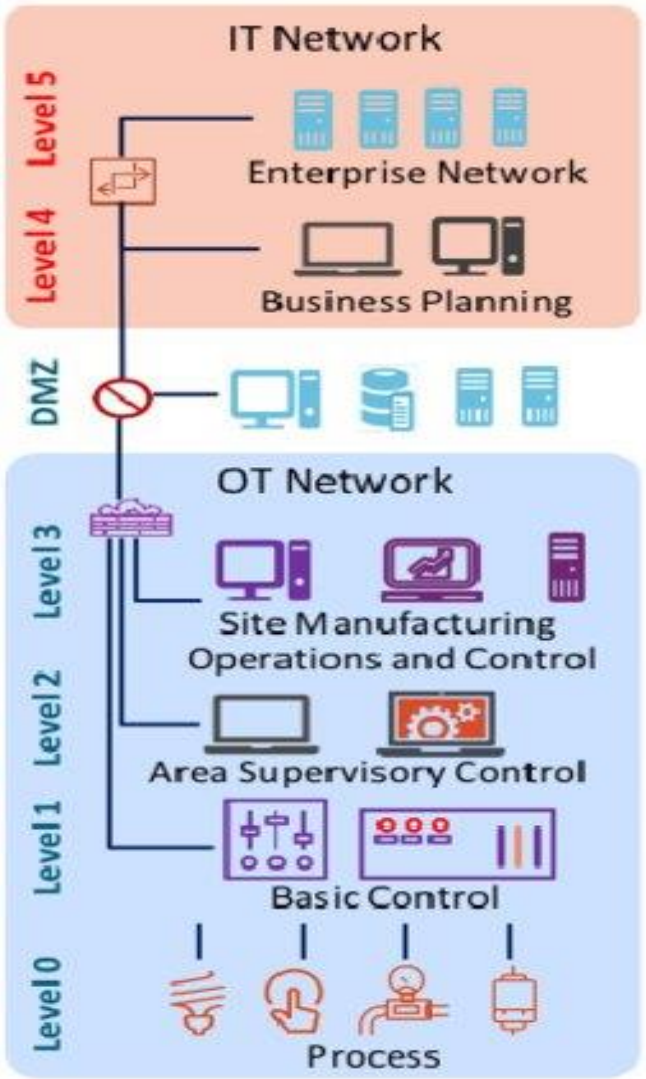
Tutorial 3

Ladder Logic

Basics
IT & ICS Kill chain



Planning		Reconnaissance
Preparation	Weaponization	Targeting
Cyber Intrusion	Attempt	Delivery
		Exploit
	Success	Install/Modify
Management & Enablement		C2
Sustainment, Entrenchment Development & Execution		Act
Attack Development & Tuning		Develop
Validation		Test
ICS Attack		Deliver
		Install/Modify
		Execute

First stage : Ladder Logic (diagrammatic notation)

- Diagrammatic Boolean symbols:

Input 1

True → contact ON

False → contact OFF

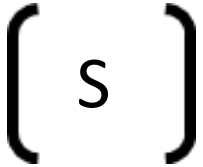
Input 2

True → contact OFF

False → contact ON

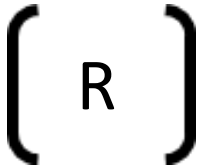
First stage : Ladder logic (diagrammatic notation)

output 1



Set output 1 when it is True

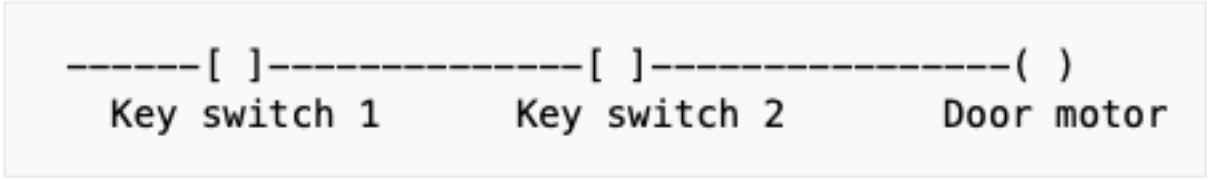
output 1



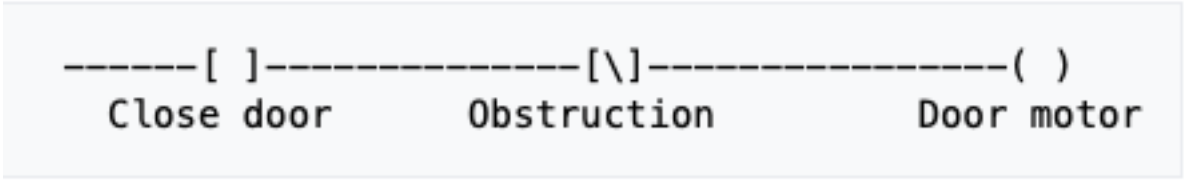
Reset output 1 when it is True

Ladder Logic (Wikipedia)

AND



NOT

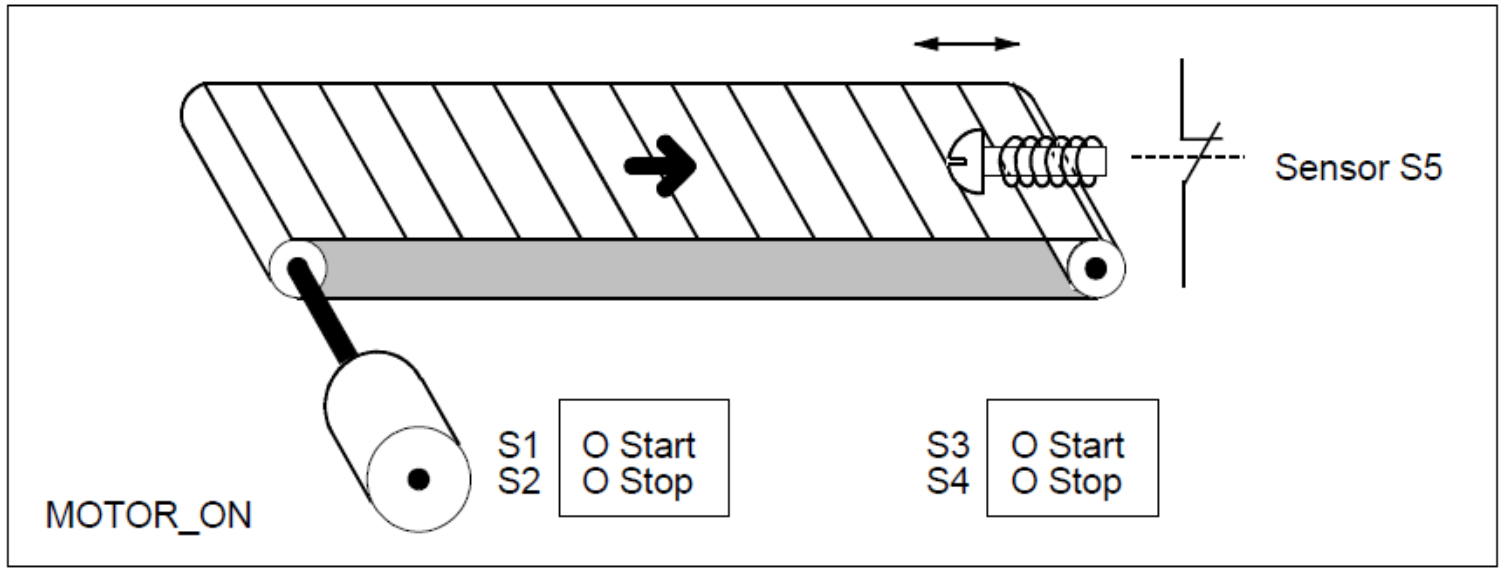


OR

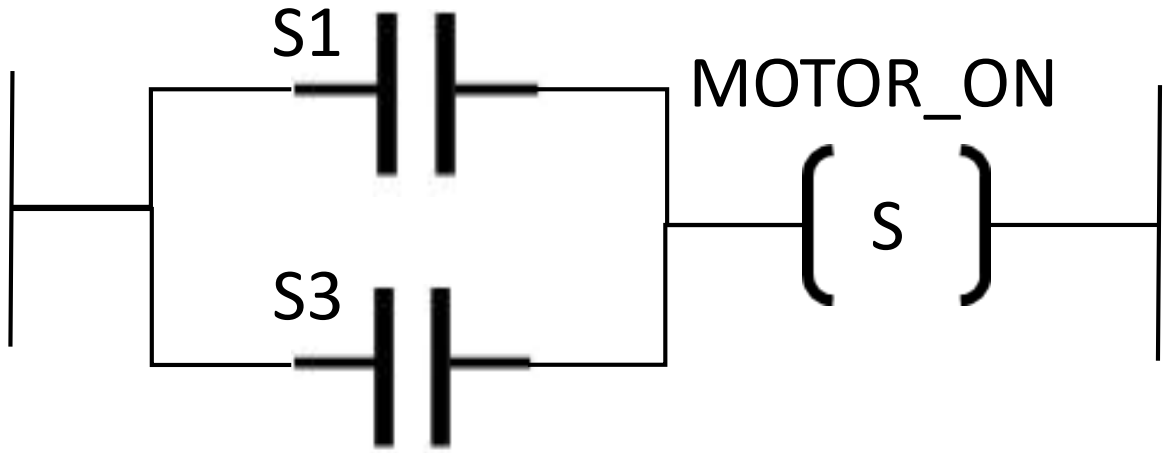
[ ] input ( ) output

Example 1: Controlling a Conveyor Belt

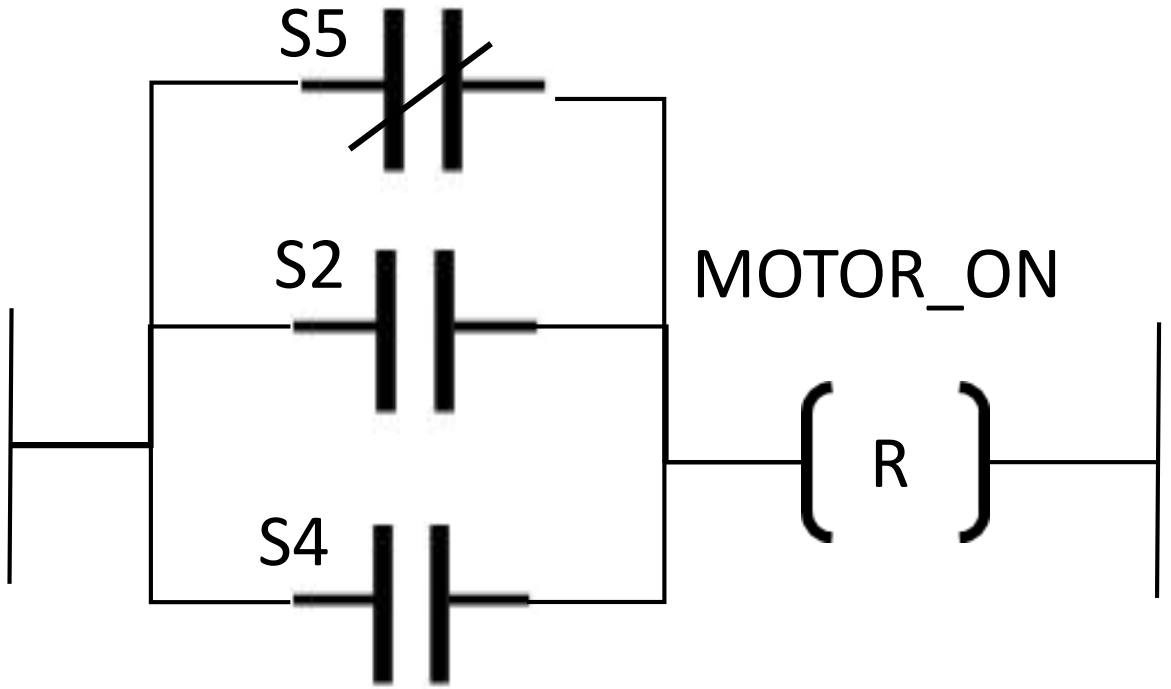
The following figure shows a conveyor belt that can be activated electrically. There are two push button switches at the beginning of the belt: S1 for START and S2 for STOP. There are also two push button switches at the end of the belt: S3 for START and S4 for STOP. It it possible to start or stop the belt from either end. Also, sensor S5 stops the belt when an item on the belt reaches the end.



Ladder Logic for example 1



Turn ON the motor belt



Turn OFF the motor belt

Second stage: Symbolic Programming

- Symbolic Programming codes (From the table at page 261)

Mnemonic	Program Elements Catalog	Description
AW	Word logic instruction	And Word
OW	Word logic instruction	Or Word
CD, CU	Counters	Counter Down, Counter Up
S, R	Bit logic instruction	Set, Reset
NOT	Bit logic instruction	Negate RLO
FP	Bit logic instruction	Edge Positive
+I	Floating-Point instruction	Add Accumulators 1 and 2 as Integer
/I	Floating-Point instruction	Divide Accumulator 2 by Accumulator 1 as Integer
*I	Floating-Point instruction	Multiply Accumulators 1 and 2 as Integers
>=I, <=I	Compare	Compare Integer
A, AN	Bit logic instruction	And, And Not
O, ON	Bit logic instruction	Or, Or Not
=	Bit logic instruction	Assign
INC	Accumulator	Increment Accumulator 1
BE, BEC	Program Control	Block End and Block End Conditional
L, T	Load / Transfer	Load and Transfer
SE	Timers	Extended Pulse Timer

Symbolic Programming for example 1

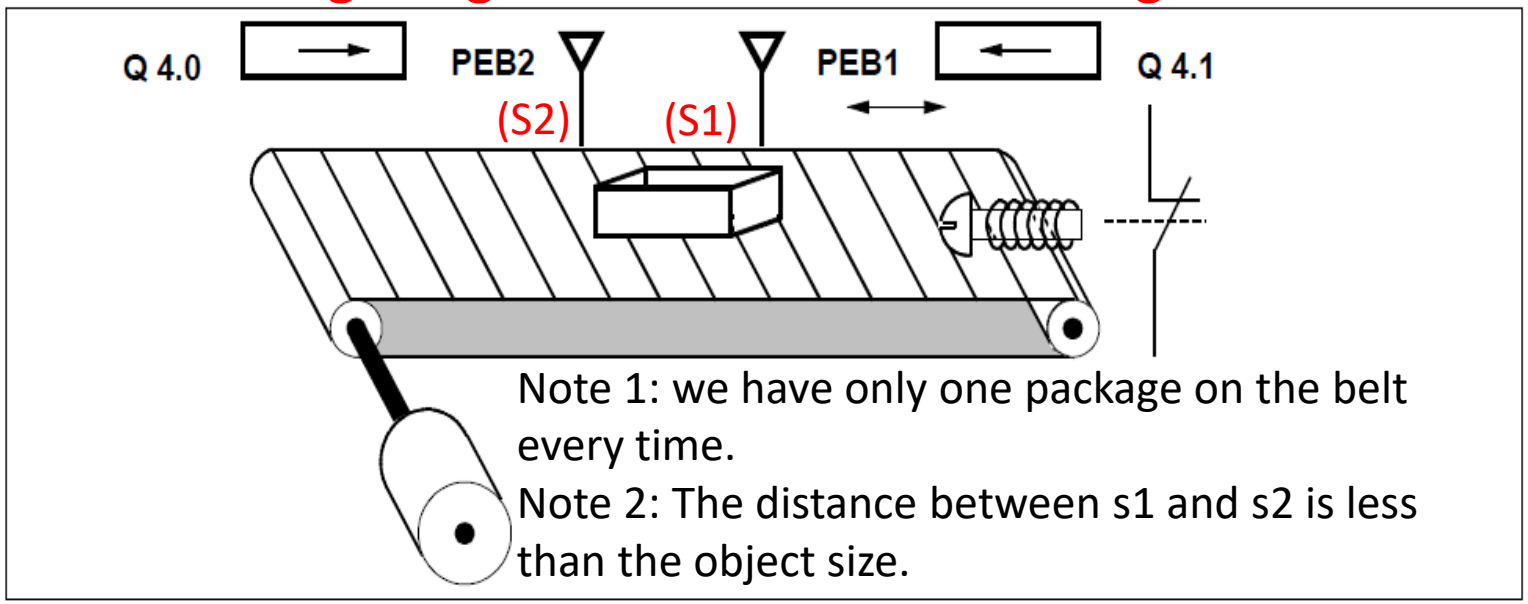
Symbolic Program	
O	S1
O	S3
S	MOTOR_ON
O	S2
O	S4
ON	S5
R	MOTOR_ON

Example 2: Detecting the Direction of a Conveyor Belt

The following figure shows a conveyor belt that is equipped with two photoelectric barriers (PEB1 and PEB2) that are designed to detect the direction in which a package is moving on the belt. Each photoelectric light barrier functions like a normally open contact.

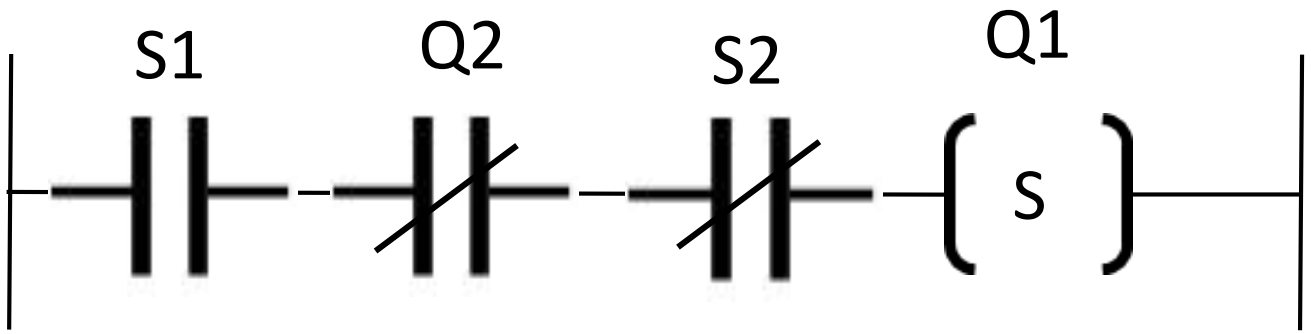
Q2 : Right sign

Q1 : Lift sign

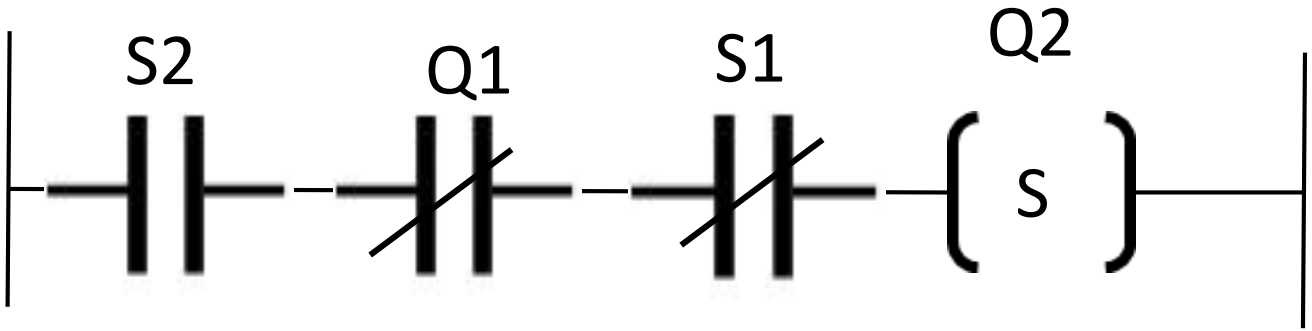


Design a Ladder Logic for this operation using sensors (S1, S2) as inputs, and Q1 and Q2 as outputs.

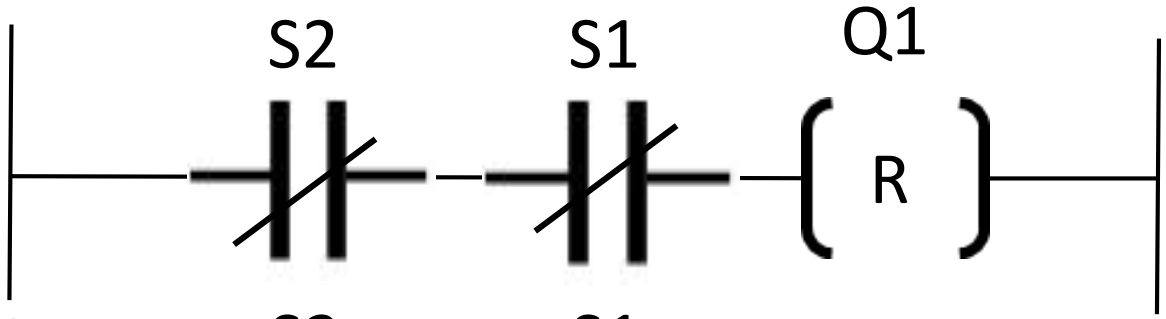
(you have 20 minutes only)



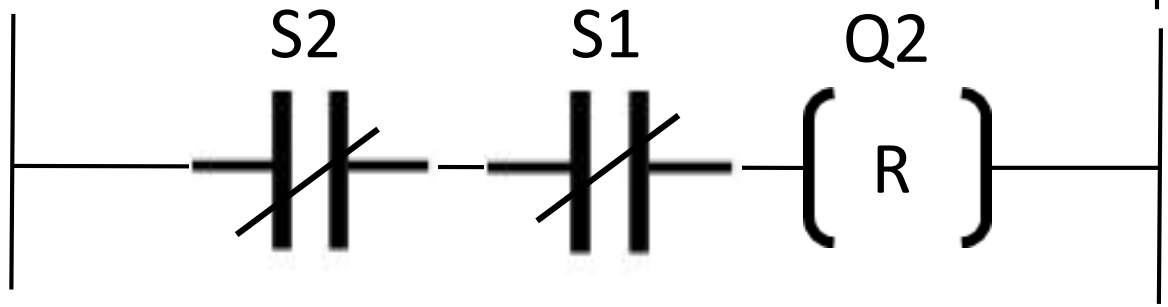
The package is moving to the Right direction



The package is moving to the Left direction



No package on the belt



No package on the belt