* **Basic System Architecture Understanding**

**Q1:** What is the purpose of the DMZ Network in the provided system architecture?

* **Answer**: The DMZ network (Zone 3) is a buffer zone between the enterprise (corporate network) and the control networks, allowing safe communication while protecting the control network from direct exposure to external networks.

**Q2:** What devices are connected to the Control Network (Zone 1)?

* **Answer**: Devices connected to the Control Network include the SCADA OPC UA server, Robot Controller, Safety Controller, Proximity Sensor, and Conveyor Belt​.

**Q3**: What security level is assigned to the Supervisory Network (Zone 2)?

* **Answer**: SL=2.

**Q4**: Explain the function of the Jump Server in the Supervisory Network (Zone 2).

* Answer: The Jump Server acts as an intermediary gateway that provides secure access to the control network (Zone 1) from the supervisory network. It helps reduce the attack surface by limiting direct access to critical components.

**Q5**: Is there a remote access to Control Network Zone?

* **Answer** : No.

**Q6**: Is there a remote access to Supervisory Network Zone?

* **Answer** : Yes.

**Q7:** What method is used to protect communication between Zone 1 and Zone 2?

* a) VPN Tunnel
* b) Firewall filtering
* c) Direct Ethernet connection
* d) Unencrypted TCP/IP

**Q8:** Are all communication channels between different zones encrypted?

* **Answer** : No.

**Q9:** What is the role of Human in Control Network Zone?

* **Answer** : Operator.

**Q10:** What type of actions the operator is permitted to perform?

* **Answer**: Control, Shut down, Monitor.
* **Basic Security Requirements Understanding**

**Q1:** What is the purpose of the DMZ Network in the provided system architecture?

* **Answer**: The DMZ network (Zone 3) is a buffer zone between the enterprise (corporate network) and the control networks, allowing safe communication while protecting the control network from direct exposure to external networks.

**Q2:** Which security requirements make the use of PKIs important?

* **Answer**: SR 1.8, SR 1.1, SR 1.2, SR 5.2.

**Q3:** How does the IEC 62443 standard recommend handling unsuccessful login attempts in a control system?

* **Answer**: The system should implement a limit on unsuccessful login attempts to prevent brute-force attacks. However, it must not lock out accounts that are necessary for essential functions.

**Q4:** Which foundational requirement ensures that malicious code is detected and blocked?

* a) Use Control (UC)
* b) Data Confidentiality (DC)
* c) System Integrity (SI)
* d) Timely Response to Events (TRE)

**Q5:** Which foundational requirement ensures that all human users are identified?

* a) Identification and authentication control (IAC)
* b) Data Confidentiality (DC)
* c) System Integrity (SI)
* d) Timely Response to Events (TRE)
* **Compliance Check**

**Q1:** Is security requirement SR1.1 applicable to Control Network zone?

* **Answer**: Yes.

**Q2:** Is security requirement SR1.6 applicable to Supervisory Network Zone? Why?

* **Answer**: No. There is no wireless connectivity in this zone.

**Q3:** Is SR5.1 fulfilled in the system?

* **Answer**: Yes.

**Q4:** Is SR5.1 fulfilled in Control Network zone?

* **Answer**: Yes.

**Q5:** Is Least Functionality requirement fulfilled in Control Network Zone? Why?

* **Answer**: No. There is an unused port while is active on Controller, called EthernetPort3.