Whitepaper

Introduction to remote control systems and remote maintenance systems for system monitoring

Author:
Eike Wedekind
Industry Solutions
ewedekind@phoenixcontact.com

CIS07-15.000.PR5

Table of contents

Overview: development of remote control technology

Just a few years ago it was extremely difficult to monitor and maintain distributed stations. The reason for this was that the remote systems were either unable to communicate with a control center or communication involved a great deal of effort and expense.

Today, all installations in supply and disposal technology, such as water, gas or energy supply, pipelines or even transportation technology applications, must be connected to a central control system. This allows smaller installations such as pumping stations, transformer stations or transformer substations to be monitored and controlled remotely. This connection presents new challenges for the technology.

Remote control and remote maintenance have since become the established standard in communication. Remote systems or external stations can be easily connected to the control center using a wide range of transmission paths. Standardized transmission is made easier thanks to defined, standardized protocols. The predictive maintenance that has been made possible as a result of this enables huge cost savings.

But which communication path is best suited to the relevant application?

This white paper is intended to provide all users with a practical selection guide to the communication mechanisms and media for remote maintenance and remote control technology that are relevant to them.

Difference between remote control and remote maintenance

In industrial communication, there is a vast difference between remote control and remote maintenance, even when using identical technology. This often leads to confusion when it comes to selecting the right communication media. The particular features of the different applications are therefore described below.

Remote maintenance

Due to globalization, central control systems are being used to operate systems and machines that are in ever more distant locations. In addition, the installed systems are constantly growing in complexity. This often leads to problems when needing to diagnose and remove errors in the event of a fault. Nowadays in the event of a fault, there is much more to it than just remote maintenance. Thanks to developments in recent years, complete support and monitoring of the production process is now possible.

Remote maintenance describes remote access to a station for fault diagnostics or for maintenance purposes. This saves costs, as a technician does not have to be on site or travel long distances in order to return the system to operation. Downtimes are also reduced.

Remote control technology

Using suitable remote control technology it is possible to influence all the parameters of the substations at all times. System states are continuously displayed in the control center. The required documentation of flow rates or liquid levels, for example, can be stored centrally for many years. Thanks to special protocols, process data can be transmitted securely over wide area networks, even with low bandwidth and with poor transmission quality.

Communication used to be performed via proprietary control lines with discrete digital and analog signals. As processes became more complex, more information was needed from the process, and it was possible to process this information in control systems, the discrete lines were, in many cases, replaced by serial connections via permanent line modems. Stations that did not have proprietary permanent line connections were connected via analog dial-up connections, leased permanent lines or wireless systems. Mobile communication connections were also later used. One of the disadvantages of dial-up connections is that there is no permanent connection to the control system and, as with voice telephony, connection establishment takes some time. Recently there has been a clear move away from serial transmission paths toward IP-based communication. Modern communication options such as Internet, DSL, GPRS/EDGE/3G, UMTS or LTE are also integrated in remote control technology.

Remote control technology describes the remote monitoring and control of physically separate system parts by means of data transmission. Measured values and control commands are transmitted over long distances and visualized, processed, and stored in a control center. In contrast to remote maintenance, remote control requires a permanent connection to a remote station in the vast majority of cases.

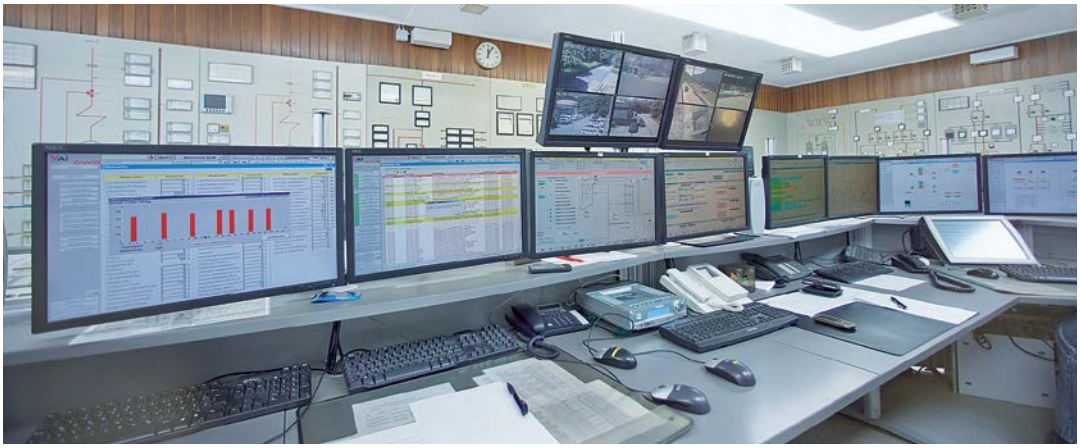

Figure 1
Control room

Communication protocols

There are specific protocols for every type of industrial communication. Fieldbuses with defined transmission paths are one particular protocol type. Even the cables are often specified and process information is usually exchanged cyclically with the fieldbus stations.

Another group of industrial protocols originates from the time of serial communication via permanent lines. These are mostly what are referred to as polling protocols. One example is the Modbus protocol, which is used worldwide.

A typical feature of this form of data exchange is that the control system polls each external station cyclically. Polling either only identifies changes or transmits all data points to the control system. However, in the event of a connection abort, it is impossible to later determine what happened at the external station during this time or whether specific threshold values were exceeded. The advantage of these protocols is their easy parameterization. The disadvantage is the setup of time dependencies which can be laborious.

With the introduction of remote control technology and the associated expansion of systems, a new type of industrial protocol was needed. Previously a physical connection was required between the control system and the external station, which limited the amount of data that could be sent. Over time the mobile communication network was increasingly used to connect external stations to the control system. As a result it was no longer possible to use time-critical polling protocols.

Mobile communication networks are storage networks that can retain the individual data packets which are then only reassembled again at the receiver. Once a connection has been established, the user no longer has to deal with data transmission. It is controlled by using TCP/IP, for example.

Connection abort is a known disadvantage of mobile communication networks. While an interruption on a permanent line means there is a fault, when it comes to data links via a mobile communication network, connection aborts are frequently caused by the provider without warning.

This behavior places new demands on a transmission protocol. It must provide internal security mechanisms in order to prevent data loss in the network.

Basic requirements

A remote control protocol must feature the following in order to satisfy current requirements:

Bidirectional, event-oriented transmission

It must be possible to send data to the external station and receive data from the external station simultaneously. For example, an external station must not be hindered by control system polling if it is transmitting an alarm message.

Storage of process information, e.g., in the event of connection interruptions

Some of the data in the processes is relevant for billing. It must not be lost as a result of a connection abort and must be stored by the external station as historical data until it has been received by the control system.

Time stamping of process information

For the control system to be able to reconstruct the data trend, the historical data must at least have an exact time stamp.

Time synchronization

In order to reconstruct data trends using the time stamp, all external stations of a system must use the same time as the control system. A remote control protocol must therefore offer the option of synchronizing all devices in the system.

Serial communication via proprietary permanent line

In some systems, distributed system parts are connected via the supplier's proprietary permanent lines. One example is the connection of the pumping station to the central process control system. Serial communication is possible here because copper cables are traditionally installed along with the supply lines. With protocols according to IEC 60870-5-101 or IEEE 1815 (DNP3), for example, the system is equipped with communication standards that are established in remote control technology. All requirements for secure remote control technology are therefore satisfied. In the event that the permanent line fails, the selected remote control protocol ensures that the data for a pumping station is stored in the remote control device.

Communication via TCP/IP or cables

If no proprietary cables are present, communication via a TCP protocol for networking distributed systems to the control system is a reliable method for data transmission. Protocols according to IEC 60870-5-104 or IEEE 1815 (DNP3) support standardized connections for stormwater overflow tanks, pumping stations or well shafts – via the mobile communication network or wired communication depending on the application. If such interfaces already exist at the control system, the remote control devices used can reliably communicate with the control system. Depending on the protocol used, communication is event-oriented and prepared for the use of GPRS-based hardware. In the event of the failure of the communication infrastructure, the remote control protocol ensures that data is stored.

Figure 2
Mobile phone tower

Protocols

Protocols for remote control

Various remote control protocols are listed and described below:

IEC 60870-5-101

IEC 60870-5-101 is an official communication standard for remote control technology in infrastructure sectors. This protocol is used as a general transmission protocol between (network) control systems and substations. Messages are transmitted via serial connections. This standard enables devices and systems for remote control and station control technology from different manufacturers to communicate with one another without the need for fundamental adaptations.

Protocol IEC 60870-5-101 is the standard protocol for serial data transmission in Europe and is also used in Asia.

IEC 60870-5-104

IEC 60870-5-104 enables communication between the control center and substation via a standard TCP/IP network. The TCP protocol is specifically used for connection-oriented, secure data transmission. As the name of the standard suggests ("Network access for IEC 60870-5-101 using standard transport profiles"), the protocol follows standard IEC 60870-5-101 with respect to the application layer. The biggest advantage of IEC 60870-5-104 is communication via a TCP/IP network, which enables simultaneous data transmission with multiple devices and services. Because the Internet can be used for communication, security by means of data encryption is an important topic. In addition, this is an event-oriented protocol where the substation can send data to the control system automatically.

Protocol IEC 60870-5-104 is the standard protocol for data transmission with TCP/IP in Europe and the USA and is also used in some Asian countries.

IEEE 1815 – DNP3

DNP3 (Distributed Network Protocol) enables communication between a substation and control room via a serial connection as well as via an Ethernet connection.

DNP3 was developed between 1992 and 1994 by Westronic and is based on IEC 60870-5. However, the protocol is more restrictive and offers less room for interpretation than its European counterparts.

Over time DNP3 has been extended to include authentication. Authentication means that external stations check the authenticity of the control system before executing critical operations. They do this by exchanging encrypted data.

Protocol IEEE 1815 is the standard protocol for serial and data transmission via TCP/IP. It is used in North, Central, and South America, South Africa, the UK, Australia, and also in Asia.

ODP – Open Data Port

The Open Data Port (ODP) communication protocol was developed by Bremen-based company Videc and is used for GPRS-based communication between a control system and remote control substations. The AX ODP server installed in the remote control center makes all data from the remote control substations available via a standardized OPC interface. This concept offers the user open communication with various OPC-based process control systems.

Both serial and Ethernet-based ODP communication has been implemented in the ReSyOdp function block library. The various hardware requirements must be observed when configuring the remote control substations.

The ODP specification is divided into three areas and supports online data, historical data, and alarms and messages.

Online data

The process image data is read cyclically from the PLC and displayed in the control system via the OPC interface. Switching operations can also be performed from the control center.

Historical data

Historical data is retrieved cyclically or in a user-controlled way. The time-stamped historical data is sorted in chronological order into *.csv files by the AX ODP server. The memory capacity in the PLC depends on the number of variables and the corresponding memory cycle.

Malfunctions, alarms, and messages

Malfunctions, alarms, and messages are transmitted to the control system by the substation in an event-oriented way. These can then be stored in chronological order and evaluated in the control system.

If the external stations are connected via the ODP server by means of GPRS, they can communicate with virtually any control system. In order to do this, the AX ODP server must be installed in the control center. The ODP server developed specifically for GPRS communication makes data for connection to the control system available via OPC. They are therefore manufacturer-neutral and can communicate with every OPC-based control system.

Protocols (not for remote control)

In addition to the remote control protocols listed, a number of other protocols have become established. These protocols are frequently used, however they do not save any data in the event of a connection interruption. Data that does not reach the control system can no longer be reproduced.

Modbus

Modbus is frequently used to allow devices from different manufacturers to communicate with one another based on a standard protocol. The Modbus protocol is a communication protocol based on a master/slave or client/server architecture. It was developed in 1979 by Modicon for communication with programmable logic controllers. Modbus has become a de-facto standard in the industry, as it is an open protocol. Modbus can be used to connect a client (e.g., a PC) and several servers (e.g., measurement and control systems). There are three versions of Modbus: Modbus ASCII, Modbus RTU, and Modbus TCP. The last two are by far the most popular. Modbus is probably the most widely used communication protocol in the world.

SEAB-1F

The SEAB-1F protocol was developed in 1972 by AEG and was later given the name Modnet-1F. It connects substations and control centers from the Geadat-120 product range. SEAB stands for serial system bus and 1F stands for remote control technology.

What is specific to the SEAB-1F protocol is that all data traffic is time-critical. The control center requests data from a substation which must be received within a specified time.

The difficulty when using SEAB-1F is that in order to operate several devices on one cable, FSK modems must be used. This requires very precise parameterization of the communication times (Tv, Tn, Tp). If just one of these times is off, errors will occur during data exchange, or the entire system will be so badly disrupted that communication will no longer be possible.

There are still many systems in use today where the control system uses the SEAB-1F protocol for communication with the substations. This technology has proved itself over decades.

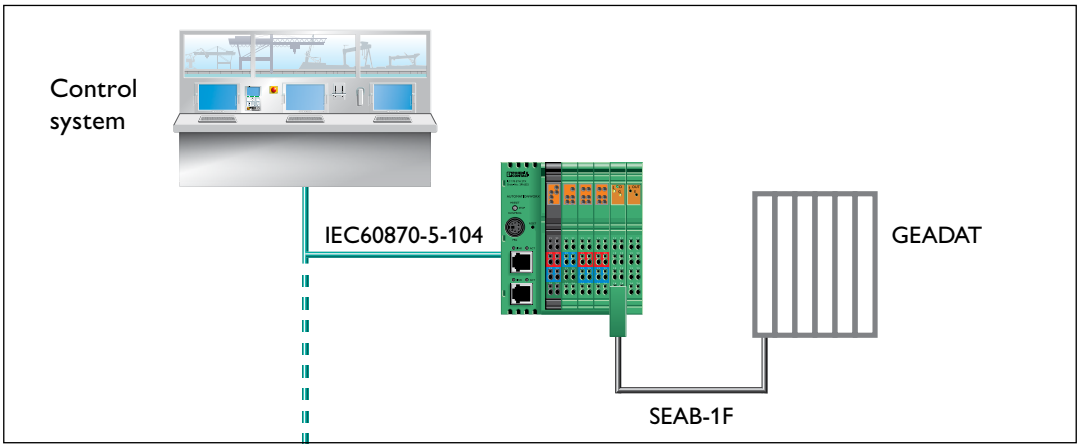

Figure 3

Connection of an SEAB-1F substation to IEC 60870-5-104

SMS

SMS stands for Short Message Service and is also used for communication between an external station and the control system – usually as an alarm message. The SMS can be used by any receiver: mobile phone, landline, fax or e-mail account. In addition, several programmable logic controllers can be networked together. The provision of an acknowledgment function ensures that the SMS reaches the receiver. Otherwise, the SMS is sent to another address.

Use of the SMS function in remote control technology

In addition to its function as a means of communication, the SMS service is also used to control and monitor technical devices and equipment. In applications where only alarm messages are to be transmitted or where control commands are sent relatively infrequently, the SMS service of the GSM network is a viable option for reasons of cost.

For example, industrial modems offer configurable warning and alarm inputs and are therefore ideal for monitoring small applications. An alarm SMS can be sent directly to a service technician's mobile phone, informing them directly of the type of error and its location. When dealing with an increased number of messages or control commands, GSM modems can also be connected to programmable logic controllers. This allows the I/O area of the PLC to be linked to text messages. It is also frequently the case that an SMS alarm message is not only intended to be sent to a mobile phone, but also to the alarm management of a control system. When a PLC is combined with a GSM modem, SMS messages can, for example, be received, decoded, and forwarded to a control system in a variety of ways.

Transmission paths

Wired transmission

When a proprietary data line is used for the remote control technology connection, e.g., in the power supply network of municipal works, it should be noted that if the copper cable is longer than 1.5 kilometers, the signals to be transmitted must be modulated in order to increase the range. Whether based on copper cables or fiber optics, this means that process information can be exchanged with a central control system over long distances.

Figure 4
Server room

Permanent line modem

Serial interfaces (RS-232, RS-485) are often available at the remote control substations and in the control system; these interfaces should be used to transmit standard protocols such as IEC 60870-5-101. Analog permanent line modems, which are specifically tailored to industrial requirements, are used to transmit this serial data. A digital signal is modulated to a carrier frequency in the high-frequency range by the transmitting modem; the original information is then retrieved by the receiving modem by means of demodulation. This technology has a maximum transmission speed of 33.6 kbps.

SHDSL modem

It is not usually possible to remotely program external stations that are connected in series. An Ethernet-capable network is required for this. An SHDSL modem can be used to make a serial communication network Ethernet-capable. Modems based on the newer DSL standard operate with higher carrier frequencies and larger bandwidths for the phone line than the models based on the older standard (narrowband). With industrial SHDSL permanent line modems, existing cables can also be used for modern Ethernet applications. Transmission speeds of up to 30 Mbps are possible via in-house cables. Automatic detection of the DSL data rate, as well as automatic adjustment to the Ethernet cable (1:1, crossed) and protocol transparency simplify startup considerably. In addition to point-to-point connection, a line structure (daisy chain) is also possible. With respect to transmission, there are modems for Ethernet, fieldbus or serial interfaces.

Fiber optics

Nowadays when new trunk lines are laid they are usually fiber optic (FO) lines. FO communication is immune to electromagnetic interference and, depending on the technology, allows several kilometers to be covered with a bandwidth in excess of 100 Mbps. Media converters can be used to forward Ethernet data as well as all common remote control or fieldbus data. Even in power distribution, external stations, e.g., in a substation, are usually connected to the central node point via fiber optics.

Non-wired connections (wireless)

If no cable is present, other means of communication must be found. Depending on the distance and the required bandwidth, it is also possible to use wireless connections. Depending on the requirements, one of the following three connections can be used:

Trusted Wireless

The application of Trusted Wireless was developed specifically for industrial use. As a result, large distances of up to 3 kilometers can be covered from one serial interface to another. For example, Trusted Wireless is used for communication between the control center and a pumping station. There should be a line of sight between the systems.

With visual contact, it is possible to transmit over a distance of up to 5.5 kilometers, e.g., when networking well fields. In the event of failure, a new communication path is selected and data transfer is still ensured. 255 devices can be connected per network. Multiple networks can be operated in parallel without any restrictions.

Figure 5
Wireless in practice

Bluetooth

Bluetooth is a standard for wireless transmission over short paths involving up to seven devices. The 2.4 GHz ISM frequency band is used, which does not require a license and is free of charge worldwide. It allows serial data to be transmitted even if another network is already active.

Bluetooth in use

Slip rings are frequently used to transmit measured values or process data from the scraper bridge of a wastewater treatment plant to the PLC. This technology is very high maintenance, resulting in high costs for the operator. Additional signals are often required, however there are no slip rings available for them. By using Bluetooth devices, maintenance costs can be saved and any number of signals can be transmitted over a distance of up to 400 meters with visual contact.

WLAN

WLAN is recommended in applications where, in addition to process-specific data, data from webcams or IP phones is also transmitted. Wireless Local Area Network describes a local wireless network with a data rate of up to 54 Mbps in the wireless application which can be used by a large number of devices. Wireless is particularly suitable for mobile monitoring, operation, and data acquisition as it can be easily integrated into IT networks.

Continuous connections in the mobile communication network

The mobile communication network or the Internet provide a solution for transmission over long distances and on a global scale. An almost constant connection can be achieved in this way.

GSM – 1G

Global System for Mobile Communications (GSM) is a standard for mobile communication networks that is primarily used for telephony and SMS transmission.

Text messages containing up to 160 characters can be sent in this way, e.g., for alarm generation or the transmission of status information. In the event of a power grid fault, a PLC sends an error message to the relevant user who can promptly rectify the error. Before this technology was used, the technician had to localize the fault on site before being able to remove it.

GPRS/EDGE – 2G

GPRS (General Packet Radio Service) supports transmission of up to 210,000 bps. This is possible because the data packets are split into many small packets that are reassembled again at the receiver. Since billing by providers is based on the volume of data and not the connection duration, a permanent modem connection is not a problem. Security plays an extremely important role here. The use of preconfigured modems with a fixed IP interface with point-to-point connections enables the constant connection of devices. In order to ensure secure data transmission, for a fee it is possible to apply for a closed network from the provider. A second option may be to use hardware solutions (security routers and GPRS routers) which protect data communication by means of VPN encryption, for example.

UMTS – 3G

3G UMTS (Universal Mobile Telecommunications System) is a third generation mobile communication standard with transmission speeds of up to 7.2 Mbps in the GSM network.

LTE – 4G

Due to the ever-increasing use of smartphones and tablets, as well as the networking of stand-alone machines and devices with the control center, increasing strain is being placed on the network. So that this high level of demand can also be accommodated in future, a new technology like LTE is required. LTE (Long Term Evolution) is also referred to as the fourth generation (4G) of mobile communication technology. The technology is the new standard in mobile communication and is the successor to UMTS (Universal Mobile Telecommunications System, 3G). This technology enables a high-speed connection of up to 300 Mbps and, unlike conventional standards, it supports different bandwidths. A peak data rate of up to 300 Mbps for download and 75 Mbps for uplink with 5-millisecond latency is theoretically possible. An important feature of LTE is its downward compatibility with older technologies. LTE retains the basic schema of UMTS, which means that the existing infrastructure can still be used. Missing components can simply be retrofitted.

DSL

DSL (Digital Subscriber Line) refers to a series of transmission standards for bit transmission. In the high data range, this standard can achieve a transmission speed of up to 500 Mbps using simple copper cables.

Selection matrix

Various communication options are available for data transmission in remote or wide-ranging networks and for monitoring machines all over the world. This overview helps users to select the optimum form of communication for the application.

		Range	Protocols	Technical parameters	Operating costs	Transmission speed	Ideal field of application
Mobile communication network systems	**GPRS/ EDGE/ 3G**	World-wide	IEC 60870-5-104 DNP3 ODP Modbus TCP	Mobile communication network coverage	Basic monthly charge and billing based on the transmitted data volume	Up to 7.2 Mbps	• Remote data acquisition
	SMS	World-wide	–	Mobile communication network coverage	Basic monthly charge and billing per SMS message	–	• Connection of Ethernet networks • Connection of substations • Worldwide alarm generation
	GSM	World-wide	IEC 60870-5-101 DNP3 Modbus RTU	Mobile communication network coverage	Basic monthly charge and usage-dependent billing based on time	Serial data up to 9600 bps	• Transmission of I/O information • Worldwide remote programming connection
Public telephone network	**Analog dial-up connec-tion**	World-wide	IEC 60870-5-101 DNP3 Modbus RTU	Analog telephone connection	Basic monthly charge and usage-dependent billing based on time	Serial data up to 33,600 bps	• Worldwide remote programming connection
	ADSL broad-band connec-tion	World-wide	IEC 60870-5-104 DNP3 ODP Modbus TCP	Analog telephone connection and DSL access	Basic monthly charge (usage/time-independent billing)	Annex A: Up to 25 Mbps downstream (from the Internet) Up to 3.5 Mbps upstream (to the Internet) Annex B: Up to 24 Mbps downstream (from the Internet) Up to 1 Mbps upstream (to the Internet)	• Remote data acquisition • Connection of substations • Connection of Ethernet networks
Wired systems	**SHDSL**	Up to 20 km	IEC 60870-5-104 DNP3 ODP Modbus TCP	Existing two/ four-wire cable for optimum range	• Installation and maintenance costs for two/ four-wire cable • No monthly costs	Ethernet data of up to 30 Mbps	• Remote data acquisition • Connection of substations • Connection of remote PROFIBUS devices • Connection of Ethernet networks • Connection of substations

		Range	Protocols	Technical parameters	Operating costs	Transmission speed	Ideal field of application
Wireless systems	**Trusted Wireless 2.0**	Up to 4 km	–	Line of sight for optimum range	Free of charge and no license required in the 2.4 GHz ISM band	• Serial data up to 115,200 bps • I/O data bidirectional and unidirectional	Wireless networking of sensors and actuators
	WLAN	Up to 2 km	IEC 60870-5-104 DNP3 ODP Modbus TCP	Line of sight for optimum range	Free of charge and no license required in the 2.4 GHz and 5 GHz ISM band	• WLAN data rates of up to 300 Mbps • Ethernet net data rates of up to 95 Mbps	• Protocol-transparent Ethernet communication with PLCs, I/O stations, PCs, etc. • Wireless network integration of remote installations
	Blue-tooth	Up to 300 m	IEC 60870-5-104 DNP3 ODP Modbus TCP	Line of sight for optimum range	Free of charge and no license required in the 2.4 GHz ISM band	Serial data up to 187,500 bps Ethernet Up to 1 Mbps net	• Wireless programming connection • Cable replacement for PROFIBUS, PROFINET, Modbus RTU/TCP, and serial TCP/IP data in the case of busy and mobile system parts

PHOENIX CONTACT

Phoenix Contact is a worldwide market leader for components, systems, and solutions in the fields of electrical engineering, electronics, and automation.

Our extensive manufacturing capability means that it is not just screws and plastic and metal parts that are produced in-house, but also highly automated assembly machines.
The product range consists of components and system solutions for energy supply including wind and solar energy, device manufacturing and machine building, as well as control cabinet manufacturing.

With a wide range of terminal blocks and special terminal blocks, PCB terminal blocks and connectors, cable connection technology, and installation accessories, we offer innovative components. Electronic interfaces and power supplies, automation systems based on Ethernet and wireless, safety solutions for people, machines, and data, surge protection systems, as well as software programs and tools provide comprehensive systems for installers and operators of systems as well as device manufacturers.

Markets within the automotive industry, renewable energy, and infrastructure are supported by means of consistent solution concepts, ranging from engineering and maintenance to training services, in line with specific needs. Product innovations and specific solutions for individual customer requirements are created in the development facilities at our sites in Germany, China, and the USA. Numerous patents emphasize the fact that many developments from Phoenix Contact are unique. Working closely with universities and scientific institutes, technologies of the future such as E-Mobility and environmental technologies are researched and transformed into marketable products, systems, and solutions.

PHOENIX CONTACT GmbH & Co. KG
32825 Blomberg, Germany
Phone: + 49 5235 3-00
Fax: + 49 5235 3-41200
phoenixcontact.net