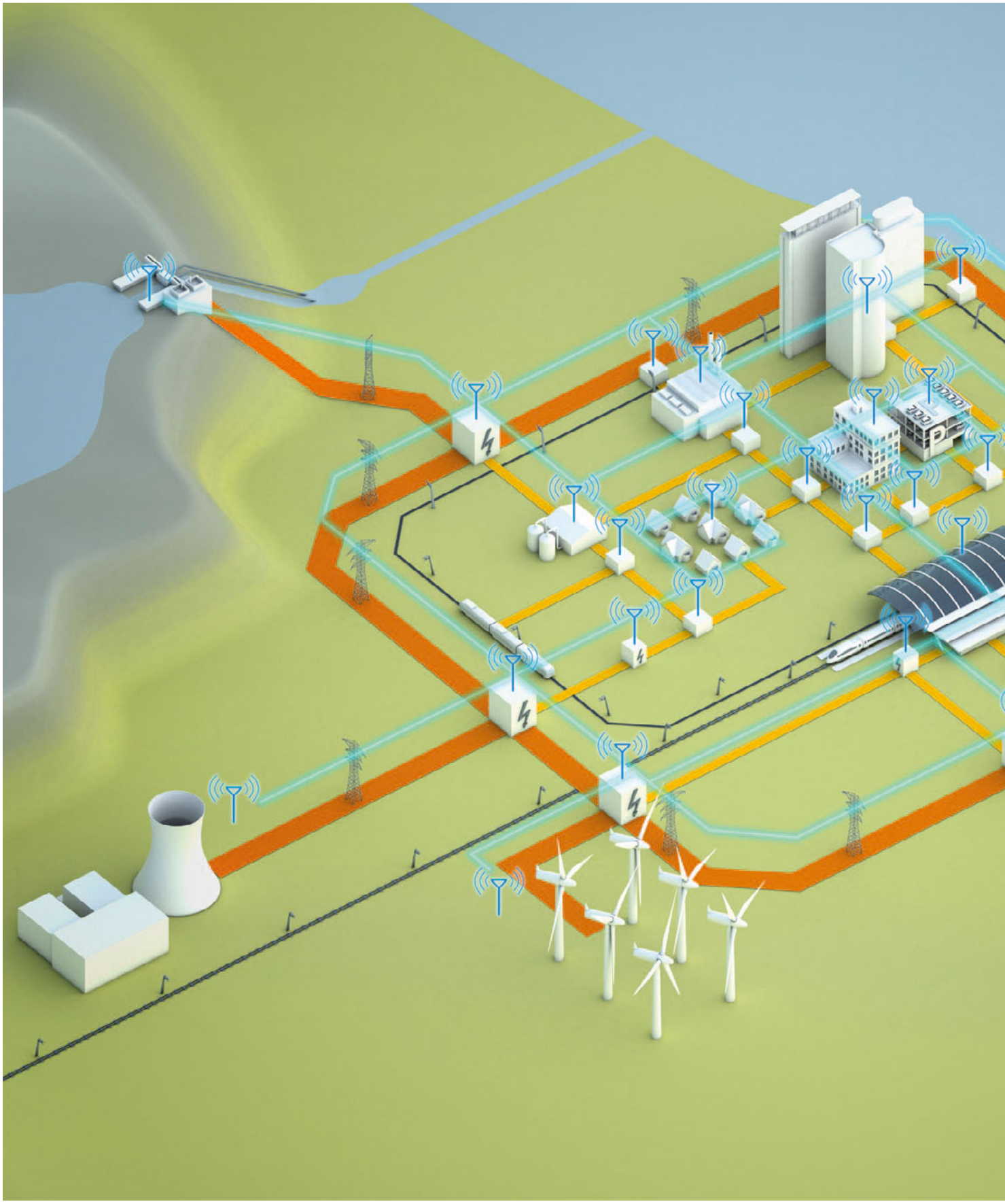
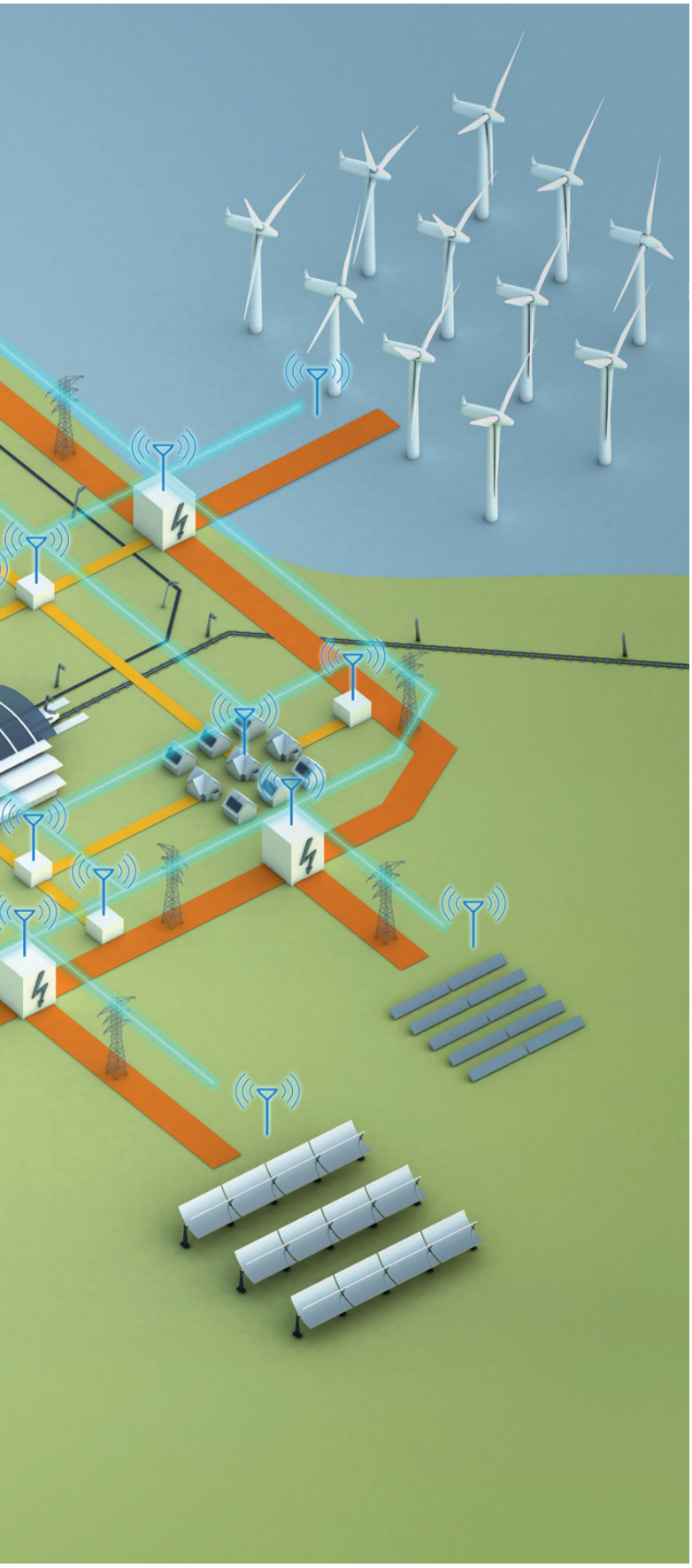


Communication Network Solutions for Smart Grids



8 Communication Network Solutions for Smart Grids

8.1 Introduction

A secure, reliable and economic power supply is closely linked to a fast, efficient and dependable communication infrastructure. Planning and implementation of communication networks require the same attention as the installation of the power supply systems themselves (fig. 8.1-1).

Telecommunication for utilities has a long history in the transmission level of the power supply system and Siemens was one of the first suppliers of communication systems for power utilities. Since the early 1930s Siemens has delivered Power Line Carrier equipment for high-voltage systems. In today's transmission systems, almost all substations are monitored and controlled online by Energy Management Systems (EMS). The main transmission lines are usually equipped with fiber-optic cables, mostly integrated in the earth (ground) wires (OPGW: Optical Ground Wire) and the substations are accessible via broadband communication systems. The two proven and optimal communication technologies for application-specific needs are Synchronous Digital Hierarchy (SDH) and Ethernet. Fiber-optic cables are used whenever it is cost-efficient. In the remote ends of the power transmission system, however, where the installation of fiber-optic cables or wireless solutions is not economical, substations are connected via digital high-voltage power line carrier systems.

The situation in the distribution grid is quite different. Whereas subtransmission and primary substations are equipped with digital communication as well, the communication infrastructure at lower distribution levels is very weak. In most countries, less than 10 % of transformer substations and ring-main units (RMU) are monitored and controlled from remote.

The rapid increase in distributed energy resources today is impairing the power quality of the distribution network. That is

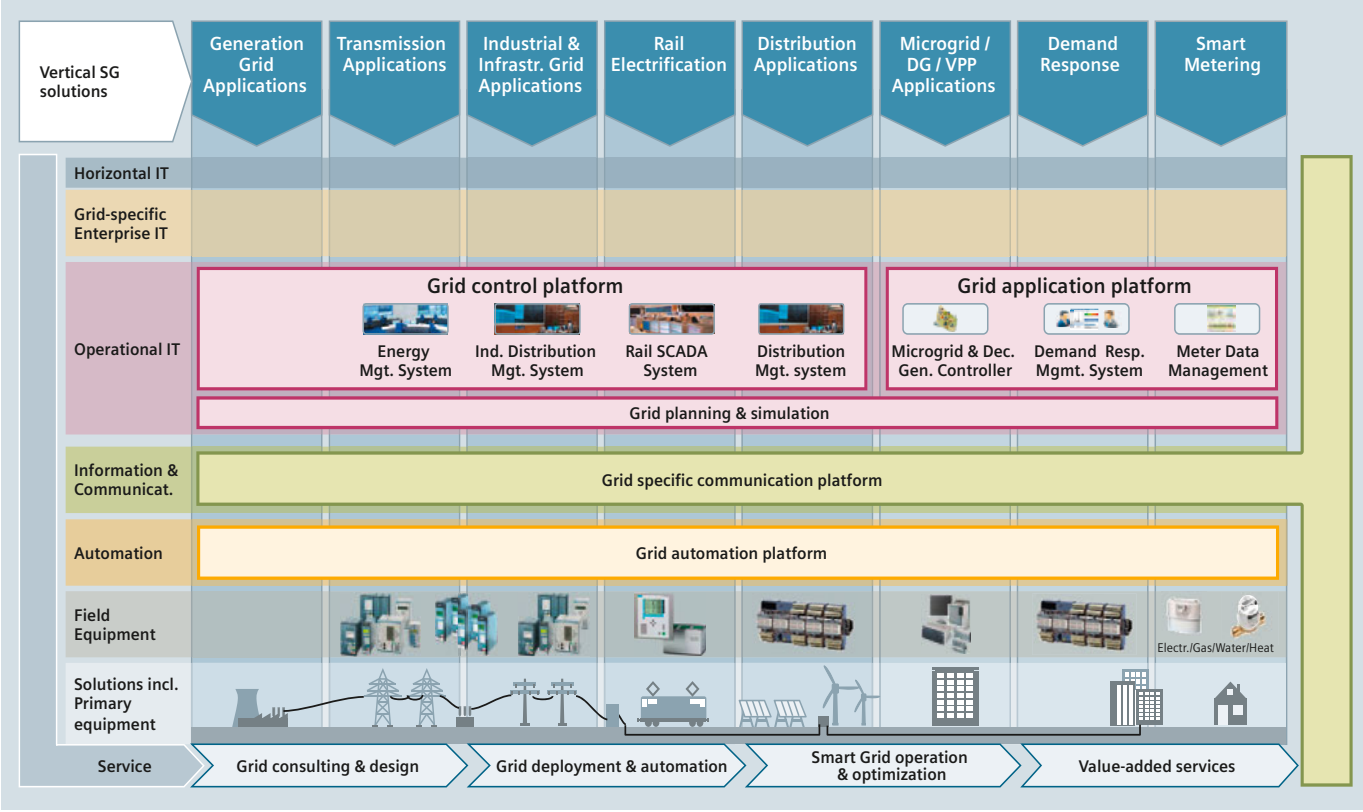


Fig. 8.1-1: **Siemens offers complete communication network solutions to build a Smart Grid for power utilities**

why system operators need to be able to respond quickly in critical situations. A prerequisite for this is the integration of the key ring-main units as well as the volatile decentralized wind and solar generation into the energy management system, and thus into the communication network of the power utilities. Because the local environment differs widely, it is crucial that the right mix of the various communication technologies is deployed. This mix will need to be exactly tailored to the utilities' needs and the availability of the necessary infrastructure and resources (e.g., availability of fiber-optic cables, frequency spectrum for wireless technologies, or quality and length of the power cables for broadband power line carrier).

In the consumer access area, the communication needs are rising rapidly as well. The following Smart Grid applications request a bidirectional communication infrastructure down to consumer premises.

- Exchange of conventional meters with smart meters, which provide bidirectional communications connections between the consumer and energy applications (e.g., meter data management, marketplace, etc.)
- Management of consumers' energy consumption, using price signals as a response to the steadily changing energy supply of large distributed producers
- If a large number of small energy resources are involved, the power quality of the low-voltage system must be monitored, because the flow of current can change directions when feed conditions are favorable

The selection of a communication solution depends on the customer's requirements. If only meter data and price signals are to be transmitted, narrowband systems such as narrowband power line carriers or GPRS modems are sufficient. For smart homes in which power generation and controllable loads (e.g., appliances) or e-car charging stations are to be managed, broadband communication systems such as fiber-optic cables, broadband power line carriers or wireless solutions are necessary.

For these complex communication requirements, Siemens offers tailored ruggedized communication network solutions for fiber optic, power line or wireless infrastructures, based on the standards of the Energy Industry. Naturally, this also includes a full range of services, from communication analysis to the operation of the entire solution (fig. 8.1-2).

For further reading please visit:

www.energy.siemens.com/hq/en/automation/power-transmission-distribution/network-communication

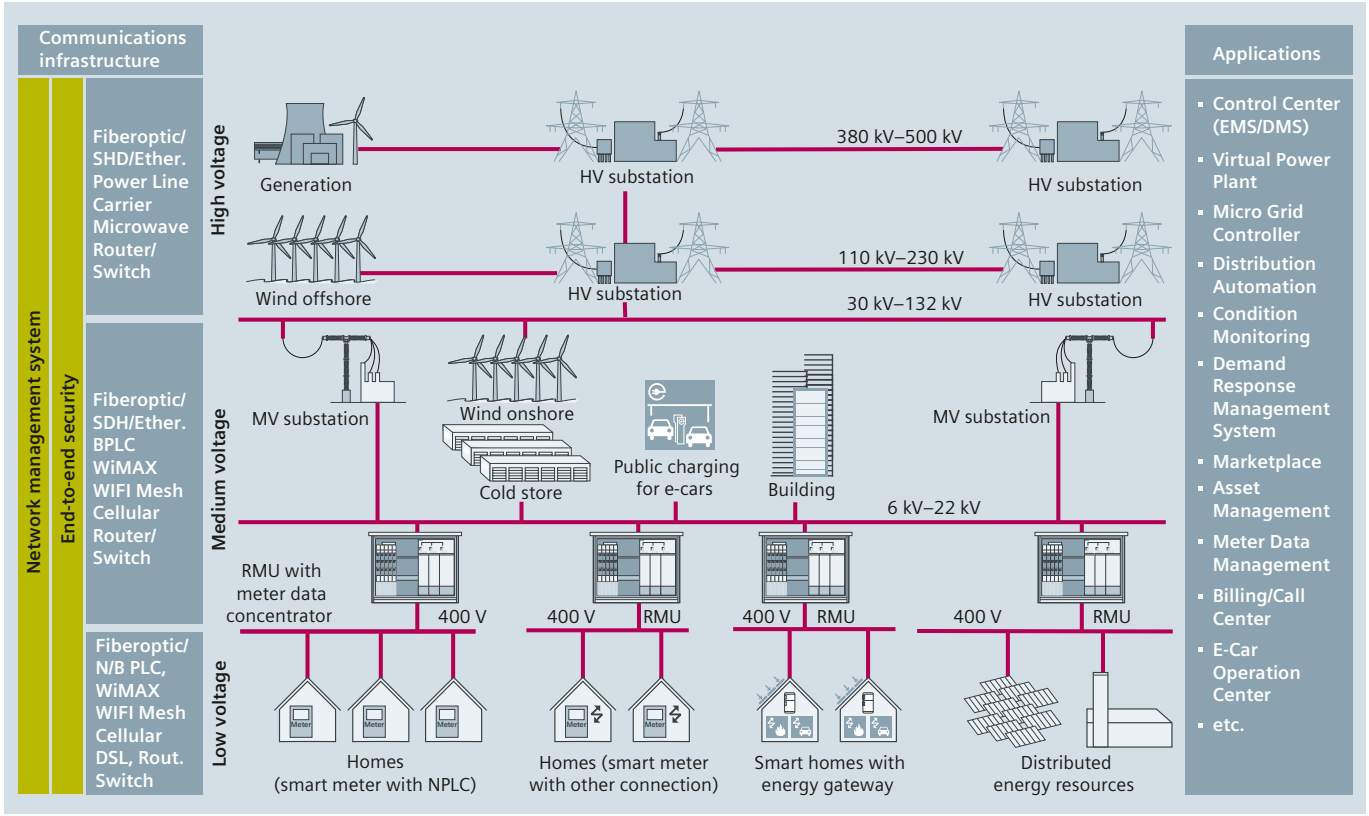


Fig. 8.1-2: **Communication network solutions for Smart Grids**

8.2 Communication Network Solutions for Transmission Grids (Communication Backbone)

8.2.1 Synchronous Digital Hierarchy (SDH)/Ethernet Solutions

For communications at transmission and subtransmission levels, Siemens offers the latest generation of SDH (Synchronous Digital Hierarchy) equipment, commonly referred to as NG (Next Generation) SDH (fig. 8.2-1).

NG SDH technology combines a number of benefits that make it well-suited to the needs of energy utilities. Among those benefits are high availability, comprehensive manageability and monitoring features, and last but not least SDH's unique ability to seamlessly support both legacy applications and new, primarily packet-based emerging standards. Ethernet-over-SDH provides the capacity to transport packet-based traffic over the SDH backbone with high reliability and low latencies. As a result, Ethernet-over-SDH is the solution of choice for enabling IEC61850 across the entire communication backbone.

State-of-the-art NG SDH systems are highly integrated, providing all of the above-mentioned capabilities in a single device. In order to address the varying needs and requirements of the energy utilities, Siemens offers a wide range of products, from a single-board CPE to a multiservice platform for PDH (Plesiochronous Digital Hierarchy), SDH, WDM (Wavelength Division Multiplexing), and Ethernet.

Benefits at a glance

- High availability
- Very short delay times in protection signal transmission
- For both legacy and packet-based applications/systems
- Supports IEC 61850 standard
- Full-spectrum network management system

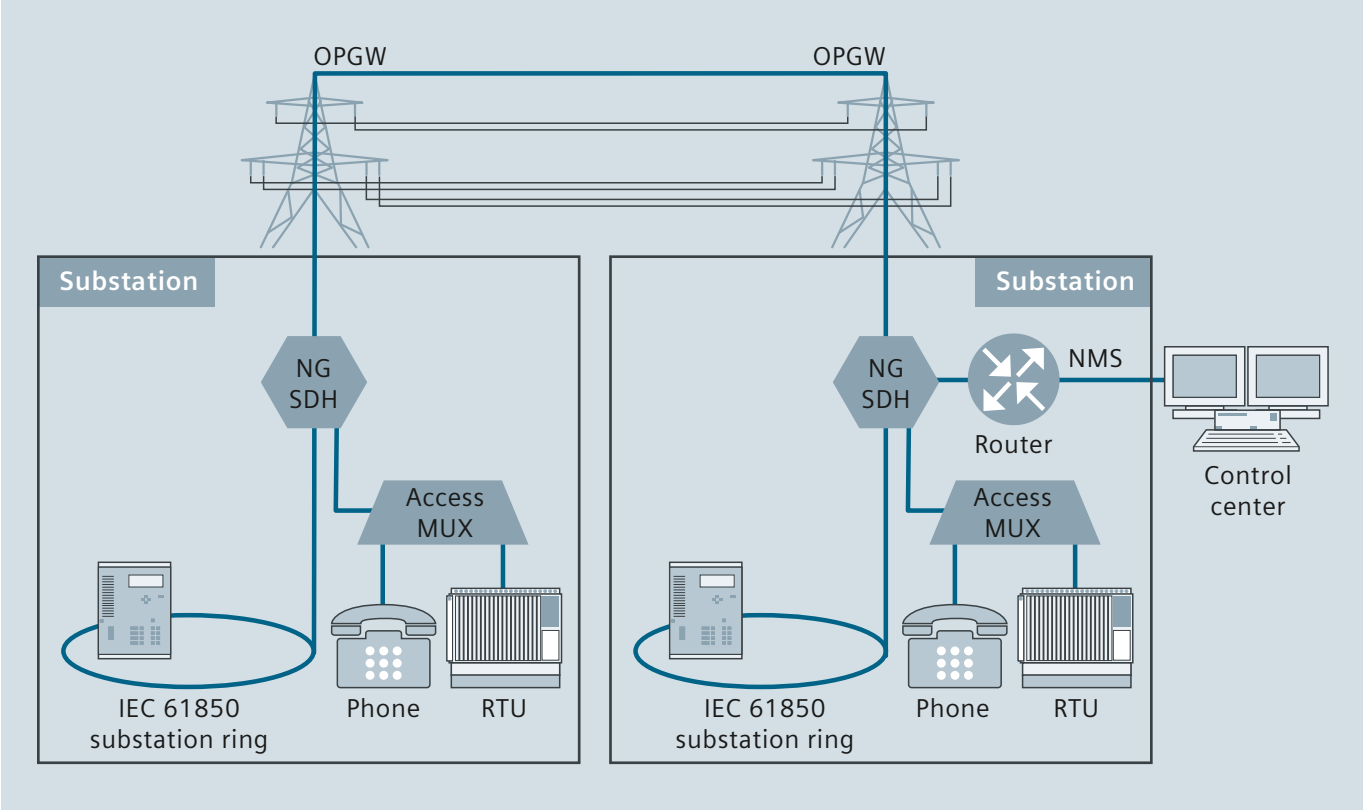


Fig. 8.2-1: **Typical Next Generation SDH solution for transmission grids**

8.2.2 Access Multiplexer

Today there is still a need to operate a number of different conventional communication interfaces in one substation (e.g., a/b phone, ISDN, V.24, X.21, etc.) and this will also apply in the near future. For this purpose, access multiplexers are used to bundle these communication signals and pass them on to the backbone system.

An access multiplexer can be employed to create flexible networks which can react rapidly to changes in network requirements. The modular design enables channel units to be combined as required for telephone, data and ISDN signal transmission. The multiplexer allows free assignment of user interfaces to the channels in the 2-Mbit/s signal and rapid configuration. Fig. 8.2-2 shows an overview of the interfaces provided by an typical access multiplexer.

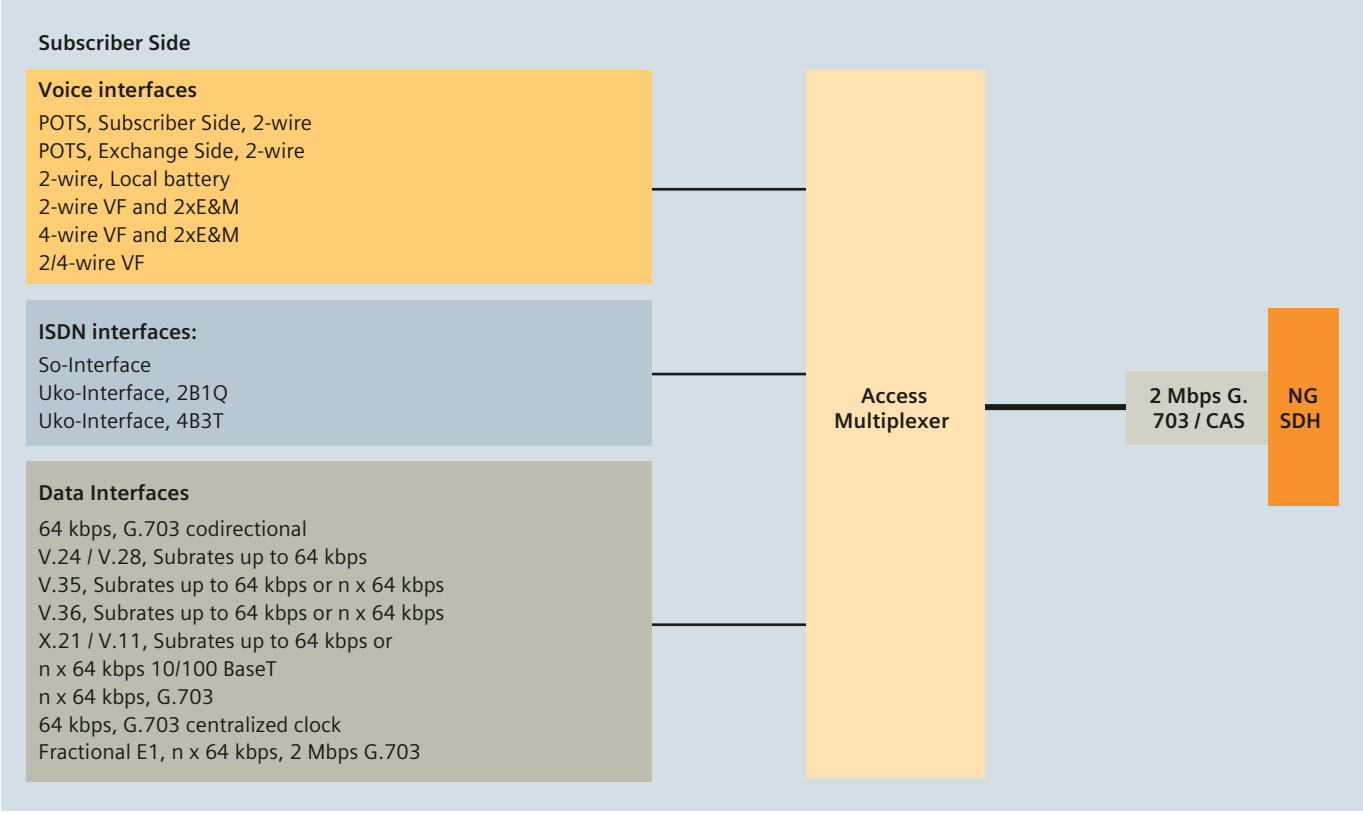


Fig. 8.2-2: **Typical interfaces of an access multiplexer**

8.2.3 PowerLink – Power Line Carrier for High-Voltage Lines

The digital power line carrier system PowerLink from Siemens uses the high-voltage line between substations as a communication channel for data, protection signals and voice transmission (table 8.2-1). This technology, which has been tried and tested over decades, and adapted to the latest standards, has two main application areas:

- As a communication link between substations where a fiber-optic connection does not exist or would not be economically viable
- As backup system for transmitting the protection signals, in parallel to a fiber-optic link

Fig. 8.2-3 shows the typical connection of the PowerLink system to the high-voltage line via the coupling unit AKE 100, coupling capacitor.

Flexibility – the most important aspect of PowerLink
Versatility is one of the great strengths of the PowerLink system. PowerLink can be matched flexibly to your infrastructure (table 8.2-2).

Multi-service device
PowerLink offers the necessary flexibility for transmitting every service the customer might want in the available band. All services can be combined in any way within the available bandwidth/bit rate framework.

Bridge to IP
IP functionality is best suited for the migration from TDM to packet-switched networks. PowerLink offers electrical and optical Ethernet interfaces, including an integrated L2 switch, extending the IP network to remote substations with a bit rate up to 320 kbps.

Optimal data throughput under changing environmental conditions
PowerLink adapts the data rate to changes in ambient conditions, thus guaranteeing maximum data throughput. Thanks to PowerLink's integral prioritization function, which can be configured for each channel, routing of the most important channels is assured even in poor weather conditions.

Variable transmission power
The transmission power can be configured via software in two ranges (20 – 50 W or 40 – 100 W), based on the requirements of the transmission path. This makes it easy to comply with national regulations and to enable optimized frequency planning.

Maximum efficiency:
The integrated, versatile multiplexer (vMUX)
A large number of conventional communication interfaces today (e.g., a/b telephone, V.24, X.21, etc.) and in the foreseeable future must be operated in a switching station. For this purpose, PowerLink uses an integrated versatile multiplexer that

Application
Transmission of protection signals, telecontrolling information, data and voice via HV transmission lines
Advantages
Cost-effective for small to medium data volumes over long distances
Processes analog and digital signals
Adjustable transmission power
Variable bandwidth
Integrated TCP/IP interface
Voice compression
Versatile multiplexer
Integrated teleprotection systems
Cross-functional management system for all integrated services
Can be used effectively in combination withbroadband technologies for optimal availability

Table 8.2-1: **Progressive PLC technique with PowerLink**

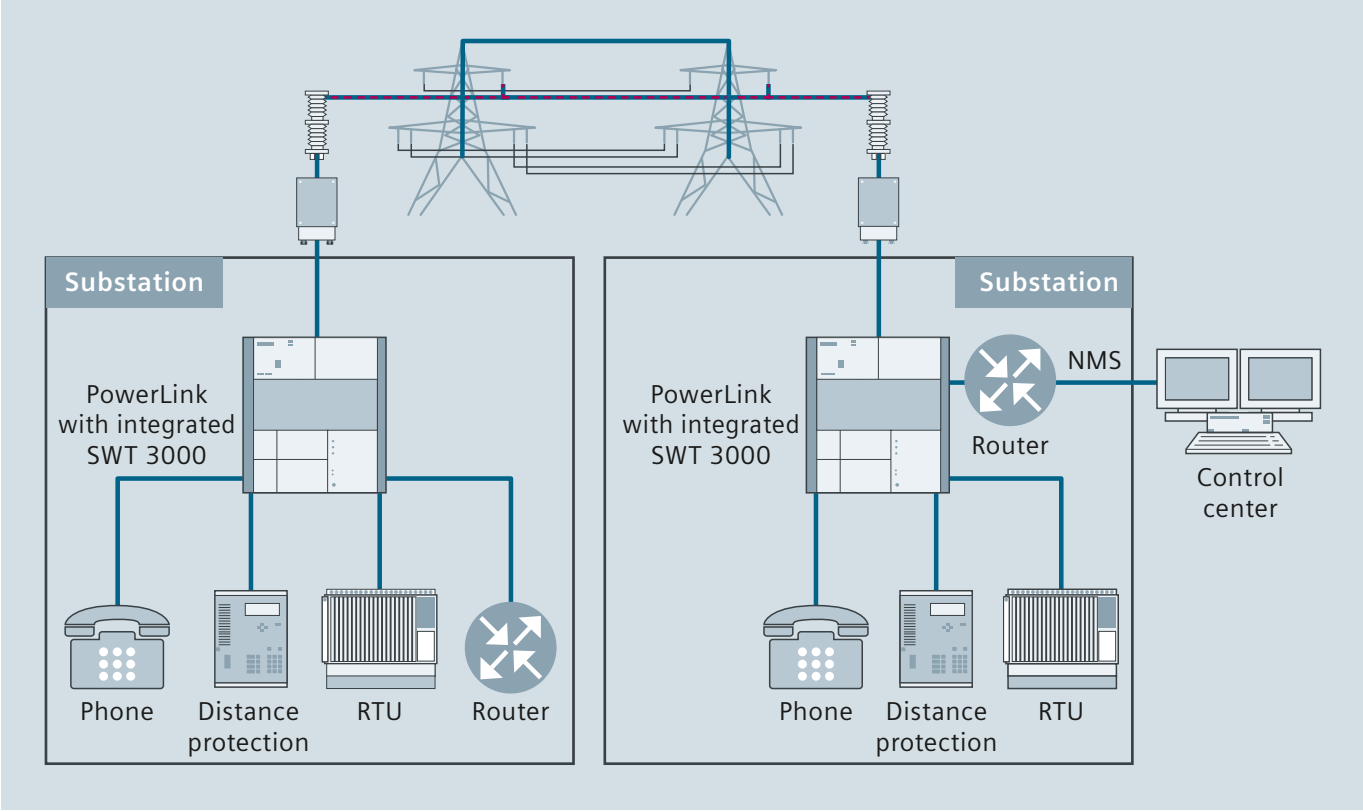


Fig. 8.2-3: **PowerLink high-voltage line communication**

bundles these communication forms together and transmits them by PLC. The vMUX is a statistical multiplexer with priority control. Asynchronous data channels can be transmitted in "guaranteed" or "best effort" modes, to guarantee optimum utilization of available transmission capacity. The priority control ensures reliable transmission of the most important asynchronous and synchronous data channels and voice channels even under poor transmission conditions. Naturally, the vMUX is integrated in the management system of PowerLink, and is perfectly equipped for the power line communication requirements of the future with extended options for transmitting digital voice and data signals.

Voice compression
Voice compression is indispensable for the efficient utilization of networks. Naturally, quality must not suffer, which is why PowerLink offers comprehensive options for adapting the data rate to individual requirements. PowerLink offers different compression stages between 5.3 and 8 kbit/s. To prevent any impairment of voice quality, the compressed voice band is routed transparently to PowerLink stations connected in line, without any further compression or decompression.

Protection signal transmission system SWT 3000
A maximum of two independent SWT 3000 systems can be integrated into each PowerLink. Every integrated teleprotection system can transmit up to four protection commands. The command interface type for distance protection devices can be either standard binary or compliant with IEC 61850. Even a combination of both command interface types is supported. For highest availability, an alternate transmission path via a digital communication link can be connected. SWT 3000 systems are also fully integrated into the user interface of the PowerLink administration tool.

One administration system for all applications
PowerLink not only simplifies your communications, but also makes communications cost-efficient. The PowerSys software administers all integrated applications of PowerLink under a standard user interface. This ensures higher operating security while cutting training times and costs to the minimum.

Integration of PowerLink in network management systems via SNMP
PowerLink systems can also be integrated in higher level management systems via the IP access by means of the SNMP protocol (Simple Network Management Protocol). System and network state data are transferred, for example, to an alarm, inventory or performance management system.

Features	Digital PLC system	Analog PLC system
Universally applicable in analog, digital, or mixed operation	■	■
Frequency range 24 kHz–1,000 kHz	■	■
Bandwidth selectable 2–32 kHz	■	■
Data rate up to 320 kbit/s at 32 kHz	■	
Transmission power 20/50/100 W, fine adjustment through software	■	■
Operation with or without frequency band spacing with automatic cross talk canceller	■	■
Digital interface		
Synchronous X.21 (max. 2 channels)	■	
Asynchronous RS 232 (max. 8 channels)	■	
TCP/IP (2 x electrical, 1 x optical)	■	
E1 (2 Mbps) for voice compression	■	
G703.1 (64 kbps)	■	
Analog interface		
VF (VFM, VFO, VFS), max. 8 channels for voice, data, and protection signal	■	■
Asynchronous RS232 (max. 4) via FSK		■
Miscellaneous		
Adaptive dynamic data rate adjustment	■	
TCP/IP layer 2 bridge	■	
Integrated versatile multiplexer for voice and data	■	
Max. 5 compressed voice channels via VF interface	■	
Max. 8 voice channels via E1 interface	■	
StationLink bus for the cross-connection of max. 4 PLC transmission routes (compressed voice and data without voice compression on repeater)	■	
Reverse FSK analog RTU/modem data via dPLC (2 x)	■	
Protection signal transmission system SWT 3000		
Integration of two devices	■	■
Remote operation via cable or fiber-optic cable identical to the integrated version	■	■
Single-purpose or multipurpose/alternate multipurpose mode	■	■
Element manager, based on a graphical user interface for the control and monitoring of PLC and teleprotection systems	■	■
Command interface binary and in accordance with IEC 61850	■	■
Remote access to PowerLink		
Via TCP/IP connection	■	■
Via in-band service channel	■	■
SNMP compatibility for integrating NMS	■	■
Event memory with time stamp	■	■
Simple feature upgrade through software	■	■

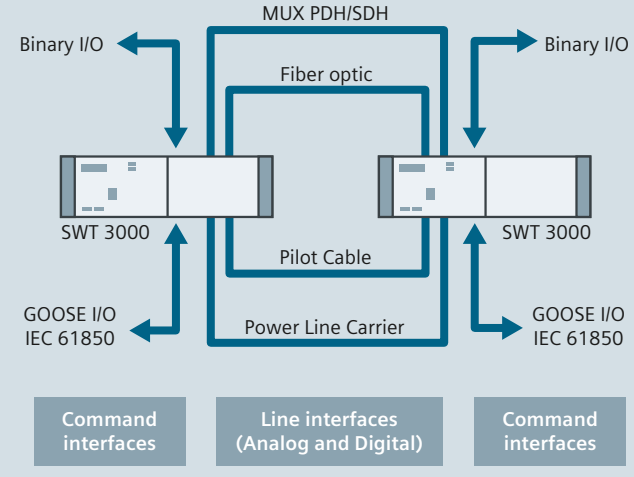
Table 8.2-2: **Overview of features**

8.2.4 SWT 3000 – Teleprotection for High-Voltage Lines

The SWT 3000 is an highly secure and reliable system for transmitting time-critical distance protection commands via analog and digital transmission channels (fig. 8.2-4). This enables faults in the high-voltage grid to be isolated selectively as quickly as possible. The SWT 3000 system can be integrated in the PowerLink system or be operated as a stand-alone system.

Security, reliability and speed of protection signal transmission is one of the central factors in the operation of high-voltage grids. For maximum operating reliability, SWT 3000 can be configured with two separately fed power supplies. If possible, protection signals should be transmitted over two alternative communication paths to safeguard maximum transmission security. Fig. 8.2-5 shows the different analog and digital transmission paths between SWT 3000 systems.

The SWT 3000 also demonstrates its high degree of flexibility when existing substations are migrated to protection devices via the IEC 61850 communication standard. The SWT 3000 has all necessary command interfaces – both as binary interfaces and as GOOSE. This always keeps investment costs economically manageable, because the substations can be updated step by step for a new network age.



Application
Transmission of protection signals to quickly identify, isolate and resolve problems in the transmission network of a utility
Advantages
Keeps downtimes to an absolute minimum
Supports IEC 61850 interfaces as well as conventional binary interfaces
Flexible integration into various customer communication networks
Path protection via two different transmission routes for increased reliability

Fig. 8.2-4: **SWT 3000 teleprotection system – overview**

1 2 Pilot cable connections
For operation via pilot cable, two SWT 3000 devices can be linked directly through the analog interfaces (CLE).

3 Power line carrier connections
The analog link (CLE) between two SWT 3000 devices can also be a PLC link. Depending on device configuration, SWT 3000 can be used with PowerLink in alternate multipurpose, simultaneous multipurpose, or single-purpose mode.

4 12 Fiber-optic connections between SWT 3000 and PowerLink
A short-distance connection between an SWT 3000 and Siemens's PowerLink PLC terminal can be realized via an integrated fiber-optic modem. In this case, an SWT 3000 stand-alone system provides the same advanced functionality as the version integrated into PowerLink. Each PowerLink can be connected to two SWT 3000 devices via optical fibers.

5 6 7 11 SWT 3000 digital connections
The digital interface (DLE) permits protection signals to be transmitted over a PDH or SDH network.

6 9 11 12 14 Alternative transmission routes
SWT 3000 enables transmission of protection signals via two different routes. Both routes are constantly transmitting. In the event that one route fails, the second route still bears the signal.

7 8 9 Direct fiber-optic connection without repeater
SWT 3000 protection signaling incorporates an internal fiber-optic modem for long-distance transmission. The maximum distance between two SWT 3000 devices is 150 kilometers.

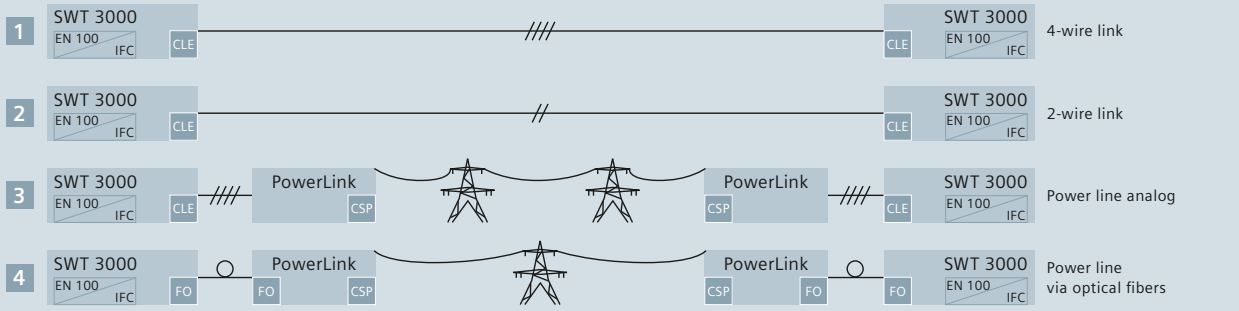
9 10 12 Fiber-optic connection between SWT 3000 and a multiplexer
A short-distance connection of up to two kilometers between SWT 3000 and a multiplexer can be realized via the integrated fiber-optic modem according to IEEE C37.94. Alternately, the multiplexer is connected via FOBox, converting the optical signal to an electrical signal in case the MUX does not support C37.94.

13 14 SWT 3000 integration into the PowerLink – PLC system
The SWT 3000 system can be integrated into the PowerLink equipment. Either the analog interface or a combination of the analog and the digital interfaces can be used.

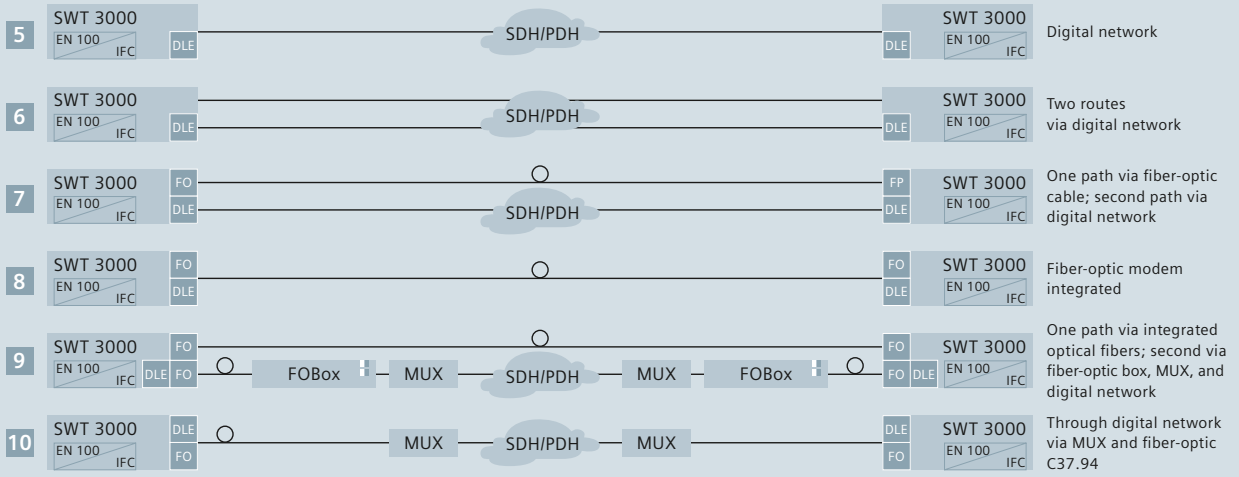
Fig. 8.2-5: **SWT 3000 transmission paths**

PowerLink	Power Line Carrier System	EN 100	Interface IEC 61850
IFC	Interface Command Binary	SDH	Synchronous Digital Hierarchy
DLE	Digital Line Equipment	FOBox	Fiber-Optic Box
CLE	Copper Line Equipment	FO	Fiber-Optic Module
PDH	Plesiochronous Digital Hierarchy	MUX	Multiplexer

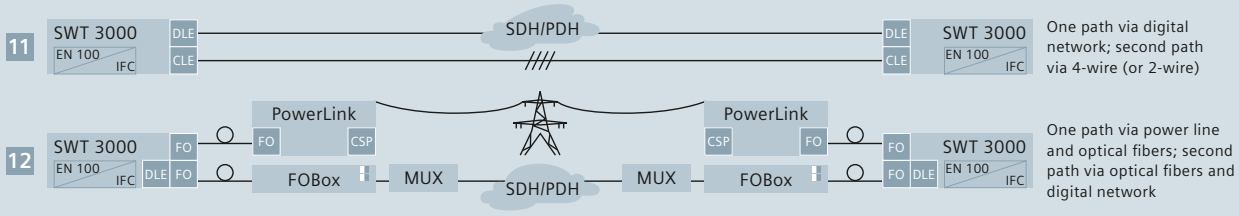
Analog transmission



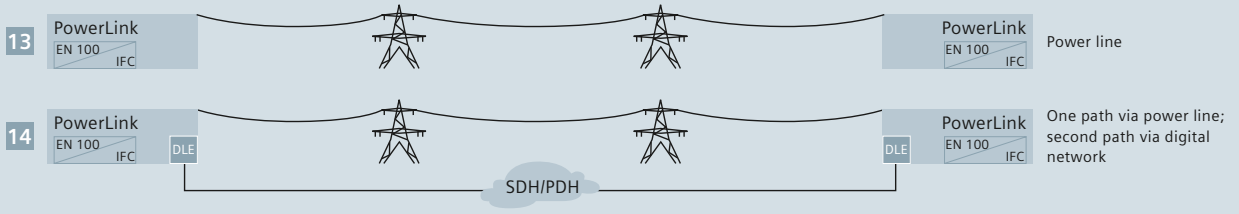
Digital transmission



Analog & digital transmission



Integrated into PowerLink



8

8.2.5 Coupling Unit AKE 100

The PLC terminals are connected to the power line via coupling capacitors, or via capacitive voltage transformers and the coupling unit. In order to prevent the PLC currents from flowing to the power switchgear or in other undesired directions (e.g., tapped lines), traps (coils) are used, which are rated for the operating and short-circuit currents of the power installation and involve no significant loss for the power distribution system.

The AKE 100 coupling unit from Siemens described here, together with a high-voltage coupling capacitor, forms a high-pass filter for the required carrier frequencies, whose lower cut-off frequency is determined by the rating of the coupling capacitor and the chosen matching ratio.

The AKE 100 coupling unit is supplied in four versions and is used for:
- Phase-to-earth coupling to overhead power lines
- Phase-to-phase coupling to overhead power lines
- Phase-to-earth coupling to power cables
- Phase-to-phase coupling to power cables
- Intersystem coupling with two phase-to-earth coupling units

The coupling units for phase-to-phase coupling are adaptable for use as phase to-earth coupling units. The versions for phase-to-earth coupling can be retrofitted for phase-to-phase coupling, or can as well be used for intersystem coupling.

8.2.6 Voice Communication with PowerLink

The TCP/IP protocol is gaining increasing acceptance in the voice communication area. However, considerably higher bandwidth requirements must be taken into account in network planning with VoIP compared with analog voice links. Table 8.2-3 shows the bandwidth requirement for a voice link via TCP/IP as a function of the codec used for voice compression.

In the office area today, the LAN infrastructure is usually sufficiently generously dimensioned to make VoIP communication possible without any restrictions. The situation is distinctly different if it is necessary to connect distant substations to the utility's voice network. If these locations are not integrated in the corporate backbone network, Power Line Carrier connections must be installed. Fig. 8.2-6 shows the basic alternatives for voice communication via PowerLink.

Codec	Net bit rate	Gross bit rate
G.711	64 kbit/s	87.2 kbit/s
G.726	32 kbit/s	55.2 kbit/s
G.728	16 kbit/s	31.5 kbit/s
G.729	8 kbit/s	31.2 kbit/s
G.723.1	5.3 kbit/s	20.8 kbit/s

Table 8.2-3: **Bandwidth requirement for VoIP**

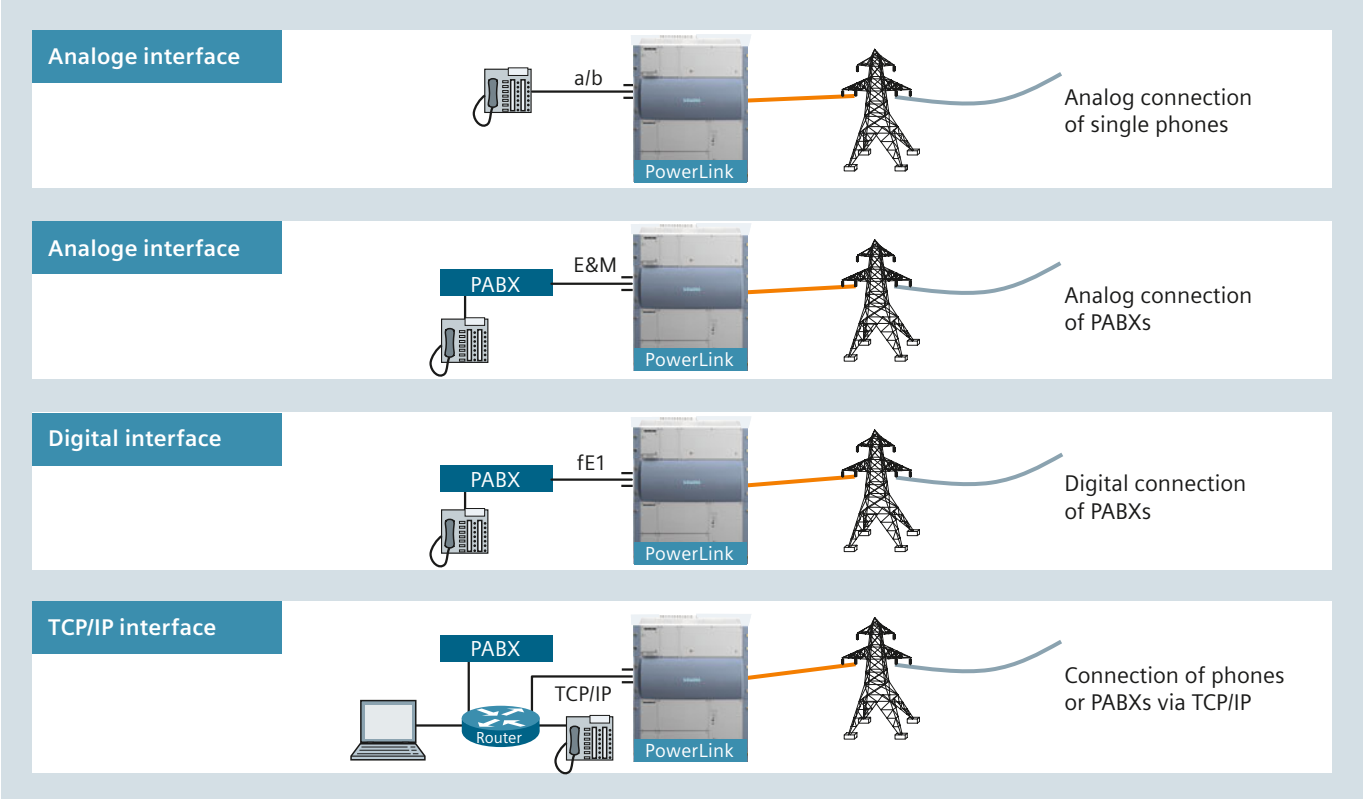


Fig. 8.2-6: **Basic options of voice communication via PowerLink**

Analog connection
The telephone system is connected to the PowerLink via the analog E&M interface. A telephone system or an individual analog telephone can also participate in a PowerLink system at a different location. The bandwidth requirement can be reduced to about 6 kbit/s (including overhead) per voice link by means of voice compression in the PowerLink.

Digital connection
With digital connection, the telephone system is connected to PowerLink via the digital E1 interface. Because of the restricted bandwidth, up to 8 of the 30 voice channels (Fractional E1) can be used. This alternative is only suitable for communication between telephone systems. Individual telephones must be connected locally to the particular telephone system. The bandwidth requirement is made up of the user data per voice channel (e.g., 5.3 kbit/s) and the D-channel overhead for the entire E1 link (approximately 2.4 kbits/s), (i.e., for a voice channel less than 10 kbit/s).

In the case of series connected locations with both analog and digital connection, multiple compression/decompression of the voice channel is prevented by the unique PowerLink function "StationLink".

TCP/IP connection
The telephone system, voice terminals and the PowerLink system are connected directly to the TCP/IP network. Voice communication is conducted directly between the terminals. Only control information is transmitted to the telephone system. Use of the TCP/IP protocol results in a broadband requirement per voice channel of at least 21 kbit/s (5.3 kbit/s voice plus TCP/IP overhead).

Telephone systems
To ensure the operation along high-voltage transmission lines or pipelines and power plants, voice communication is an important part of the entire solution. The Siemens Enterprise Communication portfolio addresses all the different requirements of utilities, and can be deployed in various scenarios.

The limited bandwidth availability of Power Line Carrier systems in the high-voltage area will ensure an important role for conventional telephone systems (e.g., HiPath 4000) with analog interfaces in this segment in the future as well (fig. 8.2-7).

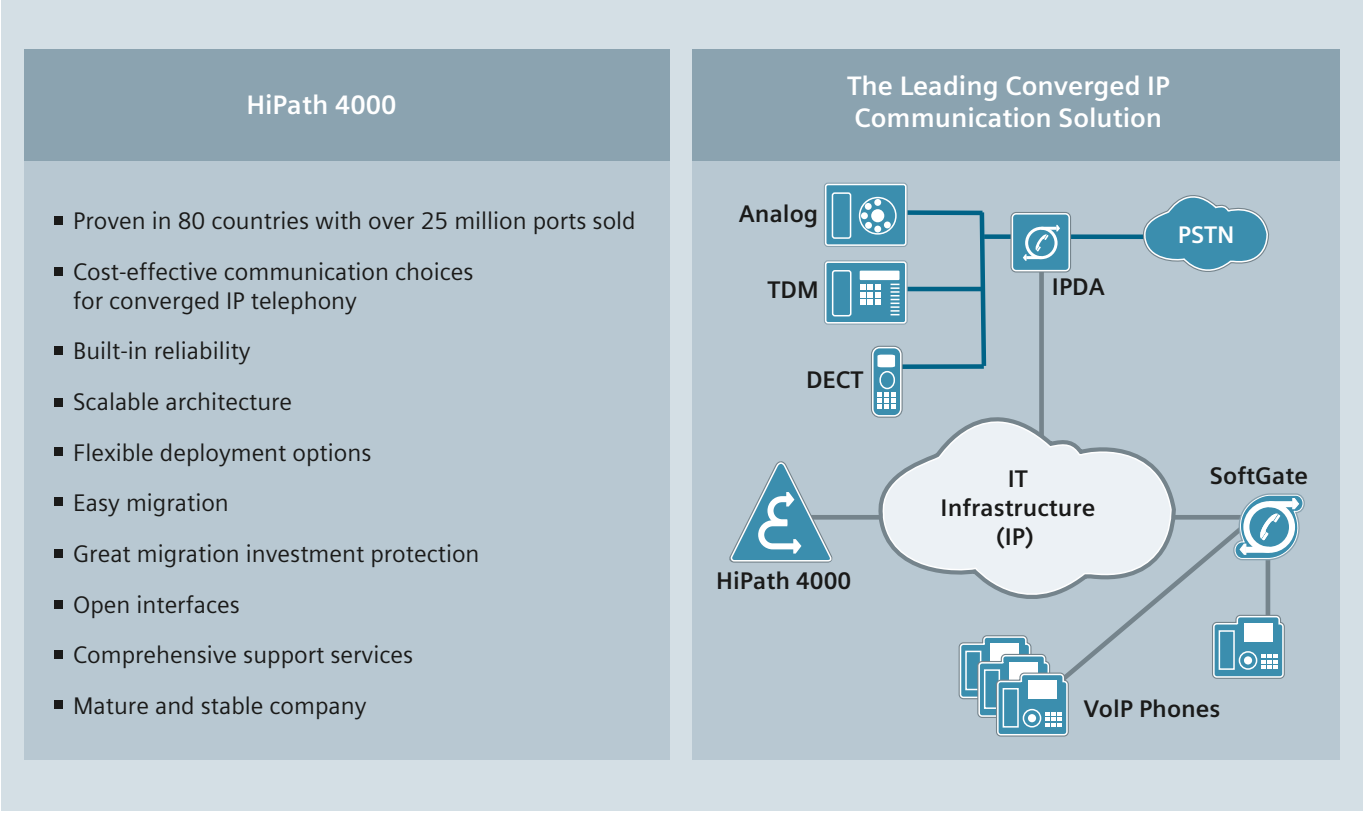


Fig. 8.2-7: **HiPath 4000 overview**

8.2.7 Live Line Installation of OPGW (Optical Ground Wire)

The transformation of power supply systems into Smart Grids is closely related to the growing communication requirements (bandwidth demand) in the transmission and distribution areas.

To allow for quick data transfers between large substations in the transmission system, fiber-optic cables are being used to replace ground wires on high-voltage lines (OPGW: Optical Ground Wire).

As a result of the growing and often unpredictable feeding of energy into the power supply system by decentralized generators, it is becoming increasingly difficult and sometimes impossible for transmission companies to shut off line segments for installation measures to improve the communication infrastructure.

The Siemens Live Line Installation process makes it possible to perform such installations or repairs on energized power lines. This installation concept was developed in a joint effort by Siemens and a team at Dresden University in Germany.

The Siemens Live Line Installation process can be used for the following purposes:

- To replace the ground wire with an optical ground wire, in order to provide broadband communication even to smaller substations
- Additional installation of a second optical ground wire below the top of the tower, on especially communication-intensive segments
- To replace an obsolete or defective optical ground wire.

Safety of both personnel and equipment is the utmost priority: Live Line Installation supplies a new earthing concept as well as pulling machines and brakes on the ground (fig. 8.2-8).

With live line installation, optical ground wires can be installed either directly at the top of the tower or below the top between the power-carrying lines (fig. 8.2-9).

Special security precautions are taken when high-risk areas (highways, bodies of water, railways, etc.) are to be crossed when installing the optical ground wires below the top of the tower.

During live line installation, the existing ground wire serves as a messenger and carries all the installation equipment, such as pulleys, the full dielectric prepulling rope and the OPGW itself. Thus, the new hybrid cable can be pulled from tower to tower across the entire delivery length. In high-voltage lines, the usual delivery length is approximately 4 km.

Siemens is the most experienced and most successful supplier of live line installation of optical ground wires on high-voltage lines worldwide, and conducted the first live line installation already in the year 2000.

Fig. 8.2-8: **Live line installation of optical ground wire**

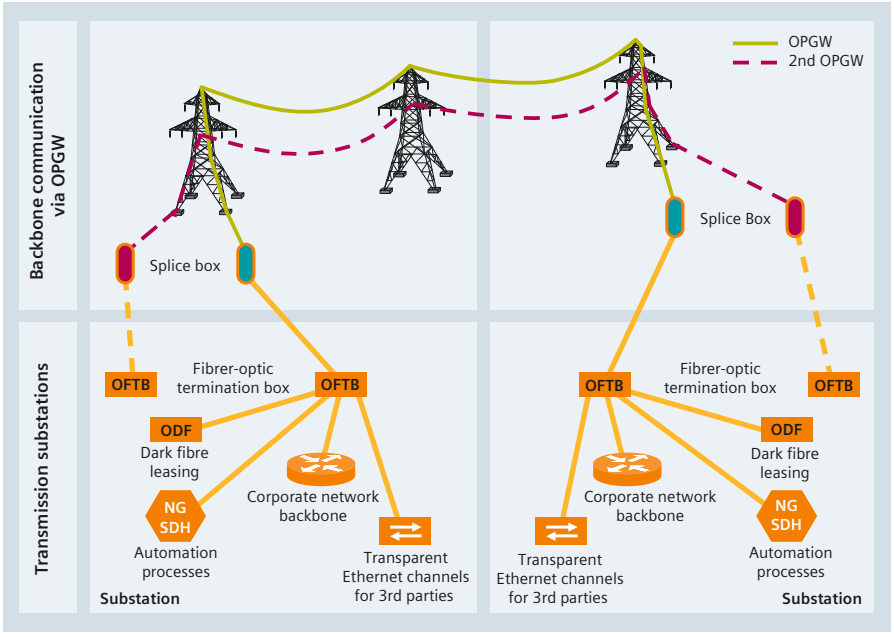


Fig. 8.2-9: **Live line installation of OPGW – installation alternatives**

8.3 Control Center Communication

Redundant control center communication
A control center for power supply systems such as Spectrum Power (fig. 8.3-1) is typically configured with full redundancy to achieve high availability. This includes communications. Depending on the system operator's requirements, various mechanisms are supported to achieve this goal for communication. This includes:

- Automatic failover of communication servers
- Configurable load sharing between two or more communication servers
- Automatic failover of communication lines
- Supervision of standby communication line, including telegram buffering

Process communication to substations and power plants
Process communication to the substations and to Remote Terminal Units (RTUs), e.g., in power plants or power supply systems, is implemented via serial interfaces or by means of TCP/IP-based network communication with a Communication Front End. The Communication Front End includes data-pre-processing functionality like :

- Routine for data reduction, e.g., old/new comparison, threshold check
- Data conversion
- Scaling and smoothing of measured values
- Integrity checks for incoming data
- Data completeness checks and cycle monitoring
- Statistical acquisition of the data traffic with the RTU.

All kinds of different protocols are used for historical reasons. However, as a result of international standardization there is also a market trend here towards standardized protocols like IEC 60870-5-104, DNP3i protocol or IEC-61850.

The more recent protocol standards all rely on TCP/IP-based communication. However, it must be possible today and in the near future to continue connecting conventional telecontrol devices (already installed RTUs) via serial interfaces.

Interface for industry automation/third-party applications
OPC (OLE for process control) and OPC UA provide a group of defined interfaces. OPC in general enables the overall data exchange between automation and control applications, field systems/field devices, as well as business and office applications.

OPC is based on OLE/COM and DCOM technology. OPC UA (Unified Architecture) is a continuation and further innovation of OPC. OPC UA is based on native TCP/IP and is available for multiple operating system platforms, including embedded devices.

Communication between control centers
The communication between control centers is provided via the communication protocols ICCP or ELCOM, and is based on TCP/IP.

The Inter Control Center Communication Protocol (ICCP) is an open and standardized protocol based on IEC 60870-6 and Telecontrol Application Service Element Two (TASE.2).

The exchanged data is primarily real-time system information like analog values, digital values and accumulator values, along with supervisory control commands.

Remote workstations/office communication
Remote workstations can communicate with the control center via the office LAN or an Internet connection. System and data integrity has to be ensured by the system security configuration for

- Protection against external attacks
- Protection against unauthorized usage
- Protection against data loss

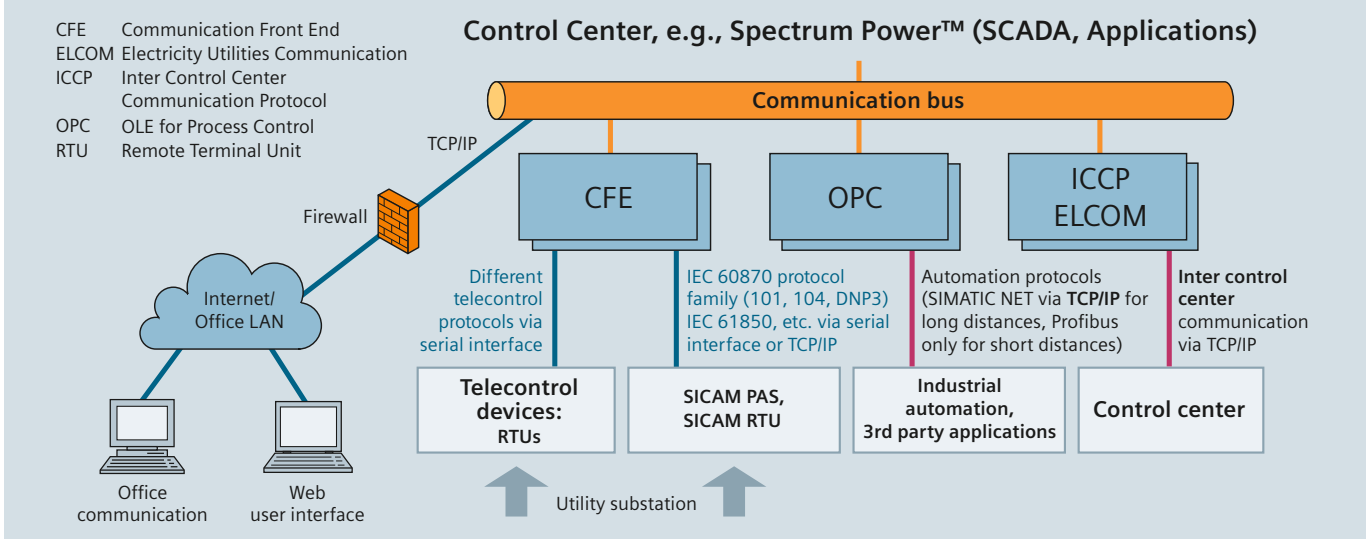


Fig. 8.3-1: **Typical communication interfaces and communication partners of a control center using the example of Spectrum Power™**

8.4 Substation Communication

8.4.1 Overview of IEC 61850

Since being published in 2004, the IEC 61850 communication standard has gained more and more relevance in the field of substation automation. It provides an effective response to the needs of the open, deregulated energy market, which requires both reliable networks and extremely flexible technology – flexible enough to adapt to the substation challenges of the next twenty years. IEC 61850 has not only taken over the drive of the communication technology of the office networking sector, but it has also adopted the best possible protocols and configurations for high functionality and reliable data transmission. Industrial Ethernet, which has been hardened for substation purposes and provides a speed of 100 Mbit/s, offers bandwidth enough to ensure reliable information exchange between IEDs (Intelligent Electronic Devices), as well as reliable communication from an IED to a substation controller.

The definition of an effective process bus offers a standardized way to connect conventional as well as intelligent CTs and VTs to relays digitally. More than just a protocol, IEC 61850 also provides benefits in the areas of engineering and maintenance, especially with respect to combining devices from different vendors.

Key features of IEC 61850
As in an actual project, the standard includes parts describing the requirements needed in substation communication, as well as parts describing the specification itself.

The specification is structured as follows:
- An object-oriented and application-specific data model focused on substation automation.
- This model includes object types representing nearly all existing equipment and functions in a substation – circuit-breakers, protection functions, current and voltage transformers, waveform recordings, and many more.
- Communication services providing multiple methods for information exchange. These services cover reporting and logging of events, control of switches and functions, polling of data model information.
- Peer-to-peer communication for fast data exchange between the feeder level devices (protection devices and bay controller) is supported with GOOSE (Generic Object Oriented Substation Event).
- Support of sampled value exchange.
- File transfer for disturbance recordings.
- Communication services to connect primary equipment such as instrument transducers to relays.
- Decoupling of data model and communication services from specific communication technologies.
- This technology independence guarantees long-term stability for the data model and opens up the possibility to switch over to successor communication technologies. Today, the standard uses Industrial Ethernet with the following significant features:
  – 100 Mbit/s bandwidth
  – Non-blocking switching technology
  – Priority tagging for important messages
  – Time synchronization
- A common formal description code, which allows a standardized representation of a system's data model and its links to communication services.
- This code, called SCL (Substation Configuration Description Language), covers all communication aspects according to IEC 61850. Based on XML, this code is an ideal electronic interchange format for configuration data.
- A standardized conformance test that ensures interoperability between devices. Devices must pass multiple test cases: positive tests for correctly responding to stimulation telegrams, plus several negative tests for ignoring incorrect information
- IEC 61850 offers a complete set of specifications covering all communication issues inside a substation
- Support of both editions of IEC 61850 and all technical issues.

8.4.2 Principle Communication Structures for Protection and Substation Automation Systems

SIPROTEC – communication of protection relays and bay controllers
Communication interfaces on protection relays are becoming increasingly important for the efficient and economical operation of substations and networks.

The interfaces can be used for:
- Accessing the protection relays from a PC using the DIGSI operating program for aspects of configuration, access of operational and non-operational data.

Remote access via modem or Ethernet modem is possible with a serial service port at the relay. This allows remote access to all data of the protection relay.

By using the remote communication functions of DIGSI it is possible to access relays, e.g., from the office via the telephone network (fig. 8.4-1). For example, the error log can be transferred to the office and DIGSI can be used to evaluate it.
- Integrating the relays into control systems with IEC 60870-5-103 protocol, PROFIBUS DP protocol, DNP 3.0 protocol and MODBUS protocol.

The new standardized IEC 61850 protocol (section 8.3.1) has been available since October 2004, and with its SIPROTEC units Siemens was the first manufacturer worldwide to provide this standard.
- Thanks to the standardized interfaces IEC 61850, IEC 60870-5-

103, DNP 3.0 (serial or over IP), MODBUS, PROFIBUS DP, SIPROTEC units can also be integrated into non-Siemens systems or in SIMATIC S5/S7. Electrical RS485 or optical interfaces are available. The optimum physical data transfer medium can be chosen thanks to opto-electrical converters. Thus, the RS485 bus allows low-cost wiring in the cubicles and an interference-free optical connection to the master can be established.

- Peer-to-peer communication of differential relays and distance relays (section 8.5.2) to exchange real-time protection data via fiber-optic cables, communication network, telephone networks or analog pilot wires.

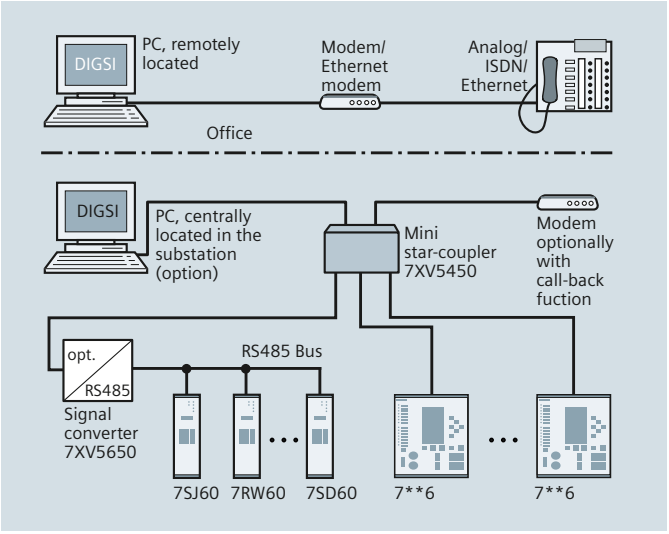


Fig. 8.4-1: **Basic remote relay communication**

Ethernet-based system with SICAM

SIPROTEC is tailor-made for use with the SICAM power automation system together with IEC 61850 protocol. Via the 100 Mbit/s Ethernet bus, the units are linked electrically or optically to the station unit. Connection may be simple or redundant. The interface is standardized, thus also enabling direct connection of units from other manufacturers to the LAN. Units featuring an IEC 60870-5-103 interface or other serial protocols can be connected via the Ethernet station bus to SICAM by means of serial/ Ethernet converters. DIGSI and the Web monitor can also be used over the same station bus. Together with Ethernet/IEC 61850 an interference-free optical solution can be provided. Thus, the installation Ethernet interface in the relay includes an Ethernet switch. Thus, the installation of expensive external Ethernet switches can be avoided. The relays are linked in an optical ring structure (fig. 8.4-2).

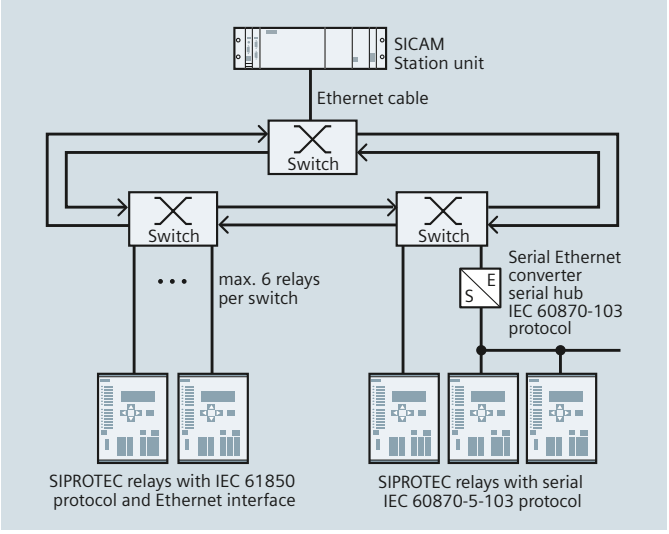


Fig. 8.4-2: **Ethernet-based system with SICAM**

Further communication options for IED connection

Apart from supporting IEC 61850, modern substation automation systems like SICAM also support the connection of IEDs (Intelligent Electronic Devices) with other protocol standards like the well-known standard IEC 60870-5-103 for protections units as well as DNP3 (serial or over IP), and also protocols such as PROFIBUS DP and MODBUS.

Specifically with SICAM PAS, the devices with serial communication can be reliably connected directly to the substation controller. Moreover it is also possible to use LAN for backbone communication throughout the substation, connecting such serial devices with serial hubs in a decentralized approach.

Additionally it is also possible to connect subordinated substations and Remote Terminal Units (RTU) using the protocol standards IEC 60870-5-101 (serial communication) and IEC 60870-5-104 (TCP/IP).

Especially for communication with small RTUs, dial-up connections can be established based on IEC 60870-5-101.

Additional features of TCP/IP communication

Besides the traditional protocols mentioned for data exchange with IEDs, in the world of Ethernet it is also important to be aware of the status of communication infrastructure devices such as switches. In this context, the protocol SNMP (Simple Network Management Protocol) helps a lot. SICAM PAS supports this protocol, thereby providing status information, e.g., to the control center, not only for IEDs and substation controllers, but also for Ethernet switches and other "SNMP devices".

Another communication protocol, well-known from the industrial automation sector, is also required for substation automation applications: OPC (OLE for Process Control, see also Control Center Communication). Additional interoperable solutions are possible with OPC, especially for data exchange with devices and applications of industrial automation. SICAM PAS supports both OPC server and OPC client.

The linking of protection relays and/or bay controllers to the station level is chosen according to the size and importance of the substation. Whereas serial couplings with IEC 60870-5-103

are the most economical solution in small distribution substations (only medium voltage), Ethernet in compliance with IEC 61850 is normally used for important high-voltage and extra-high-voltage substations. In addition there are a number of different physical designs, based on the local situation as regards cable runs and distances, and on the requirements in terms of availability and EMC influences.

The simplest version is the serial bus wiring in accordance with RS 485 in which the field devices are electrically connected to a master interface on the SICAM central unit (fig. 8.4-3). This wiring is particularly recommended in new installations. Special attention should also be paid to correct handling of the earthing, and also to possible impact on the EMC due to the primary technology or power cables. Separate cable routes for power supply and communications are an essential basis for this. A reduction of the number of field devices per master to about 16 to 20 devices is recommended in order to be able to make adequate use of the data transfer performance.

A star configuration of the wiring is rather easy to handle and can be in the form either of electrical wiring as per RS 232, or optical fiber. Here again, the number of devices per master should be limited as before (fig. 8.4-4).

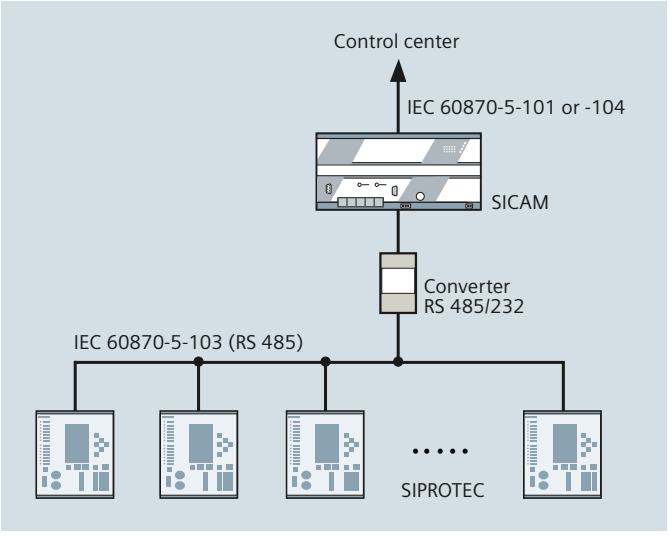


Fig. 8.4-3: **Serial bus wiring in accordance with RS 485**

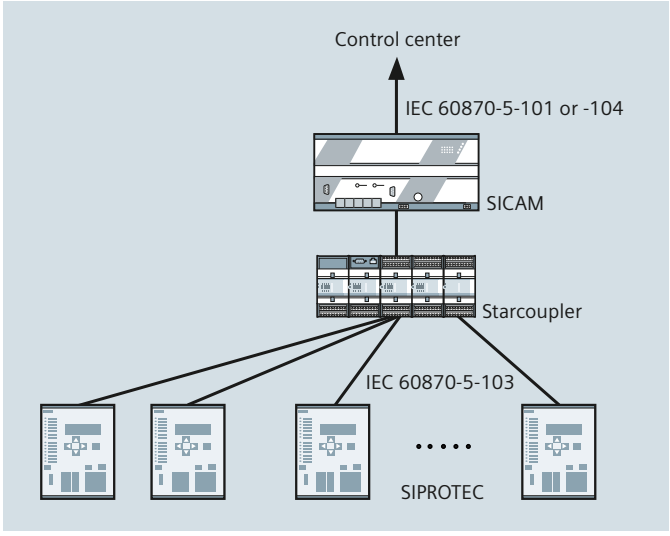


Fig. 8.4-4: **Star wiring in accordance with RS 232 or per fiber-optic cable**

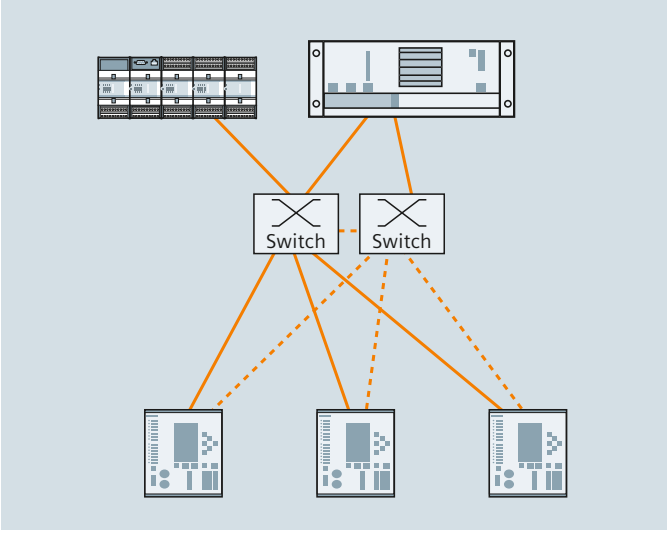


Fig. 8.4-5: **Ethernet: Star configuration electrical or optical**

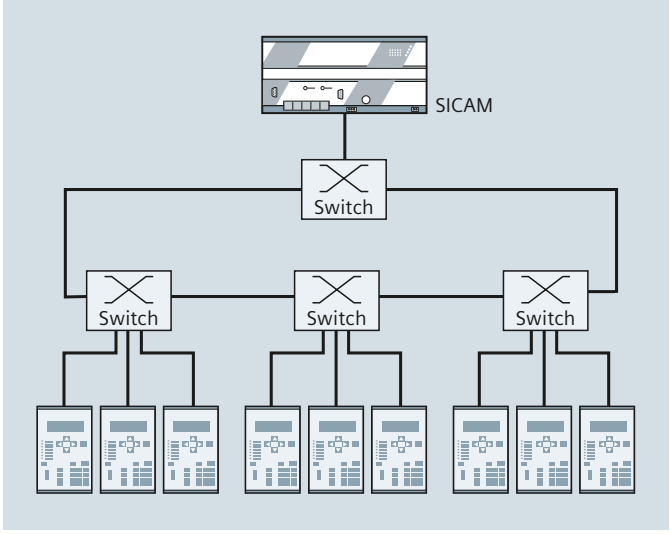


Fig. 8.4-6: **Ethernet: Optical ring with external switches**

The configurations with Ethernet are similar, with star and ring versions available. Variants with redundancy complete these configurations. The star configuration is especially recommended for central arrangements with short distances for the cable routes (fig. 8.4-5).

A fiber-optic ring can be made up of individual switches. That is especially advisable if several devices are to be connected in each feeder (fig. 8.4-6).

A more economical solution is the fiber-optic ring with SIPROTEC relays because these devices have a switch directly integrated (fig. 8.4-7). In this application, though, a suitable device from RuggedCom must be used for the central switch so that the fast switchover times can also be used in the case of a malfunction on the ring. The number of devices in the ring is restricted to 27.

Several rings can also be combined on the basis of this fundamental structure, e.g., one per voltage level. Usually these rings are combined to form a higher level ring which then communicates with redundant station devices. This version offers the highest availability for station-internal communication (fig. 8.4-8).

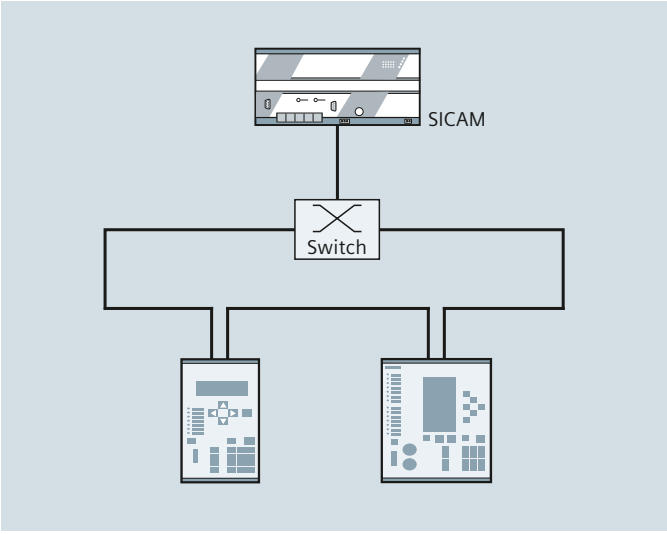


Fig. 8.4-7: **Optical ring with integrated switches**

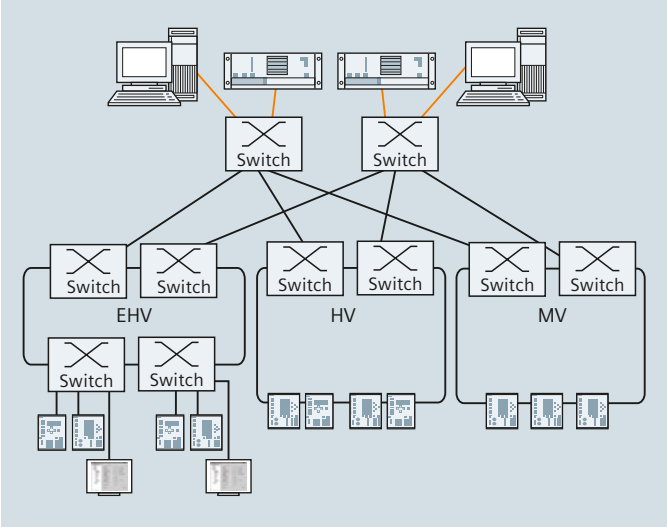


Fig. 8.4-8: **The combination of several rings offers the highest availability**

8.4.3 Multiple Communication Options with SIPROTEC 5

The SIPROTEC 5 modular concept ensures the consistency and integrity of all functionalities across the entire device series. Significant features here include:

Powerful and flexible communication is the prerequisite for distributed and peripheral system landscapes. In SIPROTEC 5 this is a central element of the system architecture enabling a wide variety of communication requirements to be satisfied while providing utmost flexibility. Fig 8.4-11 shows a possible hardware configuration equipped with 4 communication modules. Fig 8.4-12 shows the CB202 expansion module with 3 slots for plug-in modules. Two of these slots can be used for communication applications.

Owing to the flexibility of hardware and software, SIPROTEC 5 features the following system properties:

- Adaptation to the topology of the desired communication structure, such as ring or star configurations
- Scalable redundancy in hardware and software (protocols)
- Multiple communication channels to various superordinate systems
- Pluggable communication modules that can be retrofitted
- The module hardware is independent of the communication protocol used
- 2 independent protocols on a serial communication module
- Up to 8 interfaces are available
- Data exchange via IEC 61850 for up to 6 clients using an Ethernet module or the integrated Ethernet interface.

Fig. 8.4-11: **SIPROTEC 5 device with 4 communication module**

Fig. 8.4-12: **CB202: expansion modules with communication modules and analog input module**

Communication examples with SIPROTEC 5
Regardless of the desired protocol, the communication technology used enables communication redundancies to be tailored to the requirements of users. They can basically be divided into Ethernet and serial communication topologies.

Protocols
- Serial protocols
- Ethernet protocols

Different degrees of protocol redundancy can be implemented. The 4 plug-in module slots limit the number of independent protocol applications that run in parallel. For serial protocols, 1 or 2 masters are usually used.

Serial protocols
Redundant or different serial protocols are capable of running simultaneously in the device, e.g., DNP 3 and IEC 60870-5-103. Communication is effected to one or more masters.

Two serial protocols can run on a double module (fig 8.4-13). It is not relevant in this context whether these are two protocols of the same type or two different protocols.

The communication hardware is independent of the required protocol. This protocol is specified during parameterization with DIGSI 5.

Ethernet protocols
The Ethernet module can be plugged in once or multiple times in the device. This enables running identical or different protocol applications in multiple instances. Multiple networks are possible for IEC 61850 or DNP3 TCP, but they can also be operated in a common Ethernet network. A module implements the IEC 61850 protocol application, e.g., the data exchange between devices using GOOSE messages. The other module is responsible for the client-server communication over the DNP TCP protocol. The client-server architecture of IEC 61850 enables one server (device) to send reports to up to 6 clients simultaneously. In this case, only one network is used.

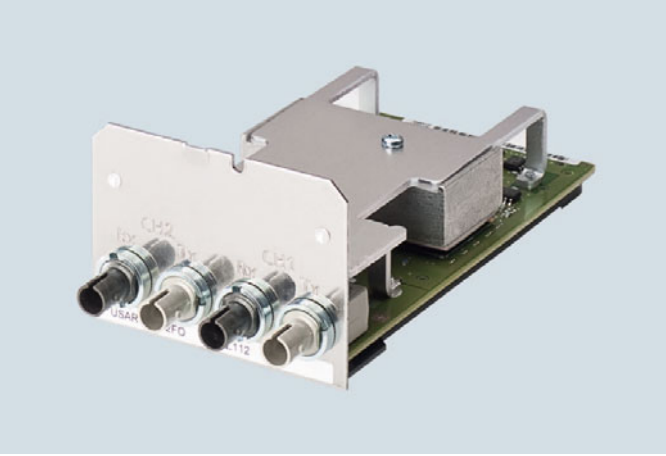


Fig. 8.4-13: **Serial optical double module**

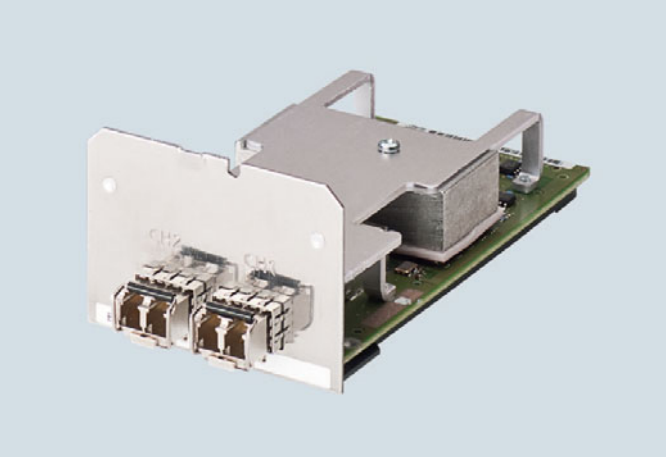


Fig. 8.4-14: **Optical Ethernet module**

Examples
Redundancies to substation automation systems
- 2 redundant substation automation systems
- 2 different substation automation systems.

Example 1: Two redundant substation automation systems
Fig. 8.4-15 show shows a serial optical network which connects the serial protocol interfaces of the device to one master, respectively. Transmission is accomplished in multipoint-star configuration and with interference-free isolation via optical fiber.

For the IEC 60870-5-103 protocol, the device supports special redundancy procedures. For instance, a primary master can be configured that is preferred to the second master in control direction. The current process image is transmitted to both masters.

The fig. 8.4-16 describes a fully redundant solution based on IEC 61850. 2 Ethernet communication modules are plugged into each SIPROTEC 5 device. 2 redundant fiber-optic rings are set up by means of the switches integrated in the module and connected to the redundant clients (substation automation systems). Alternatively, the redundant IEC 61850 communication could also be accomplished via a common optical ring.

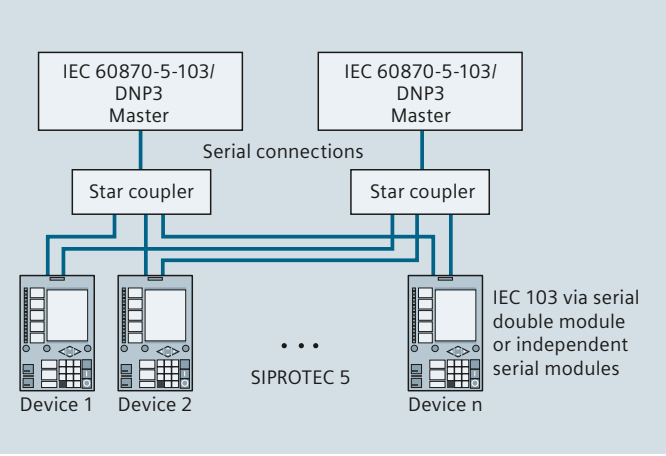


Fig. 8.4-15: **Redundant IEC 60870-5-103 or DNP 3 communication**

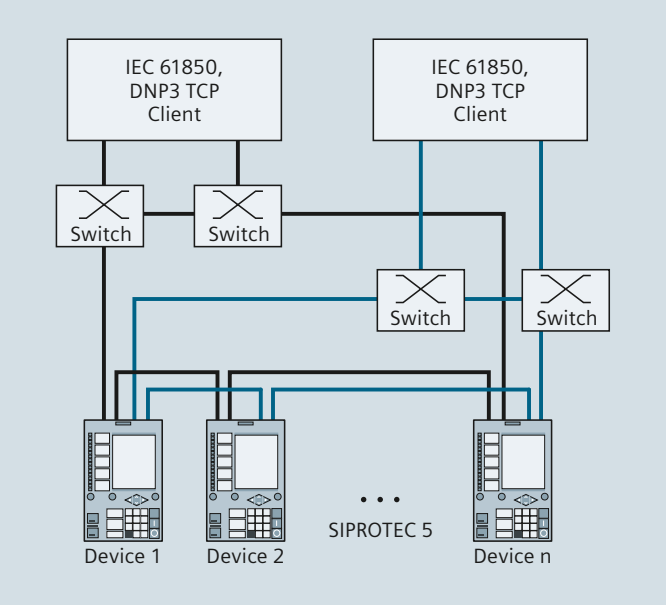


Fig. 8.4-16: **Redundant communication to two IEC 61850 or DNP3 TCP clients**

Example 2: Two substation automation systems with different protocols

Since both the serial protocols and the Ethernet-based protocols are only specified during parameterization, the configuration described previously can also be implemented using mixed protocols. This can be a particularly interesting case of application if different control centers are connected via different protocols. This could be, for example, the control center of the transmission system and the control center of the distribution system. Fig. 8.4-17 and fig. 8.4-18 show a possible combination.

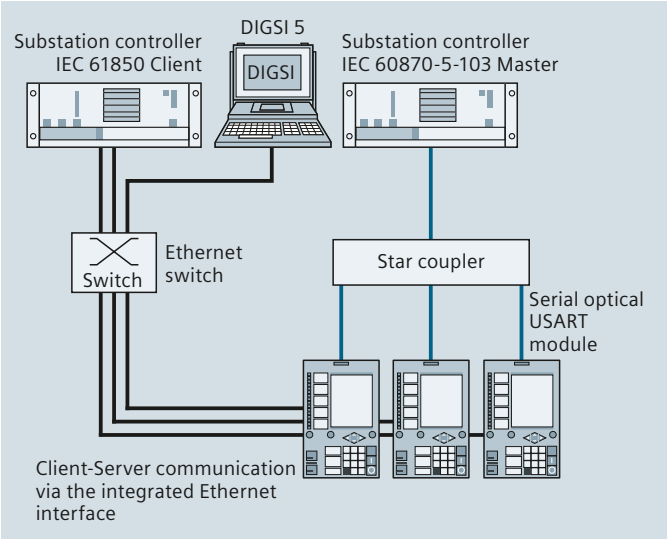


Fig. 8.4-17: **Communication to IEC 61850 client and serial connection to an IEC 61870-5-103 master**

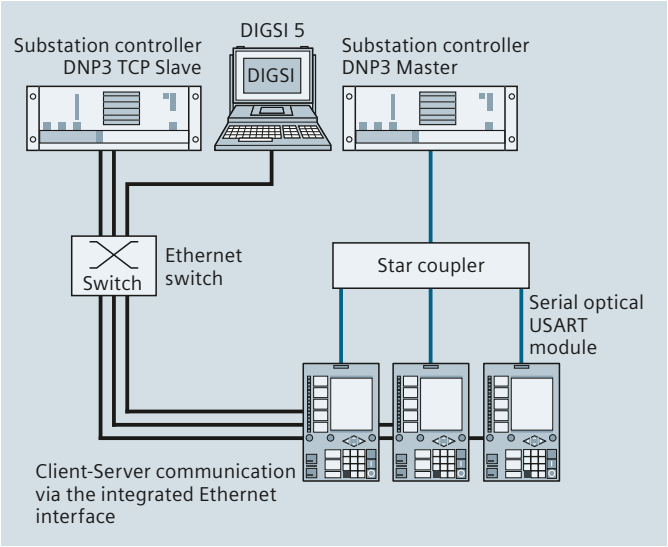


Fig. 8.4-18: **Communication to DNP3 TCP slave and serial connection to an DNP3 master**

Multiple substations buses

Substation-wide Ethernets are increasingly being used in modern substation automation systems in practice. These networks transport both the communication services to the central substation computer controller and the signals between the devices of the bay level. Usually, a single Ethernet subsystem is set up for this purpose since the bandwidth of today's Ethernet networks is sufficient for the entire data traffic.

By using multiple communication modules and protocols in SIPROTEC 5 it is now possible to set up several subsystems, and to separate the different applications. For example, a separate process bus for process signals (GOOSE) could be implemented on bay level, and a separate bus to the central substation computer. See fig. 8.4-19 (2 substation buses).

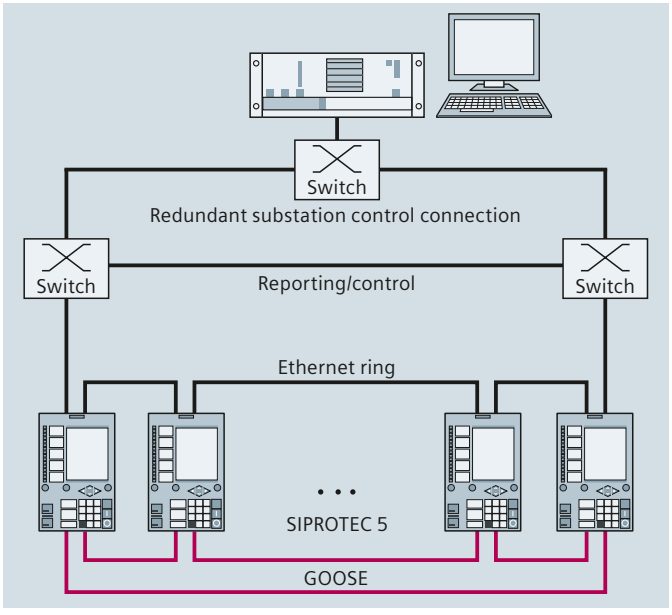


Fig. 8.4-19: **Separate buses for reporting and GOOSE communication**

8.4.4 Network Redundancy Protocols

Today's configuration of a substation network – RSTP
The electrical and optical Ethernet modules of SIPROTEC devices support different network topologies. This applies independently of the selected protocol (IEC 61850 or DNP TCP).

If the module operates in dual homing redundancy (without integrated switch), it can be connected to external switches either in simple or redundant configuration. Only one interface at a time processes the protocol applications (e.g., IEC 61850) in this case. The second interface operates in standby mode (hot standby), and the connection to the switch is monitored. If the interface which processes the protocol traffic fails, the standby interface is activated within a few milliseconds and takes over) – (fig. 8.4-20).

When activating the integrated switch, SIPROTEC devices can be integrated directly into the optical communication ring consisting of up to 40 devices (fig. 8.4-21). In this case, both interfaces of the module send and receive at the same time. The ring redundancy procedure Rapid Spanning Tree Protocol (RSTP) ensures short switchover times if the communication is interrupted, allowing the protocol applications to continue operation virtually without interruption. This configuration is independent of the protocol application running on the Ethernet module.

Today, more than 250,000 Siemens devices in more than 3,000 substations are in operation worldwide in stations with RSTP. In case of ring interruptions, RSTP reconfigures the communication within a short time, and provides a secure operation of substations.

Seemless redundancy PRP and HSR
New technologies reduce the time for reconfiguration of communication networks in case of interruptions to about nothing. These technologies are:
- PRP = Parallel Redundancy Protocol
- HSR = High Available Seamless Ring Redundancy

Both systems have the same principle and are specified in IEC 62439-3.

The same information (Ethernet frame) is being sent over two ways. The receiver takes the first that comes in and discards the second one. If the first does not get through, the second one is still available and will be used. The mechanism is based deeply in the Ethernet stack, means one MAC and one IP address for both.
- PRP uses two independent Ethernet systems. This means double amount of network equipment and respectively cost, but it is simple.
- HSR is using the same principle, but in one Ethernet network in a ring configuration. The same information (Ethernet frame) will be sent in the two directions into the ring, and the receiver gets it from the two sides of the ring. This means some more effort in the devices but saves the costs for a second Ethernet network.

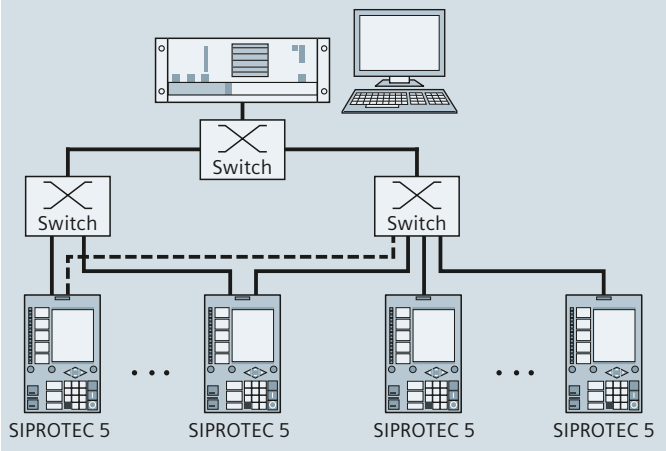


Fig. 8.4-20: **Redundant or single star connection to external switches (dual homing redundancy)**

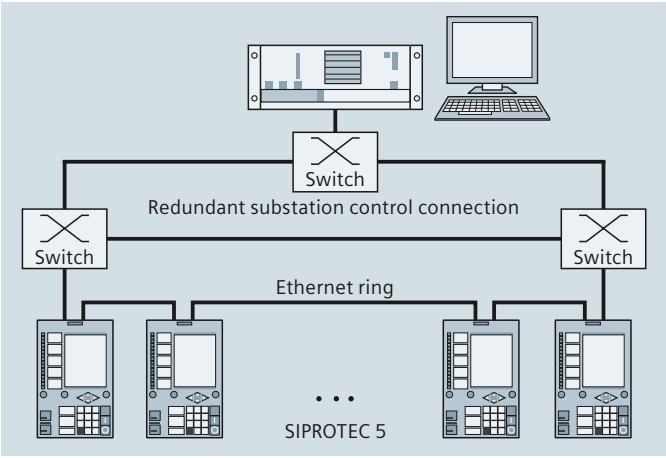


Fig. 8.4-21: **Operation with integrated switch and ring redundancy**

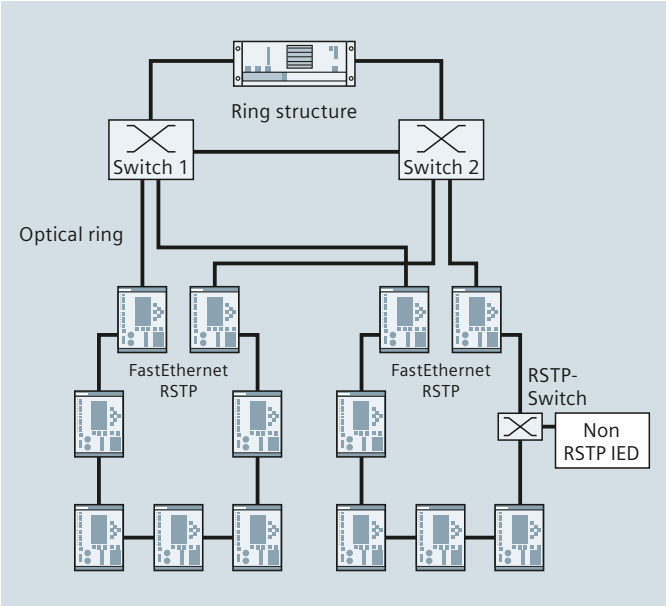


Fig. 8.4-22: **Example of an RSTP solution**

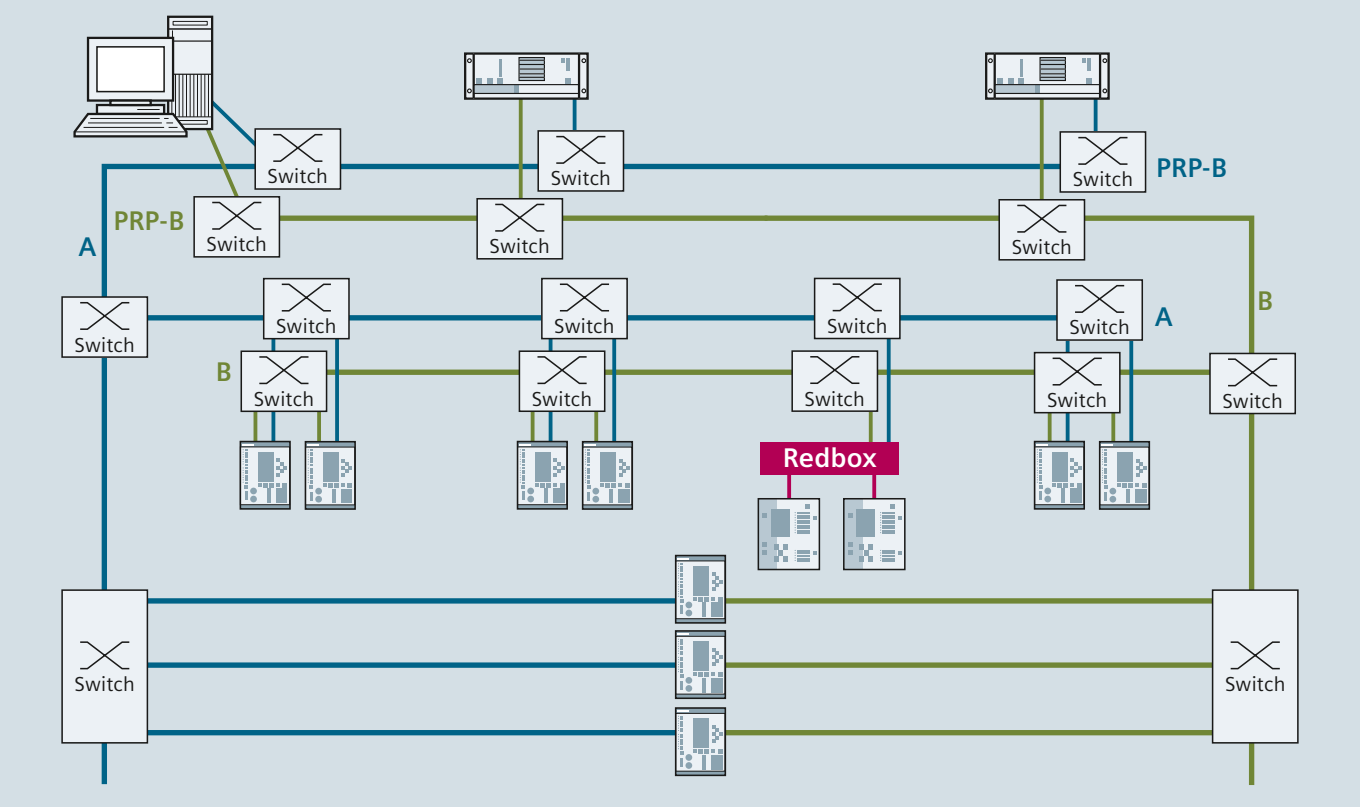


Fig. 8.4-23: **Seamless redundancy by use of PRP only**

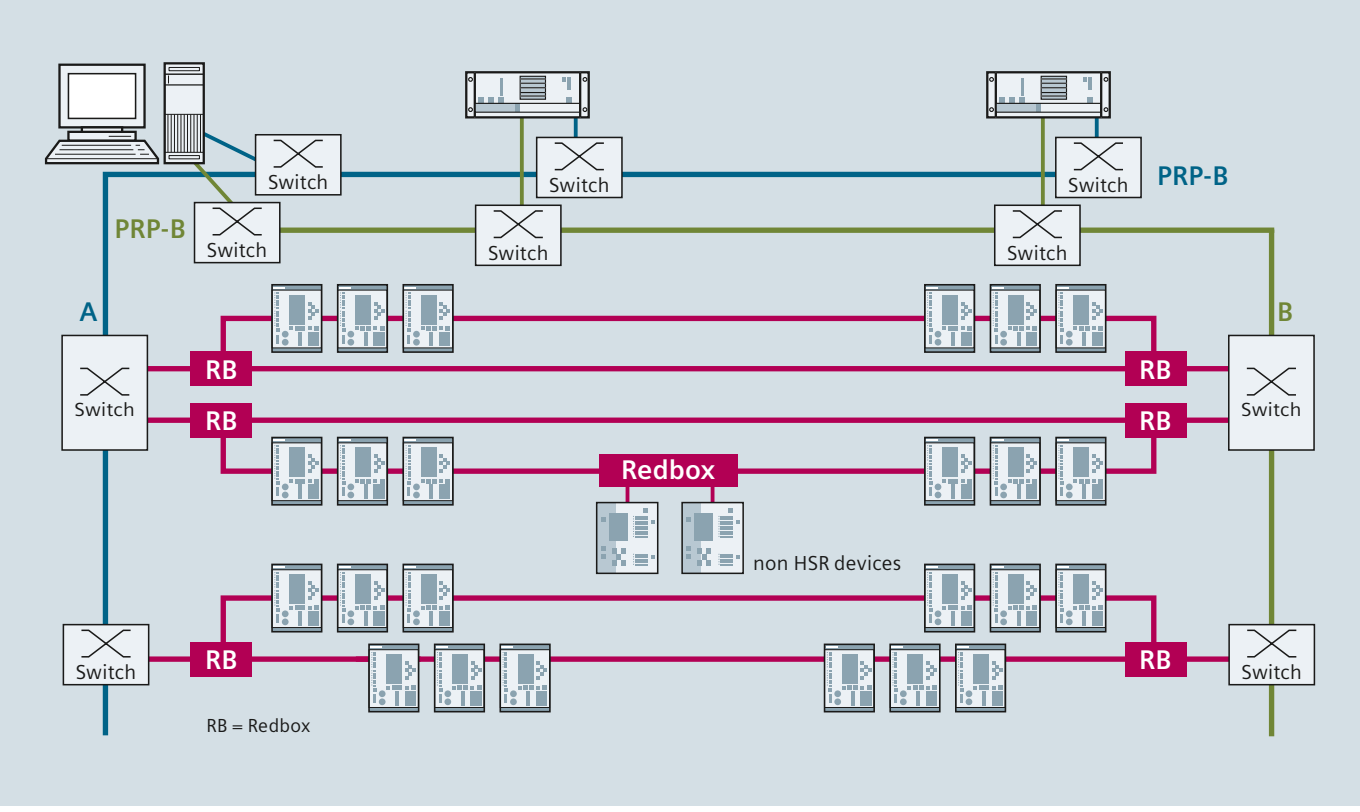


Fig. 8.4-24: **Seamless redundancy by use of PRP/HSR combined**

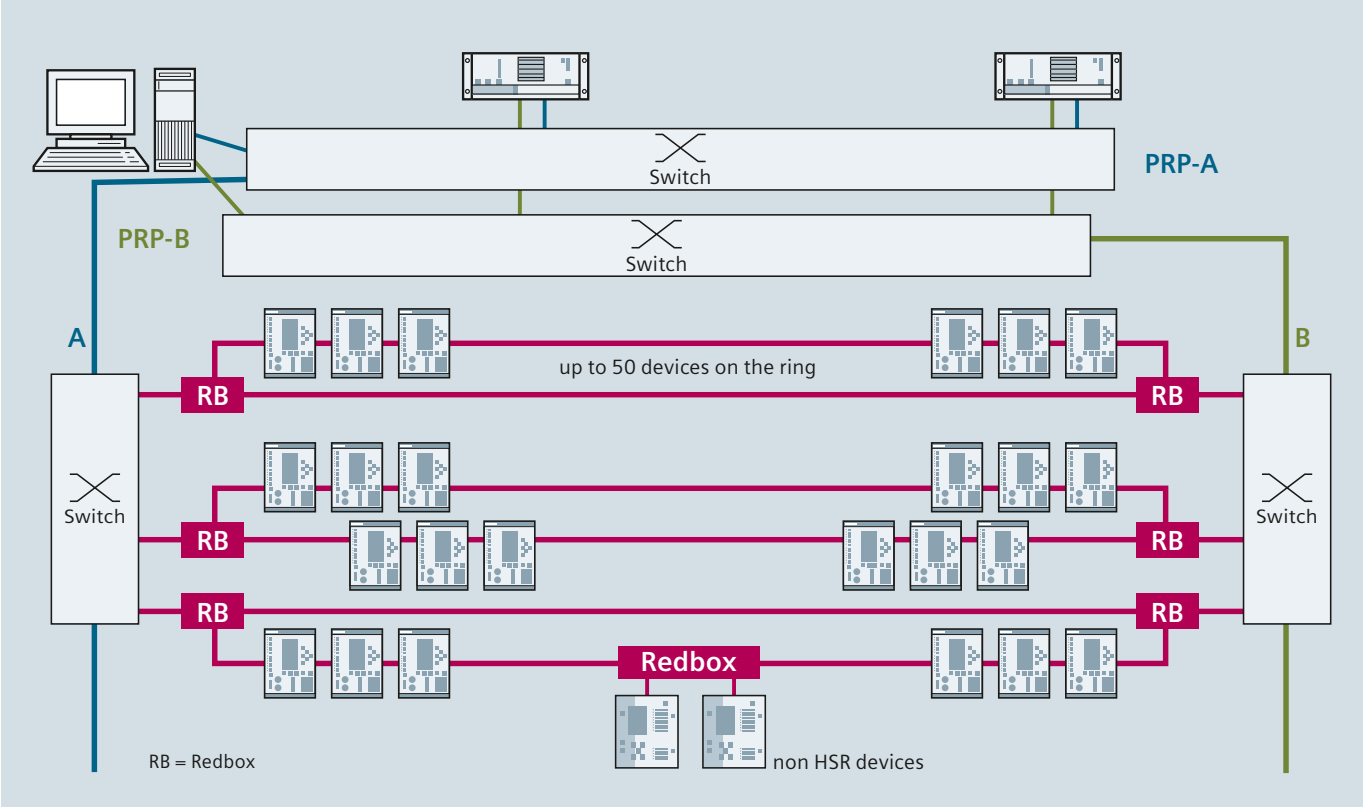


Fig. 8.4-25: **Most cost-effective seamless n-1 structure**

HSR and PRP can be combined by so called RedBoxes (Redundancy Boxes).

The figs. 8.4-23 to 8.4-25 show some examples of PRP and HSR configurations.

This cost-effective solution of fig. 8.4-25 can be achieved by:
- 2 switches at the control room
- 2 switches in the field
- 2 Redboxes (RB) per HSR ring
- Up to 50 devices per HSR ring
- Easy expansion by additional 2 PRP switches

Summary
- Siemens offers redundancy solutions
  - Dual link redundancy
  - RSTP
  - PRP (seamless)
  - HSR (seamless)
- Dual link and RSTP: Field proven established technology
- PRP: High level redundancy through double network solution
- HSR: High level redundancy through cost effective ring network structure. Combinable with PRP network.
- Siemens Seamless Ethernet Media Redundancy Suite: SICAM PAS, SIPROTEC and Redbox
- SIPROTEC with integrated RSTP/PRP/HSR switches

–> Siemens solutions produce significant user advantage in terms of functionality.

8.4.5 Communication Between Substation Using Protection Data Interfaces

SIPROTEC 4 – differential and distance protection
Typical applications of differential and distance protection are shown in fig. 8.4-26. The differential protection relay is connected to the current transformers and to the voltage transformers at one end of the cable, although only the currents are required for the differential protection function. Direct connection to the other units is effected via single-mode fiber-optic cables and is thus immune to interference. Various communication modules are available for different communication media. In the case of direct connection via fiber-optic cables, data communication is effected at 512 kbit/s and the command time of the protection unit is reduced to 15 ms.

SIPROTEC 4 offers many features to reliably and safely handle data exchange via communication networks. Depending on the bandwidth available, a communication converter for G703-64 kbit/s or X21-64/128/512 kbit/s can be selected. For higher communication speed, a communication converter with G703-E1 (2,048 kbit/s) or G703-T1 (1,554 kbit/s) is available.

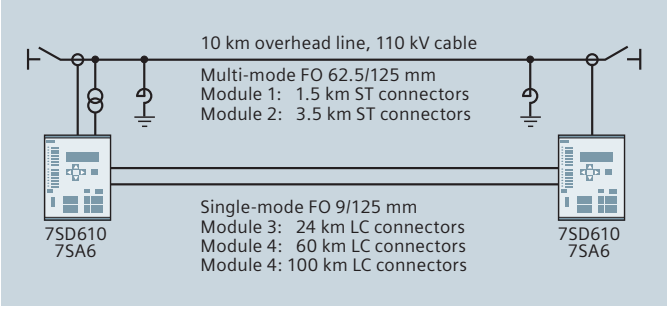


Fig. 8.4-26: **Protection Data Interface using direct FO connection**

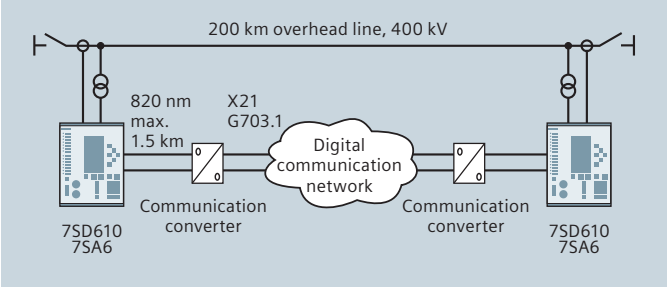


Fig. 8.4-27: **Protection Data Interface using digital communication networks**

Teleprotection using protection data interface
The teleprotection schemes can be implemented using digital serial communication. The distance protection SIPROTEC 7SA6 is capable of remote relay communication via direct links or multiplexed digital communication networks. The link to a multiplexed communication networks is made by separate communication converters (7XV5662). These have a fiber-optic interface with 820 nm and ST connectors to the protection relay. The link to the communication networks is optionally an electrical X21 or a G703.1 interface (fig. 8.4-27).

SIPROTEC 5 – transfer of data via the protection interface
The protection interface and protection topology enable data exchange between the devices via synchronous serial point-to-point links from 64 kbit/s to 2 Mbit/s. These links can be established directly via optical fibers or via other communication media, e.g., via dedicated lines or communication networks.

A protection topology consists of 2 to 6 devices, which communicate point to point via communication links. It can be structured as a redundant ring or as a chain structure (see fig. 8-4.20), and within a topology the protection links can have different bandwidths. A certain amount of binary information and measured values can be transmitted bi-directionally between the devices depending on the bandwidth. The connection with the lowest bandwidth determines this number. The user can route the information with DIGSI 5.

This information has the following tasks:
- Topology data and values are exchanged for monitoring and testing the link
- Protection data, for example differential protection data or direction comparison data of the distance protection, is transferred.
- Time synchronization of the devices can take place via the link, in which case a device of the protection topology assumes the role of timing master.
- The link is continuously monitored for data faults and failure, and the runtime of the data is measured.

Protection links integrated in the device have previously been used for differential protection (fig. 8-4.26) and for teleprotection of the distance protection. In addition to these protection applications, you can configure protection links in all devices in SIPROTEC 5. At the same time, any binary information and measured values can be transferred between the devices. Even connections with low bandwidth, e.g., 64 kbit/s can be used for this.

Use of the protection link for remote access with DIGSI 5
Access with DIGSI 5 to devices at the remote ends is possible via the protection interface. This allows devices at the remote ends to be remotely read out, or parameters to be set using the existing communication connection.

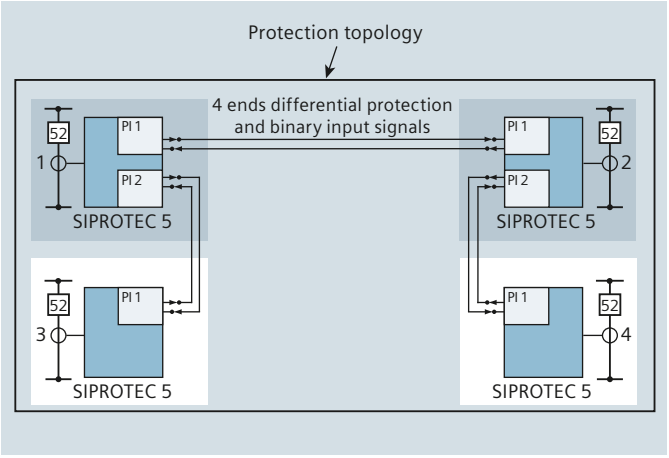


Fig. 8-4.28: **Protection communication of the differential protection and transfer of binary signals**

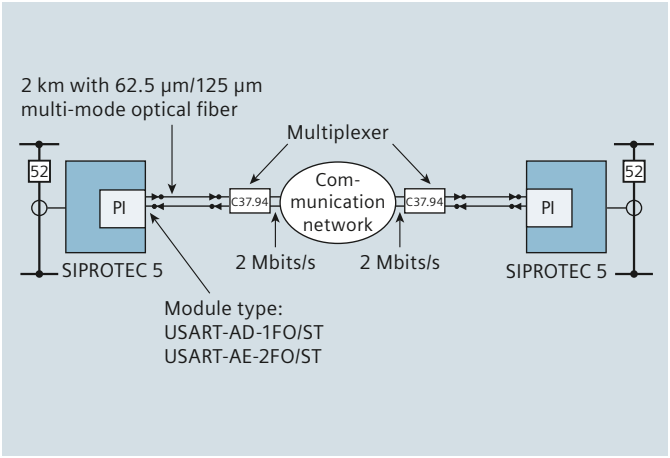


Fig. 8-4.31: **Protection communication via an IEEE C37.94 (2 Mbits/s) interface – direct fiber-optic connection to a multiplexer**

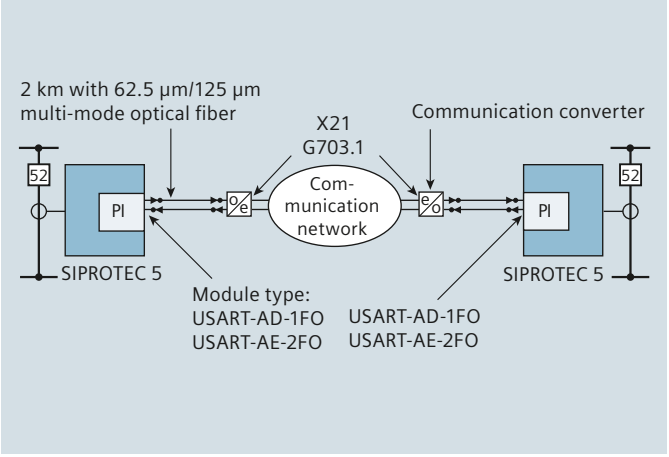


Fig. 8-4.29: **Protection communication via a communication network with X21 or G703.1 (64 kbit/s), G703.6... (2 Mbit) interface**

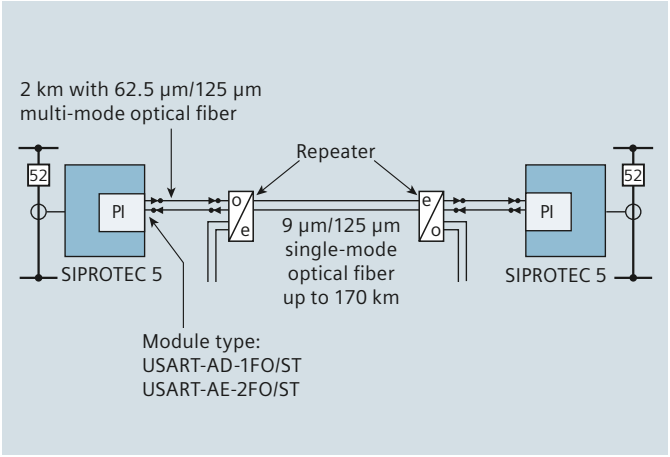


Fig. 8-4.32: **Protection communication via single-mode fiber and repeater**

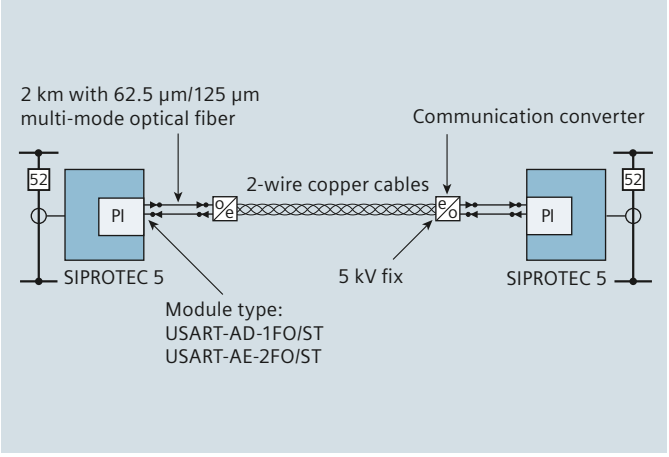


Fig. 8-4.30: **Protection communication via a copper connection**

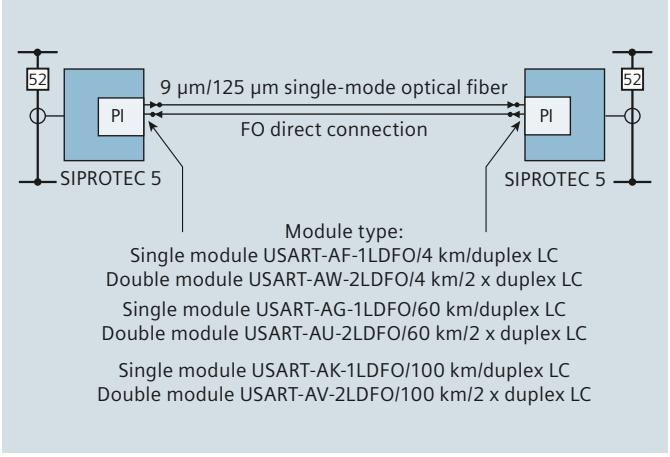


Fig. 8-4.33: **Protection communication via direct fiber-optic connections**

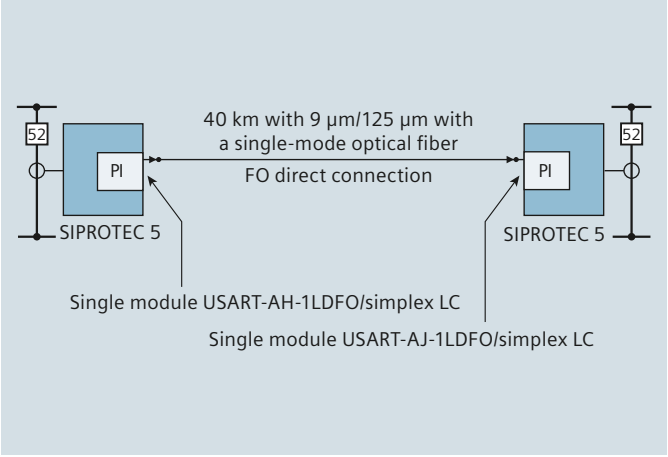


Fig. 8-4.34: **Protection communication via a single-mode fiber**

Figs. 8-4.28 to 8-4.34 show possible communication variants for establishing protection communications.

8.4.6 Requirements for Remote Data Transmission

In principle, both RTUs and station automation are very flexible for adapting to any remote communication media supplied by the user.

- Small substations are usually associated with small data volumes and poor accessibility of communication media. Therefore, dial-up modems are often used, also radio (if no lines available) or PLC communication. Sometimes even GPRS is an alternative, depending on the availability of a provider. Protocols also depend on the capabilities of the control center, but are mostly based on international standards like IEC 60870-5-101 (serial) and IEC 60870-5-104 (Ethernet), although DNP 3.0 is also found in some places (serial or over TCP/IP). Some small substations do not necessarily need to be online continuously. They can be configured to occasional calls, either locally or by external polling from the control center.
- Medium-size substations are generally connected via communication cables or optical fibers with serial end-end links. Serial lines with 1,200 Bd or higher are sufficient for IEC ...-101 or DNP. Sometimes, multiple lines to different control centers are necessary, while redundant communication lines are reserved for important substations only. WAN technology is increasingly used in line with the trend towards more bandwidth.

- Large substations, especially at transmission level, can have serial links as before, but with higher transmission rates. Anyway there is a trend towards wide area networks using Ethernet. For IEC ...-104 or similar protocols a minimum of 64 kbit/s should be taken into account. If large data volumes are to be exchanged and additional services (e.g., Voice over IP, Video over IP) provided, the connection should have more bandwidth (64 kbit/s < Bandwidth ≤ 2,048 kbit/s).

8.5 Communication Network Solutions for Distribution Grids (Backhaul/Access Communication)

8.5.1 Introduction

In the past, electricity was mainly produced by bulk generation at central locations, and distributed to consumers via the distribution systems. Energy peaks (e.g., at midday) were well known and balanced out by reserve capacity of central power plants. It was therefore usually not necessary to specially control the lower-level distribution networks, or even to integrate the consumers into the grid monitoring system.

Ever since renewable energy has been significantly expanded, electricity is being fed into both the medium-voltage and low-voltage systems, depending on changing external conditions (e.g., weather, time of day, etc.). These fluctuating energy resources can severely impair the stability of the distribution grids.

Buildings account for 40 % of the world's energy consumption and 20 % of total CO_2 emissions. Therefore, smart buildings also play a central role in the Smart Grid as they provide a huge potential for energy efficiency. Actively influencing their consumption and generation, smart buildings support the system stability and allow generators to consider other options before adding new generation facilities.

One of the key challenges of a Smart Grid therefore is quickly balancing out the energy supply and energy consumption in the distribution system (fig. 8.5-1).

A prerequisite for implementing a solution for this demand is monitoring and managing as many components of a power supply system as possible all the way to the consumer. The basis for this is a reliable communication infrastructure. For medium voltage, at least the following system components must be integrated into a Smart Grid and managed:

- The key ring-main units
- All large distributed producers (solar/wind farms, biogas/hydroelectric power plants, etc.)
- Large buildings, campuses, refrigerated warehouses, etc.

For low voltage, primarily households and small producers of renewable energy are involved.

With respect to their role in the power supply system, consumers can be divided into two groups:

- "Standard consumers", who have smart meters and optimize their electricity costs via ongoing price signals depending on supply and demand
- "Prosumers" (prosumer = producer + consumer), who can feed surplus energy into the power grid – such as solar power or energy generated by combined heat and power systems (CHP); many can also intermediately store energy using possibilities such as night storage heaters or e-cars.

While the communication requirements for standard consumers are concentrated on smart metering including price signals, time-critical control signals and power quality data must also be transmitted for prosumers. Therefore, in addition to smart meters, prosumers have energy gateways, which process and forward these control signals accordingly.

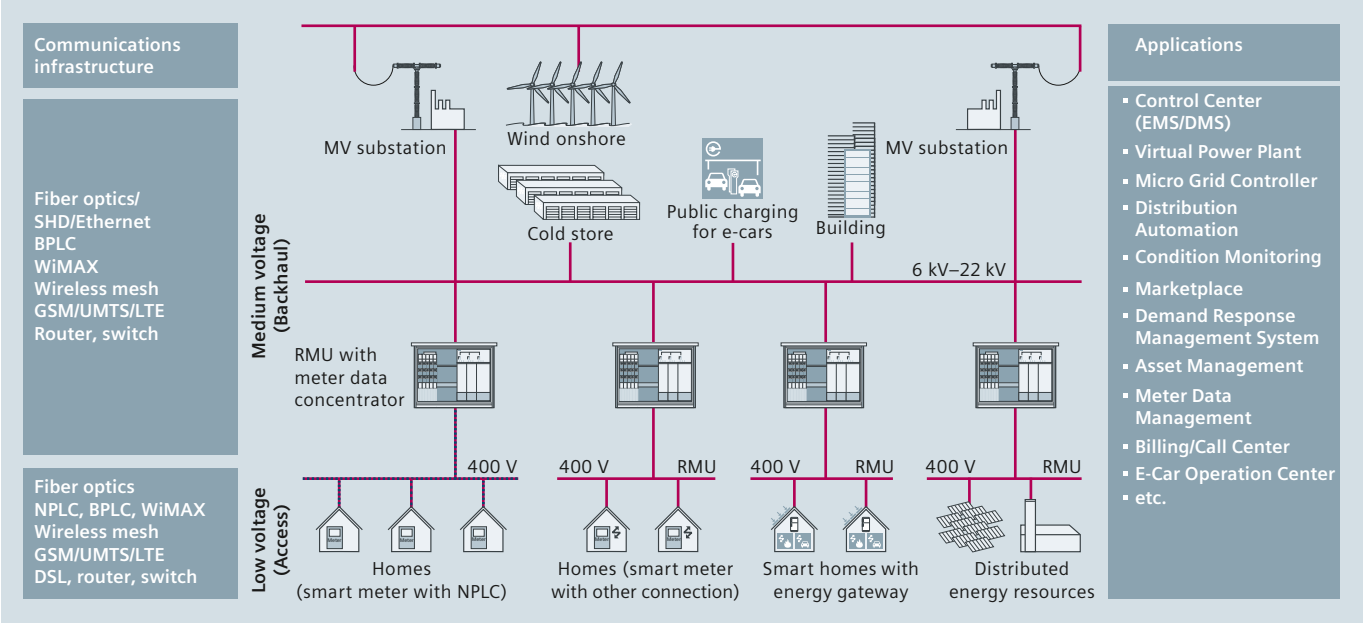


Fig. 8.5-1: **Typical power distribution network integrating ring-main units, consumers, prosumers, distributed energy resources, etc.**

The young history of Smart Grids has already shown that utilities do not implement it as a whole from the scratch. They usually start with smart metering projects with later extensions of Smart Grid applications.

Already with the first roll-out, the design of the communication infrastructure has to consider the growing requirements for these extensions. After a large deployment of metering infrastructure in the first step, it is not acceptable to replace the communication network a few years later because the requirements for the next subsets of Smart Grid applications cannot be met anymore.

Communications infrastructures for all conditions
The communication infrastructure in the medium-voltage and low-voltage distribution systems is usually heterogeneous, and the suitable technologies depend to a large extent on the local topology (large city, rural region, distances, etc.). It must therefore be specifically tailored for each customer.

In general, the following communication technologies are available:
- Fiber-optic or copper cables are the best option, if present
- Narrowband Power Line Carrier (NPLC) systems for transmitting meter data; they are frequently already integrated into the smart meters
- Broadband PLC systems offering IP connectivity with > 1 Mbps
- Setup of own private wireless networks (e.g., wireless mesh, private WiMAX), when spectrum is available at reasonable prices or local regulations allow for it
- Public wireless networks, depending on the installation for narrowband communication in the kbps range (e.g., GPRS), or in the future in the Mbps range (LTE, WiMAX providers). Attractive machine-to-machine (M2M) data tariffs and robust communication in case of power outages are key ingredients to make this communication channel a viable option.

Depending on the applications being installed inside the RMU, an Ethernet switch/router might be needed in order to concentrate the flow of communications. These data concentrators can be implemented as customized solutions or integrated, for example, in the RTU (remote terminal unit). To meet these requirements, Siemens offers a full range of all above-mentioned communication technologies including rugged switches and routers that comply with energy industry standards.

8.5.2 Communication Infrastructures for Backhaul and Access Networks

Optical fibers
The best choice for all communication needs
Optical fibers is the best transmission medium for medium-voltage and low-voltage applications because it is robust and not susceptible to electromagnetic disturbances or capacity constraints. That is why system operators who choose this technology will be well prepared when their communication needs multiply in the future.

Fiber-optic cables are laid underground to connect individual substations. This work is associated with heavy civil works, and therefore with great expense. However, when new power cables are installed, the cost-benefit analysis paints a clear picture. Fiber-optic cables should generally be the first choice in this case.

Benefits in detail
- At the core of a variety of communication systems, from passive optical networks (PON) to Ethernet and SDH
- Durable, insusceptible to electromagnetic disturbances
- Practically unlimited transmission capacity

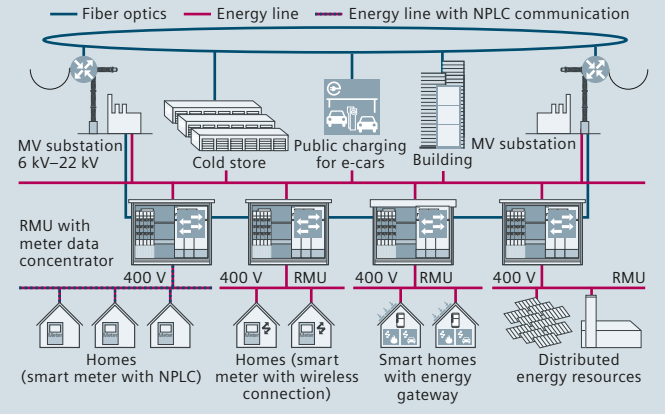


Fig. 8-5.2: **Fiber-optic infrastructure for distribution network**

Broadband power line carrier

For low-voltage to medium-voltage applications, using the existing power line

BPLC is an attractive alternative for many applications in medium-voltage and low-voltage Smart Grid scenarios.

It uses the utility-owned infrastructure in the distribution system, and thus has no continuous OPEX for the communication channel (operational expenditure). Therefore it is especially useful for connecting elements in the power supply system where there are no other communication media available.

Battery buffers allow the use of remote control with automation systems, even in cases of power loss.

Initially, the BPLC uses the medium-voltage lines between the distribution substation and the transformer substations as a communication infrastructure for process control in the medium-voltage domain.

In addition, the BPLC can use low-voltage lines as a communication infrastructure for applications linking the transformer substations and consumers/households (for example, the integration of smart homes). The BPL modules feature both IP and RS 232 interfaces, and can therefore be used flexibly for diverse communication applications. Transmission range and bandwidth are heavily depending on the quality and the age of the power cable. As a rule of thumb, if the bandwidth in MV systems is in the range of up to 5 Mbps, a distance of up to 1,5 km is possible.

WiMAX

For RMU backhaul and prosumers

The main application area for WiMAX is considered to be RMU backhaul. It also serves to connect scattered consumers or endpoints with more demanding communication requirements – in other words, prosumers.

WiMAX (worldwide interoperability for microwave access) is a standards-based telecommunication protocol (IEEE 802.16 series) that provides fixed and mobile broad-band connectivity. Originally designed as a wireless alternative to fixed network broadband Internet access, it has evolved over the past ten years into an advanced point-to-multipoint system that also supports mobile applications like workforce management. The technology is field-proven, globally deployed, and continues to evolve. WiMAX networks can be scaled from small to large, which allows for privately owned networks even on regional and local levels.

Detailed requirements as well as specific regional conditions and spectrum availability must be carefully assessed in order to select the best-suited technology and product combination from a wide variety of options.

Basic technical data

- Average data rate: ~10 Mbps;
  can be extended with IEEE 802.16m to over 50 Mbps
- Average coverage:
  up to 10 km in non-line-of-sight and
  up to 30 km in line-of-sight conditions
- Radio spectrum in licensed or license-exempt frequency bands

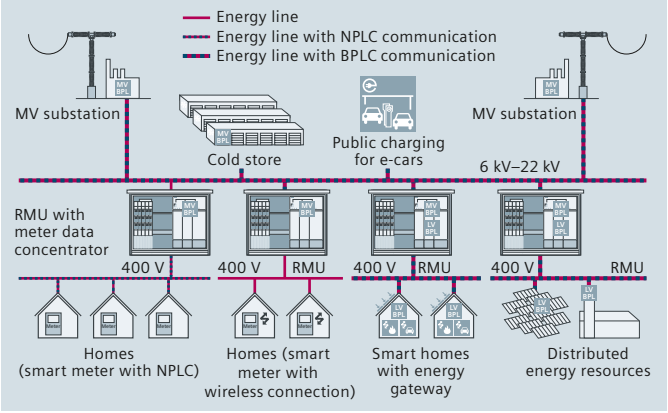


Fig. 8-5.3: **Broadband power line carrier for medium-voltage and low-voltage applications**

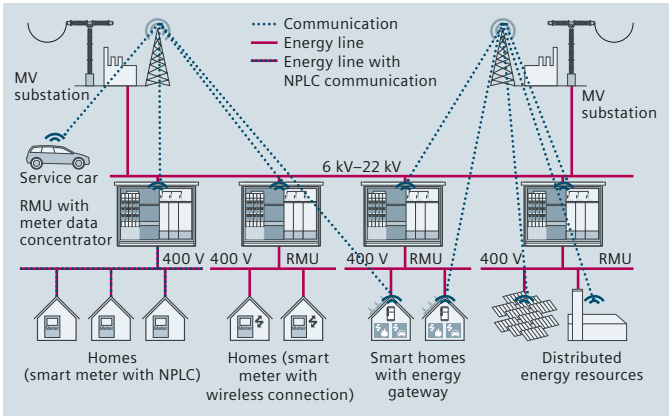


Fig. 8-5.4: **WiMAX network**

Wireless mesh

From consumer access to RMU backhaul

The applications for wireless mesh networks stretch from consumer access to RMU backhaul. Wireless mesh networks are composed of cooperating radio nodes organized in a mesh topology. The underlying technology for communication from one hop to another can be standardized (for example, the IEEE 802.11 series [Wi-Fi] or IEEEE 802.15.4 [low-rate wireless personal area network, LoWPAN]) or proprietary (for example, U.S. 900-MHz technologies). The mesh protocols and corresponding routing mechanisms are, on the other hand, more recent developments and therefore are still predominantly proprietary. Thanks to their mesh properties along with self-setup and self-healing mechanisms, mesh networks inherently offer ease of operation and redundancy for fixed applications – but performance is limited in terms of either coverage or bandwidth.

Detailed requirements as well as specific regional conditions must be carefully assessed in order to select the best-suited technology.

Basic technical data

- Average data rate per hop:
  from ~100 kbps (U.S. 900-MHz) up to ~10 Mbps (Wi-Fi);
  net data rates per hop decrease with increasing number of hops
- Average range hop-to-hop:
  ~1 km nLoS/~5 km LoS (U.S. 900-MHz);
  ~100 m nLoS/~1 km LoS (Wi-Fi) coverage extension by means of mesh
- Radio spectrum primarily in license-exempt frequency bands

Public cellular networks

For the extension of private communication networks

The main application areas for public mobile radio networks in the Smart Grid context are meter reading and energy grid monitoring functions.

In contrast to constructing new, proprietary networks for Smart Grid communication, there is also the option of using existing cellular radio networks owned by communication service providers. These networks are standards-based, deployed worldwide, and continuously upgraded and expanded. Activities like acquiring spectrum licenses, building, operating and maintaining the network as well as assuring sufficient coverage and bandwidth on a nationwide scale are naturally managed by the communication service providers. Data rates normally available range from 50 kbps (GPRS), over 10 Mbps (HSPA), to over 50 Mbps (upcoming LTE). Attractive data tariffs and the availability of the network are key to use public cellular networks for Smart Grid applications.

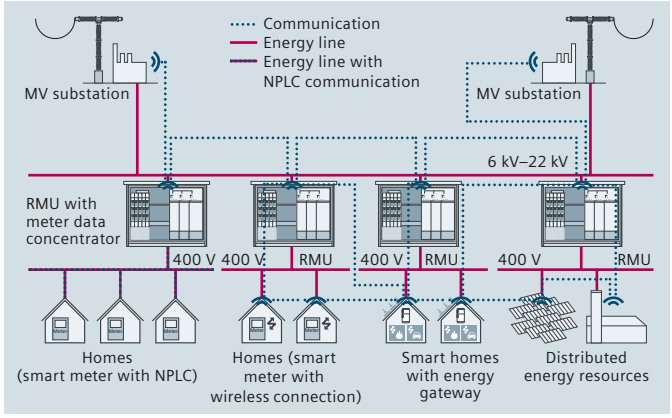


Fig. 8-5.5: **Wireless mesh network**

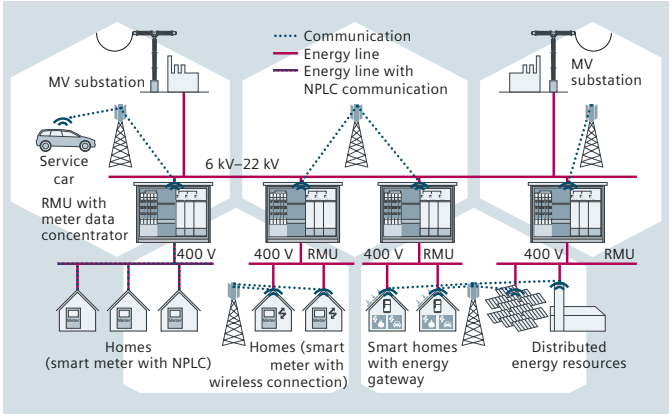


Fig. 8-5.6: **Public cellular network**

8.6 IT Security

If you imagine plant availability as an equation with a large number of variables, dependable IT security is one of the essential variables. It comprises, in particular, protection against unauthorized access, physical attacks and operator errors, as well as internal or external threats. What counts more than anything ultimately, though, is the result, namely a functioning energy automation system. That is precisely the philosophy of Integrated Energy Automation (IT Security). Integral solutions combine the individual variables to create a transparent equation that is maximized with regard to system uptime. With Integrated Energy Automation, Siemens offers an IT security concept that not only ensures the confidentiality and integrity of data, but most importantly its availability. Users profit especially from the simplified workflow, reliable operation and significantly reduced total costs of ownership.

8.6.1 Integral Approach

The graphical display of the security network or network blueprint, as it is called, forms the infrastructure and architecture of a system. It is the basis for a clear segmentation with which the risk for every link in the automation chain can be analyzed precisely – while still keeping an eye on the impact on the system as a whole.

The network is therefore divided up into manageable zones in order to equip them with precisely the IT security that is necessary and worthwhile in order to protect the data in this zone, as well as ensuring smooth operation of the system at the same time (fig. 8.6-1).

The zones are protected at network level by a SCADA firewall that controls data traffic between the zones and blocks dangerous packets. Suspicious network activities within critical zones themselves, for example, the control center network or field level can be detected and signaled by an intrusion detection system.

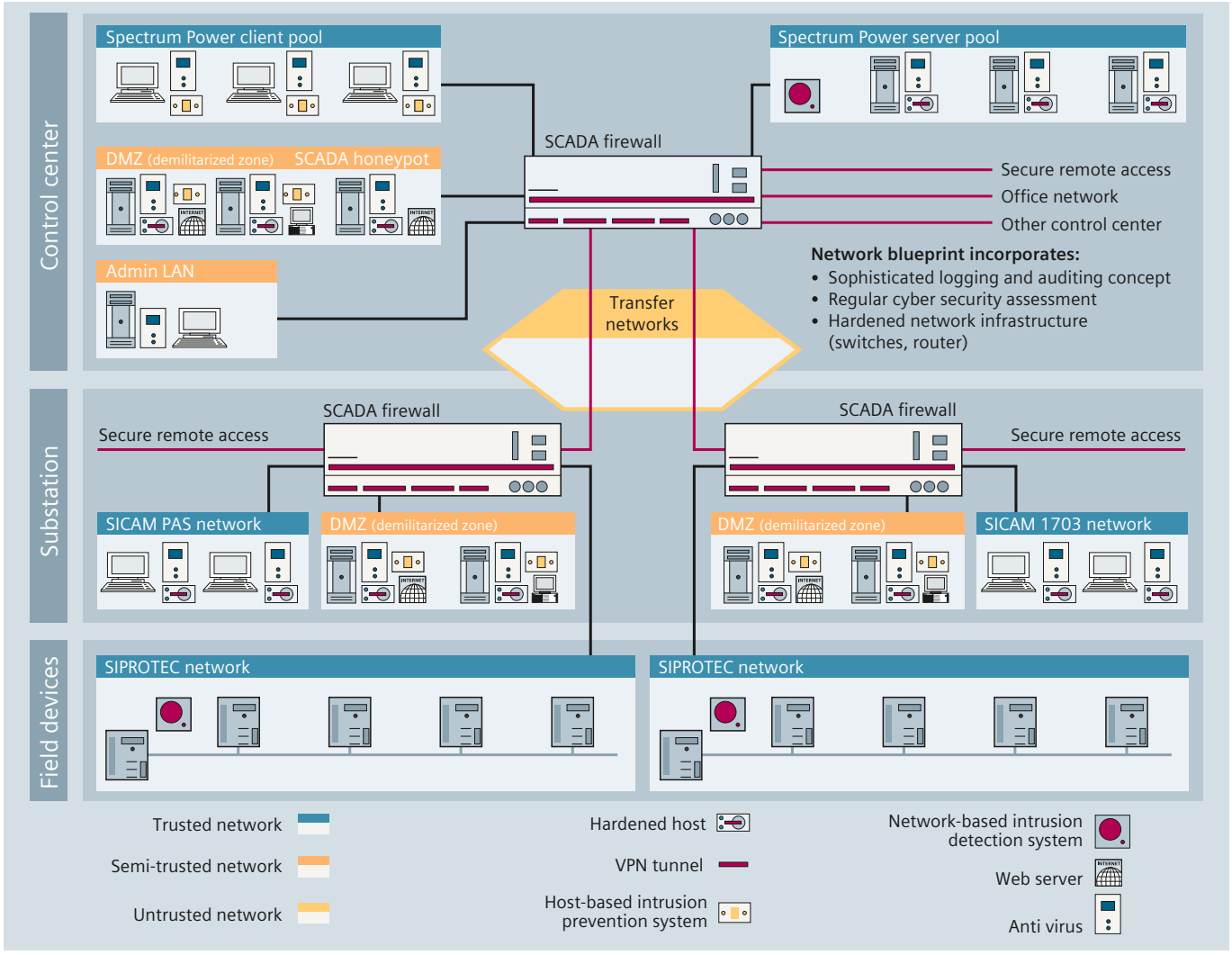


Fig. 8.6-1: **Zoned IT security concept**

Computers exposed to special risks, for example, in the demilitarized zone (DMZ), can also be protected with a host-based intrusion prevention system. All computer systems are equipped with virus scanners in order to withstand the permanent threat due to malware. The remote administration and connection of other networks is effected by VPN tunnels that guarantee access protection at the highest level.

The load-carrying network infrastructure itself (routers, switches) also undergoes system hardening in order to match up to the consistently high security requirements for the system as a whole.

8.6.2 Secure throughout from Interface to Interface

With the advent of the Internet and increasing networking within the systems, every interface represents a potential risk. These risks must be easy to estimate in the system. With Integrated Energy Automation, Siemens therefore applies the philosophy of IT security offering simple protection. For this reason, Siemens attaches greatest importance to homogenization by means of standardized and reproducible processes for authentication, authorization, intrusion detection and prevention, malware protection, effective patch management for third-party components, standard logging and continuous security tests.

8.6.3 Continuous Hardening of Applications

Reliable products are an essential basis for a secure network. Siemens therefore continuously hardens its products to protect them against attacks and weak points. Individual risk analyses and regular tests – also specially for third-party components – with a defined combination of IT security test programs for detecting weak points (Test Suite) are used for this.

8.6.4 In-House CERT as Know-how Partner

Siemens has its own in-house Computer Emergency Response Team (CERT). An organization such as this that discusses subjects critical to IT security and issues current warnings is normally only maintained by universities or governments in order to provide users with cross-industry information.

The Siemens in-house CERT was established in 1997 and since then has issued warnings about security loopholes, while offering approaches for solutions which are processed especially for the company's areas of competence. As know-how partner, the work of the Siemens CERT also involves drawing up rules for the secure development and programming of in-house products and the continuous further training of in-house programmers.

CERT checks the products for weak points by means of selective hacker attacks. The team also collects and distributes reports on weak points and upgrade reports for third-party components and links them to recommendations, concrete proposals and implementation specifications.

8.6.5 Sensible Use of Standards

The object of standards is to guarantee quality, to increase IT security in the long term, and to protect investment. There are now hundreds of IT security standards in existence, but only some of them are really necessary and worthwhile for a system.

On the basis of its many years experience in the market, Siemens chooses those standards and guidelines that protect a network reliably and effectively. This also includes advising customers on which IT security standards need to be observed at international and also at regional level.

The object of Integrated Energy Automation (IT Security) is permanent IT security for the system in the long term. Therefore reliable and secure products and infrastructures are not enough. With Integrated Energy Automation, Siemens also implements appropriate security processes that ensure that IT security is actively implemented throughout, both internally and at the plant operator's, and is guaranteed over the entire life cycle of the plant.

8.6.6 IT Security Grows in the Development Process

The integral approach with Integrated Energy Automation not only involves keeping an eye on the entire system, but also means that security of products is already integrated in the entire development process, and not just in the test phase.

IT security guidelines for development, processing, service and other functions ensure that IT security is actively implemented throughout all processes. Examples of this are security briefings for product management before a product is developed or programmed in the first place. Programmers operate according to defined guidelines for secure coding, which are specified by the Siemens CERT.

For an effective patch management, Siemens tests updates of third-party security products, for example, firewalls, already in the development process of the products. Continuous penetration tests of all relevant products are stipulated in a test plan. This also includes the definition and establishment of a security test environment and matching test cases.

In this way, Siemens subjects its products to an objective and critical certification process with which IT security is guaranteed and made transparent on the basis of suitably selected standards.

8.6.7 Integrating IT Security in Everyday Operations

A system is only as secure as the user operating it. A high standard of security can therefore only be achieved by close cooperation between manufacturers and operators. The patch management process is also important after acceptance testing of a system. For this purpose, the Siemens CERT issues automated reports on newly discovered weak points that could affect third-party components in the products. This enables the Siemens customers to be informed promptly, and allows time to define any service activities arising from this.

A very wide choice of helpful tools is available to enable users to make IT security a regular part of everyday operation of a system. Standardized security processes, for example, for updates and system backups, are implemented directly. At the same time, efficient tools are provided for administering access in a system network. This includes effective management of rights as well as reliable logging tools. Automatically created protocols or log files are not only stipulated by law, but also help determine at a later time how damage to a system occurred.

With Integrated Energy Automation, Siemens offers an intelligent interaction of integral solutions for simple and reliable energy automation.

8.7 Services

Business with communication solutions for power supply companies does not only mean to provide state-of-the-art products, but to offer a complete range of build and professional services. With more than 75 years of experience and know-how, Siemens offers a wide range of products for communication solutions, and a comprehensive portfolio of services tailored to the demand of our customers (fig. 8.7-1).

Consult
Finding the right communication solution in a pre-sales or after sales phase for the costumers requires planning and analysis. Siemens consultants offer every support in planning and realization of the best technical and economic solution for communication networks, system configuration, and integration of the new equipment into the existing network.

Design
Designing a telecommunication network means much more than just supplying hardware and software. The Siemens experience makes it possible to create a and prove a communication solution designed exactly for the operator's purposes.

Build
The fast implementation of a project depends crucially on effective management. It ensures that the build-up of a network will be completed quick and effective.

Maintain/Care
The Siemens hotline, its technical level supports, and repair and replacement concept for defective modules as part of the after-sales service, gives full support and provides the required hardware and software for updating or upgrading communication systems already in operation in existing networks.

Educate
Well-trained staff that knows how to bring the communication network to its optimal use is crucial in obtaining the full benefits from the investments. Siemens therefore focuses not only on providing custom-made communication network solutions, but also on sharing its knowledge and experience with its others. Siemens offers a comprehensive training program for the complete area of communication solutions for power supply companies. Training is always tailored to the area of responsibility, as well as to the corresponding technology and practice.

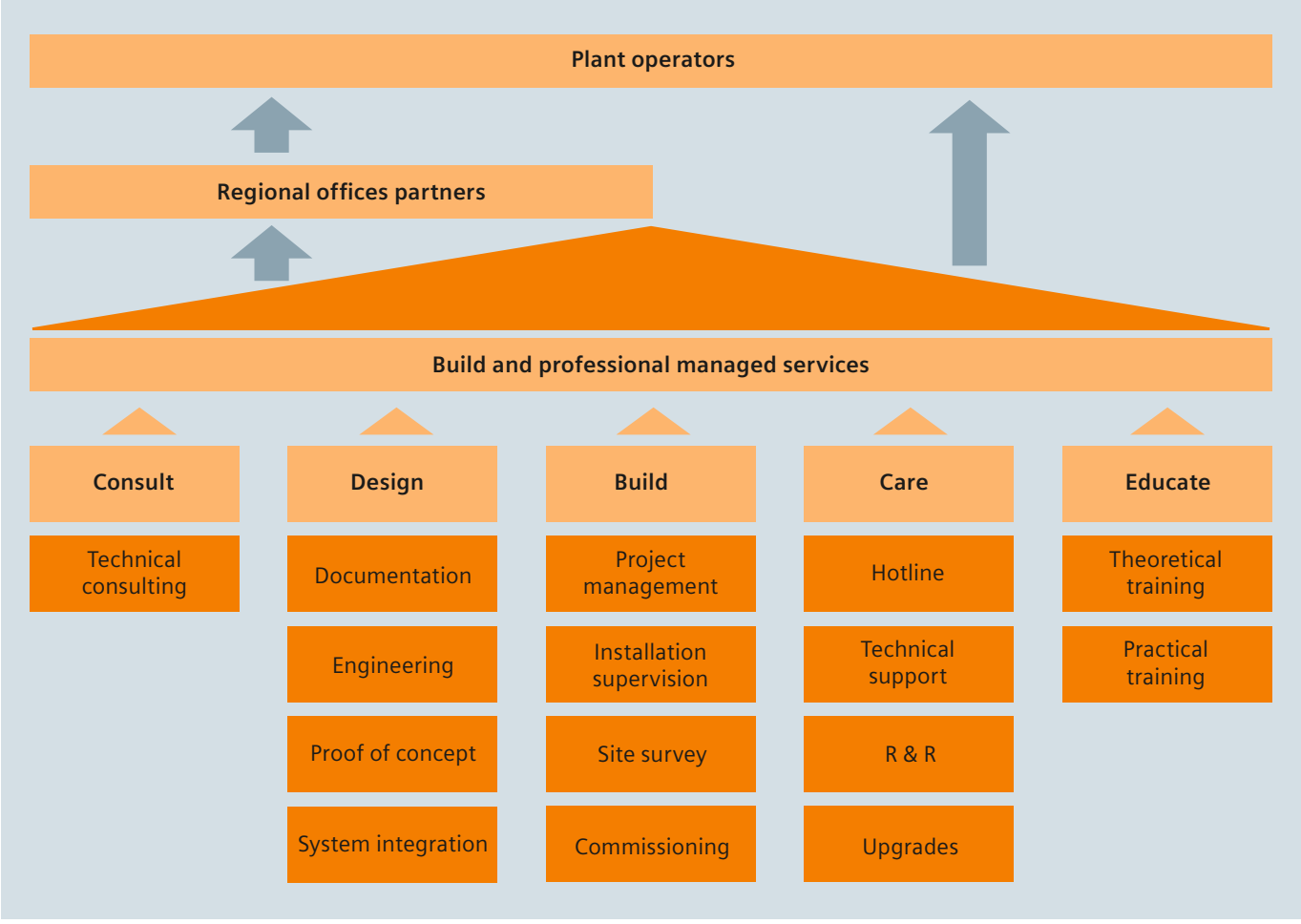


Fig. 8.7-1: **Service portfolio**