SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

INFORMATION SYSTEMS TECHNOLOGY AND DESIGN

51.508 – Secure Cyber Physical Systems

Week 2 – PLC Programming

Created by **Jianying Zhou** (2018)

Last updated: 12 Jan 2019

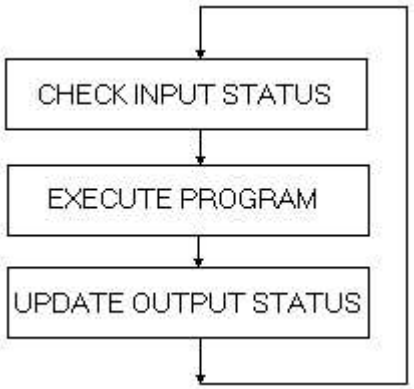
Learning Objectives

- Understand basic programmable logic controller (PLC) languages – ladder diagram (LD) and structured text (ST).
- Able to program and test PLCs.

What is PLC ?

- **PLC = Programmable Logic Controller**, first introduced in 1960's.
- A device that was invented to replace the necessary sequential relay circuits for machine control.
- Look at its inputs and depend upon their state, turn on/off its outputs.
- Continually scan a program.
- **PLCs available in iTrust lab:** Allen-Bradley, National Instruments, Schneider Electric, Siemens.

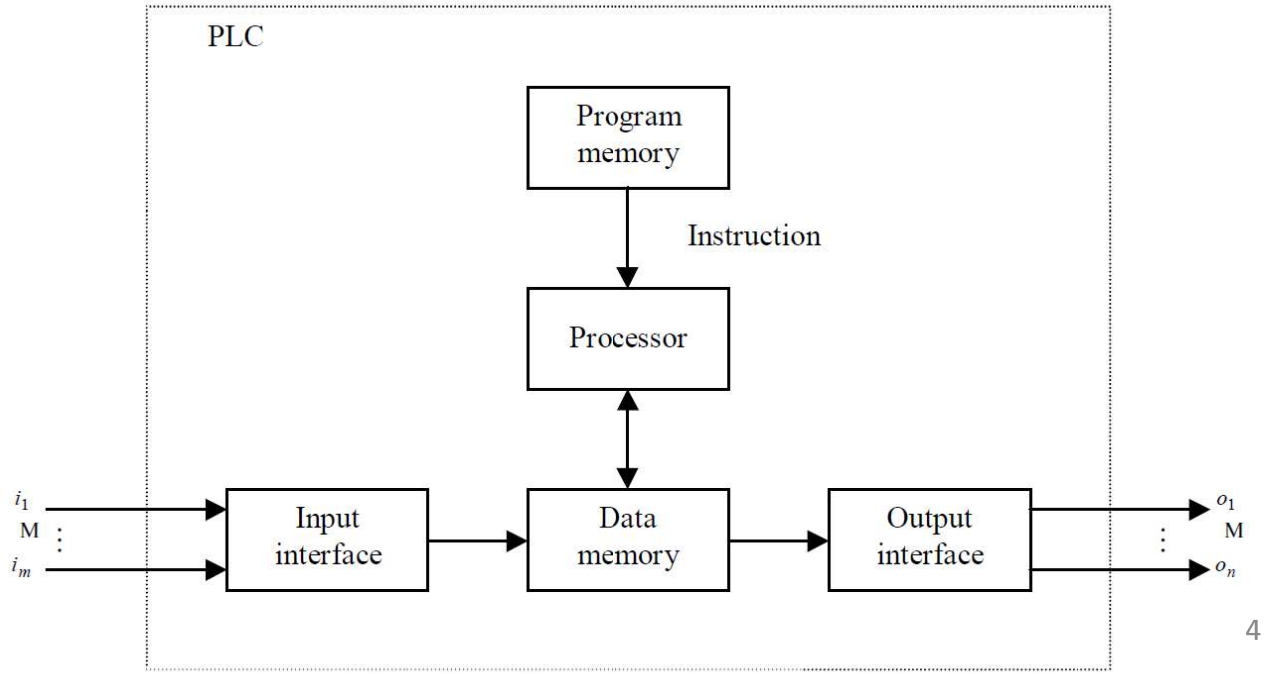
Typical PLCs



Discussion: Give more examples of PLC manufacturers.

PLC Hardware Architecture

- PLC is a miniaturized version of a general-purpose computer.
- Get **input signals** from the system of processes to be controlled, and store in PLC's **data memory**.
- Processor executes instructions from PLC's **program memory**.
- The **output interface** communicates the final result back to the system of processes under the PLC's control.



PLC vs RTU

- **RTU = Remote Terminal Unit**
- The functions of RTUs and PLCs overlap – Performs on-site control and transfers the data to the central SCADA system.
- RTUs are more suitable for wider geographical telemetry, and can withstand harsh conditions, for example, oil and gas pipelines.
- PLCs are more suitable for local control, for example, assembly lines in a factory.

Part 1: PLC Programming Languages

PLC Programming Languages – IEC61131-3

Defined in IEC 61131-3 (1996):

1. **Ladder Diagram (LD)** – graphical, based on Relay Ladder Logic
2. **Structured Text (ST)** – textual, resembling Pascal/C
3. Function Block Diagram (FBD) – graphical, resembling electronic circuit
4. Sequential Function Chart (SFC) – graphical, derived from Petri Nets
5. Instruction List (IL) – textual, resembling assembler

Discussion:

- What PLC languages are you familiar with?
- Why would you prefer those PLC languages?

PLC Programming Languages – LD

- **Ladder Diagram (LD):**
  1. Invented in the U.S. decades ago.
  2. Used in probably 95% of all applications in U.S.
  3. Resembles a series of control circuits, with a series of **inputs** needing to be "made" or "true" in order to activate one or more **outputs**.
- **Pros:**
  1. Easy to start writing a program in Ladder Diagram, especially for a non-programmer with an electrical background.
  2. Allow a program to be organized into folders or subprograms that are downloaded to the PLC, allowing for easy segmentation.
- **Cons:**
  1. Ideal for a simple material handling application (with timers , or some basic comparisons or math), but there are no complex functions involved.
  2. As program size grows, the ladder can become very difficult to read and interpret.

PLC Programming Languages – ST

- **Structured Text (ST):**
  1. A textual programming language that uses **statements** to define what to execute.
  2. Closely resembles a high level computer programming language such as Pascal/C.
  3. Best embraces the growing complexity of PLC programming, such as the process control functions.
  4. Seen the greatest increase in adoption of all the IEC61131-defined programming languages.
- **Pros:**
  1. Decision loops and pointers (variables used to do indirect addressing) allow for a more compact program implementation.
  2. Easy to insert comments throughout a program, and to use indents and line spacing to emphasize related sections of code.
  3. **Runs much faster than Ladder.**
- **Cons:**
  1. Unsuitable for troubleshooting for non-programmer with an electrical background.
- **LD + ST:**
  1. Use Structured Text "behind the scenes".
  2. Encapsulate a Structured Text program inside an instruction called on in Ladder.

PLC Programming Languages – FBD

- **Function Block Diagram (FBD):**
  1. The second most widely used PLC programming language.
  2. A graphical language which resembles a wiring diagram even more so than Ladder code.
  3. The blocks are “wired” together into a sequence that’s easy to follow.
- **Pros:**
  1. Easy to follow – just follow the path!
  2. Ideal for simpler programs consisting of digital inputs and outputs.
- **Cons:**
  1. Not ideal for large programs using special I/O and functions.
  2. The large amount of screen space required by this style of programming can quickly make a program unwieldy.
  3. More difficult to make corrections of the codes later.

PLC Programming Languages – SFC

- **Sequential Function Chart (SFC):**
  1. Resembles the computer flowcharts.
  2. An initial step “action box” is followed by a series of transitions and additional action steps.
  3. Code inside an action box can be written in any language of the programmer’s choice.
- **Pros:**
  1. Ideal for applications which have a repeatable multi-step process or series of repeatable processes.
  2. Very friendly to maintenance engineers for troubleshooting.
- **Cons:**
  1. The structure that is forced on a program could add unneeded complexity.
  2. The overhead required for this type of program causes it to **execute slower than the other languages.**
  3. **The inability to convert to other languages.**

PLC Programming Languages – IL

- **Instruction List (IL):**
  1. Consists of many lines of code, with each line representing exactly one operation.
  2. Very popular in Europe.
- **Pros:**
  1. A program written in this language can be moved easily between hardware platforms.
  2. A low level language and executes much faster in the PLC than a graphical language.
  3. Much more compact and consumes less space in PLC memory.
- **Cons:**
  1. Hard to enter complex functions.
  2. Not in any form of structured programming, limiting its usefulness for implementing large programs.

PLC Programming Languages – comparison

- **Choosing an appropriate language**

Requirement	Choices
Ease of maintenance by the final user	SFC
Universal acceptance of language	LD
Speed of execution by the PLC	ST or IL
Applications mainly using digital I/O and basic processing	LD or FBD
Ease of changing code later	LD
Ease of use by engineers with IT background	ST
Ease of implementing complex mathematical operations	ST
Applications with repeating processes or processes requiring interlocks and concurrent operations	SFC

- **In this course, we choose LD + ST.**

Part 1: PLC Programming Languages

Structured Text

Structured Text – syntax

Syntax

Structured text is a *textual* programming language that uses *statements* to define what to execute.

- Structured text is *not case sensitive*.
- Use *tabs* and *carriage returns* (separate lines) to make your structured text easier to read.

Structured Text – comments

Comments

- Comments let you use *plain language* to describe how structured text works.
- Comments *do not affect the execution* of the structured text.

Format	Example

//comment	**At the beginning of a line**
	`//Check conveyor belt direction`
	`IF conveyor_direction THEN...`
	At the end of a line
	`ELSE //If conveyor isn't moving, set alarm light`
	`light := 1;`
	`END_IF;`

(*comment*)	`Sugar.Inlet[:=]1;(*open the inlet*)`
	`IF Sugar.Low (*low level LS*)& Sugar.High (*high level LS*)THEN...`
	`(*Controls the speed of the recirculation pump. The speed depends on the temperature in the tank.*)`
	`IF tank.temp > 200 THEN...`

/*comment*/	`Sugar.Inlet:=0;/*close the inlet*/`
	`IF bar_code=65 /*A*/ THEN...`
	`/*Gets the number of elements in the Inventory array and stores the value in the Inventory_Items tag*/`
	`SIZE(Inventory,0,Inventory_Items);`

Structured Text – assignments

Assignments

- Use an assignment to change the value stored within a tag.
- Syntax: **tag := expression;**
- The ***tag*** retains the assigned value until another assignment changes the value.
- The ***expression*** can be simple, such as an immediate value or another tag name, or can be complex and includes several operators and functions.

Structured Text – expressions

Expressions

- An expression can be a tag name, equation, or comparison:
  - Tag name that stores the value (variable)
  - Number that you enter directly into the expression (immediate value)
  - String literal that you enter directly into the expression
  - Functions, such as: ABS, TRUNC
  - Operators, such as: +, -, <, >, And, Or

- When writing expressions, follow these **general rules**:
  - Use any combination of upper-case and lower-case letter. For example, these three variations of "AND" are acceptable: AND, And, and.
  - For more complex requirements, use parentheses to group expressions within expressions. This makes the whole expression easier to read and ensures that the expression executes in the desired sequence.

Structured Text – expressions

Expressions

- **BOOL expression:** Produces either the BOOL value of 1 (true) or 0 (false).
  - A bool expression uses bool tags, relational operators, and logical operators to compare values or check if conditions are true or false. For example, tag1 > 65.
  - A simple bool expression can be a single BOOL tag.
  - Typically, you use bool expressions to condition the execution of other logic.

- **Numeric expression:** Calculates an integer or floating-point value.
  - A numeric expression uses arithmetic operators, arithmetic functions, and bitwise operators. For example, tag1 + 5.
  - May nest a numeric expression within a BOOL expression. For example, (tag1 + 5) > 65.

- **String expression:** Represents a string
  - A simple expression can be a string literal or a string tag.

Structured Text – operators & functions

Operators and Functions

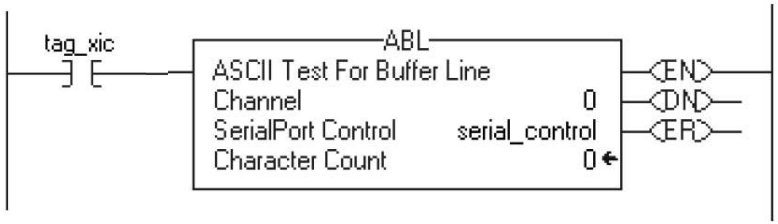
- Operators calculate new values:
  - Arithmetic operators: **+**, **-**, *, ** (exponent), **/**, **MOD**
  - Relational operators: **=**, **<** , **<=**, **>**, **>=**, **<>**
  - Logical operators, yielding a Boolean value of TRUE or FALSE: **AND**, **OR**, **XOR**, **NOT**
  - Bitwise operators, for each bit of two numbers: **AND**, **OR**, **XOR**, **NOT**

- Functions perform math operations: **LOG**, **SQRT**, …

Structured Text – instructions

Instructions

- In structured text, instructions will execute each time they are scanned unless you pre-condition the execution of the structured text instruction.
- This differs from relay ladder instructions that use rung-condition-in to trigger execution.



Case 1: The ABL instruction will execute every scan if tag_xic is set, not just when tag_xic transitions from cleared to set.

```
IF tag_xic THEN ABL(0,serial_control);
END_IF;
```

Case 2: If you want the ABL instruction to execute only when tag_xic transitions from cleared to set, you have to condition the structured text instruction. **Use one-shot rising with input (OSRI) to trigger execution.**

```
osri_1.InputBit := tag_xic;
OSRI(osri_1);
IF (osri_1.OutputBit) THEN
ABL(0,serial_control);
END_IF;
```

Structured Text – constructs

Constructs

If you want to	Use this construct
Do something if or when specific conditions occur	IF. . . THEN
Select what to do based on a numerical value	CASE. . . OF
Do something a specific number of times before doing anything else	FOR. . . DO
Keep doing something as long as certain conditions are true	WHILE. . . DO
Keep doing something until a condition is true	REPEAT. . . UNTIL

Structured Text – construct (IF…THEN)

Construct:

IF…THEN: to do something if or when specific conditions occur.

```
IF bool_expression1 THEN
   <statement>;
    .
    .
ELSEIF bool_expression2 THEN
 <statement>;
    .
    .
ELSE
 <statement>;
    .
    .
END_IF;
```

optional

optional

Statements to execute when *bool_expression1* is true.

Statements to execute when *bool_expression2* is true.

Statements to execute when both expressions are false.

If you want this	Enter this structured text
If conveyor direction contact = forward (1) then	IF conveyor_direction THEN
light = off	light := 0;
Otherwise light = on	ELSE
	light [:=] 1;
	END_IF;

Structured Text – construct (CASE…OF)

Construct:

CASE…OF: to select what to do based on a numerical value.

- Executes only the statements that are associated with **the first matching selector value**.
- Execution always breaks after the statements of that selector and goes to the END_CASE statement.

```
CASE numeric_expression OF
    selector1: <statement>;
    .
    .
   selector2: <statement>;
    .
    .
ELSE
                <statement>;
    .
    .
END_CASE;
```

optional

Specify as many alternative selector values as you need.

If you want this	Enter this structured text
If recipe number = 1 then Ingredient A outlet 1 = open (1) Ingredient B outlet 4 = open (1)	CASE recipe_number OF
	1: Ingredient_A.Outlet_1 :=1; Ingredient_B.Outlet_4 :=1;
If recipe number = 2 or 3 then Ingredient A outlet 4 = open (1) Ingredient B outlet 2 = open (1)	2,3: Ingredient_A.Outlet_4 :=1; Ingredient_B.Outlet_2 :=1;

Structured Text – construct (FOR…DO)

Construct:

FOR…DO: to do something a specific number of times before doing anything else.

optional

```
FOR count := initial value
    TO final_value
    BY increment
    DO
        <statement>;
          .
          .
END_FOR;
```

If you don't specify an increment, the loop increments by 1.

If you want this	Enter this structured text

Clear bits 0…31 in an array of BOOLs:
Initialize the subscript tag to 0.
Clear i . For example, when subscript = 5, clear array[5].
Add 1 to subscript.
If subscript is ≤ to 31, repeat 2 and 3.
Otherwise, stop.
	For subscript:=0 to 31 by 1 do
	array[subscript] := 0;
	End_for;

Structured Text – construct (WHILE…DO)

Construct:

WHILE…DO: to keep doing something as long as certain conditions are true.

```
WHILE bool_expression DO
   <statement>;
    .
    .
END_WHILE;
```

Statements to execute while *bool_expression* is true.

If you want this	Enter this structured text	
The WHILE…DO loop evaluates its conditions first. If the conditions are true, the controller then executes the statements within the loop. This differs from the REPEAT…UNTIL loop because the REPEAT…UNTIL loop executes the statements in the construct and then determines if the conditions are true before executing the statements again. The statements in a REPEAT…UNTIL loop are always executed at least once. The statements in a WHILE…DO loop might never be executed.	pos := 0;	
	While ((pos <= 100) & structarray[pos].value <> targetvalue)) do	
		pos := pos + 2;
		String_tag.DATA[pos] := SINT_array[pos];
	end_while;	

Structured Text – construct (REPEAT…UNTIL)

Construct:

REPEAT…UNTIL: to keep doing something until conditions are true.

```
REPEAT
   <statement>;
    .
    .
UNTIL bool_expression
END_REPEAT;
```

Statements to execute while *bool_expression* is false.

If you want this	Enter this structured text

The REPEAT…UNTIL loop executes the statements in the construct and then determines if the conditions are true before executing the statements again. This differs from the WHILE…DO loop because the WHILE…DO The WHILE…DO loop evaluates its conditions first.
If the conditions are true, the controller then executes the statements within the loop. The statements in a REPEAT…UNTIL loop are always executed at least once. The statements in a WHILE…DO loop might never be executed.
	pos := -1;
	REPEAT
	pos := pos + 2;
	UNTIL ((pos = 101) OR (structarray[pos].value = targetvalue))
	end_repeat;

Structured Text – exercise

Constructs:

- Give the example codes using the construct of **CASE…OF**.
- Rewrite using the construct of **IF…THEN** which has the same effect.
- Explain the difference between **CASE…OF** and **IF…THEN**.

Structured Text – exercise

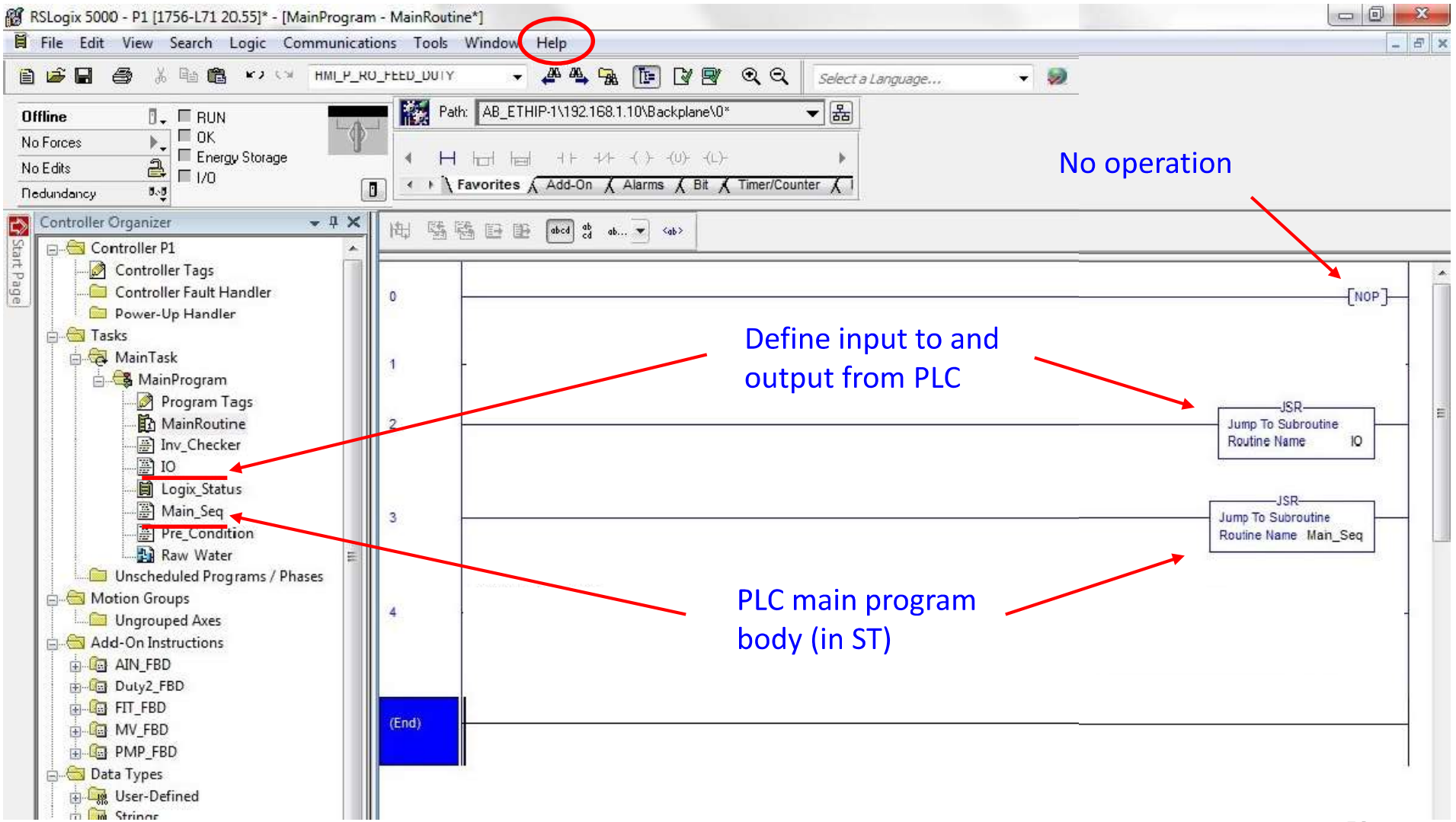
```
FUNCTION Ave_REAL : REAL
        VAR_INPUT
                Input1, Input2 : REAL;
        END_VAR
        Ave_REAL := (Input1 + Input2) / 2;
END_FUNCTION

Average1 := Ave_REAL(4.0, 6.0);
Average2 := Ave_REAL(Input2 := 6.0);
```

What are the values of Average1 and Average2?

Average1 = 5.0

Average2 = 3.0 (default value of Input1 = 0)

PLC Programming – example (LD + ST)



Summary – Part 1

1. Introduction of basic PLC programing languages, especially about ladder diagram (LD) and structured text (ST).
2. You are expected to be able to use LD and ST to program PLCs.

3. Will continue the topic on PLC programming in the next session (Security Tools Lab), using iTrust PLC training skid.
   - **Time:** Tue, 12 Feb (Group 1-5); Fri,15 Feb (Group 6-10)
   - **Venue:** iTrust lab @ Building 2, Level 7
   - Please bring your own laptop.

4. Week 3: Modeling CPS (Aditya)
   - **Time:** Tue, 19 Feb

Reading Materials – Part 1

1. Ted Thayer. “Understanding the IEC 61131-3 Programming Languages”. Control Engineering, 2009.
2. PLC Programming & Automation Online. “Ladder Logic Examples and PLC Programming Examples” – http://www.plcacademy.com/ladder-logic-examples/
3. Info PLC. “Structured Text Programming” – http://www.infoplc.net/files/descargas/rockwell/infoplc_net_plc_st.pdf

Part 2: PLC Training Skids & Lab Exercise

PLC Training Skids in iTrust Lab

Four different types of PLC training skids are available in iTrust Lab:

1. **Allen-Bradley – Rockwell Automation**
2. National Instruments
3. Schneider Electric
4. Siemens

PLC Training Skid – NI

- **NI cRIO-9063**, an embedded real-time controller with reconfigurable FPGA
- Runs on NI Linux Real-Time OS
- Remote digital/analogue I/Os
- A secure router and wireless client
- Milliamp meter, potentiometer, key switches, light push buttons, ultra mini photo sensor

PLC Training Skid – Schneider

- **Modicon Quantum CPU**, a special-purpose computing system with digital processing capabilities
- Remote digital/analogue I/Os
- A secure router and wireless client
- Milliamp meter, potentiometer, key switches, light push buttons, ultra mini photo sensor

PLC Training Skid – Siemens

- **SIMATIC S7-1500 controller**, compatible with Siemens Step 7 and TIA software
- Remote digital/analogue I/Os
- A secure router and wireless client
- Milliamp meter, potentiometer, key switches, light push buttons, ultra mini photo sensor

PLC Training Skid – Allen Bradley

PLC Training Skid – AB (HW & SW)

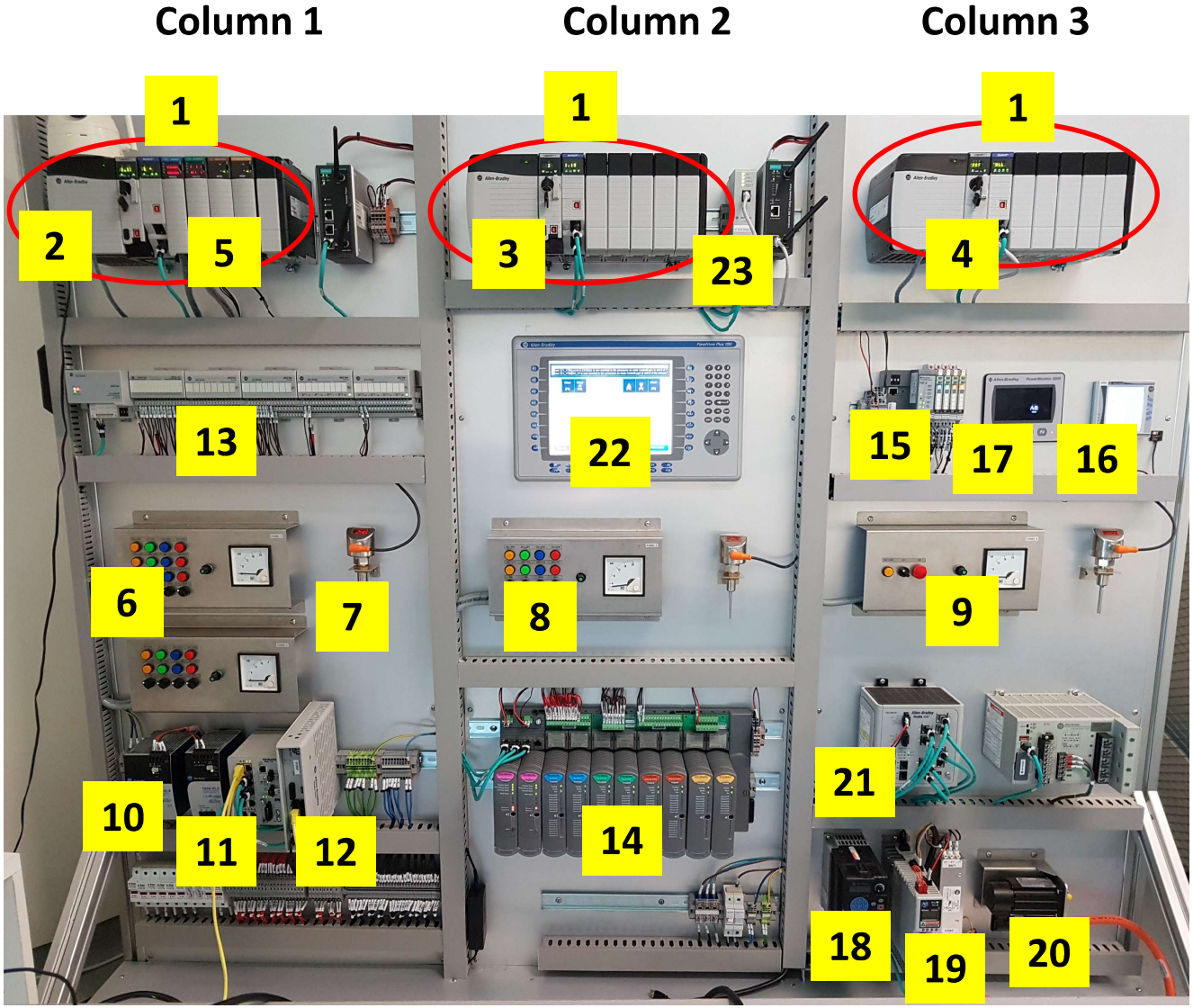
Hardware (3 separate columns of Allen Bradley PLCs)

- AC power supply
- CPU, communication processor with digital & analogue I/Os
- A set of control instruments – temperature probe, analogue ammeter, potentiometer and illuminated push buttons.

Software

- Studio 5000

PLC Training Skid – AB (components)



1. PLC setup rack
2. AC power unit
3. CPU
4. Communication processor
5. Analog and digital I/O
6. Illuminated push buttons
7. Temperature probe
8. Potentiometer
9. Analog ammeter
10. Power supply
11. Ethernet switch
12. Service router
13. Flex I/O
14. Redundant I/O
15. Point I/O
16. Power meter
17. Power quality meter
18. Variable speed drive
19. Servo drive
20. Servo motor
21. 10 ports switch
22. Panel view plus terminal
23. Wireless access point

PLC Training Skid – AB (components)

1. **PLC setup rack** = A layout of PLC with Power supply, CPU, communication processor and optional I/O module.
2. **AC power unit** = Power up PLC with required direct current.
3. **CPU** = Central processing unit, which carries out instructions with the program setup.
4. **Communication processor** = A small sized computers for interfacing with networks (connecting to remote I/O: No. 13, 14, 15).
5. **Analog and digital I/O** = Input to and output from PLC.
6. **Illuminated push buttons** (DI/DO)
7. **Temperature probes** (AI) = Temperature measuring device.
8. **Potentiometer** (AI) = A resistive instrument to increase or decrease resistivity.
9. **Analog ammeter** (AO) = A meter showing the readings of the measure current.
10. **Power supply** = Power supply to instruments which converts AC to DC.
11. **Ethernet switch** = Network access
12. **Service router** = Connects PLCs
13. **Flex I/O** (remote) = Offers flexibility for applications with digital, analog and specialty I/O.

PLC Training Skid – AB (components)

14. **Redundant I/O** (remote) = Has fault tolerance and redundancy for critical process applications.
15. **Point I/O** (remote) = For applications requiring flexibility and low cost of ownership.
16. **Power meter** = An instrument that measures the power through the lines.
17. **Power quality meter** = An instrument that measure the power quality by analyzing the sag, dip, swell, interruptions and impulses in a power system.
18. **Variable speed drive** = A type of adjustable-speed drive used in electro-mechanical drive systems to control AC motor speed and torque by varying motor input frequency and voltage.
19. **Kinetic 5500 servo drive** = A drive that controls servo and induction motors via a single cable. Optimization of power and energy.
20. **Servo motor**
21. **10 ports switch** = A hub that receives, processes data to destination device.
22. **Panel view plus terminal** = Human Machine Interface visually through touch screen.
23. **Wireless access point** = Converts hard-wired access to wireless (providing wireless connection between PLCs, or with remote I/O).