# Three-Layer PLC/SCADA System Architecture in Process Automation and Data Monitoring

Mohamed Endi
Electrical Engineering Branch, MTC, Cairo, Egypt foldzen@yahoo.com

Y. Z. Elhalwagy
College of Engineering &Technology, Arab Academy for Science & Technology
foldzen@yahoo.com

Attalla hashad
Maritime Transport, Cairo, Egypt
foldzen@yahoo.com

***Abstract*—This paper presents the State-of-the-Art and recent trends of SCADA system Architecture, which is usually three-layer SCADA system architecture depending on open system technology rather than a vendor controlled, proprietary technology.A Real-time Industrial process is simulated (boiling system), and a complete three-layer model SCADA system is developed for this process, supervision control layer, Process control layer, and field instrument layer. National Instruments, Labview with the associated data logging and supervisory control toolset (DSC) is used to develop the SCADA/HMI in supervision layer. Industrial programmable logic controllers (PLCs) from SIEMENS (S7-CPU222 and EM231) and related software package are used to build up process control layer. Finally simulation unit is designed and developed to be used as field instrument layer. OPC service protocol (open standards protocol) is used to solve compatibility problem raised from different vendors' tools.**

***Keywords- SCADA; DCS; RTU; LabView; SCADA architecture; Multilayer SCADA Network.***

## I. INTRODUCTION

Traditional industrial automation supposes the operator responsibility on monitoring and controlling of processes in real time. As complexity of industrial processes increases, the need for remote controlling and monitoring from a central location increases also. This will make the operator function (monitor and control) easier and proficiently. Furthermore, aggregation of feedback data, which gives supervisors and management personnel the ability to monitor trends, forecast requirements, and optimizes procedures. A common term used to describing this solution is A SCADA system. [1]

A SCADA "supervisory control and data acquisition" is the generic terms for the hardware, software, and procedures used to control and monitor industrial process.

SCADA systems are widely used in most industrial processes: e.g. steel making, and power generation (conventional and nuclear). It can provide information in a real-time environment that identifies problems as they occur and can take corrective action when assistance is needed. Proper monitoring of process can maintain operations at an optimal level by identifying and correcting problems before they turn into significant system failures.

SCADA systems have made substantial progress over the recent years in terms of functionality, scalability, and performance. This paper describes recent trends of SCADA system architecture as shown in section II. The OPC service protocol is utilized while communication among the multi-layer SCADA architecture is highlighted in section III. Section IV presents a prototype for the designed and implemented based on the three-layer SCADA architectural. The paper terminates with the drawn conclusions.

## II. THREE-LAYER SCADA SYSTEM ARCHITECTURE

SCADA systems have evolved in parallel with the growth and sophistication of modern computing technology. Its architecture has been improved depending on technology revolutions. The latest trend of SCADA system is the three-layer SCADA architecture which depending on open system technology rather than a vendor controlled proprietary environment.

There are various vendors for PLCs, industrial networks, SCADA systems and HMIs which need to communicate with each other. Therefore, the open system architecture is suitable for this situation.

There are also still RTUs (process control layer\remote terminal unit) utilizing protocols that are vendor-proprietary. But the major improvement in the last generation is that of opening the system architecture, utilizing open standards and protocols, which eliminate a number of the limitations of previous generations of SCADA systems.

Figure 1 bellow illustrates the three-layer SCADA system architecture [1-3].

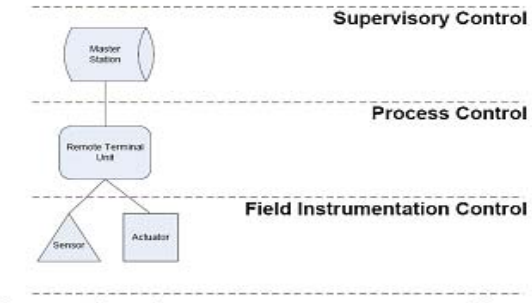



Figure 1. The 3-layer SCADA system architecture.

978-1-4244-5586-7/10/$26.00 © 2010 IEEE

*A. Supervisory control layer (Master Station)*

Master stations have two main functions:

*1)* Periodically obtain data from RTUs/PLCs (and other master or sub-master stations).

*2)* Control remote devices through the operator station.

Master stations consist of one or more personal computers (PC), which, although they can function in a multi-purpose mode (email, word processing, etc), are configured to be dedicated to master station duties. These duties include trending, alarm handling, logging and archiving, report generation, and facilitation of automation. These duties may be distributed across multiple PCs, either standalone or networked.

*B. Process control layer (Remote Terminal Units (RTUs))*

This layer usually consists of more than one device depending on the situation, these devices like:

*1)* Programmable Logic Controllers: The modern RTUs typically use a ladder-logic approach to programming due to its similarity to standard electrical circuits. A RTU that employs this ladder logic programming is called a Programmable Logic Controller (PLC). PLCs are quickly becoming the standard in control systems. The PLC is special purpose computer contains CPU and different kinds of memory. Advances in CPUs and the programming capabilities of RTUs have allowed for more sophisticated monitoring and control. Applications that had previously been programmed at the central master station can now be programmed at the RTU.

*2)* Analog Input and Output Modules: The configuration of sensors and actuators determines the quantity and type of inputs and outputs on a PLC or RTU. Depending on the model and manufacturer, modules can be designed solely for input, output, digital, analog, or any combination.

An analog input module has a number of interfaces. Typical analog input modules have 4, 8, 16, or 32 inputs. Analog output modules take digital values from the CPU and convert them to analog representations, which are then sent to the actuators. An output module usually has 4, 8, 16 or 32 outputs, and typically offers 8 or 12 bits of resolution.

*3)* Digital Input and Output Modules: Digital input modules typically are used to indicate status and alarm signals. A specialized digital input module is used for counting pulses of voltage or current, rather than for strictly indicating "open" or "closed." This functionality, however, can also be implemented using standard input modules and functions found in the ladder-logic programming language of the PLC.

*C. Field instrument control layer (Sensors and Actuators)*

This layer mainly consists of sensors and actuators. The Sensors perform measurement and actuators perform control. Sensors get the data (supervision and data acquisition) and actuators perform actions dependent on this data (control). The processing and determination of what action to take, is done by the master control system (i.e. SCADA).

## III. COMMUNICATION AMONG THREE-LAYER SCADA SYSTEM ARCHITECTURE

Each PLC vendor created their own fieldbus standard, which quickly became a problem since it is necessary for PLC from different vendors to communicate. During the 80s consent on some fieldbus standards emerged, so today most vendor equipped them RTU with a standard communication interface to get more market share [3]. Figure 2 illustrates the typical means of communications between SCADA components.

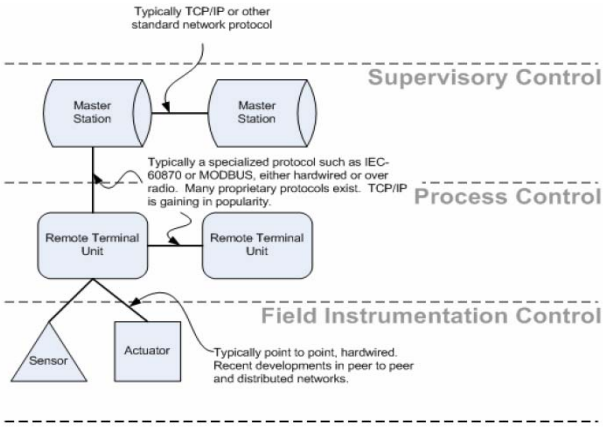



Figure 2. The typical means of communications between SCADA components.

*A. Communications among Supervisory Control Peers*

At the Supervisory Control layer between peers, communications are usually through a standard networking protocol such as TCP/IP or IPX over Ethernet or Token Ring. The SCADA applications involved in the communications are typically installed on standard PC systems capable of using standard operating-system provided protocols.

Options exist for employing proprietary protocols between peers from the same manufacturer or SCADA-specific, open source protocols between peers of dissimilar manufacturers.

*B. Communications between Supervisory Control and Process Control and Among Process Control Peers*

The means of communications between supervisory control and process Control, as well as among process control peers, vary greatly and are usually dependent on hardware manufacturer. If a suite of RTUs, sensors and actuators is purchased from a single vendor, the protocol may be proprietary. Recent trends indicate a move to the option of using open source protocols like, Modbus, profibus, and UCA “Utility Communications Architecture”, in order to incorporate a variety of manufacturer's equipment.

*C. Communications between Process Control and Field Instrumentation Control*

As communications between process control (RTU) and field instrumentation control is typically a point to point

running over wire pairs, transmitting voltage pulses or current level (4-20mA) that are interpreted by the RTU based on how it is programmed. Recent trends in "intelligent" sensors and actuators provide more capabilities, and allow for peer to peer or distributed networks among sensors and actuators; protocols in intelligent sensors used today are Foundation Fieldbus, and profibus-AS.

*D. Software communication tool (OLE for Process Control (OPC))*

As there are numerous vendors of automation equipment which all use their own protocols to communicate with, in addition to the large variety of network interfaces, it is difficult to carry out software which can be used for all variations. To make it easier for software developers to communicate with this large variety of automation equipment, a standard communication interface was needed. With a standard communication interface the software developer can create programs which are hardware independent. Independence is always good as it simplifies upgrades, as not all components have to be updated at once, with a standard communication interface.

To be able to create a standard and implement it quickly, the industry decided to use Microsoft's Component Object Model (COM) and Distributed COM (DCOM) as the basis for the communication interface. The communication interface was named OLE for Process Control (OPC). COM is used to communicate between processes on one computer, whilst DCOM is used to communicate between processes on different computers. So OPC works as a server/client solution, where the user creates clients which ask for data from the server. The server can be on the same computer as the client (COM), or on another computer (DCOM). The server then handles all communication with the automation equipment. The main benefit of the server/client model is that one server can support several clients.

Today OPC is often the interface of choice for HMI and SCADA systems [3].

## IV. Design and development of three-layer SCADA prototype

A prototype has been implemented based on the three-layer SCADA architectural. This prototype helps visualize real-time process data, and enables to configure and monitor process status (data input/output), and information archives, remotely from master station. The testing of the prototype in a laboratory setting showed satisfactory performance as it was expected from the design.

*A. Industrial process (boiling system) function description*

This system is used usually in food industrial. Which responsible to pasteurizing some liquid like milk, to be used in the food manufacture process, and its operation pass through the following steps:

*1)* Filling the tank to certain level.

*2)* Starting the heater and continue hitting until retches desired temperature Degree.

*3)* Keeping the liquid at that temperature Degree or little above to certain desired time.

*4)* After the certain time passed, Stopping the heater. And the liquid is ready to use by reaming industrial process stages.

The goal is to design and devolve three-layer SCADA systems to monitoring and controls this process.

*B. Field instrument control layer (Sensors and Actuators) designed and development*

Because of the industrial process itself, not our issue, a simulator box is designed and developed to simulate this process status, pump, valve, tank level, and temperature degree, etc. Table I and II below show the I/O status of the process. In Fig. 3 simulation unit is depicted. From table I and II, the RTU must be containing at least 8 digital inputs, 6 digital outputs, and 2 analog inputs.

TABLE I. NDUSTRIAL PROCESS STATUS

| N | Status discretion | simulated on Simulator unit | RTU connection |
|---|---|---|---|
| 1 | Op. mode A\M | ON\OFF switch | Digital-I |
| 1 | Process on indicator | Orange LAMP | Digital-O |
| 2 | Normal Process end indicator | Green LAMP | Digital-O |
| 3 | PUMP On/Off | Green LAMP | Digital-O |
| 4 | Heater On-Off | Green LAMP | Digital-O |
| 5 | Valve out On-Off | Green LAMP | Digital-O |
| 6 | Alarm indicator | Red LAMP | Digital-O |
| 7 | Start button | Green Push button | Digital-I |
| 8 | Stop Emerg. button | Red Push button | Digital-I |
| 9 | Level sensor | Potentiometer-resistance 500Kohm | Analog-I |
| 10 | Temperature sensor | Potentiometer-resistance 50Kohm | Analog-I |

TABLE II. HARDWARE FAILURE SIMULATION:

| N | Hardware failure (HF) | simulated on Simulator unit by | RTU connection |
|---|---|---|---|
| 1 | Filling PUMP (HF) | Red Push button (Normal open) | Digital input |

| | | | |
|---|---|---|---|
| 2 | Valve out (HF) | Red Push button (Normal open) | Digital input |
| 3 | Heater (HF) | Red Push button (Normal open) | Digital input |

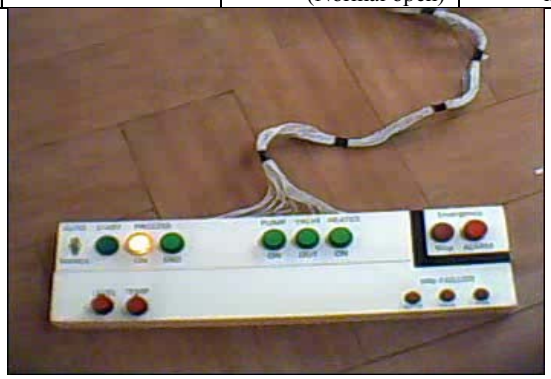


Figure 3. Final simulation unit.

### *C. Process control layer (RTU) designed and development*

The main part used in RTU is the programmable logic controller (PLC). Therefore, the design of RTU began with the selection of The PLC unit depending on I\O signals of field instrument control layer. After evaluating various manufacturers and models, the SIEMENS manufacturer brand is selected as reason of know and trusted brand name and also because of prevalence use in Egypt. After careful consideration of the industrial process (boiling system) needs, the CPU222 (8DI/6DO) series S7200 PLC is selected with extension model EM231 (4 analog inputs). This selection gives the designer 8 digital inputs, 6 digital output, and 4 Analog inputs which are sufficient for this industrial process. The AC power supply version is selected to avoid need to extra DC power supply.

A personal computer (PC), with Micro/WIN32 software was used as a programming device with the selected PLC and EM, standard language (Ladder Logic Diagram) is used to develop a source code which implements the industrial process (boiling system) function description described previously.

The PLC is connected to computer by using a USB/PPI Multi-master cable. The whole developed RTU and associated components is depicted in Fig. 4 and listed in Table III and IV.

TABLE III. RTU COMPONENTS

| N | Item | Model | Description |
|---|---|---|---|
| 1 | PLC | CPU Siemens STEP7-222 | See table 4 |
| 2 | Extension module | EM231 | 4 analog inputs |
| 3 | Programming Cable | Multi-Master PPI | PPI\USP |

TABLE IV. TABLE IVPLC SPECIFICATION [13]

| N | Features | Description |
|---|---|---|
| 1 | Model | CPU222 DC\AC\Relay |
| 2 | Physical size (mm) | 90 x 80 x 62 |
| 3 | Program memory | 4096 bytes |
| 4 | Local on-board Digital I | 8 |
| 5 | Local on-board Digital O | 6 |
| 6 | Communications ports | 1 RS 485 |
| 7 | Sensor Power Supply | 20.4-28.8 VDC |

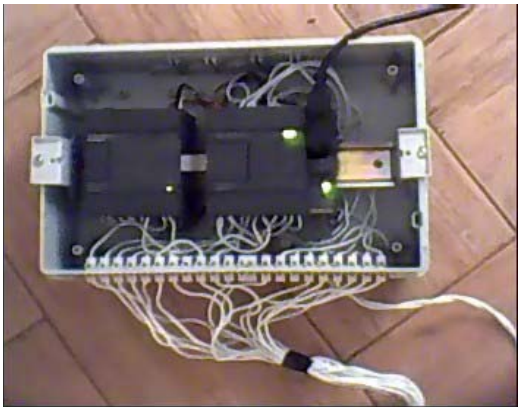
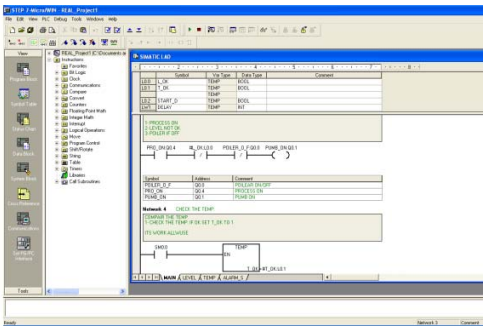


Figure 4. RTU component (S7-222 PLC+EM231)



(B) Programming RTU with Micro/WIN32 Package

TABLE V. CONNECTION OF RTU WITH FIELD INSTRUMENT LAYER

| RTU | Field points | | RTU | Field Points |
|---|---|---|---|---|
| I0.0 | Start button | | Q0.0 | Heater ON\OFF |
| I0.1 | Stop Emergency | | Q0.1 | Valve in ON\OFF |
| I0.2 | Operation mode | | Q0.2 | Pump ON\OFF |
| I0.3 | Heater HW failure | | Q0.3 | Alarm indicator |
| I0.4 | Valve HW failure | | Q0.4 | Process ON indicator |
| I0.5 | Pump HW failure | | Q0.5 | Normally Process End |
| I0.6 | | | AWI 0 | Level sensor |
| I0.7 | | | AWI 1 | Temp. sensor |

*D. Supervision layer (Master station) designed and development*

A personal computer (PC), with National Instruments' LabView is used to develop the SCADA/HMI layer. LabVIEW VI can implement SCADA functionalities such as logging of data in a historical file, trend views, alarms, etc. Also by chosen of Labview from NI vendor which is different from RTU vendor (SIMENSE), gives us opportunity to show how open standard technology solve this compatibility problem.

The OPC technology is utilized for data exchange between supervision control layer and RTU layer. Labview works like an OPC client and SIMENSE S7-200 PC access software package works as OPC serves. Table VI lists the component of master station layer.

TABLE VI. MASTER STATION COMPONENT (SUPERVISION LAYER)

| N | Item | Description |
|---|---|---|
| 1 | PC | personal computer |
| 2 | Operating system | Window XP |
| 3 | Labview SW package | As developer tool for |
| | with DSC module | SCADA HMI |
| 4 | S7-200 PC Access SW package | OPC serves. |
| 5 | Communications ports | USP using MPPI cable |

The plant itself is carefully simulated with a Labview program as Graphic user interface (GUI) illustrated in figure 5. This program facilitate the user to implement the following functions; starting and stopping the operation, monitoring the real-time events of process, temperature, and level, monitoring the trend of real-time events, level and temperature measurements, monitoring alarm indictor for any failure or emergency stop, archiving the events with its timestamp, as historical data for later use for analysis, maintenance, etc.

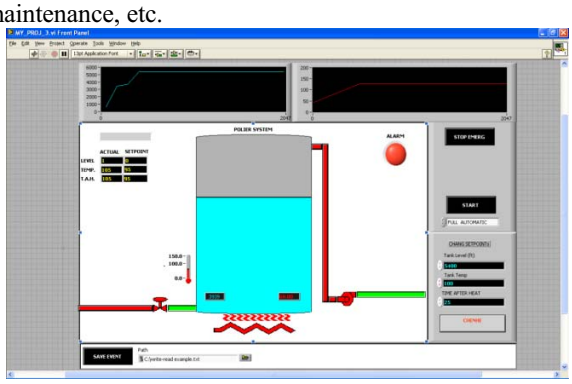
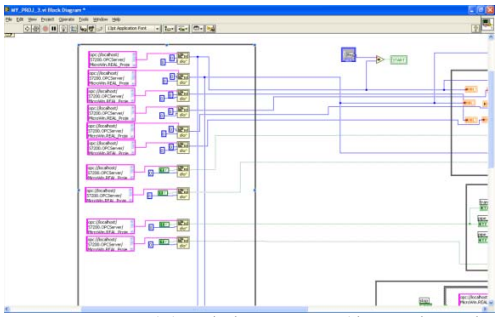


Figure 5. (A) Master station UGI.



(B). Labview program (data exchange loop between Labview and OPC server).

## V. DETAILED TEXT FORMATTING

The SCADA system had been successfully designed, developed, and tested. It's function as the followings:

*1)* The prototype automation is started by pushing the start button (from the program or from simulation unit), indicator process ON (Orange light) is ON and the valve out is closed.

*2)* The Level sensor (potentiometer resistance) returns the tank level, if it is less than level set point, the pump will be on (Green light) to fill-up the tank, if the level reaches the

set point the pump will set off, and the heater starts on (Green light).

*3)* Finally, When the Temperature reaches the desired set point , the counter will count up until it reaches the delay set point after that the operation cycle is finished, and the (Green light) for normally process ending will be light, and the valve out will be open to allow transferring the liquid to next stage.

*4)* When the tank become empty, if the Process mode set to full automation mode the process will start automatically, if the process mode set to half automation mode the new process cycle needs to push start button to start again.

*5)* During all process stage the program watch stop emergency button and any hardware failure to stop the system and arising alarm indication.

Also the system equipped with operation mode switch, which allow user to transfer between two modes, the first is automation control mode where the control signal received from RTU and Master station layers, and the second is manual mode where process will controlled directly by operator and no control signal will be received from RTU nor master station.

## VI. CONCLUSION

In this paper, the three layer SCADA system architecture which depending on open system technology is presented. A complete prototype is designed and developed to represent this architecture. The resultant multi-layer SCADA system architecture has more benefit than traditional SCADA system. The features of the proposed system are among the followings;

*1)* It can be easily integrated and developed using different device vender. The resultant prototype demonstrates how easily data exchanged between different vendor tools (e.g. Labview software and PLC SIEMENS hardware).

*2)* It is easy to upgrade and maintain the system.

*3)* Distribute SCADA functionality across a WAN and not just a LAN is easier with the utilization of open standards.

Moreover, the trend of integration of SCADA equipment is moved to achieve high interoperability and plug-and-play configuration by use open standard architecture.

Finally it is truth to say that: Using three-layer SCADA system architecture, which depends on open system standard, eliminates number of the limitations of previous generations of SCADA systems.

## REFERENCES


[1] Michael P. Ward, “An architectural framework for describing supervisory control and data acquisition (SCADA) systems”, Naval postgraduate school Monterey, California, Master Thesis, September 2004.

[2] Kenneth C. Wiberg, “Identifying supervisory control and data acquisition (SCADA) systems on a network via remote reconnaissance”, Naval postgraduate school Monterey, California, Master thesis, September 2006.

[3] Tapir Uttrykk, “Measurement and Supervision in Automated Production”, Norwegian University of Science and Technology, doctor THESIS, Trondheim, July 2007.

[4] Lian Chen, “A framework of a web-based distributed control system”, The university of Calgary, Master thesis, Calgary, Alberta MAY 2003.

[5] Jonas Lidén, “Design and Implementation of an IEC 61850 gateway for PLC Systems ”, KTH Electrical Engineering, Master Thesis Stockholm, Sweden 2006

[6] David Conway, Edwin Wright, GordonClarke, Deon Reynders, Steve Mackay , “Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems”, British Library Cataloguing in Publication Data, 2004.

[7] Osama Siddig , Ahmed Elhaj Mokhtar , Montasir Esameldeen and Osama Abdalla .”Design and development of a Low Cost Programmable Logic Controller Workbench for Education Purposes“.International Conference on Engineering Education – ICEE, Coimbra, Portugal, 2007.

[8] Francesco Adamo, Filippo Attivissimo, Giuseppe Cavone, and Nicola Giaquinto,” SCADA/HMI systems in Advanced Educational Courses “, IEEE TRANSACTIONS ON INSTRUMENTATION AND MEASUREMENT, VOL. 56, NO. 1, FEBRUARY 2007.

[9] Ahti Mikkor, Lembit Roosimölder ” Programmable logic controllers in process automation“, 4th International DAAAM Conference "Industrial engineering – Innovation as competitive edge for SME ", Tallinn, Estonia, 29 - 30th April 2004.

[10] J. I. Escudero, J. A. Rodríguez, M. C. Romero, and S. Díaz,” Deployment of Digital Video and Audio Over Electrical SCADA Networks “,IEEE TRANSACTIONS ON POWER DELIVERY, VOL. 20, NO. 2, APRIL 2005.

[11] Yang Haijing, Yang Yihan and Zhang Dongying,” The Structure and Application of Flexible SCADA“,Authorized licensed use limited to: STRATHCLYDE UNIVERSITY LIBRARY IEEE,2006.

[12] Zafer Aydogmus, Omur Aydogmus, ,” A Web-Based Remote Access Laboratory Using SCADA “,IEEE TRANSACTIONS ON EDUCATION, VOL. 52, NO. 1, FEBRUARY 2009.

[13] SIMATIC, ”S7-200 Programmable Controller System Manual”, order number: 6ES7298-8FA24-- 8BH0, September 2007