PLC Fundamentals

Understanding Programmable Logic Controllers in Industrial Environments

OT Security Learning Series

Document 020 | January 2026

Contributors: OT Security Community

Created with AI assistance

LEARNING RESOURCE

Contents

1 Introduction

Information

A **Programmable Logic Controller (PLC)** is a ruggedized industrial computer designed to control manufacturing processes, machinery, and other automation equipment. PLCs are the backbone of industrial automation and a critical component in OT security.

PLCs replaced hard-wired relay-based control systems in the late 1960s, offering flexibility, reliability, and programmability. Today, they are found in virtually every industrial sector, from manufacturing and energy to water treatment and transportation.

Understanding PLC architecture, operation, and vulnerabilities is essential for OT security professionals. This document covers the fundamentals of PLC technology from a security perspective.

2 PLC Architecture

A PLC consists of several key components working together to monitor inputs, execute control logic, and drive outputs.

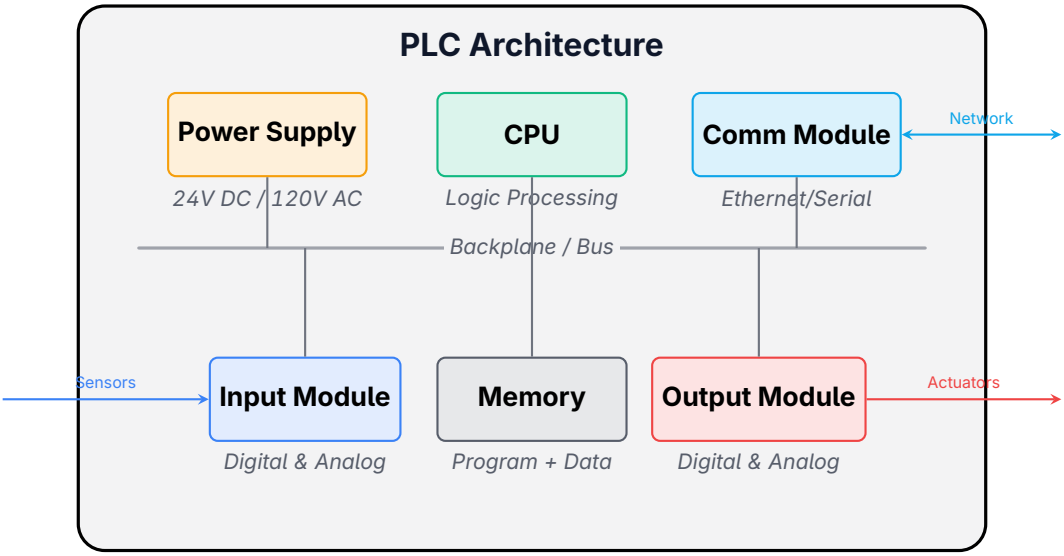

Figure 1: PLC Hardware Architecture

2.1 Central Processing Unit (CPU)

The CPU is the brain of the PLC, responsible for:

- Executing the control program (ladder logic, function blocks, etc.)
- Managing memory and data storage

- Handling communication with other devices
- Performing diagnostic functions

2.2 Memory Types

PLCs use several types of memory:

Type	Purpose	Persistence
RAM	Runtime data, I/O status	Volatile
ROM/EPROM	Firmware, operating system	Non-volatile
Flash	User program storage	Non-volatile
Battery-backed RAM	Retentive data	Semi-persistent

Table 1: PLC Memory Types

2.3 Input/Output Modules

I/O Modules

I/O modules are the interface between the PLC and the physical world. They convert electrical signals from sensors into data the CPU can process, and convert CPU commands into signals that control actuators.

Digital I/O:

- Discrete on/off signals (24V DC, 120V AC)
- Examples: pushbuttons, limit switches, indicator lights, solenoids

Analog I/O:

- Continuous signals (4-20mA, 0-10V)
- Examples: temperature sensors, pressure transmitters, variable speed drives

3 PLC Scan Cycle

The PLC operates in a continuous loop called the **scan cycle**. Understanding this cycle is crucial for both programming and security analysis.

Warning

Security Implication: The scan cycle time affects how quickly a PLC can respond to malicious commands or anomalies. Attackers can time their actions between scan cycles to avoid detection.

3.1 Scan Time Considerations

- **Fast processes** require short scan times (< 10ms)
- **Complex programs** increase scan time

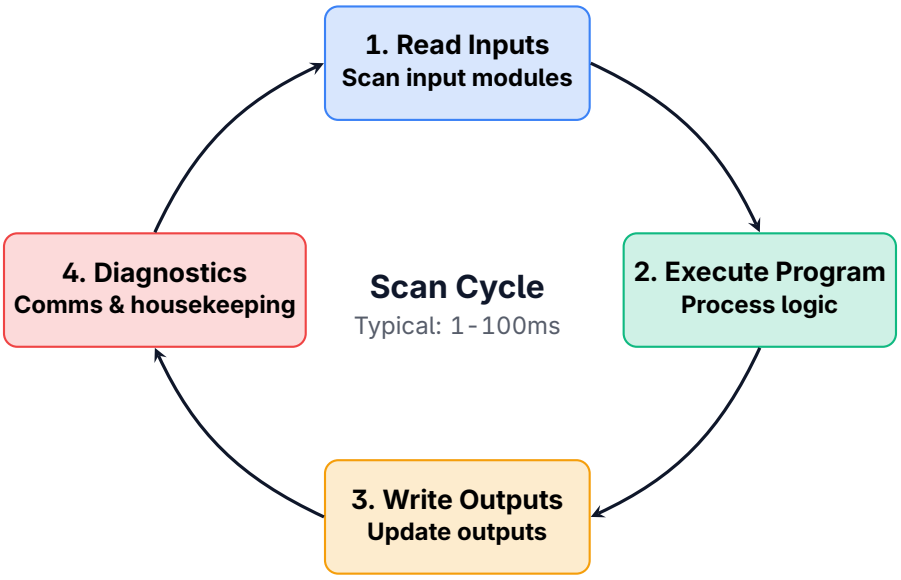

Figure 2: PLC Scan Cycle

- **Watchdog timers** reset the PLC if scan time exceeds limits
- **Interrupts** can preempt the normal scan for time-critical tasks

4 Programming Languages

The IEC 61131-3 standard defines five programming languages for PLCs:

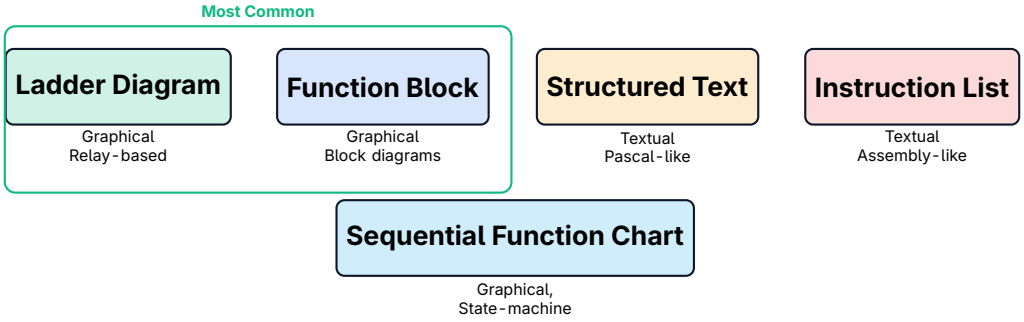

Figure 3: IEC 61131-3 Programming Languages

4.1 Ladder Diagram (LD)

Ladder logic is the most widely used PLC programming language, especially in North America. It resembles electrical relay schematics.

4.2 Structured Text (ST)

Structured Text is a high-level textual language similar to Pascal or C:

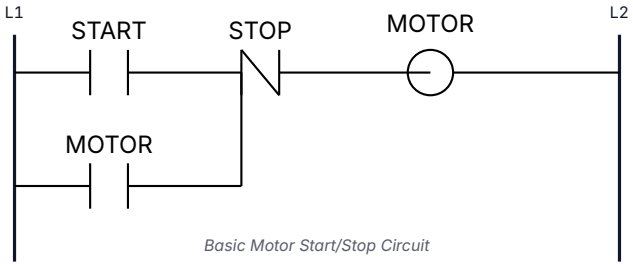

Figure 4: Ladder Logic Example

```
IF Start_Button AND NOT Stop_Button THEN
    Motor := TRUE;
    Run_Time := Run_Time + Scan_Time;
ELSIF Stop_Button OR Emergency_Stop THEN
    Motor := FALSE;
END_IF;
```

Listing 1: Structured Text Example

5 Communication Protocols

Modern PLCs support various communication protocols for integration with other systems:

Protocol	Use Case	Security Level
Modbus TCP/RTU	Legacy systems, simple I/O	LOW None built-in
EtherNet/IP	Rockwell/Allen-Bradley	MEDIUM Optional CIP Security
PROFINET	Siemens environments	MEDIUM TLS available
OPC UA	Modern integration	HIGH Built-in security

Table 2: Common PLC Communication Protocols

Critical

Critical Security Gap: Many legacy protocols like Modbus have **no authentication or encryption**. Anyone with network access can read/write PLC registers and potentially cause physical damage.

6 PLC Security Considerations

6.1 Common Vulnerabilities

- **Default credentials** – Many PLCs ship with known default passwords
- **Insecure protocols** – Modbus, older EtherNet/IP lack authentication
- **No encryption** – Program uploads/downloads often unencrypted

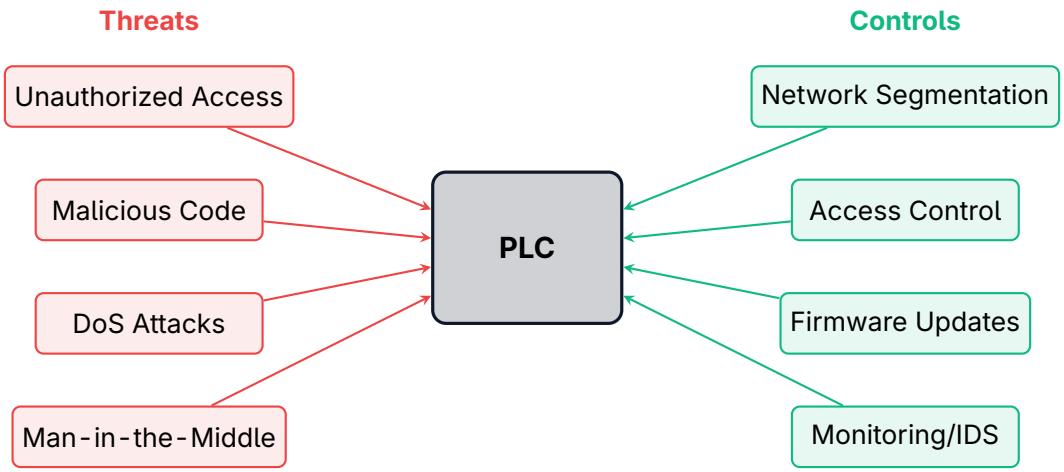

Figure 5: PLC Security: Threats and Controls

- **Limited logging** – Most PLCs have minimal audit capabilities
- **Firmware vulnerabilities** – Buffer overflows, hardcoded keys
- **Physical access** – USB ports, serial connections often unprotected

6.2 Security Best Practices

Key Point

Key Security Controls for PLCs:

1. Change default passwords immediately
2. Segment PLC networks from IT/business networks
3. Disable unnecessary services and ports
4. Implement network monitoring and anomaly detection
5. Maintain firmware update procedures
6. Use encrypted protocols where available (OPC UA, CIP Security)
7. Restrict physical access to PLC hardware
8. Back up PLC programs regularly and verify integrity

7 Major PLC Vendors

Understanding vendor-specific implementations helps with security assessments:

Vendor	Product Lines	Common Industries
Siemens	S7-300/400/1200/1500	Manufacturing, Energy
Rockwell/Allen-Bradley	ControlLogix, CompactLogix	Automotive, Food & Beverage
Schneider Electric	Modicon M340/M580	Water, Building Automation
Mitsubishi	MELSEC iQ-R/F	Electronics, Automotive
ABB	AC500	Process Industries
Omron	NX/NJ Series	Packaging, Assembly

Table 3: Major PLC Vendors and Applications

8 PLC vs. Other Controllers

Controller Types Comparison

- **PLC** – Discrete/hybrid control, fast I/O, rugged, ladder logic
- **DCS** – Process control, continuous processes, integrated HMI
- **RTU** – Remote sites, telemetry, low power, wide-area comms
- **PAC** – Combines PLC + PC capabilities, complex applications
- **Safety PLC** – SIL-rated, redundant, for safety instrumented systems

9 Summary

Key Takeaways

- PLCs are specialized industrial computers that control physical processes
- They operate in a continuous scan cycle: read inputs, execute logic, write outputs
- IEC 61131-3 defines five programming languages; ladder logic is most common
- Many PLCs use insecure legacy protocols without authentication
- Security controls include network segmentation, access control, and monitoring
- Understanding PLC architecture is essential for OT security assessments

10 Further Reading

Standards and Guidelines

- **IEC 61131-3** – Programmable controllers - Programming languages
  https://www.iec.ch/
- **IEC 62443** – Industrial communication networks - Security
  https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

- **NIST SP 800-82** – Guide to ICS Security
  https://csrc.nist.gov/pubs/sp/800/82/r3/final

Resources

- **CISA ICS Advisories** – Vendor-specific PLC vulnerabilities
  https://www.cisa.gov/news-events/cybersecurity-advisories
- **PLCopen** – PLC programming standards organization
  https://www.plcopen.org/

Books

- Bolton – *Programmable Logic Controllers* (Newnes)
- Petruzella – *Programmable Logic Controllers* (McGraw-Hill)
- Knapp & Langill – *Industrial Network Security* (Syngress)

Part of the OT Security Learning Series