Mobile Communications

Data transmission in industry

PHOENIX CONTACT
INSPIRING INNOVATIONS

Imprint

1st Edition 2012

Printing, binding, and processing:
druck.haus rihn GmbH, Blomberg, Germany

Author, publisher, editor, setting, design (including cover design),
Text, images, cover image: PHOENIX CONTACT GmbH & Co. KG, 32823 Blomberg, Germany

Table of contents

We are communicative … at least we think we are

We are all available 24 hours a day. We have at least one cell phone, use the Internet on the go every day, and learn about the latest global news through our communication media. Having information at one's fingertips is now essential to us all and nobody wants to give it up.

In the field of machines, systems, and power stations, even leading industrialized nations are still a generation behind. Many of the systems in the production environment, as well as numerous machines and power stations, are networked only in subsystems – if at all. As such, operators often lack consistency and important information from remote stations. While a cell phone generation has a product life cycle of less than 12 months, the life cycle of systems and power plants can be up to 30 years. New communication structures are only integrated into old systems on a gradual basis, as part of renovations and upgrades.

Think about the latest trends for new decentral, distributed energy production systems – whether by means of windmills, solar systems or combined heat and power units. Think about the latest energy efficiency trend to use available resources wisely and economically. Think about the global competition in industrial production, which calls for us to continuously optimize our systems. As a production manager, you need to know at all times what is being produced worldwide on each machine, at what quality level and when the next maintenance interval is due. Such new systems are hardly imaginable today without efficient communication networks, which are essential for reliable system operation.

This rapid development in the exchange of information and data that we have experienced in the telecommunications industry in the last few years is about to break into the industrial sector.

I am absolutely certain that in the future all PLC systems, distributed control systems, and PC-based control systems will be networked and integrated into remote control, remote maintenance, and diagnostic concepts. Indeed, many of these M2M applications will be implemented over telecommunications networks. Now is the perfect time to consider these topics, applications, and technologies in the industrial sector, and that is exactly where this guide comes into its own.

I hope that this guide offers you new ideas for your applications and provides you with background information about the technical options and limits of M2M communication.

Christoph Leifer
Spring 2012

1 Introduction

This guide is designed for project planners who intend to transmit data in industrial applications over the mobile phone network for the first time. In terms of the guide's content, customer questions were evaluated after being gathered from different departments at Phoenix Contact, such as Sales and the Technical Hotline.

The aim is to answer the most frequently asked customer questions as succinctly as possible and with minimal IT terminology. As such, the focus is on the practical benefits for the project planner. For in-depth theoretical context, references to technical literature are provided in the appendix.

If you enjoy this guide, please pass it on. If you have any suggestions for improvements or additions to this book, e-mail them to our sales office, which will forward this information onto us.

This guide is also available for free in electronic format. Visit the Phoenix Contact website to download the latest version.

Happy reading!

Gerrit Boysen
Business Unit I/O and Networks
Product Marketing Communication Interfaces

2 Mobile phone networks

2.1 Advantages of mobile phone communications

The desire to remotely monitor and maintain machines and systems has been steadily increasing. There are many reasons for this, from simple cost savings to developing new service business models.

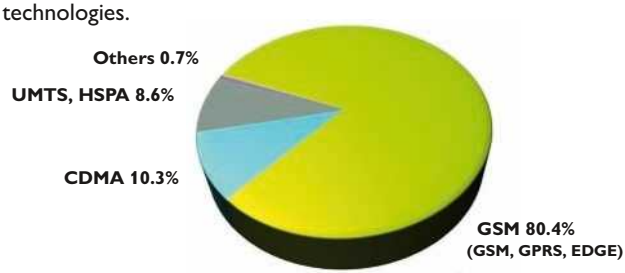
Most customers favor remote access to machines and systems over fixed networks, however problems do occur in practice. Here are three typical examples:

1. The component is in a mobile unit.
2. There is no fixed network connection at the planned location.
3. The subsequent end customer prohibits the machine/system supplier from using its local network.

In all three cases, mobile phone communications can prove an effective solution.

2.2 Mobile phone networks: A brief overview

The requirements for mobile phone networks are continually rising. For this reason, older mobile phone networks are being modified or replaced by new ones. Today's mobile phone networks can be roughly divided into mobile phone networks of the second, third, and fourth generation. The boundaries are not fixed. Currently, all mobile phone technologies of the second to fourth generation are operated in parallel and with overlap on a global scale. **Fig. 1** shows the global market share of individual technologies.



Source: http://www.mobileworldlive.com (as of 2010)

◄ **Fig. 1**
Market share of technologies used worldwide (as of 2010).

As can be seen in **Fig. 1**, *GSM (Global System for Mobile Communications) mobile phone technology has a global market share of about 80 % and is therefore of significant interest for industrial applications, especially if global communication is required.*

2.2.1 2G (GSM, GPRS, EDGE)

At the beginning of the 1990s, the GSM mobile phone network was established in Europe and later worldwide. GSM is a second generation mobile phone technology. The goal at the time was to transmit voice, not data, as the latter was not as relevant as it is in today's industry. The demand for transmitting data over the existing mobile phone network did not rise until the Internet boom at the end of the 1990s. For this reason, the GSM mobile phone networks were extended at the end of the 1990s with GPRS (General Packet Radio Service) and later with EDGE (Enhanced Data Rates for GSM Evolution). The GSM networks modernized with GPRS and EDGE are also described as networks of generation 2.5. The technical differences are considerable, even if they are not readily apparent. In GSM the data transmission is circuit switched, while in GPRS/EDGE it is packet-oriented (see Section 3.2/3.3). For the GSM/GPRS/EDGE mobile phone networks, four frequency bands are available worldwide: 850 MHz, 900 MHz, 1800 MHz, and 1900 MHz. The frequency band used locally differs by country and by network operator.

A mobile phone modem that supports all four frequency bands can be used virtually anywhere in the world. Two exceptions are South Korea and Japan. These countries decided on a mobile phone standard that is not compatible with GSM.

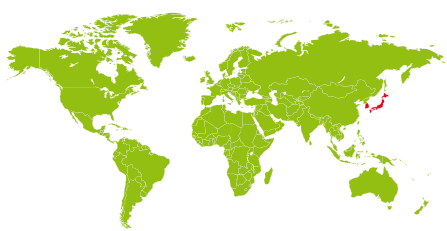


Fig. 2 ►
A GSM/GPRS/EDGE modem can be used in virtually every country.

◄ **Fig. 3**
Here, for example, you can see the network coverage of the mobile phone service provider MTC in Namibia (as of 2011).

You can learn more about GSM network operators all over the world, the GSM frequencies they use, and their GSM network coverage on the following website: http://www.mobileworldlive.com

2.2.2 3G (UMTS, CDMA2000, TD-SCDMA)

About eight years after GSM was launched, the mobile phone networks of the third generation were established. Unlike with GSM, data transmission was now given much more consideration than telephony. New technologies within the 3G networks enable significantly higher data transmission speeds than with GSM, GPRS or EDGE.

For the mobile phone networks of the second generation, GSM is regarded across the world as *the* mobile phone technology. In contrast, the forerunner for the mobile phone networks of the third generation is not so clear. Several third-generation technologies are competing on an international scale, yet they are incompatible with each other. Unfortunately, agreement on a common 3G mobile phone technology was not possible for economic and political reasons. The two most important 3G technologies (as of 2011) are:

- UMTS + extensions
- CDMA2000 + extensions

To put it simply, UMTS and its extensions, such as HSPA, dominate the European market. In the USA and Asia, CDMA2000 and its extensions are widespread. In China, TD-SCDMA, a separate Chinese mobile phone standard, is being heavilly promoted. However, TD-SCDMA is yet to play an important global role.

The regional network operator decides which technology is used in a particular company. For example, the North American network

Fig. 4 ►
You can find information about network operators that use UMTS and its extensions on the GSMA website.

http://www.mobileworldlive.com/

Fig. 5 ►
You can find information about network operators that use CDMA2000 and its extensions on the CDG website.

http://www.cdg.org/

operator *AT&T* uses the mobile phone technology UMTS, while its competitor *Verizon* uses CDMA2000. Integrating both mobile phone technologies into one chipset is a goal that is currently being pursued by several mobile phone chipset manufacturers.

On the following websites, you can discover whether the 3G technology in question is used in your destination country, including the network operators, their frequencies, and their network coverage.
UMTS network operators: ***http://www.mobileworldlive.com/***
CDMA network operators: ***http://www.cdg.org/***

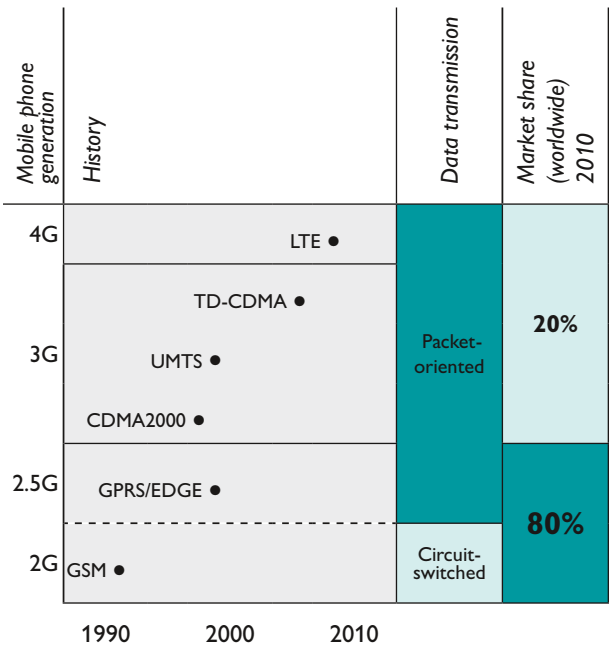
2.2.3 4G (LTE)

As shown in **Fig. 1**, the fourth mobile phone generation did not have a significant market share in 2010 from a global perspective. Nevertheless, we discuss LTE (Long Term Evolution) briefly here because the mobile phone markets change rapidly.

LTE is advertised in the media as a new 4G mobile phone standard. The networks have rapidly expanded regionally since 2010 and offer the end customer as well as the network operator many advantages, such as:

- Higher data speed
- Shorter latency
- Better energy efficiency

In addition, LTE is supported by the CDG (CDMA Development Group), which supports the CDMA2000 mobile phone standard, and by the GSMA (GSM Association), which supports the UMTS mobile phone standard. LTE therefore has great potential to become *the* global high-speed mobile phone technology. The first LTE mobile phone components suitable for industrial applications are already in development. However it is not yet clear when these will be available on the market (as of 2011).



◀ **Fig. 6**
History of mobile phone technologies.

3 Data transmission via mobile phone network

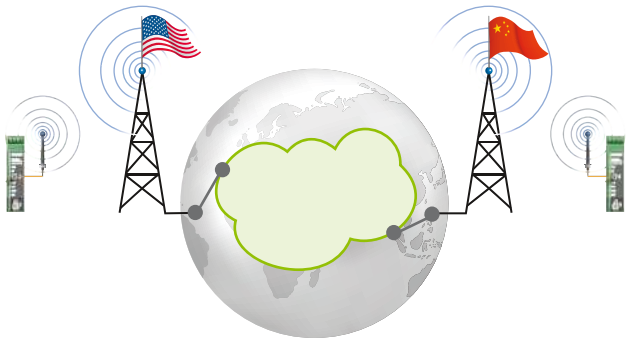
To many customers, communication over mobile phone networks is wireless data transmission. For this reason, mobile phone networks are often equated with other wireless transmission technologies, such as WLAN, Bluetooth or Trusted Wireless. Although data are transmitted wirelessly in all the methods mentioned above, the technologies are not equivalent, in fact they differ greatly.

Data transmission over mobile phone networks is wireless communication at first glance, but cannot be equated with other wireless communication technologies.

One major advantage of mobile phone communication is that data can be transmitted virtually worldwide. However, the data are never transmitted directly from the transmitter to the receiver. To put it simply, communication is as follows (see **Fig. 7**): The data are transmitted from the mobile transmitter through the air to the nearest mobile phone tower. From there, the data are fed into the fixed network (the core network of the mobile phone service provider) and guided by cable to the mobile phone tower closest to the mobile receiver. From this mobile phone tower, the data are transmitted through the air to the mobile receiver. Mobile phone communication is therefore a mixture of wireless communication (air interface) and wired communication (fixed network/core network of the mobile phone service provider). Direct communication between the transmitter and the receiver through the air is never established.

If a mobile phone solution is installed on a ship or on an offshore installation, it must be ensured that communication with the mobile phone tower on the mainland is supported. A ship or an offshore installation that is too far out to sea can no longer communicate via a mobile phone network; in this case, communication via satellite is recommended.

Fig. 7 ►
In mobile phone communication, the transmitter and receiver never communicate with each other directly and wirelessly, but rather through the fixed network/ core network of the mobile phone service providers.

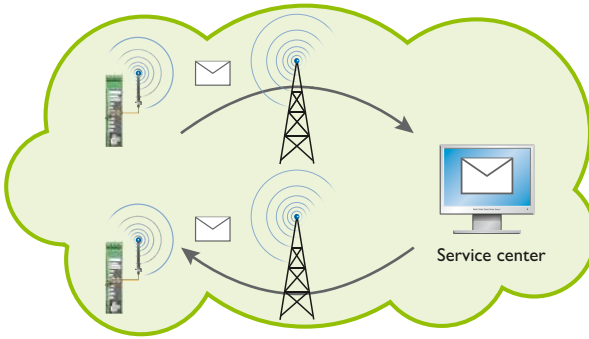


If, for example, the mobile phone tower of the network operator fails, communication between the transmitter and the receiver is no longer possible, even if the devices are adjacent to each other. For optimum reception, always direct the antennas toward the mobile phone tower, not toward the terminals.

One challenge in mobile phone communications is that the network operator is the unknown third party in the communication chain. Not every network operator has a worldwide mobile phone network and they often cooperate globally with regional partners. As such, for data to be transmitted to a foreign country, more than one mobile phone service provider is almost always involved.

Each mobile phone service provider can apply its own rules for data communication: What is possible for a mobile phone service provider in country A is not necessarily possible for a mobile phone service provider in country B.

Therefore only plan services that are supported by all mobile phone service providers. Below, you will discover more about the typical services and specific questions you can ask your mobile phone service provider.



◄ **Fig. 8**
The service center for short messages forwards the SMS.

3.1 Communication via SMS

The service of sending short messages over the mobile phone network (SMS = Short Message Service) began operating about four years following the emergence of GSM networks and was initially viewed as a handy extra for the customer. Within a short period of time, this service became so popular with consumers that network operators now gain huge revenue from this service.

Communication via SMS can be described in a simplified manner as follows: The transmitter sends an SMS to the mobile phone network. The SMS is forwarded on the network of the mobile phone network operator to the service center for short messages. The service center for short messages determines the location of the receiver and then forwards the SMS to them. If the first delivery attempt of the SMS did not succeed, another attempt to send the SMS is generally made.

The mobile phone service provider defines how often, at what time intervals, and with what priority an attempt is made to transmit the message to the recipient. This can differ from mobile phone service provider to mobile phone service provider.

Unfortunately, an end-to-end receipt confirmation was not implemented in the SMS specification at the time. The sender is normally informed only that the short message was sent to the service center, but not whether the recipient has received the message accordingly. Some network operators (but not all) have

their own solutions to this problem. For example, the transmitter can place a special text code before the actual message. If the service center detects this code, it is automatically removed from the actual message and a confirmation is sent to the transmitter as soon as the SMS has been transmitted from the service center to the recipient. Important to know: The confirmation message indicates only that the SMS was transmitted to the terminal. It does not indicate whether the short message was actually read, e.g., by the service technician.

Service provider	Country	Text for receipt confirmation (as of 2011)
Vodafone	Germany	*N#
Telekom	Germany	*T#
E-Plus	Germany	*N#

If the sender of the SMS has a mobile phone contract with service provider A, but the recipient has a mobile phone contract with service provider B, confirmation across networks is usually not supported. However, it is important to check each individual case.

To ensure, for example, that a service technician has actually read the SMS, the service technician should generally reply with a short message as a confirmation, for example, with the text "OK". This is the only way to ensure that the recipient has actually received and also read the message.

Within a mobile phone network, short messages are generally sent in a matter of seconds. The mobile phone service providers do not guarantee whether and when the text message will arrive, especially if the short message is forwarded to another mobile phone service provider. This should be considered in the planning phase.

Even if an SMS alert is not suitable for time-critical applications, the sending of messages has several advantages:

◄ **Fig. 9**
The SMS relay from Phoenix Contact offers, among other things, the option for the recipient to confirm the SMS within a specified time. If the SMS is not confirmed, other persons are informed.

A key advantage to using an SMS is that many people are already familiar with this service and use it privately. Therefore, there is very little inhibition to overcome, minimal instructions are required, and SMS is particularly easy to use. The service is widespread, and virtually every mobile phone service provider allows short messages to be transmitted and received in its mobile phone network.

At locations with poor network coverage and where GPRS data transmission is no longer supported, it is often still possible to transmit a short message.

Sending an SMS as an e-mail or fax

Some mobile phone service providers offer a service to convert an SMS to an e-mail or fax for customers. The customer is therefore able to generate an e-mail or fax with little effort, for example, which is transmitted to the control center in parallel with the SMS as soon as an alarm is triggered.

To create an e-mail from an SMS, the e-mail address must be positioned at the beginning of the text message. The SMS is then transmitted to the phone number of the corresponding service center of the mobile phone service provider. The service center automatically removes the e-mail address from the message and forwards the rest of the text message to this address. Important to know: If the e-mail address is entered at the beginning of the short message, a * must usually be entered instead of the e-mail

character @. In addition, the length of the e-mail message is limited to 160 characters minus the e-mail address, and only one e-mail recipient can be selected.

If the SMS should be converted to a fax, two phone numbers must be combined: The phone number of the service center and that of the fax machine. The phone number of the fax machine is appended directly to the phone number of the service center. If the service center phone number is "99" and the fax number is "555", then the SMS must be sent to "99555". In contrast to sending an e-mail, the phone number does not have to be included in the SMS text. Here too, the length of the fax message is generally limited to 160 characters.

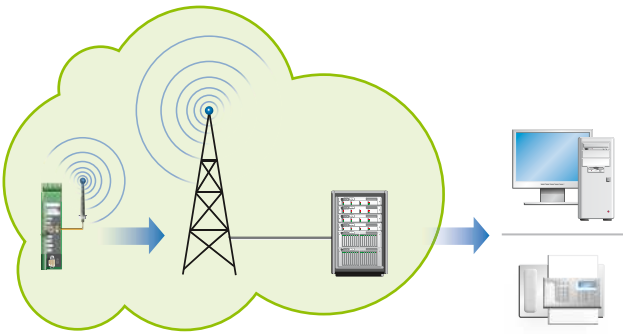
The service for sending an SMS as an e-mail or fax is offered by many network operators, but not all. If you are including this service in your plans, first ask your mobile phone service provider.

3.2 Circuit switching via GSM

If data communication via mobile phone networks is planned, the inexperienced planner is often unable to differentiate between GSM and GPRS/EDGE. To such a planner, both are identical types of mobile phone communication. However, the technical differences are substantial.

In order to transmit data via GSM (not GPRS/EDGE), "a cable" is exclusively connected between A and B (to put it simply). This type of data link is called CSD (Circuit Switched Data). A key advantage of transmitting data via CSD is the ease of use. The user only has to call the GSM modem using a telephone number, the modem then "picks up" and the connection is established. As such, communication via CSD is similar to an analog fixed network modem, except the data speed is lower. It is generally 9600 kbps instead of 33.6 kbps (14.4 kbps is also possible for some mobile phone service providers).

One point that is often neglected is that the SIM cards for incoming CSD data calls often must be activated by the particular mobile phone network operator. However, many mobile phone network operators do not allow CSD communication by default.



◄ **Fig. 10**
Some network operators allow an SMS to be converted to an e-mail or a fax.

If you do not activate this service separately, you usually cannot reach your mobile phone modem via the mobile phone number, which is a typical error during the initial startup.

The main disadvantage of CSD is that the exclusive cable remains switched even if the data transmission is stopped intermittently, e.g., during short transmission pauses. From the customer's point of view, this does not pose a problem. However from the network operator's point of view, this is a considerable waste of resources. The mobile phone network is generally in high demand and an expensive resource. In order to increase efficiency of the mobile phone networks, the existing mobile phone networks are being rapidly converted from circuit-switched networks to packet-oriented networks.

CSD is a dying technology. It is supported by less and less mobile phone service providers worldwide. In many countries, it is no longer offered at all. For future projects, packet-oriented data transmission should definitely be planned. This includes mobile phone technologies from GPRS to LTE.

Experiences with the network conversion (CSD to IP)

A CSD connection consists of acoustic data transmission via mobile phone networks. A mobile phone call is established and the data are transmitted via tones. The conversion of the mobile phone network to the Internet Protocol (IP) increases the data transmission time of the communication, as the tones

are converted to the Internet Protocol, transmitted, and then converted back into tones. This can increase the data transmission time, called the round-trip time (RTT), to as much as 8 seconds (for the round trip). In practice, this can lead to an interruption of communications in systems that have been running stably for years because the response times are suddenly exceeded. For example, old electric meters operate using the standardized protocol DIN EN 61107 or IEC 62056-21:2002 and require a response time of 1.5 to 2.2 seconds. Devices that handle data transmission according to the 3GPP standard (technical reference: 3GPP TS 22.105 V4.3.0 [2002- 03], Section 5.5) should not be affected (source: Deutsche Telekom 2010).

Fig. 11 ►
Put very simply, data transmission via CSD is comparable to an "exclusive cable" for customers.

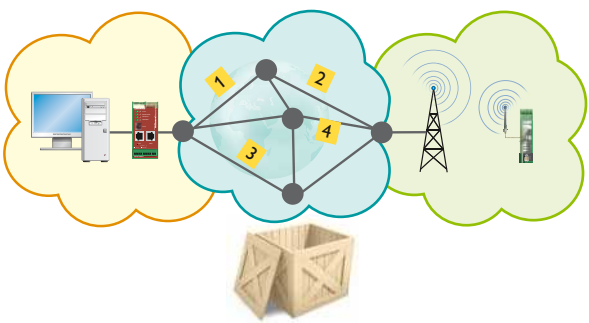


Fig. 12 ►
In packet-oriented data transmission, the data can reach the destination over the widest range of routes. The communication rules are complex, but the network can be used much more efficiently.

◄ **Fig. 13**
The GSM/GPRS modem from Phoenix Contact has an integrated TCP/IP stack. This means that even older controllers can also be integrated into modern IP networks.

3.3 Packet-oriented communication (GPRS to LTE)

In packet-oriented data transmission, the data to be transmitted are divided into small packets. Each packet is given a source address and a destination address. On the way to the destination, the data packets can be transmitted over different routes. The packets can therefore arrive in a different sequence and at different times, which makes communication more complex. A great advantage of this approach is the significantly better network utilization. As soon as individual paths on the network fail or become overloaded, the transmitted packets are automatically re-routed via other paths. This allows the network to be optimally utilized.

Packet-oriented data transmission is state-of-the-art in today's industry and will probably remain so in the future. However, it is important to note that packet-oriented data transmission has two significant disadvantages for the user when compared with a GSM dial-up line connection. Firstly, there are no longer fixed delay times. This means that data packets can reach the destination devices faster or slower. Secondly, the mobile phone network operators do not guarantee the customer a fixed bandwidth. It can be higher or lower depending on network capacity. This must be taken into consideration during the planning phase.

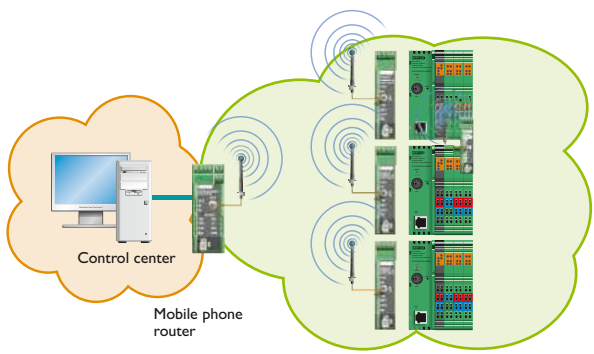
Fig. 14 ►
Comparison of circuit switching and packet switching

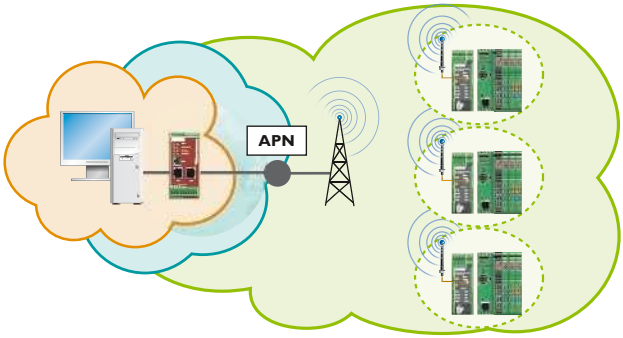
	Circuit switching	Packet switching
Technology	GSM (CSD)	GPRS to LTE
Bandwidth	Constant following connection establishment	Dynamic
Delay time	Constant following connection establishment	Dynamic
Advantage	Easy to use for the end customer	Flexible, robust, versatile, optimum network capacity, shorter connection times
Disadvantage	Network capacity not optimum, often not cost-effective enough for the network operator, not a long-term solution	More complexity
Application	Point-to-point connection	Point-to-point and multipoint connections

Packet-oriented data transmission does not offer the customer fixed delay times or a constant bandwidth. If the mobile phone network is not fully utilized, the bandwidth can be several times the bandwidth for CSD.

An advantage of packet-oriented communication lies in the connection establishment, which generally takes less than five seconds for a GPRS connection and up to twenty seconds for a dial-up line connection. This is important if the control center wants to communicate with numerous remote locations in sequence. Another significant advantage is that packet-oriented data communication enables point-to-point connections as well as multipoint connections, such as a star structure.

Fig. 15 ►
A multipoint connection over the mobile phone network.





◄ **Fig. 16**
Multipoint connection over the mobile phone network and Internet.

If a star topology is established with mobile phone subscribers (see **Fig. 15**), it should be noted that all connections converge in the control center. If simultaneous communication with all the remote stations is required, more bandwidth is required in the head station than in the remote stations. For this reason, a connection of the greatest possible bandwidth should be planned for the head station. An Internet connection via a fixed-line is recommended (see **Fig. 16**). If this is not possible, a broadband mobile phone router should be used. Be aware of the possible limitations here, which are described later in Section 3.6.3. In contrast, mobile devices with low bandwidth can be used in the remote stations. These tend to be cheaper to purchase. In addition, broadband mobile phone networks are rare in sparsely populated areas (see network coverage in Section 2.2.2).

You can find tips on establishing a star topology and information about a pure mobile phone star topology in Section 3.6.3.

				under preparation
GSM	**GPRS**	**GPRS / EDGE**	**GPRS/EDGE/UMTS**	**LTE**
Circuit switching	Packet-oriented	Packet-oriented	Packet-oriented	Packet-oriented

Fig. 17 ►
Phoenix Contact offers the appropriate hardware for every transmission technology.

3.4 APN (Access Point Name)

The mobile phone network is linked to other networks such as the Internet or private company networks, via access points. The access point is located in the core network (fixed network) of the mobile phone network operator (**Fig. 18**).

If a mobile phone subscriber would like to access the Internet, the device must store the APN (Access Point Name), i.e., the name of the corresponding access point, in their mobile phone router. Some network operators also ask for a user name and password when the connection is being established.

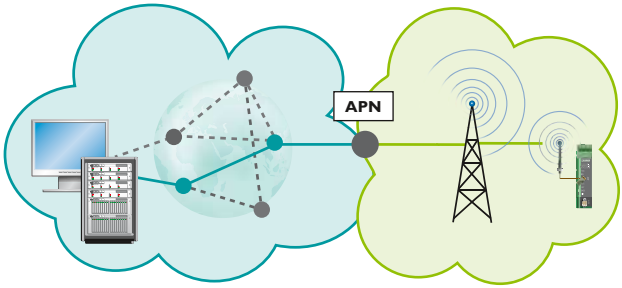
Your mobile phone service provider can supply you with the Internet access data.

Public and private access points

Public and private access points can generally be distinguished between. All mobile phone customers of a mobile phone service provider can use public access points, for example to surf the Internet using a cell phone. Private access points are available only to certain mobile phone customers, e.g., field employees who want to connect directly to the company network using their mobile devices without using the public Internet (greatly simplified, see **Fig. 19**). For several reasons, the use of the wrong access point must be avoided.

Here are two examples:

a) Your company is directly connected to the mobile phone network operator via a private access point. Consequently, data from the mobile device are not transmitted over the public Internet but rather directly into the company network. Therefore, encrypted data transmission is not planned. However, the technicians on site configure the devices so that the communication occurs through a public access point and not through a private APN. The data are then transmitted over the Internet without encryption, which represents a considerable security risk (see **Fig. 19**).

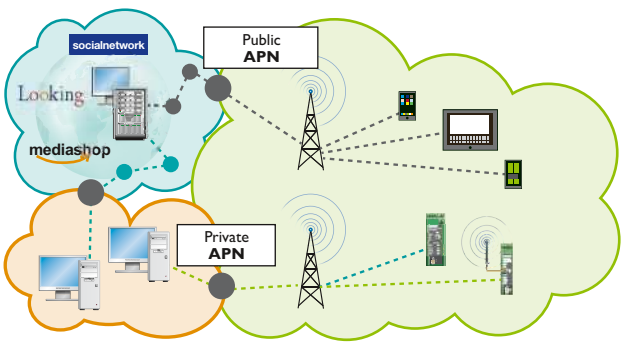


◄ **Fig. 18**
The mobile phone subscriber establishes connection to the Internet via APN (Access Point Name).

When using a public access point, ensure that data are sent over the Internet with encryption. You can find details on using the Internet safely in Section 3.7.

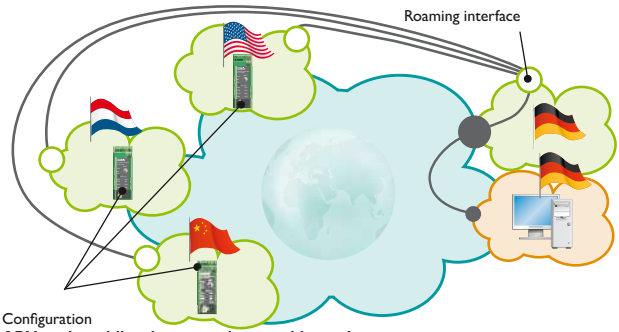
b) A mobile phone service provider often has several public access points, such as one for contract customers and one for prepaid customers. If for example you want to use the access point for M2M applications, in accordance with your low-cost M2M contract, but you use the public access point for prepaid customers, this can have a significant effect on your bill in the case of some mobile phone service providers.

Ensure that you always communicate via the correct access point. Your mobile phone network operator can tell you which access point you should use.



◄ **Fig. 19**
Public and private access points are available.

Fig. 20 ►
If a roaming agreement is in place between the local network operators, the devices do not have to be reconfigured.



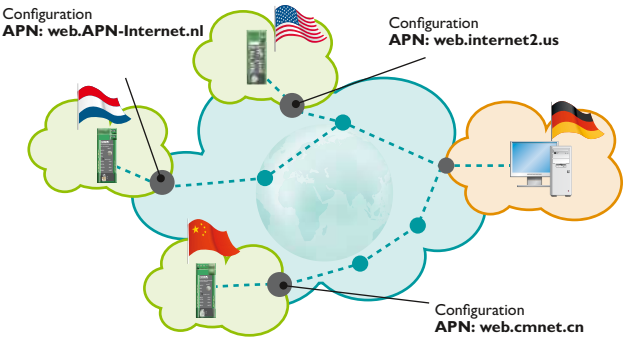
3.5 Roaming

Mobile phone service providers arrange strategic partnerships so that customers can use their mobile devices internationally. If a customer goes abroad and uses a foreign mobile phone network, the foreign mobile phone service provider forwards the data to the network operator in the customer's home country. This occurs through a special internal roaming interface without the customer noticing (**Fig. 20**).

Ask your mobile phone service provider which of its access points are "roaming-capable", as not all public and private access points are.

Roaming has the following technical advantage: If the mobile device is in a foreign country and would like to establish a connection to the company, the foreign mobile phone service provider forwards the data packets to the domestic mobile phone service provider via the internal roaming interface between the mobile phone service providers.

From there, the data are forwarded to the domestic access point. Consequently, devices used at home and those used abroad do not have to be configured differently. Compare **Fig. 20** with **Fig. 21**. In series production this can prove to be advantageous e.g., in machine building, although the high costs currently charged for roaming are a disadvantage.



◄ **Fig. 21**
If roaming is not supported or desired, each device operating in a foreign country must be configured with the access data of the foreign mobile phone service provider.

Ask your network operator if it has a roaming partner in the country you travel to and how much roaming costs.

Nevertheless, roaming can cause problems, for example if the device is used in the home country but near a national border. The device can suddenly register itself in the mobile phone network of the neighboring country, because the network coverage is better. Communication with the control center occurs to some extent via the foreign country, which can cause high costs, even though the device is not in the foreign country.

When purchasing a device, make sure that you can deactivate the roaming feature in the device configuration.

3.6 Restricted connection establishment

When you go to make a call on your mobile phone, there is little to consider in terms of connection establishment. You can easily call a mobile phone number or a fixed network number or accept a call from a mobile phone or from a fixed network connection. Communication can take place in either direction, although this is usually not the case with data transmission. A connection from the mobile phone subscriber to the Internet can be established, but a connection from the Internet to the mobile phone device generally CANNOT be established. However, in industrial applications, it is often necessary to be able to connect the control center to the

remote station (mobile subscriber) via the Internet and not in the other direction. This causes difficulties during the initial startup. In Section 3.6.2, we describe how to solve these problems in detail.

Each mobile phone service provider establishes the rules for data communication. If you have several mobile phone service providers in the chain of communication, always start from the smallest common denominator supported by all the network operators during planning.

3.6.1 From a remote station to the control center via the Internet

In the following example, the connection establishment from a mobile phone device (remote station) to a wired Internet connection (control center) is described (see **Fig. 22**). Please note that, in the example below, the connection is initiated by the mobile device to the control center, not by the control center to the mobile device. To ensure an improved understanding of this topic, security and dynamic addresses are not taken into account here.

The mobile device would like to send data to the control center. In order to communicate via the Internet, the mobile device needs the public access point (APN) key data. These data are provided by the mobile phone service provider. In addition, the device must know with which device a connection should be established. In the simplest case, the target address of the wired Internet connection

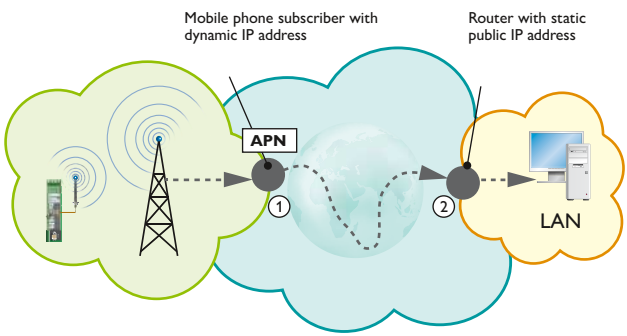


Fig. 22 ►
The remote station would like to transmit data to the control center over the public Internet.

is a static public IP address. All data packets which are later sent to the recipient also contain the transmitter's IP address. This means that the recipient can reply to the sender (this is greatly simplified). A public fixed IP address is not required for the mobile device. Public fixed IP addresses are only rarely offered by mobile phone service providers and therefore should not be planned in the technical implementation. Public fixed IP addresses should not be confused with private fixed IP addresses, which are offered also by mobile phone service providers (see Section 3.6.3).

A connection establishment from the mobile phone subscriber to the control center is supported by almost every mobile phone service provider worldwide. The mobile phone subscriber bears the costs of data communication. A connection from the control center to the mobile phone subscriber is usually blocked. An approach to solving this problem is described in Section 3.6.2.

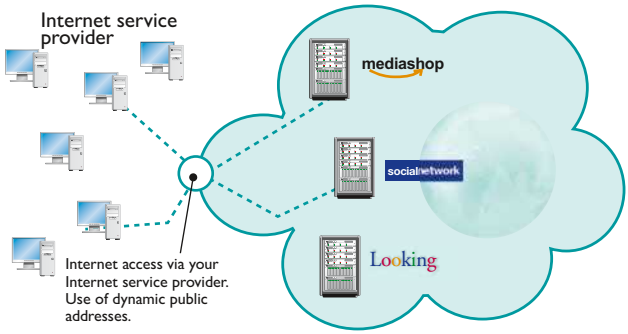
Names instead of IP addresses

In general, the customer does not receive a static public IP address for its fixed-network Internet connection from its Internet service provider, as shown in **Fig. 22**, but rather is assigned a dynamic public IP address.

Why is it done this way? The classic IP address are IPv4 addresses, such as 123.156.123.2. Each of the four numbers can assume a value from 0 to 255. This format can represent about 4.3 billion addresses. When IPv4 was being developed, the Internet boom was not predicted, which is why IP addresses are scarce worldwide today (2011). Not all Internet users are on the Internet at the same time, therefore the following solution (among others) was developed to reduce the problem of address scarcity. To simplified terms, the solution is as follows:

Each Internet service provider is assigned a number of IP addresses. The typical ratio of IP addresses to customers is between 1:10 and 1:20, meaning that the Internet service provider has ten to twenty times more customers than IP addresses. As soon as a customer of the Internet service provider wants to use the Internet, the customer is temporarily assigned an address from this IP address pool. If the address is

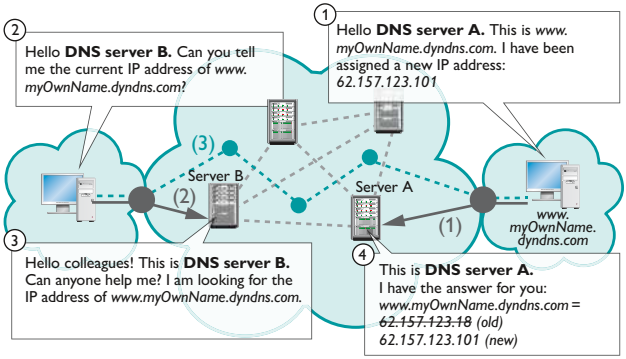
Fig. 23 ►
In general, Internet service providers have a pool of IP addresses, which are temporarily assigned to customers as required.



no longer needed or if the time has expired, this IP address is returned to the address pool. In this way, many people can use the Internet with relatively few IP addresses.

How can I reach a subscriber that is continually assigned a different address? The Domain Name System (DNS) helps with this. Put simply, the approach is as follows: The recipient reserves a fixed name on the Internet, such as *www.myOwnName.dyndns.com*. There are special companies that offer this service, such as *DynDNS.com*. The service provider (DNS server) then links the name to the current IP address of the recipient. If the recipient is then assigned a new IP address by the recipient's Internet service provider, for example because the duration of use has expired, the recipient immediately sends the new IP address to the DNS server. This occurs automatically if the recipient has implemented the software functionality of a DNS client. Therefore, the DNS server always has the current IP address for the corresponding name (see **Fig. 24**).

If the transmitter wishes to communicate with the receiver, the transmitter can ask their own DNS server for the receiver's IP address, by name. If the transmitter's DNS server does not know the answer, it asks other DNS servers for help until it can tell the sender the corresponding IP address of the recipient. The transmitter then has the temporary IP address of the recipient and can transmit the data to the recipient. This query occurs quickly and is usually not noticed by the customer.



◄ **Fig. 24**

Greatly simplified principle: If the receiver has a dynamic IP address, a domain name server helps to provide the IP address to the transmitter.

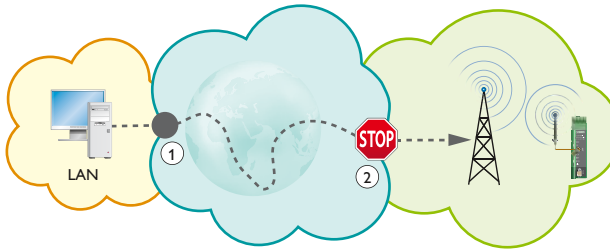
If you are not assigned a static IP address for your fixed network Internet connection, then you can use the services of ***DynDNS.org*** *in order to communicate with names instead of IP addresses. However, ensure that your router supports the DNS functionality first.*

"Connecting" mobile phone subscribers with dynamic IP addresses via DNS is not supported by some mobile phone service providers (see also Section 3.6.3). Please query this with your mobile phone service provider.

◄ **Fig. 25**

DynDNS.com allows you to assign names to routers. These names can then be used worldwide for communication over the Internet.

Fig. 26 ►
A connection establishment from the Internet to the mobile subscriber is blocked by most mobile phone service providers.



3.6.2 From the control center to a remote station via the Internet

In the next example (**Fig. 26**), the control center (fixed Internet connection [1]) accesses the remote station (mobile subscriber [2]); this type of use occurs frequently. To ensure an improved understanding of the initial steps, security and dynamic IP addresses are not taken into account here.

Control centers often need to temporarily access a remote subscriber, for example in order to exchange data or software updates. If a connection establishment is initiated from the control center via the Internet, the mobile phone service provider generally prevents this connection establishment. Why does this happen? One important reason for this is to protect the mobile subscriber from Internet attacks. Another reason is the mobile phone service provider's invoicing. Accessing a mobile device from the Internet creates data traffic in the mobile phone network, a very scarce resource. The question is, who pays for this data traffic? The customer with the mobile device, who perhaps did not want a connection to be established from the Internet, or the unknown party from the Internet who initiated the data link? Furthermore, how should a bill, possibly for just a few cents, be sent to a unknown party from the Internet? These are two important reasons why a establishing a connection from the Internet to the mobile phone subscriber is blocked by most mobile phone service providers.

Many mobile phone service providers block a connection establishment from the Internet to the mobile phone network. A solution to this problem is presented next.

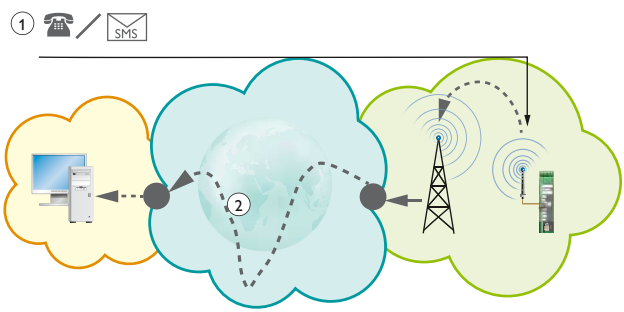
How can the problem be solved?

Many mobile phone service providers block a connection establishment from the Internet to a mobile subscriber. For this reason the following trick should be made use of and it works almost worldwide (see **Fig. 27**).

The control center does not establish the connection directly, but rather indirectly. How does it work? The control center first calls the mobile terminal or sends it an SMS. The mobile terminal then establishes the connection to the control center. When the connection has been established, data can be exchanged from the control center to the controller via the mobile phone router. The owner of the SIM card pays for the connection establishment. The big advantage of this approach: You circumvent the blockade of most mobile phone service providers.

Some end customers do not want data to be read out or firmware updates to be performed by the machine or system supplier without a request. For this reason, industrial mobile phone routers from Phoenix Contact have an additional option of initiating the connection establishment by turning a key switch on the machine. A connection can be established only if the key switch has been turned.

*The trick of initiating the connection establishment through a call or an SMS helps to circumvent the blockade of the mobile phone service providers (**Fig. 27**).*



◀ Fig. 27

Connection is established via a call, an SMS or a key switch. Data can then be exchanged between the control center and the remote station. This approach works virtually worldwide.

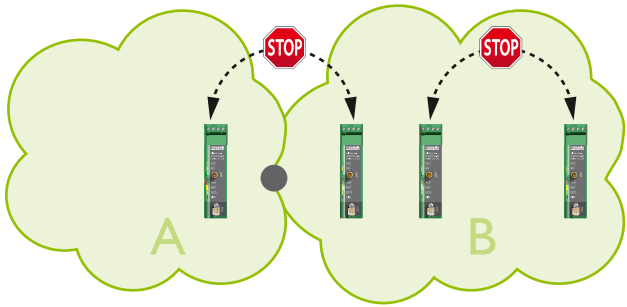


Fig. 28 ►
Mobile phone network operators usually block communication between two mobile phone subscribers, whether across networks or within a single network.

3.6.3 Communication between two mobile subscribers

In many applications, a straightforward point-to-point connection should be created between two mobile terminals. However, many mobile phone service providers block data exchange between two mobile subscribers. The reader should not equate data communication with a voice connection, for which there are generally no limitations.

A frequent justification for blocking data exchange between two mobile subscribers is reducing the load on the mobile phone network. Mobile phone service providers are mainly thinking about how many smartphones and tablets consumers have and less about industrial applications.

Most mobile phone service providers block data exchange between two mobile phone subscribers, whether this occurs across networks or within the same network.

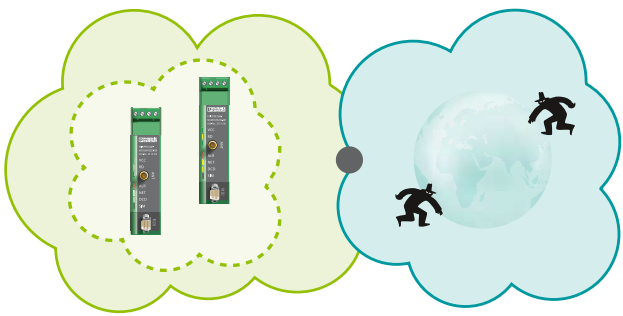


Fig. 29 ►
Closed user group by using static, private IP addresses from the mobile phone service provider.

How can the problem be solved?

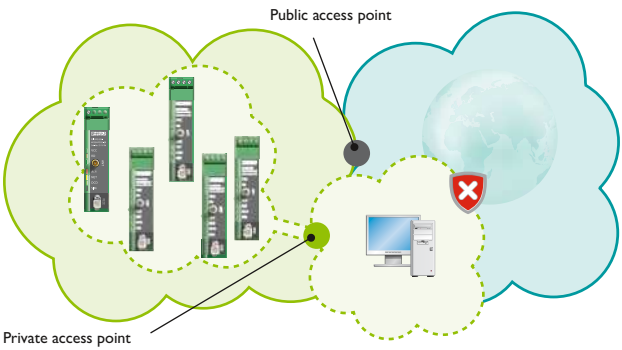
Some mobile phone service providers offer a special service of establishing closed user groups so that mobile phone subscribers can exchange data among each other. The mobile phone service provider then assigns the mobile devices static private IP addresses (not to be confused with static public IP addresses, which few mobile phone service providers offer).

The big advantage of a closed user group is that the devices can communicate among each other but cannot be contacted from the Internet. This ensures high levels of security and protection from internet attacks by third parties is provided (see **Fig. 29** and **Fig. 30**).

Private static IP addresses offer many advantages. Unfortunately, not all mobile phone service providers offer this service.

In the case of a closed user group, the customers often forgo additional data encryption, reducing the complexity of the mobile devices and lowering their cost. In addition, the amount of data to be transmitted is lower, because the overhead of the security protocol is eliminated, and therefore the transmission costs can be reduced further. You can find more information about IT security in Section 3.7.

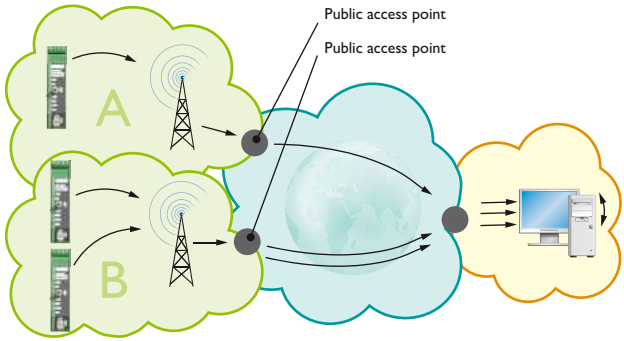
Unfortunately, this approach has its own problems. Depending on the country, private static IP addresses can be expensive or even are not offered at all. Communication between different



◀ Fig. 30
Mobile devices with a private, static IP address can be linked directly to the company network via the private APN.

Fig. 31 ►

If a multipoint connection is desired, this can also be established using special software in the central computer. This computer links the communication connections to each other.



mobile phone service providers is often not possible and static private IP addresses are often only worthwhile for national projects.

Another approach that can be used worldwide is the use of special software on the company computer systems. Each mobile terminal establishes a connection to the company network via the Internet. The software in turn links the mobile subscribers to each other. If the mobile devices are linked to each other via the server in the company network, they can exchange data. The advantage of this solution is that it works with nearly all mobile phone service providers worldwide. In addition, the customer is not bound to a mobile phone service provider. The mobile terminals can use different mobile phone networks (see **Fig. 31**).

The disadvantage of this solution is that it is only worthwhile if several mobile terminals are used. For a simple point-to-point connection between two mobile devices, the approach is relatively expensive. In addition, communication occurs over the public Internet and if this is the case, the data should be transmitted with encryption.

Portal instead of software

Several mobile phone service providers already offer this kind of software functionality. This solution is called a portal. The advantage of a portal is that the customer does not have to worry about the software used to link the mobile devices. The mobile phone service provider assumes responsibility for this. The disadvantage is that the customer connects to the mobile

phone service provider's network, which may be problematic for international projects. This must be clarified in the project planning phase with the mobile phone service provider.

Communication with several mobile devices

Packet-oriented data communication permits point-to-point connections as well as multipoint connections. Many users desire a multipoint connection between mobile terminals (see **Fig. 15** on page 26), but the difficulties associated with them are often forgotten.

One problem, described above, is that many mobile phone service providers often do not support data exchange between mobile terminals by default. If data exchange is supported by a mobile phone service provider, the user often does not consider the bandwidth allocation.

In the example of **Fig. 15**, three mobile phone devices in the field should communicate simultaneously with a mobile phone router in the control center. All connections converge in the control center. As such, the bandwidth requirement in the control center is greater than that of the individual remote stations. A device with the greatest possible bandwidth should therefore be used in the control center. A mobile device with low bandwidth would be of little use there. A 3G router would be a much better solution than a GPRS modem.

A multipoint connection consisting only of mobile terminals is wise only if the number of remote stations remains low.

If many remote stations are supposed to communicate simultaneously with the control center, a broadband fixed network Internet connection is recommended in the control center. The bandwidth of a fixed network Internet connection is generally greater and more stable than the bandwidth of mobile Internet access. In addition, there are no restrictions in terms of establishing connections from the mobile device to the fixed network Internet connection (see Section 3.6). Establishing a connection from the mobile terminal to the Internet is supported virtually worldwide, whereas data exchange among

Fig. 32 ►
IT security from Phoenix Contact. From the safety clip to the security router.

mobile phone devices tends not to be.

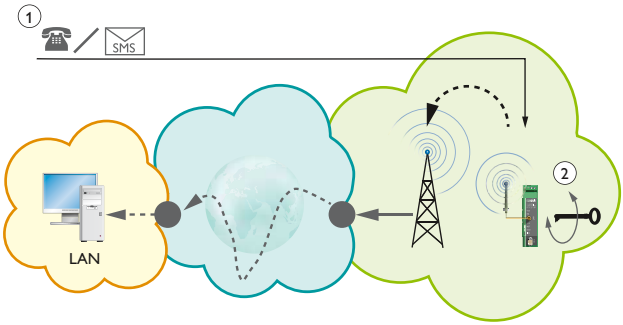
With the mGuard product range from Phoenix Contact, you can establish several hundred connections to the control center in parallel. This allows you to establish a professional multipoint connection on a global scale.

3.7 IT security

The worldwide networking of systems and machines offers significant competitive advantages to numerous companies, such as time savings, cost savings, and the opportunity to offer completely new service business models. Yet each opportunity brings certain risks. One risk is that someone will access the machine or system without the customer's consent. As such, IT security is becoming of paramount importance in industrial applications.

For this reason, Phoenix Contact already offers a large range of industrial IT security solutions, from the simple RJ45 safety clip for protecting switch ports to IT security routers with firewalls and IPsec encryption.

IT security in the industrial sector is a complex matter. Phoenix Contact has offered seminars on this topic for several years now. Please contact us if you are interested.



◀ **Fig. 33**
You cannot be attacked if you are not on the network. A connection to the Internet is established only upon command, by a call (selective call answering), by SMS (password protection) [1] or by turning the key switch [2].

3.7.1 Advantage of a mobile phone router

If you are only accessing a machine or system temporarily, it would be ideal for the device to be connected to the Internet for this period only. The device should be disconnected from the Internet for the remaining time. This approach considerably reduces the risk of being attacked. This is due to the fact that you cannot be attacked if you are not on the network.

This is particularly easy with a mobile phone router. There are various options available to establish the mobile phone router Internet connection only when required. One option is to send the mobile phone router an SMS (see **Fig. 33** [1]). The mobile phone router detects the SMS, checks the password and the phone number of the sender if required, and only then establishes a connection to the Internet. At a second connection level, the mobile phone router can be configured so that it establishes encrypted data communication with you in the control center, for example, a VPN tunnel via IPsec encryption. In doing so, other channels of communication are deactivated. So you have the greatest possible protection against Internet-based attacks.

Another point that should be considered in the planning phase is whether an attack from one's own network can be ruled out or not. A typical question to ask is: Can third parties connect a notebook to the mini network of the machine or system unhampered?

If an attack from one's own network cannot be ruled out, secure communication should be planned, usually all the way to the terminal. Data are therefore encrypted and decrypted

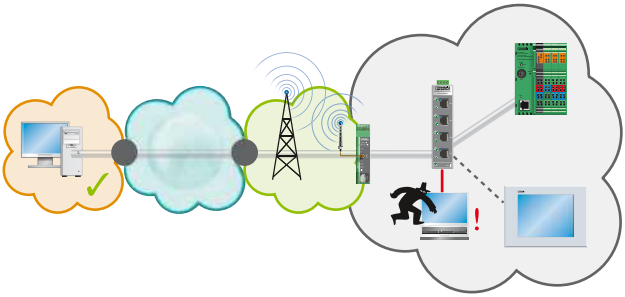
directly in the terminal, which makes the terminal more complex and often more expensive. However the requirements for the mobile phone router are lower because it only has to forward the encrypted data between the networks.

Make sure that third parties cannot easily connect directly to your mini network via notebook.

If the entire mini network is in a closed control cabinet, third parties often do not have direct access to the network. In such cases, an attack from one's own network is often classified as negligible risk. Advantage: In such cases, the terminals do not all have to encrypt or decrypt the data packets but rather only the routers, which communicate directly with the Internet. The requirements for communication security are therefore centralized on the routers and the configuration of the rest of the system is much easier.

Depending on the desired security, there are different encryption methods that are used between the remote routers. Each security protocol creates additional data that must be transmitted over the wireless interface. In each case, one must decide whether higher data encryption is desired, with the disadvantage that the data volume to be transmitted increases, possibly resulting in higher costs from the mobile phone service provider, or whether only weak data encryption is used in order to reduce the security overhead to a minimum and thereby optimize data transmission costs.

Each security protocol generates additional data that must be transmitted over the wireless interface. You must therefore often decide whether data transmission will be security-optimized or cost-optimized depending on the application. In most cases, cost-optimized data transmission means NO additional encryption for the customer. At this point we should also point out the potential costs arising from damage to your brand if the public discovers that your company transmits confidential machine data belonging to the end customer over the Internet with inadequate protection.



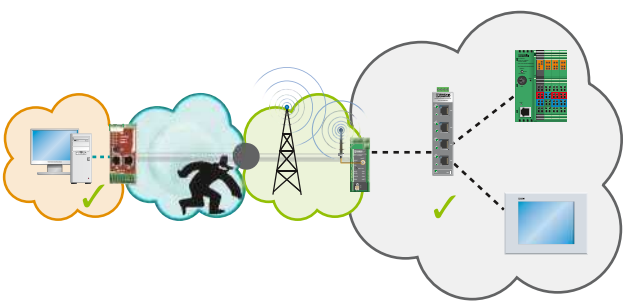
◀ **Fig. 34**

Prevent attacks from your own network to the greatest possible extent. In this case, the data packets would have to be encrypted and decrypted directly in the terminal and the complexity of terminals is thereby increased.

The damage to your brand resulting from data being intentionally transmitted insecurely is much greater than the costs of secure data transmission.

Typical security protocols include SSL and IPsec. The IPsec protocol is common in the industrial sector because it is also classified as secure by company IT departments. IPsec offers a number of configuration options that also have an effect on the security overload. High security creates a greater overhead, while just adequate security enables a lower overhead.

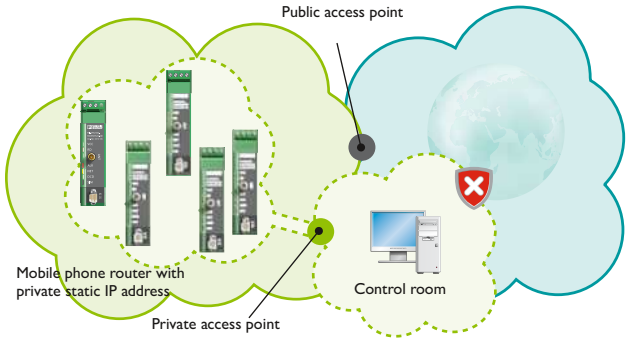
Ask your IT department or the IT department of your end customer for their minimum required security standard.



◀ **Fig. 35**

The greatest danger is an attack from the Internet. The routers, which are positioned between the public and private networks, are responsible for encrypting and decrypting data packets. The other network subscribers do not have to concern themselves with the security configuration.

Fig. 36 ►
If the customer uses a private APN, the risk associated with his mobile devices being attacked from the Internet is reduced considerably.



3.7.2 Using private access points

Decrypted communication over the Internet is a security risk that should generally be avoided. One approach is to generally bypass the Internet in communications. This is possible by using mobile phone routers in conjunction with a private APN. As can be seen in **Fig. 36**, a closed user group can be created using private static IP addresses assigned by the mobile phone service provider. The devices of this group can communicate with each other and with the control center, but not directly with the Internet. The mobile phone devices are therefore well protected against attacks from the Internet. As such, data encryption is a secondary matter for many customers.

The result is that the requirements placed on the communication hardware can remain relatively low because the devices do not have to encrypt the data. The data volume to be transmitted is minimized because the security overhead caused by the normally necessary encryption is eliminated. The device configuration is therefore is much easier.

The disadvantage of private access points is that SIM cards with private static IP addresses are usually more expensive than standard SIM cards. In addition, not every mobile phone service provider offers these special SIM cards. For international projects in which several mobile phone service providers are involved, roaming to the private access point in the home country is often not supported by the mobile phone service providers in the host country, unlike roaming to the public access points of the mobile phone service provider. Furthermore, the mobile

phone network operator can view data in private APNs. This risk should not be underestimated, especially in international projects, for example. Ensure that you discuss this with the mobile phone service providers in your home country in advance.

Check whether you can use static private IP addresses as an alternative, as they offer many advantages.

3.7.3 Using public access points

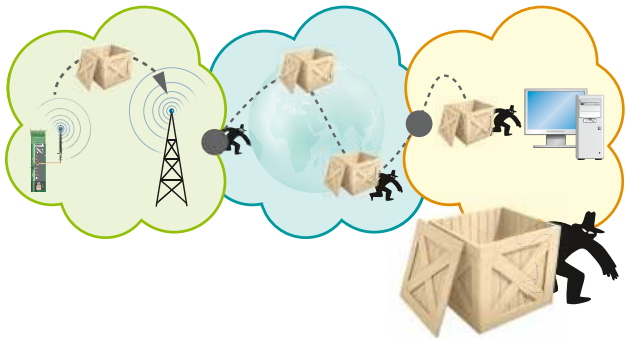
If you nevertheless decide to use the public access point, communication is also established over the public Internet. Many users often forget that the IP data packets that are transmitted over the Internet from A to B are generally not encrypted. As such, each party involved in the communication chain can view the content or even change it, which poses a particular security risk.

If you compare these data packets to wooden crates (see **Fig. 37**), they would be open wooden crates that are sent around the world. The contents can be viewed and changed by each party involved in the transport chain. In order to make communication over the public Internet secure, the following must be ensured:

a) Third parties cannot intercept the message (confidentiality)
b) Third parties cannot change the contents of the message even if they do not understand the message themselves (integrity)
c) The message actually originates from the specified sender (authenticity)

The above can be achieved using security protocols such as IPsec. If a data packet encrypted by IPsec is compared to a wooden crate, the wooden crate is now closed and sealed instead of open (see **Fig. 38**). All parties involved in the transport chain still see the wooden crate, but can neither view nor change the contents (in this example, the contact information of the sender are also stored in the closed crate).

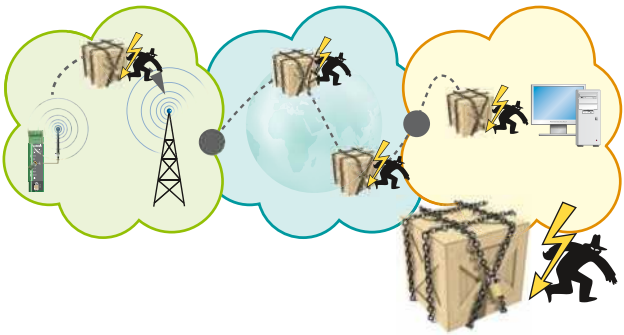
Fig. 37 ►
Data packets are often transmitted over the Internet without encryption. If you compare these data packets to wooden crates, they would be open wooden ones that are sent around the world. The contents can be viewed and changed by each party involved in the transport chain.



3.7.4 Symmetrical and asymmetrical encryption

There are many mathematical methods for data encryption. A general distinction can be made between symmetrical and asymmetrical encryption methods.

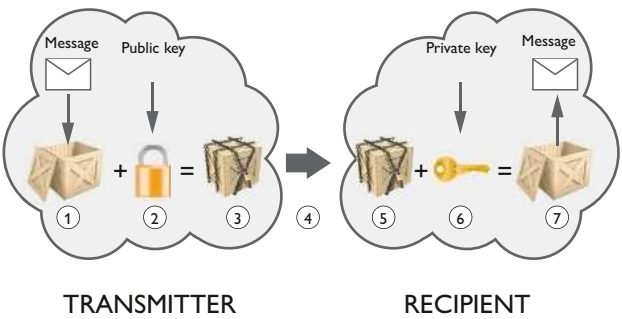
Symmetrical encryption methods have the advantage that they can be mathematically 100% secure. The main disadvantage is that the transmitter and receiver must have the same key for encryption or decryption. The handover of the key therefore poses a high risk. How do I deliver the key? Can the deliverer be trusted? In point-to-point communication, for example, between the presidents of two countries, this is logistically possible. In multipoint communication, in other words if many devices want to communicate securely with each other, this approach is unsuitable. Each communication device needs the particular secret key of each device in order to exchange data securely with all devices. If a new device is added, all devices must update their key file. In addition, each of the communication partners must trust that none of the other communication partners will divulge the secret keys of the others. In practice, this poses a big problem. This is the reason why the asymmetrical encryption



◀ **Fig. 38**
Encrypted data packets cannot be viewed by external users, and content cannot be modified.

method was developed.

In the asymmetrical encryption method, the transmitter and receiver have *different* keys for encrypting or decrypting the message, the public key and the private key. The public key is used to encrypt the message, whereas the private key is used to decrypt the message. The public key can be compared to a padlock, which automatically locks when it is pressed closed. This padlock (including identical copies) is freely available to all communication partners who want to send the device a message. For example, if subscriber A wants to send a message to subscriber B, subscriber A retrieves the padlock from device B, locks its crate with it (by closing the padlock), and sends this crate to subscriber B. After the crate has been locked, subscriber A can no longer change the contents of the crate, because the padlock has already been closed and she does not have the key



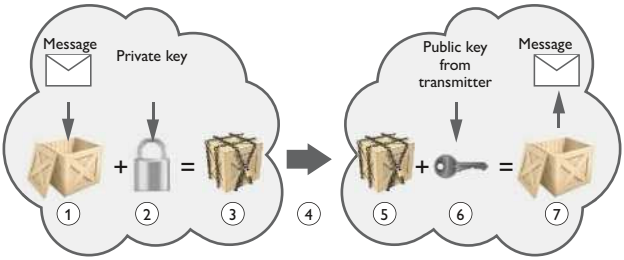
◀ **Fig. 39**
Basic concept of asymmetrical encryption.

to open the lock. Only the recipient of the message has this key.

If the public key is compared to a padlock, the private key can be compared to the key to the padlock. Only the recipient uses the private key, so he must keep it secret under all circumstances. As soon as device B has received the crate from device A, he can open the crate with using his private key and remove the contents.

A key advantage of asymmetrical encryption is that there is no longer the problem of securely delivering the key. The key for encryption is publicly available to everyone. In addition, each device, no matter how many devices communicate with each other, must manage only two keys: Its private (secret) key and public key (the lock identical to padlocks), which it provides to every other device.

This is a significant advantage compared to the symmetrical method. It sounds a relatively simple process, but in actual fact is much more complex. While the principle of symmetrical encryption has been used for hundreds of years with different degrees of complexity, the asymmetrical encryption method



◄ **Fig. 40**
Basic concept of authentication using asymmetrical encryption. Here the public key and private keys are used in reverse order.

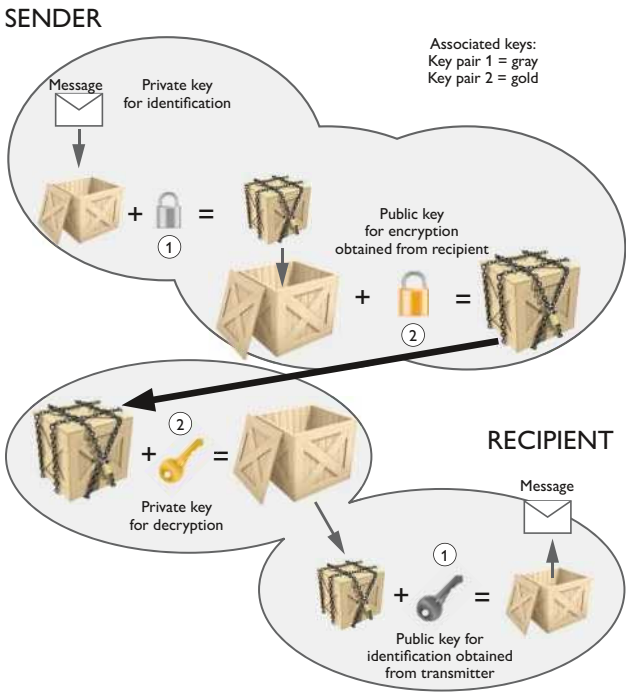
was only presented to the public in 1977.

Important to know: The asymmetrical encryption method is not 100% mathematically secure. The security is based on the fact that there is still no mathematical method that enables a quick "backward calculation" without the appropriate key. Therefore it can take years, centuries or even millennia to decrypt a message depending on the length of the key. For this reason, if the basic mathematical conditions are fulfilled, asymmetrical encryption is today classified as very secure and is used in many applications, for example, in the military, at banks, in wholesaling, and in government agencies:

In the example, the public key and the private key were compared to a padlock and the appropriate key. Yet in reality, two mathematical methods are applied to the message. What is special here is that these mathematical rules can also be used to create electronic signatures. To do so, the application is simply turned around (see **Fig. 40**).

Subscriber A does not encrypt his message with the public key of the recipient but rather with his private (secret) key. Subscriber B, who receives the message, does not then use his private key but rather the public key from subscriber A. If device B can decrypt the message, the following conclusion can be drawn: Because device B can only decrypt the message with the public key from device A and device A is the only one who has the private (secret) key to encrypt the message, the message could have originated only from subscriber A.

Fig. 41 ►
Basic concept of combining encryption and authentication using asymmetrical encryption.



Confidentiality comes second in this approach because each device on the network can use the public key from device A for decryption. In this case, unique identification is the focus.

If both operations are linked to each other (see **Fig. 41**), confidentiality and authorship can be ensured. To do so, imagine the message packed into two crates.

The first crate is encrypted with a private key for later identification. At the same time, a public key is provided to all later recipients. This crate is then packed into another crate. The second crate is then locked using the public key of the recipient, the actual padlock, the encryption.

The recipient can then open the larger crate using his private key. In order to open the inner crate, the recipient uses the public key, which the transmitter provided at the same time. Confidentiality and authentication are thereby ensured.

Purchased digital certificates

Self-created digital certificates

◀ **Fig. 42**
Certificates are available from accredited approval boards for a fee. However, it is also possible to create digital certificates oneself for free.

3.7.5 Certificates

Certificates are often used when secure communication is established between two subscribers. Certificates can be compared to IDs and are used to identify the particular subscriber. A digital certificate contains, for example, the name of the issuer, the name of the certificate owner, and much more. Standards are available describing the structure of certificates so that they have a uniform look and feel. One of the most important standards for digital certificates is X.509. As such, people often refer to these as X.509 certificates.

Official digital certificates can be purchased from certification authorities (CAs). A well-established provider is *VeriSign*. The use of such purchased certificates is recommended if completely unknown network subscribers want to communicate with each other. For example, a customer visits the website of a new bank and wonders if the bank even exists. The bank's website can identify itself to the customer's computer using the digital certificate.

A digital certificate can be compared to a passport. The vacationer applies for the passport from city hall, which is then created by the Federal Printing Office. At a passport check at the airport, for example, the customs official asks to inspect the passport, as the official and the traveler do not know each other. The official trusts the information in the passport, as it was created by a trustworthy organization, the Federal Printing Office and the vacationer is therefore allowed to travel. The official is the customer's computer, the passport is the digital certificate,

the Federal Printing Office is the CA, and the vacationer is the website.

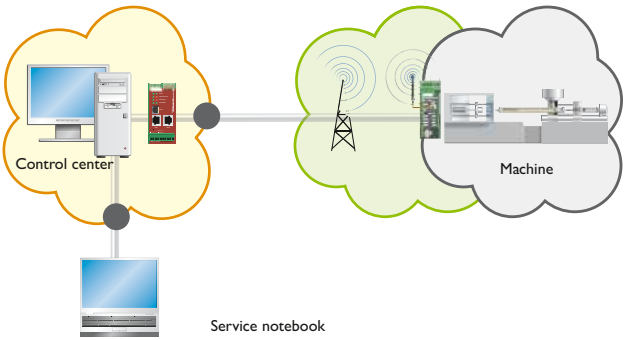
However it is also possible to generate digital certificates oneself for internal use. Self-generated digital certificates can be compared to internal company IDs. The IDs are created by the company itself, so no fees have to be paid to city hall. These IDs are not suitable for the passport check at the airport. Yet for the company's security department, the ID is fully sufficient as a means of identification because the company creates the ID itself.

The choice of certificate greatly depends on the later use. For networking a company's own routers, self-generated digital certificates are generally fully sufficient. The company trusts itself and does not require an inspection by a third party.

3.7.6 Use of service notebooks

In the project planning phase, it is often assumed that communication with machines and systems should be established directly from the employee's service notebook. However, such an approach may pose a big security risk for the company. What would happen if the employee's notebook were stolen or the employee left the company because of disagreements? For security reasons, all keys and certificates in machines and systems would have to be changed, which may result in costs and significant damage to the company's image.

A much better approach is to always establish communication with machines and systems through a central point, e.g., through the control center. The service technician connects to the control center through a VPN tunnel and from there is automatically forwarded to the machine through another VPN tunnel. This approach appears to be more complicated, yet has its advantages. If the service technician loses his notebook, it is stolen from him, or he leaves the company, the VPN tunnel from the service notebook to the control center simply has to be deactivated. As the service employee never had direct contact with the access data of the machine, the system remains secure. In addition, this approach allows you to grant temporary machine access to third



◄ **Fig. 43**
Accessing machines directly via the service notebook poses a security risk, which can be avoided by establishing the connection through the control center.

parties without having to give them access data directly.

When considering security, also consider the employee as a potential weak link.

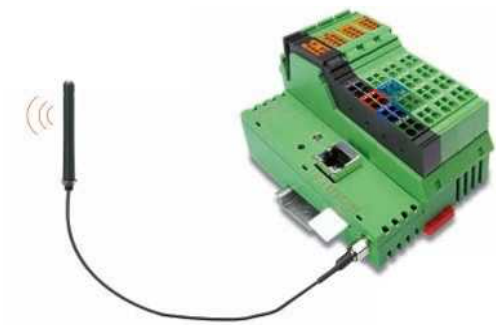
4 Mobile phone hardware

4.1 Integrated or separate communication modules

In industrial applications, there are often two possible solutions: Firstly an integrated mobile phone solution is desired by the customer, such as a controller, in which a mobile phone communication interface is already integrated. Alternatively, the customer adds a separate module to his application, such as a mobile phone modem. Both approaches have their strengths depending on the application and site in question.

4.1.1 Temperature range

When using mobile phone modules in an industrial environment, the temperature range is a key criterion for both integrated and separate solutions. If the temperature specifications of unbranded products are much better than those of products from well-established manufacturers, then begin to question the solution. Ensure that the manufacturer has not accidentally equated the maximum temperature of the most critical device component with the maximum possible ambient temperature. This approach is usually inaccurate, as the device operating temperature is always higher than the ambient temperature. The maximum permitted ambient temperature must therefore be *lower* than that of the most critical component.



◄ **Fig. 44**
Controller with integrated mobile phone interface, ILC150 GSM/ GPRS from Phoenix Contact.

Fig. 45 ►
Mobile phone modem/routers as separate components from Phoenix Contact.

Compare the temperature specifications of the device with comparable products from well-known manufacturers. If there are considerable differences, contact the supplier regarding this matter.

4.2 Power supply

4.2.1 Battery

Most devices of a mobile phone network are mobile, battery-operated terminals, such as mobile phones. In such applications, energy management is especially important in order to maximize battery life. The transmission power is therefore automatically reduced to a minimum level when good network coverage is available and increased when network coverage is poor. As such, local coverage has a significant effect on the energy consumption of the device.

When planning battery-operated applications, it is important to consider the network coverage in order to achieve efficient energy management.

4.2.2 Power supply unit

Inexpensive mobile phone products are often offered with a separate plug-in power supply unit as an accessory, for example, from 230 V to 5 V or from 24 V to 5 V. On the one hand, the price is divided into two components and appears lower. The printed price for the mobile phone product looks very reasonable,

however this does not take into account the higher price for the essential accessory. Remember to bear the total price in mind. More importantly however is the fact that the manufacturer of the mobile phone products can pass the cost of tests and approvals onto the provider of the plug-in power supply unit. What's more, plug-in power supply units are often not developed according to industry standards, so ensure you compare temperatures and EMI.

The customer usually pays for the savings made by the manufacturer of the mobile phone product, so be skeptical.

In practice, the following disadvantages often occur:

- The separate power supply unit requires more space in the control cabinet.
- Power supply units are often not designed for industry, from electromagnetic compatibility (EMC) to the lack of DIN rail mounting.
- When a plug-in power supply unit is used, a socket and a special attachment for the separate power supply unit may have to be installed in the control cabinet.
- Separate power supply units are additional replacement parts that have to be warehoused.
- The separate plug-in power supply units are often unbranded products that do not necessarily offer long-term availability.
- High-quality data sheets and product information for plug-in power supply units are rarely available.
- Lack of responsibility if the device fails: Was it the fault of the mobile phone product manufacturer or the power supply unit supplier?
- Temperature range of power supply units is smaller than the temperature range of industrial components.
- Missing approvals, such as EX.
- Worse MTBF times (Mean Time Between Failures).

These disadvantages along with others often mean that the cheapest solution is not the optimum solution. Less space and greater expense for mounting, replacement parts inventory,

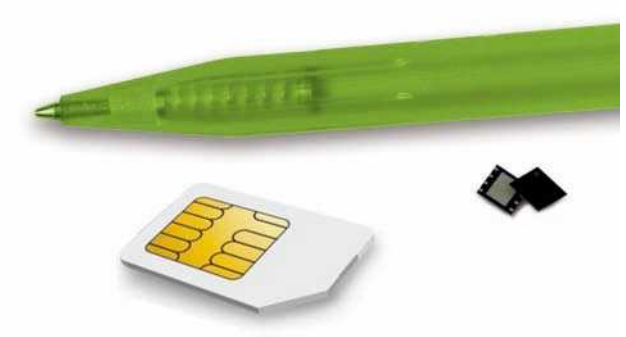


Fig. 46 ►
On the left, a conventional SIM card; on the right, a SIM chip with the same functionality but for soldering purposes.

documentation, and communication are just a few of the disadvantages.

Mobile phone products with a separate plug-in power supply unit are often the best solution for the manufacturer, but not for the customer.

4.3 The SIM

The SIM (Subscriber Identity Module) contains all the key data about the device and is used for authentication purposes in the mobile phone network. Despite its small design, it is an essential device component.

Two approaches to the design are currently favored. On the one hand is the SIM chip, which can be permanently soldered, and on the other hand is the plug-in SIM card (see **Fig. 46**). Both types have their advantages and disadvantages.

4.3.1 The SIM chip

The SIM chip has many technical advantages over the SIM card. It is extremely small, has a better temperature response, is vibration-resistant, and cannot be incorrectly inserted or stolen: Ideal for a large-quantity series product.

However, the main disadvantage is that the chip is currently permanently associated with one mobile phone service provider. The chips are pre-configured ex works for *one* mobile phone service provider. If the customer wishes to switch from mobile phone service provider A to mobile phone service provider B at

a later date, for example, because mobile phone service provider B has better local network coverage, this is not currently an option.

Another problem with SIM chips is evident in international business. Who enters into a contract with the mobile phone network operator? The manufacturer of the mobile phone hardware, the mechanical engineer or the end customer?

Is the telecommunications law in the destination country comparable to that of the home country? Can contracts with mobile phone service providers in the foreign country (home country of the supplier) actually be concluded in the destination country? Such legal queries must be clarified in advance.

These questions and others can to the greatest extent be avoided with a plug-in SIM card.

4.3.2 The SIM card

The greatest advantage of the SIM card over the SIM chip is the high level of flexibility for the customer. The customer can enter into a contract with any network provider across the globe. If network operator A has no local network coverage, the installer can simply use a SIM card from network operator B. However, for this flexibility the customer must accept technical disadvantages.

Temperature response

If the SIM card is installed in the communication module, it forms a sub-component of the device and must therefore meet the same temperature requirements. A mobile phone modem with a temperature range of -40° C to +100° C, for example, is of little use to the customer if the subsequently installed SIM card does not share these properties.

In the planning phase, also take the temperature range of the SIM card into consideration, as this is often neglected.

Service life

A chip is located on the SIM card. This chip cannot be read and written in an unlimited manner. This is rarely a problem for consumers, as the product lifecycle is relatively short, typically from two to four years. In industrial applications, which often run reliably for ten to fifteen years, this is entirely a different matter. Frequent writing of the SIM card can reduce service life, and must therefore be taken into consideration in the planning phase.

Ask your mobile phone service provider if it offers special SIM cards for industrial use. SIM card manufacturer *GEMALTO* has recently started to offer SIM cards designed with industrial applications in mind. An increased temperature range and a longer service life are some of the essential features to bear in mind.

If you cannot obtain an industrial SIM card from your mobile phone service provider, use a mobile phone router, which keeps the writing and reading of the SIM card to a minimum.

Mobile phone components from Phoenix Contact aim to minimize the writing and reading of the SIM card in order to maximize service life of the SIM card.

PIN

To prevent misuse of the SIM card, a PIN (Personal Identification Number) can be activated on the card. This is a wise idea if, for example, external staff have access to the SIM card of the machine or system.

If the SIM is removed from the system and inserted into an external device, the PIN is automatically requested. If the PIN is not entered, the SIM cannot be used. If an incorrect PIN is entered, the card is blocked after the third attempt.

Mobile phone modules should always allow SIM cards with an activated PIN to be used. This simple security feature is not supported by all product providers. Please ask your supplier for further details.

Contract

The end customer usually signs a contract with the local mobile phone service provider in the destination country. This has two key advantages. Firstly, the machine supplier does not have to worry about a mobile phone contract in the destination country. Secondly, the end customer is the telecommunications contract party and assumes the costs of the data transmission.

A potential disadvantage is that the end customer signs the wrong mobile phone contract, such as a pure voice contract instead of the necessary data contract. The installer then experiences problems during the initial startup of devices.

Another risk is that the end customer later agrees to a contract change as a result of a sales call without being aware of the consequences. Seemingly out of nowhere, communication with the machine is no longer possible or becomes extremely expensive. If the new, unsuitable contract also has a long contract term, such as 24 months, this is all the more frustrating.

The decision as to whether it is better for the end customer or the machine engineer to handle the mobile phone contract must be made on a case-by-case basis.

If the end customer is responsible for a SIM card contract, make sure that he

- *does not sign the wrong contract*
- *does not change the mobile phone contract without consulting with the machine and system engineer*

Conclusion: The plug-in SIM card currently offers customers the greatest degree of flexibility. In most cases, this flexibility is more important than the technical advantages of a SIM chip. A solution that combines the flexibility of a SIM card with the technical advantages of a SIM chip would be a freely configurable SIM chip, also known as a soft SIM. Discussions have begun regarding these soft SIM solutions, but they are not yet available (as of November 2011) on the market.

The major problem, regardless of whether a SIM chip, SIM card or soft SIM is used, is entering into the right mobile phone contract.

4.3.3 The mobile phone engine

In addition to the SIM, another important component is the actual transmitting and receiving module, the mobile phone engine. Bad experience with mobile phone transmission is often blamed on the mobile phone network. For example, if you make a call with a cell phone and the connection is quite poor, the end customer is convinced who is to blame: The network. The cell phone itself is rarely called into question. This biased approach works against many manufacturers in the consumer industry. By forgoing "unnecessarily" high-quality modules, production costs can be significantly reduced. As such, the price advantage gained outweighs the technical quality of the product.

High-quality transmitting and receiving modules ensure communication even where lower-quality devices would have interrupted the connection.

The mobile phone industry is currently still highly focused on the fast-moving consumer mass market and less on industrial applications. It is for this reason that mobile phone engines for consumer solutions are usually available on the market one or two years earlier than high-quality products for industry. What's more, modules are more cost-effective due to the large quantities available.

To quickly offer industrial customers a solution as well, temptation to use mobile phone engines from the consumer sector in industrial components is great. By using inexpensive consumer modules, entry onto the market is faster, product-based profits are usually higher, and the provider can offer its devices at competitive prices. However, the customer often also reaps the disadvantages. The product service life of consumer mobile phone engines is shorter than that of industrial products, and consumer mobile phone engines rarely meet the technical requirements demanded by industrial applications. The following section should help you to distinguish the cheap products from the products offering a good value.

Customers are looking to purchase the device offering the best value. The mobile phone engine is currently a relatively

expensive yet essential device component. A number of providers therefore attempt to save on the mobile phone engine by using ones that are not suitable for industrial applications. Compare the prices with competing devices on the market. If the product is inexpensive compared to other competing products, take a skeptical approach. Mobile phone modules for industrial applications should contain only modules designed specifically for industrial applications.

The mobile phone engine is a relatively expensive component that manufacturers often try to make savings on. Ask your supplier which mobile phone engine (type, manufacturer) is used in their product. It should be suitable for industrial applications.

While the product life may only be months in the consumer sector, it is often years or decades in the industrial environment. Engine manufacturers for industrial mobile phone engines are aware of this difference. As such, high-quality mobile phone engines are offered in long-term programs.

Even in the industrial sector, mobile phone engines differ in terms of quality. Ask your supplier which products it uses.

The temperature range of the mobile phone engine is another important variable. Some mobile phone engine manufacturers attempt to sell consumer-based mobile phone engines produced by themselves on the industrial market as well, under the guise of being suitable for industrial applications. An "extended" temperature range is promoted so that a large temperature range can be specified on the data sheet. Only in the fine print, if at all, does the reader discover that in this temperature range the devices have only limited functionality or no longer meet the required mobile phone specifications.

Ask your supplier if the devices have limited functionality at increased ambient temperatures. If so, take this into consideration in your project planning.

4.3.4 The antenna

For mobile phones from the consumer sector, integrated antennas are state-of-the-art. However, in industrial applications communication modules are usually located in metal control cabinets, so the following has to be considered:

A closed metal control cabinet virtually prevents radio waves from entering the inside by acting as a shield. For good reception, you must therefore route the antenna out of the control cabinet.

Certain mobile phone modules are installed in rooms, in which there is no mobile phone reception, so the following rules must be considered:

The network coverage can be quickly checked on site using a cell phone. If you cannot make a call using the cell phone or have very poor reception, the antenna of the mobile phone router must also be routed out of the room.

What else has to be considered when using an external antenna? In practice, it is not simple to calculate the maximum antenna cable length because the mobile phone devices, as already described, independently regulate their transmission power depending on the local network coverage. As a general rule, the antenna cable should be kept as short as possible and should consist of one piece in order to minimize the attenuation. In addition, the mobile phone antenna should be mounted in the direction of the mobile phone tower, not in the direction of the remote station.

If the planned antenna cable distances are greater than 15 m, you should check if the communication module can be moved. If you have to decide between a long or longer data cable, a longer

◄ **Fig. 47**
Providers with broad product ranges can offer industrial turn-key solutions in addition to the communication module.

data cable should be preferred. In public invitations to tender, surge protection is often specified for antennas. Ask your supplier if he can also offer you this component as an accessory.

4.3.5 The turn-key solution

The customer requirement of getting all sub-components, possibly even a turn-key solution, from one source is continually on the rise. Perhaps this is where Phoenix Contact can also lend a hand?

5 What is next?

Data transmission over mobile phone networks is still relatively unknown in the industrial sector. Yet it offers a great deal of potential for customers, from simple cost savings to developing completely new business models.

Even in 2010 thousands of devices were being used, and the trend has continued to rise since then. In recent years, mobile phone service providers have also picked up on this trend and are responding to demand.

Specially designed industrial SIM cards and M2M contracts (M2M = machine-to-machine) are already available from various mobile phone service providers. The global SIM card was already being promoted by a number of network operators back in 2011. This SIM card is the ideal solution for export products because it functions virtually worldwide. In addition, SIM cards are offered with national roaming. If the mobile phone network of provider A fails, the mobile device can automatically connect to the network of provider B. In this way, maximum availability is ensured.

Communication between network operators and the industrial sector has begun! Many of the obstacles mentioned in this guide will soon be eliminated in practice. Phoenix Contact

◄ **Fig. 48**
Phoenix Contact has a global sales network.

has been offering mobile phone products for the industrial sector for several years now. At the same time, communication and cooperation with major network operators is being continually improved and strengthened on a global scale. Indeed, the goal is for customers to be offered the ideal solution by Phoenix Contact. Discover Phoenix Contact's expertise for yourself:

- Vast long-term knowledge of various industrial mobile phone applications.
- A complete solution from one source, from modular terminal blocks to controllers.
- Extensive global sales network, with 48 subsidiaries and 30 representatives in other countries.

Being at home all over the world and speaking the language of our customers is how we understand customer proximity. Proximity that ensures the best service for our partners.

6 Epilog

Dear Customer,

I hope that reading this guide has provided you with a lot of useful information for your next project.

Please briefly estimate how much time you saved by reading this guide, starting from your first Internet search through to initial startup.

- Time saved in hours: _____
- How expensive is an average hour of work for you?
  €/hour: _____
- How valuable was the guide?
  Saved hours * €/hour = value
  _____ h * _____ €/h = _____ €

A personal request from the author:
This guide is provided to you free of charge, and will continue to be provided to you and your colleagues for free in electronic format. Would you consider donating a small proportion of the calculated savings or using the money to do something together with your colleagues?

I would be very appreciative.

Regards,
Gerrit Boysen

7 Appendix

7.1 The major mobile phone network operators worldwide

Rank	Operator	Total Connection (million)	Markets
1	China Mobile	478.8	2
2	Vodafone Group	247.3	19
3	Telefónica Group	190.1	20
4	América Móvil Group	175.0	17
5	China Unicom	137.7	1
6	Deutsche Telekom Group	127.1	12
7	Telenor Group	96.6	10
8	Airtel (Bharti)	93.9	1
9	MTS Group	92.2	5
10	Verizon Wireless	86.6	1

◄ Fig. 49

Top ten largest network operators in the world.

Source: Intelligence Wireless

Some of the network operators also have subsidiaries under different names in various countries. As a general rule, information regarding these subsidiaries can be found on the network operator's website.

7.2 Overview of mobile phone standards

v • d • c	Mobile Telephony Standards	
0G (radio telephones)	MTS • MTA • MTB • MTC • MTS • MTD • AMTS • OLT • Autoradiopuhelin	
1G	AMPS family	AMPS • TACS • ETACS
	Other	NMT • Hicap • Mobitex • DataTAC
2G	GSM / 3GPP family	GSM • CSD
	3GPP2 family	CdmaOne (IS-95)
	AMPS family	D-AMPS (IS-54 and IS-136)
	Other	CDPD • iDEN • PDC • PHS
2G transitional (2.5G, 2.75G)	GSM / 3GPP family	HSCSD • GPRS • EDGE/EGPRS
	3GPP2 family	CDMA2000 1xRTT (IS-2000)
	Other	WiDEN
3G (IMT-2000)	3GPP family	UMTS (UTRAN) • WCDMA-FDD • WCDMA-FTDD • UTRA-TDD LCR (TD-SCDMA)
	3GPP2 family	CDMA2000 1xEV-DO (IS-856)
3G transitional (3.5G, 3.75G, 3.9G)	3GPP family	HSPA • HSPA+ • LTE (E-UTRA)
	3GPP2 family	EV-DO Rev. A • EV-DO Rev. B
	IEEE family	Mobile WiMAX (IEEE 802.16e-2005) • Flash-OFDM • IEEE 802.20
4G (IMT-Advanced)	3GPP family	LTE Advanced
	IEEE family	IEEE 802.16m
5G	*unconfirmed*	*unconfirmed*

◄ Fig. 50

Overview of mobile phone standards

Source: http://wikipedia.org

7.3 References

Mobile phone network

Schulungsunterlagen: GSM-Grundlagen
(Training documents: GSM basics)
Phoenix Contact, 2010

Martin Sauter:
Grundkurs – Mobile Kommunikationssysteme – Von UMTS und HSDPA, GSM und GPRS zu Wireless LAN und Bluetooth Piconetzen
(The basics: Mobile communications systems – From UMTS and HSDPA, GSM and GPRS to Wireless LAN and Bluetooth Piconets)
3. Auflage (3rd edition), Vieweg, 2008, ISBN: 978-3-8348-0397-9

Basics of network technology/cryptography

Schulungsunterlagen (training documents): Ethernet Security
Phoenix Contact, 2010

Rüdiger Schreiner:
Computernetzwerke – Von den Grundlagen zur Funktion und Anwendung (Computer networks **– From the basics to functional applications)**
3. Auflage (3rd edition), Hanser, 2009, ISBN: 978-3-446-41922-3

Martin Lüders, Stephan Sausel:
Netzwerke – Lokale Netzwerke analysieren, einrichten und anbinden (Networks – analyzing, establishing, and connecting local networks)
1. Auflage, (1st edition) Westermann, 2009,
ISBN: 978-3-14-222522-7

Andrew S. Tanenbaum:
Computer Networks
Pearson Education International, Fourth Edition, 2003,
ISBN: 0-13-038488-7

Simon Singh:
Geheime Botschaften: Die Kunst der Verschlüsselung von der Antike bis in die Zeiten des Internet (Secret messages: The art of **encryption, from the ancient world to the Internet generation)**
8. Auflage, (8th edition) dtv, 2008, ISBN: 978-3-423-33071-8
Albrecht Beutelspacher, Heike B. Neumann, Thomas Schwarzpaul:
Kryptographie in Theorie und Praxis – Mathematische Grundlagen für elektronisches Geld, Internetsicherheit und Mobilfunk (Cryptography in theory and practice – The mathematical basics for electronic money, Internet security, and mobile phones).
1. Auflage (1st edition), Vieweg, 2005, ISBN: 3-528-03168-9

Dr. Michael Alexander:
Netzwerke und Netzwerksicherheit – Das Lehrbuch (Networks and network security – The guide)
1. Auflage (1st edition), Hüthig, 2006, ISBN: 979-3-8266-5048-2

Alberto Leon-Garcia, Indra Wildjaja
Communication Networks – Fundamental Concepts and Key Architectures
Second Edition, McGraw Hill, 2003, ISBN: 7-302-07873-4

CISCO Network Academy:
CCNA 1 and 2 – Companion Guide
Revised Third Edition, CISCO Press, 2005, ISBN: 1-58713-150-1

Space for notes

Space for notes

Space for notes

Space for notes

Space for notes

Space for notes

Space for notes

Space for notes

The desire to remotely monitor and maintain machines and systems has been steadily increasing. There are many reasons for this, from simple cost savings to developing new service business models.

This guide is designed for project planners who intend to transmit data in industrial applications over the mobile phone network for the first time.

In terms of the guide's content, customer questions were evaluated after being gathered from different departments at Phoenix Contact, such as Sales and the Technical Hotline.

The aim is to answer the most frequently asked customer questions as succinctly as possible and with minimal IT terminology. As such, the focus is on the practical benefits for the project planner.

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Phone: +49 (0) 52 35 3-00
Fax: +49 (0) 52 35 3-4 12 00
E-Mail: info@phoenixcontact.com
www.phoenixcontact.com

Printed in Germany

MNR 52000746/15.03.2012-00

ISBN 978-3-00-037387-9

PHOENIX CONTACT
INSPIRING INNOVATIONS