Industrial Communication Systems for Automation

This document provides a practical introduction to industrial communication networks used in automation systems. It covers Fieldbus technologies, Industrial Ethernet protocols, network topologies, PLC-to-PLC communication, and basic troubleshooting techniques with formulas and examples.

1. Fieldbus Basics: Modbus RTU and Modbus TCP

Fieldbus systems are communication networks designed for real-time data exchange between controllers and field devices such as sensors, actuators, and drives.

Modbus RTU:

Modbus RTU is a serial communication protocol typically using RS-485. It follows a master-slave (client-server) architecture where one master polls multiple slaves.

Modbus RTU Frame Structure:

```
[Slave Address] [Function Code] [Data] [CRC]
```

Example: Reading holding registers (Function Code 03) from slave address 05.

Modbus TCP:

Modbus TCP is the Ethernet-based version of Modbus. It uses TCP/IP on port 502 and does not require CRC because Ethernet already provides error checking.

Modbus TCP Frame:

```
[MBAP Header] [Function Code] [Data]
```

2. Industrial Ethernet: Profinet and EtherNet/IP

Industrial Ethernet protocols are designed for deterministic and real-time communication in automation environments, extending standard Ethernet technologies.

Profinet:

Profinet is widely used in Siemens-based systems and supports real-time (RT) and isochronous real-time (IRT) communication for motion control applications.

EtherNet/IP:

EtherNet/IP is based on the Common Industrial Protocol (CIP) and is commonly used in Rockwell Automation systems. It supports cyclic and acyclic data exchange.

Update Time Formula:

```
Update Time = Packet Size / Network Bandwidth
```

Example: A 512-byte cyclic packet on a 100 Mbps network results in an update time of approximately 0.04 ms.

3. Network Topology and Addressing

Network topology defines how devices are connected. Proper addressing ensures reliable communication and easy maintenance.

Common Topologies:

- Star topology (most common in Ethernet networks)
- Line topology (often used with Profinet devices)
- Ring topology (supports redundancy)

IP Address Structure:

```
IP Address = Network ID + Host ID (e.g., 192.168.1.10 / 255.255.255.0)
```

Example: PLC at 192.168.1.1 communicates with an HMI at 192.168.1.20 within the same subnet.

4. PLC-to-PLC Communication

PLC-to-PLC communication allows multiple controllers to exchange data for synchronization, interlocking, or data sharing between machines.

Communication Methods:

- Modbus client/server data exchange
- Profinet IO Controller / IO Device
- EtherNet/IP produced/consumed tags

Data Exchange Example:

PLC_A sends a BOOL 'Machine_Ready' to PLC_B to allow synchronized startup.

5. Basic Troubleshooting of Communication Errors

Communication errors can lead to data loss, machine stops, or unsafe conditions. Systematic troubleshooting helps quickly identify and resolve issues.

Common Issues:

- Incorrect IP address or subnet mask
- Cable faults or poor shielding
- Wrong baud rate or parity (serial communication)
- Duplicate device addresses

Error Rate Formula:

```
Error Rate (%) = (Number of Failed Messages / Total Messages) × 100
```

Example: If 5 messages fail out of 1000, the error rate is 0.5%.

End of document.