OT Industry Side

Here on the OT side, we have on Field devices like, cameras, temperature measuring device, etc. from where you can get the reading or data from the field devices and that are further transferred to the sensors which are located the site only from there the data goes to the transmitter and then data goes to the PLC where the data in PLC will be got from the physical devices by writing the logic in the PLC.

There are two **types of data in form of signals** that are going to be passed from physical devices that are as follows:

(1) Digital Signals
(2) Analog Signals

These two types of data get transferred in the OT side and that further get convert into the numerical, binary form, string form, etc, which gives the data of how the plant or company is working or performance of company or plant.

From PLC data goes to Firewall protection where in upper layer there is one device present that in Human Machine Interface (HMI) which is also further connected to the Firewall to protect the data from get changed or stolen and PLC are also connected to the Firewall because to protect the PLC from getting the Logic change and securing the data.

Types of PLC's in the industry that are used by the company are as follows:

1. Nano PLC: It has less than 32 input/output functions.
2. Micro PLC: It has more than 32 and less than 128 input/output functions.
3. Small PLC: It has more than 128 and less than 256 input/ output function. It does not have any I/O enhancements that are given under the basic system of this PLC. But here according to the industrial usage here in Small PLC we can use up to 200 input/output functions only.
4. Medium and Large PLC: It has more than 256 input/output functions that can be used to sense the signal and transfer the signal to the database. Here this type of PLC also controls large number of Discrete Elements which are used for fast scanning of data or signal and further transmit it.

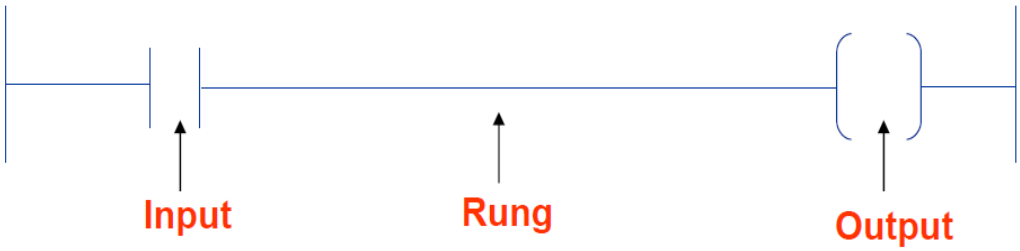
Here in PLC for retrieving the data from the Physical devices we must write the logic from retrieve data which we have to write in following **programming languages:**

(1) Ladder Logic
(2) Function Block Diagram
(3) Sequential Function Charts
(4) Structured Text
(5) Instruction list

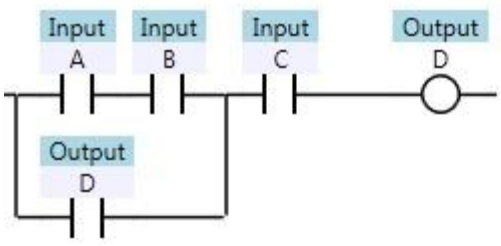
Here in the PLC the data does not get stored but as data is in the form of signals so it senses the signals that are received are and differentiate that this are Digital and Analog signals.

1. Ladder Logic:

Ladder Logic is one of the programming languages used to write logic to sense the data and transfer signals/data in PLC. Following are the examples of the Ladder Logic:

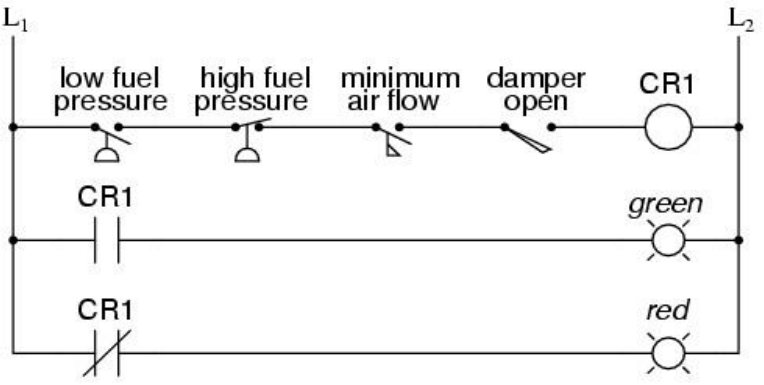


- **Basic Ladder Logic Programs:**



- **Fail Face Ladder Logic:**

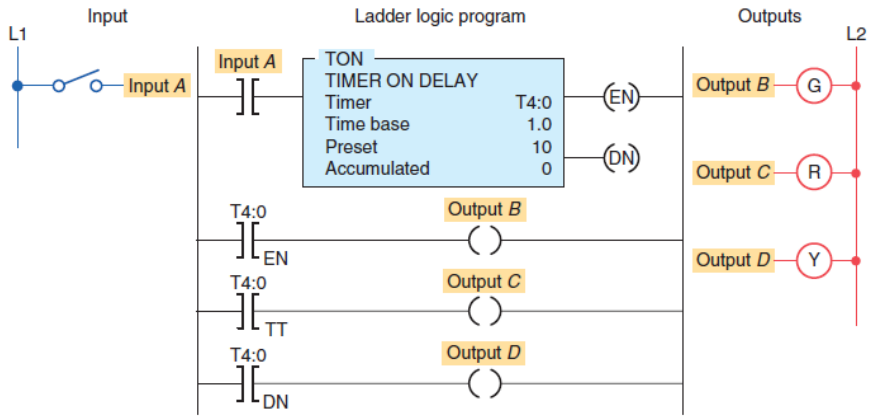
- **Permissive Circuits in PLC:**



Green light = *conditions met: safe to start*

Red light = *conditions not met: unsafe to start*

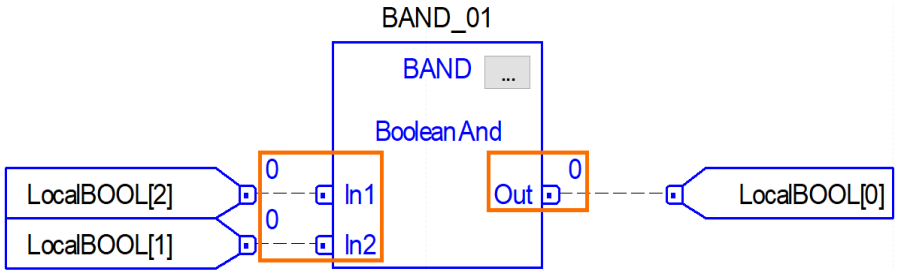
- **PLC Logic for timers:**



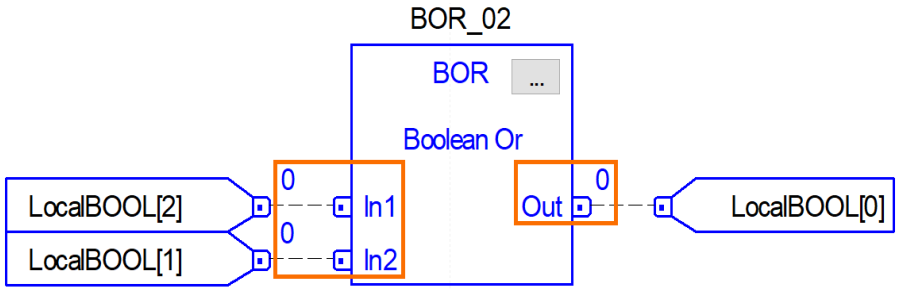
2. Function Block Diagram:

Function Block Diagram is one of the programming languages used to write logic to sense the data and transfer signals/data in PLC. Following are the examples of the Function Block Diagram:

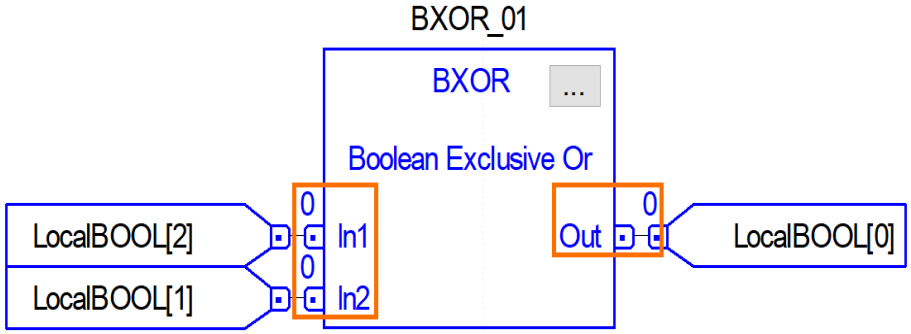
- **For BAND Function Block Diagram Instruction**:



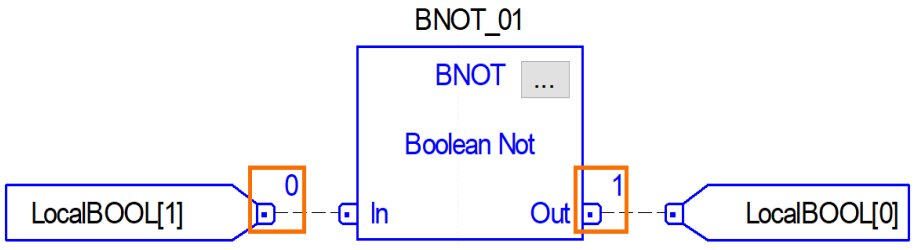
- **For BOR Function Block Diagram:**



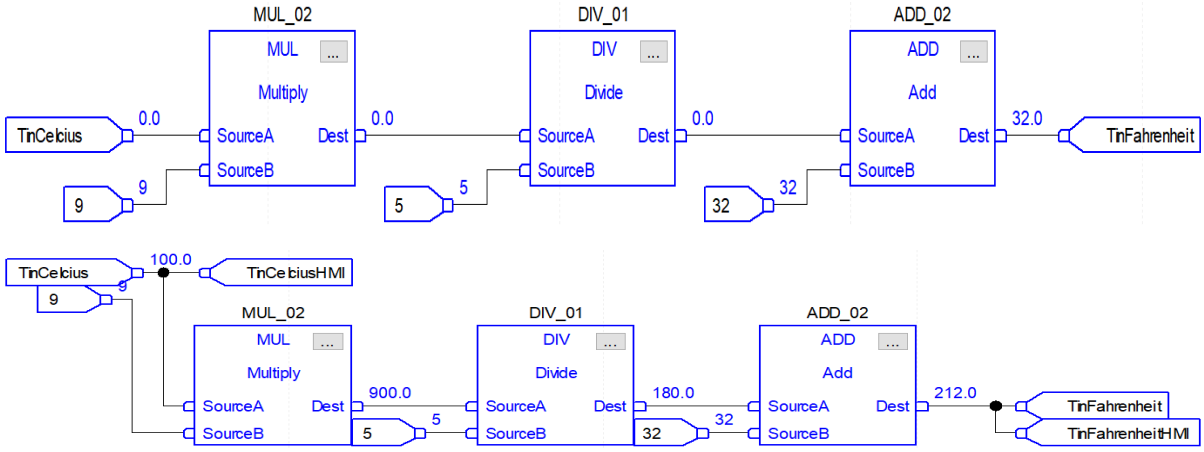
- **For BXOR Function Block Diagram:**



- **For BNOT Function Block Diagram:**



- **For Mathematical Logic Function Block Diagram:**



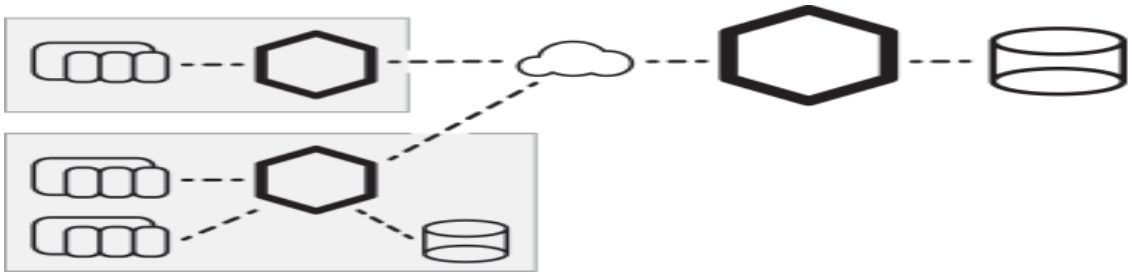
Now here we have discussed so of the Logic writing Languages and examples that can be written in PLC for performing many Industrial operation.

From the PLC the data does to the Database where the first the signal are transferred in to data of number, string, etc,. Here is where the data is stored and data can be control from here. As we have said before about to type signals that are analog and digital signal that get convert in data.

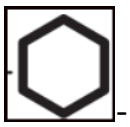
Here to get the data from the PLC to the database we must write the code or logic to get that data from PLC. For storing the data here we use some tools that is the Historian tool or cloud which is used to store and manage the data.

To take the data from PLC to the Historian Tool are as follows:

(1) First we have connect the PLC with the Historian Database using the Connectors.
(2) Here we should provide the network gateway between the PLC's and Historian Database.
(3) Provide the internet connection to add, manage and update the database.



 - PLC/RTU

 - Connector

 - Database(Historian database)

To take the data from PLC to the Cloud are as follows:

(1) Define the data collection tags:

We have to create or form data collection tags in the database of the cloud platform like SQL Server, MS Azure,etc. We have created additional PLC variables like calculated values or counters to support your data needs. For example, you can choose to extract data about machine vibrations, kWh consumption of an energy source or the number of actions of your robot.

(2) Prepare all requirements:

- Create an account in Cloud services providing platform.
- Give the Internet access to the cloud to add, manage, update and delete the data.
- Ethernet Connection is also needed to directly get connected to the third-party devices.
- Protocol and Variables are formed to get data.

(3) PLC IOT Gateway:

Here PLC IOT Gateway is created because the make a Virtual Cloud Network (VPN) in the Cloud to take all devices in it and can access it easily.

(4) Configure PLC data protocol:

Here we must configure the data protocol which includes the data processing and transferring of data and provide security to the data while managing and transferring.

(5) Setup variables and tags to transmit PLC data to cloud

(6) Design your PLC data dashboards

To Get Data from the cloud to the dashboard are as follows:

(1) You can download the database in the from of excel sheet and than you can access that database.
(2) Can access the cloud database by directly using the by authenticating factor the Cloud database.

Types of Injection attacks that can be applied in OT Section that are as follows:

(1) SQL Injection
(2) Cross-Site Scripting
(3) Code Injection
(4) Command Injection
(5) CCS Injection
(6) Injections application in the Network:
    a. SMTP/IMAP Command Injection.
    b. Host Header Injection.
    c. Lightweight Directory Access Protocol (LDAP) Injection.
    d. “Carriage Return” & “Line Feed” (CRLF) Injection.

Sr.No.	Type of Injection	Where Applied
1	SQL Injection	On database of cloud and in data storage in OT(historian)
2	Cross-Site Scripting	It is from the IT side
3	Code Injection	It is from the IT side
4	Command Injection	It is from the IT side and OT side the operators can also do
5	CCS Injection	It is their between Physical Device to PLC to Database
6	SMTP/IMAP injection	It is from the IT side, it can their at PLC level as it is in network
7	Host Header Injection	It is from the remote access side
8	LDAP Injection	It is on the both IT and OT side as it deals with data
9	CRLP Injection	It is network injection.

FLOWCHART OF THE OT SIDE DATA FLOW WITH INDICATING INJECTION APPLIED PLACES: