PLC Basics (a/b)

Full-time / Distance Learning

Exam Questions

2026.

1.

a. Generations of control systems (Generations 1-6), structure and characteristics of generations, potential diagrams.

b. The role of industrial communication networks in PLC-based control. Describe the relationship between the field, control and supervisory levels, and illustrate typical network topologies using a production-line example.

2.

a. Structure of PLCs, functional block diagram, connection and operation of individual blocks. Compact and modular structures.

b. The structure of Ethernet-based PLC networks. Explain the functions of switches and routers, and describe the communication links between PLCs, HMIs, remote I/O and SCADA.

3.

a. Structure and operation of BIT-processor-based PLCs (explanation of operation through a short 3-line program).

b. The ISO–OSI reference model and its application in industrial networks. Describe the functions of the layers and explain how a layered approach helps to isolate a PLC communication fault.

4.

a. Structure and operation of the Arithmetic Logic Unit (ALU) of BIT-processor-based PLCs (diagram explanation).

b. The role of MAC addressing and ARP in an Ethernet network. Explain the purpose of a switch’s MAC address table and describe how two devices on the same subnet establish communication.

5.

a. Structure (block diagram) and operation of byte-processor-based PLCs, functions of individual blocks (components), their most important bus systems and their operation.

b. The role of the IPv4 address, subnet mask and default gateway. For a PLC network with the address 10.10.10.10/31, determine the network and broadcast addresses and the assignable address range, and examine whether two devices can communicate directly.

6.

a. Structure of a general byte processor, its most important special registers, and their operation (diagram, operational description).

b. Segmentation of OT networks and the use of VLANs. Describe the purpose of logical network separation, the conditions for communication between VLANs and the considerations for segmenting a production cell.

7.

a. Typical operations (cycle) of the CPU from the most elementary time unit to instruction retrieval. Description of the "fetching" operation.

b. The role of access and trunk ports in a VLAN-based network. Explain the functions of the VLAN identifier and PVID, and the conceptual difference between configuring a port serving a PLC and configuring a link between two switches.

8.

a. Processor states (min. 5 states) and the description of their operation.

b. Static and DHCP-based IP address assignment in industrial networks. Compare the approaches in terms of predictable startup, device replacement and troubleshooting.

9.

a. Most typical co-processors of modular multiprocessor systems, and the structure and operation of remote I/O modules.

b. The role of NAT when interconnecting industrial networks. Explain the use of 1:1 address translation through an example of a system containing machine cells with identical internal IP addressing, and describe the information to be recorded in the addressing plan.

10.

a. How hardware and software counters operate in PLCs, and how timers work.

b. The use of firewalls and NGFWs in OT environments. Explain the role of rules based on source, destination and service, and describe why it may be necessary to distinguish between read operations and program downloads.

11.

a. What types of memory units can be found in a PLC and what each memory is used for (RAM, ROM, EEPROM, SD). Potential presentation of the PLC RAM map.

b. The structure and participants of a PROFINET IO system. Describe the relationship between the controller and field devices, the purpose of cyclic I/O data exchange and the importance of real-time communication.

12.

a. Structure and operation of a two-state, BIT-organized input unit (diagram, operational description).

b. The role of the PROFINET update time and communication watchdog. Calculate the monitoring time from a given update time and watchdog factor, and explain how a communication loss is detected and what its consequences are.

13.

a. Structure and operation of a two-state, BIT-organized output unit (diagram, operational description).

b. Ring redundancy and MRP in industrial Ethernet networks. Explain the Ethernet loop problem, the role of the redundancy manager and the operation of an intact and a broken ring.

14.

a. Structure and operation of a two-state, BYTE-organized input and output unit (diagram, operational description).

b. The structure and basic operation of a Modbus RTU network. Explain the roles of the bus topology, network participants and termination at the physical ends of the bus; describe the considerations for investigating incorrect termination.

15.

a. Galvanically isolated AC and DC input units (diagrams, operational description).

b. Identification and commissioning of PROFINET devices using DCP. Explain the roles of the device name and IP address, and the name and address assignments to be checked when replacing a device.

16.

a. Galvanically isolated "Darlington" output unit (diagram explanation).

b. The role of S7 communication between PLCs and data acquisition systems. Describe how to examine a client–server connection using packet capture, and how to detect connection loss and missing data updates.

17.

a. Galvanically isolated "TRIAC" output unit (diagram explanation).

b. The operating principle and applications of EtherCAT. Describe the essence of on-the-fly frame processing, the connections between devices and the technology’s place among industrial communication systems.

18.

a. Structure of the PLC system software (firmware), system software components, and their functions.

b. The fundamentals of EtherNet/IP communication. Explain its use in industrial control systems, the impact of multicast traffic on the network and the role of IGMP in limiting unnecessary traffic.

19.

a. Blocks (modules) of the PLC system software, their functions, and their hierarchical structure.

b. Bus access and collision resolution in CAN. Explain bitwise arbitration and the roles of dominant and recessive states, and describe how message priority is enforced when multiple devices attempt to transmit simultaneously.

20.

a. Text-based programming languages of PLCs and their characteristics. Demonstration of operation through a short program.

b. A comparison of Modbus RTU and Modbus TCP. Describe the connection architecture, master–slave and client–server roles, request–response operation and the typical industrial applications of each variant.

21.

a. Graphical programming languages of PLCs and their characteristics. Demonstration of operation through a short program.

b. The Modbus data model and addressing. Describe the roles of bit-oriented and register-oriented data tables, read and write operations, and the potential errors caused by differences between documented register notation and protocol addresses.

22.

a. The concept of cycle time and response time, and their calculation. What are the consequences of an incorrectly chosen (calculated) response time?

b. Examining PLC communication using Wireshark. Using a Modbus TCP or S7 packet capture as an example, describe how to identify endpoints, requests and responses, and missing responses, and explain the troubleshooting process.

23.

a. What is the essence and operation of continuous and block I/O processing? Types of I/O assignments.

b. Design considerations for a complex industrial communication network. For a system connecting BMS, production and energy subsystems to a common SCADA system, describe the physical and logical topology, protocol and gateway selection, the IP and VLAN plan, and the required firewall rules.