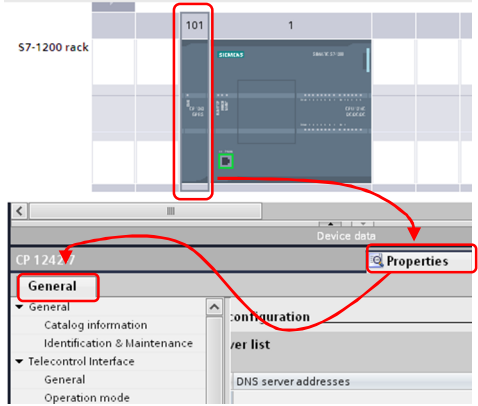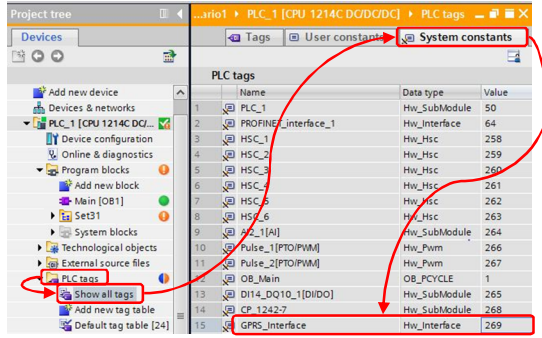| **Note**	The Telecontrol Manager has two functions which can be activated with shortcut keys: • STRG + ALT + double click on the TCS icon opens the "Database" info window. • STRG + SHIFT + double click on the TCS icon in the task bar opens the "Log and Trace Control" window.

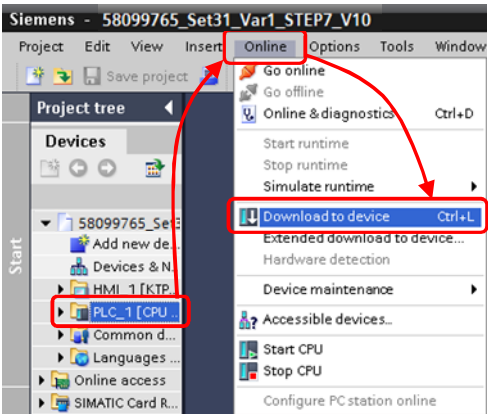| **Note**	The default password for the "Config and Monitoring Tool" is "0000".

5.2.2 Configuration of the remote stations (S7-1200)

This chapter is relevant for all variants. Please take note of the differences in the parameter assignment for the individual variants which are highlighted in yellow.

Table 5-4

No.	Action	Notes
1	Interconnect the S7-1200 controllers with your programming device. Assign the Ethernet parameters for all remote stations as stated in Table 5-2.	Allocate an IP address to S7-1200: See document \7\ chapter 5.6.4.
2	Open the STEP 7 V11 project for your variant.	• Variant 1: Table 2-5 No. 1 • Variant 2: Table 2-8 No. 1 • Variant 3: Table 2-12 No. 1
3	Open the "Device configuration" for the relevant controller, e.g. "PLC_1".	

No.	Action	Notes
4	Select the CP 1242-7 and open the "Properties" dialog where you can enter the connection parameters. Define the parameters for the relevant remote station according to your selected variant as described in the following steps. A detailed description of the parameters, is available in document \6\ chapter 5.2.	
5	Enter the static IP address for the modem, see Table 5-2.	Select "Telecontrol Interface > Operation mode > Assign CP 1242-7 to Telecontrol Server" (name or IP address) **Variant 1**
6	Enter the PIN number for the SIM card placed in the modem. Many M2M SIM cards have no PIN number. In this case, deactivate the PIN in the device configuration.	Telecontrol interface>> Modem settings >> PIN, confirm PIN and activate PIN" **Variant 1, variant 2, variant 3**
7	Enter the project number, station number and password for identification of the remote station in the telecontrol server. These parameters must not be changed, if the file stated in Table 2-5 No. 2 is used or if the same parameters have been entered manually in Telecontrol Server Basic.	"Telecontrol Interface > Modem identification > Project number, Station number, Password and Confirm password" **Variant 1**
8	APN address, APN user name and APN user password to log into the provider's GPRS network.	"Telecontrol Interface > GPRS Access > APN name, APN user name, APN password and Confirm APN password" **Variant 1, variant 2, variant 3**
9	<u>As an option:</u> Deactivate the automatic network dial-in and define a list of preferred parameters for GSM networks. See the note at the end of this table.	"Telecontrol Interface > List of preferred GSM networks > Contract and alternative networks" **Variant 2, variant 3**
10	Check the hardware ID of the CP 1242-7 and, if required, adapt the parameter "INTERFACE" to the blocks "TC_CON", "TC_DISCON","TC_RECV" and "TC_SEND" in the function "Z_call_telecontrol_blocks".	"PLC_1 > PLC tags > Show all tags > System constants > GPRS_Interface > Value"
11	Enter the IP address of the ISO-on-TCP partner station of the remote station's CP in the corresponding parameter field.	"Station XY > Program blocks > Z_TC_param_DB > connect_param > RemoteAddress > ADDR[1-4]" **Variant 2, variant 3**

No.	Action	Notes
12	Save the project. Click the program folder of the S7-1200 unit and select "Online/Download to device" to transfer the program to the controller. Make sure that the LED of the S7-1200 controller indicates "RUN" status.	

Note In order to use the project in STEP 7 V12 you need to upgrade it. Go to "STEP 7 V12> Project view> Project> Upgrade".

Note If so-called global SIMs are used which are not related to a home country network, the "roaming" function must be activated for the CP 1242-7. As "preferred GSM network" a combination of "Mobile Country Code MCC" and "Mobile Network Code MNC" must be selected.

These are the first four or five digits of the IMSI.

Link: http://en.wikipedia.org/wiki/International_Mobile_Subscriber_Identity

Note In the following chapters we assume that the remote station has been successfully logged into Telecontrol Server Basic. This is indicated at the remote station as follows:
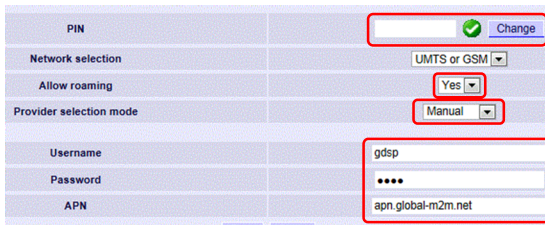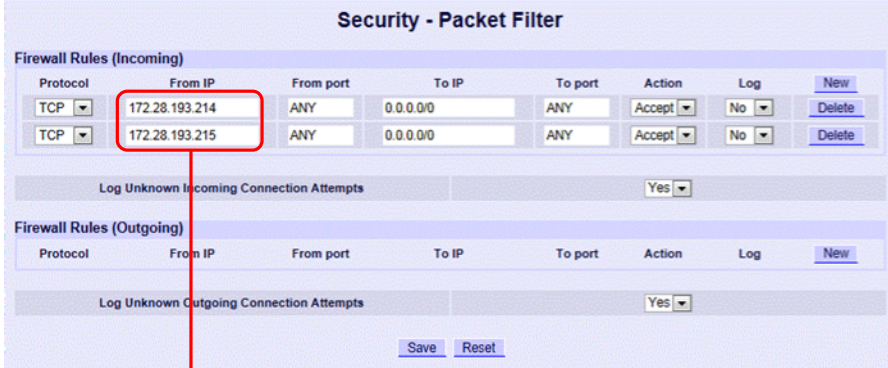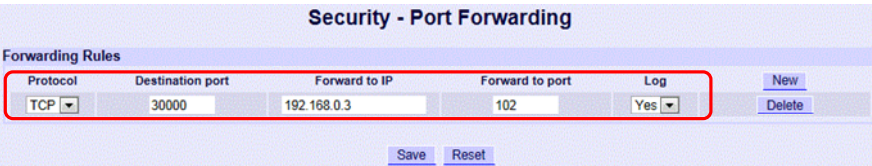
- Variant 1: Three permanently lit LEDs (NETWORK, CONNECT, SIGNAL QUALITY) at the CP 1242-7. In the Telecontrol Server Basic program this is indicated by a blue check mark in front of the station used here.
- Variants 2,3: Two permanently lit LEDs (NETWORK, SIGNAL QUALITY) at the CP 1242-7. During data transmission, the LED CONNECT is flashing.

Note When changing parameters in the data blocks, the controller must be set to the operating mode "STOP" and, after completion, to the operating mode "RUN" again.

5.2.3 Configuration of SCALANCE M873-0

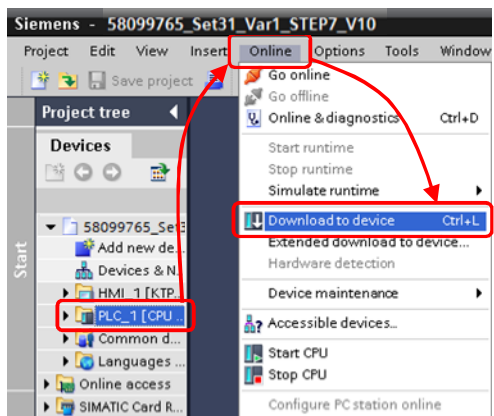This chapter refers only to variant 3 "M2M with S7-1200 and S7-300 directly via GPRS".

Table 5-5

No.	Action	Notes
1	Open your browser on the programming device and enter https://192.168.0.4 to open the configuration page for SCALANCE M873-0 (or use the standard IP address, if not adapted yet) .	Standard IP address: • 192.168.1.1 (if you need help for access to SCALANCE M873-0, please refer to document \8\ chapter 3.1 pp) Access data • User name: admin • Password: scalance
2	Navigate to the menu item "Maintenance > Configuration profiles > Upload profile" to transfer the file from Table 2-12 No. 2. to the UMTS router.	
3	Select the menu item "External network >> UMTS/EDGE" and enter the network-relevant information for WAN access.	
4	Enter the following parameters in the "Security > Packet Filter" window. Input fields for the IP addresses of the CPs of the two remote stations.	
5	Only if you do not use the configuration file provided for the SCALANCE M873-0: Select the menu item "*Security >> Port Forwarding*" and define forwarding from port 30000 to port 102 with the destination SIMATIC S7-300. 	

5.2.4 Configuration of the control station (S7-300)

This chapter refers only to variant 3 "M2M with S7-1200 and S7-300 directly via GPRS".

Table 5-6

No.	Action	Notes
1	Interlink the S7-300 controller with your programming device. Assign the Ethernet parameters as shown in Table 5-2.	Allocate an IP address to the S7-1200 CPU in the same way as described above. See document \7\ chapter 5.6.4
2	Open the STEP 7 V11 project as stated in Table 2-12 No. 1.	
3	Save the project. Click the program file of the S7-300 and select "Online/Download to device" to transfer the program to the controller. Make sure that the LED of the S7-300 controller indicates "RUN".	

5.2.5 Configuration of the control panel
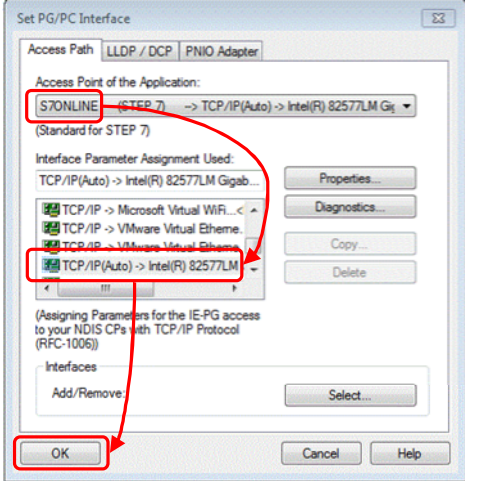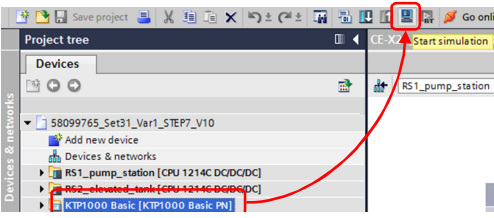
This chapter refers to all variants.

All start-up projects include a configured KTP1000 and in chapter 6 "Operating the Application", the "simulation" function is used to operate the example programs. The "simulation" function in the TIA portal enables operation without requiring a real KTP1000 unit. The following steps show all settings to be defined on the programming device to enable simulation in the TIA portal.

Table 5-7

No.	Action	Notes
1.	Open the "PG/PC Interface" of your control panel.	Windows 7: • "Start > Control Panel" • Select the "Small icons" view • Click "PG/PC Interface"

No.	Action	Notes
2.	• Define "S7ONLNE" as "Access point". • Select the Ethernet interface to be used for connection setup to the controller. • Click "OK" to confirm your settings.	
3.	Open the STEP 7 V11 project tree and select the KTP1000 configuration to start simulation.	

6 Operation of the Application

In each variant, the application is operated with the help of a configured SIMATIC KTP 1000 TouchPanel which is operated in simulation mode directly on the programming device.

Set the Ethernet card of the PG/PC interface of your programming device to "S7ONLINE", so as to enable the use of this function.

6.1 Variant 1 "M2M telecontrol"

The start-up code simulates a series of process values from the applied automation task, and with the help of KTP 1000 Basic these values are graphically displayed.

After having downloaded the start-up code into the controllers, simulation will start automatically. Data transmission starts automatically, as soon as the main connection to the Telecontrol Server Basic and the sub-connection between the two remote stations have been established.

Table 6-1

No.	Function
1	The two pictures in the KTP 1000 Basic project represent the two remote stations. Use the arrow keys to change between the two control images.
2	Output: Simulated filling level. Increases when the pump of the *Pump Station* is activated. This value will then be sent to the *Pump Station*.
3	Output: Status display of the *Elevated Tank*.
4	Input/output: Setpoint and actual value for the seconds counter which has started the sending process.
5	Output: Number of data transmissions to the *Pump Station*.
6	Output: Simulated pump status. The pump will be activated, if the filling level of the *Elevated Tank* is too low. This value will then be transmitted to the *Elevated Tank*.
7	Output: Status display of the *Pump Station*.
8	Output/input: Operating hours counter of the pump.
9	Output/input: Setpoint and actual value of the elapsed time (in seconds) until the next sending process starts.
10	Output: Number of data transmissions to the *Elevated Tank*.

6.2 Variant 2 "M2M with S7-1200 directly via GPRS"

The start-up code simulates a series of process values from the applied automation task, and with the help of KTP 1000 Basic these values are graphically displayed.

After having downloaded the start-up code into the controllers, simulation will start automatically. Data transmission starts automatically, as soon as the main and sub-connections between the two remote stations have been established.

Table 6-2

No.	Function
1	The two pictures in the KTP 1000 Basic project represent the two remote stations. Use the arrow keys to change between the two control images.
2	Input: The input bits in the controller increment in 5-second intervals. As an alternative you may set the input bits directly with the help of the these buttons. When operating the buttons, the automatic incrementation function will be stopped for a period of 10 seconds. This value will be sent to the *Wind Farm*.
3	Output: This field shows the input bit values received at the *Wind Farm*.
4	Input /output: Actual and setpoint value for the seconds counter which starts the transmission process.
5	Output: Number of successful and incorrect data transmissions to the *Wind Farm*.
6	Output: Number of successful and failed attempts to establish a connection to the *Wind Farm*.
7	Input: The input bits in the controller increment in 5-second intervals. As an alternative you may set the input bits directly with the help of the these buttons. When operating the buttons, the automatic incrementation function will be stopped for a period of 10 seconds. This value will be sent to the *Electrical Substation*.
8	Output: This field shows the input bit values received at the *Electrical Substation*. (Until the first successful receipt of data by the partner station, this field shows a diamond-pattern)
9	Input /output: Actual and setpoint value for the seconds counter which has started the transmission process.
10	Output: Number of successful and incorrect data transmissions to the *Pump Station*.
11	Output: Number of successful and failed attempts to establish a connection to the *Pump Station*.

6.3 Variant 3 "M2M with S7-1200 und S7-300 directly via GPRS"

The start-up code simulates a series of process values from the applied automation task, and with the help of KTP 1000 Basic these values are graphically displayed.

After having downloaded the start-up code into the controllers, simulation will start automatically. Data transmission starts automatically, as soon as the main and sub-connections between the two remote stations have been established.

Table 6-3

No.	Function
1	The two pictures in the KTP 1000 Basic project represent the control station and the two remote stations. Use the arrow keys to change between the control images.
2	Output • Green: Connection has been established. • Yellow: Waiting for connection request, or connection buildup or termination is in progress. • Red: Error during connection buildup or termination
3	Output: This output field shows the number of the *Pump Station* from which data was received last. Consequently, this value always changes shortly after the "Connection Status" (2) has turned green.
4	Input: This button is used to set the release of simulated oil production in the *Pump Stations*. This value will be successively transmitted to all *Pump Stations*.
5	Output: This output field shows the status of the control value for global release as stored in the *Pump Station*. The control command is implemented only when this value matches with the value in the input field "Global enable" (4). This value is received in the *Pump Stations*.
6	Output: This field shows the operating hour counter (1h = 1s) of the *Pump Stations*. This value is received in the *Pump Stations*.
7	Output: This output field shows the current oil production quantity of the *Pump Station*. This value is received in the *Pump Stations*.
8	Output: Number of successful and incorrect data transmissions to all *Pump Stations*.
9	Output: Number of successful and incorrect receipt of data at all *Pump Stations*.
10	Output: Number of successful and failed attempts to terminate connection by the *Pump Stations*.
11	Output: Number of successful and failed attempts to establish a connection by the *Pump Stations*.

No.	Function
12	Output • Green: Connection has been established. • Yellow: Waiting for connection request, or connection buildup or termination is in progress. • Red: Error during connection buildup or termination
13	Output: Number of successful and incorrect data transmissions to the *Control Station*.
14	Output: Number of successful and incorrect receipts of data at the *Control Station*.
15	Output: Number of successful and failed attempts to establish a connection to the *Control Station*.

7 Links & Literature

The following list is by no means complete and only provides a selection of appropriate information.

Table 7-1

	Topic	Title
\1\	S7-1200 Set 30: Telecontrol for the S7-1200	http://support.automation.siemens.com/WW/view/en/39863979
\2\	Siemens Industry Online Support	http://support.automation.siemens.com
\3\	Release for delivery – SOFTNET Security Client 2008	http://support.automation.siemens.com/WW/view/en/30823829
\4\	SCALANCE S and SOFTNET Security Client	http://support.automation.siemens.com/WW/view/en/21718449
\5\	SIMATIC NET; PG/PC – Industrial Ethernet; SOFTNET-IE RNA V8.1; Operating Instructions	http://support.automation.siemens.com/WW/view/en/58058556
\6\	CP 1242-7 Operating Instructions	http://support.automation.siemens.com/WW/view/en/42330276
\7\	SIMATIC S7-1200 System Manual	http://support.automation.siemens.com/WW/view/en/36932465
\8\	SCALANCE M873-0 System Manual	http://support.automation.siemens.com/WW/view/en/49507278
\9\	Support Packages for CP1242-7	http://support.automation.siemens.com/WW/view/en/54164095
\10\	S7-1200 IP Tool	http://support.automation.siemens.com/WW/view/en/41737436
\11\	Primary Setup Tool	http://support.automation.siemens.com/WW/view/en/19440762
\12\	Industry Mall	http://eb.automation.siemens.com

8 History

Table 8-1

Version	Date	Revisions
V1.0	June 2013	New set number, project tested with STEP7 V12
V1.0	April 2013	New layout
V1.0	July 2012	First issue