SECURE IOT PLATFORM FOR INDUSTRIAL CONTROL SYSTEM

G.NAGA RATHNALU
M. Tech VLSI& Embedded systems student
Gouthami Institute of Technology & Management for women, proddatur, India

G.SANJEEVA RAYUDU
Assistant professor, Department of ECE
Gouthami Institute of Technology & Manegement for women, proddatur,India

ABSTRACT

The project is designed to implement a SCADA system, to monitor and control the various Environment parameters. Here, the parameters are temperature, humidity, smoke and light. These Parameters are sensed by using relevant sensors. Basically, the sensors are physical quantities, which are giving values in analog form. But ARM Microcontroller is a digital circuit, which understands the values in digital format only. So, by using ADC, which can convert the values from analog to digital will interface to ARM Microcontroller. Now, the ARM Microcontroller has the values of parameters and this will be displayed on PC as well as LCD. The buzzer will buzz if the sensors values exceed the threshold limit. Based upon these values we can control the corresponding appliances like turn ON or OFF using commands from pc.

Keywords: SCADA, IOT, LPC2148, ICS

I. INTRODUCTION

Supervisory control and data acquisition (SCADA) systems, are part of industrial control system (ICS), have been playing crucial roles in real-time industrial automation and controls. Through the evolution of 3rd generation, or networks based system, SCADA systems are connected to almost types of networks such as wired, wireless, and cellular and satellite communication, but security is still a big challenge for SCADA system while communicating within.

Internet of things (IoT) is a ubiquitous platform, a new advance enhancement, for efficient SCADA system, where billions of network devices, with smart sensing capabilities, are networked over the Internet access. Deployment of smart IoT platform, SCADA system will significantly increase system efficiency, scalability, and reduce cost. Security is still a major issue for both-, as they were initially designed without any priority and requirements of security. This study modeled IoT-SCADA system and deployed a security mechanism, employing of cryptography based algorithm, which provided a secure transmission channel while each time communication occurred, between the field devices in the SCADA system. Proposed security implementation, and computed measurements analyzed as potential security building block against authentication and confidentiality attacks.

Internet of things (IoT), is another advance technology in IT sector, provides internetworking for numerous of devices such as sensors, actuators, PLCs and other electronic embedded smart devices and controls, and various software's' and provides systems network configuration and connectivity, which enables communication between these numerous devices for information exchanging. Nowadays, IoT is one of the most advanced, efficient, and cost less technological solution which encompasses various hardware and software resources; and allows remotely connected sensing devices to sense with more capabilities, provides efficiency and can be monitored and controlled through deployed of existing systems or infrastructures, resulting the physical World integration with computer controllers (or systems). As IoT provides interconnectivity among various real-time sensing sensors and PLC and other intelligent devices, therefore this technology will be an entity indicated for the more advance cyber-systems encircling the significant developments, "such as smart grid, smart vehicle systems, smart medical systems, smart cities, and others smart systems." In early future, IoT has striven to provide advance or smart connectivity for variety of electronic and intelligent equipment's or devices, IT-based systems and the more advanced services through deploying of various traditional and real-time protocols, networks domains, and system software/hardware applications, which will be an work followed by machine-to-machine technological

concept. Through interconnection of various devices and managing of applications for remotely monitoring and controller, the IoT becomes a tremendous development in the arena of industrial control systems (ICSs), or for real-time industrial infrastructures, including SCADA systems.

II. LITERATURE SURVEY

WSNs have been used in many fields, like the military, industry, ecological monitoring, and healthcare. The WSNs are more and more getting used in your home for energy controlling services. Regular household home appliances are monitored and controlled by WSNs installed in your home. New technologies include cutting-edge advancements in information technology, sensors, metering, transmission, distribution, and electricity storage technology, in addition to supplying new information and versatility to both consumers and providers of electricity. There are many plans to interconnect various domestic appliances by wireless systems to watch and control for example provided. However the prototypes are verified using Test bed situations. Also, wise meter systems have been made to specific usages particularly associated with geographical usages and therefore are restricted to specific places. Different information and communication technologies integrating with smart meter products happen to be suggested an examined at different flats in a residential district for optimal power utilization, but individual controlling from the products are restricted to specific houses. There's been design and developments of wise meters predicting using power consumption. However, a minimal-cost, flexible, and powerful system to continuously monitor and control according to consumer needs reaches the early stages of development. Within this study, we've designed and implemented a Zigbee based intelligent home energy management and control service. We used the ZigBee technology for networking and communication, since it has low-power and occasional-cost qualites, which enables it to be broadly utilized in home and building conditions. The project concentrates on human-friendly technical solutions for Monitoring and simple charge of household home appliances. The inhabitant's comfort is going to be elevated and assistance can be provided. This project emphasizes the realization of monitoring and controlling of electrical home appliances in lots of ways. The developed system has got the following distinct
Features.

i) Utilization of Traci with opt-isolated driver for controlling electrical appliances: Household home appliances are controlled either remotely or instantly with the aid of fabricated smart warning composed of trial -BT138.

ii) No microprocessor / micro-controller: The style of smart sensing unit doesn't need a processing unit in the sensing end.

iii) Versatility in managing the home appliances: Depending on the user needs, home appliances could be supervised and controlled diversely.

Buildings all around the world consume a significant amount of energy, which is more or less one-third of the total primary energy resources. This has raised concerns over energy supplies, rapid energy resource depletion, rising building service demands, improved comfort life styles along with the increased time spent in buildings; consequently, this has shown a rising energy demand in the near future. However, contemporary buildings energy efficiency has been fast tracked solution to cope/limit the rising energy demand of this sector. Building energy efficiency has turned out to be a multi-faceted problem, when provided with the limitation for the satisfaction of the indoor comfort index. However, the comfort level for occupants and their behavior have a significant effect on the energy consumption pattern. It is generally perceived that energy unaware activities can also add one-third to the building's energy performance. Researchers and investigators have been working with this issue for over a decade; yet it remains a challenge. This review project presents a comprehensive and significant research conducted on state-of-the-art intelligent control systems for energy and comfort management in smart energy buildings. It also aims at providing a building research community for better understanding and up-to-date knowledge for energy and comfort related trends and future directions. Key areas focused on include comfort parameters, control systems, intelligent computational methods, simulation tools, occupants' behavior and preferences, building types, supply source considerations and countries research interest in this sector. Trends for future developments and existing research in this area have been broadly studied. In addition, prospective future advancements and gaps have also been discussed comprehensively.

A sensor network is composed of a large number of sensor nodes, which are densely deployed either inside the phenomenon or very close to it. The position of sensor nodes need not be engineered or pre-

determined. This allows random deployment in inaccessible terrains or disaster relief operations. On the other hand, this also means that sensor network protocols and algorithms must possess self-organizing capabilities. Another unique feature of sensor networks is the cooperative effort of sensor nodes. Sensor nodes are fitted with an on-board processor. Instead of sending the raw data to the nodes responsible for the fusion, sensor nodes use their processing abilities to locally carry out simple computations and transmit only the required and partially processed data.

The above described features ensure a wide range of applications for sensor networks. Some of the application areas are health, military, and security. In essence, sensor networks will provide the end user with intelligence and a better understanding of the environment. We envision that, in future, wireless sensor networks will be an integral part of our lives, more so than the present-day personal computers.

Realization of these and other sensor network applications require wireless ad hoc networking techniques. Although many protocols and algorithms have been proposed for traditional wireless ad hoc networks, they are not well suited for the unique features and application requirements of sensor networks. To illustrate this point, the differences between sensor networks and ad hoc networks are outlined.

III. EXISTING METHODOLAGY

A sensor network is composed of a large number of sensor nodes, which are densely deployed either inside the phenomenon or very close to it. The position of sensor nodes need not be engineered or pre-determined. This allows random deployment in inaccessible terrains or disaster relief operations. On the other hand, this also means that sensor network protocols and algorithms must possess self-organizing capabilities. Another unique feature of sensor networks is the cooperative effort of sensor nodes. Sensor nodes are fitted with an on-board processor. Instead of sending the raw data to the nodes responsible for the fusion, sensor nodes use their processing abilities to locally carry out simple computations and transmit only the required and partially processed data.

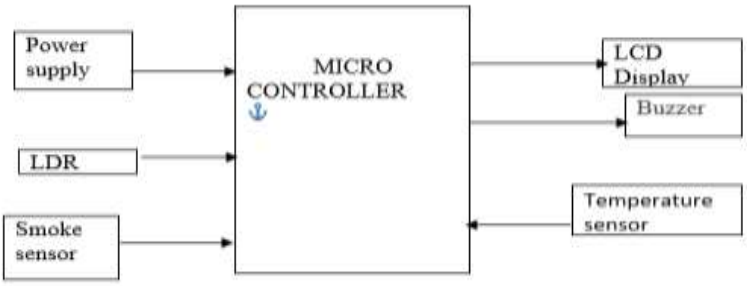

Fig 1 Block diagram for existing system

Here the above figure represents the block diagram of sensor system. Sensors are sens the atmosphere values and those values are displayed on the LCD display which is connected to the micro controller. Whenever the values of atmospheric changes increase the threshold levels the buzzer will buzz. Whenever we here the buzzer sound we have to check the display which parameter exceeds the threshold value and then we take the related action.

Disadvantages

1. Wastage of resources: if we consider the automatically operate sensor system, that is if there are any obsence of light automatically the lights are on without considering the cases like requirement whether there are work in process or not.
2. Time taking process: if there is any fire accident in the industry the smoke sensor will senses and the buzzer will buzz, but the corresponding remedy response will be taking more time why because whenever buzzer comes then check the area and related workers can go to that area and then take the action so it takes some time to monitor and do action.

   Here the main disadvantages are requirement of more man power and wastage of resources, and here also having the loss of equipment.

IV. PROPOSED SYSTEM BLOCK DIAGRAM:

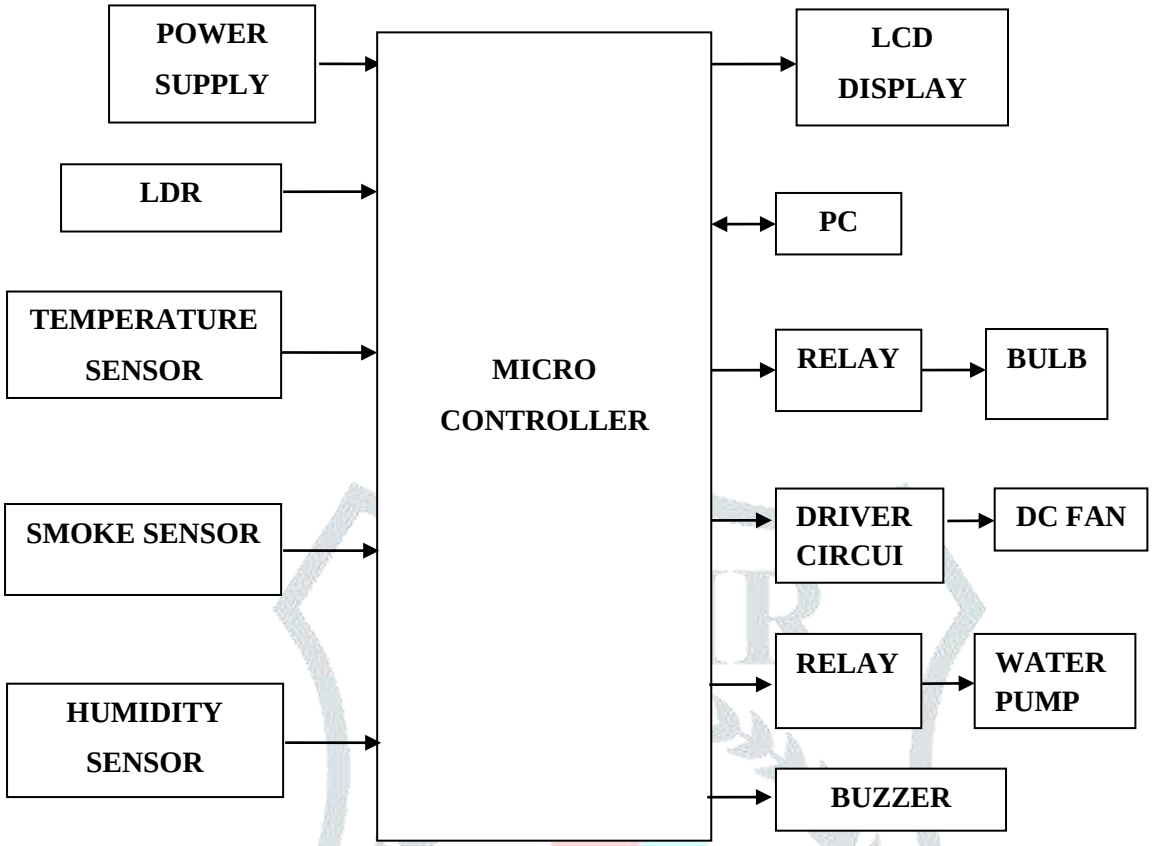

Fig 2. Block Diagram of implementation system

V. IMPLEMENTATION

The project is designed to implement a SCADA system, to monitor and control the various environment parameters. Here, the parameters are temperature, humidity, smoke and light. These parameters are sensed by using relevant sensors. Basically, the sensors are physical quantities, which are giving values in analog form. But ARM Microcontroller is a digital circuit, which understands the values in digital format only. So, by using ADC, which can convert the values from analog to digital will interface to ARM Microcontroller.

Now, the ARM Microcontroller has the values of parameters and this will be displayed on PC as well as LCD. The buzzer will buzz if the sensors values exceed the threshold limit. Based upon these values we can control the corresponding appliances like turn ON or OFF using commands from pc.

VI. WORKING MODEL AND RESUIT ANALYSIS

The overall experimental kit oh the project is shown in figure below, the gas sensor, humidity sensor, temperature sensor & light sensors are used in this project. Here explain about working process of the project.

1. Whenever the temperature levels of the industry exceeds 45 degree centigrades, then the buzzer will buzz and the LCD display also shows the temperature value as shoe in figure and then we will take related action like switch on the fans or ac by using pc, as per the programming by pressing the number 1, we can switch on the fans. As well as by pressing the number 2, we can switch off the fans.

2.If there are any fire accidents in the industry the smoke sensor will sens it and then the buzzer will buzz and also the LCD displays as G:ON which as shown in figure. Then we will take a action by pumping the water. This will be done by using the pc i.e., by giving 3 as input the motor will be ON and by giving 4 it will be OFF.

3. Whenever the light dims in the industry, the LCD display shows as Lit:Drk as shown in figure. The buzzer will buzz then we giving an instruction as 5 from pc the lights will ON and by giving 6 the lights will be OFF.

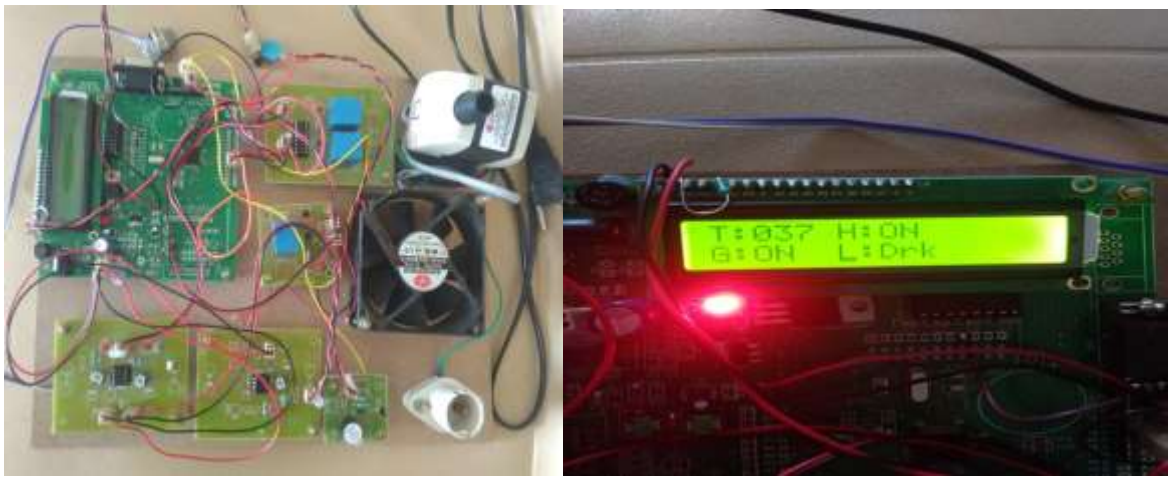

Fig3. Working model of the project and Results on Display unit

VII. ADVANTAGES AND APPLICATIONS

By implementing the model we could able reduce Human Interaction with the devices when emergency, Dynamic control of industry and daily life, Improve the resource utilization ratio, Integrating human society and physical systems, Flexible configuration. This will be useful in Industrial Plant, Medical systems, Home Awareness, Commercial Building and Home Entertainment and Control.

VIII. CONCLUSION & FUTURE SCOPE

The manufacturing sectors or/and industrial sectors are very common sectors that develop to fulfill the demands of industries, such as Oil, Gas, Water/Wastewater, Electric, and others. In past two decades, there have been several enhancements accounted in term of remote information carries, and system monitoring and control, through integration with IP-centric network technology. Moreover, nowadays, the uses of Internet of things smart technology with the existing network-based industrial infrastructures, several enhancements have made that enables more efficiency, system scalability, performance accuracy, capital saving and others, in industrial systems. With these enhancements, and employing of IoT and open IP networks, information security is a big challenge which has not been considered in the initial designing of industrial systems, including industrial protocols designing, as well security is also not a part of IoT initial designed.

Therefore, by examining IoT potentials in areas of industrial sectors or especially in SCADA systems, this study first reviewed, the IoT and SCADA system as a part of industrial control system, or IoT-SCADA system, and then analyzed security issues that have been residing in. To overcome the security issues, a cryptography based security mechanism which implementation was significant in the protection of information while exchanging between several connected devices within the premises of IoT-SCADA system. The measured results were good enough to protect the IoT-SCADA system information while traveling over open networks or/and the Internet but limited to secure the IoT-SCADA system against authentication and confidentiality attacks.

In future, a generic model for IoT-SCADA system will be designed where numerous of devices will network in order to exchange information within secure channels, developing with cryptography mechanisms that will have potentials to fight against IoT-SCADA system insecurities.

REFERENCES

[1] S, J., K. K., “Guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control Systems Security,” Recommendations of the National Institute of Standards and Technology, 2006

[2] M, S. A, “Secure security model implementation for security services and related attacks base on end-to-end, application layer and data link layer security,” Proceedings of the 7th International Conference, 2013

[3] S.A et al., "A New Cellular Architecture for Information Retrieval from Sensor Networks through Embedded Service and Security Protocols." Sensors 16, no. 6 (2016): 821.

[4] SCADA system, https://en.wikipedia.org/wiki/SCADA

[5] J.G., J.L, “SCADA communication and security issues. Security and Communication Networks”, 2013

[6] Internet of Things, https://en.wikipedia.org/wiki/IoT

[7] IoT and SCADA: Complimentary technologies for Industry 4.0.

[8] Lopez Research LLC, “Building Smarter Manufacturing With The IoT,” 2014

[9] R., P., J. L, "Securing the Internet of Things, in Computer,: vol. 44, no. 9, pp. 51-58, Sept. 2011.
[10] ICON LABS, “Secure the Internet of Things,” http://www.iconlabs.com/prod/internet-secure-things
[11] R.M et al., "Security in the Industrial Internet of Things," 2016
[12] Harbor Research, Inc., “M2m & Smart Systems,” http://www.windriver.com/m2m/edk/Harbor_ResearchM2M_and_Smart_Sys_Report.pdf, 2014
[13] M.B et al. , Project Proposal, “Securing the Internet of Things,”https://sites.google.com/a/onid.oregonstate.edu/477project/project-proposal, 2014
[14] S.A et al., “A Secure, Intelligent, and Smart-Sensing Approach for Industrial System Automation and Transmission over Unsecured Wireless Networks,” Sensors 2016, 16, 322..