Part 1: Decompose Traffic Light System

1. **What are the actuators?**

   The actuators are the LEDs. This includes the three thar are on the breadboard as well as the other three.

2. **What are the sensors?**

   N/A

3. **What addressable variables are implemented in the ladder logic?**

Name	Type	Location
red_ns	BOOL	%QX100.0
yellow_ns	BOOL	%QX100.1
green_ns	BOOL	%QX100.2
red_ew	BOOL	%QX0.0
yellow_ew	BOOL	%QX0.1
green_ew	BOOL	%QX0.1
time_red_ns	INT	%MW0
time_green_ns	INT	%MW2
time_yellow_ns	INT	%MW1
time_red_ew	INT	%MW3
time_green_ew	INT	%MW5
time_yellow_ew	INT	%MW4

4. **What data sources are in the HMI?**

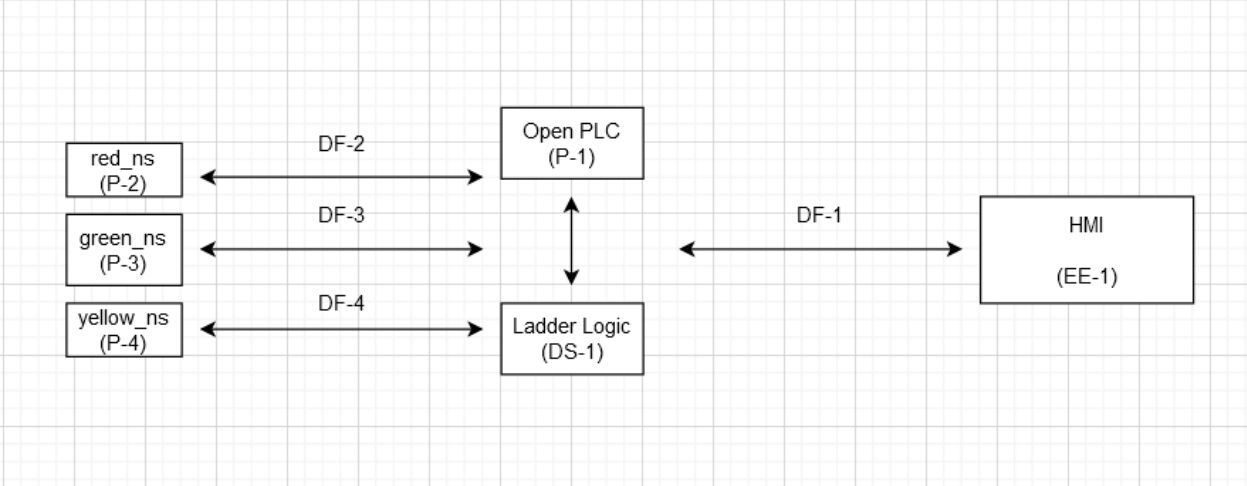
Name	Type	Offset
red_ns	Coil Status	800
yellow_ns	Coil Status	801

green_ns	Coil Status	802
red_ew	Coil Status	0
yellow_ew	Coil Status	1
green_ew	Coil Status	2
time_red_ns	Holding Register	1024
time_green_ns	Holding Register	1026
time_yellow_ns	Holding Register	1025
time_red_ew	Holding Register	1027
time_green_ew	Holding Register	1029
time_yellow_ew	Holding Register	1028

5. **What are the wired connections in the network module? (e.g.: PLC to Actuator XYZ)**

The PLC connects to the HMI via Modbus. The PLC connects to red_ns, green_ns, and yellow_ns via a cyber physical link. This is connecting to the Arduino which connects to the breadboard.

Part 2: Plot the Data Flow Diagram (DFD)



Part 3: List the Threat Consequences (TC)

Code	Description	Hazard
TC-1	Delay in LED changing	H1, H3, H4
TC-2	Delay in HMI updating	H4
TC-3	LEDs on when they shouldn't be	H1, H3, H4
TC-4	PLC and Arduino lose connection	H1, H2, H3, H4
TC-5	HMI and PLC lose connection	H4
TC-6	No LEDs on at all	H1, H4
TC-7	Arduino and LEDs lose connection	H1, H2, H3, H4
TC-8	False values displayed on HMI	H4

Part 4: STRIDE Modeling

STRIDE	Data Flow Element	Threat Consequences
S	**DF-1**	TC-5, TC-1, TC-3, TC-6
S	**DF-2**	**TC-7, TC-4**
S	**DF-3**	**TC-7, TC-4**
S	**DF-4**	**TC-7, TC-4**
T	**EE-1**	**TC-5, TC-8, TC-2**
T	**P-1**	**TC-4, TC-5, TC-6, TC-7, TC-8**
T	**P-2**	**TC-4, TC-5, TC-6, TC-7, TC-8**
T	**P-3**	**TC-4, TC-5, TC-6, TC-7, TC-8**
T	**P-4**	**TC-4, TC-5, TC-6, TC-7, TC-8**
T	**DF-1**	**TC-5, TC-2, TC-8**
T	**DF-2**	**TC-5, TC-6**
T	**DF-3**	**TC-5, TC-6**
T	**DF-4**	**TC-5, TC-6**
T	**DS-1**	**TC-4, TC-5, TC-6, TC-7, TC-8**
R	**EE-1**	**TC-5, TC-8**
R	**P-1**	**TC-4, TC-5, TC-6, TC-7, TC-8**
I	**EE-1**	**TC-5, TC-8**
I	**P-1**	**TC-4, TC-1, TC-2, TC-9, TC-10**
D	**DF-1**	**TC-5, TC-1, TC-8, TC-2**
D	**DF-2**	**TC-5, TC-1, TC-8, TC-2**
D	**DF-3**	**TC-5, TC-1, TC-8, TC-2**
D	**DF-4**	**TC-5, TC-1, TC-8, TC-2**
E	**EE-1**	**TC-4**
E	**P-1**	**TC-1, TC-2, TC-3,TC-4, TC-5, TC-6, TC-7**

Part 5: Define Intrusion Scenario

One scenario is the attacker gaining access by trying to find the server with a scanner. They could then try to login with the default credentials. The server is running on port 502, so it should be easy to find.

Part 6: List Known Exploits

Compromised Component	Exploit	STRIDE	Description
DF-1, EE-1	MiTM	S, E	Spoof values of the counter
EE-1	Default credentials	E, T	Login using the default credentials
DF-1, EE-1	DoS	D	Flood the server with packets causing loss of service
DF-1, EE-1	MiTM	E, D	Packets could be dropped

Part 7: List Attackers' Goals

Goal 1: Cause financial loss by burning out the LEDs.

Goal 2: Cause an accident to occur by causing the LEDs to be on at the wrong time.

Goal 3: Cause an accident by making a delay .

Part 8: Construct Attack Tree