International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 7, ISSN No. 2455-2143, Pages 214-217
Published Online November 2022 in IJEAST (http://www.ijeast.com)

IMPLEMENTING INTERNET PROTOCOL (IP) BASED SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) NETWORK SYSTEM

Binnaser Aziz Abdullah
Department of Computer Science
Sir Sayyed College Aurangabad (MS)

Abstract:- **SCADA (supervisory control and data acquisition) is a system that monitors and control industrial, infrastructure, or facility- based processes. Scada systems integrate data acquisition systems with data transmission systems and graphical software in order to provide a centrally located "monitor and control" system for numerous process inputs and outputs. The sensors and metering devices are connected to field control devices. These control devices take real-world physical input signals from the sensors and, convert the signals to digital data and make decisions based on programmed logic or commands from the system operators. The control devices are connected control room environments where the hmi software systems are used by system operators to interact withthe control devices.**

IP SCADA is a plug and play feature in the IDP 600 terminal series that allow common SACDA devices such as remote terminal units (RTU) and PLC to be connected to SCADA networks using the IsatData Pro satellite service. IP SCADA is well suited for SCADA devices that are located in remote sites where other communication services are unavailable, unreliable or cost prohibitive and for sites that have low data usage requirements. IP-based SCADA Network systems provides many benefits like Unlimited locations for servers and clients, Service takeover and remote support, Data saving & Global Coverage.

KEYWORDS: **- SCADA, PLC, RTU, TCP/IP, HMI, ISATDATA PRO, IDP 600**

I. INTRODUCTION

1.1 SCADA

SCADA (supervisory control and data acquisition) generally refers to industrial control systems (ICS) computer systems that monitor and control industrial, infrastructure, or facility-based processes. SCADA systems integrate data acquisition systems with data transmission systems and graphical software in order to provide a centrally located "monitor and control" system for numerous process inputs and outputs. Specifically, SCADA systems are designed to collect information, transfer it back to a central computer, and display the information to the operator, thereby allowing the operator to monitor and control an entire system from a central location in real time. Based on the setup of the individual system, control of any individual system, operation, or task can be automatic, or it can be initiated by operator commands. For example, a SCADA system could allow water in the tank to monitor continuously if the levels of water drop, the signal is given to an alarm system to take the necessary action. SCADA systems could integrate data from cameras, motion sensors, security lights, or other security devices, and provide all of this information to a central security monitoring location, allowing an operator to evaluate all of these data at once.

1.2 OVERVIEW OF SCADA SYSTEM

Although there are differences in the functionality of the various types of industrial control systems. All SCADA systems require sensors, instrumentation or other metering devices to acquire information about the physical process. The sensors, instrumentation and metering devices are connected to field control devices such as PLCs (Programmable Logic Controllers) or RTUs (Remote Terminal Units). These control devices take real-world physical input signals (voltages and currents) from the sensors and instrumentation, convert the signals to digital data and make decisions based on programmed logic or commands from the system operators to turn other equipment on or off or change system control parameters. The control devices are connected over hardwired or wireless communications back to control room environments where the HMI (human machine interface) software systems are used by system operators to interact with the control devices, change system parameters or send commands to the plant equipment.

International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 7, ISSN No. 2455-2143, Pages 214-217
Published Online November 2022 in IJEAST (http://www.ijeast.com)

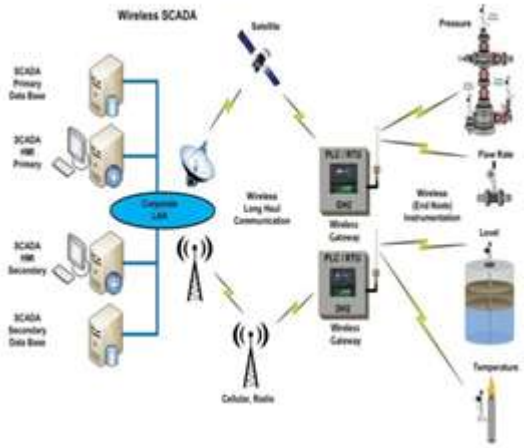

Figure 1 SCADA Network System

1.3 INTERNET PROTOCOL

Internet Protocol is responsible for addressing hosts and routing data packets from a source host to the destination host across one or more IP networks. The IP includes specific addresses to identify hosts and provide a logical location service. Each packet is tagged with a header that contains the meta-data for the purpose of delivery. This process of tagging data with IP information is also called encapsulation. The 7-layer OSI model and the 4-layer internet model are two methods of describing TCP/IP communications. The 7-layer OSI model is used to define networking protocols and the 4-Layer model defines TCP/IP communications.

II. IP BASED SCADA SYSTEMS

One of the main reasons why the Internet Protocol (IP) is enormously successful is that it can be used over virtually any physical media. In complex SCADA architectures, there is a variety of both wired and wireless media and protocols involved in getting data back to the central monitoring site. This allows implementation of strong IP-based SCADA networks over mixed cellular, satellite, and landline systems. SCADA communications can employ various ranges of both wired (telephone lines, optical fibers, ADSL, cables) and wireless media (radio, spread spectrum, cellular, WLAN, or satellite). The choice depends on a number of factors that characterize the existing communication infrastructure. Factors such as existing equipment, connections, available communications at isolated sites, data rates and polling frequency, remoteness of site, installation budget, and ability to accommodate future needs all impact the final decision for SCADA architecture.

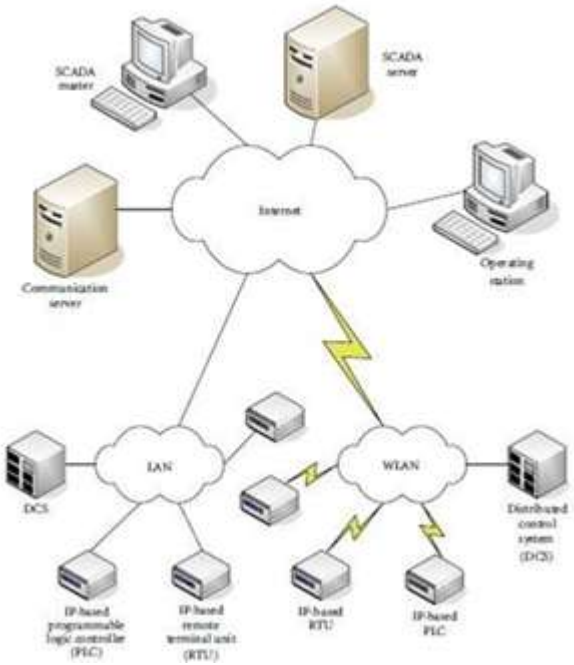

Figure 2 IP Based SCADA System

A major enhancement in new SCADA systems comes from the use of WAN protocols such as the Internet Protocol for communication between the central station and communications equipment. RTUs can communicate with the master station using an Ethernet connection. Many of the traditional utility devices such as RTUs or even relays are today equipped with Ethernet interfaces. This, however, does not imply that all services can be migrated immediately in a plug-and-play manner to an IP-based communication infrastructure. Differential protection services are known as one of the most delicate applications. To run SCADA information over an IP network, various issues have to be considered such as operating equipment types etc.

III. IMPLEMENTING IP BASED SCADANETWORK SYSTEM:-

1.4 Why IP SCADA

IP SCADA is a plug and play feature in the IDP 600 terminal series provided by Skywave Mobile Communication that allow common SACDA devices such as remote terminal units (RTU) and PLC to be connected to SCADA networks using the IsatData Pro satellite service. IP SCADA is well suited for SCADA devices that are located in remote sites where other communication services are unavailable, unreliable or cost prohibitive and for sites that have low data usage requirements.

International Journal of Engineering Applied Sciences and Technology, 2022
Vol. 7, Issue 7, ISSN No. 2455-2143, Pages 214-217
Published Online November 2022 in IJEAST (http://www.ijeast.com)

Figure 3 Remote Sites Connected to SCADA Network System

1.5 IMPLEMENTING IP SCADA NETWORK

- The SCADA Master sends data destined for a SCADA device using a VPN session to the IP SCADA gateway.
- IP SCADA gateway maps the private IP address of the IDP-600 series terminal to as IsatData Pro address, removes the TCP/IP overhead, adds a very small IsatData pro header and sends the data across the IsatData Pro satellite network.
- The IDP terminal receives the data, removes the IsatData Pro header and forwards the original bytes to the serial port to slave RTU.
- At this point, the slave RTU responds to the data poll with the requested data, which goes through the reverse process upstream to the SCADA master

1.6 BENEFITS OF IP-BASED SCADA SYSTEMS

- **Unlimited locations for servers and clients:-**

Users can install and move their SCADA servers, RTUs and terminal servers (if any) to any site. This gives high flexibility in terms of redundancy and security.

- **Failover of SCADA Servers:-**

Servers connected to the IP network (even in distributed LAN/WAN structures) provide mutual back-up for optimized availability.

- **Service takeover and remote support: -**

More and more control centers are not manned during the night. During this period, either other regions can take over control, or a supervisor logs in via VPN in case of alarms.

- **Savings: -**

With IP-enabled RTUs, many front-end devices are no longer required; a lot of hardware, spares, and cabling canbe saved and maintenance costs are reduced.

- **Connectivity: -**

IP SCADA provides a way to connect to sites that would require considerable investment in infrastructure to be connected to communication service.

- **Data saving: -**

Since the system relies on the small IDP satellite overhead to direct data to and from remote sites, IP SCADA uses less data than conventional based SCADA system.

- **Global Coverage: -**

Inmarsat System provides coverage anywhere in the world.

IV. CONCLUSIONS

The supervisory control and data acquisition (SCADA) industry's move into the TCP/IP world has been accelerated with business demand for more open and interoperable systems. Presently, operator consoles, SCADA servers, and control room system components are already most likely connected to an internet network. The last components to move to IP are embedded devices which include field controllers, meters, instrumentation, and telecommunications systems linking the control room with embedded devices in the field. Moving to IP-based communications opens up these devices in the field to other networks and systems. With the use of IsatData Pro satellite service any remote site can be connected to SCADA network system. Unfortunately, the risk from cyber threat is therefore much greater, as these devices do not have the ability to support typical security features that most computing systems require (such as antivirus, authentication, encryption, and endpoint security) . Thus, to secure IP-based SCADA systems, it is vital to implement secure architectures which prevent access to the SCADA from corporate IT and other third-party networks and to enforce excellent management practices to manage IP-based networks.

V. REFERENCES

[1]. Hyung Jun Kim**,** International Journal of Distributed Sensor Networks, Volume 2012, Article ID 268478, 10 pages, doi:10.1155/2012/268478 Security and Vulnerability of SCADA Systems over IP-Based Wireless Sensor Networks

[2]. National Communications System, "Supervisory control and data acquisition (SCADA) systems," Technical Information Bulletin 04-1, 2004.

[3]. Farkhod Alsiherov, Taihoon Kim ,Wseas transactions on systems and Control. ISSN: 1991-8763 Issue 8, Volume 5, August 2010 Research Trend on Secure SCADA Network Technology and Methods

[4]. V.Rajeswari, Prof.Y.Rajeshwari, Dr.L.Padma Suresh / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 Vol. 2, Issue 3, May-Jun 2012, pp.899-902. Real Time Implementation of Hydroelectric Power Plant Using PLC and SCADA

[5]. Bindu Pillai, Vishal Mehta, Nilam Patel,International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 5, May 2012) Development of Supervisory Control and Data Acquisition system for Laboratory Based Mini Thermal Power Plant using Lab VIEW

[6]. U. S. Patil ,International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN) ISSN No. 2248-9738 (Print) Volume-1, Issue-2, 2011. Study of Wireless Sensor Network in SCADA System for Power Plant.

[7]. Binnaser Aziz Abdullah and Quazi Khabeer, Real Time SCAD model for Public Water Distribution System, Golden Research Thoughts, Available online at www.aygrt.isrj.net, Volume 2, Issue. 11 May. 2013, ISSN:-2231-5063