CS 8803: Introduction to Cyber-Physical System Security

Mini Project 1: Programming with Ladder Logic

Assigned: February 6th, 2017 **Due: February 20th, 2017, 10pm (EST)**

Introduction

This three part project will focus on Ladder Logic programming using Schneider Electric SoMachine Basic**.** **http://www.schneider-electric.com/ww/en/download/document/SOMBASAP14SOFT**

You should not have to change the configuration of the SoMachine Basic simulation. You should only need to access the "Programming" tab to complete the project.

For students without a windows system, a VM with SoMachine basic is provided below.
https://drive.google.com/open?id=0B86Hc2O9GEPzTWV1LS03VDR0cEk

Part 1

Construct three different Ladder Logic programs, each building upon the previous one:

A. Construct a program that will simulate a push button activated LED.
   1. When Input 0 is activated, Output 1 should activate.
   2. When input 0 is deactivated, Output 1 should deactivate.
   3. Inversely, when Input 1 is activated, Output 0 should deactivate.
   4. When input 1 is deactivated, Output 0 should activate.

B. Construct a program that simulates an LED powered by an On-Off loop.
   1. When input 0 is activated, Output 0 should activate for 5 seconds, then deactivate for 5 seconds.

C. Construct a program that simulates the same On-Off power loop, except the amount of time for the loop should be dictated by the Analog Inputs.
   1. The "On" portion (Analog 0) should be 3 seconds.
   2. The "Off" portion (Analog 1) should be 1.5 seconds.

For your convenience the following can be used as a reference for how the above elements are referred in SoMachine Basic:

Input 0 = %I0.0
Input 1 = %I0.1
Output 0 = %Q0.0
Output 1 = %Q0.1
Timer 0 Preset = %TM0.P
Timer 0 Finished = %TM0.Q
Analog Input 0 = %IW0.0
Analog Input 1 = %IW0.1

Part 2

You are the Industrial Controls Systems Engineer at a Soft Drink Processing Plant. Having heard of recent attacks at similar plants that prevent the operators from shutting down their machinery when instructed, you were immediately suspicious when you saw your ladder logic program had been recently updated by someone other than you. You open the program to find it has been thoroughly tampered with to the point that a shutdown could not occur if instructed. Left alone, this would cause the machines to continue to operate nonstop, leading to soft drink spilling out and getting the floor all sticky, and possibly even irreversible machine damage.

The shutdown process, when functional, occurs in a series of checkpoints to ensure smooth and gradual cessation of the machinery. While an Emergency Shutdown button does exist, it is limited to life threatening situations, as such a sudden shutdown can damage machinery. The process should work as follows:

1. When the operator presses the Shutdown Button (Input 0), a 5 second timer begins before the first checkpoint (Output 0) is activated and the rest of the process can continue.
    a. After this point the shutdown process can be canceled (Output 1) by the operator pressing the Cancel Shutdown Button (Input 1). This cancellation cannot occur unless the Shutdown Button (Input 0) has been activated.
2. For the process to continue, the pressure inside of the machines needs to be high enough such that the piping system doesn't get damaged. The operator needs to set the pressure of the machines to above the Pressure Checkpoint (Constant Word 0) using Analog Input 0. Then, the operator activates the Confirm Pressure Change button (Input 2) to register the change in the system. This will activate the second checkpoint (Output 2).
3. Finally, the operator confirms the shutdown process by pressing The Confirm Shutdown button (Input 3), resulting in the activation of the third and final checkpoint (Output 3), and the full shutdown of the system (Output 5).
4. In the case of an emergency, the Emergency Shutdown button (Input 4) can be pressed to activate the immediate shutdown procedure (Output 4) and result in subsequent shutdown (Output 5).

You are allowed to alter the code to any extent you wish, provided you adhere to these previous specifications for the Shutdown Process. You should assume that any rung of the ladder logic program, with the exception of the Shutdown Rung, can have no, one, or several problem(s) in them which you need to fix. **Do not alter the Shutdown Rung, as this Rung is used to grade your code. Failure to adhere to this instruction will result in a deduction of points.** It is clearly labeled with a comment, so it will be obvious which one it is.

For your convenience the following can be used as a reference for how the above elements are referred in SoMachine Basic:

Constant Word 0 = %KW0
Current Pressure = %MW0
Set Pressure = %IW0.0

Part 3

Many times in industrial control systems, devices such as Programmable Logic Controllers (PLCs) are commonly used to directly interact with sensors and actuators, and perform local automatic control. PLCs are often placed at relatively exposed locations in the field and are thus vulnerable to tampering by a nearby attacker. In particular, the attacker could attempt to manipulate firmware or logic to change the behaviour of the PLC.
Ladder logic bombs, i.e. malware written in ladder logic can be inserted by an attacker into existing control logic on a PLC, and either persistently change the behaviour, or wait for specific trigger signals to activate malicious behaviour. For example, the LLB could lay dormant until a certain sequence of control actions is performed, or a certain point of time is reached. Then, the LLB could replace legitimate sensor readings that are being reported by the PLC to the ICS with manipulated values.

Building on the Part 1 construct a Logic Bomb like program wherein after an input is activated for a number of times, say 5, all the outputs are activated irrespective of the previous conditions. For this, add a couple more outputs and modify the program as required to implement the logic bomb.
(Hint: You need to make use of the counter module)

VM Instructions

To install the VM:

Download Virtual Box: https://www.virtualbox.org/wiki/Downloads

Download the OVA provided with the assignment.

When open, select 'File', 'Import Appliance', and browse for the OVA provided with the assignment.

Username: student
Password: gatech

Ensure when you run SoMachine Basic you Run as Administrator (right-click on the SoMachine Basic Icon and select 'Run as Administrator')

Deliverables

Ladder Logic Program files for each part. Have separate files for each of the parts and Sub parts and name them accordingly (i.e... Part 1A, Part1B…)

Submission Instructions

Create a zip file with your name <gatechusername.zip/tz>, that includes all your ladder logic files and submit it on T-square.