UNITED STATES
NAVAL ACADEMY
Annapolis

PLC and Ladder Logic Basics Workshop

Brien Croteau, USNA, Cyber Science

DefCon 32, ICS Village, 09 Aug 2024

Link to these slides:
https://github.com/brienc23/Defcon32_workshop_materials

My Background

25-year Active Duty Naval Officer, EE Ph.D.
Assistant Professor, USNA Cyber Science Department
Military Deputy for the Dean of Math and Science

EA-6B Naval Flight Officer

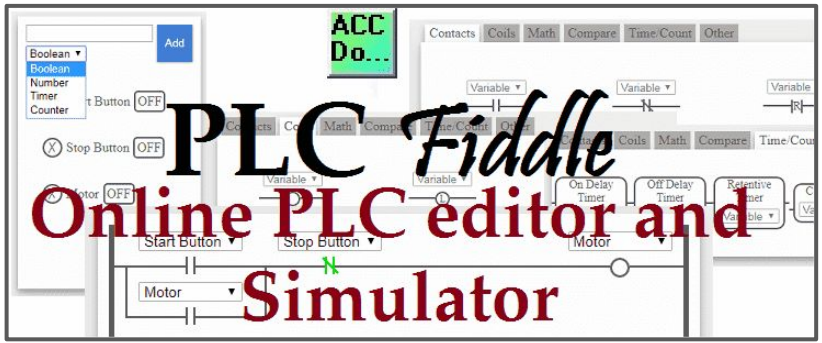
Research in Cyber-Physical Systems (CPS) Security: Detection of malicious sensors using side-channel power analysis, Alternate actuation paths, Actuation limits, Industrial Control Systems (ICS) security, Maritime Hull, Mechanical, & Electrical (HM&E) security

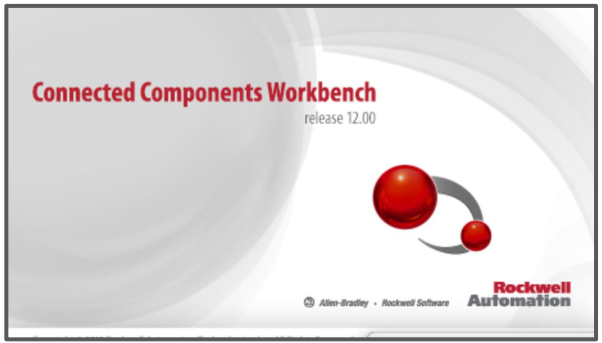
Workshop Outline

A gentle introduction to programming Industrial Controllers

Recommended Free Tools:

1. PLC Fiddle (browser-based Ladder Logic Simulator)
2. Rockwell/Allen-Bradley CCW (commercial micro800 PLCs)



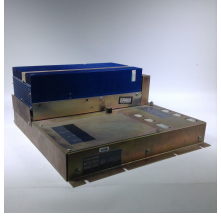


Disclaimer: None of these products are endorsed by: US Gov, US Navy, or USNA

What is a PLC?

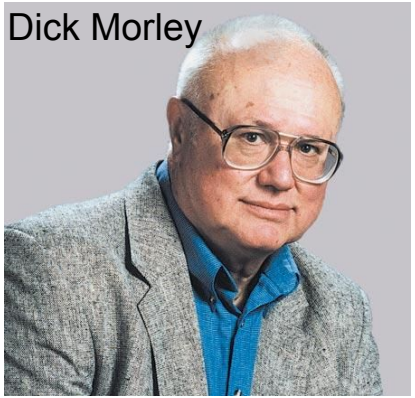
A programmable logic controller (PLC) or programmable controller is an industrial computer that has been ruggedized and adapted for the control of manufacturing processes, such as assembly lines, machines, robotic devices, or any activity that requires high reliability, ease of programming, and process fault diagnosis.

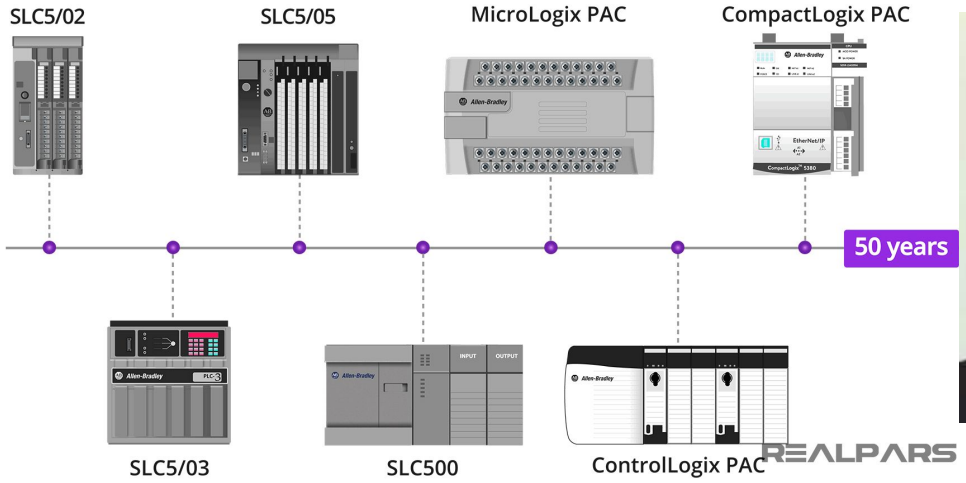
History



There are two men credited as being the "father" of the PLC.

- Richard E. Morley (1932-2017) was an American mechanical engineer who was involved with the production of the first PLC for General Motors, Modicon, and Bedford Associates in 1968.
- Odo Josef Struger (1931-1998) was involved in the invention of the Allen-Bradley programmable logic controller (PLC) and coined that term, during 1958 to 1960 based on a concept developed in his doctoral dissertation at the Vienna University of Technology.





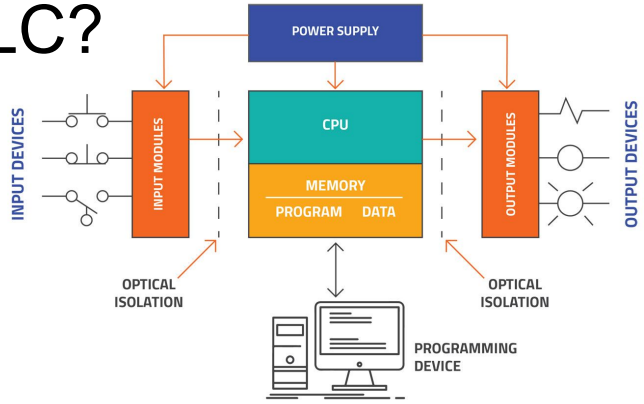
MODICON Schneider Electric

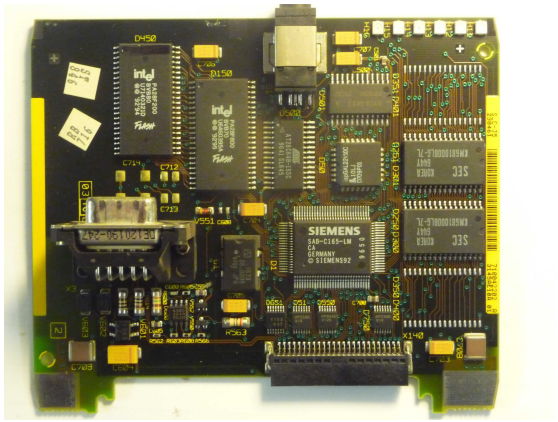
REALPARS

Allen-Bradley by ROCKWELL AUTOMATION

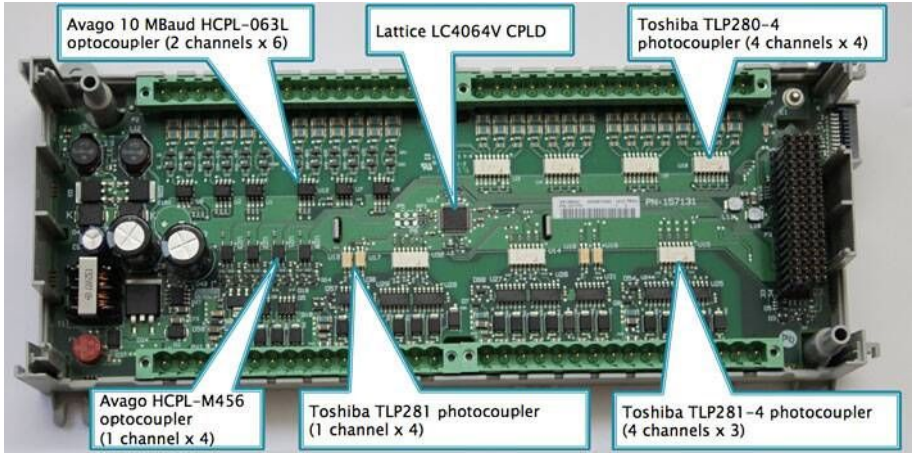
What is inside a PLC?

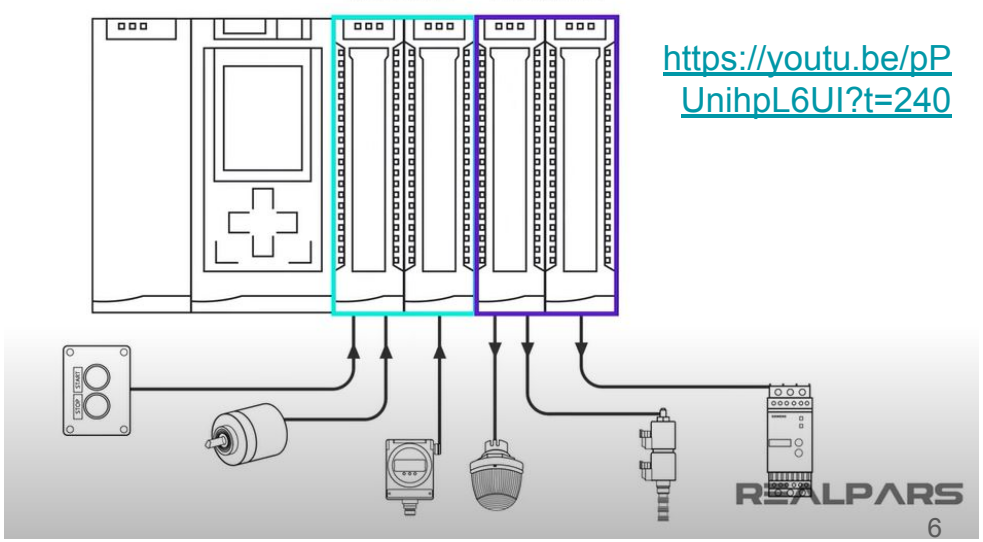
- Power Supply
- Processor
- Input Modules
- Output Modules
- Interface Modules
- Programming Interface





SIEMENS CPU314IFM with C165 series processor





https://youtu.be/pPUnihpL6UI?t=240

Simple PLC Example

"Figure 8 shows control of a manufacturing process being performed by a PLC over a fieldbus network. The PLC is accessible via a programming interface located on an engineering workstation, and data is stored in a data historian, all connected on a LAN."

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.ipd.pdf

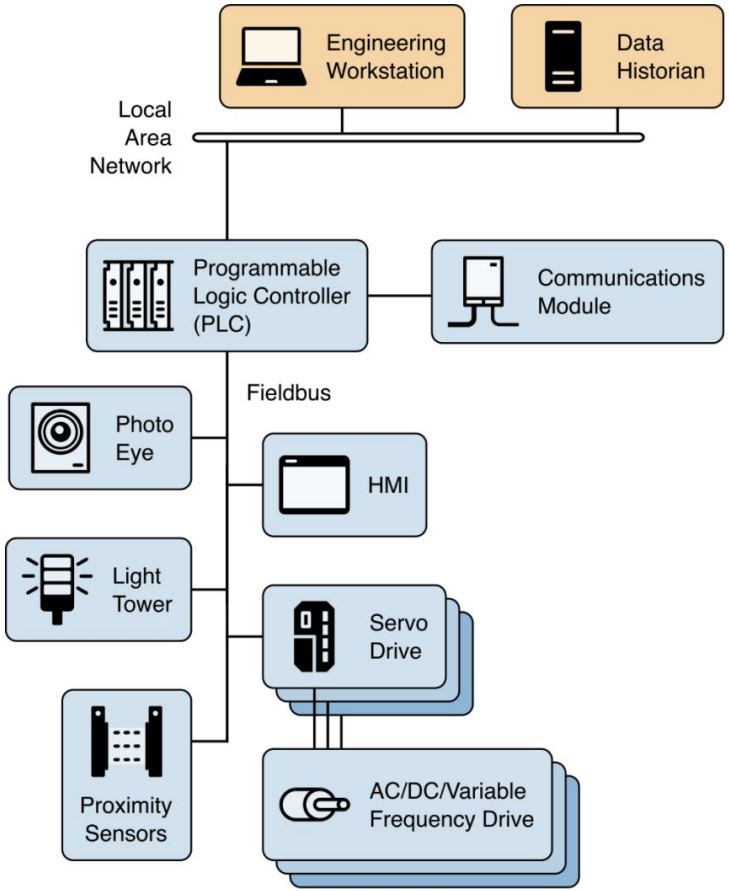
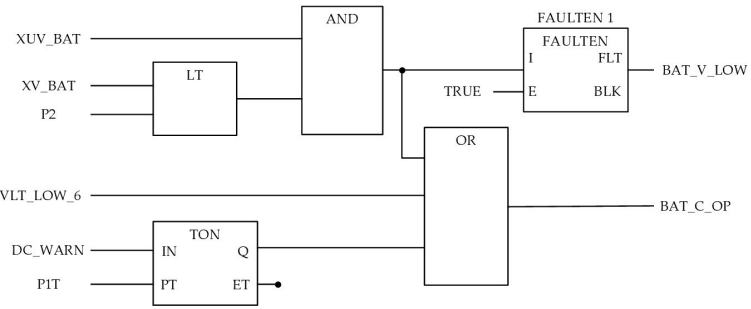


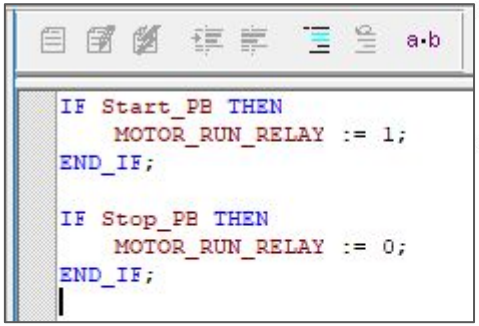
Figure 8: A PLC control system implementation example

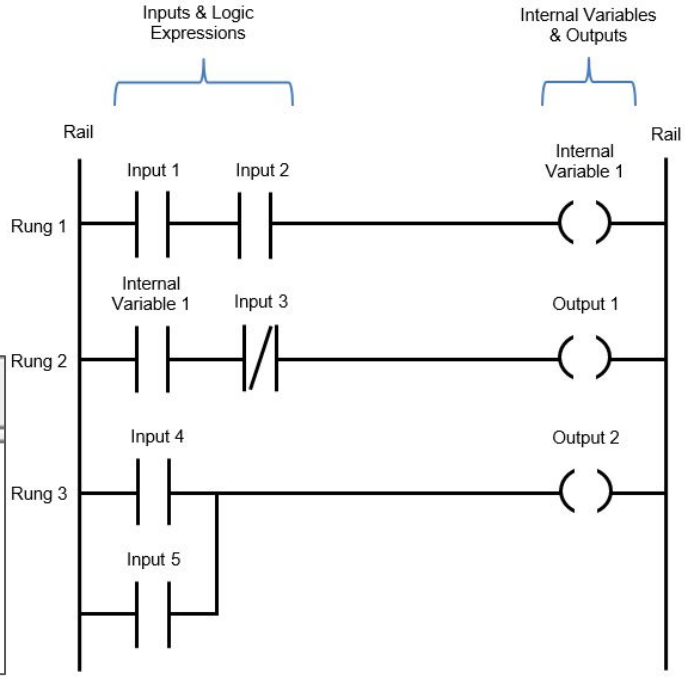
PLC Programming

Standardized with IEC 61131-3 which defines three graphical and two textual programming language standards:

- Ladder diagram (LD), graphical
- Function block diagram (FBD), graphical
- Structured text (ST), textual
- Instruction list (IL), textual (deprecated)
- Sequential function chart (SFC), graphical

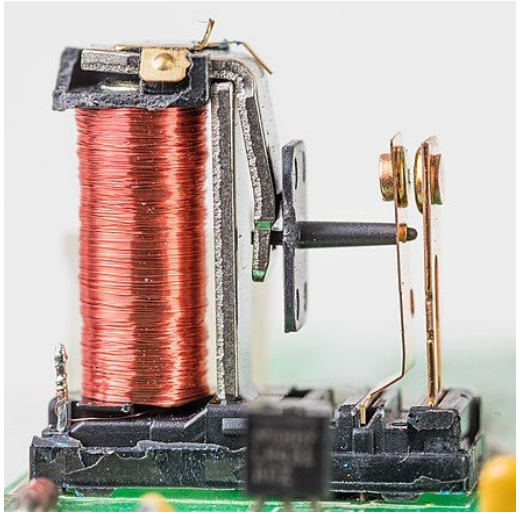


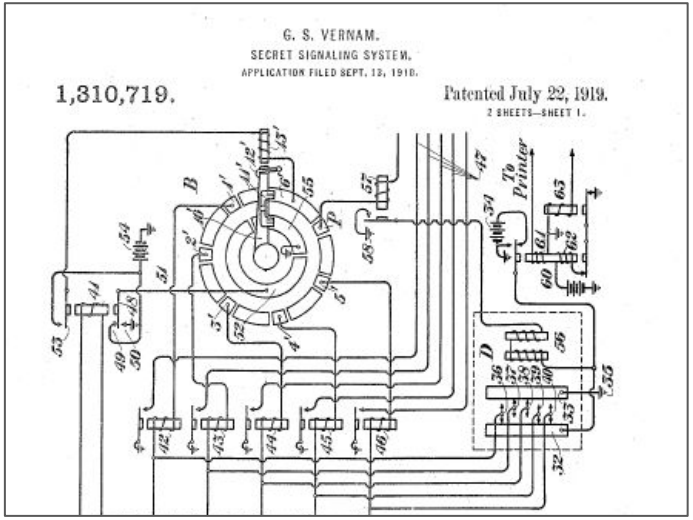


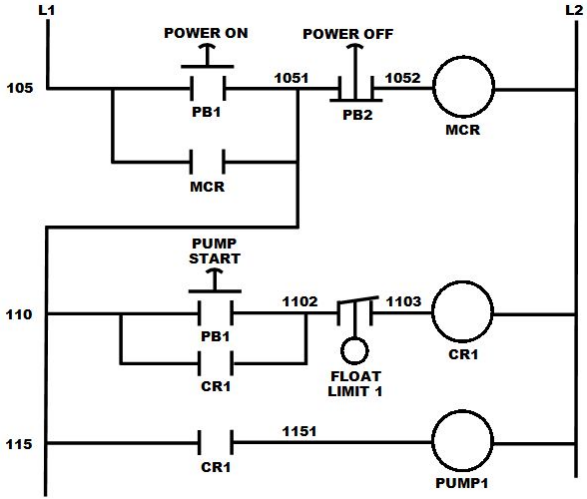


Where does LL come from?

Ladder logic was originally a written method to document the design and construction of relay racks as used in manufacturing and process control.[1] Each device in the relay rack would be represented by a symbol on the ladder diagram with connections between those devices shown. In addition, other items external to the relay rack such as pumps, heaters, and so forth would also be shown on the ladder diagram.

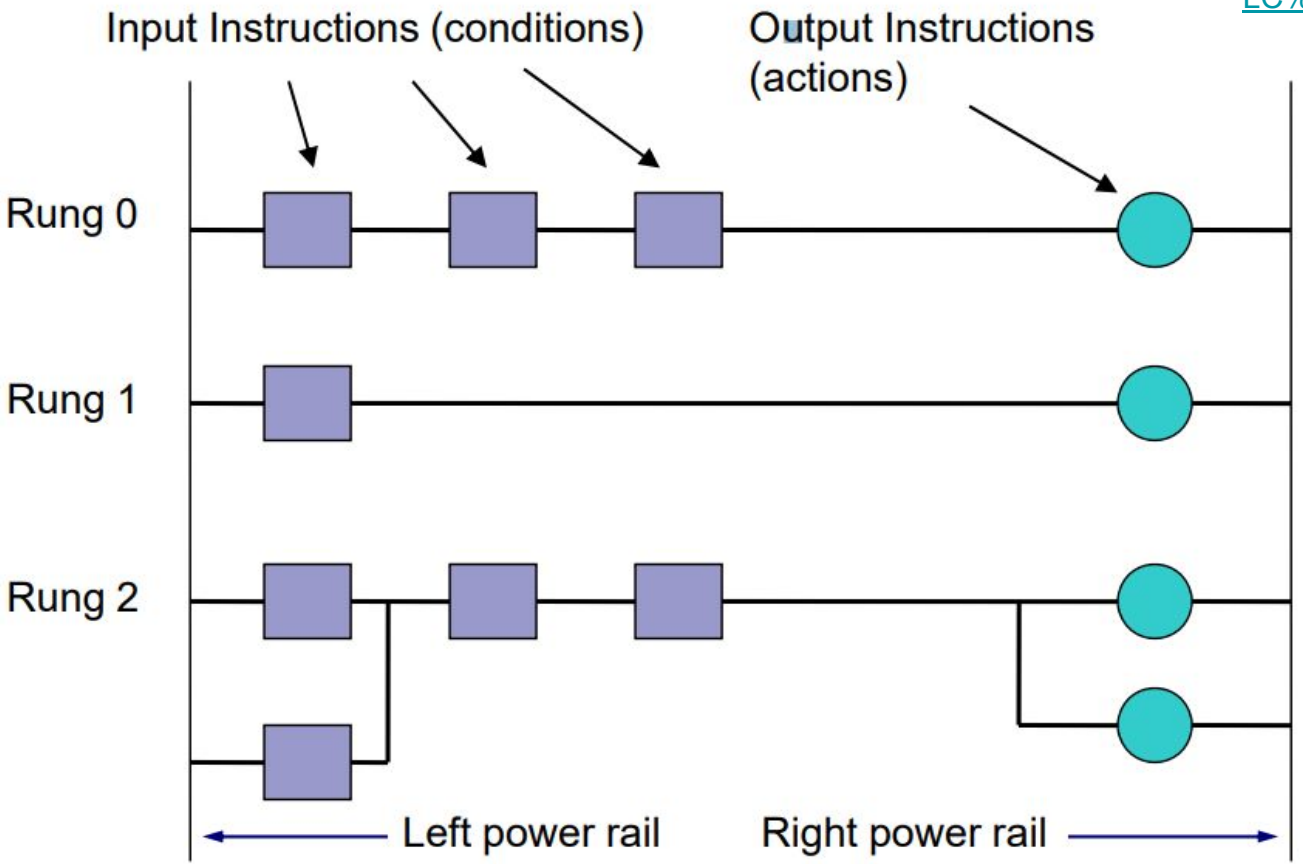






Anatomy of a Ladder Program

https://my.ece.utah.edu/~ece3510/Ladder%20Logic%20Fundamentals%20PLC%20tutorial.pdf



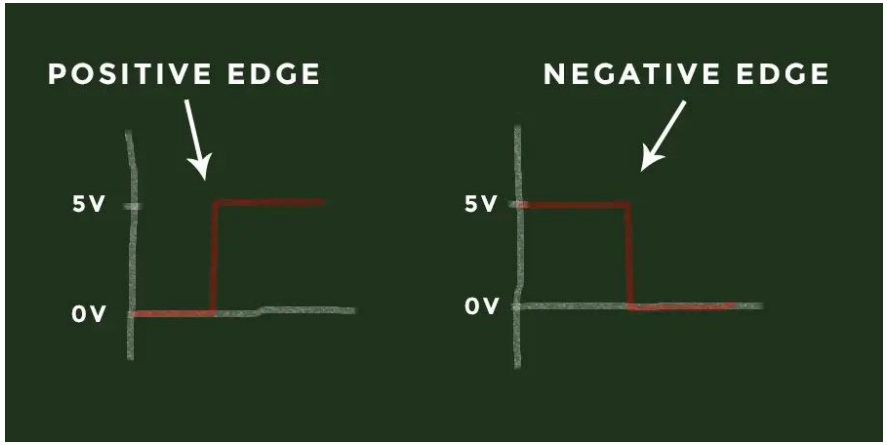
Typical Symbols

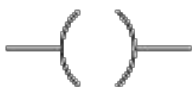
NO Contact

Positive Transition-Sensing Contact

NC Contact

Negative Transition-Sensing Contact

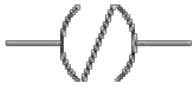




Coil

SET Latch Coil

Positive Transition-Sensing Coil



Negated Coil

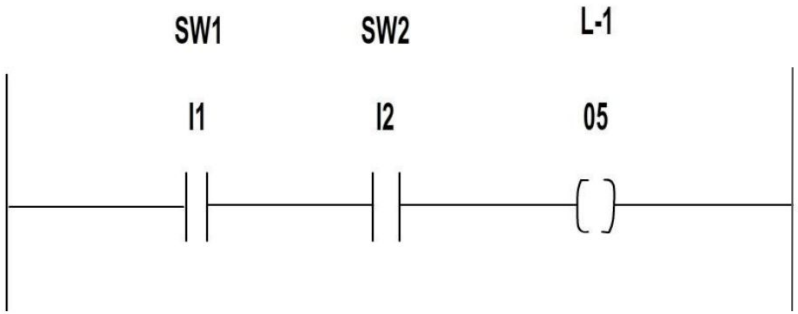
RESET Latch Coil

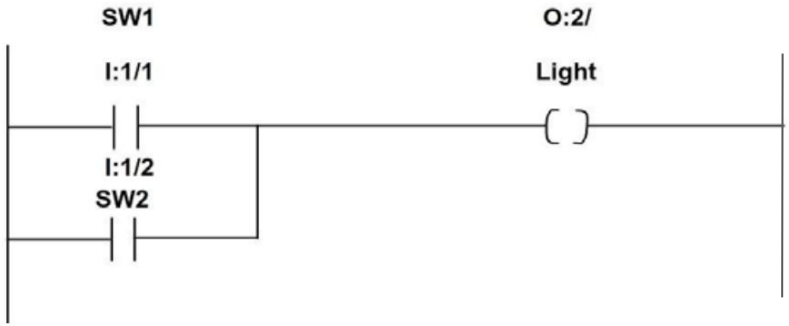
Negative Transition-Sensing Coil

https://www.plcacademy.com/ladder-logic-symbols/

Basic Logic

https://www.philadelphia.edu.jo/academics/waraydah/uploads/Introduction%20to%20PLC%20and%20Ladder%20Logic%20Programming.pdf



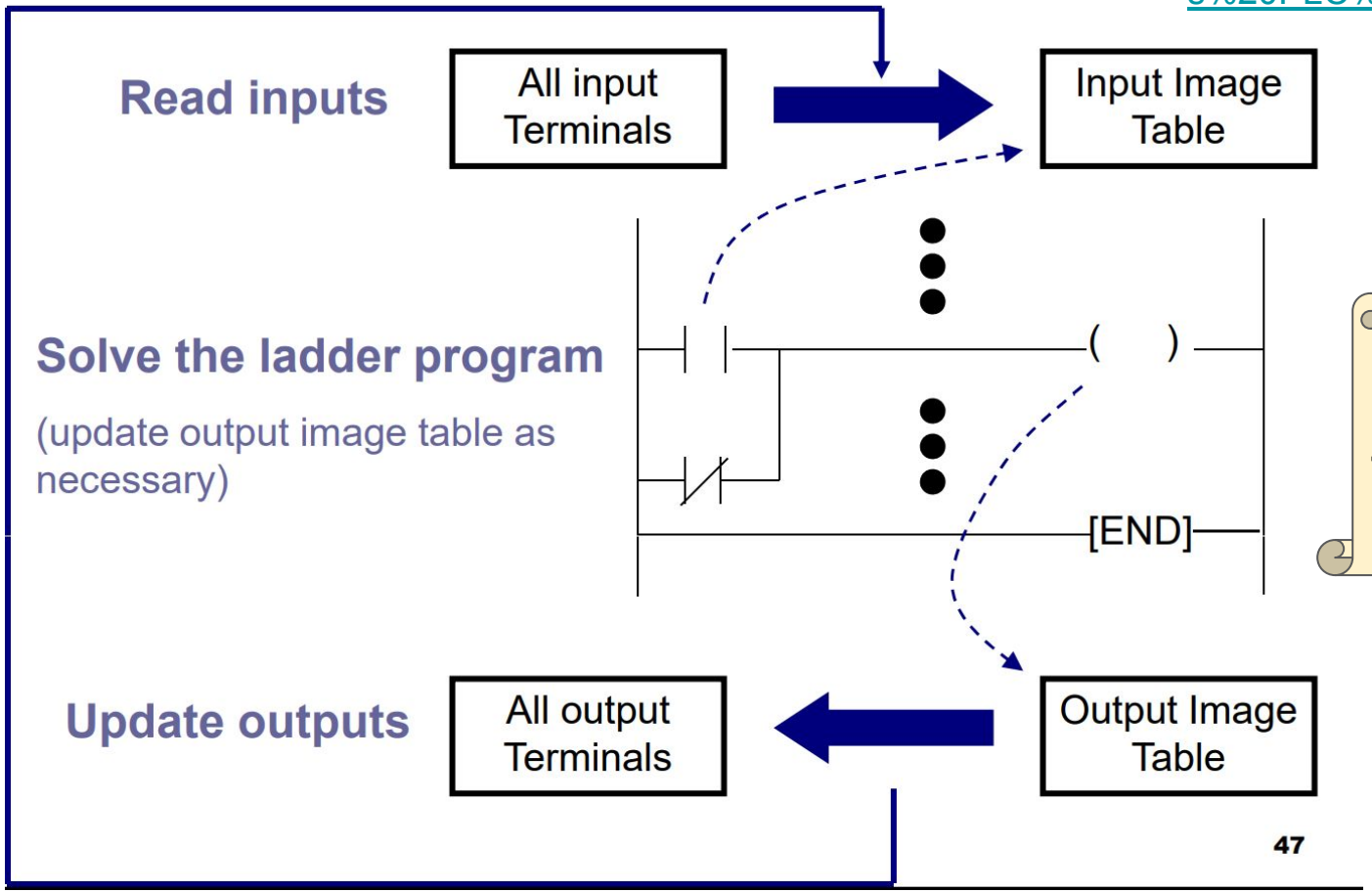


AND

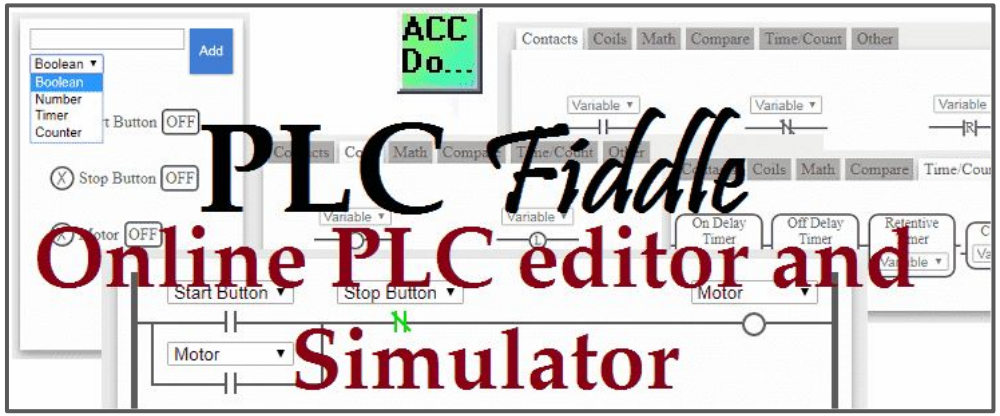
OR

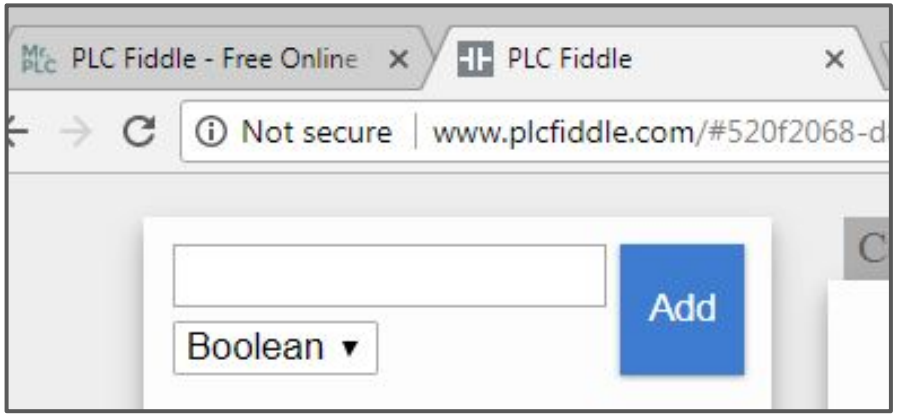
The Scanning Process

https://my.ece.utah.edu/~ece3510/Ladder%20Logic%20Fundamentals%20PLC%20tutorial.pdf



Left to Right
Top to Bottom


PLC Fiddle
Online PLC editor and
Simulator
Add
Boolean
Number
Timer
Counter
Contacts
Coils
Math
Compare
Time/Count
Other
Start Button
Stop Button
Motor
On Delay Timer
Off Delay Timer


PLC Fiddle - Free Online
PLC Fiddle
Not secure
www.plcfiddle.com/#520f2068-d
Add
Boolean

1. PLC Fiddle

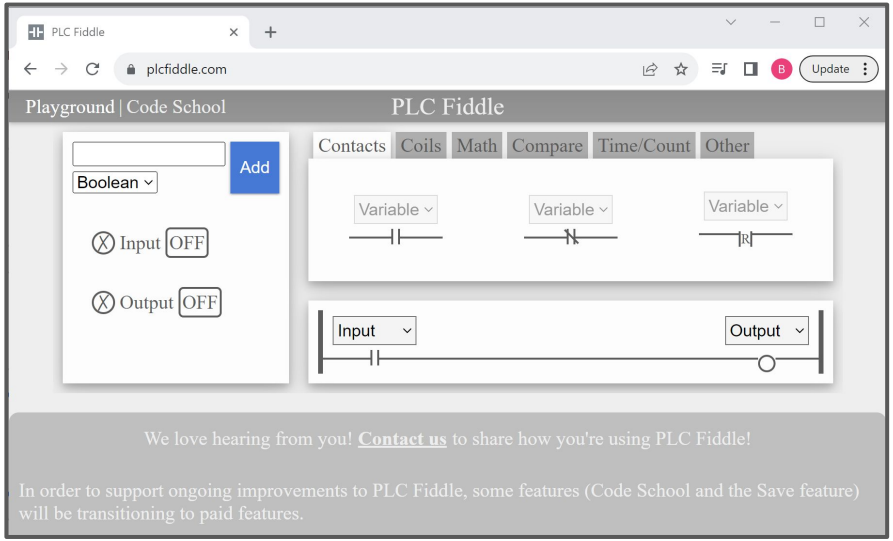
About PLC Fiddle

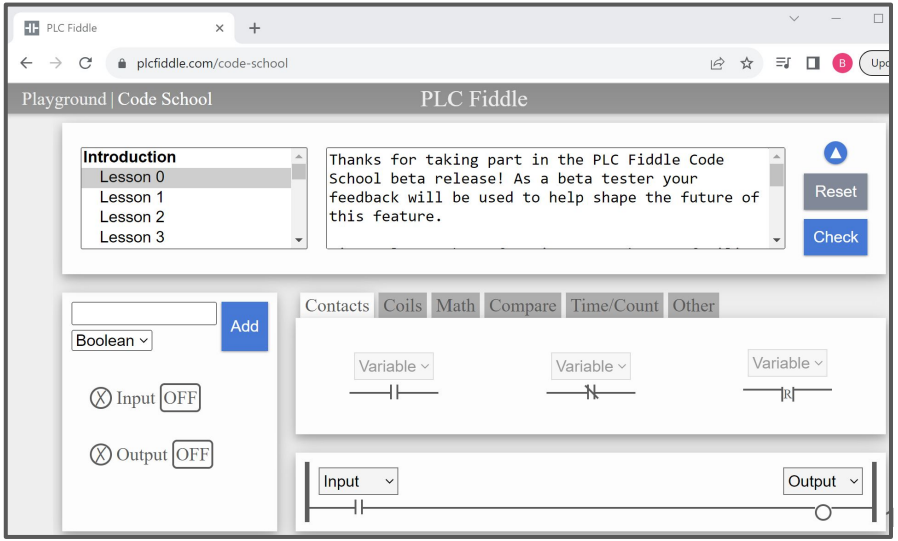
https://www.plcfiddle.com/

PLC Fiddle is a free online PLC Ladder Logic Editor and Simulator that works in your browser.

It includes:

1. Sandbox-like simulator = "Playground"
2. Interactive Tutorial/Lessons = "Code School"



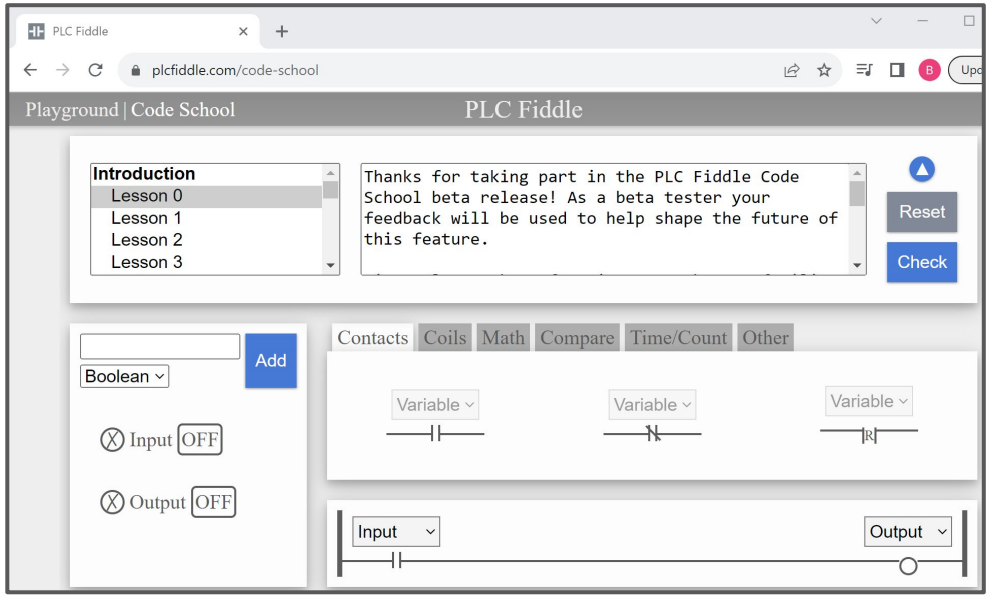


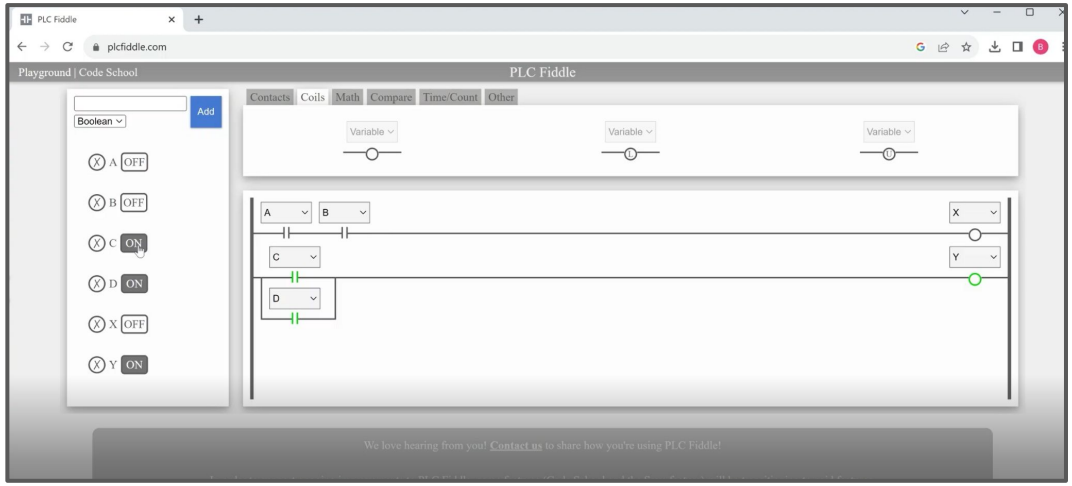
https://www.plcfiddle.com/code-school

PLC Fiddle "Code School" Topics

Here is a list of the topics the Code School covers:

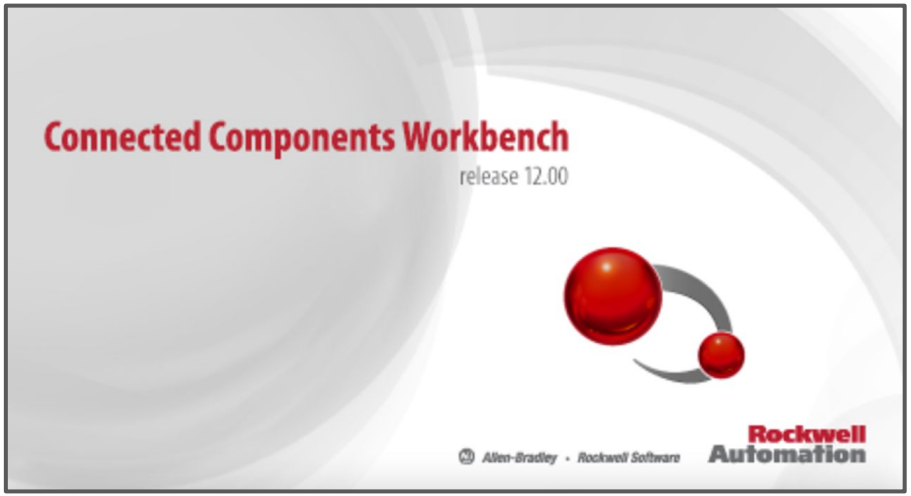
1. Introduction (to the Interface)
2. Boolean Logic Basics
3. Intro to Counters
4. Intro to Timers
5. Working with Numbers





PLC Fiddle Demo

https://github.com/brienc23/Defcon32_workshop_materials/blob/main/PLC_Fiddle_demo_v1_09Aug23_default.mp4



Rockwell Automation

Allen-Bradley
by ROCKWELL AUTOMATION

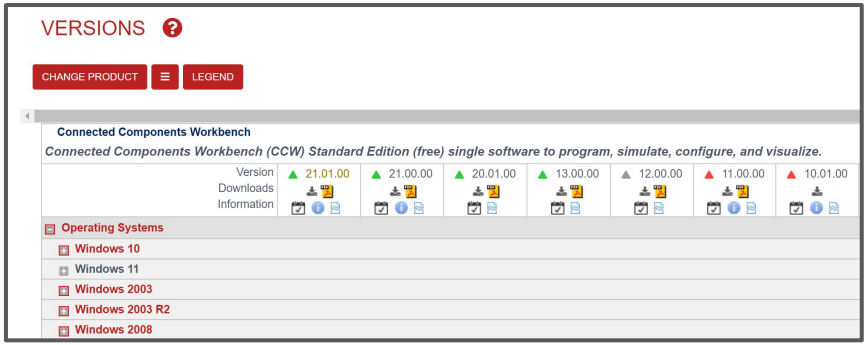
2. Rockwell/Allen-Bradley CCW

Connected Components Workbench (CCW) Overview

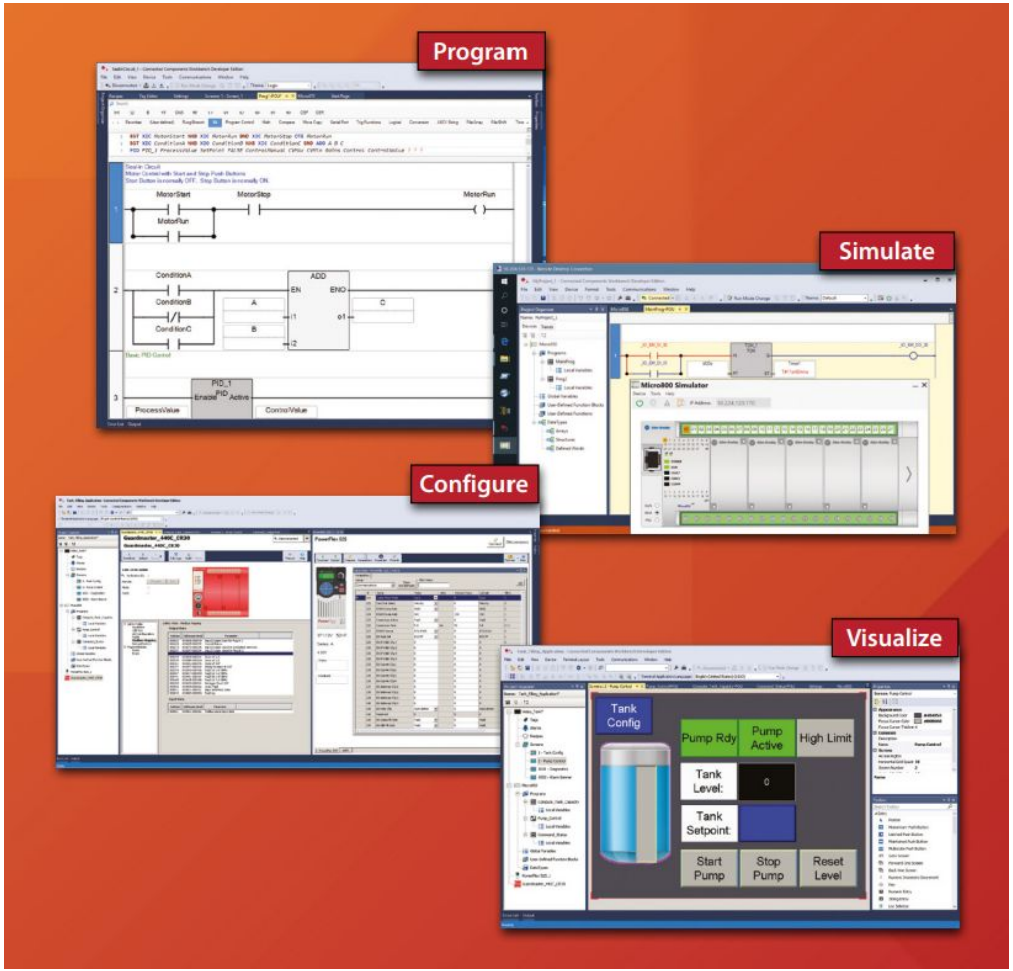
Standard Edition is Free (as in beer)

Program and run their newest low-cost line of PLC micro8X0

You need to sign up for an account on the Rockwell Automation website

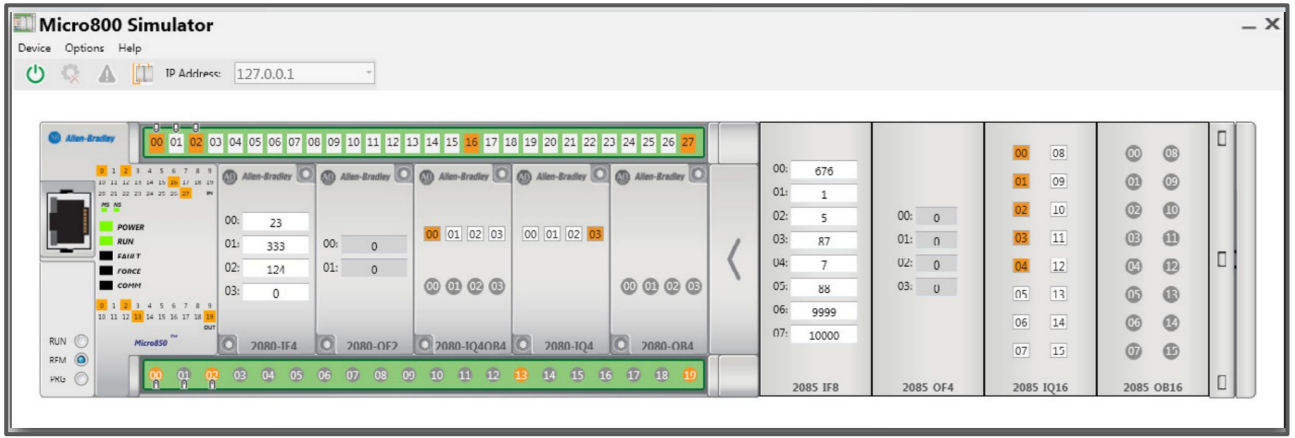


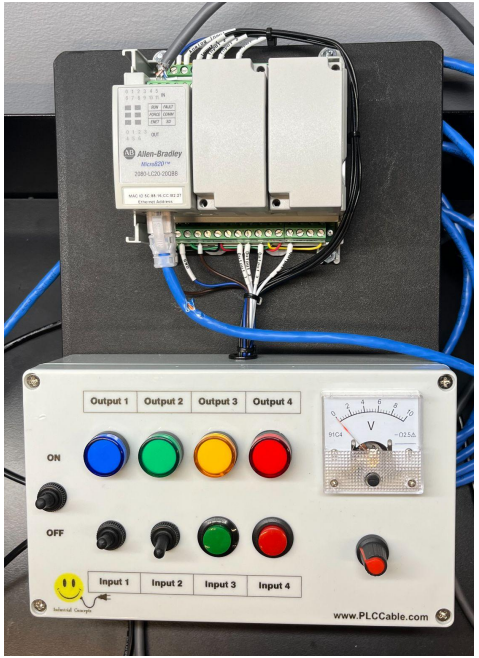
https://compatibility.rockwellautomation.com/Pages/ProductReplacement.aspx?crumb=101&restore=1&vid=62094



https://literature.rockwellautomation.com/idc/groups/literature/documents/pp/9328-pp001_-en-p.pdf

Built-in Simulator -or- Real-World Hardware

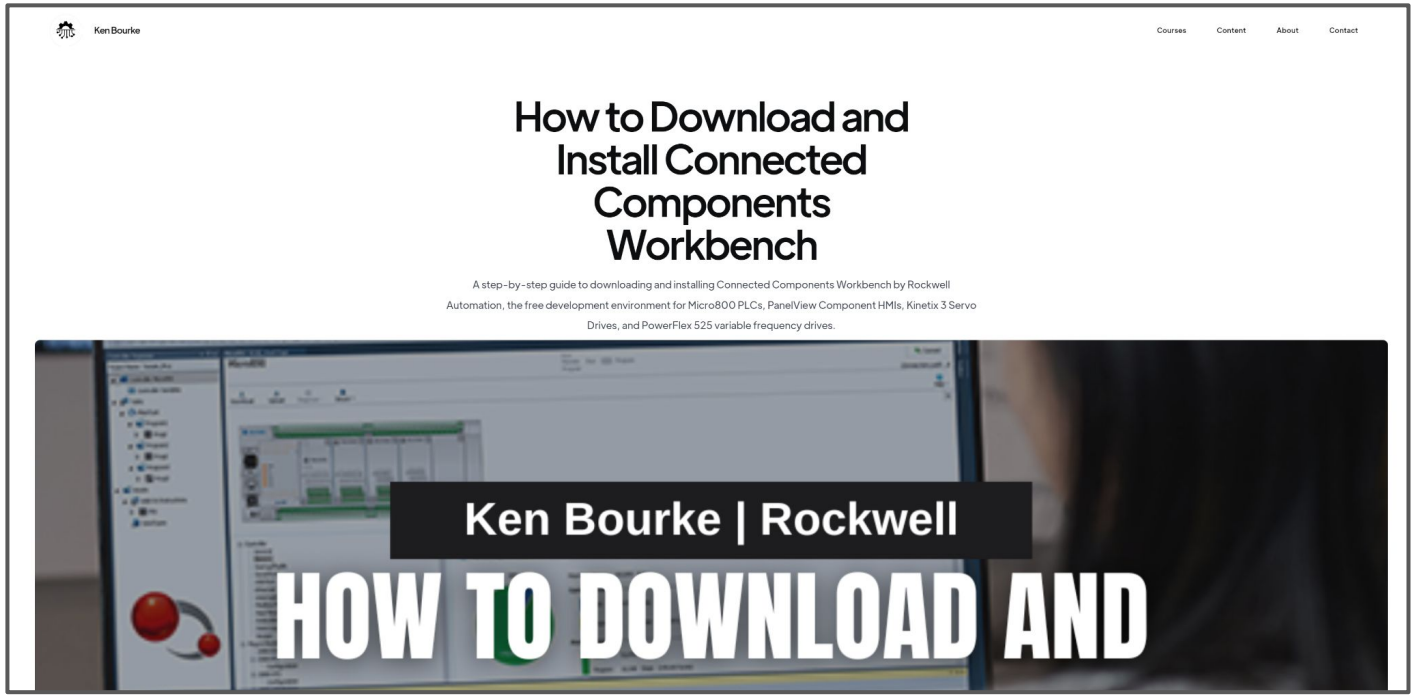




https://www.plccable.com/allen-bradley-micro820-analog-ccw-plc-trainer-micro800-training-kit/

How to Install

https://www.kenbourke.me/posts/how-to-download-and-install-connected-components-workbench



Plenty of other Online Resources

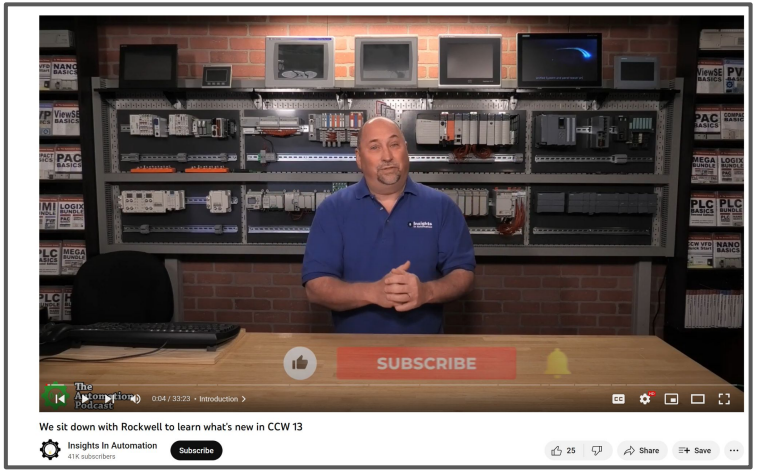
Allen Bradley Micro800 Connected Components Workbench CCW

Tim Wilborne

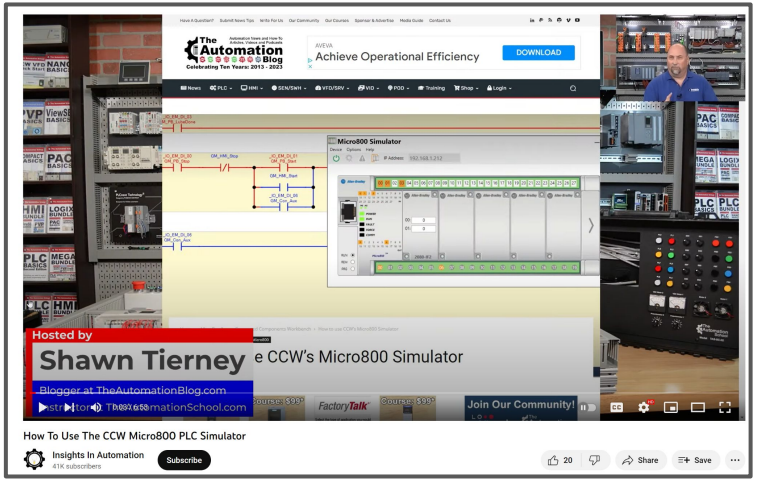
53 videos 54,980 views Last updated on Feb 2...

In this lesson series we show you how to download you software, go through the PLC programming instru ...More

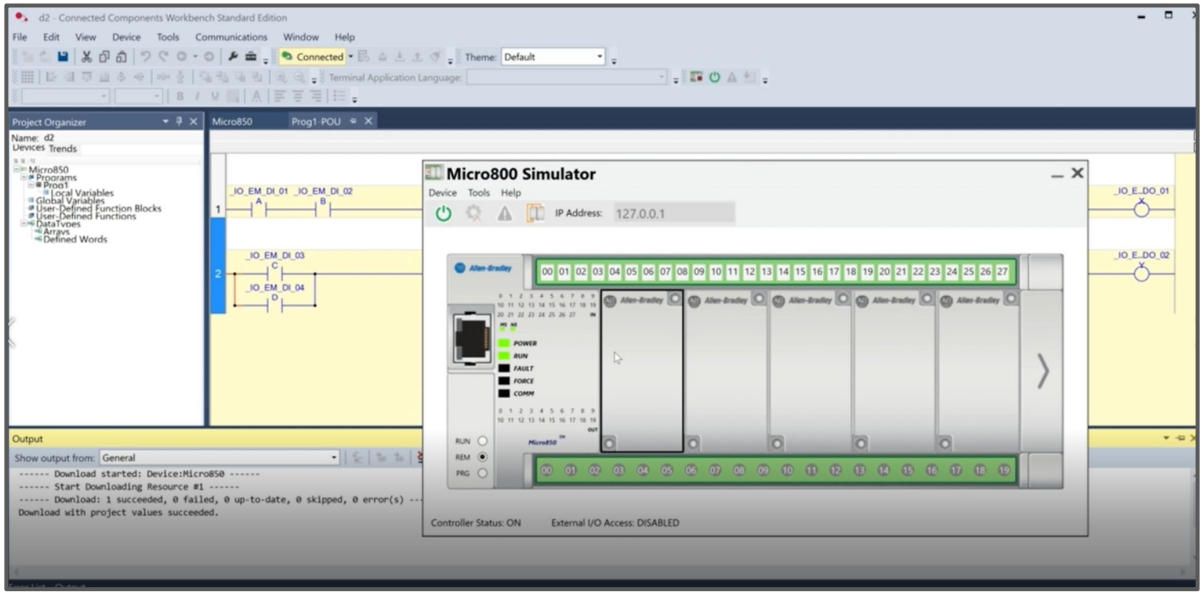
https://www.youtube.com/playlist?list=PLUi5cdVq3wTCjGF-QqwyVLDejTLhHrvAT



https://www.youtube.com/watch?v=j0uWjQD0PIY



https://www.youtube.com/watch?v=s6dRL-8meFs

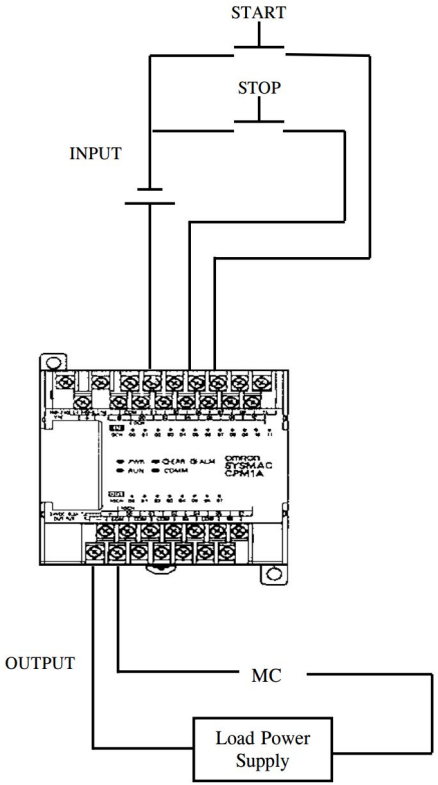


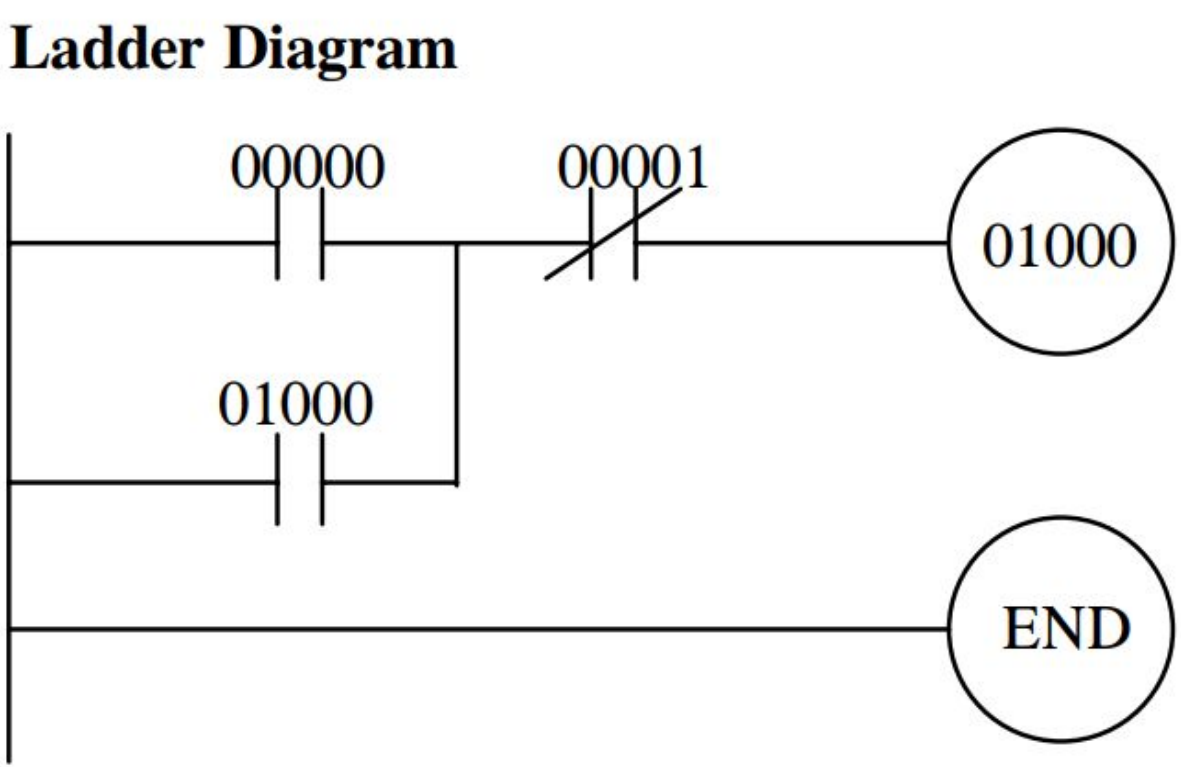
CCW Demo

https://github.com/brienc23/Defcon32_workshop_materials/blob/main/CCW_Demo_v1_09Aug23_570p.mp4

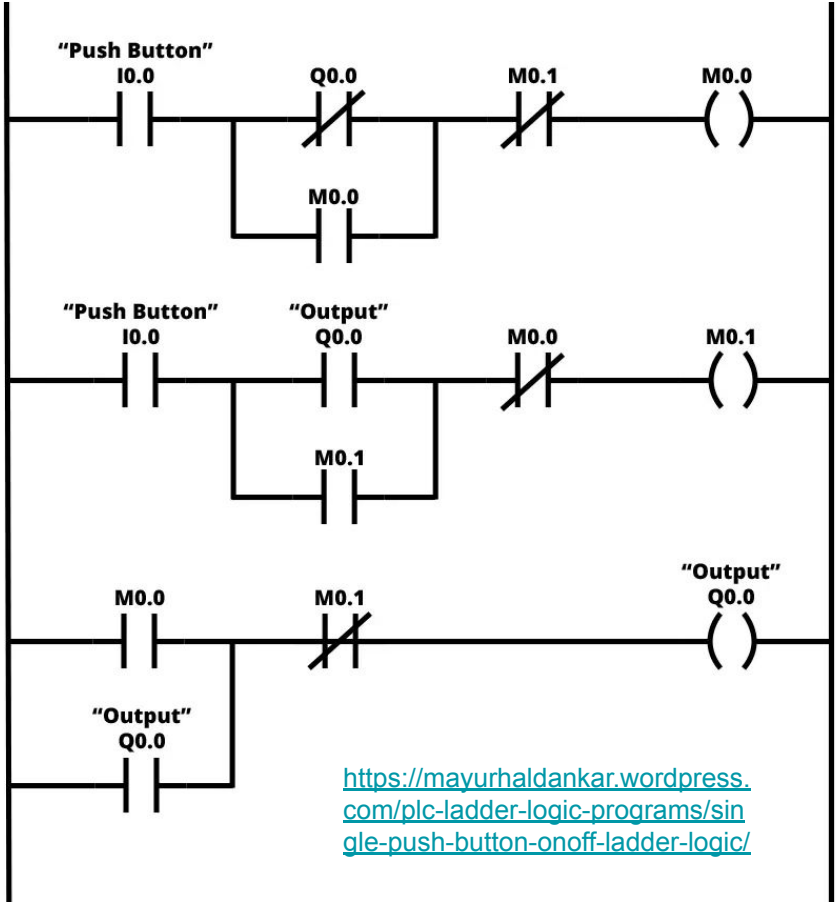
Example Circuits

Latch / Self Holding Circuit

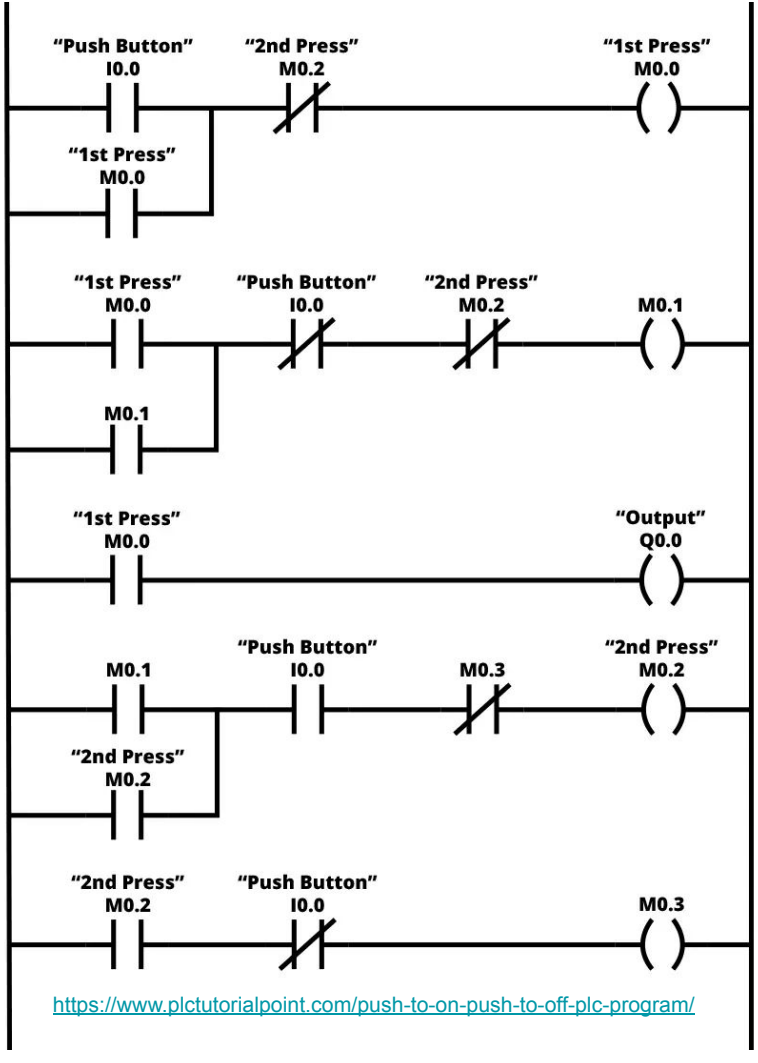




Single Push Button Toggle



https://mayurhaldankar.wordpress.com/plc-ladder-logic-programs/single-push-button-onoff-ladder-logic/

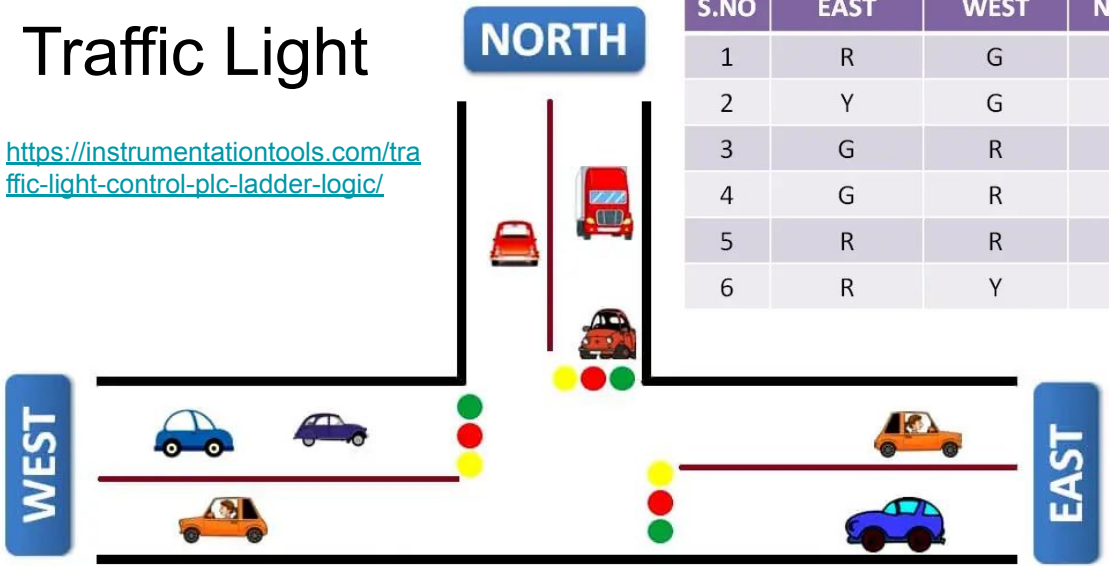


https://www.plctutorialpoint.com/push-to-on-push-to-off-plc-program/

Traffic Light

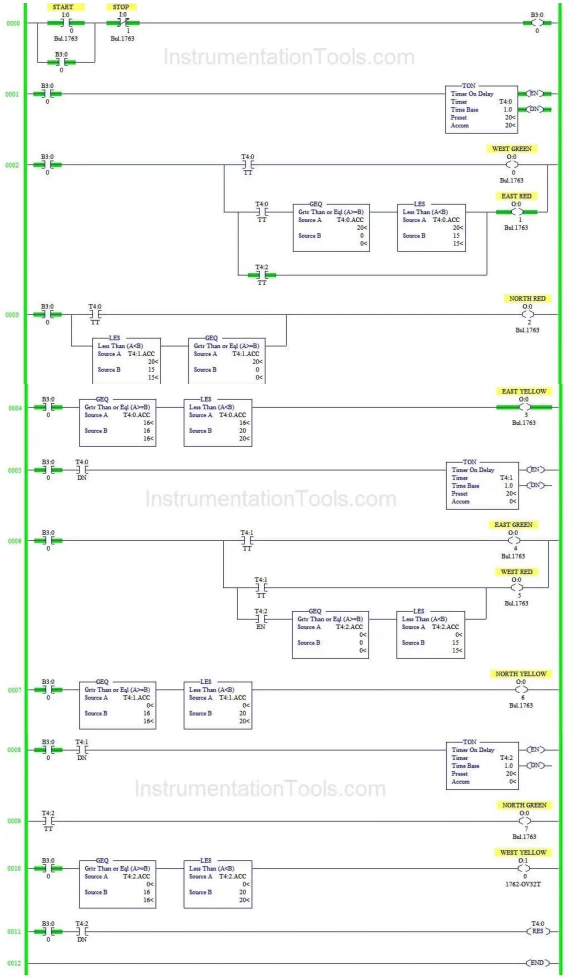
https://instrumentationtools.com/traffic-light-control-plc-ladder-logic/

S.NO	EAST	WEST	NORTH
1	R	G	R
2	Y	G	R
3	G	R	R
4	G	R	Y
5	R	R	G
6	R	Y	G

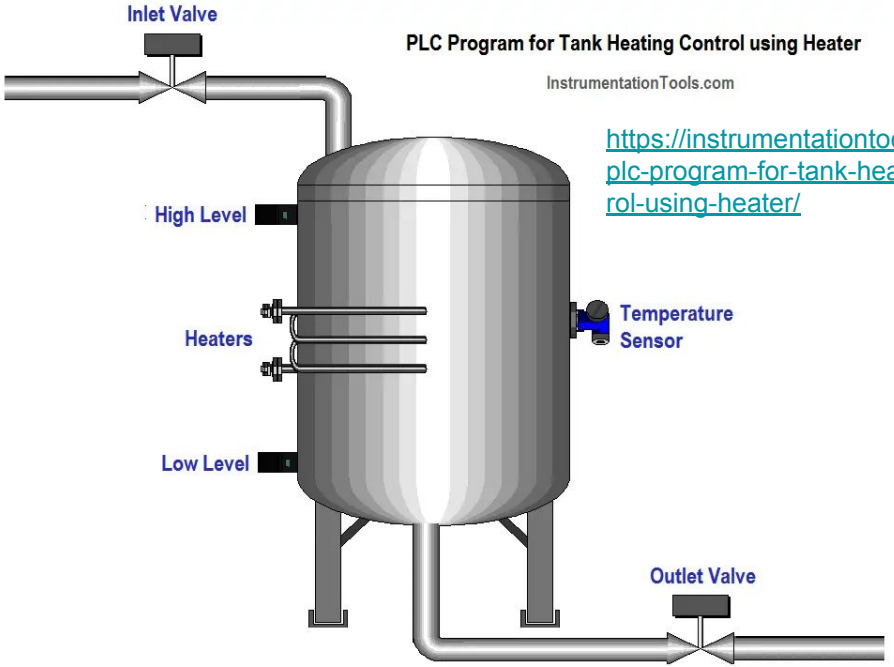


3 - Way Traffic Light Control using PLC

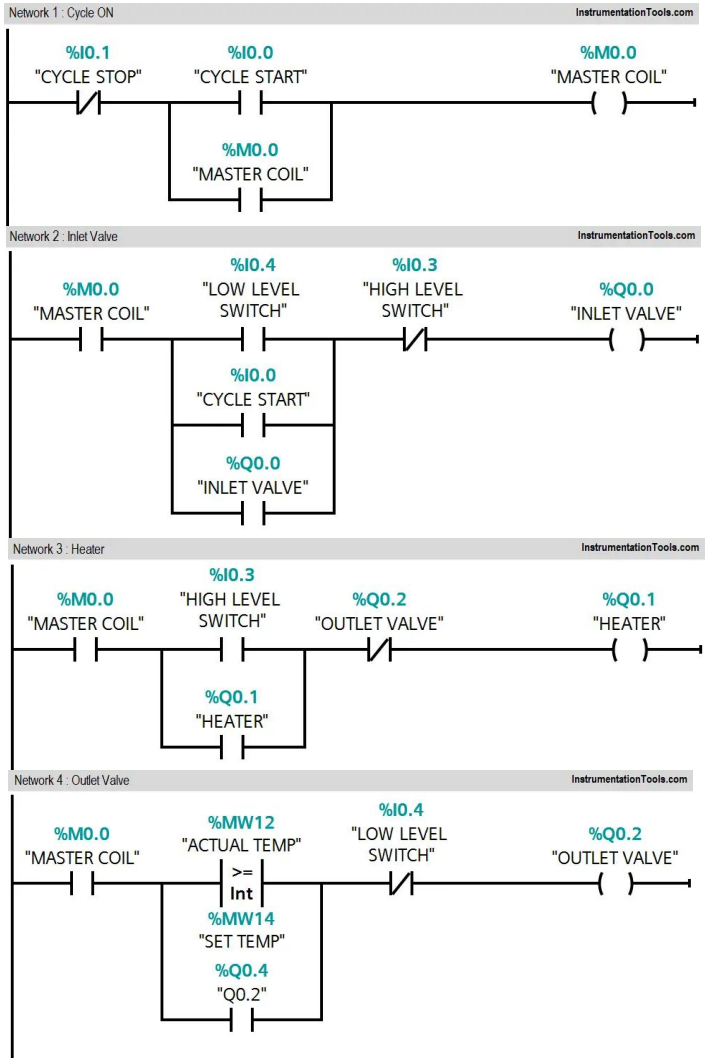
S.no	Address	Name	Input/Output
1	I:0/0	Start	Input
2	I:0/1	Stop	Input
3	B3.0	Memory	Memory
4	O:0/0	West Green	Output
5	O:0/1	East Red	Output
6	O:0/2	North Red	Output
7	O:0/3	East yellow	Output
8	O:0/4	East Green	Output
9	O:0/5	West Red	Output
10	O:0/6	North Yellow	Output
11	O:0/7	North Green	Output
12	O:1/0	West Yellow	Output



Fill and Heat a Tank



https://instrumentationtools.com/plc-program-for-tank-heating-control-using-heater/

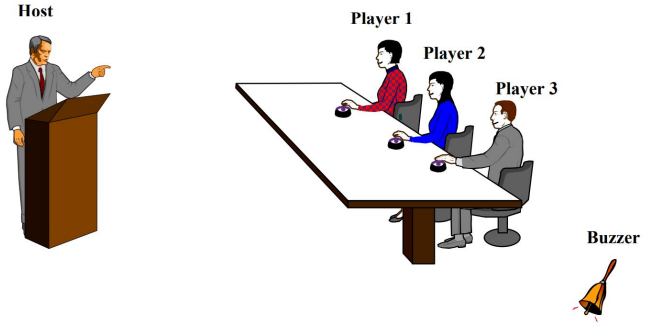


Inputs	Outputs	Physical Elements
I0.0=1	M0.0=1	Master coil ON
I0.4=1	Q0.0=1	Inlet valve ON
I0.3=1	Q0.1=1	Heater ON
MW12≥MW14	Q0.2=1	Outlet valve ON

Example - Quiz Show

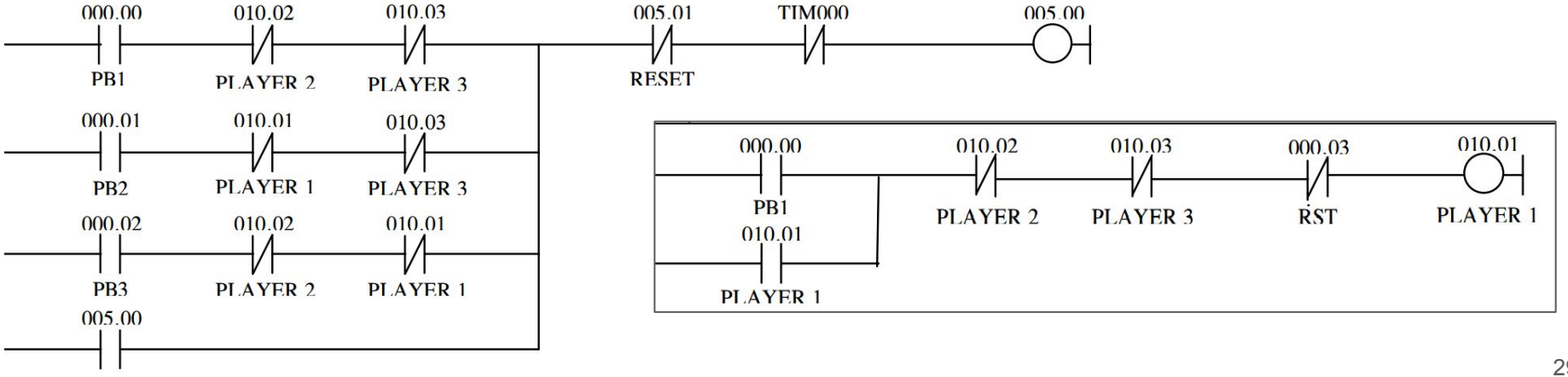
The game buzzer control requirement:

1. After the Host has finished with question.
2. The 3 players will press the switch in front of them to fight to be first to answer the question.
3. The buzzer will sound for 10 sec after any one of the players has touched the switch.
4. The light indicator in front of each player will light-up and only reset by the Host switch.



Input	Device
00000	PB1
00001	PB2
00002	PB3
00003	RST (reset)

Output	Device
01000	Buzzer
01001	Player 1 light
01002	Player 2 light
01003	Player 3 light



Backup Slides

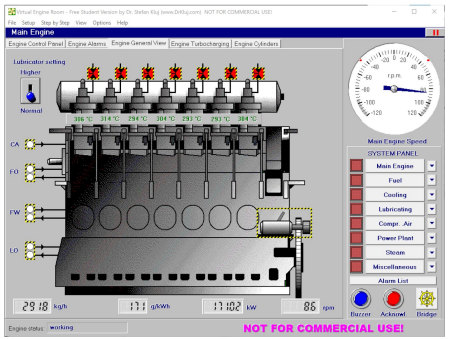
MICS Course Offering

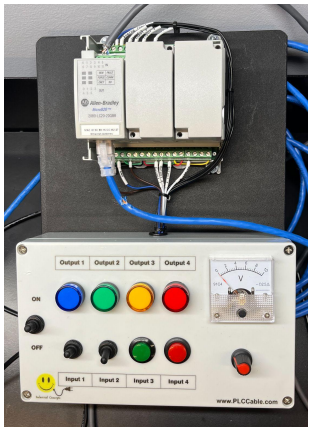
Spring 2023, SY486K Maritime Industrial Control Systems Cybersecurity

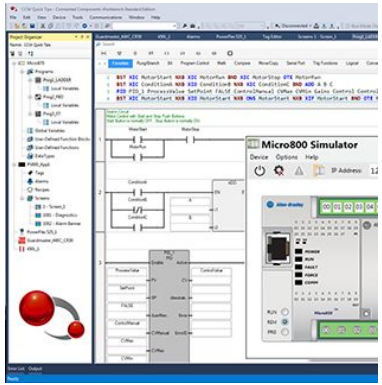
Three-credit technical elective

Lectures, Labs, Student Presentations, and YP Project

Topics included: Maritime Systems, PLC, Ladder Logic, Modbus, CIP, Attacking ICS





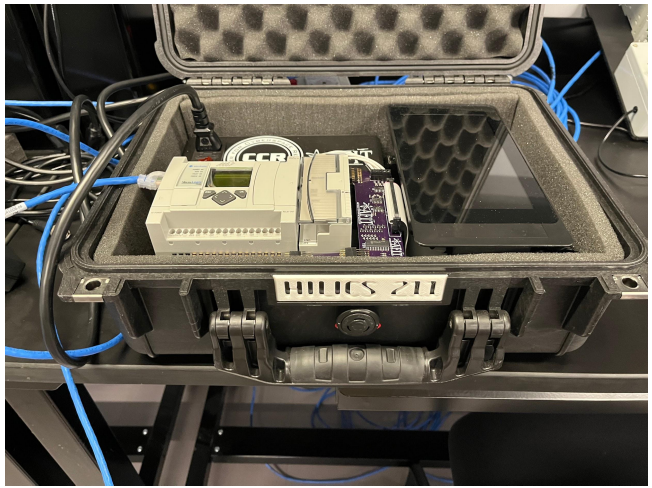


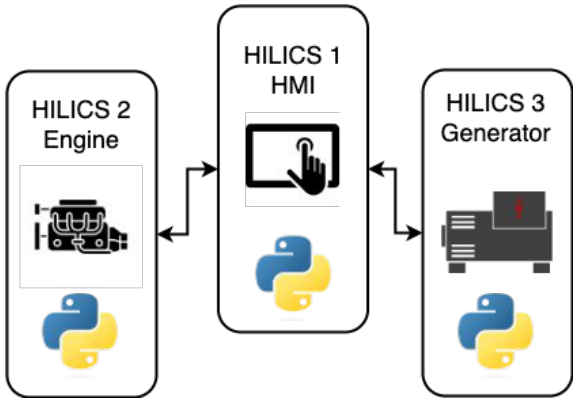
https://github.com/brienc23/MICS_Course_Materials

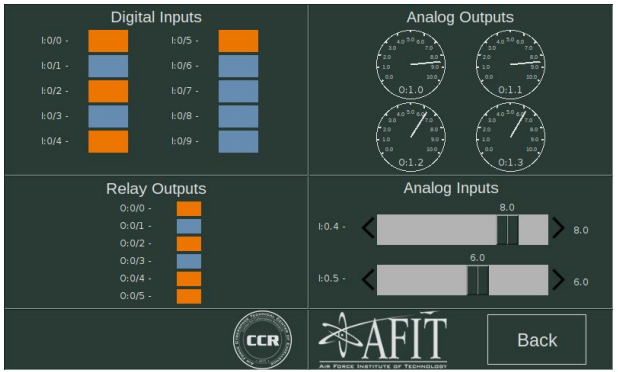
Hardware-in-the-Loop ICS (HILICS)

Produced by Air Force Institute of Technology (AFIT)
AB microLogix 1100+RasPi (with touchscreen HMI) in a Pelican case

https://github.com/sdunlap-afit/hilics







The Scanning Process

https://my.ece.utah.edu/~ece3510/Ladder%20Logic%20Fundamentals%20PLC%20tutorial.pdf

- The scan sequence can be broken into two functional parts:
  - The **Program Scan**
    - Scan the ladder program
  - The **I/O Update Scan**
    - Write outputs, Read inputs

The Program Scan:

https://my.ece.utah.edu/~ece3510/Ladder%20Logic%20Fundamentals%20PLC%20tutorial.pdf

- For each rung executed, the PLC processor will:
  - Examine the status of the input image table bits,
  - Solve the ladder logic in order to determine logical continuity (is the rung true?),
  - Update the appropriate output image table bits, if necessary.

  Note: The output will not actually be energized until the I/O update part of the scan.

https://my.ece.utah.edu/~ece3510/Ladder%20Logic%20Fundamentals%20PLC%20tutorial.pdf

The I/O Update Scan:

- Copy the output image table status to the ALL of the output terminals (discrete output circuits)
  - Power is applied to the output device if it's output image table bit has been previously set to a 1.
- Copy the status of ALL of the input terminals to the input image table
  - If an input is active (i.e., there is electrical continuity), the corresponding bit in the input image table will be set to a 1.