Programmable Logic Controller (PLC) Implementation

S. Venkatesan

Network Security and Cryptography Lab

Acknowledgement: The contents, example scripts and some figures are copied from various sources.
Thanks to all authors and sources made those contents public and usable for educational purpose

Standard

- IEC 61131 is an IEC standard for programmable controllers.

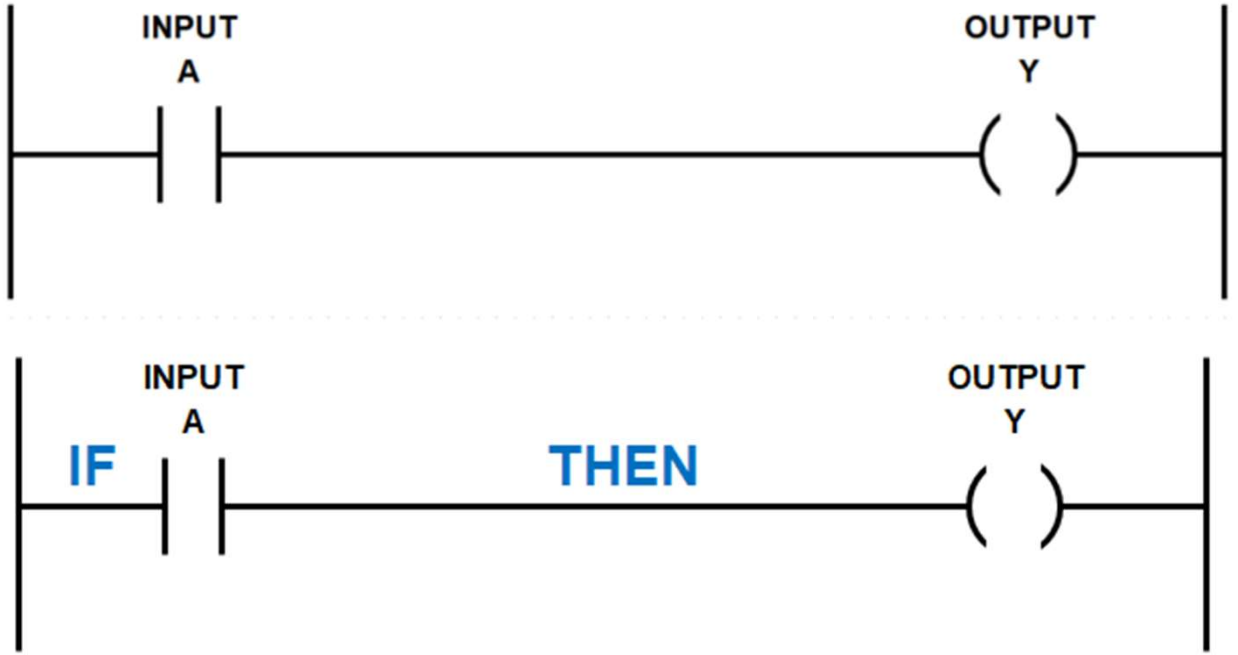
- IEC 61131-3 is for the language

Types of Languages

- Ladder Logic
- Function Block Diagram
- Sequential Function Charts
- Structured Text
- Instruction List

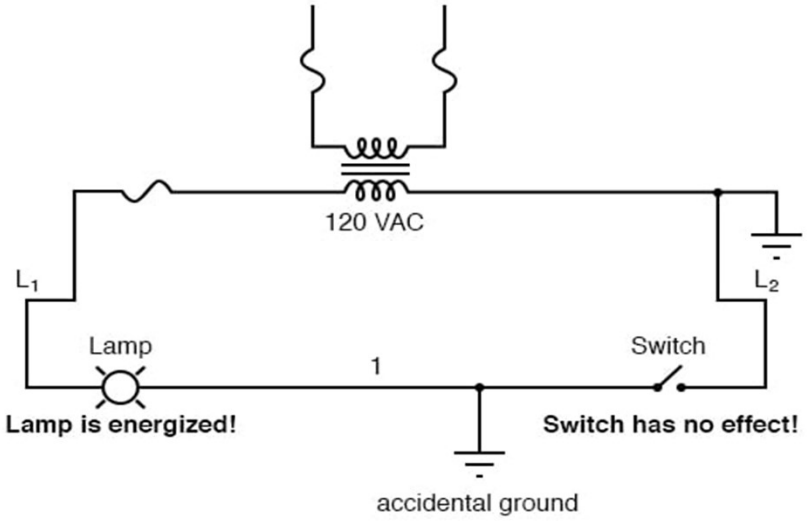
Ladder Logic

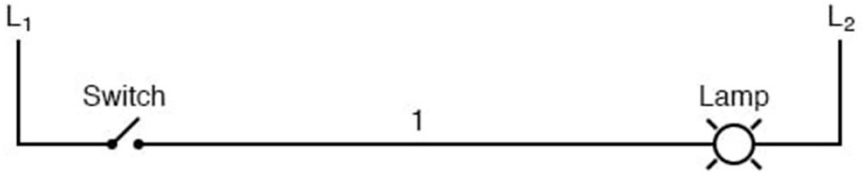
- known as Ladder Diagram, is a graphical PLC programming language based on relay logic's circuit diagrams



https://ladderlogicworld.com/ladder-logic-basics/

Ladder Process





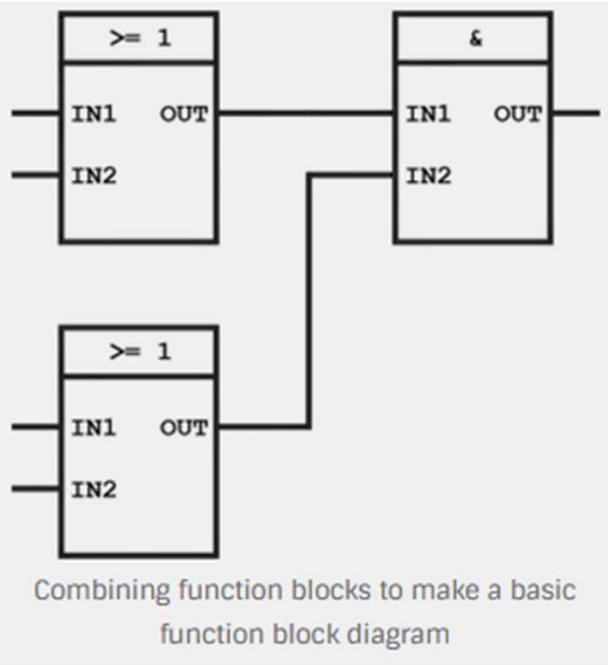
Functions

- Logics
- Timer
- Counter
- Move

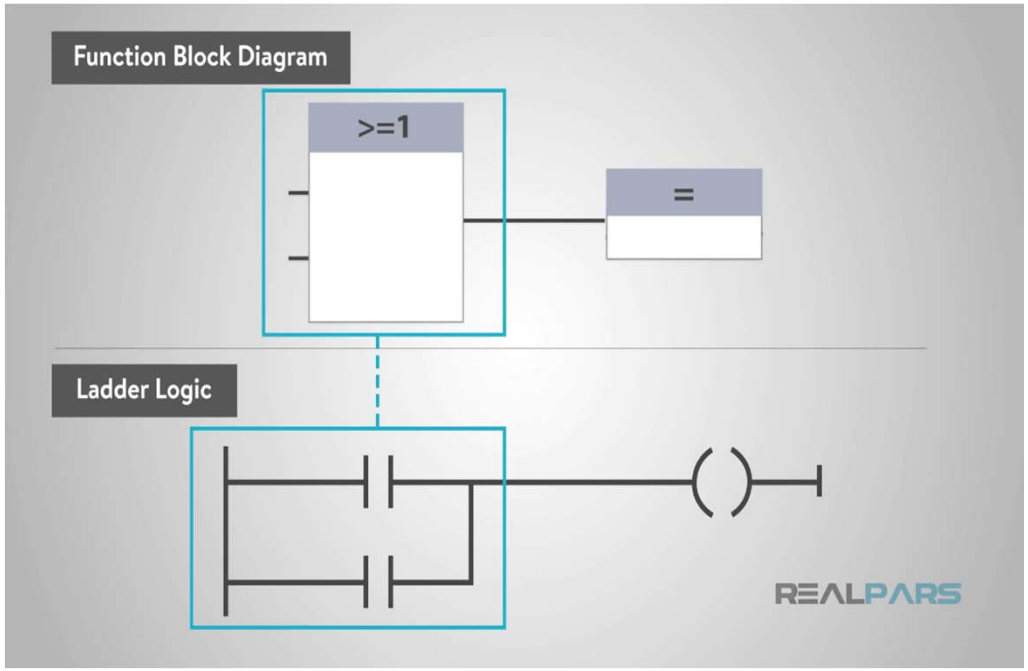
- Implementation of Latch for continuing.
  - For eg., motor runs after releasing start button

Stop Switch: The location of stop switches with many applications has to be very carefully considered to ensure a safe system. A stop switch is not safe if it is normally closed and has to be opened to give the stop action.

Functional Block Diagram



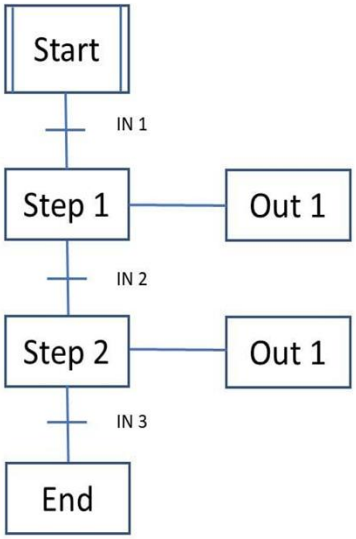
Combining function blocks to make a basic function block diagram

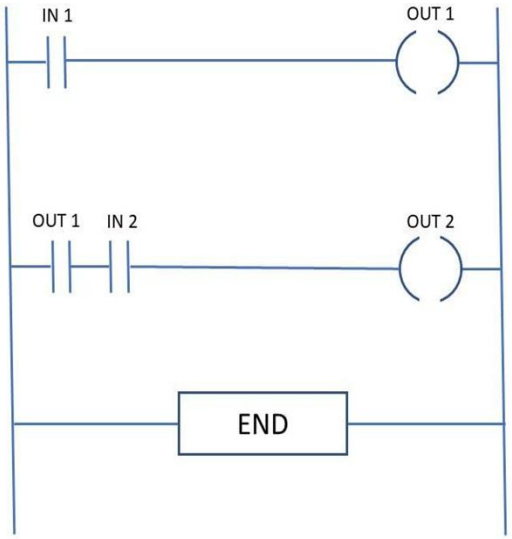


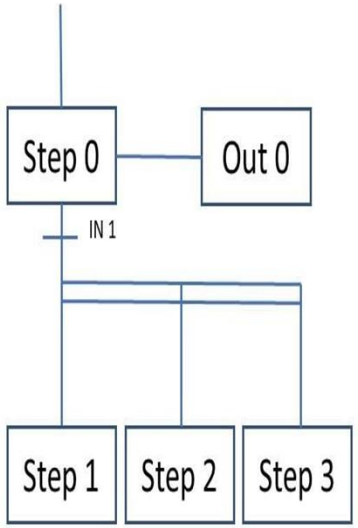
https://www.plcacademy.com/function-block-diagram-programming/

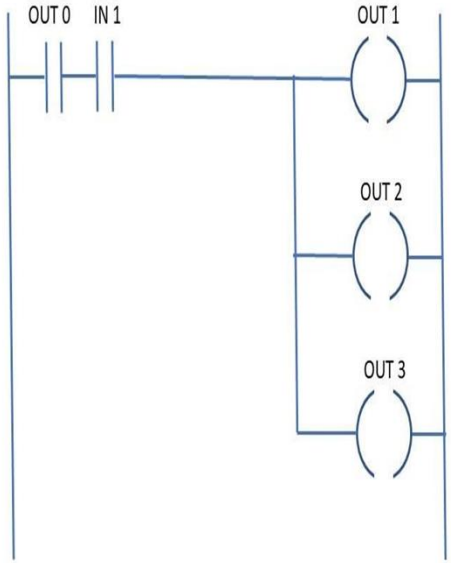
Sequential Function Charts

- Similar to a flow chart.
- Useful for sequential control operations.
- Shows the main states of a system.
- SFC shows all possible status changes









Structured Text

- Using Program

```
counter := 0;
WHILE counter < 10 DO
        counter := counter + 1;
machine_status := counter * 10;
END_WHILE;
```

Instruction List

- It is a low level language and resembles assembly.

```
          LD      Speed
          GT      2000
          JMPCN   VOLTS_OK
          LD      Volts
VOLTS_OK  LD      1
          ST      %Q75
```

Differences

Ladder Logic	Functional Block Diagram	Sequential Function Charts	Structured Text	Instruction List
Supports online changes well Some process control instructions are not available Instructions take up little memory Difficult for motion programming	Instructions take up more memory than in Ladder Good for motion controls	Built-in timers for steps Syntax can be difficult Complex Sequence to do simple tasks Online editing is a challenge	User controls operations Difficult syntax Hard to debug Hard to edit online	Complex to Write Hard to debug Mostly outdated and new PLCs do not use.

Source: https://www.dosupply.com/tech/2018/09/10/differences-between-plc-programming-languages/ [accessed on 05/08/2024]

PLC Memory

- RAM
  - Volatile (Non-Retentive) – New Memory variables
  - Non-Volatile (Retentive) - programs and data are stored. All the user programs and data variables

- ROM - The operating system, firmware version, and system-defined variables are stored

Safety PLC

- Follows Safety Integrity Level (SIL)
- Redundancy to help prevent failure.
- Device failure and malfunctions are never 100% avoidable
  - safety PLCs have predictable failure modes that reduce the amount of disruption to the system in case of failure.
- Safety PLCs are also equipped with a safety circuit between the output and connected devices to ensure extra protection during a malfunction.
- isolated from the rest of the systems logic for safety reasons.

Vulnerabilities

- 2.1.1 Vulnerabilities in configuration:
  - Configuration files are stored as plain-text in PLCs.
  - An adversary can configure the PLC by introducing malicious logic in the Ladder logic.

- 2.1.2 Vulnerabilities in network.
  - PLCs may be integrated Raspberry Pi and these can be easily exposed to malicious communication channels.
  - In the network of PLCs, an infected PLC will scan the network and look for new targets

- 2.1.3 Vulnerabilities in operating system.
  - Raspberry Pi (RPI) is a Linux distribution, which contains many vulnerabilities that can be inherited by RPI.
  - Because Linux code is not type safe, it is vulnerable to various buffer overflow attacks.

- 2.1.4 Vulnerabilities in Pin I/O.
  - Because PLCs do not sanitize commands and control signals sent from Pin I/O, they are vulnerable to invalid inputs attacks

Source: Wenhui Zhang, Yizheng Jiao, Dazhong Wu, Srivatsa Srinivasa, Asmit De, Swaroop Ghosh, Peng Liu, Armor PLC: A Platform for Cyber Security Threats Assessments for PLCs,

Threat

- 2.2.1 Hacking PLC Configuration.
  - Each PLC application running on Raspberry Pi has its separate memory space.
  - It stores local strings and variables on default memory locations.
  - Malicious attacks could change those configuration files once they logged on to the RPI which by default gives users root access.
- 2.2.2 Hacking OS.
  - Raspberry Pi by default gives users root access, and Linux-based systems have their SSH port opened for debugging.
- 2.2.3 Modifying the User Space Programs.
  - Raspberry Pi by default can give users access to modify the program and install garbage programs.
- 2.2.4 Monitoring Pin/Data/Configuration.
  - Users who have access to Raspberry Pi could monitor data traffic patterns through output/input pins and easily predict the data processed on it.
  - This passive attack could hurt confidentiality of data of PLCs.
- 2.2.5 Return Oriented Programming Attack.
  - PLC logics might be compromised.
  - Compromised logic steers the operation of devices away from normal execution path.

Source: Wenhui Zhang, Yizheng Jiao, Dazhong Wu, Srivatsa Srinivasa, Asmit De, Swaroop Ghosh, Peng Liu, Armor PLC: A Platform for Cyber Security Threats Assessments for PLCs,

Differences

PLC	Relay	Microcontroller	Industrial PC
Large amount of automation tasks	Automate a hand full of simple automation task, such as hopper level control	automate an application with a fixed set of parameters and has potential for mass production, like a washing machine.	would be best suited when high degrees of math computation is required, such as a flight simulator

Manage Risk

- Threat Analysis
- Inventory Management
- Vulnerability Analysis
- Backup and Recovery Plan

- Measures
  - Network segmentation
  - Access Control

Threats

- Unauthorized Access
- Malware Infection
- Network based attacks (DoS)
- Data Interception and manipulation
- Insider threats
- Exploitation of vulnerabilities

Ref: https://www.linkedin.com/pulse/securing-programmable-logic-controllers-plcs-key-threats-james-rabe-sdh0e [accessed on 05/08/2024]

Weakness Possibilities

Ladder Logic	Functional Block Diagram	Sequential Function Charts	Structured Text	Instruction List
Supply chain attack	Supply chain attack	Supply chain attack	Vulnerability in Code	Vulnerability in Code
Only pre-defined functions can be added or removed by attacker in case of having access	Only pre-defined functions can be added or removed by attacker in case of having access	Only pre-defined functions can be added or removed by attacker in case of having access	Anything can be modified by attacker in case of having access	Anything can be modified by attacker in case of having access

References

- https://www.tud.ttu.ee/im/Andres.Rahni/Automaatika%20alused/77511_05_LAD_and_FBD.pdf