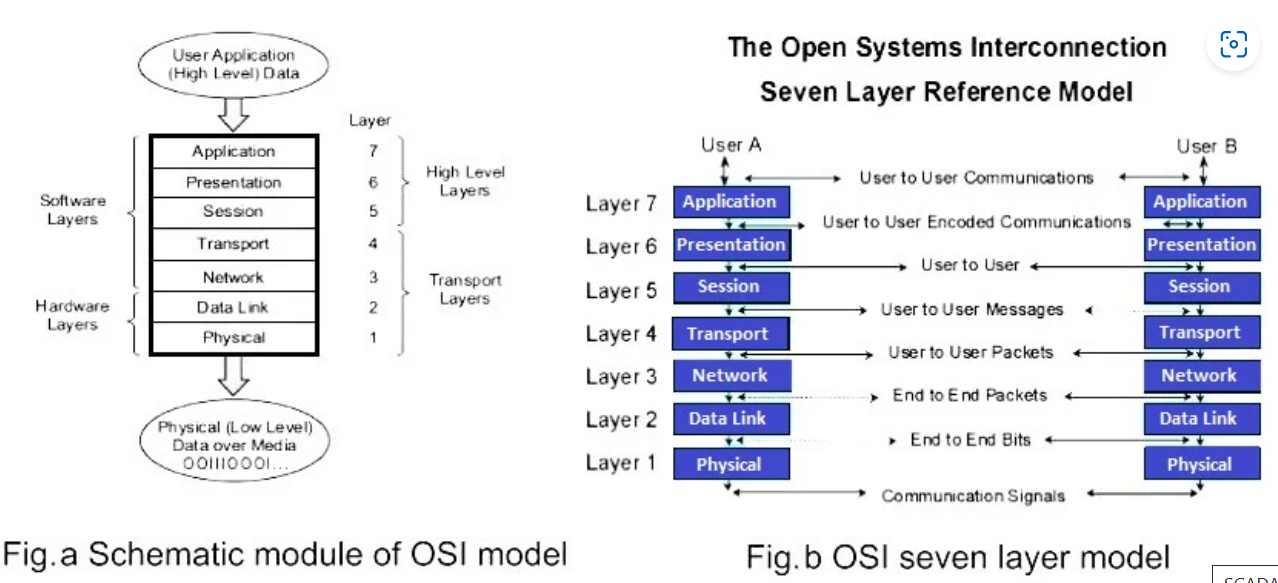
**Notes (SCADA)**

**SCADA Communication & Protocol**

1. **ISO Model (Open System Interconnection Model)**

****

* OSI Reference model has 7 layers:

|  |  |
| --- | --- |
| **Layer Name** | **Description** |
| Application Layer | Provide network services to the user’s application programs, even though actual application programs do not reside in this layer |
| Presentation Layer | Primarily takes care of data representation, including encryption |
| Session Layer | Performs the control of the communication or sessions between the users takes place |
| Transport Layer | Manages the communications between the 2 end systems |
| Network Layer | Primarily responsible for the routing of messages |
| Data Link Layer | responsible for assembling and sending a frame of data from one system to another |
| Physical Layer | Defines the electrical signals and mechanical connections at the physical level |

1. **DNP3 Protocol (Distributed Network Protocol)**

* Consists of a set of communication protocols used between components which are used in process automation systems like electric utility, chemical process plants, etc.
* Purpose: to accomplish communication between various types of monitoring, data acquisition systems and control equipment.
* ICCP (Inter-Control Center Communication Protocol): forms an integral part in SCADA systems while interconnecting the RTUs and IEDs
* ICCP is part of IEC 60870 (which is widely used in inter-master station communication)
* DNP3 protocols were not designed to be secure from hackers and threats

**Important Features of DNP3**

|  |  |
| --- | --- |
| **Feature** | **Description** |
| Interoperable with related protocols like Modbus | More efficient for communicating between components in SCADA systems. |
| Corresponds to layer 2 (refer OSI model) | Provides multiplexing of various features like error checking, link control, data fragmentation, etc. |
| Provide transport function (layer 4) and Application layer (layer 7) | For the transmission of data between master stations, terminals, and intelligent electronic devices (IEDs) in electric utility, water, and gas industries. |
| Has improved bandwidth efficiency | Accomplished through event-oriented data reporting |
| Good ability to handle error detection | It implements several error detection mechanisms:   * CRC (Cyclic redundancy check) * Error-checking bytes * Sequence numbers * ACK (acknowledgment) and NACK (Negative acknowledgement) |
| Performs time synchronization with RTU | Where time stamped variants of all data point objects are reconstructed through a sequence of events |

1. **IEC60870 Protocol**

* Widely used for controlling electric power transmission grids and other process plants
* used for interoperating various equipment from different suppliers through standardized protocols
* **IEC standard 60870** has 6 parts, defining info related to the standard, operating conditions, electrical interfaces, performance requirements, and data transmission protocols (provide communication profile for tele-control messages between 2 directly connected systems, this protocol provides tele-control and tele-protection of electric power systems thru associated tele-communication.)
* **IEC 60870-5 has 5 parts:**

|  |  |
| --- | --- |
| **IEC 60870-5-1** | Transmission frame formats |
| **IEC 60870-5-2** | Data link transmission services |
| **IEC 60870-5-3** | General structure of application data |
| **IEC 60870-5-4** | Definition and coding of information elements |
| **IEC 60870-5-5** | Basics application functions |

1. **HDLC (highly used in SCADA)**

* Also known as high level data link control
* bit-oriented, synchronous data link layer protocol that provides error-free transfer of data between devices
* preferable to use one to one connection, known as asynchronous balanced mode (ABM). (basis of all modern protocols.)

1. **Modbus (highly used in SCADA)**

* Serial communication protocol
* widely used standard communication protocol for connecting industrial electronic devices
* **Advantages of MODBUS:**

1. Industry centric
2. Open source
3. Easy to use and deploy
4. Vendor independent

* **Flow of Modbus:**

1. Modbus allows communication between several devices connected to the network through RTUs in SCADA
2. The master may initiate a Modbus command to activate the connected device
3. The command contains the Modbus address of the device, only the intended device will act on receiving the command though other devices receive them
4. The Modbus command ensures that the command is received unchanged through an inbuilt checking information
5. No standard way exists for a node to find the description of a data object,

**Moxa Gateway**

A device that enables communication between different devices and systems, allowing them to exchange data and control commands.

1. **What is a Moxa Gateway?**

Device that acts as a bridge between different communication protocols, networks, and devices.

* Allows devices that use different protocols or communication methods to communicate with each other, enabling seamless data exchange and control

1. **Functions of a Moxa Gateway in SCADA:**

* **Protocol conversion:** gateway converts data from one protocol to another, allowing devices that use different protocols to communicate with each other. For example, it can convert Modbus to DNP3 or IEC 61850 to Modbus.
* **Network Bridging:** The gateway connects different networks, such as Ethernet, serial, or wireless networks, allowing devices on different networks to communicate with each other
* **Data Routing:** The gateway routes data between devices, ensuring that data is delivered to the correct destination.
* **Device Integration:** The gateway integrates devices from different manufacturers and protocols, enabling them to work together seamlessly in the SCADA system.
* **Security:** The gateway provides security features, such as encryption, authentication, and access control, to protect the SCADA system from unauthorized access and cyber threats.

1. **Types of Moxa Gateways:**
2. **Serial-to-Ethernet Gateways:** connect serial devices to Ethernet networks, enabling them to communicate with other devices on the network
3. **Protocol Gateways:** These gateways convert data between different protocols, such as Modbus to DNP3 or IEC 61850 to Modbus
4. **Wireless Gateways:** connect wireless devices to the SCADA system, enabling wireless communication and control.
5. **Industrial Ethernet Gateways:** connect industrial Ethernet devices to the SCADA system, enabling communication and control over Ethernet networks.

**Basics of SCADA Hardware and Software**

**What is SCADA?**

* Supervisory control and data acquisition system
* remote monitoring of the control system

**Steps to Follow**

1. design the process in the SCADA software
2. tag creation
3. interlinking of tags with PLC addressing
4. communication link between PLC hardware and SCADA software

**AI Utilization in SCADA**