IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 9, Issue 9, September 2020

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 9, September 2020 ||

Design of SCADA System Using PLC for Power Control Equipments

Sayed Qayem Hussain[1], Adnan Hussain Dar[2], Iyman Taha[3], Lovneesh Talwar[4].

UG Students, Department of Electrical Engineering, YCET, Jammu, India[1, 2, 3]

Assistant Professor, Department of Electrical Engineering, YCET, Jammu, India[4]

ABSTRACT: Supervisory Control and Data Acquisition (SCADA) system was getting used in industries to regulate easily and easily. It is a computer control and a software application. This paper describes implementation of control unit to control the filling system with modelling design. It aims a producing system using SCADA system. It has been designed to work on the computer for the process. The main purpose of this paper is to implement the hardware components for the filling process and to interface between master station and control unit for controlling the info. Microcontroller and control circuits have been used for control unit. This paper will be supporting manufacturing of systems to be easy, simple and accurate.

KEYWORDS: Control Unit, Filling process, Manufacturing system, Motor driver, Microcontroller and SCADA System.

I. INTRODUCTION

Using powerful technologies, supported experience of qualified personal, SCADA (Supervisory Control and Data Acquisition) applications are created as a main tool for performing management, required by technical reengineering of an industrial company. In modern manufacturing and industrial processes, mining industries, public and personal utilities, leisure and security industries, control systems are often needed to attach equipment and systems separated by large distances. These systems are wont to send commands, programs and receive monitoring information from these remote locations. SCADA refers to the mixture of control systems and data acquisition. In the youth of knowledge acquisition, relay logic was wont to control production and plant systems. With the arrival of the CPU (Central Process Unit) and other intelligent electronic devices, manufacturers incorporated digital electronics into relay logic equipment. The PLC (Programmable Logic Controller) remains one among the foremost widely used control systems in industry.

II. WHY SCADA?

A. Drawback Of Conventional System

Conventional equipment systems are susceptible to errors, thanks to the involvement of humans within the data collection and processing using complicated mathematical expressions. Thus what we require is a system that collects raw data, processes it and presents it in values which can be verified and compared with the standard values. In the coding process of this implementation with micro-controller, it requires a quick and efficient processing which on the opposite part depends on the length and sub-routines of the coding process. Thus it provides a true challenge with systems involving.

SCADA provides several unique features that make it a very good selection for several control problems. The features are as follows:

The computer control primary equipments, record a store a very large amount of data from process.

- The operator can incorporate real data simulations into the system.
- The operator is assist by computer that recommends actions to stay the system safety.
- Many types of data can be collected from the RTUs (Remote Terminal Unit), this creates online the image of the system.

B. CHALLENGES AND APPLICATIONS

Supervisory Control and Data Acquisition (SCADA) systems are widely utilized in industry applications. Due to their application specific nature, most SCADA systems are heavily tailored to their specific applications. For example, a foreign terminal unit (RTU) that monitors and controls a production well in an oilfield is merely connected with a couple of sensors at the well it resides. The RTU usually collects sensor data at pre-defined

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 9, September 2020 ||

intervals, and only sends data back when being polled by a central data server. A user can only access the info in one among the 2 ways: directly connecting to the RTU within the field or reading from the info server within the room. A major drawback of typical SCADA systems is their inflexible, static, and sometimes centralized architecture, which largely limits their interoperability with other systems. For example, during a SCADA system developed for oil and gas fields, the RTUs are usually places at production wells and injection wells. However, there are many other places, like pipeline, tanks, etc., that have valuable data but are too expensive (e.g., cable requirement) to deploy more RTUs. In such cases, sensor networks are an ideal solution to increase the sensing capability of the SCADA system. However, it's difficult to integrate sensor networks with current SCADA systems thanks to their limited interoperability. We identify that enabling such interoperability is a crucial task for future SCADA systems another drawback of the present SCADA systems is their limited extensibility to new applications. In the above oilfield monitoring example, a user within the field can only access a sensor's data by physically getting to that well and connecting to its RTU. If the corporate wants to increase its SCADA system by adding a security alarm, it'll be very difficult to feature the new application. The original application only monitors well production at predefined intervals or on demand. The new application requires real-time interaction between sensors and mobile users within the field. The RTUs that detect a security problem got to proactively report the matter without waiting. The rigid design of current RTUs makes it hard to increase the SCADA from one application to a different. Deploying a SCADA system during a large field is extremely expensive if the SCADA system is interoperable with new technologies, like sensor networks, and extensible for brand spanking new applications, it'll be ready to significantly improve the productivity at a minimal cost.

III. RESEARCH ISSUES OR FUTURE SCOPE

This section identifies major research issues to
enable interoperability and extensibility of future SCADA systems. We roughly classify them in three categories:
• Flexible communication architecture,
• Open and interoperable protocols, and
• Smart remote terminal units.

IV. FLEXIBLE COMMUNICATION ARCHITECTURE

Current SCADA systems are essentially a centralized communication system, where the info server polls each link-attached terminal unit (RTU) to gather data. There is no data sharing and forwarding between different RTUs. Usually these RTUs only communicate with the info server. This communication architecture isn't flexible to interact with other systems, like the embedded sensor networks and mobile users within the field. Designing flexible communication architecture is one among the key factors to enable interoperability and extensibility.

V. OPEN AND INTEROPERABLE PROTOCOLS

We suggest that SCADA systems should adopt the utilization of Internet technologies for networking, instead of proprietary or link-level approaches. Collect and manipulate different types of sensor data. It also includes the way to discover and configure sensors. An open protocol should be extensible to support various sorts of sensors. These protocols should also address what types of data should be transmitted and to whom. For example, raw data are only sent to data server for archival. Status summaries are going to be sent to managers and engineers, while emergency safety alarms should be broadcast to all or any field operators.

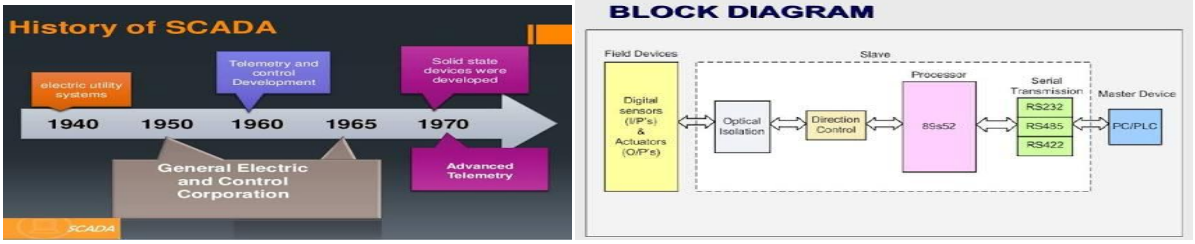
VI. SMART REMOTE TERMINAL UNITS

Remote terminal units play a crucial role within the new communication architecture we described above. They function bridge points to sensor networks also as access points to mobile users within the field. They respond to users queries and collect data from specific sensors. These RTUs should be smart enough to perform preliminary processing. The first reason is to validate the data collected from different sensors. Sensors can give false values due to various reasons. It is important to validate them before use them to form important decisions. For example, in oilfield monitoring, a false sensor reading may end in a mistaken decision to enclose a well and lose production. The RTU is during a good position to validate sensor readings by cross checking from adjacent sensors. Another reason of requiring smart RTUs is that they're important in changing the reactive operation to proactive operation. Current SCADA systems mainly operate within the reactive mode, where data are usually sent in response to the info server's polling. In a new class of applications, detection must be wiped out real time, and events got to be reported immediately, like pipeline leakage, or H2S detection. Intelligent algorithms will run on these smart RTUs

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

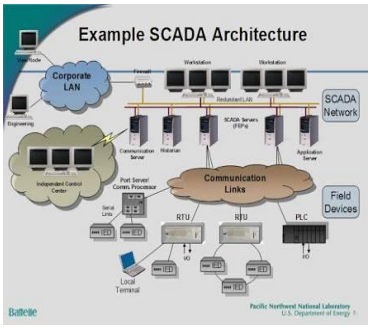
|| Volume 9, Issue 9, September 2020 ||

to process data in real time. Finally, these RTUs got to be smart enough to guard data from unauthorized access and altering. Access control and security measures need to be installed to protect the sensing system from attackers and ensure data integrity.



(a) (b)

Fig.1 (a) History of SCADA, (b) Block diagram of SCADA



(c)

Fig.1 (c) SCADA Architecture

VII. CYBER SECURITY FOR SCADA

Cyber security for SCADA Systems provides a high-level overview of this unique technology, with an evidence of every market segment. Cyber security for SCADA Systems is suitable for the non-technical management level personnel also because it personnel without SCADA experience. The security issues with SCADA systems as follows:

Traditionally SCADA systems were designed around reliability and safety. Security was not a consideration. However, security of those systems is increasingly becoming a problem due to:

• increasing dependence on public telecommunications networks to link previously separate SCADA systems is making them more accessible to electronic attacks;

• increasing use of published open standards and protocols, especially Internet technologies, expose SCADA systems to Internet vulnerabilities;

•the interconnection of SCADA systems to corporate networks may make them accessible to undesirable entities;

•lack of mechanisms in many SCADA systems to supply confidentiality of communications means intercepted communications could also be easily read;

• Lack of authentication in many SCADA systems may end in a system user's identity not being accurately confirmed.

VIII. SCADA SECURITY

The majority of SCADA systems have useful lifetimes starting from 15 to 30 years. In most instances the underlying protocols were designed without keeping modern security requirements in mind. The rapid advance of technology and therefore the changing business environment is driving change in SCADA specification, introducing new vulnerabilities to legacy systems. The current push towards greater efficiency, consolidated production platforms and bigger companies with smaller staffing levels is resulting in changes in SCADA systems which are raising many questions on security.

In summary, these involve:

•an increasing dependence on public telecommunications networks to link previously separate SCADA systems;

• increasing use of published open standards and protocols, especially Internet technologies; and

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 9, September 2020 ||

• The interconnection of SCADA systems to other business networks to reinforce the quantity, detail and timeliness of data available to management.

IX. COMMODITY INFRASTRUCTURE

The changes in SCADA systems have exposed them to vulnerabilities which will not have existed before. For example, the switch from using leased telecommunications lines to public infrastructure i.e. Public CDMA and GSM networks, the utilization of commodity computers running commodity software and therefore the change from proprietary to open standards have meant that vulnerabilities are introduced into SCADA systems.

X. NETWORK ARCHITECTURE

Effective network design which provides the acceptable amount of segmentation between the web, the company's corporate network, and therefore the SCADA network is critical to risk management in modern SCADA systems. Network architecture weakness can increase the danger from Internet and other sources of intrusion.

XI. CONFIDENTIALITY

Generally, there are not any mechanisms in SCADA to supply confidentiality of communications. If lower level protocols don't provide this confidentiality then SCADA transactions are communicated "in the clear" meaning that intercepted communications could also be easily read.

XII. AUTHENTICATION

Many SCADA systems give little reference to security, often lacking the memory and bandwidth for classy password or authentication systems. As a result there's no mechanism to work out a system user's identity or what that user is permitted to access. This allows for the injection of invalid requests or replies into the SCADA system.

XIII. LACK OF SESSION STRUCTURE

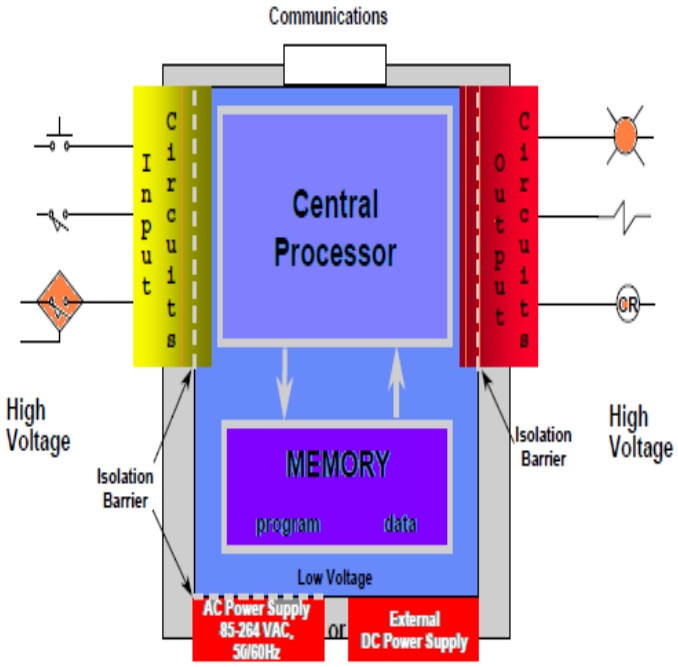
SCADA systems often lack a session structure which, when combined with the shortage of authentication, allow the injection of erroneous or rogue requests or replies into the system with none prior knowledge of what has gone on before.

XIV. AUTOMATION

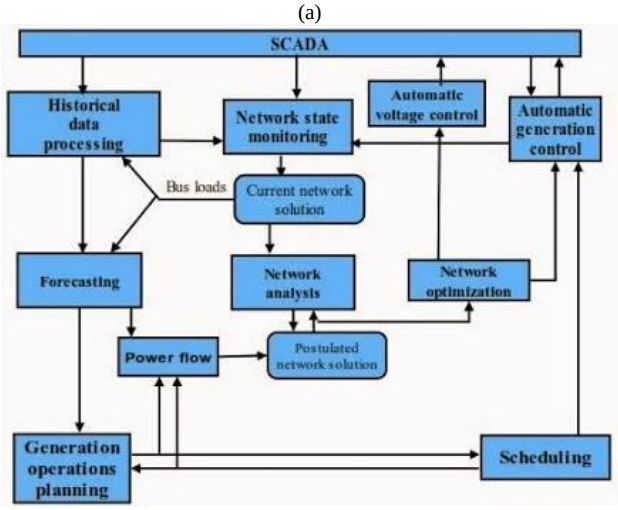
The automation of SCADA includes
• PLC
• ELECTRICAL CONTROL WITH LOGIC GATES
• MANUAL CONTROL
PLC
In this, rather than achieving desired control and automation through physical wiring of control devices, it's achieving through program say software.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 9, September 2020 ||



(a)



(b)

Fig.2 (a) Inside View of PLC (b) Line Diagram of SCADA

The above figure shows the inside view of PLC and line diagram of SCADA, it also depicts that how PLC works in this system and how SCADA assists the working if the system.

REFERENCES

[1] Asdrubali F., Grignaffini S., "Experimental Evaluation of the Performances of a H2O-LiBr Absorption Refrigerator under Different Service Conditions", International Journal of Refrigeration, Vol.28, (2005), pp.489-497.

[2] Antonio De Lucas, Marina Donate, Carolina Molero, Jose Villasenor, Rodriguez J 22uan F., "Performance Evaluation and simulation of a New Absorbent for an Absorption Refrigeration System", International Journal of Refrigeration, Vol.27, (2004), pp.324-330.

[3] Talbi M.M., Agnew B., "Exergy analysis: an absorption refrigerator using lithium bromide andwater as the working fluids", Applied Thermal Engineering, Vol.20, (2000), pp.619-630

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 9, Issue 9, September 2020 ||

[4] Misra R.D., Sahoo P.K., Gupta A., "Thermoeconomic evaluation and optimization of a double-effect H2O/LiBr vapor-absorption refrigeration system", International Journal of Refrigeration, Vol.28, (2005), pp.331-343

[5] Xu S.M., Zhang L., Xu C.H., Liang J., Du R., "Numerical simulation of an advanced energy storage system using H2O-LiBr as working fluid, Part 1: System design and modeling", International Journal of Refrigeration, Vol.30, (2007), pp.354-363.

[6] H. K. Agarwal, Smart Grid Initiative in India and supreme's Experience in Electrical India, vol. 53, no. 9, Sept. 2013, pp. 78

[7] Official website of the Bureau of Energy Efficiency, Govt. of India, www.beeindia.nic.in

Detailed information and case studies on energy audits, www.energymanagertraining.com

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details