SCADA Network Topologies

Tarun Sharma[1, a], Chetan Bis t[2,b] Moon Verma[3c]

[1]Department of CE,JNU, Jodhpur

[2]Department of EC, RTU,Kota

[3]University College of Engg Kota
Rajasthan

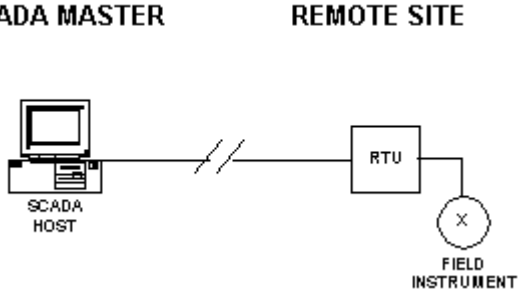
[a]tarun.sharma@bapugkv.ac.in, [b]chetan_bist@yahoo.in

Abstract. Automation (ancient Greek: = *self dictated*), **roboticization** or industrial automation or numerical control is the use of control systems such as computers to control industrial machinery and processes, reducing the need for human intervention. In the scope of industrialization, automation is a step beyond mechanization. Whereas *mechanization* provided human operators with machinery to assist them with the *physical* requirements of work, *automation* greatly reduces the need for human *sensory* and *mental* requirements as well. Processes and systems can also be automated

Introduction

SCADA is the acronym for *Supervisory Control And Data Acquisition*. In Europe, SCADA refers to a large-scale, distributed measurement and control system, while in the rest of the world SCADA may describe systems of any size or geographical distribution. SCADA systems are typically used to perform data collection and control at the supervisory level. Some systems are called SCADA despite only performing data acquisition and not control.

- The supervisory control system is a system that is placed on top of a real-time control system to control a process that is external to the SCADA system (i.e. a computer, by itself, is not a SCADA system even though it controls its own power consumption and cooling). This implies that the system is not critical to control the process in real time, as there is a separate or integrated real-time automated control system that can respond quickly enough to compensate for process changes within the time constants of the process. The process can be industrial, infrastructure or facility based as described below: Industrial processes include those of manufacturing, production, power generation, fabrication, and refining, and may run in continuous, batch, repetitive, or discrete modes.
- Infrastructure processes may be public or private, and include water treatment and distribution, wastewater collection and treatment, oil and gas pipelines, electrical power transmission and distribution, and large communication systems.

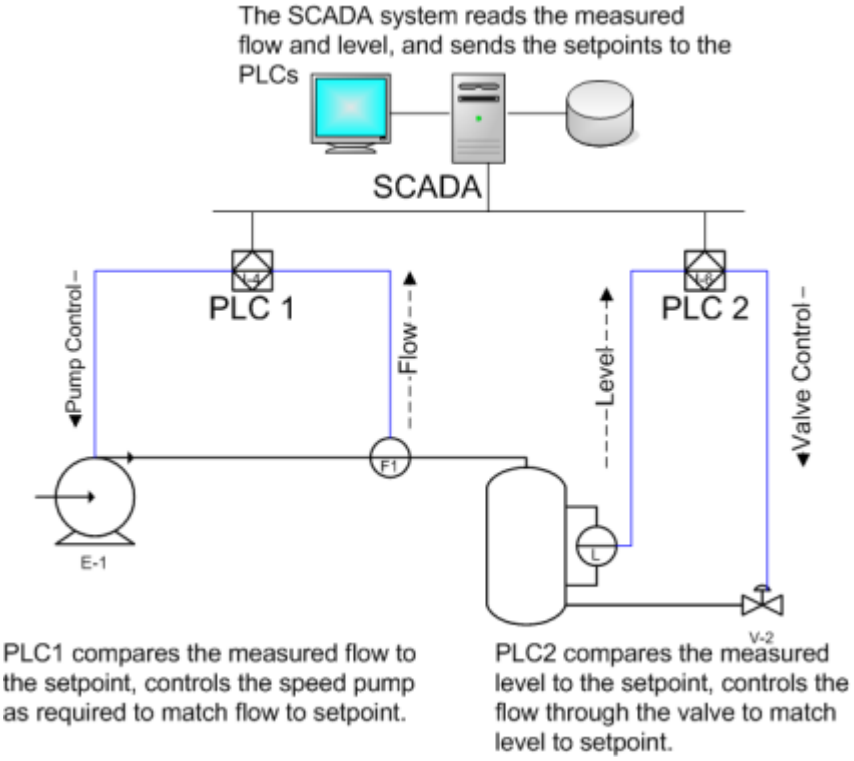


Facility processes occur both in public facilities and private ones, including buildings, airports, ships, and space stations. They monitor and control HVAC, access, and energy consumption.

Data acquisition begins at the RTU or PLC level and includes meter readings and equipment status

reports that are communicated to SCADA as required. Data is then compiled and formatted in such a way that a control room operator using the HMI can make supervisory decisions to adjust or override normal RTU (PLC) controls. Data may also be fed to a Historian, often built on a commodity Database Management System, to allow trending and other analytical auditing.

SCADA systems typically implement a distributed database, commonly referred to as a *tag database*, which contains data elements called *tags* or *points*. A point represents a single input or output value monitored or controlled by the system. Points can be either "hard" or "soft".



Fieldbus

A field bus or field bus is an industrial computer network for real-time distributed control.

A complex automated industrial system — say a manufacturing assembly line — usually needs an organized hierarchy of controller systems to function. In this hierarchy there is usually a Human Machine Interface (HMI) at the top, where an operator can monitor or operate the system. This is typically linked to a middle layer of programmable logic controllers (PLC) via a non time critical communications system (e.g. Ethernet).

The US-based Fieldbus Foundation defines fieldbus as:

"...an all-digital, serial, two-way communication system that interconnects measurement and control equipment such as sensors, actuators and controllers. At the base level in the hierarchy of plant networks, it serves as a Local Area Network (LAN) for instruments used in process control and manufacturing automation applications and has a built-in capability to distribute the control application across the network. Furthermore, a Fieldbus must be an open system that is supported by several vendors, and not tied to a single technology."

Simulation

A simulation is an imitation of some real thing, state of affairs, or process. The act of simulating something generally entails representing certain key characteristics or behaviors of a selected physical or abstract system.

Interactive simulation is a special kind of physical simulation, often referred to as a *human in the loop* simulation, in which physical simulations include human operators, such as in a flight simulator or a driving simulator.Human in the loop simulations can include a computer simulation as a so-called *synthetic environment.*

Potential benefits of SCADA :

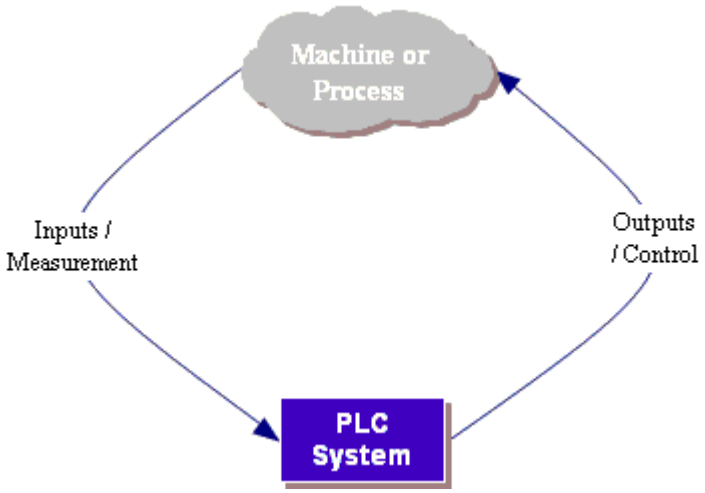
The benefits one can expect from adopting a SCADA system for the control of Experimental physics facilities can be summarized as follows:

- A rich functionality and extensive development facilities. The amount of effort invested in SCADA product amounts to 50 to 100 p-years.
- The amount of specific development that needs to be performed by the end-user is limited, especially with suitable engineering.
- Reliability and robustness. These systems are used for mission critical industrial processes where reliability and performance are paramount. In addition, specific development is performed within a well-established framework that enhances reliability and robustness.
- Technical support and maintenance by the vendor.

For large collaborations, as for the CERN LHC experiments, using a SCADA system for their controls ensures a common framework not only for the development of the specific applications but also for operating the detectors. Operators experience the same "look and feel" whatever part of the experiment they control. However, this aspect also depends to a significant extent on proper engineering.

Programmable Logic Controller :

A programmable controller is a digitally operating electronic apparatus which uses a programmable memory for the internal storage of instructions for implementing specific functions, such as logic, sequencing, timing, counting and arithmetic, to control through digital or analog input/output, various types of machines or process. Programmable Logic Controllers, programmable controllers, or PLCs are specialized industrial computers.



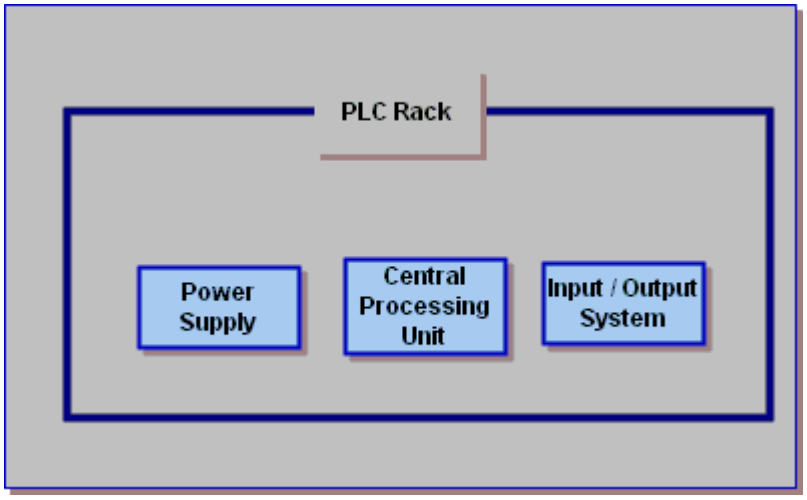
The PLC accepts inputs from switches and sensors (measures or senses the system), evaluates these based on a program (logic), and changes the state of outputs to control a machine or process.

Initially, programmable logic controllers were used to replace traditional hard-wired relay logic; however, with its ever increasing functionality it is found in many more complex applications. PLCs are used in any industrial application where operating requirements are complex, are constantly changing, or where high reliability is necessary.

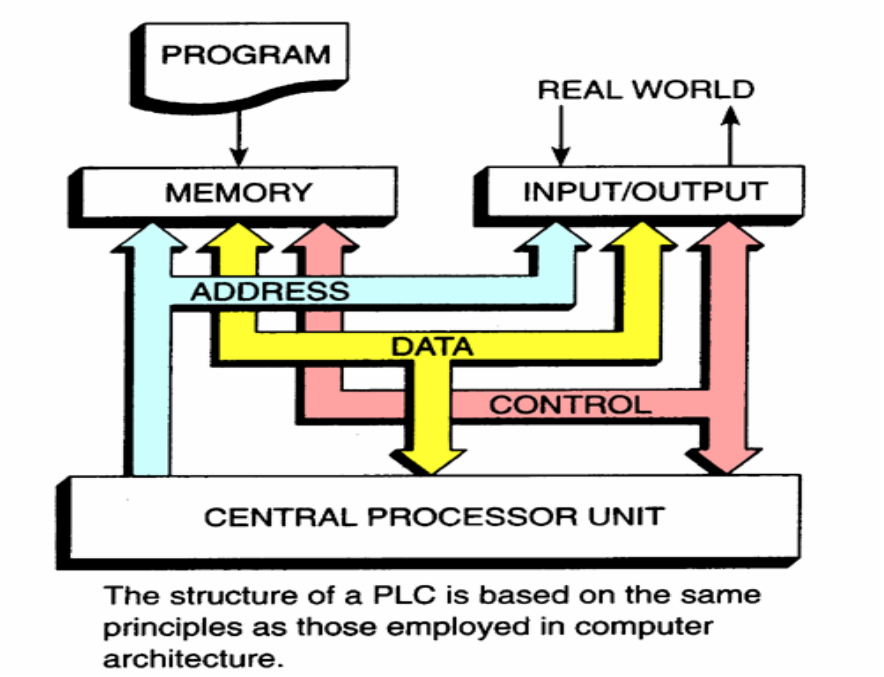
Programmable controllers have grown throughout industrial control applications because of the ease they bring to creating a controller: ease of programming, ease of wiring, ease of installation, and ease of changing. PLCs span a wide range of sizes, but all contain six basic components:

- processor or central processing unit (CPU);
- rack or mounting;

- input assembly;
- output assembly;
- power supply;



PLC Architecture :



The structure of a PLC is based on the same principles as those employed in computer architecture.

For the PLC to be useful, it must first have a Program or Logic for the CPU to execute. A system engineer or PLC programmer will first create the program logic in a programming device (these days it is usually software running on a personal computer). This logic can be written in Ladder Logic, Instruction List, Sequential Function Charts, or any of the IEC languages.

References

[1] http://en.wikipedia.org/wiki/SCADA

[2] E. Byres, Understanding Vulnerabilities in SCADA and Control Systems, October 2004

[3] http://www.modbus.org/specs.php

[4] http://www.modbus.org/docs/Modbus_Application_ Protocol_V1_1b.pdf

[5] http://www.obvius.com/pdfs/TN27-ModbusRS485QandA.pdf

[6] http://en.wikipedia.org/wiki/Modbus

[7] http://www.Modbus-IDA.org October 2006

[8] http://en.wikipedia.org/wiki/Man-in-the-middle_attack

[9] http://www.modbus.org/docs/ MODBUS_Messaging_ Implementation_Guide_V1_0b.pdf

[10] R. Carlson. Sandia SCADA program high-security SCADA L – DRD final report. Sandia National Laboratories report, SAND2002-0729; April 2002.

[11] J. Pollet. Developing a solid SCADA security strategy. In: Second ISA/IEEE sensors for industry conference, 19 21 November 2002. p. 148 56.