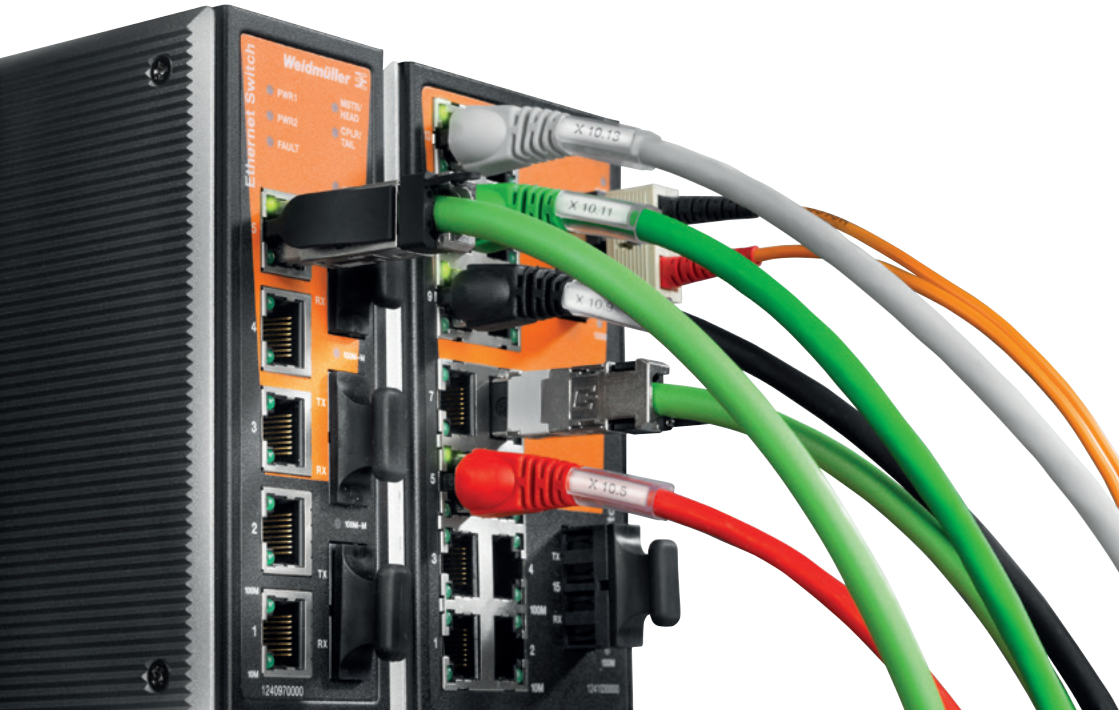
Weidmüller

Industrial Ethernet Handbook

A practical guideline

Planning – Installation – Start-up



Preface

Revision History

Version	Date	Modification
0.0		First edition
1.0	10/11	Updated version
2.0	11/12	Updated version

Contact address

Weidmüller Interface GmbH & Co. KG
P.O. Box 30 30
32720 Detmold
Klingenbergstraße 16
32758 Detmold
T +49 5231 14-0
F +49 5231 14-292083
info@weidmueller.com
www.weidmueller.com

Contents

1 Introduction

1.1 Objectives of the best practice guideline

This guideline is intended for planners, installation engineers and startup engineers for Industrial Ethernet (IE) networks. It communicates, from experience, tips, tricks and shortcuts that make the work easier. This guidelines is not an IE compendium from a basic manual.

1.2 We value your opinion!

We have selected and consolidated elements of our best practices in the best possible format - it is not in a final or complete form. Is there anything missing? You can help us to improve this best practice guideline even further. Send us your experience, opinions, tips, tricks and also any questions you may have to ethernet@weidmueller.com.

1.3 Disclaimer

To the best of our knowledge, all information has been included in the preparation of this best practice guideline. At the same time, deviations cannot be excluded, and we cannot accept any liability for complete conformity. In addition, we do not accept any warranty for the currency, accuracy or completeness of the information provided.

1.4 Weidmüller – Partner of Industrial Connectivity

As experienced experts, we support our customers and partners around the world with products, solutions and services in the industrial environment of power, signals and data.
We are at home in their industries and markets and are aware of future technological challenges. We are therefore continuously developing innovative, sustainable and value-adding solutions for their individual needs. Together we set standards in industrial connectivity.

1.5 Office Ethernet and Industrial Ethernet

Why Industrial Ethernet is necessary

Unlike fieldbus systems, Industrial Ethernet offers significant advantages:

- Integrated communication from the machine to the office
- No gateways required at transition from field level to office
- Remote diagnostics and monitoring through Internet connection
- Advantageous assignment of stations using virtual private networks (VPNs)

Ethernet requirements in the office and industrial area

	Office Ethernet	Industrial Ethernet
Cabling	• Fixed building installation • Variable connection options • Pre-assembled connecting lines • Star topology is the most common type	• Individual plant-influenced networks • Robust components • Connections that can be assembled on-site • Redundant network topologies (ring)
Cont.'d	• High data traffic • Moderate network availability • Mostly only acyclic transmission • No real-time behaviour required for standard applications	• Small data packets (measured values) • Very high network availability • Mainly acyclic transmission • Extremely high real-time requirement
Environment	• No extreme conditions	• Extreme temperatures • Dust, dirt, water splashes, oils, gasses, vibration • Electromagnetic fields • Hazard and damage from mechanical or chemical load

1.6 Explanation of symbols

The following symbols are used in this best practice guideline to highlight key sections of text:

Symbol	Meaning
	This symbol provides you with notes and tips that will help you make your work easier.
	This symbol indicates the danger of faults. Observing these notes will help you reduce faults.

2 Planning

This chapter includes, among other things:
- Planning basics, requirements and planning guidelines
- Requirements for generic communication cable facilities
- Fire protection and surge protection
- Ethernet protocols
- Description of active Ethernet components
- Description of passive Ethernet components

2.1 Basic ideas on planning an Industrial Ethernet network

2.1.1 Data and control networks

First decide whether you are planning a data or a control network.

Data network:
- Large volume of data
- Open connection to the office network
- The transmission time is relatively non-critical.
- Typically, works with Standard Ethernet protocol (TCP/IP)
- Availability and redundancy are focused on the server.

Control network:
- Low volume of data
- Highly controlled restrictions for connection to the office network
- High real-time requirements
- Special network protocols (PROFINET, EtherNet/IP, Modbus/TCP ...)
- Availability and redundancy are extremely critical at all levels of the network.

2.1.2 Devices for external connection

Designate the end devices and their access points (I/O modules etc.).

1. Designate the number and spatial arrangement of the I/O modules.
2. Define the terminals: exactly which terminals are required? In which protection degree: IP 20, 54, 67...?
3. Data volume of the terminals: define this at this point for the later determination of the network equipment.
4. Define the connections to external networks.
5. Define the connections to the Internet.
6. **Define the remote maintenance access (e.g., via modem).**

2.1.3 Network structure

Here, you should define the complete structure which will be used to co-ordinate the components later on.

Main networks and subnetworks

If necessary, subnetworks can be operated at a lower speed depending on the volume of data. For example, the backbone (main line) can be operated with Gigabit Ethernet and the subnetworks with Fast Ethernet.

Collision domains (CSMA and CD)

A collision domain is an interface in a network at which there is the possibility of collisions. When, for example, several PCs are connected in series, collisions can occur if two PCs attempt to transfer data in parallel to each other. Such collisions can be avoided by using a router or switch which provides a separate port for each PC. In the case of real-time applications, special attention must be paid to avoiding collisions and thus time delays.

Address areas

IP address

The IP address is comparable to a street address (street, house number). The IP address is used to clearly identify a PC in the network. Each IP address can only be assigned once in a network.

IP-address structure

An IP address consists of 4 bytes = 32 bits, each byte can adopt its own value between 0 and 254. Represented in decimal form, the IP address is divided into four octets.

Example: 192.168.2.1

IPv4

Since IPv4 uses 32-bit addresses, a maximum of 4294967296 unique addresses are possible.
Since 8 bits are available per block, the value range per block is from 0 to 255.

Example: 192.168.2.1

A defined method from the office area generally exists. You should take this over for reasons of consistency. In each case, co-ordinate the address area with the IT department in order to avoid complications later.

Redundancies

Redundancies increase the availability of networks.Redundancy can relate to devices on the one hand, and to cabling on the other. Redundancies in the device require special components in every case. This is always vendor-specific and is not to be found in any standard. Redundancies for cabling are more common. For this you can select between the standardised redundancy methods STP, RSTP as well as vendor-specific methods.

Determine:

- Which components are are networked redundantly
- The art of redundancy:
- Standardised (STP, RSTP):
  The advantage of this method is that it is supported by many managed switches.
  The disadvantage is the sometimes very long recovery times
- Vendor-specific:
  The advantage in this case is the significantly shorter recovery time.
  The disadvantage is that these protocols are only supported by one or a few manufacturers and not compatible with each other.

2.1.4 Network devices

Define all infrastructure components by their functionality and select the required devices.

1. Take into account the existing control cabinet and, if necessary, define additional distributions.
2. Definition of network access and partitioning of the network (router, modem ...)
3. Definition of coupling elements: always plan at least 20 percent reserve on the ports for future expansions.
   - Unmanaged switches
   - Managed switches
   - Uplinks
4. Define the WLAN access:
   - WLAN bridges
   - WLAN access points and slaves
5. Integrating sub-systems:
   - COMServer
   - Gateways
6. Selecting the devices according to customer specification or user-group guidelines
7. Determining the power requirement and the power supplies.

2.1.5 Network connection technology

1 Determine the mode of installation.
- Cable routes and cable channels
- Additional protective measures against mechanical damage

2 Determine the cabling requirements.
- Standards
- Transmission rates: the requirements for shielding and number of wires change according to transmission rate.
- Cable lengths
- Electromagnetic requirements (MICE): the sheath-material and shielding requirements depend on these.

3 Determine the connector requirements
- Standards
- Transmission rates: this gives the required connector class (Cat. 5, 6_A) and also the connector type.
- Cable requirements: depending on the cable, certain connector requirements have to be met (shield connection, external diameter, possible wire insulation and wire diameter).
- Electromechanical requirements (MICE): this results in the requirements for shielding and protection degree.
- Size

4 Select additional connecting components:
- Patch distributor
- Media converter
- Converter from a solid to flexible conductor (e.g., terminal rail outlets)

2.2 Planning guidelines

Planning according to the applicable standards is the basis for trouble-free and durable operation of the Ethernet network. The execution, along with later use, is defined here.

- Observe the corresponding DIN regulations (safety, EMC).
- (DIN) EN 50173 is vital for cabling that is not application-specific, and (DIN) EN 50174 is important for communication cables in general.
- Observe the cable's minimum bending radius.
- Use only suitable installation systems.
- It is not permitted to route copper communication cables together with high-power cables. Comply with the separation spacing as outlined in the EMC conditions in the environment (see DIN EN 50174-2).
- Verify the quality requirements by measuring and logging according to the standards and using the correct engineering practice.

2.3 Requirements for communication cable installations that are not application specific

2.3.1 International standards

	Office buildings	Industry
	ISO/IEC 11801	ISO/IEC 24702

2.3.2 German and European standards

	Office buildings	Industry
	(DIN) EN 50173-1 in conjunction with (DIN) EN 50173-2	(DIN) EN 50173-1 in conjunction with (DIN) EN 50173-3

2.3.3 Equivalent American standards

	Office buildings	Industry
	Standards series ANSI/TIA/EIA 568	

2.3.4 Structure of generic communication cable systems

Primary area (Campus Distributor)
- Cabling of individual buildings together at the same site

Secondary area (Building Distributor)
- Vertical storey cabling

Tertiary area (floor distributor / machine distributor)
- Cabling to the end user
- Cabling to a machine and inside a machine

2.4 EN 50174-2 Information technology – Installation of communication cabling

EN 50174-2 contains requirements for planning and implementing a cabling.

2.5 MICE matrix

The MICE matrix according to (DIN) EN 50173-1 covers the environmental requirements for cabling.
Ambient conditions are classified by:

Mechanical	Mechanical properties
Ingress	Sealing properties
Climatic/Chemical	Climatic/chemical properties
Electromagnetic	Electromagnetic properties

There are three different degrees of severity:
1 – Generally sufficient for office environments
2 – Generally sufficient for light industry
3 – Sufficient for heavy industry

	Class		
Mechanical	M1	M2	M3
Protection	I1	I2	I3
Climate	C1	C2	C3
Electromagnetic	E1	E2	E3

M_1 I_1 C_1 E_1: Office, master office, office container
M_3 I_1 C_1 E_1: Connection in enclosed control cabinet
M_3 I_3 C_2 E_3: Connection in field area

Observe special environments such as mining, petrochemicals, tunnels, pipelines etc. The MICE classification is not valid for these.

2.6 Power capability of the cabling

Both IEC 11801 and EN 50173 contain a classification of symmetric copper cabling. To date, classes A-F have been described. As a rule: the higher the class the better the quality of transmission of the cable.

General transmission path classes for industrial applications

Class D – specified up to 100 MHz;
frequently used transmission route with capacity for 100 Mbps or 1,000 Mbps

Klasse E – specified up to 250 MHz;
Transmission routes with capacity for 100 Mbps, 1,000 Mbps and additional capacity reserves

Klasse E_A – specified up to 500 MHz;
Transmission routes with capacity for 100 Mbps, 1,000 Mbps and 10 Gbps

Advantages of Gigabit Ethernet

- Higher data rates for higher network performance
- Full downward compatibility with the large number of installed Ethernet and Fast-Ethernet nodes

Currently, more and more 10-Gigabit components are coming onto the market at prices comparable to Gigabit components. Make use of these components to make your network viable for the future. This will also allow you to integrate bandwidth-hungry image processing and video components into your network, in step with technical advances.

2.7 Assembling generic cabling

Generic cabling can be assembled using:

- components identified at planning stage (cables, connection technology) or
- Use of standardised components

2.7.1 Standardised components

Standardised components are divided into quality categories (also Cat.).

Standard categories for industrial applications:

- Category 5 – Parameters specified up to 100 MHz
- Category 6 – Parameters specified up to 250 MHz
- Category 6_A – Parameters specified up to 500 MHz

The integrated use of components of

- Category 5 results in Class D
- Category 6 results in Class E
- Category 6_A results in Class E_A

When categories are mixed, the following applies: the components with the lowest category determine the class of connection or the class of the network.

Cable category	Connector category Cat. 5	Cat. 5e	Cat. 6	Cat. 6_A	Cat. 7	Cat. 7_A
Cat. 5	Class D 1995	Class D 1995	Class D 1995	Class D 1995	Class D 1995	Class D 1995
Cat. 5e	Class D 1995	Class D 2002	Class D 2002	Class D 2002	Class D 2002	Class D 2002
Cat. 6	Class D 1995	Class D 2002	Class E	Class E	Class E	Class E
Cat. 6_A	Class D 1995	Class D 2002	Class E	Class E_A	Class E_A	Class E_A
Cat. 7	Class D 1995	Class D 2002	Class E	Class E_A	Class F	Class F
Cat. 7_A	Class D 1995	Class D 2002	Class E	Class E_A	Class F	Class F_A

2.7.2 Cable lengths for copper cabling

Using components that meet the minimum requirements for standardised components, a length of max. 100 metres can be achieved for the entire copper connection between devices/distributors.
The following applies in this case:

	5 m	Connecting cables
+	90 m	Installation cable
+	5 m	Connecting cables
=	100 m	Cable run length

- Longer cable runs can be achieved using higher quality components. However, these are outside of the specification.
- If you use longer patch cable, the length of the cable installation does not decrease linearly, but can be disproportionate (please note in (DIN) EN 50173-1/ IEC 11801 “Table 21 horizontal link length equations”).

2.7.3 Cable lengths for fibre-optic cabling

Determining the cable length of fibre-optic cables is more time-consuming and dependent on various factors. Put simply, all attenuations that affect the fibre-optic cable run must be lower than the power budget of the active devices.

$$\text{Power budget} \geq \sum \text{Attenuation}_{\text{connector}} + \sum \text{Attenuation}_{\text{splices}} + \sum \text{Attenuation}_{\text{cable}} * \text{Cable length}$$

- Power budget: difference between the capacity of the output signal of device 1 and the readable input capacity of device 2 (e.g.: 4 dB with Multimode)
- Attenuation $_{\text{connector}}$: the attenuation of all connectors of the transmission path (depending on the plug type, in each case approx. 0.3 dB)
- Attenuation $_{\text{splices}}$: the attenuation of all splices along a transmission path (in each case approx. 0.1 to 3.0 dB)
- Attentuation $_{\text{cable}}$: the attenuation of the cable depending on the wavelength of the light (e.g.: 1.5 dB/km at 1,300 nm wavelength of a Multimode fibre)
- Cable length: length of the cable in km (e.g.: 1.2 km)

For example, the result could be as follows for the above equation:
4 dB ≥ 2 * 0.3 dB + 2 * 0.1 dB + 1.5 dB/km * 1.2 km = 2.6 dB
→ the cable length fits

2.8 Electromagnetic compatibility (EMC)

2.8.1 Equipotential bonding and earthing system

	**CAUTION! EMC**
	An equipotential bonding system that meets the current standards is an absolute must for good EMC and, in particular, for an adequate **protection against personal injury**.

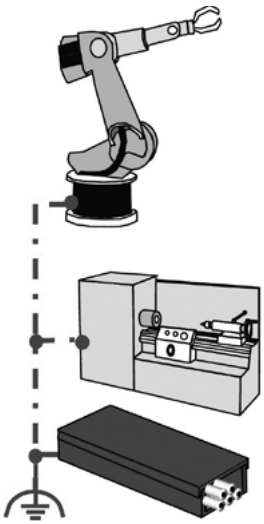
Requirements for equipotential bonding and earthing systems are described mainly in:

- DIN VDE 18014
  Requirements for foundation earths
- (DIN) VDE 0100 540
  Installing low-voltage systems
- (DIN) EN 50310 (DIN VDE 0800 2 310)
  Use of measures for equipotential bonding and earthing in buildings with IT installations

Connect metallic conductive cable raceways with the building's equipotential bonding system.

For this, observe the notes on equipotential bonding in Section 2.9.

(Source: PROFINET-Installation Guideline, Version 1.0, January 2009)



2.8.2 EMC – general

Select suitable materials and make sure that installation is professionally executed, in order to ensure the compatibilty properties of the EMC.
Observe the following EMC standards for the operation of the system:

- (DIN) EN 55022 [13]
  Limits and measuring methods for radio interference of IT installations
- (DIN) EN 61000-6-1 [19]
  Generic standard; interference immunity for residential areas, office and commercial areas, as well as small enterprises
- (DIN) EN 61000-6-3 [20]
  Generic standard; emitted interference for residential areas, office and commercial areas, as well as small enterprises

(DIN) EN 55022, (DIN) EN 61000-6-1 and (DIN) EN 61000-6-3 are valid in all cases for the operation of LANs.

CAUTION! EMC

Use fibre-optic cables (FO cables) in areas with a higher EMC. POF or Multimode cables with SC-Duplex- or SC-RJ connectors are recommended in particular.

2.9 Earthing and equipotential bonding

A good earthing system and good equipotential bonding system are very important for the electrical interference immunity of PROFINET networks. Earth the PROFINET cable shields on both sides, i.e. on each of the connected devices, in order to reduce the effects of electromagnetic interference. The equipotential bonding ensures that the earth potential is equal throughout the entire PROFINET network. This protects against equipotential bonding currents that could otherwise flow over the shielding of the PROFINET cable. The following explanations provide basic information on installing the earthing and the equipotential bonding.

Manufacturer's instructions
Please read the information provided by the manufacturer. This information provides you with important details on how to best connect the PROFINET stations with the earthing and the equipotential bonding.

2.9.1 Protective earth

The protective earth is essentially used to protect people against an electric shock in the event of a fault. However, the protective earth also protects machines and installations against damage from faults. Metallic conductive parts, such as frames, control cabinets or plant parts must be connected to the protective earth. The conductor used must be measured so that it can discharge residual current in the event of a fault.

The protective earth is designated by the following symbol:

Since the protective earth is part of the general electrical system, it will not be described in any more detail in this document. However, the applicable regulations are to be observed in each case!

Note
Some PROFINET devices also have a connection for the protective earth. In particular, these are PROFINET devices that have an additional power supply with a higher voltage. Connect the protective earth in accordance with the applicable regulations.

2.9.2 Functional earthing

The functional earth is used to discharge EMC interference to earth. This increases the interference immunity of the data transmission. The functional earth is used to earth the cable shields and housing of devices in order to discharge interference to earth.

Manufacturer's instructions
Read the manufacturer's documentation. The manufacturer information gives you details about how you need to connect the PROFINET nodes in terms of earthing and equipotential bonding

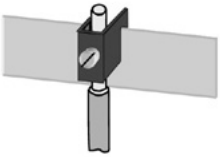
Some PROFINET devices have a connection terminal for the functional earth. The connection terminal is marked with the symbol for the functional earth. To connect the connection terminal of the PROFINET devices to the functional earth of the system, use a cable that has the shortest possible length and a large cross-section. In many cases the entire metallic structure of the system is used as functional earth. With other devices, the functional earth is implemented by means of the installation fastening. Therefore, also connect the system's top-hat rails to the functional earth.

For the earth connection of the PROFINET devices, use copper cable with a corresponding cross-section (> 2.5 mm²). As a rule, the earthing cable has a green-and-yellow insulation. In some countries the green-and-yellow marking is a regulation (in the USA only green).

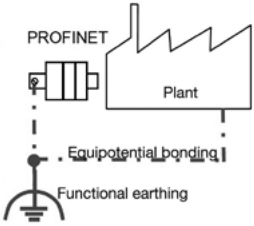
The functional earth is identified by the following symbol:

2.9.3 Equipotential bonding

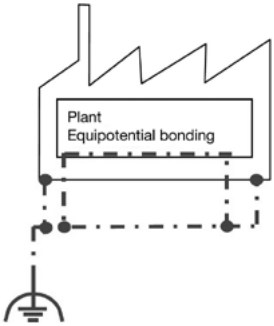
Equipotential bonding ensures that the earth potential is equal throughout the system. This means no compensating currents flow over the shielding of the PROFINET cable. Use copper cable or galvanised earthing strips for the equipotential bonding in the system and between the system parts.



Connect large areas of the equipotential bonding with the earth terminal or earth bus.



Connect all shields and earthing connections (if any). As the name indicates, the equipotential bonding ensures that the potential is equal in all parts of the system. This prevents compensating currents from flowing over the shielding of the PROFINET cable.



Connect the installation surfaces (e.g., top-hat rails) to the equipotential bonding.

Connect the system's equipotential bonding as often as possible with the building's equipotential bonding.

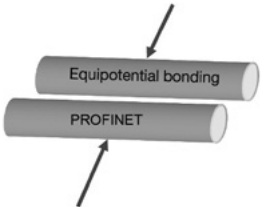
In the case of painted parts, remove the paint from the connection point prior to connecting.

After installation, protect exposed connecting points against corrosion, using zinc paint or enamel.

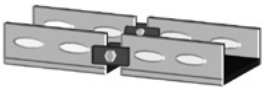
Protect the equipotential bonding against corrosion. One option, is to paint the contact points.

Use secure screw or clamp connections. Under no circumstances should the connection come loose on its own.

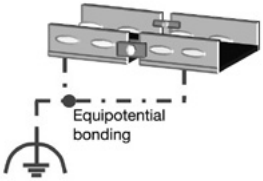
Make sure to use wire-end ferrules or cable lugs for flexible equipotential bonding cables. Under no circumstances should the cable ends be tin-plated (as this is no longer permitted)!



Install the equipotential bonding as close as possible to the PROFINET cable.



Connect all individual parts of the cable raceways (metal) with each other. Use special-purpose connecting material to do this. Make sure to use the same material for the cable raceways and the connecting pieces. Appropriate material is available from manufacturers of cableways.



Connect the metallic cableways as often as possible with the equipotential bonding.

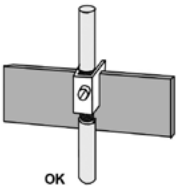
Use expansion or articulated joints for flexible earthing strips. Earthing strips are usually available from cable manufacturers.

Fibre-optic cables are used for the connection between various buildings or building sections. Owing to their insensitivity to EMC loads, no equipotential bonding is required for these fibre-optic cables, provided they contain no metal.

2.9.4 Connect the shielding with the equipotential bonding.

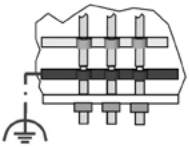
The shielding is an important part of the PROFINET copper cable.
This shielding protects the data wires in the cable against electromagnetic interference.
For the shielding to perform this function, it must be connected to the equipotential bonding of the system.
Connect the shielding of the PROFINET copper cables to the equipotential bonding at the following points:

- **At PROFINET devices**



The equipotential bonding is implemented using the appropriate connector and by connecting the cable to the equipotential busbar.

- **At the cabinet entry**



Connect the shielding of the PROFINET cable to the equipotential bonding at the entry to the control cabinet. This means that interference that acts on the PROFINET cable outside the control cabinet is prevented from being directed into the cabinet.

To achieve this, mount an equipotential busbar behind the strain-relief on the cabinet entry.

2.9.5 Connect the shielding to the equipotential bonding

Various options are available to create a connection between the shielding and the equipotential bonding. The following figure shows you three such connection options. These options have been tried and proven in practice.

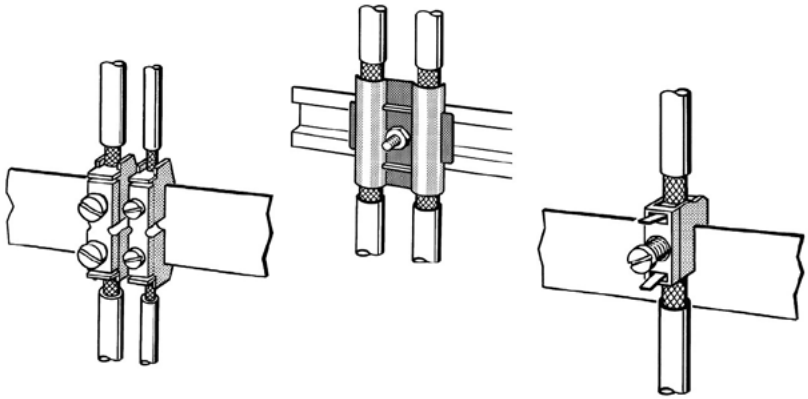
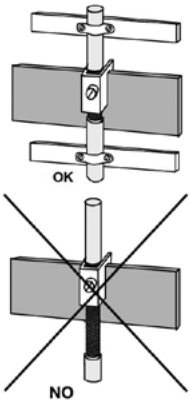


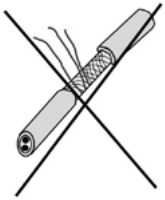
Figure 2.1: Connections between shielding and equipotential bonding

Make sure that the PROFINET cable is not pinched by the connection between the shielding and the equipotential bonding. Use shield contact clips that fit the cable diameter. Pinching can impair the electrical properties of the PROFINET cable.

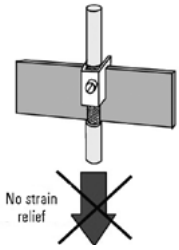
When installing the shielding connection, observe the following:



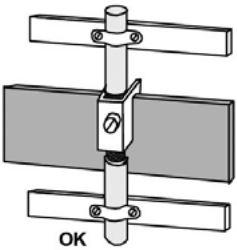
Remove the sheath of the PROFINET cable only to the extent required for the connection. The PROFINET cable is sensitive to mechanical loads in the area where the sheath was removed.



Make sure you don't damage the shielding when you strip the sheath off the PROFINET cable.



Do not use the shielding connection as strain-relief. This would impair the contact between the shielding and the equipotential bonding. Exception: installation material specially designed for this purpose.

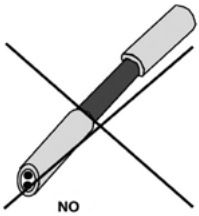


Fasten the PROFINET cable in place before, and after, the shield laying. This protects the sensitive PROFINET cable against kinking and bending in this area. This is particularly important if the cable is subject to movement.

Use only connecting materials that fit the diameter of the stripped cable.

Do not mount the equipotential busbar on painted surfaces. Galvanised or chromium-plated surfaces are very suitable for mounting.

Use tinned, galvanised or other electroplated installation material. This is protected against corrosion and provides a durable and good contact.



Only use the shielding braid to provide the contact between the shielding and the equipotential bonding. PROFINET cables also have a foil shield. It is not permitted to use this for the connection. To improve stability, it is generally plastic coated on one side. The plastic coating has an insulating effect.

Source: PROFINET-Installation Guidelines Version 1.0, January 2009)

2.10 Surge protection

Surge voltages are extremely high voltages that can interfere with or even destroy the insulation and function of electrical and electronic components.
Your machines and systems are therefore safeguarded against:

- Lightning strikes
- Switching operations (direct and indirect effects)

Be sure to:

- Spatial separation of systems that have different rated voltages
- The correct protection classes of surge protection modules

2.10.1 Protocols (Ethernet)

Use Industrial Ethernet protocols. This ensures the real-time behavior and determinism in your plant. The most common protocols are:

- PROFINET
  http://www.profibus.com/pn
- EtherNet/IP
  http://www.odva.org
- EtherCAT
  http://www.ethercat.org
- Ethernet Powerlink
  http://www.ethernet-powerlink.org
- Modbus TCP

http://www.modbus.org/

2.11 Fire protection and fire load

Fire protection

The main causes of fire in electrical lines include:

- Short-circuits and earth faults, e.g. on mechanical or thermally damaged cables or lines
- Faulty electrical connections (loose contact)
- Previous damage to insulation
- Overload
- Heat accumulation

Note:

- Install large quantities of cables in the space above suspended ceilings or the space below raised floors.
- Use cables whose sheath is made of zero-halogen, non-corrosive, flame-retardant, low-smoke and low-gas materials.

Fire load/fire propagation

Fire load is the combustible energy of a cable.

Fire propagation describes the behaviour of the cable in the event of a fire:

- Good fire propagation means the fire can be spread by the combustible material of the cable in the event of a fire (like an igniter cord).
- Poor fire propagation (desirable) is achieved by using materials that have a low combustible energy.
- Calculate and document the fire load of the cabling in every zone.

	**CAUTION!**
	Observe the local fire and building regulations!

IP protection class

Electrical devices that are intended for use in industrial environments are subjected to influences other than household appliances.
The following table shows the protection classes with the associated limit values. The protection classes are defined in the IP standard, DIN EN 60529: protection degree provided by housing (IP code).

Table 2.1: Protection degrees against solid foreign matter

Code number	Term - explanation
0	Not protected
1	Protected against solid foreign matter, 50 mm diameter and larger
2	Protected against solid foreign matter, 12.5 mm diameter and larger Example: the air slots in a PC power-supply-unit housing.
3	Protected against solid foreign matter, 2.5 mm diameter
4	Protected against solid foreign matter, 1 mm and larger
5	Dust-protected: Penetration of dust is not completely prevented, but dust may not penetrate to such an extent that the operation of the device or the safety is impaired.
6	Dust-tight: No penetration of dust at a pressure of under 20 mbar in the housing

Table 2.2: Protection degrees against water

2. Code number	Term - explanation
0	No protection
1	Protected against dripping water: vertically falling drops may not have any damaging effects.
2	Protection against dripping water, when the housing is inclined by up to 15°
3	Protected against spray-water: water that is sprayed at an angle of up to 60° on both sides of the vertical may not have any damaging effects.
4	Protection against splashing water: Water that is splashed from every direction against the housing may not have any damaging effects.
5	Protection against water jets: Water that is directed as jets from every direction against the housing may not have any damaging effects. Note: corresponds to approx. 12.5 litres/minute (garden hose) Test period approx. 5 minutes (all information subject to correction).
6	Protection against strong water jets: Water that is directed from every direction as strong jets against the housing may not have any damaging effects.
7	Protection against the effects of being temporarily submersed in water
8	Protected against the effects of being submersed in water for a long period of time. An additional specified number indicates the submersion depth.

2.12 Quality planning

Basic requirements for the quality plan and the documentation are described in (DIN) EN 50174-1.

Documentation

Make sure to adequately document all installations for later operation and any required changes.
As-built documentation includes:

- Supply information on materials used (cables, junction boxes etc.) including data sheets
- Technical information (e.g., terminal diagrams, installation instructions etc.)
- Test records for all installed lines
- Layout plans with the connection points and distributor locations
- Details about equipotential bonding measures

Test method

Tests are used to:

- Optimise production
- Improve production quality
- Increase production efficiency
- Reduce the costs caused by defective components

Test for:

- Interruptions and short-circuits (feed-through)
- Defective, missing and incorrect components
- Faulty assembly
- Compliance with the electric parameters of the cabling

Labelling

Label all connecting parts of your network on both sides. Use conventional markers and components that offer prepared labelling options. For this purpose, Weidmüller offers an extensive range of industrial markers for every situation.

Do not use normal marker pens directly on the cable or the connector, as these are not durable.

2.13 Active components

2.13.1 Basic information

Networks consist of two or more devices that are connected via a central point. The central node is generally a switch that manages the communication between the individual devices.

IP address

- Unique addressing within the network
- Precise communication between the individual clients

To avoid conflicts and malfunctions do not assign the same IP address twice within a network.

The IP address consists of four decimal numbers with a value range 0 to 255. The decimal numbers are separated by a decimal point.
The IP address is made up of

- the address of the (sub-)network and
- the address of the device (generally also referred to as host or network node).

Example: 192.168.0.110

MAC address
- World-wide unique, non-interchangeable serial number for all Ethernet components
- Stored permanently on the network card
- Is comprised of a 48-bit long sequence, which is normally represented as six hexadecimal numbers, separated by hyphens (-)

Divided into:
- 3-byte vendor ID and
- 3-byte device ID (consecutive number)

Example: 00-15-7E-01-00-2F-vendor ID Weidmüller: 00:15:7E

Subnet mask
The subnet mask is used to demarcate a related address area of IP addresses. This option can be used to subdivide a large company network in numerous subnetworks and, for example, into company sectors.

A subnet mask consists of 32 bits and is always used in conjunction with the IP address. It has the same length as an IP address.

The subnet mask consists of the network part and the host part. The number of the "1-bits" from left indicate the network part. The zeros indicate the network part.

255.0.0.0 (/8)	11111111	00000000	00000000	00000000
255.255.0.0 (/16)	11111111	11111111	00000000	00000000
255.255.240.0 (/20)	11111111	11111111	11110000	00000000
255.255.255.0 (/24)	11111111	11111111	11111111	00000000
255255255240 (/28)	11111111	11111111	11111111	11110000

Main task:
- To separate the network part of the IP address from the host part
- Is critical for communication via an IP network

Example: 255.255.255.0

Broadcast address
The broadcast address is a special address that includes every PC within a specified network.
In each case the last address of the host part is used as the broadcast address of a network.

Example: 192.168.0.255

Never specify a broadcast address as an address for an individual PC, otherwise various network functionalities will simply not work!

Broadcast
A broadcast is used to obtain recipient addresses from still unknown devices from the network. Data packets are sent to all switches and all these then report back providing the sender with an overview of the devices in its network.
A device in the network sends its data packets to the entire network.

Multicast
With Multicast, the user has the option of selecting a group of recipients that are to be supplied with the data packets.

Unicast
With Unicast, the data packets to be transferred are sent only to the one desired recipient.

Default Gateway
This is the network address the components send data packets to, if the target address is not in their own network, and no information is available as to how the target network can be reached.
- It provides information on how the target network is reached or
- it forwards the packets to its default gateway in the next instance.

The default gateway can be compared to a standard exit. All requests that are not directed to a device's own subnet are forwarded via the default gateway to another network For example, the requests can then be directed to the internet.

Example: 192.168.0.1

Dynamic Host Configuration Protocol (DHCP)
- Is used to automatically configure IP addresses of a network component
- This function is taken over by a router.

As soon as a component responds after activation using the so-called DHCP request, the DHCP server responds and assigns to the component an IP address from a previously defined IP address range. Apart from the IP address, a subnet mask, a default gateway and, if required, a DNS address and lease time are assigned.
The domain name server translates the IP address into a computer name.
The lease time is used to determine for how long a network node receiving its IP address dynamically from the DHCP server can keep that IP address.

Subnets

A subnet is a part of a network. A large network is divided into lots of small virtual networks in order to minimise, and thus accelerate, data traffic in a network. The sections of the entire network are called subnets. Subnets are parts of a network with their own subnet address.

If devices are to communicate with each other across subnet borders you have to set the router to allow such communication.

Collision domain

A collision domain is a segment of a network.
In all Ethernet networks, the terminals are connected to one single, physical Ethernet segment.

Virtual Local Area Network (VLAN)

- Groups individual devices from different physical structures into one joint logical structure.
- Changes to the network can be made with relatively little effort.
- Is not subject to any geographical restriction

A difference is made between static and dynamic VLANs:

a) Static VLAN
- Assignment of a physical port to the VLAN
- A component connected to the port automatically forms part of that port's VLAN.

b) Dynamic VLAN
- The port is assigned a VLAN ID based on the component's MAC address.
- Different from the static VLAN, a component's assignment remains the same when it is connected to a different port of the device.

Quality of Service (QoS)

This is a method to control the data traffic and the quality of service of networks.

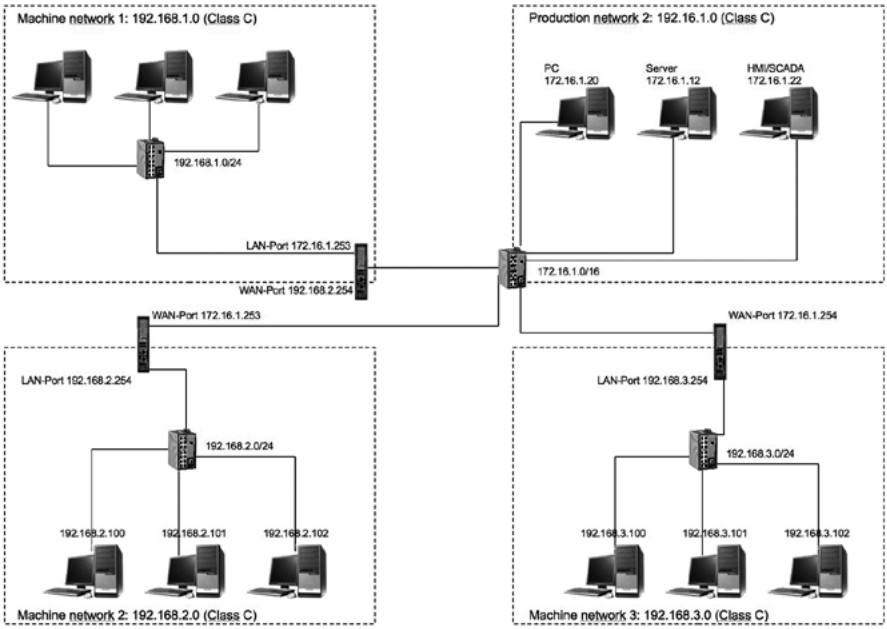
Objective: Data from specific services reach the recipient in accordance with predefined quality parameters.

QoS ensures optimisation of the network traffic by:

- Higher predictability of data transmission in the network
- Provision of stepped bandwidths for data transmission
- Assignment of transmission priorities throughout the entire network
- Improvement of the loss properties of the network

Network Address Translation (NAT)

Network Address Translation refers to the translation and switching between IP addresses of the local and the public domain.



a) Source NAT (SNAT)

Static method:

- The IP address of the source is replaced.
- Is used with packets
- The router stores this address translation.
- Is normally used for address translation between two local users only

b) Destination NAT (DNAT)

Dynamic method:

- The IP address of the target is replaced.
- Synonymous for incoming data packets
- For the terminal devices involved these processes are transparent, i.e. they are not affected by this address translation.
- Is used for mapping addresses of numerous local devices to a few public IP addresses

2.13.2 Security

Port security

Port security ensures that an unused port is not accessed without authorisation. This is done, e.g., by software-controlled deactivation of the port. It must be possible to undo the port deactivation when the port is used again.

Ports

Each network component is assigned a unique IP address which is used to address this component directly. Ports enable the individual addressing of various applications using this IP address.
If you wish to address an FTP server with the IP address 192.168.100.125, enter this address followed by a colon (:) and the port number 21.

Example: 192.168.100.125:21

This way, you can address a network component directly and reach the requested application via the port.
The ports

- 0 to 1023 are reserved for specific services such as FTP (21), SMTP (25), HTTP (80), Pop3 (110) etc.,
- 1024 to 49151 are registered ports for specific applications,
- 49152 to 65535 are private ports that anyone may use .

Trunking for higher bandwidth

Multiple physical fast Ethernet connections between two devices are summarised to a logical totality (virtual trunk) of the connection. This way, it is possible to transfer Fast Ethernet (100 Mbps) to Gigabit Ethernet (1,000 Mbps).

Port mirroring
Port mirroring means that the entire network traffic of the ports to be monitored is emulated to a mirror port to obtain control of the data volume and data contents. This way it is possible, e.g., to create history entries or logfiles.

Fault relay (security/debugging)
Many switches provide the triggering option of a programmable relay, in order to obtain information about a change of status. You can, for example, connect visual or acoustic signal transmitters to this relay.

Bandwidth limitation
A bandwidth limitation is advisable as soon as a 10-Mbps terminal has no auto-negotiation function. The terminal can then use the maximum bandwidth that is technically possible for it.

IGMP
The IGMP protocol can be used to send identical content to several user PCs. The IGMP-capable router duplicates the data packets that are to be sent to several users and then sends them on the requested trip.

IGMP snooping
- A checking of the Multicast flow
- Monitors the exchange between router and host
- Modifies the bridge table

2.13.3 Infrastructure components

Industrial Ethernet switches

A switch is a network component for combining several components into a local network.

Tasks:
- Structuring the networks
- Optimising the data transfer paths and times for the network traffic
- Increasing the data throughput

Features:
- Very robust and reliable
- Top-hat rail mounting and wall mounting

Industrial networks with Industrial Ethernet require high-performance, managed switches that act as a central exchange in the control cabinet. These differ significantly from unmanaged switches.

Global functions / operating modes

Auto-Crossing:

- Automatic detection of a crossing of outgoing and incoming lines on twisted-pair interfaces.
- Allows the connection of both a single-strand cable and a crossover cable.

Auto-negotiation

- Switches handle the data rate with the link partner on each port independently and automatically.
- The link is established with the highest possible common data rate both partners can handle.

Blocking:

- Non-blocking – if the capacity of the switches is adequate to master connections with full data rate between the partners
- Blocking – if no connections can be established because of overload

Half-duplex:

- Operating mode in which one Ethernet component either sends or receives data at a specific time

Full-duplex:

- Both communication partners can communicate in both directions at the same time.

Managed switches

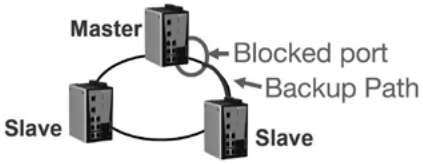
Owing to the numerous functions of managed switches, a configuration of the devices is essential. Programming via a Web interface or a terminal program facilitates the setting of components and allows the user to use the network to configure almost all connected PCs, even if the devices are spatially, very distant from each other.
Implementation of a monitoring function for individual ports makes it easier to evaluate the fault in the event of a malfunction.

Use:
- Port Trunking
- Port Mirroring
- VLAN
- IGMP Snooping
- DHCP
- Network redundancy

Turbo-Ring V2

Turbo-Ring V2: performance characteristics

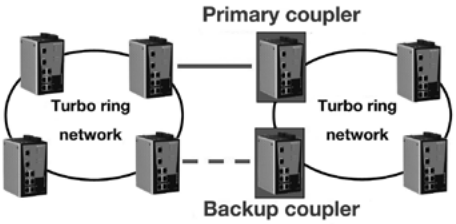
- Technology protocol for redundant ring structures
- Recovery time in case of a fault < 20 ms for a ring with up to 250 switches
- Advanced options for coupling several "Turbo-Rings" (Dual Homing and Dual Ring)
- Can be operated together with the standard redundancy protocol RSTP/STP



Ring Coupling

Redundant connection of 2 turbo-ring networks via 2 switches

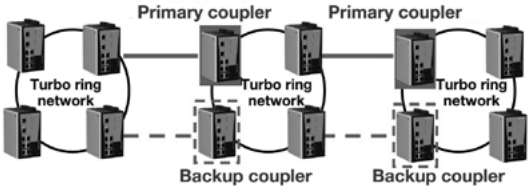
- Data exchange in normal conditions via the primary coupler
- In the event that the primary coupler connection fails, the backup connection is automatically activated (recovery time < 20 ms).
- Only the primary and backup coupler have to be configured for the ring coupling.



Multiple Ring Coupling

Connection of multiple turbo-ring networks in series

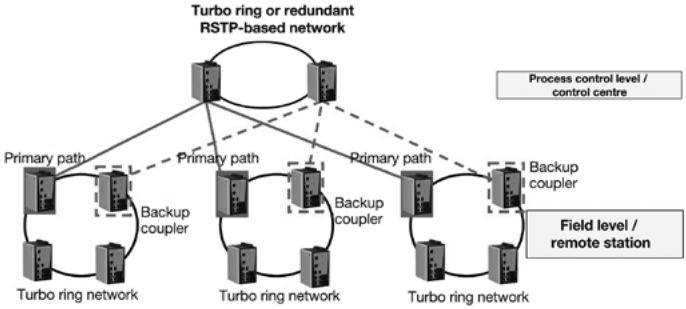
- Each ring may have only one primary coupler.
- Each ring may have only one backup coupler.



Multiple Ring Coupling 2

Connection of multiple turbo-ring network in a hierarchical tree structure

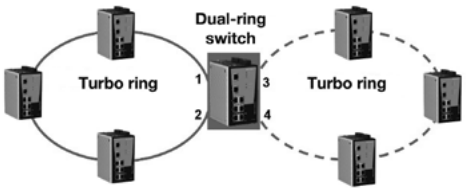
- Turbo-ring networks can also be coupled to RSTP-based network structures (e.g. to a control level).



Dual Ring

Connection of 2 turbo-ring networks via a common central switch

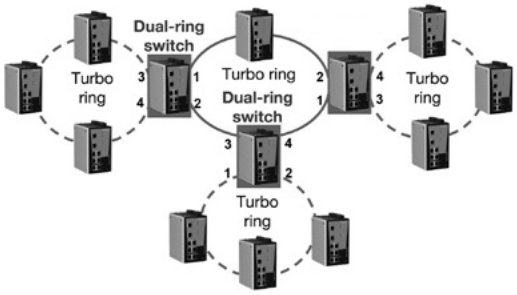
- Each switch can be located in a maximum of 2 rings.
- The "dual ring" switch must be explicitly configured for membership in 2 rings.



Multiple Dual Ring

Connection of multiple turbo-rings networks, each via a switch that is a member in 2 turbo-rings.

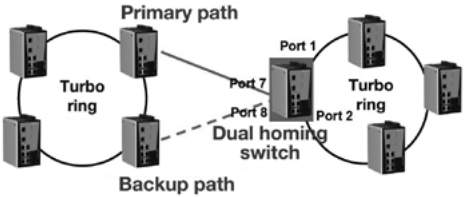
- Each switch can be located in a maximum of 2 rings.
- The "dual ring" switch must be explicitly configured for membership in 2 rings.



Dual Homing

Connection of 2 turbo-ring networks via a switch

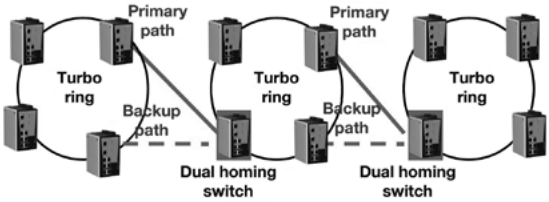
- Only the "dual homing" switch has to be configured for the ring connection.
- The "dual homing" switch controls the primary and backup patch for the redundancy.
- The "dual homing" switch can be inside the ring, but can also be operated as a stand-alone, redundantly connected switch.



Multiple Dual Homing 1

Connection of multiple turbo-ring networks, in each case via a "dual homing" switch (as series connection)

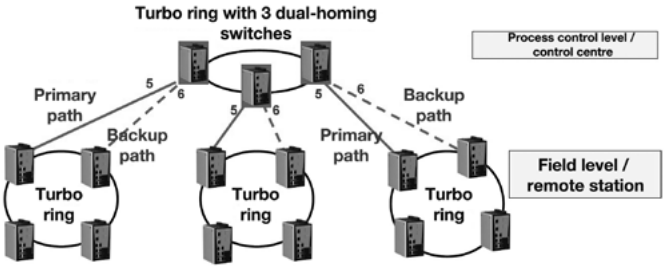
- Only the "dual homing" switch must be configured for the ring connection.
- The "dual homing" switch controls the primary and backup patch for the redundancy.



Multiple Dual Homing 2

Connection of multiple turbo-ring networks, in each case via a "dual homing" switch (in hierarchical tree structure)

- Each switch in the control level can be operated as a "dual homing" switch.



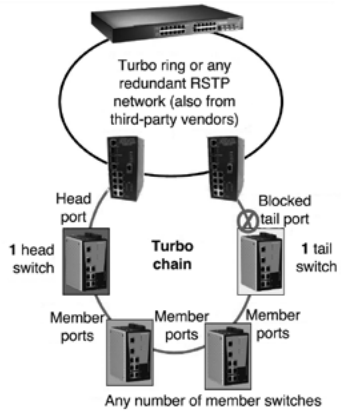
Turbo chain

Turbo-chain technology

- Universal "chain" network that can be connected with any number of other network structures
- Recovery time of turbo chain in case of fault < 20 ms (e.g. with cable break)

How does the turbo chain work?

- Connection in series (daisy chain)
- Chain consists of a head switch, any number of member switches and a tail switch.
- Both ends of the chain are connected with a randomly structured network.
- The tail switch blocks its connection (redundancy) and only opens if the backbone fails via the head switch



Unmanaged switches

Unmanaged switches allow a cost-effective entry into Industrial Ethernet engineering. They require no configuration, since they function using plug-and-play.

Use

- In price-sensitive applications
- If they are designed as compact plug-and-play modules
- To allow simple installation of Industrial Ethernet networks
- Do not have to be configured or given parameters.

When you use unmanaged switches with EtherNet/IP in networks with realtime I/O traffic, you have to understand that the multicast messages for certain address circles will be sent unfiltered to all ports with this type of switch (per broadcast), which increases the network load.

Wireless LAN (WLAN)

Wireless LAN refers to a local non-wired network.
To use wireless technology you need an access point that acts as a gateway between the wired and wireless world.

Safety features:

- Current encryption standards are WPA and WPA2.
- MAC address filters that only permit authorised network devices to access the wireless network

The use of a WLAN network in company areas should be well thought through and be provided with best possible protection if this option is implemented.

a) Types of application

- Mobile connection of laptops
- In motor vehicles or machines for data acquisition in storage area
- In automation
- For measured data acquisition or control of machines

b) Frequencies

Two licence-free blocks of frequencies are released for wireless network communication:

Standard	Frequencies	Channels
802.11a	5,15 GHz - 5,725 GHz	Channels: 19, all overlap-free, in Europa mit TPC und DFS nach 802.11h
802.11b/g	2,4 GHz - 2,4835 GHz	Channels: 11 in the USA / 13 in Europe / 14 in Japan. Maximum 3 channels overlap-free

With all standards the channel bandwidth is between 10 and 30 MHz.

c) Channels

The standard 802.11b/g is the most widely used standard and has a frequency range of 2.4 GHz to 2.4835 GHz. The frequency ranges divide as following among the individual channels:

Channel	Frequency	Country
1	2.412 GHz	Europe, USA, Japan
2	2.417 GHz	Europe, USA, Japan
3	2.422 GHz	Europe, USA, Japan
4	2.427 GHz	Europe, USA, Japan
5	2.432 GHz	Europe, USA, Japan
6	2.437 GHz	Europe, USA, Japan
7	2.442 GHz	Europe, USA, Japan
8	2.447 GHz	Europe, USA, Japan
9	2.452 GHz	Europe, USA, Japan
10	2.457 GHz	Europe, USA, Japan
11	2.462 GHz	Europe, USA, Japan
12	2.467 GHz	Europe, Japan
13	2.472 GHz	Europe, Japan
14	2.483 GHz	Japan

d) Range

The permitted radiated power of conventional WLAN terminals is 100 mW.

- The usual range is 30m to 25 km depending on the hardware and the application.
- The range depends ultimately on obstacles,and the type and shape of construction.
- Metallic infrastructure cannot be penetrated and increases the attenuation; so too does masonry or concrete walls.

e) Data rates

Take into account that all components in the network share the bandwidth for upload and download. Moreover, the specified data rates are theoretical values and refer to optimal conditions. The actually achieved data rates are several times less than the theoretical data rates.

IEEE/Group	Description
802.11	WLAN for1-2 Mbps on the 2.4-GHz band
802.11a	WLAN for 54 Mbps on the 5-GHz band
802.11b	Extension of 802.11 to 11 Mbps on the 2.4-GHz band on the 2.4-GHz band
802.11g	Higher data rate (20 Mbps and higher) on the 2.4-GHz band

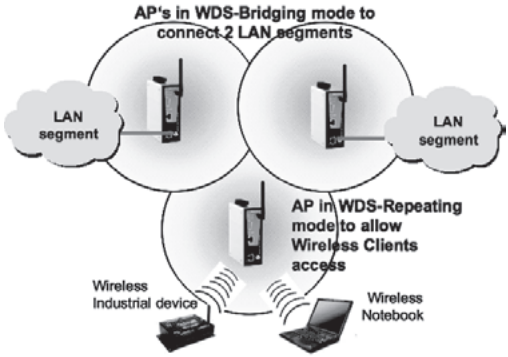
f) Interference

Interference can certainly occur in conjunction with other wireless transmission systems, since WLAN uses the same licence-free frequency blocks such as, for example, Bluetooth technology.

Wireless Distribution System (WDS)

What is WDS?

- A Wireless Distribution System (WDS) allows the wireless connection of access points to one another to form a wireless network (in acc. with IEEE-802.11 network standard).
- A WDS based wireless network-can comprise a maximum of eight wireless access points.
- Integrated RSTP technology to prevent data loops (Looping Protection)
- Wireless access points within the wireless network connect via MAC addresses.
- WDS is a standard technology; however, you should always use devices from the same manufacturer.



Note: per definition, WDS technology allows only WEP security.

2 Modes of operation

- Wireless bridging: each access point communicates with each AP and together these form a common network. Client connections are not permitted (wireless networking of wired networks).
- Wireless repeating: wireless networking of wired networks, WLAN clients can also connect to the APs.

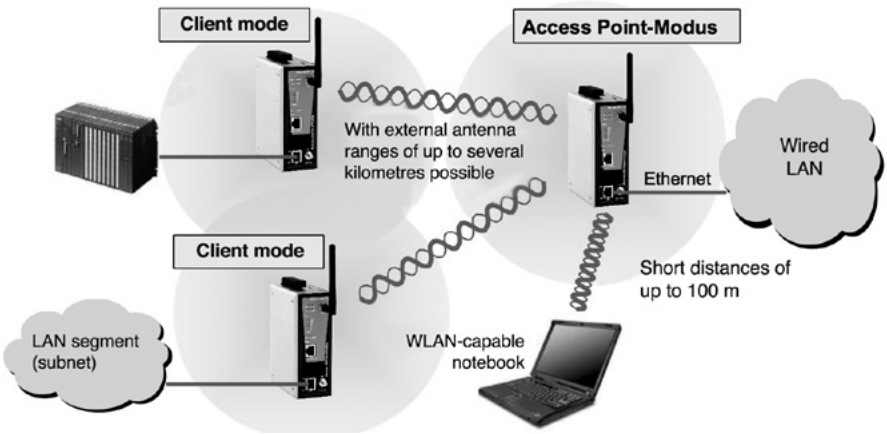
Modes of Operation: Access Point and Client Modes

Access point mode

- Allows the connection of WLAN components to a wired Ethernet network

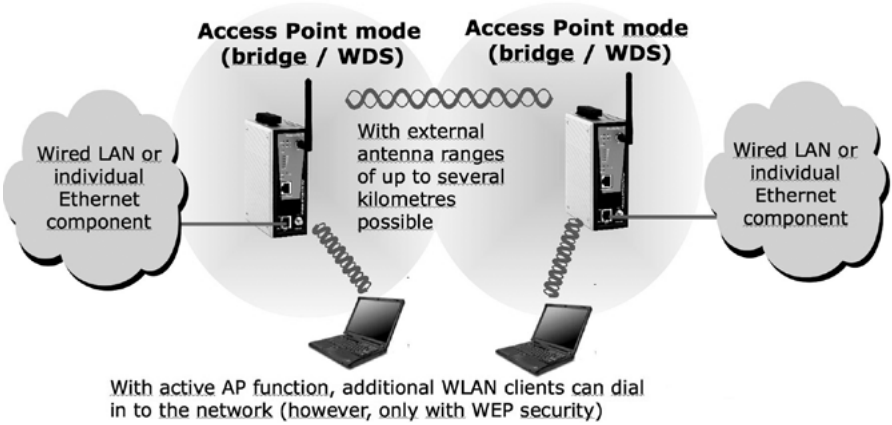
Client mode

- Makes wired Ethernet components WLAN capable



Mode of operation "Bridging with WDS" (WDS = Wireless Distribution System)

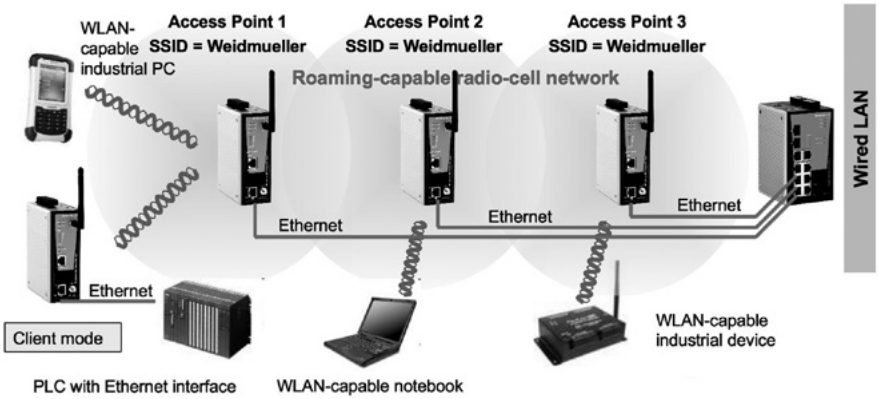
- WLAN link between various wired networks
- The “bridges” are linked to each other by means of MAC address that have to be mutually entered.
- In this mode of operation the devices can be access points at the same time.



Wireless network with multiple access points (scenario 1)

Access Points are connected by means of the wired LAN (WDS off)

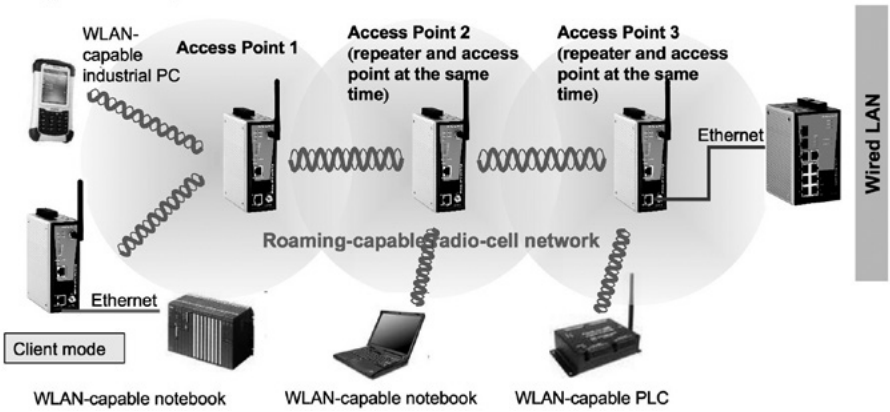
- Suitable for establishing acellular radio network (which can, theoretically, be any size)
- All APs have the same wireless name (SSID) for fast roaming of the WLAN clients
- Connection security can be set to WEP, WPA/WPA2 (personal and enterprise)
- No broadband dependency for connection of the access points to one another due to LAN Ethernet cabling



Wireless network with multiple access points (scenario 2)

Access points are connected to each other by radio link (WDS on)

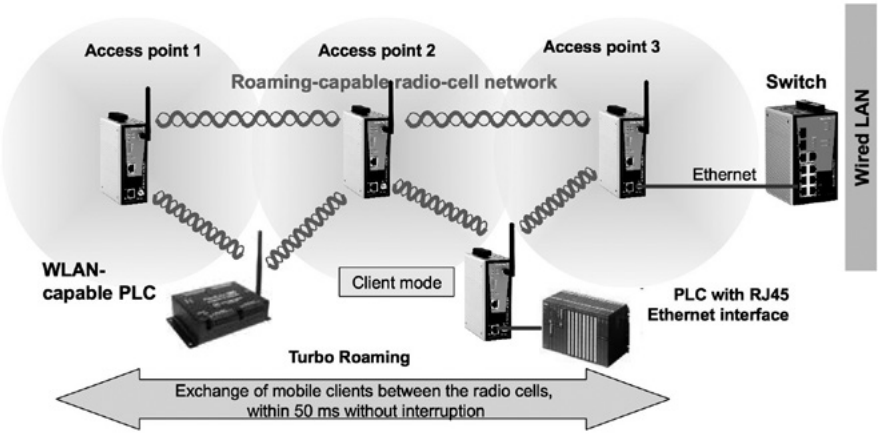
- Establishing a cellular radio network with only one cabling point to the wired LAN
- Meshed wireless networking of up to eight access points is possible
- However, there is a reduction of the bandwidth due to the twin load repeater and access point
- WLAN clients can only log onto WDS based wireless networks using WEP security.
- Typical roaming times with WEP security: < 100 ms



Turbo-roaming performance characteristics

Access points are connected to each other by radio link (WDS on)

- Roaming (also called "Handover") is the ability for an interruption-free changeover of a WLAN client between two access points.
- Turbo-roaming technology allows a changeover time < 50 ms (using WPA/WPA2 encryption).



Media converter

Media converters connect copper cables and fibre-optic cables.

In most applications copper conductors are sufficient, but fibre-optic cables are required in special applications:

- Cable length > 100 metres
- EMC interference
- No equipotential bonding

Serial/Ethernet converters

A serial/Ethernet converter allows you to connect a device with serial interfaces in a network. This allows trouble-free integration of an existing production facility with an RS232/422/485 interface into an Ethernet network. You can access the interface from all PCs within the network.

Robust, industrial power supply units

The correct power supply is a critical factor in ensuring the reliable functioning of the connected components.

2.14 Passive components: copper cabling

2.14.1 Basic information on copper cabling

Copper cables are the first choice for use in the office environment and in harsh industrial environments.

Advantages:

- Available in many variants and lengths
- Robust
- Easy to assemble
- RJ45 connections are the most widely available type.

Raw cable/metre

Industrial installation cable/horizontal cable

For permanent, durable installation in cable conduits and cable trays

- In Cat. 5 or Cat. 7
- Also for PROFINET
- With sheath in PUR or PVC

Industrial connecting cable

For flexible installation in machines and facilities in industrial environments / in harsh environments

- In Cat. 5 or Cat. 7
- Also for PROFINET
- With sheath in PUR, PVC or LSZH

Industrial tow-chain cable and torsion cable

For constant movement, e.g. in tow chains

- In Cat. 5
- Also for PROFINET
- With sheath in PUR

Assembled cables

Industrial patch cables/CabinetLine

Not only for use in the office area, but also for industrial use in control cabinets

- In Cat. 6
- With sheath in LSZH – low smoke and zero halogen
- In the variants straight and crossover

Industrial system cable

Pre-assembled cable for flexible installation in machines and facilities in industrial/harsh environments

- In Cat. 5 or Cat. 6
- With sheath in PUR

Industrial tow-chain cable

Pre-assembled cables for constant movement, e.g., in tow chains

- In Cat. 5
- Also for PROFINET
- With sheath in PUR

System cable for railway applications

Pre-assembled cable for flexible installation inside and outside of rail vehicles

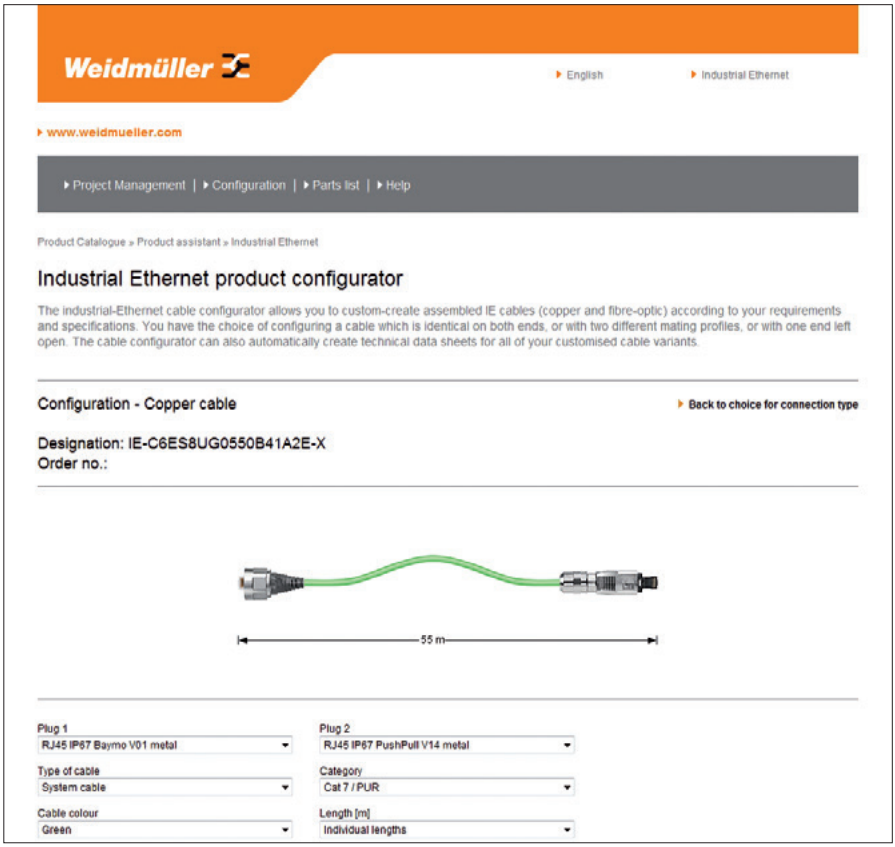
- In Cat. 5
- In acc. with PROFINET
- With Radox sheath

Customer-specific cable production

Numerous vendors offer to produce customised connecting cable; use this offer to

- make your assembly easier,
- make your ordering processes easier,
- make your storage and your logistics work easier.

In connection with this, also take a look at Weidmüller's **Galaxy** configuration software on the Internet at www.weidmueller.com/conf Here, you can individually create your connecting cable and directly send a request and order with at a click of the mouse.



AdvancedLine

Weidmüller's AdvancedLine offers all combinations of cables that are available with the extensive range of connectors.

This means flexibility and robustness due to the high quality of the components used. The range is made up of standard cables and customer-specific variants. Standard cables are shown in the catalogue. Customer-specific variants can be assembled online as desired using the "Galaxy" configuration software. All AdvancedLine cables are discernable by their special suitability for industrial applications.

- High-quality cables with very good technical properties
- Also suited for demanding IP 20 to IP 67 applications
- For temperatures from –40 to +70 °C
- High-quality shielding

CabinetLine

The new patch cable range, CabinetLine, from Weidmüller is available in various colours to distinguish between different networks.

Additional advantage: all items from the CabinetLine are equipped with Weidmüller TM marking sleeves to clearly label the cables and ports. CabinetLine is available in grey, blue, red and magenta colours, in conjunction with the sheath material LSZH and transmission capacity Cat. 6_A. CabinetLine is also available in the colour green and from Cat. 5, alternatively with the sheath material PUR or PVC. All of the variants are fitted with protected locking clasps which allow them to be pulled through a cable duct.

- For applications in the control cabinet and in simple environmental conditions
- Suited for temperatures of 0 to +60 °C
- Simple shielding

2.14.2 Normative characteristics for copper cabling

Note that the transmission properties of your network depend on:

- Spatial expansion of the network (conductor lengths)
- Transmission properties of the components

(DIN) EN 50173 also describes the characteristics:

Transmission link

- Transmission path between network device (switch) and connected stations
- A typical transmission link consists of horizontal cabling and two connecting cables (patch cables).

Permanent link

- Transmission path for the measurement of the quality of transmission of the installed components of a transmission link

2.14.3 Symmetric cable types

UTP	Unshielded cable
F/UTP	Cable with full foil shielding, unshielded pairs
SF/UTP	Cable with braided shield and foil shield, pairs unshielded
S/FTP	Cable with braided shield, pairs with foil shield

2.14.4 Special-purpose cable

Use tow-chain cables in locations where the cable is subject to frequent or constant movement in an industrial environment.

- SF/UTP cable
- Preferably 7-core stranded Litz conductor
- Cat. 5
- PUR sheath: zero halogen and high wear resistance

Use an armoured cable **(rodent cable)** for locations in the tropics or in geographically remote facilities to protect the cables against termites and other rodents.
Use a **torsion cable**, which can withstand twisting in a longitudinal direction, especially for robotics applications.

2.14.5 Definition of cable sheath material

Sheath material	PVC	LSZH	PE	PUR
DIN VDE designation	Y	H	2Y	11Y
Conventional temperature range	–40 °C to +115 °C	–25 °C to +70 °C	–35 °C to +80 °C	–40 °C to +85 °C
UV resistance	yes	yes	yes	yes
Resistance to spread of flame	++	++	–	+
Contains no halogen	no	yes	yes	yes
Oil resistance	+	no	+	++
Chemicals resistance	+	no	+	++
Resistance to abrasion	+	–	+	++
Applications	Building	Fire protection	Food	Industrial Tow chain
Water absorption	–	+	––	–
Can be used outdoors	yes	yes	yes	yes
Flexibility	+	–	–	++
	++ very good + good – low –– very low			

2.15 Copper connector in acc. with (DIN) EN 50173-3

In (DIN) EN 50173-3 there are two standardised connector faces:

PushPull V4 with RJ45

- RJ stands for "Registered Jack" (standardised socket).
- The established connection technology in IT is described in IEC 60603-7
- Further development of the RJ45 in the protection degree IP 67 is described in IEC 61076-3-106 and elsewhere.

M12

- M12 has been tried and proven in automation engineering for more than 30 years.
- Compact connection solution in IP 67
- M12 is described in IEC 61076-2-101.

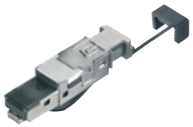
Specially equipped with a d-coded connector face, M12 is specified for use in Industrial Ethernet networks.

Apart from the standards and guidelines applicable to networks, other plug-in systems are also conceivable. These are not however compatible with the common IE connections.

2.16 Copper connectors in acc. with PROFINET specification

In the PROFINET specification there are four standardised connector faces, which are also standardised in IEC 61158

RJ45 without tools



- RJ stands for "Registered Jack" (standardised socket).
- The established connection technology in IT is described in IEC 60603-7

PushPull V14 with RJ45

- Further development of the RJ45 in the protection degree IP 67 is described in IEC 61076-3-117 and elsewhere.

M12

- M12 has been tried and proven in automation engineering for more than 30 years.
- Compact connection solution in IP 67
- M12 is described in IEC 61076-2-101.

Specially equipped with a d-coded connector face, M12 is specified for use in Industrial Ethernet networks.

M12 X-Type

- Re-standardised since 2011, 8-core solution for up to 10 Gigabits in proven M12 housing
- Compact connection solution in IP 67
- IEC 61067-2-109 describes the M12 X-Type.

Apart from the standards and guidelines applicable to networks, other plug-in systems are also conceivable. These are not however compatible with the common IE connections.

2.16.1 PROFINET end-to-end link

The PROFINET end-to-end link defines a permanent transmission link between two devices (network components or automation devices). This link is a connection between two active PROFINET components The end-to-end link itself is comprised exclusively of purely passive components. Figure 3-1 shows the basic configuration of the end-to-end link.

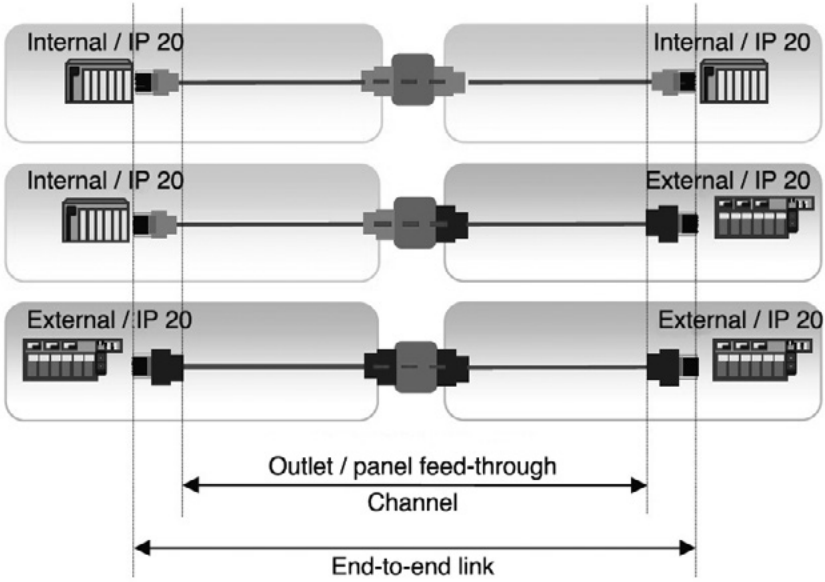


Figure 3-1: Channel/PROFINET end-to-end link

When passive network components that comply with the PROFINET component specification are used, this guarantees that the transmission link satisfies the requirements for a proper data transmission function. Passive
In terms of their mechanical and transmission structure, PROFINET components are ideally designed for the requirements in industry and especially for PROFINET. This is documented by the PROFINET Manufacturer's Declaration.

The PROFINET channel is the part of the transmission link that is defined as the end-to-end link. The end-to-end link includes the channel, as well as all connectors and the interfaces of the link.

The channel can consist of various transmission media, such as copper or fibre-optic cable.

The PROFINET component specification takes into account all connector interfaces in the transmission link (PROFINET end-to-end link).

The component specification stipulates the following rules for establishing a PROFINET cabling (PROFINET end-to-end link):

- Exclusively PROFINET network components are used.
- A maximum of six connector interfaces may be present in a transmission link. This also includes the first and last connector of the link.
- The length of the end-to-end link may not exceed 100 m.

If these rules are observed, it is guaranteed that the data requirements for the PROFINET end-to-end link will be met. No acceptance measurement of the end-to-end link or the PROFINET cabling is prescribed for using the PROFINET component standard. However, this only applies if exclusively PROFINET components were used for the installation.

Panel feed-throughs and couplings with two sockets are generally counted as two connector interfaces. The exceptions are panel feed-throughs and couplings for which the manufacturer has declared in the manufacturers declaration that these have the performance of a single socket.

An additional acceptance measurement is also advisable, if such a measurement is desired for documentation purposes, for PROFINET cabling. The acceptance procedure should then be conducted as described in this document.

The requirements in accordance with the PROFINET component standard have still to be satisfied, whatever the performance of the acceptance measurement. In particular, this applies in order to ensure the continued, proper functioning of the entire system during the entire life cycle of the automation facility, e.g., when individual PROFINET components are replaced.

(Source: PROFINET Commissioning Guideline, Version 1.01, July 2010)

2.17 Copper connectors in acc. with IEC 61158

In IEC 61158, there are three standardised connector faces for EtherNet/IP:

RJ45 crimp

- RJ stands for "Registered Jack" (standardised socket).
- The established connection technology in IT is described in IEC 60603-7

Bayonet V1 with RJ45

- Further developments of the RJ45 in the protection degree IP 67 are described in IEC 61076-3-106 and elsewhere.

M12

- M12 has been tried and proven in automation engineering for more than 30 years.
- Compact connection solution in IP 67
- M12 is described in IEC 61076-2-101.

Specially equipped with a d-coded connector face, M12 is specified for use in Industrial Ethernet networks.

M12 X-Type

- 8-core solution for up to 10 Gigabits in proven M12 housing
- Compact connection solution in IP 67
- IEC 61067-2-109 describes the M12 X-Type.

Apart from the standards and guidelines applicable to networks, other plug-in systems are also conceivable. These are not however compatible with the common IE connections.

2.18 Comparison of Ethernet interfaces

Origin	RJ45 IT	M12D Automation	M12X Automation
Mechanical design			
Degree of protection according to EN 60529	IP 67	IP 67, IP 69k possible	IP 67
Outer dimensions/installation size	average (depending on variant)	low	low
Wire connection	up to 8 wires	4 wires	8 wires
Industrial compatibility			
Can be assembled on-site	given	given	given
Energy transfer/hybrid solutions	possible	not possible	not possible
Quick connection	possible	possible	possible
Metal housing/robustness	given	given	given
Vibration resistance	very good	very good	very good
UV resistance	given	given	given
Transfer properties			
according to IEC 11801	Cat. 5 to Cat. 6_A (10-Gigabit Ethernet)	Cat. 5 (Fast Ethernet)	Cat. 6_A (10-Gigabit Ethernet)
Shielding	given	given	given
Miscellaneous			
Continuity: office → machine	given	not given	not given
Familiarity/handling	intended more for IT professionals	intended more for automation specialists	intended more for automation specialists
Availability of field devices	low	low	low

Features of the RJ45 and M12 transfer systems

2.19 *STEADYTEC*®

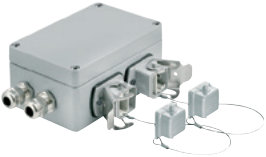
- Forward-looking connection technology for transferring data, power and signals
- Created by three leading connection technology firms
- Basis for reliable, user-focused solutions in line with standards – both in the office environment and in tough industrial surroundings
- The modular principle is used with ***STEADY****TEC*® for many possible combinations.

	Plug insert	Plug housing	Flange-mounted housing	Flange insert
Copper	 RJ45 crimp	 HDC-RockStar® / Variante 5		 RJ45 coupling
	 RJ45 can be assembled on-site	 PushPull / variant 14		 RJ45 module A, B, P
		 Bayonet / variant 1 plastic		 USB-A coupling
		 Bayonet / variant 1 metal		
Fibre-optic	 2xSC	 PushPull / variant 4		 2SC/SCRJ adapter
	 LC Duplex	 PushPull / variant 14		 LC duplex adapter

2.20 Additional infrastructure components

Junction boxes and couplings

- Form the connection points between user devices and the network
- For wall mounting



Couplings

- Intermediary piece used to connect two identical plugs together

2.21 Passive components for fibre-optic cabling

The term fibre-optic cable is used for all glass and plastic cables which are used to transfer data.

Application areas:

- Connections with high data rates over long distances
- In primary cabling (from one building to the next)
- In the secondary area

Display the following benefits over copper cables:

- No EMC influence
- Interference resistance thanks to galvanic decoupling
- Independent of potential equalisation
- Lightning and explosion protection
- Lower attenuation over longer lengths
- Higher bandwidth
- No crosstalk between the fibres
- Safety from interception

Distributor and cabinet cabling	Infrastructure and machine cabling	Application and machine cabling
		
Patch cable, zip-cord, Multimode SC, SC RJ, LC, ST connector, PVC sheath	Break-out cable Multimode SC, LC, ST connector, PVC sheath	Break-out cable Multimode SC, LC, ST connector, PUR sheath

Fibre-optic basics
a) Fibre-optic fibres

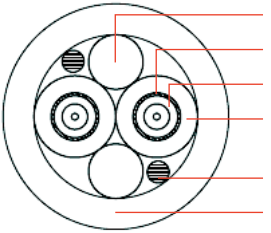
	POF/HCS	Glass
Costs (devices, cables, connection system)	low	high
Range of coverage	POF: up to 50 m HCS: up to 200 m	several kilometres
Data rates	up to 100 Mbit/s	> 10 Gbit/s
Usage, handling and packaging	relatively straightforward	complex

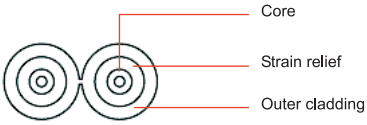
Fibres	No additional connector	One additional connector	Two additional connector
Plastic Optical Fibre (POF)	50 m	43.5 m	37 m
Plastic Cladded Fibre (PCF)	100 m	100 m	100 m
Multimode glass fibre	2,000 m	2,000 m	2,000 m
Singlemode glass fibre	14,000 m	14,000 m	14,000 m

b) Fibre categories

Fibres	Wavelength [nm]	Attenuation [dB/km]	Bandwidth/length product [MHz*km]	Coefficient of chromatic dispersion [ps/nm*km]
Multimode	850	3.5	200	
OM1	1,300	1.5	500	
Multimode	850	3.5	500	
OM2	1,300	1.5	500	
Multimode	850	3.5	1,500	
OM3	1,300	1.5	500	
Singlemode	1,310	1.0		3.5
OS1	1,550	1.0		18

Design of fibre-optic cables





Zipcord cable

Cable sheath

Sheath material	PVC	PUR
DIN VDE designation	Y	11Y
Temperature range typical for market	–40° to +115 °C	–40° to +85 °C
UV resistance	yes	yes
Resistance to spread of flame	++	+
Contains no halogen	no	yes
Oil resistance	+	++
Resistance to chemicals	+	++
Resistance to abrasion	+	++
Applications	Building	Industrial dragline
Water absorption	–	–
Can be used outdoors	yes	yes
Flexibility	+	++
	++ very good + good – low –– very low	

Connector

	SC-Simplex	SC duplex	SC-RJ
			
Standard	IEC 61754-4	IEC 61754-4	IEC 61754-24
Media	MM, SM, POF	MM, SM	MM, SM, POF
IE profile			PROFINET

	ST	LCD	E2000
			
Standard	IEC 61754-2	IEC 61754-20	IEC 61754-15
Media	MM, SM, POF	MM, SM	MM, SM
IE profile		EtherNet/IP	

2.21.1 Routing Ethernet fibre-optic cables

If the maximum permissible tractive forces are exceeded, the optical fibres can be overstretched if necessary. This can result in greater attenuation, shorter service life and/or permanent damage to the cable. Permanent or sporadic transfer faults may result. Such faults may also arise later on, sometimes years after installation. Particular attention should be paid to compliance with bending radii. The minimum bending radius for Ethernet cable is usually at least 15 times the cable diameter. Please also take into account the data provided by the manufacturer in the data sheets.

2.21.2 Protecting plug-in connectors from dirt

- Plug-in connectors for fibre-optic cables are sensitive to dirt.
- Use the dust caps provided to protect plug-in connectors and sockets that are not connected.
- Clean the front surface of a plug-in connector before plugging into devices or optical couplings. Use a fluff-free cloth soaked in isopropyl alcohol for this purpose. Place the cloth on a surface which is level and not too hard. To clean, pull the plug-in connector in one direction over the cloth. Repeat the process at a slight offset if necessary. First clean when damp, then dry. Use a microscope to check cleaning results.

(Source: PROFINET assembly guideline,version 1.0, January 2009)

2.22 Important questions to ask when planning the network infrastructure

- What kind of cabling exists in the building / system?
- What cabling/connection system is used?
- How is the connection to the building network to be made?
- Where is the machine connection point?
- How great a distance is there from the building network?
- What connection lengths are needed to the network participants?
- Is redundant cabling needed?
- Should the machine distributor be placed in the control cabinet or be a standalone unit?
- What kind of earthing concept is used?
- What connection system should be used?

2.23 Tender specification sheets

Use the service provided by many network component manufacturers and download your tender specification sheets – including some in GAEB (Joint Committee on Information Technology in the Construction Industry) format.

2.24 Checklist for planning

Requirements	Notes
Cable runs	
Have the minimum transfer distance requirements been met?	
Have the maximum permitted bending radii been met?	
Have the permitted ambient conditions been met?	
Product selection	
Are all measures resulting from applicable standards planned?	
Have the defined specifications been met?	
Distributor	
Has access from the front and rear been guaranteed?	
Has sufficient space been left for later extensions?	
Has space been provided so that the doors can be fully opened?	
Function guarantee	
Have measurement reports and documentation been produced for the cabling?	

Notes

3 Installation

This chapter contains information about:
- Installation guidelines
- Cable routing
- Connection system
- Marking
- Measurement and documentation

3.1 Installation guidelines

During installation note the compulsory elements of the (DIN) EN 50174 series of standards. This has trans-sectoral validity. Depending on the industrial protocol specified, also refer to the associated guidelines.

(DIN) EN 50174

The (DIN) EN 50174 series of standards is aimed at planners and installers of communication cable systems and architects. It includes requirements for planning, implementation, documentation and quality assurance – both during the cabling implementation phase and during operation.

PROFINET installation guideline

Produced especially for the PROFINET industrial protocol, this installation guideline describes:
- Specified connection lengths
- Specified plug-in connectors
- Specified cables
- Routing compliant with PROFINET

Installation guideline for EtherNet/IP

Produced especially for the EtherNet/IP industrial protocol, this installation guideline describes:
- Specified plug-in connectors
- Specified cables
- Routing compliant with Ethernet/IP

3.2 Cable spacing

Table 3.1 shows the minimum spacing you need to observe in accordance with IEC 61918 between Ethernet cables (shielded data cable) and other cables. The table also includes two variants with a metal isolating strip which can be used to isolate data cables from power cables.

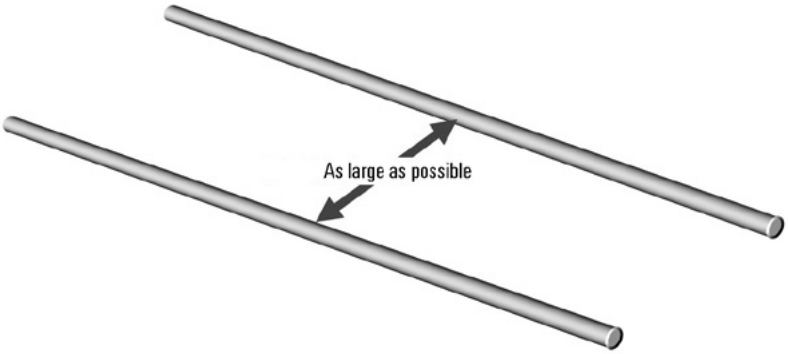


Figure 3.1: Cable spacing

Generally speaking, the risk of faults (crosstalk) falls the greater the spacing between cables and the shorter the distances over which cables run in parallel.

How to read the table!
If you want to know the minimum spacing required between Ethernet cables and other electrical cables, proceed as follows:

In the left column (Ethernet cable and cable for ...), select the electrical cable you are routing along with the Ethernet cables.
In the right part of the table (spacing), select the type of cable isolation you want to use.
Read the spacing for the relevant cable type off the column for the respective type of cable isolation.
Also note the specifications following Table 3.1 for various routing areas.

	Spacing from Ethernet cable		
	Without or with non-metal isolating strip	Isolating strip made from aluminium	Isolating strip made from steel
Signal transfer cable			
Bus signals such as other Ethernet cable, Profibus cable data cable for PCs, programming devices, printers shielded analogue inputs	0 mm	0 mm	0 mm
Power supply cable			
Unshielded power cable	200 mm	100 mm	50 mm
Shielded power cable	0 mm	0 mm	0 mm

Table 3.1: Minimum spacing for cables according to IEC 61918

(Source: PROFINET assembly guideline, version 1.0, January 2009)

3.3 Cable routing

Use the following information and assistance to simplify your work and to ensure that your system runs smoothly later on.

Please notice the strain relief specifications according to applicable standards.

Unrolling cable

With cable drums, use unwind stands to avoid harmful loading.
Unreel the cable rings on the floor to avoid torsion forces on the cable.

Bending radius

Always note the manufacturer's details on bending radii for cables. These must be observed to ensure the transfer characteristics.

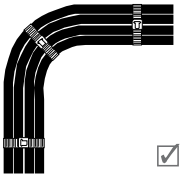
- Typical bending radii are:
- Copper installation cable: 4-5 x diameter
- Flexible copper connection cable: 4-5 x diameter (one-off bending), 8-10 x diameter (frequent bending)
- Copper dragline cable: approx. 7.5 x diameter

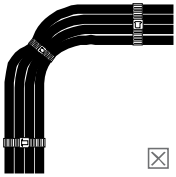
When guiding cables around sharp edges or corners, be sure not to damage them in order to maintain durability and transfer properties.

Bundling and fixing cable

Use as wide a cable tie as possible or better still use velcro ties to bundle cables or fix them to supporting parts. Ensure that the cables are stretched and that you don't squash them because this will later impair the transfer properties and ultimately result in failure during operation.

Cable conduits and cable bearers





Be aware that power, data and signal lines may have to be isolated to avoid data traffic faults.
(DIN) EN 50174-2 will assist with decisions on spacing between lines.

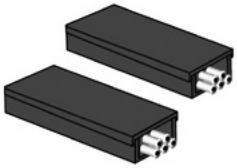
Cable reserves

When routing and isolating cables near the cabinet, leave a cable reserve of 2 to 3 metres. Circumstances often arise where cable routing and isolation change slightly from planning when installing cabinets.

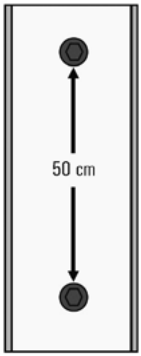
Cable routing within cabinets

Refer to Table 3.1 for the minimum spacing between two cables of different categories. Generally speaking, the risk of faults from crosstalk decreases, the greater the spacing between the cables.

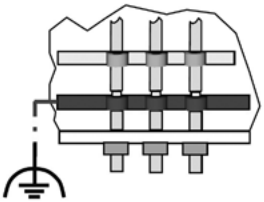
If cables of different categories have to be crossed in your system, they should be crossed at right angles. Avoid routing cables of different categories in parallel.



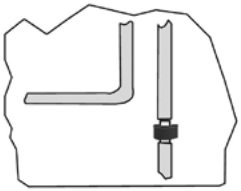
If there isn't enough space to observe the corresponding spacing between the individual categories, the cables must be routed in separate, metallic conduits. Each conduit should only hold cables of one category. These conduits can then be positioned right next to one another.



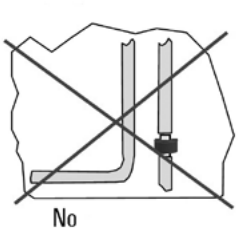
Screw a metallic cable conduit down to the rails of the frame or cabinet walls roughly every 50 cm. Ensure that there is a good conductive and flat connection between the rail and cable conduit. With coated cabinets, this can be done using lock washers for example. Another option is to remove the coating or paintwork. However, all metal parts must be sufficiently protected from corrosion.



Connect the shields of all cables routed into the cabinet with the potential equalisation at the cabinet entrance. To do this, connect large areas of the shields with the operating earth, ensuring good conductivity. Special assembly material is available from various manufacturers for this purpose. Mechanically brace the cables above the earthing clip to prevent damage caused by the cable moving.



To introduce the cable into the cabinet, use suitable cable entries such as cable glands.

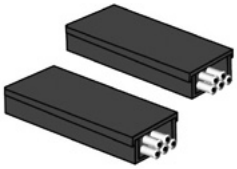


Avoid the parallel routing of cables from the outside with PROFINET cables inside the cabinet between the cabinet entrance and shield support. This also applies to cables of the same category!

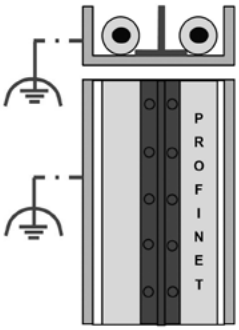
3.3.1 Routing cables inside buildings

When routing cables outside cabinets and inside buildings, note the following:

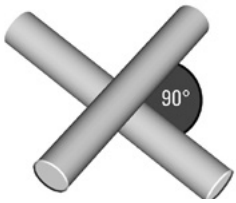
Refer to Table 3.1 for the minimum spacing between two cables of different categories. Generally speaking, the risk of faults from crosstalk falls the greater the spacing between the cables.



If the cables are routed in metallic cable conduits, the conduits can be positioned right next to one another.



If there is just one shared metallic cable conduit available for all categories, the spacing stated in Table 3.1 should be observed. If there isn't enough space, the various cable categories must be isolated using metallic partitions. The partitions must be connected to the conduit over large areas, ensuring good conductivity.



If cables of different categories cross, they should be crossed at right angles. Do not route cables of different categories over long distances in parallel.

(Source: PROFINET assembly guideline, version 1.0, January 2009)

3.4 Mechanical protection for Ethernet cables

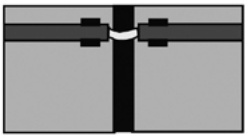
Mechanical protection measures should protect Ethernet cables from wire interrupts or short-circuits or mechanical damage to the sheath and shield.

Note

The measures described here for mechanical safety apply equally to electrical and optical cables!

Route the Ethernet cable in a plastic guard if you are routing the Ethernet cable separate from cableways.

In areas with high mechanical loading, route Ethernet cables in metal reinforced tubes. In areas with less mechanical loading, you can also use plastic reinforced tubes.



You have to interrupt the guard tube at 90° bends and building joints (e.g. expansion joints). You must avoid radii below the minimum permissible bending radius (no kinks). The possibility of damage to the Ethernet cable from, for example, falling parts, must also be excluded.

In the standing areas of walk-in building and machine parts and near transport routes, route the Ethernet cable in metallic reinforced tubes or metallic cableways.

Note

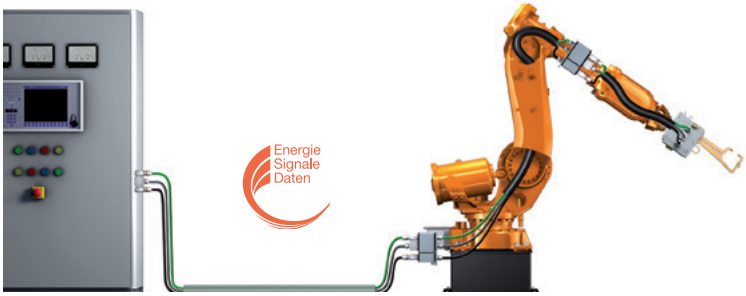
Given the maximum length of roughly 100 metres for Ethernet copper cable, we would recommend using fibre-optic cable for connections between buildings for reasons of potential isolation and for better protection from electromagnetic faults.

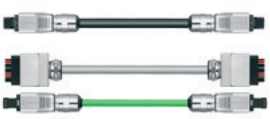
(Source: PROFINET assembly guideline, version 1.0, January 2009)

3.5 PROFINET/AIDA robotics cabling

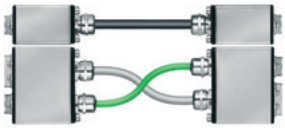
A coherent platform for power, signals and data in automotive construction

PushPull connectors and Weidmüller's junction boxes are the basis for this new cabling standard in the automotive industry. The new PushPull connectors are an integral part of Weidmüller's power-signal-data installation system for **AIDA*** (AIDA is the Automation Initiative of the German Automotive Industry). The cabling standard for PROFINET installations was established on this basis – and so it naturally includes all the benefits of ***STEADY****TEC*® technology!





Cable packet from the electrical cabinet to robot base



Hose packet from robot base to axis 3

Hose packet from axis 3 to robot head

The installation system for robotics cabling is comprehensive and complies with the PROFINET cabling guideline. It reduces the amount of work involved in assembly by around 50 percent and comprises co-ordinated, pluggable individual components for wiring the hose packets.

Users can use these components to plug in and run the three basic elements of industrial automation, power, signals and data, and therefore produce an integral solution. A cable packet is used to establish the connection from the cabinet to the robot base. Hose packet 1 connects the robot base with axis 3 and hose packet 2 provides the final connection between axis 3 and the robot head. Weidmüller's innovative installation strategy offers major benefits for the user: there is less complexity during installation and quicker replacement of the hose packets during maintenance. PushPull connectors enable you to swap out power, signal and data cabling; the procedure is simple, quick and complete. The sturdy metal housing enclosing the connector ensures a long lifespan even when used for applications in harsh environments.

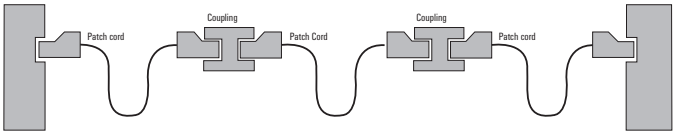
*Automation Initiative of German Domestic Automobile Manufacturers or **AIDA** for short:
- Defines the standards for automation systems in automotive construction
- Clearly acknowledges PROFINET.

***AIDA** = Volkswagen, Audi, Porsche, Daimler and BMW

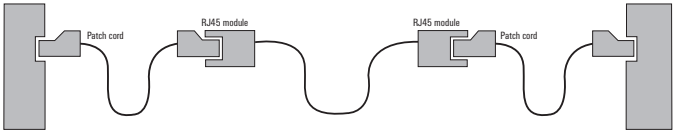
The new cabling standard consists of PROFINET PushPull connectors with two different inserts for data and signals along with the PushPull power connector. The system is completed with a FreeCon double-junction box for both power (24 V) and data (Ethernet), and also a FreeCon single-junction box for signals. The connectors and the FreeCon junction boxes are equipped with RJ45 modules. The use of RJ45 modules featuring ***STEADY****TEC*® technology allows the number of plug-in ports within a single channel to be reduced. The PROFINET specification calls for the number of plug-in ports to be limited to six. Each additional plug-in port along the channel increases the power loss and reduces the effectiveness of the entire transmission path. Weidmüller uses RJ45 components of category 6_A because these have a considerably higher system reserve for data transfer than category 5 components. This permits more plug-in ports to be used within a Cat. 5 channel than the specification describes. The PushPull connector for power lines features a 5-pole insert for 16 A,

the PushPull signal connector a 10-pole hybrid insert. The result is a perfectly co-ordinated system for power, signals and data, enabling consistent cabling between the cabinet and robot (or similar applications).

Module transmission path (channel) with six plug-in ports

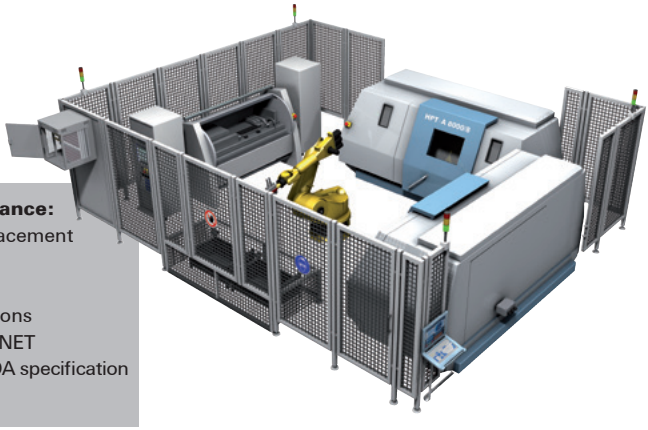


Transmission path (channel) with four plug-in ports



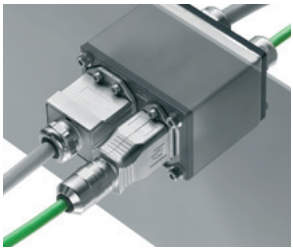
Weidmüller's FreeCon junction boxes provide other mounting options so that you can always be sure of the optimum cable feed.
There are two M4-threaded fittings on the bottom side which allow the FreeCon junction boxes to be screwed on to a floor panel. These threads are also used to secure the mounting foot. This allows the connector to be positioned within a 120° angle range. This allows the hose packet to be properly guided near the robot's axis 3. It can also be mounted on the front using four M4 screws. Thus the cable packet can be guided through e.g. a panel or a wall. An assembly opening is needed for this.

This installation system is suitable not only for robotics cabling, but also for all applications which require a sturdy, reliable and pluggable cabling solution.

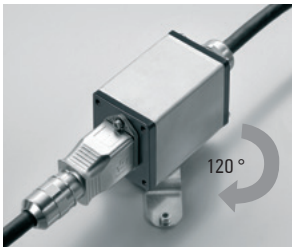


The advantages at a glance:

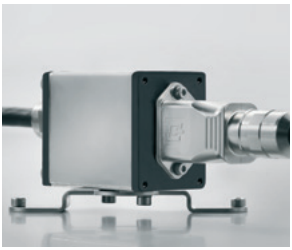
- Quick installation/replacement
- Sturdy metal housing
- High transfer security
- Various mounting options
- Compliant with PROFINET
- Compliant with the AIDA specification
- Cat. 6_A components



FreeCon junction box with front mounting



FreeCon junction box with mounting foot



3.6 Connection system

Copper connection system

a) Isolating

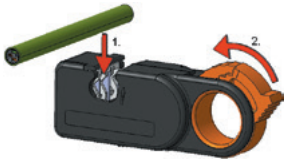
Be sure to:

- Select the right tool. The cutter shape corresponds to the relevant insert and is optimised for it
- Isolate vertical to the cable

b) Sheath stripping

To simplify the task, use a multi-stage sheath stripping tool. This removes the cable sheath at one point and the underlying shield at another point in one step.

Select the right blade settings to match the cable type.

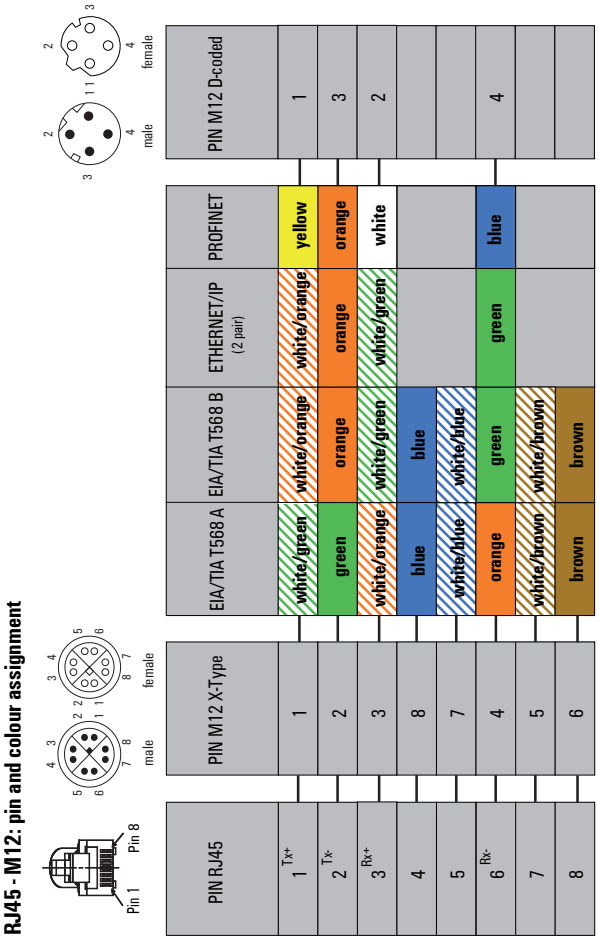


1 Insert the cable end in the tool.
2 Securely close the tool.

3 Rotate the tool in the direction indicated by the arrow to strip insulation from the cable.

4 Open the tool before removing the cable.
5 Strip the removed cable sheath by hand.

Pin assignment for RJ45 and M12 according to TIA 568 A, TIA 568 B, EtherNet/IP and PROFINET



Connection instructions

- Do not remove the twist in the pairs of wires any more than necessary.
- Do not add further twists to the pairs of wires.
- Ensure a closed sheath film.

c) Connecting RJ45 plug crimp

1 Remove sheath from cable according to assembly instructions for plug-in connector and strip the protruding braid to the rear over the cable sheath. Slide on anti-kink bushing.

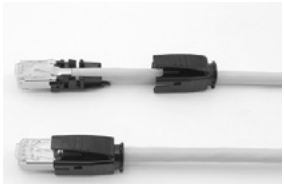
2 Guide the cable's individual wires into the pre-screener according to the chosen pin assignment (page 116) and trim the protruding ends flush.

3 Now insert the pre-screener into the plug housing. If necessary, bend the strain relief to the rear and then to the front again.

4 Insert the RJ45 plug in the crimping tool and close the tool. This one step injects the contacts, braid and strain relief.

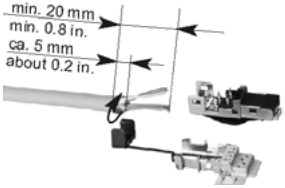
Be sure to select crimping pliers to match the plug type because not all tools go with all plug.

5 Trim the protruding braid.

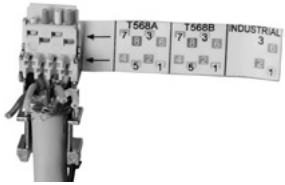


6 Slide the plug grommet over the assembled plug. Depending on the plug type, this protects the stop lever and ensures protection from bends and kinks.

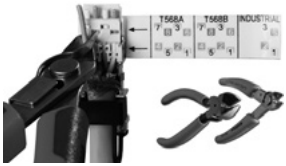
d) Connecting RJ45 plug which can be assembled on-site



1 Remove sheath from cable according to assembly instructions for plug-in connector.



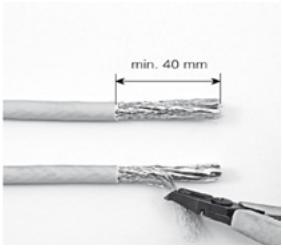
2 Sort the individual wires into the cable guides according to the codes on the lower plug section and slide the cable as far forward as possible.



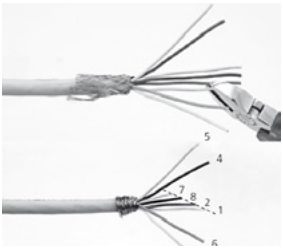
3 Close the strain relief around the cable and isolate the protruding cable ends flush.

4 Press upper section of plug onto lower section. If necessary, use pliers wrench to support plug.

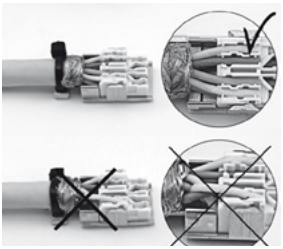
e) Connecting RJ45 module which can be assembled on-site



1 Remove sheath from cable according to assembly instructions for module. Slide protruding braid to rear over cable.



2 Untwist the pair of wires. Cut the wires at an angle for simple sorting into the bottom cable guides.



3 Slide or place the individual wires into the cable guides of the lower module section by colour. Use one of the cable ties provided as strain relief. Isolate the protruding cable ends.

4 Press upper module section onto bottom section. If necessary, use pliers wrench to support plug. Fix the braid with the second cable tie.

f) Testing

Test every cable that you route for:

- correct assignment
- end-to-end shield connection
- short-circuit
- split-pair errors

Further requirements of measurements on copper cabling are defined in the PROFINET commissioning guideline. An extract can be found on the following pages.

3.7 Measurement on the copper cabling

This chapter shows how the PROFINET copper cabling can be tested. Several measuring devices from the various performance classes are also mentioned by way of example. A distinction is made between:

- **simple cable tester (verification)**
- **function tester (qualification)**
- **acceptance tester (certification)**

3.7.1 Cable testers

Cable testers were developed to provide an easy way of testing Ethernet installations. The devices available on the market
offer different functions, scopes and in particular different forms of operation. They cannot therefore be described here in detail.

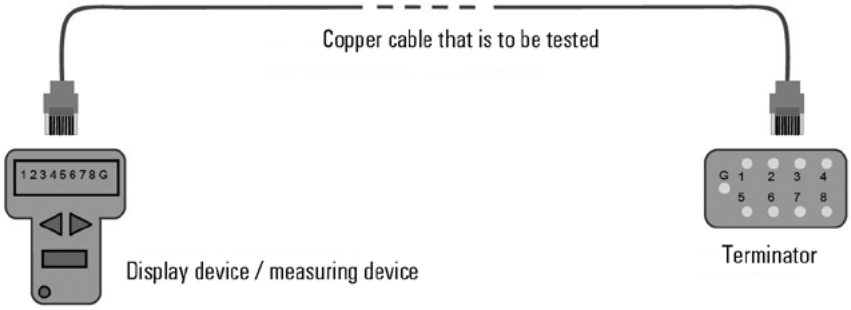


Figure 3.2: Basic setup of a simple cable test

Figure 3.2 shows the basic measurement setup for simple cable testing of PROFINET copper cabling. Basically it's a case of testing an electrical connection, i.e. testing for connection and/or short-circuit and impermissible split pairs. The testers do not check cable parameters or whether data packets can be transferred via the cable. These testers can be used during installation to check cables for connection/short-circuit and to check for correct contact assignment on the plug-in connector.

The cable tester shown here is a standard tester for the Ethernet. Special testers are not used for PROFINET.

When using a cable tester on PROFINET networks which have been set up with PROFINET copper cables (100BaseTX with 2 x 2 wires), the cable tester only shows a connection for the individual cables 1, 2, 3, 6 and shielding (G). With PROFINET, note that the pairs of wires don't have to be crossed because the active network components perform auto crossing.

3.7.2 Function testers

While the simple cable tester only tests for a correct electrical connection, the function tester checks the cabling section from the perspective of real Ethernet data transmission.

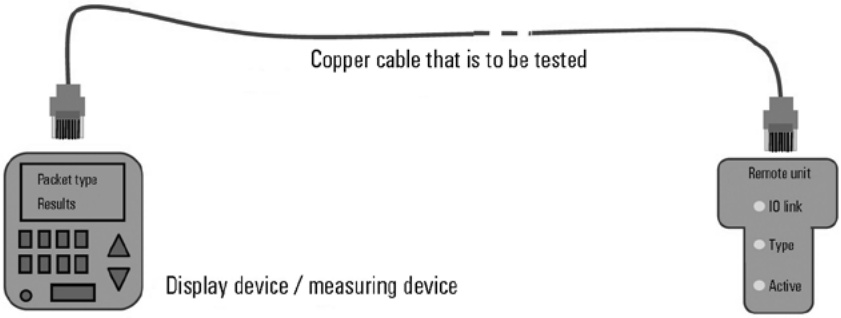


Figure 3.3: Function measurement on the cabling

This measuring device transmits pre-defined data packets over the cabling. The remote unit is the counterpart for responding to these packets.

Alternatively there are devices which can directly verify the transmission parameters in the time range that are of relevance for Fast Ethernet and display the error location in the event of parameters being exceeded.
Certain function testers can however also detect other active devices, such as switches and network participants, on the network and apply the standard diagnosis network protocols (e.g. ICMP).

The measurement data obtained then allows a statement to be made as to whether the section can transfer Ethernet data packets.

3.7.3 Acceptance testers

In certain cases, a simple function measurement with the function tester doesn't go far enough. A detailed measurement of cabling parameters (e.g. cable length, attenuation, crosstalk etc.) is needed. Such a measurement can be used to establish and document numerous cable parameters. After long periods of cable use, this can be useful if faults arise and the measured values from the acceptance measurement can be used by way of comparison.

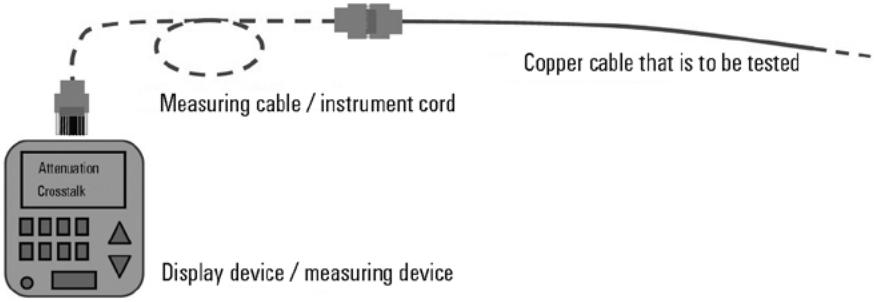


Figure 3.4: Extended acceptance measurement on the cabling

In line with the applicable standards, the cable's plug-in connector is not normally included in the measurement. If plug-in connectors can be assembled on-site, the connectors and their contacts should be included in the measurement.

Note that with this measurement procedure, special measurement cords or adapters may have to be used so that the results aren't affected.

The component approach taken with PROFINET means that a compulsory acceptance test doesn't have to be run to check the cabling if using PROFINET components with a manufacturer's declaration. An acceptance measurement can however be undertaken to:

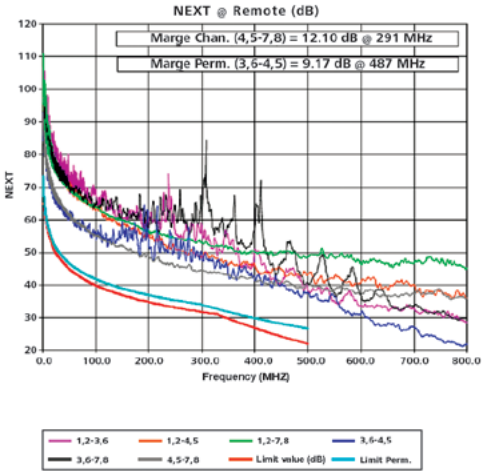
- measure and document the cable length
- measure and document the attenuation and other key cable parameters

This gives you reference data that you can refer back to when testing the cabling later on.

Contact the manufacturer of the measuring device if you need more detailed information. For operation, always read the manufacturer's instructions.

If the insertion loss of a section falls below a value of 4 dB at the measured frequency, the measured value for near-end crosstalk (NEXT) is for information only. This is known as the "4 dB rule". With short connections in particular, the insertion loss will be less than 4 dB.

(Source: PROFINET Commissioning Guideline, Version 1.01, July 2010)



Using high-quality CAT. 6_A components increases the distance from the permissible limit value and thereby improves the reliability of transmission. The above diagram clearly shows this distance to the red limit value curve.

3.8 Fibre-optic connection system
3.8.1 POF (polymer-optical fibre) connection system

a) Innovative quick-connection system for POF
Standard connection system for POF

Tools and aids
Sheath stripping, cutting and crimping tool: IE-HTX-POF

Remove the cable sheath (breakout) of the fibre-optic cable with a suitable sheath stripper. With zip-cord cables, separate the two cables slightly.

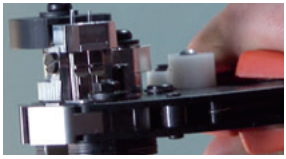
b) Fibre preparation and assembly taking the example of an IP 20-SC plug on a POF cable

1 Strip sheath from POF: insert cable, fully close tool and pull off sheath, slide cable grommet (kink protection) on to cable.

2 Slide inserts onto insertion aid with rounded surfaces facing outwards.

3 Place POF inserts in tool: only close tool such that the inserts are firmly gripped.

4 Guide in fibres



until they protrude on the other side of the tool, then close tool all the way.

5 Inserts are now crimped and can be removed.

6 Slide inserts into housing.

7 You're done.

3.8.2 Glass fibre connection system

a) Tools and aids

Fast-cure adhesive set:
The adhesive is used to fix the fibres in the plug. Select a fast-cure adhesive, which greatly simplifies and speeds up assembly.

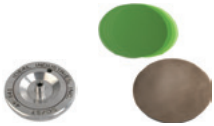
Sheath stripping tool:
Remove the cable sheath (breakout) of the fibre-optic cable with a suitable sheath stripping tool.

Stripping tool:
Use the stripping tool to remove the cable sheath (zip-cord), secondary coating and primary coating.

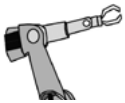
Kevlar scissors:
Use the Kevlar scissors to remove the protruding Kevlar braid.

Crimping tool:
Use the crimping tool to crimp the crimp sleeve on the plug to establish a mechanical connection between the fibre-optic cable and plug.

Stylus:
Use the stylus to score the protruding glass fibres and then break them off.



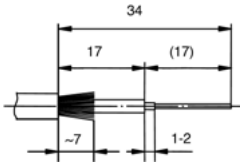
Polishing disc and polishing foils:
These are used to hold the plug and polish the face end of the fibres.

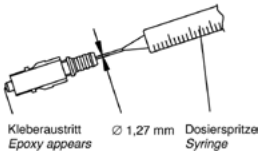


Microscope:
You use this to check that the fibres are polished correctly.

b) Fibre preparation and assembly taking the example of an SC plug on a fibre-optic glass fibre cable with the fast-cure adhesive (LC assembly is the same)

Shake the bottles of adhesive and activator before using for the first time.





1 Prepare the cable in accordance with the manufacturer's details.

2 Use the metering tip to apply activator to the glass fibres and around 5 mm of secondary coating.

3 Press the adhesive into the rear of the plug until it escapes from the hole on the plug pin's face end.

4 Slide the fibres back and forth in the plug two or three times and then hold them briefly at the stop.

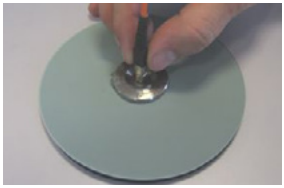
5 Spread the Kevlar braid evenly over the plug body. Slide crimp sleeve on up to stop. Crimp this with the crimping tool and cut off the protruding Kevlar braid with the Kevlar scissors.

6 Slide the anti-kink bushing forwards over the crimp sleeve and up to the plug body.

7 Score the protruding fibres with the stylus and break them off.

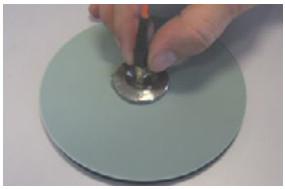
8 Hold the 30 µm (green) polishing foil in your hand, apply a little pressure and working in circular movements polish off the protruding fibres until only a little remains.

9 Place the 3 µm (pink) polishing foil on the base and evenly coat polishing foil with polishing liquid.



10 Insert the plug in the polishing fixture and polish the plug face end in figures of eight until adhesive can no longer be seen on the plug face end.

11 Place the 0.3 µm (grey) polishing foil on the base and evenly coat with polishing liquid.

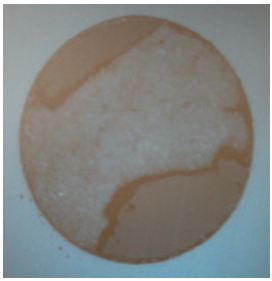


12 Insert the plug in the polishing fixture and polish the plug face end in figures of eight.

13 Insert plug in microscope (use adapter if necessary) and check the plug face end.

If the surface quality is inadequate (scratches), the plug must be polished again. The plug must be replaced if the fibres break out.

good



bad

14 Test the photoconductivity with a source of light.

Splicing

Splicing is the practice of connecting two glass fibres by fusing them so that they cannot be taken apart.
A special arc splicing device is used. The fibres, e.g. of the routing cables, are combined at their ends with "pigtails". The splicing device adjusts the trims of the glass fibres perfectly to one another. With modern devices, the trimming is fully automatic. The fibres are then fused (welded) with an arc. Depending on the quality of the splicing process, attenuation values of around 0.3 dB or with good splicing values of even less than 0.02 dB can be attained. From experience, we have attained an attenuation value of max. 0.1 dB with high-quality devices.

Splicing requires special equipment and the relevant experience.

Pigtail

- Pre-assembled glass fibre connection on which a FO connector has already been mounted by the manufacturer
- Used to connect optical components
- Goal: to reduce plug assembly work on site

Advantages of pigtails

- Low attenuation values and low-cost mechanical production
- Consistently good quality, defined ferrule surface as no manual work (polishing etc.) is needed

3.9 Measurement on the fibre-optic cable

This chapter describes how to assess your fibre-optic cabling. The measurement recommendations are based on the PROFINET commissioning guideline.

3.9.1 Attenuation measurement for fibre-optic cables

The most important parameter to monitor on a fibre-optic cable section is its attenuation. The insertion loss process (Figure 3.5) is the easiest way to do this. The measurement process detects losses in the optical fibres and their connections. Light is transmitted by a transmitter via reference fibre 2 into one end of the fibre-optic cabling. A calibrated receiver is connected to the other end of the fibre-optic cabling being tested via another reference fibre 1. The receiver measures the amount of light received and evaluates any losses incurred. The attenuation or insertion loss is usually stated in dB. The reference fibre 2 at the transmitter end is wound in several coils on a winding spindle with a defined diameter. The "mode mixer" produced in this way correctly distributes light into the reference fibre and prevents the measurement result from being affected by the radiation characteristics of the transmitter.

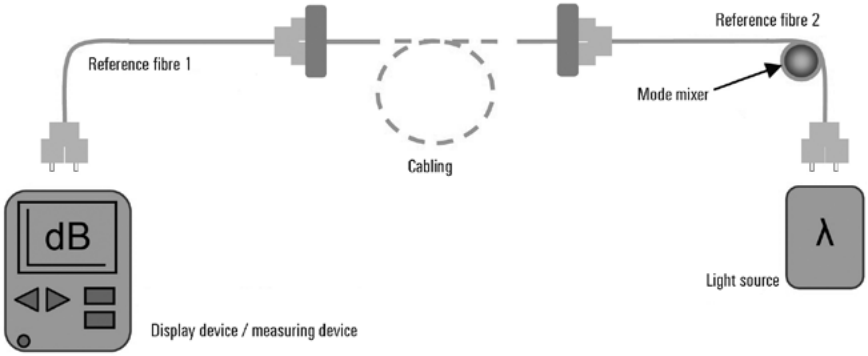


Figure 3.5: Principle of the attenuation measurement

- What type of fibre has been laid (singlemode fibre, multimode fibre, hard cladded silica, plastic optical fibre)?
- What plug type is used?
- Roughly how long a section has been laid?

Table 3.2 shows the types of glass fibre used by PROFINET and the permissible limit values for the PROFINET end-to-end link attenuation depending on the operating wavelength.

Origin	Singlemode glass fibre	Multimode glass fibre	PCF	POF
Typical wavelength	1,310 nm	1,300 nm	650 nm	650 nm
Maximum permitted end-to-end link attenuation	10.3 dB	62.5/125 µm : 11.3 dB ... 50/125 µm : 6.3 dB	4.75 dB	12.5 dB

Table 3.2: Maximum permitted PROFINET FO end-to-end link attenuation

There are two parts to the measurement. Firstly, the measurement setup has to be calibrated. To do this, the reference fibres are connected with one another as shown in Figure 3.5 and a reference measurement is taken. The receiver saves the light power received in this setup as a reference value for a section without attenuation.

The two reference fibres are then isolated and the section to be tested added. The actual section measurement then follows and the tester measures the light power received by the receiver and compares this with the saved reference value. The difference between the two measurements is displayed as the attenuation for the section added.

Defects on the plugs of the reference fibres to the test specimen influence the result. Only selected assemblies, approximating to an ideal plug, may therefore be used.

The connections must feature a high-quality polish. The reference fibre may be used for no more than 500 reference measurements. Then the connections have to be polished again. Please treat the reference fibres with great care. After 2,000 reference measurements, the reference fibres should be replaced. Please also note the details provided by the manufacturer.

Only special reference fibres may be used to connect the section requiring testing.

The measurement must be taken with the operating wavelength used later on and with the transmitter belonging to the measurement receiver. The transmitter, receiver and fibre type should be coordinated.

The limit values stated for the maximum permitted end-to-end link attenuation already contain an attenuation reserve. Do however take into account possible measurement inaccuracies and the tolerance of your measuring device. These should be included in the limit value for the maximum permitted end-to-end link attenuation.

Note in particular that the comparably high attenuation of POF coupled with several plug-in connectors reduces the maximum length of the fibre-optic connection.

3.9.2 OTDR measurement

Alongside the attenuation measurement procedure (insertion loss measurement procedure), the OTDR (Optical Time Domain Reflectometer) measurement procedure can also be used to measure fibre-optic cables. This can be used to determine faulty points in the fibre-optic cable.

To do so, the device transmits a signal into the fibre-optic cable via a forerun fibre. An overrun fibre is also fitted downstream of the section. Forerun and overrun fibres appropriate to the measurement cable should be used for OTDR measurements in order to minimise measurement errors.

Parts of the signal are reflected at connection points in the course of the fibre-optic measurement cable or interference points. The device now measures the strength of the reflected part of the signal and the time between the signal being sent and the reflection being received. From the measurement results, you can tell the location of defect and its influence.

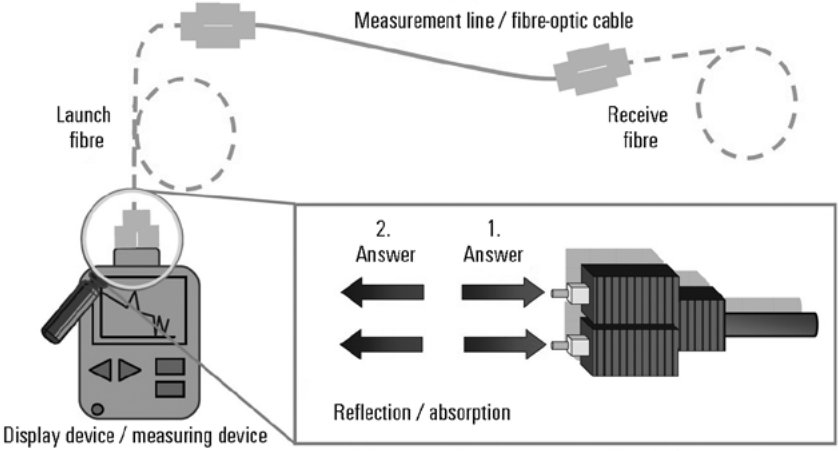


Figure 3.6: Principle of the OTDR measurement

Assessment of the measurement results requires experience because the results are not displayed in plain text. The measurement results are normally produced in graph form. Figure 3.7 shows an example of the measurement results to be interpreted.

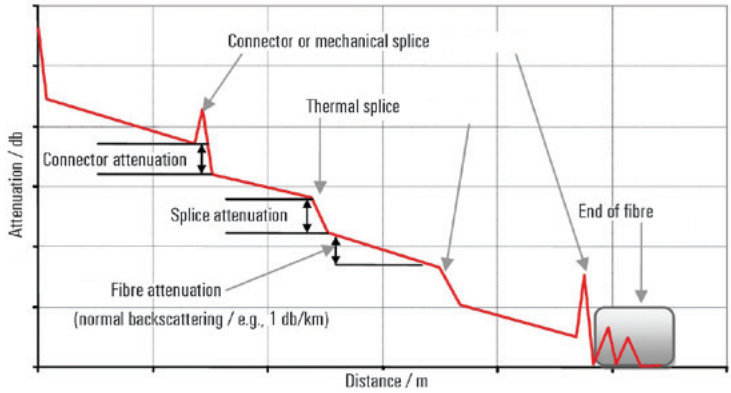


Figure 3.7: Example of OTDR measurement

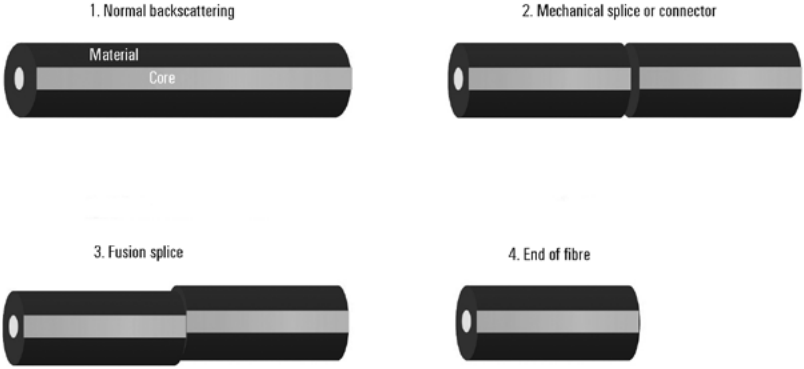


Figure 3.8: Fibre structure for OTDR measurement

Typical fibre connections are affected by various limitations which have a major impact on transmission behaviour. These limitations cause backscattering and additional attenuation. They include the various splicing connections and also the direct limitations of the fibres themselves from severe bending, fractures or cracks. Each of the limitations mentioned has its own typical reflection characteristic and can therefore be detected and analysed directly in the OTDR measurement.

(Source: PROFINET Commissioning Guideline, Version 1.01, July 2010)

3.10 Marking

Ensure that the cables are marked in a clean and permanently legible way. Use:

- marking sleeves + marking strips
- colour coding rings
- adhesive markers

3.11 Measurement and documentation

Cable measurements form part of the documentation required for many installations. This involves measuring the properties of the system's cables and documenting the quality of the network installed.

1. Set the measuring device to the appropriate transmission class.
2. Measure the transmission characteristics (copper) or attenuation characteristics (fibre-optic) of the cable.
3. Record the cable lengths.
4. Print out the values and add to the documentation.

Copper measurement

Use a mobile cable analyser to measure transmission parameters such as:

- connection assignment
- cable length
- near-end crosstalk (NEXT)
- far-end crosstalk (FEXT)
- return loss (attenuation) (RL)
- insertion loss (IL)

Fibre-optic measurement

After assembly, the most important measurement is the space-resolved attenuation measurement for the installed section using the "Optical Time Domain Reflectometer" measuring device (OTDR). The plug attenuation must be less than 0.5 dB. It is typically below 0.3 dB and very good attenuation values are less than 0.1 dB. Two wavelengths (850 nm and 1,300 nm) should be used for the measurement.
Acceptance then follows.

3.12 Checklist for installation

Requirements	Notes
Were the defined specifications observed?	
Is the cable type the planned type?	
Was the cable laid as planned?	
Were reserves provided for commissioning and extensions?	
Was the minimum cable spacing observed?	
Were the plug-in connectors used as planned?	
Are the manufacturer's plug-in connector test certificates available?	
Were all cables and connections tested?	
Were all test results documented?	
Do the transmission sections have sufficient reserves for the electrical parameters?	
Are all connections marked?	

Notes

4 Glossary

Industrial Ethernet has brought with it new specialist terminology. Some of the most important terms are briefly explained here.

4B/5B

A block coding diagram for FDDI and ATM. With 4B/5B coding, all data is divided into 4-bit units (a nibble) and recoded into 5-bit units (symbols) following a table.

10BaseT

Ethernet standard permitting a 10 Mbit/s transmission

10BaseFL

10 Mbit/s Ethernet via fibre-optic cabling

100BaseFX

100 Mbit/s Fast Ethernet via fibre-optic cable

100BaseSX

100 Mbit/s Fast Ethernet – identical to operations in 100BaseFX, but a 850 nm fibre-optic technology is used

100BaseTX

100 Mbit/s Fast Ethernet system via twisted-pair cables

802.1x

This is an authentication standard for VLAN or WLAN networks. It uses an authentication server which contains all PC login data with authorised access to the network. Users log on to the server with their normal login data and if the information (name and password) is correct, the connection to the network is enabled.
This standard is often used in universities to allow students to connect to the network without knowing the network key.

AUI (Attachment Unit Interface)

Interface between the transceiver and network card

Auto-negotiation

Auto-negotiation describes a process which allows network cards to independently recognise the correct transmission speed and the duplex procedure of the network port to which they are connected and to configure themselves accordingly.

(AWG) definition of cable diameter

AWG stands for American Wire Gauge, a designation commonly used in the US for the cable diameter. It does not detail the real diameter, but a range. It cannot therefore be converted accurately into a metric measurement. For a comprehensive comparison of AWG values with the metric cable diameter, refer to http://de.wikipedia.org/wiki/American_Wire_Gauge.

A brief overview is provided below

AWG	mm²
28	0.08
26	0.13
24	0.20
22	0.33
20	0.52
19	0.65
18	0.82
17	1.04
16	1.31
15	1.65
14	2.08
13	2.63
12	3.31
11	4.17
10	5.26
9	6.63
8	8.37
7	10.55
6	13.30
5	16.77
4	21.15
3	26.67
2	33.63
1	42.41
0	53.48

Bandwidth

The bandwidth states the amount of information that can flow from one location to another in a given time. Common units of measurement are Mbit/s or Gbit/s.

Baud

Bauds are the unit used to measure the modulation rate. A signal of a fixed duration is used for this measurement.

Bit

The word bit derives from binary and digit. It is the smallest unit of digital information, either a 0 or a 1.

Bit rate

The bit rate is also known as the speed of transmission, transmission rate or data rate. It describes the number of bits transmitted per unit of time (usually 1 second).

Bridge

According to their OSI definition, bridges connect sub-network protocols on layer 2 of the OSI reference model

Broadcast

As its name suggests, a broadcast transmission involves transmission from one point to all participants at the same time.

Bus

Buses are connection systems for electronic and electrical components. In terms of topology, a bus is always a physical medium to which the individual components are connected and which is terminated at both ends.

Category 5 / Kategorie 5

Designates conformity with the properties specified in IEC 11801. Category 5 (Cat.5) components can be used to set up networks which are suited to all Ethernet transmission standards up to 100 Mbit/s based on twisted pair cables.

Category 5e

Cat. 5e is an equivalent version of TIA/EIA 568 compared with Cat. 5 of IEC 11801 for use in 1.000BaseT networks.

CRC (Cyclic Redundancy Check)

CRC is an error detection process which reliably detects individual errors but only detects multiple errors with a high level of probability.

Crossover cable

A crossover cable is a special patch cable where the transmit and receive cables are swapped at one end. Crossover cables are usually used to connect two end devices.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

Access process in which the transmitters of a shared network only check the network for availability before transmitting (is not needed for full duplex mode)

DHCP (Dynamic Host Configuration Protocol)

A specially configured server can use the DHCP to dynamically assign IP addresses and other network parameters to computers in the network.

DTE (Data Terminal Equipment)

Every device in the network where a communication channel starts or ends. A station (computer or host) in the network which is able to transmit or receive data.

Ethernet

Ethernet is a networking technology for local networks (LANs).

Fast Ethernet

Today Fast Ethernet is a very commonly used version of the Ethernet offering 100 Mbit/s via category 5 or higher twisted-pair cables. The maximum permissible range is 100 metres.

Flow Control

Flow Control is a function for adapting transmission to the receptiveness of the receiver. Flow Control controls the transmission between transmitter and receiver by only allowing the transmitter to transmit an amount of data that the receiver can receive.

Forwarding

A process in which data is forwarded from one port to another in the switch.

Frame

A frame is a data transmission frame of the data link layer (layer 2 in the OSI model), containing the header and trailer information which the bit transmission layer needs for transmission. All frame formats have in common the start delimiter, the destination and source address, of course the data itself and a frame check sequence.

Frames

In networks, the data packets awaiting transmission with a standard size of 1518 bytes are known as frames in standard IEEE 802.3..

Jumbo Frames

All data packets (frames) larger than the standard size of 1,518 bytes are known as jumbo frames.
A header, containing the path, is always attached to each frame. In order to reduce the attachment of headers and increase the speed of transmission, the frame size can be varied. The problem with jumbo frames is that defective data packets can only be detected once the file has arrived in full. Given the longer transmission time, they are also only detected later on. Jumbo frames are mainly used for data backups.

Gigabit Ethernet / 10 GbE (10-Gigabit Ethernet)

Gigabit Ethernet is a version of Ethernet with a data transmission speed of 1,000 Mbit/s. 10 GbE operates in the same way with 10 Gbit/s. Weidmüller has a plug-in connector system with ***STEADY****TEC*® technology especially for these 10 GbE applications.

Fibre-optic cable (FO cable)

Type of cable with a glass fibre or plastic core which transports digital signals in the form of light pulses.

GPRS (General Packet Radio Service)

Extension of the mobile GSM standard for the packet-oriented transmission of data.

Half-duplex mode

The half-duplex process permits the alternating use of transmission cable in both directions. At the interfaces data can only be transmitted or received at any one time.

Hub

A hub is a form of data communication equipment which allows three or more devices to link up in a star topology. Incoming data is forwarded to all other participants as a broadcast. Hubs are no longer used with Fast Ethernet networks.

IEEE 1588

This is time synchronisation software for connected devices.
If I connect a router to a server, I can keep the time live using the IEEE 1588 standard.

IEEE 802.3

1. Working group of the IEEE (Institute of Electrical and Electronics Engineers) concerned with the CSMA/CD transmission process
2. Is used as a collective term or a synonym for LAN or Ethernet

IGMP snooping

IGMP snooping is a switch function. The switch snoops on the IGMP traffic on its ports. This prevents all ports from being flooded with multicast-traffic, which reduces the network load.

Internet

The Internet is the world's largest network. The Internet was developed in the 1960s for military purposes and released for commercial use in the 1990s. Data transmission on the Internet is based on the TCP/IP protocol.

IPv6

The IP address range of IPv4 features a potential 4294 967 296 addresses but is barely sufficient for today's network age. A larger Internet protocol was therefore produced a number of years ago. The address size is 128 bits compared with IPv4 which has 32 bits.
IPv6 addresses are usually written in hexadecimal (IPv4: decimal) where the number is broken down into eight blocks of 16 bits each (four hexadecimal points). These blocks are listed separately using colons (IPv4: full stops).
Example: 1475:0000:8233:04a3:1000:806e:0300:7368
If the IP address contains several zeros one after another in a segment, they can be replaced by one single zero.
Example: 1475:0:8233:04a3:10:806e:030:7368
If the IP address contains several blocks of zeros, they can be replaced by two colons one after another.
Example: 1475:0:0:0:0:806e:030:7368 = 1475::806e:030:7368
This scenario is only permitted once per IP address. The following example is not permitted.
Example: permitted: 1475:0:00:23ad:0:0:030:7368 = 1475::23ad:0:0:030:7368
Not permitted: 1475:0:00:23ad:0:0:030:7368 = 1475::23ad::030:7368
The last four bytes of the address can use the standard decimal notation. ::ffff:127.0.0.1 is therefore an alternative way of writing ::ffff:7f00:1. This form is used especially when embedding the IPv4 address space in the IPv6 address space.

Jabber

The Jabber messaging protocol is a process used in Ethernet networks that prevents one station from occupying the transmission medium for too long.

Collision

A collision is said to occur when two or more stations transmit in a shared data channel at the same time. Because the transmitted data overlaps, it is unusable.

Collision domain

A collision domain is a segment of a CSMA/CD network.
Ethernet networks according to IEEE 802.3 contain all end devices in a physical Ethernet segment (including those which are linked via a repeater) in the same collision domain.

LAN (Local Area Network)

For example inside a building

Layer-2-Switch

Data link layer. This is the level at which the unmanaged switches operate which can be incorporated in a network and only write an entry to the source address table using the MAC address and a physical port. This distinguishes the unmanaged switch from the hub. The hub forwards the data packets to all connected end devices while the switch only forwards to the end device stated in the source address table; if there is no entry in the SAT, the data packet is sent to all end devices as with a hub.

Layer-3-Switch

Network layer. This is the level at which the managed switches operate which provide functions above and beyond simply forwarding data packets. The operator can use the managed functions to configure various settings via the web interface on the switch. Examples of these could be control functions, monitoring functions, IP filtering, VLAN, prioritisation for quality of service and routing.

Link integrity test

This test checks whether an Ethernet connection is correctly connected and whether the signals are correctly transferred. It is a useful addition but does not guarantee that the link is fully functional.

Link layer

Link layer in the OSI reference model

Link pulse

A detection pulse which is transmitted from 10BaseT stations to 100BaseT stations for auto-negotiation

M12, d-coded

M12, d-coded is a 4-pole plug-in connector variant for Industrial Ethernet according to ISO IEC 61076-2-101. It undertakes data transmission according to cat. 5 and ensures IP 67 level of protection.

MAC address

A 6-byte long hardware address which is used to uniquely identify a device in the network

MDI

MDI stands for Medium Dependent Interface and refers to an Ethernet connection. It generally describes a network card's connection for the network cable – i.e. the network socket.

MDI-X

MDI-X stands for a crossed Ethernet connection. Transmit and receive interfaces were swapped.

Auto MDI/MDI-X (autocrossing) enables the automatic adaptation of a port's transmit and receive cable, i.e. the connected Ethernet cable (crossed/not crossed) and the remote station's configuration (MDI/MDI-X) are automatically detected and the port configured accordingly.

Media converter

Media converters convert electrical signals into optical ones and vice versa. Both copper and fibre-optic cables can thereby be used together in one network.

Multicast

Multicast is a form of transmission from one point to several participants at the same time.

NIC (Network Interface Card)

A NIC (network adapter card) is a PCB or other hardware component which connects the network directly to an end device.

OLE (Object Linking and Embedding)

Object Linking and Embedding (OLE) is an interface developed by Microsoft for linking and incorporating data between different applications. External, although only OLE-capable texts, graphics and tables can thereby be incorporated in other OLE applications.

OSI (Open Systems Interconnection)

OSI describes internationally agreed standards with which open systems function.

OSI 7 layer model

The OSI 7 layer model is a reference model which is used to depict the data transfer of networks/network adapters! It displays communication over seven levels.

Packet

A data packet is a defined arrangement of characters which is treated as one unit.

Patch cable

The patch cable is used in the distributor room to flexibly connect between the sub-distribution board and horizontal cabling. Patch cables may be both fibre-optic cables and copper cables. They are very flexible and require a small bending radius.

PAUSE

One single frame is sent to the available stations via full duplex mode to instruct the stations to reduce the transmissions.

PHY (Physical Layer)

1. Physical transmission layer
2. This designation is also used for a transceiver in Fast and Gigabit Ethernet.

Point-to-point technology

A connection variant which establishes a connection between two end devices. These point-to-point connections exist in the network environment, for wireless transmission in radio relay systems and in connections.

Port

A port is a hardware unit connection: usually an input/output channel for a computer or another hardware unit like a modem, router, hub or switch.

Port mirroring

Port mirroring can be used with a switch to mirror the data traffic of one port (for error analysis or for throughput measurements) onto another port.

Promiscuous mode

Promiscuous mode describes a receive mode for network devices. The device reads all the incoming data traffic to the network interface switched in this mode and forwards the data to the operating system for processing.

Propagation delay

The propagation delay is the time which a signal needs to pass from one point in the transmission channel to another.

Protocol

The data transmission protocol defines the rules for exchanging information in the form of a database. A protocol is an agreement on the connection setup, monitoring of the connection and its removal.

Quality of Service (QoS)

Quality of service covers all processes which influence the flow of data in LANs and WANs such that the receiver receives the service at a defined level of quality.

Radius

This is an authentication server for networks which contains a database with user names and passwords. If a user wants to log on to a network PC, he or she sends his or her login data to the authentication server which enables the PC if the log-in data is correct and blocks it if the data is incorrect.

RSTP (Rapid Spanning Tree Protocol)

The Rapid Spanning Tree Protocol (RSTP, IEEE 802.3w) is another way of establishing redundancy in a network.

Remote management

Remote management of a switch is undertaken by every network station fitted with Telnet or web browsers. It requires every switch to have its own IP address.

Repeater

A repeater is an active component which handles regeneration functions in Ethernet LANs, i.e. amplifies and processes signals.

Repeating hub

A repeater with more than two ports (is also simplified to hub)

RJ45 / RJ-45

The RJ45 plug-in system is an eight-pole miniature plug-in system for use in connections with STP and UTP cables, described by IEC 60603-7. RJ45 is characterised by its compactness and simplicity. It is used predominantly in horizontal wiring and wiring workstations.

SC duplex

SC duplex is a form of plug for fibre-optic cables for simply plugging and disconnecting. It features small dimensions and a high packing density. It is described in IEC 61754-4 and is used with singlemode and multimode fibres.

SC-RJ

The SC-RJ plug-in connector is an even smaller SC plug-in connector. The connector face is described in IEC 61754-24. It is used in singlemode, multimode and POF fibres.

Segment

In networks, a segment is part of a network limited by bridges, routers or switches. In LANs, we talk of a LAN segment or a collision domain.

Slot time

An important Ethernet parameter. The slot time corresponds to twice the signal dispersion speed between the two furthest apart network stations and the minimum packet length of 64 bytes. The longer the slot time, the lower the Ethernet performance.

SNMP (Simple Network Management Protocol)

SNMP enables central network management for many network components. The primary goals of SNMP are reduced complexity of management functions, the extendability of the protocol and the independence of network components. SNMP is a standardised network management protocol which can be used to exchange statistics regardless of platform and set parameters. Elements of a network (e.g. router, server, switch, printer, computer etc.) can be monitored and controlled from a central station.
Range of tasks of SNMP:

- Monitoring network components
- Remote control and remote configuration of network components
- Error detection and reporting

SNTP/NTP

This is a software solution which enables the time to be updated. With SNTP one single time server is used for synchronisation. With NTP several time servers are used and compared.
NTP uses more resources, but this problem is trivial given the high computing power of today's machines.

Spanning tree protocol

See RSTP

ST plug

This FO plug specified by AT&T (IEC 61754-2) is suited to both singlemode fibres and multimode fibres. The ST plug is a common plug used in LANs.

Star topology

In the star topology, the transmission stations are connected in a star shape around a central node. Star topologies can only exchange data indirectly via the central node.

Star-quad cable

A star-quad cable is a symmetrical copper cable whose four wires are stranded in parallel.

Straight-through

Unlike crossover cables, straight-through cables are patch cables whose transmit and receive cables are not swapped but are connected 1:1.

Station

Hardware components in a network: connected end device, server, router, phone, fax machine etc.

Switches

Switches are network components which perform switching functions. These switching functions can take the form of relaying functions in wide area networks and in local networks.

Topology

Structure of a network:

- Line topology
- Ring topology
- Star topology
- Tree topology

Transceiver

The word transceiver is made up of transmitter and receiver and describes transmission / reception equipment for fibre-optic networks.

Trunking

Trunking in Ethernet networks describes the parallel connection of several Ethernet links between the same devices. The transmission via the parallel links is used for bandwidth scaling.

Twisted-pair cable

A twisted-pair cable is a symmetrical copper cable consisting of pairs of wires which are twisted together.

VLAN (Virtual Local Area Network)

Virtual networks or virtual LANs are a technological concept for implementing logical network segments within a network. Such a network is produced using virtual routing.

Full duplex mode

With full duplex or duplex mode, both communication partners can transmit and receive at the same time.

Web server

A web server is a server program which provides files via the HTTP protocol. These files are usually web pages, images ...

Thanks

An undertaking like the best practice guide is never the work of just a handful of people. We would like to thank the following people for their advice, input and support: André Gerlach from Bildungsinitiative der Netzwerk-Industrie (BdNI), Manfred Patzke and Jan Klüter, and the many other people working hard behind the scenes.

Simon Seereiner Klaus Leuchs

Weidmüller – Your partner in Industrial Connectivity

As experienced experts we support our customers and partners around the world with products, solutions and services in the industrial environment of power, signal and data. We are at home in their industries and markets and know the technological challenges of tomorrow. We are therefore continuously developing innovative, sustainable and useful solutions for their individual needs. Together we set standards in Industrial Connectivity.

Weidmüller Interface GmbH & Co. KG
Klingenbergstraße 16
32758 Detmold, Germany
T +49 5231 14-0
F +49 5231 14-292083
info@weidmueller.com
www.weidmueller.com

Your local Weidmüller partner can be found on our website:
www.weidmueller.com/countries

Made in Germany

4 050118 412420

Order Number: 2053260000/05/2015/SMDM