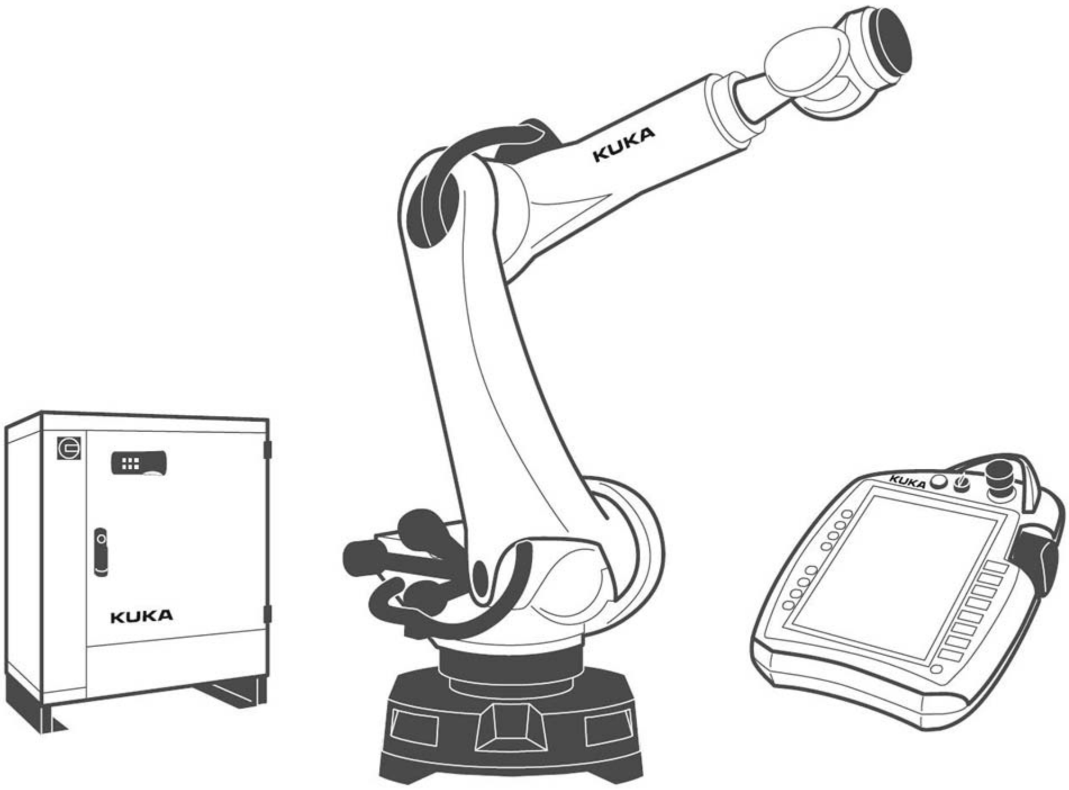
KUKA College

KUKA Roboter GmbH

Basic Principles of Network Technology

Handout to the Web Based Training (WBT)



Version: 28.09.2011

KUKA Roboter GmbH
Zugspitzstrasse 140
D-86165 Augsburg
Germany

Other functions not described in this documentation may be operable in the controller. The user has no claims to these functions, however, in the case of a replacement or service work.

We have checked the content of this documentation for conformity with the hardware and software described. Nevertheless, discrepancies cannot be precluded, for which reason we are not able to guarantee total conformity. The information in this documentation is checked on a regular basis, however, and necessary corrections will be incorporated in the subsequent edition.

Subject to technical alterations without an effect on the function.

Translation of the original documentation

Document: Handout_WBT_NWT_V1_en

Version: 28.09.2011

Contents

Welcome

Topic 1 Welcome

Welcome to the eLearning module “Basic Principles of Network Technology” from KUKA College.

This eLearning module introduces you to data transmission in KR C4-controlled robot cells.

You will find out about the basic network architecture in automation systems and the hardware and software used for data transmission.

Each lesson is followed by exercises to consolidate your newly acquired knowledge.

Once you have successfully completed the final test, you will be optimally prepared for your next steps in network technology.

KUKA College wishes you an enjoyable and successful learning experience!

You will need about 3 hours for the entire eLearning module.

Networks in robotic automation

Topic 2 Overview

In the same way that communication is an important part of our lives, it is also an important part of automation systems. The success of manufacturing systems is increasingly dependent on the ability of the controllers, robots and production machinery to exchange control commands and statuses effectively and without errors. Communication networks are the backbone of modern automation systems.

In this lesson, you will learn the fundamentals of typical communication networks in robot automation. Data exchange between the different network devices is illustrated by means of several application scenarios.

This lesson takes about 23 minutes.

Topic 3 Physical components of a network

A network is a structure in which different technological systems exchange data with one another.

Every data exchange involves a sender and a receiver, e.g. a PC and the network printer.

Sender and receiver do not exchange the data directly with one another.

All network devices are connected by cable to a **switch** which forwards the data from the sender to the receiver. This is known as **star cabling**.

The network cards of the sender, receiver and switches have their own power supply and can amplify the signals received. They are thus called **active components** of a network.

Multiple networks can be connected to each other via **routers**.

Topic 4 Networks in robotic automation

A typical automation network comprises the following networks:

- A **production network** with the controllers, production machinery and field devices of the production level
- A **company network** or **IT network** with the office workstations, shared hardware and archive servers

Topic 5 The production network

In industrial systems, a programmable logic controller (**PLC**) controls the entire system.

- The robot controllers and other production machinery are connected to the PLC.
- The field devices, such as the grippers, are connected to the robot controller.

The network of PLC, robot controllers, field devices and production machinery is the **production network** of a system.

A so-called field bus is used for the data exchange.

Topic 6 Connecting the field devices

Each robot controller exchanges data with a large number of field devices, e.g. with the valves for controlling the gripper.

The field devices are connected via **bus terminals** to a **bus coupler**.

This, in turn, is connected to the controller via a **field bus**.

- The robot controller and the field devices of the field bus system belong to the **production network**.
- For areas in which failsafe data transmission is essential, additional field bus-based networks that meet special safety requirements can be set up. These are referred to as **safety networks**.

Multiple networks can be operated via a single cable. Safety networks and “normal” networks are then connected to a single bus coupler.

Topic 7 Field bus standards

Within the field bus-based networks, the data exchange is carried out on the basis of industry standards for automation.

These include, for example, **PROFINET, EtherCAT** and **EtherNET/IP**.

Where failsafe data transmission is required, field buses that meet special safety requirements are set up.

The standards used are **PROFIsafe** or **FSoE – Fail safe over Ethernet**.

Topic 8 The company network

For remote maintenance, backups of the robot configuration, etc., the robot controllers are connected to the **company network**.

A switch distributes the data to the correct receiver.

Since the devices in a company network are mostly not field-bus capable – and do not need to be – data exchange is carried out on the basis of different standardized protocols, e.g. **TCP/IP protocols**.

Topic 9 Data exchange within the production network

The following simplified example illustrates data exchange within the production network.

A robot tends a press. Robot and press are coordinated by the higher-level programmable controller (**PLC**).

1. The PLC polls the status of the press via the field bus.
2. The PLC inquires of the robot whether it is ready to pick up a new blank.
3. The KR C4 then polls the different statuses of the connected field devices, e.g. the gripper, via the field bus.
4. The KR C4 evaluates the statuses and informs the PLC when the robot is ready to pick up a new blank.
5. The PLC instructs the KR C4 to pick up a new blank from the stack and load it into the press.
6. The KR C4 translates the command into individual control instructions for drive motors and valves.
7. The KR C4 informs the PLC as soon as the blank has been loaded and the PLC instructs the press to process it.

Topic 10 Master/slave procedure

Access to the field buses is controlled using the **master/slave procedure**.

- During data exchange within the production network, the PLC establishes the field bus as the higher-level controller and assumes the role of **master**.
  As **master**, the PLC is always authorized to send. The connected robot controllers are subordinate to the **master** and assume the role of **slaves**.
- In the case of data exchange between the robot controller and the field devices, the robot controller assumes the role of **master**.

The connected field devices are the slaves.

Alternative designations for **master** and **slave** include:

- **Controller** and **Device**, or
- **Producer** and **Consumer**.

Topic 11 Accessing the robot controller via the company network

Projects can be deployed via the company network:

- The robots are integrated into the company network via a switch.
- The service technician configures the field buses and parameterizes the control program of a robot conveniently from his office workstation. For this, he works with the central development platform **KUKA.WorkVisual**.
- The technician then transfers the project to the robot controller where it is automatically installed.
- The modified project can then be activated simply on the robot.

Topic 12 Accessing the robot controller via the Internet

Customers who grant KUKA Support an insight into the current situation on site receive particularly efficient and effective troubleshooting support.

The service technician on the hotline starts a **KUKA.Remote View** session and communicates an automatically generated session number to the customer.

The customer enters the session number in the user interface of his **KUKA smartPAD**.

The user interface is mirrored in the KUKA.Remote View session.

The **KUKA.Remote View** session grants the service technician access to the customer's robot controller. Errors in the customer's system are located and rectified as quickly as possible.

A precondition for remote maintenance via **KUKA.Remote View** is that the customer's robot controller has access to the Internet.

Topic 13 Archiving a project

Service technicians can archive projects using the **KUKA smartPAD**.

The archiving location is predefined by the start-up technician, e.g.:

- The hard drive on the control computer
- A USB memory stick
- A network drive as central archive

The archived project can be imported easily into other robot controllers.

Topic 14 Exercise

Network architecture

In a [____], the sender and receiver are connected via a distributor – typically a [____]. [____] are also distributor devices. They are used for data exchange with other networks.

A typical [____] comprises the PLC as higher-level controller, the production machinery, the robot controllers and the [____].

These are connected via bus terminals to a [____] which is connected in turn to the robot controller.

Data exchange between the specified components is carried out using [____].

[1] -> [Routers]

[2] -> [Company network]

[3] -> [Switch]

[4] -> [Production network]

[5] -> [Bus coupler]

[6] -> [Network]

[7] -> [Field buses]

[8] -> [Field devices]

Master/slave procedure

Access to the field buses is controlled using the master/slave procedure. What functions as the master and what functions as the slave when the PLC and KR C4 exchange data with one another?

Using the mouse, drag the labels onto the orange-highlighted placeholders.

Topic 15 Summary

In this lesson, you have learnt about the most important subnetworks in robot automation.

- The **production network** that links the devices of the field or robot level to those of the control or production level
- The **company network**

You now know that data exchange within the production network is based on field bus technologies with the higher-level controller taking on the role of the master and the devices to be controlled functioning as slaves.

Fundamentals of data transmission

Topic 16 Overview

In order for data from the sender to reach the correct receiver and be interpreted correctly by the receiver, all devices and components involved in the communication must speak the same language. They must be familiar with the rules used for exchanging data in their network.

In this lesson you will learn about the principles used for effective data transmission in communication networks, i.e. so that the receiver receives the data sent by the sender.

This lesson takes about 16 minutes.

Topic 17 Data packeting

The data to be sent are broken down into smaller blocks.

To ensure that the individual blocks reach the correct receiver and are re-assembled there in the correct order, additional data are added to the blocks step by step, e.g. the sender and receiver addresses and the consecutive number of the individual blocks.

The process of packing data into a packet is called **encapsulation**.

When the data packets are received, they are decapsulated step by step.

Topic 18 Layer models as theoretical model

The encapsulation of data and the transmission of the data packets are highly complex processes. The data transmission is thus broken down into individual steps by means of layer models which are processed in sequence.

The best-known layer models are the **OSI reference model** and the **TCP/IP model**.

The **OSI reference model** distinguishes between seven different layers, for example, and the **TCP/IP model** only four.

The following principles apply:

- One layer provides a service for data transmission, e.g. ensuring that the data packets are re-assembled in the correct order.
- On the sender side, data are added to every layer; on the receiver side, these are then removed again from the same layer in the data packet.

What is left is the user data – the original information.

Topic 19 Data transmission using the OSI reference model

The OSI reference model is the most important layer model for data transmission in networks. OSI stands for Open Systems Interconnection. The following simple example illustrates how a data packet is expanded from layer to layer. On the sender side, the layers are processed from top to bottom, i.e. from the seventh layer to the first.

- The seventh layer, the **Application Layer**, contains the function call of the user.

- In the **Presentation Layer**, the user data are converted to a format that is not application-specific so that they can be understood by the receiver, e.g. text is converted to ASCII format.
- In the **Session Layer**, the data are assigned to the application or process that is to be used for exchanging the data.
- In the **Transport Layer**, information is added that is required to ensure that all data packets are transmitted completely and re-assembled by the receiver in the correct order.
- In the **Network Layer**, the logical network addresses – the IP addresses – of the sender and receiver are added. IP addresses contain the address of the network and the address of the network device within the network.
- In the **Data Link Layer**, the physical addresses – the MAC addresses – of the network devices between which the data packet is to be transported are added.
  In the case of transportation to a different network, the MAC addresses of the sender and receiver are overwritten repeatedly on the way to the receiver.
- In the first layer, the **Physical Layer**, the data packets are encoded as electrical signals and sent to the cable.

At the receiver, the same data are evaluated in every layer as were added to that layer at the sender. The data are decapsulated step by step in the reverse sequence: from the first layer to the seventh.

Topic 20 Protocols as rules

Within a network, all devices and components involved in the communication must know the rules used for exchanging data packets.

These rules are defined in **protocols**. A protocol usually only governs the service of

Multiple protocols are often grouped together in **protocol stacks**.

The best-known is the TCP/IP protocol stack for Internet-based data transmission:

- The Transmission Control Protocol (**TCP**) is used, for example, for establishing a connection between two network devices.
- The Internet Protocol (**IP**) controls the way in which the data packets are forwarded.

Data transmission always involves the use of multiple protocols and/or protocol stacks. These can contain software and hardware specifications.

In its robot networks, KUKA uses industry-proven field bus standards, e.g. **PROFINET, EtherCAT** and **EtherNET/IP**. These standards are basically protocol stacks.

Topic 21 Exercise

Data packeting

What are the advantages of data packeting?

- The data of multiple network devices can be transmitted in parallel or overlapping in time. Without packeting, the data from one network device would first have to be transmitted completely before the data of another network device could be sent.
- Data transmission is more efficient. In the case of an error, only the incorrectly transmitted data packets have to be sent again, not all data.

- There are fewer data collisions, as the “impact surface” of smaller data packets is smaller.

OSI reference model

Data transmission in networks can be broken down into seven individual steps using the OSI reference model. Complete the graphic so that all layers/steps are processed in the correct sequence on the receiver side.

Using the mouse, drag the layers/steps onto the orange-highlighted placeholders.

- Function call of the user
- Convert the data to a format that is not application-specific
- Add logical network addresses with location information
- Encode data in electrical signals and send to cable

➔ [Physical Layer]

➔ [Network Layer]

➔ [Application Layer]

➔ [Presentation Layer]

Layer models

What does one layer make available to another layer?

- Service
- Packet
- Protocol

Topic 22 Summary

In this lesson, you have learnt that the user data are broken down into smaller data packets and sent together with a wide range of addressing and administration information.

You have learnt how data transmission is broken down into individual steps on the basis of theoretical models – e.g. the OSI reference model – and thus becomes easier to manage.

Furthermore, you know that protocols govern all aspects of data transmission within a network – covering both software and hardware.

Network adapters

Topic 23 Overview

Network adapters function as an interface between the computer and the network and are responsible for the entire data output and input traffic of the computer. Without network adapters, a computer can neither send nor receive data.

In this lesson, you will learn the tasks and some of the characteristics of network adapters.

This lesson takes about 9 minutes.

Topic 24 Tasks of a network adapter

Network cards implement the first and second layers of the OSI reference model.

They ensure that the data packets to be sent are converted into electrical signals and that the received electrical signals are converted back into data packets.

1. First of all, the network adapter converts the data packets into binary numbers, i.e. into a sequence of ones and zeros.
2. The network adapter then encodes the sequence of numbers in accordance with the system defined by the network protocols used.
3. Finally, the network adapter generates the voltage signals and sends them to the connected network cable.

Topic 25 Connection to network

Network adapters are either integrated into the motherboard of the PC or plugged onto it as separate circuit boards – so-called network cards.

Every network adapter has at least one port to which a network cable can be connected.

The status of the connection is generally indicated by means of LEDs. Example:

- The orange LED lights up if there is a connection to another device, e.g. to the switch.
- The yellow LED flashes if data are being transmitted.

Topic 26 Network cards in the automation network

Different network cards can be found in automation networks:

- Office PCs are generally fitted with **single network cards** with one port. These days, even single network cards support high data transmission rates.
- The KR C4 robot controller is fitted with a **Dual NIC** with two ports. Depending on the version, one port of the network card is routed outside the control cabinet, e.g. to enable connection of a service laptop to the KR C4.

Topic 27 Dual NIC network card in KR C4

The KR C4 controller is integrated into several networks.

With the two ports of the Dual NIC, the KR C4 can be connected, for example, to two networks that are physically separated from one another:

- To the KUKA Controller Bus (**KCB**) for internal data traffic for drive control
- To the KUKA Line Interface (**KLI**) for data exchange with the customer network

Furthermore, the controller can manage multiple networks that are logically separated from one another, i.e. virtual networks or **VLANs**.

The controller is integrated into two VLANs via the port that is used for the **KLI**: the field bus-based production network and the company network.

Topic 28 Exercise

Ports of Dual NIC

How many network cables can be connected to the Dual NIC in the KR C4?

- One
- Two
- Three
- Four

Network adapter connection

How are network adapters typically integrated into PCs?

- Network adapters are integrated into the motherboard of the PC.
- Network adapters are plugged onto the motherboard of the PC as expansion boards.
- Network adapters are installed in the connectors of the network cables.
- Network adapters are connected to the PC as separate, external hardware.

Topic 29 Summary

In this lesson, you have learnt that network adapters encode data as electrical signals, send them to the cables and decode received voltage signals as digital data.

You now know that the KR C4 robot controller is connected to at least three different networks via a Dual NIC network card with two ports.

Switches and routers

Topic 30 Overview

If only two devices exchange data with one another, they can be connected directly using a cable. If several devices exchange data with one another, a distributor device communicates between the senders and receivers.

In this lesson, you will learn about what distributor devices, such as switches and routers, are required for.

This lesson takes about 12 minutes.

Topic 31 What is a switch?

Switches are intelligent network distributor devices to which all devices in a network are connected.

Switches save which network device is connected to which port.

They read the receiver address from the data packets and forward them to the corresponding receiver. The direct routing of the data packets minimizes the load on the network.

New network devices can exchange data with all network devices as soon as they have logged onto the switch.

Topic 32 Managed and unmanaged switches

Depending on the network requirements, different types of switches are required:

- For normal IT networks, simple **unmanaged switches** are generally sufficient.
- **Managed switches** have an advanced range of functions and can be configured. Managed switches can, for example, manage multiple virtual networks (VLANs) of a physical network and prioritize data packets if required.

A Cabinet Control Unit (CCU) is installed as standard in the KR C4 as a managed switch. The CCU manages multiple virtual networks.

If required, further switches can be installed in the KR C4, e.g. to set up a separate safety network.

Topic 33 What is a router?

If data are to be exchanged with other networks, **routers** are required, e.g. if service hotline technicians use **KUKA.Remote View** to exchange data with customers' robot controllers via the Internet.

Typically, it is not the network devices themselves, but the switches of a network that are connected to the router.

Routers connect networks not only physically, but also logically, as routers translate between different networks with different protocols and data transmission rates.

Topic 34 Routing – the way through the network

Routers manage so-called routing tables with which they send the data packets along the best, i.e. fastest, route to the receiver.

- Typically, a router only knows its neighbors. The route itself is determined dynamically, i.e. not until the time it is sent.
- If required, static routes can also be configured.

The data packets are forwarded along the route, from one router to the next, until they reach the network of the receiver.

The passage from one router to the next is called a hop because the data packets “hop” from station to station.

Tip: The router hopping can be made visible with the system command “tracert”.

Topic 35 What is the difference between routers and switches?

In order to fulfill their tasks, routers are much more powerful than switches.

A **switch** only understands the physical addresses of the network devices, i.e. a switch performs the tasks of the first two layers of the OSI reference model.

A **router**, on the other hand, works with logical network addresses and can translate between different networks. A router performs the tasks of the first, second and third layers of the OSI reference model.

Furthermore, routers can be configured while switches cannot.

These days, the difference between switches and routers is becoming ever more fuzzy. Switches are becoming ever more intelligent and powerful and taking over the tasks of routers. Conversely, there are switch-capable routers.

Combinations of switches and routers are also called **Layer 3 switches** or **high-performance switches**.

Topic 36 Exercise

Switches and routers

In a certain company, three internal networks are to be set up over two different floors. All network devices are to use the high-speed printer in the basement and have access to the Internet. Drag the distributor devices onto the placeholders so that the physical network meets all communications requirements.

➔ [Router]

➔ [Managed switch]

➔ [Unmanaged switch]

Routing tables

Static routes to the directly neighboring devices are configured in the routing tables of different routers. Data are transmitted via the shortest route (indicated in orange) between a sender and a receiver. When router 2 fails, data transmission is interrupted.

Which routing table must be revised in order for the data to be transmitted via an alternative route?

- [R1]
- [R2]
- [R3]
- [R4]
- [R5]
- [R6]

Topic 37 Summary

In this lesson, you have learnt how switches forward the data packets within a network to the correct receivers and how routers forward the data packets from one network to another.

Twisted pair cables

Topic 38 Overview

Data transmission via cable is more efficient and more stable than data transmission via radio.

Depending on the specific circumstances in the building, data transmission via radio may not be possible.

Cables remain the standard transmission medium in industrial communication networks.

In this lesson, you will learn about the cable structure, performance features and connection standards for the most commonly-used cable type – the twisted pair cable.

This lesson takes about 20 minutes.

Topic 39 Cable structure

Twisted pair is the designation for a copper cable with up to 8 individual wires, pairs of which are twisted together.

- The cable pairs each consist of a single-colored wire and a wire with stripes of the same color: striped wires are positive, while single-colored wires are negative.
- For standards such as Ethernet and PROFINET, only 4 wires are used, i.e. 2 wire pairs: the orange ones for sending and the green ones for receiving data.
- For higher bandwidths (e.g. gigabit Ethernet), brown and blue wire pairs are also used for sending/receiving.

Ethernet allows different transmission media. In addition to twisted pair cables based on copper wires, these include, for example, fiber-optic cables based on glass fibers or plastic. In field buses, **fiber-optic cables** with a polymer optic fiber – so-called **POFs** – are used.

Topic 40 Why are the wires twisted?

Twisting the electrical conductors counteracts the reciprocal impairment of signal quality due to electromagnetic interference.

The greater the twisting of the cables, the better.

The following applies: Twisted pair cables should not be routed in a straight line where possible!

Topic 41 Shielding as protection against crosstalk

Wire pairs and/or conductor bundles can be protected against **crosstalk** by means of shielding.

- In the case of **shielded twisted pair cables**, the wire pairs are shielded.
- In the case of **unshielded twisted pair cables**, the wire pairs are not shielded.
- Cables with an overall shield, i.e. the conductor bundle is shielded, are called **screened twisted pair cables**.

- Cables without an overall shield are called **unscreened twisted pair cables**.

Electrically conductive metal foil or wire braiding are used as shields.

Shielding is important in the case of high transmission frequencies such as those required in automation networks. As a general rule: The weaker the shielding, the greater the distance that must be maintained between current-carrying components and cables. The stronger the shielding, the greater the outer diameter and the more difficult the cable is to work with.

Topic 42 Nomenclature in accordance with ISO/IEC-11801

Twisted pair cables generally have an abbreviation printed on them, describing the composition and structure of the cable.

The designation scheme is **x/yTP**.

x specifies the overall shielding and **y** the shielding of the wire pairs:

- “U” stands for unshielded (no shielding).
- “F” stands for foil shielding.
- “S” stands for braided shielding.

Topic 43 Twisted pair cables in industrial cabling

Networks in industrial applications require cables that are specially constructed for the specific application and place of use:

- In robust industrial environments, twisted pair cables with an overall shield and braided wire pair shields are used.
- In environments with high electromagnetic interference, cables with particularly strong shielding are required.
- There are also 4-wire cables with just 2 wire pairs.

Topic 44 Performance capability of twisted pair cables

Twisted pair cables are divided into 7 categories by performance capability. Cables of category 5 or higher are suitable for field bus networks.

The higher the category, the higher the maximum possible frequency and the higher the maximum possible data transmission rate.

The data transmission rate is determined by the frequency and the coding system. Depending on the coding system, more or fewer level changes are required for a character.

Tip: Information about the performance capability is usually printed on twisted pair cables.

In the KR C4, KUKA is currently using CAT-5 cables with a data transmission rate of 100 Mbit/s.

Topic 45 Cable limits of twisted pair cables

In the case of twisted pair cables, the cable length influences the actual transmission rate.

The greater the cable length, the more the signal is attenuated.

After a maximum of 100 meters, an active component (such as a switch) must therefore be inserted as a signal amplifier.

Topic 46 Standard RJ45 connectors

There are generally **RJ45 connectors** at the ends of twisted pair cables.

The individual wires are each connected to a contact in the connector.

The connector contacts to which the wires must be connected varies according to the specific connection standard.

Topic 47 Connection standards for RJ45 connectors

There are two different connection standards: **T568A** and **T568B**.

The only difference between these two standards is that the green and orange wires are interchanged.

The same connection standard must be used throughout a network!

Tip: The specified wire assignment can be read off the underside of a standard RJ45 connector.

Caution is required, however: Always check both connectors on the cable. **Crossover cables** – which are required, for example, to connect two computers directly to one another – cross over the wires for sending and receiving. In the connectors, the wires for sending and receiving are swapped.

Topic 48 Angled RJ45 connectors with locking mechanism

Special angled RJ45 connectors with a locking mechanism are used in the KR C4 robot controller.

- To lock the connector after plugging it in, you must push the blue retaining slide towards the socket.
  The plug-in connection is now vibration-proof.
- The connector must be released before it can be unplugged. To do so, pull the blue retaining slide away from the socket.
  When pulling out the connector, hold onto the connector and not the retaining slide. There is otherwise a risk of the retaining slide being torn off.

Topic 49 Exercise

Twisted pair cables

A cable manufacturer wishes to market its products using a new Internet shop that is to be set up. For the twisted pair cables, details about the cable structure in accordance with ISO/IEC-11801 must still be added. Complete the page by dragging the correct designations onto the placeholders that are highlighted in color.

➔ [U/U-TP]

➔ [F/F-TP]

➔ [SF/F-TP]

➔ [S/S-TP]

Connection standards

An additional workstation is to be integrated into an existing network. Connect the new network device to the switch. To do so, drag the required twisted pair cable to the placeholder that is highlighted in color.

➔ [T568A]

➔ [T568B]

Topic 50 Summary

In this lesson, you have learnt about the most important characteristics of the most commonly-used network cables.

- You now know that industrial networks require twisted pair cables of category 5 or higher, why the wires are twisted, and that shields of metal foil or wire braiding protect against interference such as crosstalk.
- You have also learnt that signals transmitted via twisted pair cables must be amplified after a maximum of 100 meters.
- Furthermore, you also know that when wiring network devices, it must be ensured that the cables and connectors within the network are connected in accordance with the same standard.

Addressing

Topic 51 Overview

Other people can track you down by means of your address and telephone number. Similarly, every network device in a network has a unique address by means of which it can be accessed.

In this lesson, you will learn what types of network addresses exist, how the addresses are structured and how a network device receives its address. You will also learn how the data packets get from the sender to the receiver by means of addressing.

This lesson takes about 28 minutes.

Topic 52 What is a MAC address?

Every network device has a unique hardware address assigned by the manufacturer: a so-called **MAC address**.

- A MAC address consists of the manufacturer number and the device number.
- MAC addresses cannot be changed. On network cards, for example, they are saved in a read-only memory (ROM).
- Network distributor devices, such as **managed switches** and **routers**, can receive data packets, modify them if required, and forward them. For sending and receiving, they require a MAC address of their own.
- **Simple switches** forward data packets without modification. They have no MAC address of their own.

Topic 53 What is an IP address?

In addition to the MAC address, each network device has a logical address that is unique within a single network: a so-called **IP address**.

- The IPv4 addresses commonly used today are 32-bit binary numbers which, for the sake of greater legibility, are written as four decimal numbers separated by full stops.
- Similar to a telephone number, an IP address consists of an area code – the **network address** – and a line number – the **host address**. All network devices within a network have the same network address. Each network device can be unambiguously identified by its host address.
- The IP address with the host number 0 is the IP address of the network.
- As standard, the last IP address is used as the **broadcast address**. Data packets to the broadcast address are forwarded to all hosts in the network.

Topic 54 Why are IP addresses required?

IP addresses are required for two reasons:

1. Firstly, unlike MAC addresses, IP addresses contain information about the location of a network device.

2. Secondly, the IP protocol used for data transmission via the Internet specifies the IP addresses.
   Industry standards based on Internet technology thus also use the IP protocol.

Note: Without IP addresses, it is not possible to exchange data either within a network or between networks, even if the MAC addresses would be sufficient for data transmission within a network!

Topic 55 Public IP addresses

Network devices that want to exchange data via a public network, e.g. the Internet, require a public IP address.

These are issued centrally by the Internet Assigned Numbers Authority (**IANA**) to regional issuers who, in turn, issue IP addresses and IP address ranges to large companies or local issuers, e.g. Internet Service Providers.

The central issuing of IP addresses ensures that every network device, even in a network the size of the Internet, sends and receives data with a unique IP address.

For this reason, the network devices are also routable, i.e. they can be found in the network by means of their IP address.

Note: If you surf the Internet from your PC at home, you do so using a public IP address.

Topic 56 Private IP addresses

Private networks are self-contained. When configuring a closed network, any IP addresses can be issued provided that they are unique.

IANA has also reserved a number of IP addresses for private use. By convention, data are not forwarded to these private IP addresses in the Internet.

The last of the 4.3 billion IPv4 addresses were issued in February 2011. The new standard is called IPv6 and is designed to create 340 sextillion addresses. An IPv6 IP address is 128 bits long, while the old IPv4 addresses are only 32 bits long.

Topic 57 Conversion of private IP addresses to public IP addresses (NAT)

Network Address Translation (**NAT**) allows network devices to exchange data via the Internet using a private IP address.

The router converts the private IP address of the sender to a public IP address and vice versa.

- The router enters a dynamically assigned IP address as the sender in the data packet.
- In replies, the router replaces the dynamically assigned IP address with the private IP address of the original sender.

NAT has the following advantage: since multiple network devices can exchange data via the Internet using the same public IP address, fewer public IP addresses are required.

Topic 58 Static IP addresses

Network devices that are to be permanently accessible in the network require a **static IP address**. These include, for example, routers, network printers and servers hosting an Internet page.

Instead of using static IP addresses, it is also possible to surf on the Internet using meaningful names – so-called **URLs**.

The Domain Name System (**DNS**) that is available worldwide translates the static IP addresses of the Internet into names and vice versa.

Topic 59 Dynamic IP addresses

Dynamic addressing by means of the Dynamic Host Configuration Protocol (DHCP) is widespread in local networks:

- A pool of IP addresses is managed on a server.
- When a connection is established, the network device is assigned an IP address from this pool.
- The IP address is only valid for a limited period of time – the so-called **lease time**. Once the **lease time** has expired, a new IP address is assigned.

Advantage: New or different network devices can be integrated into a network without the need for additional configuration work.

Internet Service Providers use dynamic addressing via Point-to-Point Protocol (**PPP** or **PPPoE**) to save IP addresses.

Topic 60 Traditional IP address classes

In order to meet the requirements of large, medium-sized and small networks, various IP address classes have been defined by IANA, the central issuer of public IP addresses: A to D.

In decimal notation, the IP address class can be recognized from the first number.

The number of digits reserved for the host address varies according to the IP address class. The number of network devices that can be integrated into a network varies.

Reminder: In the IP address of the network, the host address is zero. The network with the IP address 165.067.0.0 belongs, for example, to class B – together with a total of 16,384 different networks. In each of these networks, the last two digits are used for the host address; up to 65,534 network devices can be connected.

Topic 61 Today: IP addresses with variable address boundary

The traditional address classes are not very flexible and IP addresses remain unused, particularly in small networks.

For this reason, Classless Inter-Domain Routing (**CIDR**) was introduced in the 1990s. This allows free division between the network address and the host address.

In order to derive the network address from the IP address, a **subnet mask** is placed over the IP address as a filter:

The following applies:

- A “0” in the subnet mask blocks the number in the same group in the IP address.
- The value “255” (the maximum possible value for a group) lets the number through.
- The result of this link is the network address – the address with which the router works.

Topic 62 Determining the MAC address of the receiver

The IP addresses issued during network configuration are known to all network devices.

According to the rules of the IP protocol, however, a data packet requires not only the logical address within the network, but also the physical address of the hardware: the MAC address.

How does the sender find out the MAC address of the receiver?

Easy: by asking the receiver for its address.

This task is performed by the **Address Resolution Protocol**.

Topic 63 Address Resolution Protocol (ARP)

To determine the MAC address of the receiver, the Internet protocol of the sender transmits a data packet to its ARP service or **Address Resolution Protocol**.

If the MAC address of the receiver has already been saved from a previous request, the data packet is sent to the receiver without delay.

Otherwise, the sender sends a so-called ARP request to all network devices in its network. This procedure is also known as **broadcasting**.

The network device with the requested IP address returns its MAC address.

The ARP service temporarily saves the MAC address so that all subsequent data packets can be sent directly to the receiver.

Topic 64 Sending to receivers in other networks

In the case of data exchange with network devices outside the network, the MAC address of the next receiver in each case is entered in the data packet.

1. The sender enters the MAC address of the router (requested, for example, via an ARP request or copied from the ARP cache) as the receiver MAC address and sends the data packet.
2. The switch forwards the data packet to the router.
3. The router looks up the best way through the network in its routing table.
4. It replaces the original sender MAC address with its own MAC address and enters the MAC address of the next node on the way to the receiver as the receiver MAC address.
5. The MAC address of the next router in each case is also determined by means of an ARP request if necessary.
6. This procedure is repeated all the way down to the last router in the chain.
7. When the switch of the receiver network receives the data packet, it forwards it to the receiver.

Topic 65 Exercise

MAC addresses of switches (test)

Do switches need a MAC address?

- No.
- Only switches performing routing tasks need a MAC address.

- Yes. All network devices need a MAC address.

IP address(es) of Dual NIC (test)

The KR C4 is connected via the two ports of the Dual NIC network card to two physical networks: the KUKA Controller Bus (KCB) and the KUKA Line Interface (KLI).

Since multiple networks can be operated with a single cable, the KR C4 exchanges data, via the port reserved for the KLI, with two logical networks: the company network and the production network.

How many IP addresses does the Dual NIC have?

- One.
  The following rule applies: a network adapter requires a single, unique IP address – irrespective of how many ports it has.
- Two – one for each physical network.
  The following rule applies: a network adapter requires a unique IP address for each port. -> [b]
- Three – one for each logical network.
  The following rule applies: a unique IP address is required for each network. -> [c]

Determining the network address

Determine the network address of the following IP address. Drag the correct network address to the placeholder that is highlighted in color. {T3 >>> Address 160.87.62.118 with subnet masks: 255.255.0.0 }

➔[1]

➔[2]

➔[3]

➔[4]

➔[5]

➔[6]

➔[7]

Topic 66 Summary

In this lesson, you have learnt that not only the physical address of the hardware is required for Internet-based data exchange, but also the logical address within the network.

- You now know that public, centrally managed IP addresses are required for data exchange via the Internet.
- If the routing procedure **NAT** is configured on the router, network devices with a private IP address can also exchange data via a public network.
- With the aid of the **DHCP** protocol, IP addresses can be issued dynamically (i.e. only for the duration of data exchange) so that multiple network devices can use the same IP address within a network – albeit not simultaneously.

You have also learnt how to determine the network address and host address of a network device using the subnet mask.

Characteristics of a network

Topic 67 Overview

In addition to the security of data transmission, the data transmission speed is also an important requirement for networks. Generally speaking: the faster, the better. But how fast is your network?

In this lesson you will learn to distinguish between frequently-used characteristics for the data transmission speed.

This lesson takes about 14 minutes.

Topic 68 Data transmission rate

The data transmission rate specifies how much data can be transmitted in one second.

It is a constant value and takes into consideration all transmitted data.

- The **data transmission rate** is typically specified with the units Mbit/s or Mbyte/s.
- The maximum data transmission rate of the network devices generally differs.
  In the case of a network card, the maximum data transmission rate depends, for example, on the system clock of the network card.
  Cables also have a data transmission rate.
- If the data transmission rates of the components are different, it is the component with the slowest data transmission rate that determines the speed at which data are transmitted and may constitute a bottleneck.
- For this reason, all components in a network ideally work with the same data transmission rate.
  In the case of configurable devices, this is easy to achieve: you set the same data transmission rate for all components. Or – better still – you set a data transmission rate for one component and select the setting **Autonegotiation** for all other components. The network devices then negotiate the most favorable data transmission rate among themselves.
  Important: If **autonegotiation** is activated for all components, no connection is established.

Topic 69 Network capacity

Like the **data transmission rate**, the **network capacity** is also an expression of how much data can be transmitted in one second.

Unlike the **data transmission rate**, the **network capacity** does not take all data into consideration, but only the user data that are transmitted *without errors* in one second.

The following data are not taken into consideration:

- The **protocol overhead**, i.e. address and transport information that is required for processing the data transmission.
- Data packets that are sent repeatedly for safety reasons, e.g. in order to be able to detect transmission errors.
- Data packets that cannot be decoded correctly, e.g. due to interference, such as attenuation or crosstalk, and have to be sent repeatedly.

Topic 70 Data transmission rate versus network capacity

- Unlike the data transmission rate, the network capacity is a variable and subject to fluctuation.
- The maximum data transmission rate is greater than the network capacity.
- The **network capacity** is the speed perceived by the receiver. From the point of view of the receiver, data transmission is completed when all user data have been received without errors.

Topic 71 Network overload

If the data traffic within a network exceeds the data transmission rate, the network capacity drops or the data transmission is even canceled.

This may be caused, for example, by sending large quantities of data or large numbers of broadcasts.

Furthermore, the connection to other networks can be interrupted by hacking.

In this case, the router signals “Denial of Service”.

Topic 72 Double data transmission rate with duplex mode

Network devices can work in full or half duplex mode:

- In full duplex mode, data are sent and received simultaneously. The data transmission rate is thus doubled.
  These days, all devices are full-duplex-capable.
  Field buses require full duplex operation.
- In half duplex mode, data are sent and received alternately.
  You will rarely still come across devices that are only half-duplex-capable.

Topic 73 Exercise

Data transmission rate versus network capacity I

Network capacity and data transmission rate specify how much data can be transmitted in one second. Unlike [______], [_____] only takes the user data arriving at the receiver without errors into consideration.

The same data transmission rate [______] be configured for the network devices and distributor devices. Generally, the data are transmitted within the network at the [______] data transmission rate.

The network capacity depends on various factors, e.g. the quantity of data to be transmitted. It is a variable.

Almost all devices work in [______]. Data can be transmitted [______], meaning that data can be sent and received [______].

[1] -> [Half duplex mode]

[2] -> [Network capacity]

[3] -> [in one direction only]

[4] -> [Full duplex mode]

[5] -> [consecutively]

[6] -> [lowest configured]

[7] -> [in both directions]

[8] -> [simultaneously]

[9] -> [must]

[10] -> [must not]

[11] -> [highest configured]

[12] -> [Data transmission rate]

[13] -> [should]

[14] -> [average]

Data transmission rate versus network capacity II

Is the network capacity generally greater or less than the data transmission rate?

- The network capacity is generally greater than the data transmission rate.
- The network capacity is generally less than the data transmission rate.
- The difference between the network capacity and the data transmission rate is so small as to be negligible. The two terms are thus often used as synonyms.

Topic 74 Summary

In this lesson, you have learnt about the characteristics for the data transmission speed of a network:

- the **data transmission rate** as a gross value, and
- the **network capacity** as the tangible net value for the receiver.

Furthermore, you now also know that an excessive load on the network, e.g. data traffic that exceeds the data transmission rate, causes the data transmission to slow down or even stop.

Important protocols and industry standards

Topic 75 Overview

Within a network, protocols specify the rules used by all devices and components involved in the communication for exchanging data.

The Internet – the best-known and largest network – uses over 500 different protocols, for example.

Multiple protocols are often grouped together in **protocol stacks**, some of which have become established industry standards.

This lesson contains an overview of the most important Internet protocols and the industry standards that are relevant for networks in robot automation.

This lesson takes about 14 minutes.

Topic 76 HTTP and HTTPS

The Hypertext Transfer Protocol (**HTTP**) controls the loading of websites from the World Wide Web into a web browser.

HTTPS is used for data transmission that is secure against tapping, e.g. for transmission of personal data.

HTTP and **HTTPS** are assigned to the uppermost layers of the most commonly-used layer models.

Topic 77 FTP

The File Transfer Protocol (**FTP**) is a network protocol for transferring files.

Like HTTP and HTTPS, FTP is assigned to the uppermost layers of the layer models.

Topic 78 TCP and UDP

Two widespread protocols are the Transmission Control Protocol (**TCP**) and the User Datagram Protocol (**UDP**).

They control the data flow and are assigned to the Transport Layer.

- **TCP** is used when error-free data transmission is required, i.e. when it is important for all data to be received completely and in the correct sequence by the receiver. This is necessary, for example, when displaying websites.
- **TCP** achieves this by means of additional header data, e.g. a checksum and a sequence number.
- **UDP** is used when the priority is on fast transmission of large data quantities, and incorrect or missing data packets are not conspicuous, e.g. for the transmission of music, video and live streams.
- With **UDP**, fewer data are transmitted for the sake of higher network capacity.

Topic 79 Ethernet and Industrial Ethernet

The **Ethernet protocol** is the most widely-used standard protocol in IT networks and office environments.

It includes specifications regarding cable type, connectors and transmission of the electrical signals and is assigned to the lower layers of the layer models.

- A distinction is made between different types of Ethernet protocols according to the performance of the network, e.g. 10 Mbit/s Ethernet or 10 Gbit/s Ethernet.
- Industrial Ethernet is the generic term for Ethernet systems in industrial environments. In addition to common protocols, such as TCP/IP, they also use other secure transmission protocols. The protocols vary from system to system, i.e. from manufacturer to manufacturer.
  With the Industrial Ethernet Protocol, networks meet the requirements of robust environments and can be simply integrated into an existing office IT network.

Topic 80 PROFINET and PROFIsafe

As the name suggests, **PROFINET** is an industry standard that has been specially developed for communication between automation components and field devices.

- **PROFINET** is based on Industrial Ethernet and uses TCP/IP for the transmission of data that are not time-critical.
- There are various different protocol versions for the transmission of time-critical data, e.g. **PROFINET RT** for real-time communication and **PROFINET IRT** for cycle-synchronous real-time communication.
- **PROFIsafe** is a supplement to PROFINET and enables error-free data transmission.

Topic 81 EtherCAT and FSoE

Ethernet for Control Automation Technology (**EtherCAT**) is a real-time-capable field bus for industrial automation.

In the case of EtherCAT, a large data packet, a so-called telegram, is processed cyclically in the network, starting with the master. A certain storage space is reserved for each slave. Within this range, it reads or writes user data and forwards the telegram to the next slave.

Advantages

- **EtherCAT** networks can be set up using existing Ethernet networks.
- With **EtherCAT**, it is possible to dispense with a switch so that common line, tree and ring cabling is also supported in field bus systems.

Safety over EtherCAT – also called FailSafe over EtherCAT or FSoE – can be used to transmit safety-relevant data.

Topic 82 Ethernet/IP

EtherNet/IP is another real-time-capable field bus for industrial automation.

- **EtherNet/IP** expands Ethernet to include the Common Industrial Protocol (**CIP**) and ensures that the commonly-used transport protocols TCP/IP and UDP can also be used in automation networks.
- For particularly short cycle times, time-critical data are transmitted via the more compact **UDP**.

- Data that are not time-critical are transmitted via the more secure **TCP**.

Topic 83 Exercise

Protocols for data transmission via Internet (test)

Industry standards in robot automation use many protocols that are also used on the Internet. Assign the following well-known Internet protocols to the layers of the OSI reference model or TCP/IP layer model.

➔ Ethernet with specification of cable, connectors and signal transmission

➔ TCP (Transmission Control Protocol) for controlling the data flow

➔ IP (Internet Protocol) for forwarding data packets on the basis of IP addresses

➔ HTTP (Hypertext Transfer Protocol) for loading websites into a web browser

Topic 84 Summary

In this lesson, you have learnt about the most important Internet protocols and a number of industry standards for field bus systems in automation.

Most industry standards are based on general Internet protocols, such as **TCP, UDP** or **Ethernet**. Some industry standards, however, used modified forms of the protocols.

It must therefore be ensured that all components in the network support the selected industry standard, e.g. **PROFINET, PROFIsafe, EtherCAT, Safety over EtherCAT** / **FSoE** or **EtherNet/IP**.

Virtual networks (VLANs)

Topic 85 Overview

Many network architectures map the hardware: the network devices are connected to a switch and exchange data with other networks via a router.

Intelligent hardware can reduce the hardware still further.

In this short lesson, you will learn about the advantages of virtual networks.

This lesson takes about 10 minutes.

Topic 86 Virtual networks (VLANs)

Managed switches are able to divide the network devices connected via one physical network into multiple logically separated network segments, so-called virtual networks or **VLANs**.

The division into virtual networks is carried out using different address spaces which are managed by the managed switch.

A virtual network has the same properties as a “normal” hardware network. For example, only the network devices of one VLAN can exchange data directly with one another.

Topic 87 Advantages of VLANs

What are the advantages of setting up VLANs?

- Less hardware is required with VLANs: one intelligent switch takes over the tasks of multiple simple switches.
- VLANs increase flexibility, as the division of the network segments is independent of location and cabling.
- VLANs increase the performance of the entire network, as the data transmission rates of the network segments can be adjusted according to the specific application, e.g. a higher data transmission rate can be used to prioritize transmission within a network segment.
- VLANs reduce data traffic, as broadcasts are not sent to all connected network devices, but only to the network devices of a single network segment.

Topic 88 VLANs in the KUKA network

The Dual NIC in the KR C4 performs the task of a managed switch and can, if configured accordingly, be integrated into two networks via the port used for the **KLI**:

- In the field bus-based production network
- In the company network

In this case, the Dual NIC manages two virtual networks: typically “Virtual 5” and “Virtual 6”.

- “Virtual 5” is provided with a static IP address.
- “Virtual 6” is assigned a dynamic IP address by the DHCP server when the connection is established.

Note: PROFINET requires static IP addresses. Other field bus standards also allow dynamic IP addresses. For PROFINET, DHCP must not be configured for “Virtual 5”.

Topic 89 Exercise

Distributor devices in VLANs

If virtual networks are used, a distributor device must manage different address spaces.

- What network distributor devices can perform this task?
- Configurable (i.e. managed) switches -> [a]
- Standard routers -> [b]
- Combinations of switches and routers, also called Layer 3 switches or high-performance switches -> [c]

Connection to VLANs

The Dual NIC network card in the KR C4 performs the task of a managed switch. The KR C4 can be integrated into the company network and production network using the Dual NIC.

How many cables are required to connect the KR C4 to the company network and production network?

- Two cables. The Dual NIC is equipped with two ports. One port is reserved for connection to the company network, the other for connection to the production network.
- One cable. The Dual NIC is equipped with two ports. Only one port is required for connection of the KLI. The KLI controls data exchange between the KR C4 and the company network and between the KR C4 and the production network.

Network addresses for VLANs

The workstations, servers and printers of a department are divided by workgroup into three virtual networks. A single managed switch controls the data exchange within the different VLANS. A workstation is to be switched from VLAN 2 to VLAN 3. Assign it a new IP address. Drag the correct IP address to the placeholder that is highlighted in orange.

➔TCP (Transmission Control Protocol) for controlling the data flow

➔192.198.17.10

➔10.255.255.255

➔198.100.100.0

➔10.192.08.18

Topic 90 Summary

In this lesson, you have learnt how the KR C4 can be integrated into the customer’s company network and production network using a single cable.

KUKA tools for network configuration

Topic 91 Overview

Programming, configuration, archiving, simulation and diagnosis are routine tasks when working with KR C4 controllers.

These tasks can be performed conveniently using a single software package: **KUKA.WorkVisual**.

KUKA.WorkVisual contains all tools and functions for successful configuration of KR C4 controllers.

Furthermore, **KUKA.Virtual Remote Pendant** makes it possible to access KR C4 controllers from the workstation.

This lesson illustrates the new **KUKA.WorkVisual** and **KUKA.Virtual Remote Pendant** software by means of a number of examples.

This lesson takes about 10 minutes.

Topic 92 KUKA.WorkVisual

KUKA.WorkVisual allows integrated engineering in automation.

- The field buses of the production network are configured in the **field bus configuration**.
  The inputs and outputs of the robot controller and the inputs and outputs of the field devices are mapped in the **mapping editor**.
- The **online administration** displays system information of all KR C4 controllers in the network and is thus an effective tool for diagnosis and monitoring.
  In the **diagnostic monitor**, it is even possible to display the individual operating states of the control components.
- The **drive bus configuration** can be conveniently edited in the topology view. Thanks to the ease of operation, the connections of the **KUKA Controller Bus** can be modified quickly, e.g. to add external axes to the drive bus.
- A graphically oriented editor simplifies **programming** by highlighting syntax, allowing quick entry of commands and offering standard functions, such as copy, replace, find and undo.
- For **diagnostic purposes**, oscilloscope trace recordings can be made.
  The configured trace parameters (e.g. motor currents, speeds and signals) are output in a trace evaluation.
- Configurations and programming are saved as **projects** and then activated on the controller.
  The systematic storing of the project data allows the simple archiving and loading of projects.
  The loading of projects onto a controller is called deployment.

Topic 93 KUKA.Virtual Remote Pendant

The **KUKA.Virtual Remote Pendant** software package can be used to establish a connection from a computer in the company network to a robot controller in the production network.

- The user interface is then displayed on the screen of the workstation and not on the **KUKA smartPAD**.

- Inputs made on the workstation are forwarded to the controller and, conversely, controller outputs are forwarded to the workstation.
- Once all safety requirements have been met, the robot can be controlled from the workstation.

Single Point of Control

For safety reasons, robot motions may only be initiated from a single location ("Single Point of Control"). In the case of remote access, it must be ensured that there is no danger of collisions with persons or devices in the system when the robot is moved. The safety gate of the robotic cell must always be closed.

Topic 94 Exercise

KUKA configuration tools I

Which software tool is used for all cell configuration steps?

- KUKA.WorkVisual
- KUKA.Virtual Remote Pendant
- Visual Project
- KUKA smartPAD

Configuration tools II

Which software tool allows control of the robot from the workstation?

- KUKA.WorkVisual
- KUKA.Virtual Remote Pendant
- KUKA Controller Bus
- KUKA smartPAD
- KUKA.Remote View

Topic 95 Summary

In this lesson, you have gained a first impression of the future tools for configuration and maintenance of KR C4-controlled robotic cells: **KUKA.WorkVisual** and **KUKA.Virtual Remote Pendant**.

In practical operation, these software tools are characterized by their large range of functions and ease of operation.

Fault diagnosis and remote maintenance

Topic 96 Overview

Industrial-grade hardware components and correct cabling are prerequisites for a fully functioning industrial network.

If errors occur in data transmission, simple commands from the Microsoft Windows operating system can help with troubleshooting and maintenance.

In this lesson you will learn about a number of Windows system commands and tools that you can put to good use in your everyday work.

Furthermore, you will receive a preview of **KUKA.Remote View**, KUKA’s remote diagnosis tool.

This lesson takes about 10 minutes.

Topic 97 Testing a connection with “ping”

If it is not possible to establish a connection between two network devices, the Windows system command ping can be entered at the command prompt to test whether both devices are connected to the network and operational.

- Following entry of the system command **ping** together with the IP address of the other network device, **ping** sends an echo request to the network device.
- A connection exists if the network device responds.
- In the case of a timeout, check the cabling between the network devices and distributor devices and whether all devices are operational.

Topic 98 Retrieving own IP address data with “ipconfig”

The Windows system command **ipconfig** displays IP address information, such as the IP address and subnet mask, for all local networks of a computer.

Adding **/all** causes additional information to be displayed about the dynamic address issuing with DHCP.

Renewing an IP address

If a service laptop is disconnected from the production network and plugged into the company network, the IP address of the laptop must be renewed. This is also carried out with **ipconfig**:

- Adding **/release** causes all IP addresses or the IP address of the specified network adapter to be released.
  This logs the computer out of the network.
- Adding **/renew** renews the IP address of all network adapters or of the specified network adapter.

Simply try out the command **ipconfig** on your private PC or service laptop.

Topic 99 Retrieving IP address data of the KLI with “PuTTYtel”

The PuTTYtel software pre-installed on the KR C4 can be used to display information about the status and configuration of the KUKA Line Interface (KLI).

- The command getKLIStatus displays whether the KR C4 is connected to the company network via the KLI.
- The command kagaShow displays an overview of the network adapters present and their settings.
  These include, for example, the IP addresses for “Virtual 5” and “Virtual 6”, the two virtual networks addressed via the KLI connection of the Dual NIC.

Topic 100 Setting up a network drive with “net use”

For data exchange, a file folder on one network device can be shared for use by other network devices:

1. First of all, the desired folder is shared on one computer.
2. Subsequently, a connection to the shared folder is established from the other network device by means of net use.

The directory is now available for both network devices as a **network drive**: both can save data to the directory and use data from it.

Tip: **net use /?** displays a detailed description of all call parameters.

Topic 101 KUKA.Remote View

KUKA.Remote View supports remote diagnosis via the Internet.

A session is started in **netviewer**. The customer logs on using an automatically generated session number or session ID.

- The customer can now grant read-access to the KR C4 controller.
- The user interface of the **KUKA smartPAD** is displayed in parallel on the connected computer.
- Functions such as online diagnosis, program analysis and trace recordings can now be called from the connected computer.
- **KUKA.Remote View** exchanges data via a secure Internet connection and is BSI-certified for data security.

Topic 102 Exercise

Windows system commands I

After connecting your service laptop to the KR C4 robot controller, you are unable to establish a connection to the KR C4 robot controller via **KUKA.WorkVisual**.

What Windows system command do you use to check whether your laptop can establish a connection to the robot controller? The IP address of the robot controller is 10.192.10.100.

- ipconfig /renew 10.192.10.100
- ipconfig /release 10.192.10.100
- net use x: \\10.192.10.100
- ping 10.192.10.100

Windows system commands II

For maintenance of a KR C4, you require data from the archive. At the managed switch, you connect your service laptop from the production network into a free port of the company network. Since you cannot access the required archive drive in the Windows file manager, use the IP address to check whether your service laptop is logged into the company network.

What Windows system command do you use to display the IP address of the network adapter?

- tracert
- ipconfig
- net use
- ping

Windows system commands III (test)

After you have disconnected your service laptop from the production network and connected it to a free port of the company network, the IP address is not updated.

What Windows system command do you use to enable the current IP address that is invalid in the company network?

- ping
- ipconfig/renew
- ipconfig/release
- net use

Topic 103 Summary

In this lesson, you have learnt about a number of system commands and tools which can be used as a first step for checking connections and address data during fault diagnosis.

You have also learnt how to transfer technology packages to a KR C4 using standard Windows software.

You can learn about troubleshooting strategies and the use of more complex tools in the practical training courses at KUKA College.

Topic 104 Final test

What have you learnt? Find out – with the following final test!

The test contains 10 exercises from the previous lessons. It includes cloze tests, multiple-choice and single-choice questions, and interactive exercises in which you have to insert graphical elements or texts at the right point in a graphic by means of Drag&Drop.

You must solve at least 50% of the exercises correctly to pass the test.

If you do not pass the test, you can repeat it as often as you like. During the test, however, you only have one attempt to solve each exercise. Repeat individual lessons if necessary and use the exercises at the end of each lesson to consolidate your knowledge of the contents.

You will need approx. 15 minutes to work through all exercises.

Successful completion of the test will be rewarded with a participation certificate.

Good luck!

Topic 105 Learn more!

You have completed the eLearning module “Basic Principles of Network Technology”.

Keep your knowledge of robotics up to date in the future: KUKA College always offers practical specialist knowledge.

You can find out more about our range of courses on the KUKA College website.