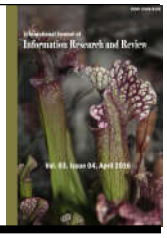
IJIRR

International Journal of Information Research and Review
Vol. 03, Issue, 04, pp. 2253-2257, April, 2016



Research Article

SCADA IMPLEMENTATION BASED ON RF TECHNOLOGY

[1,*]Sachin Kumar, [2]Ravinder Poonia, [3]Akshay Kumar and [4]Mr. Vikas Kumar

[1,2,3]B.Tech Student (Electrical Engineer) at BKBIET, Pilani
[4]Assistant Professor, Electrical Department at BKBIET, Pilani

ARTICLE INFO

Article History:

Received 22nd, January 2016
Received in revised form
19th, February 2016
Accepted 24th, March 2016
Published online 27, April 2016

Keywords:

Utilization,
Communications,
Impractical,
Increasing Widening.

ABSTRACT

The SCADA (Supervisory Control and Data Acquisition) systems are collecting data from various sensors nodes deployed in remote locations of field and then transmitted to a central controller which then manages and control this data. Wireless communication for SCADA is required to applications where wired communications to the remote site is too expensive or it is too time consuming to construct wired communications. Utilization of wired or line communications become impractical as the scope is increasing widening. This paper discusses the role of wireless communication for SCADA systems.

INTRODUCTION

SCADA systems are computer controlled systems that control and monitor industrial processes that exist in the physical world. SCADA systems are combination of computers, instruments, controllers, actuators, networks, and interfaces that manage the control of automated industrial process and allow analysis of those systems through data collection. These processes include infrastructure, industrial, and facility-based processes, and are used in all types of industries, from electrical distribution systems, to food processing, to facility security alarms. Traditionally, SCADA communication took place over radio, modem, or dedicated serial lines. Typical wireless communications for a SCADA system Point-Multipoint with one master polling multiple remote RTU's or PLC's using data communication protocols including protocols such as MODBUS and DNP3. Each RTU or PLC at the remote site is programmed with a unique system address and those addresses are all configured into the SCADA host HMI. SCADA host then polls these addresses and stores the acquired data into database. It will perform centralized data trending, alarm management, operator display and control. In present time, it is much more common for SCADA communications to travel over LAN or WLAN.

Corresponding author: Sachin Kumar,
B. Tech Student (Electrical Engineer) at BKBIET, Pilani.

Wireless communication can be applied to any setup where a central controller needs to communicate with a remote device. Wireless communications for SCADA is required to application where wired communication to the remote site is expensive or it is too time consuming to construct wired communications.

SCADA

SCADA means Supervisory Control and Data Acquisition. SCADA is a computer-based system for gathering and analyzing real-time data to monitor and control equipment that deals with critical and time-sensitive materials or events. SCADA systems were first used in the 1960s and are now an integral component in virtually all industrial plant and production facilities.

SCADA System Importance

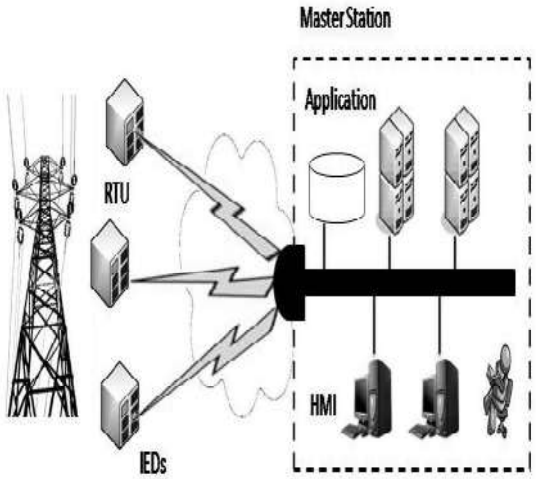
The importance of SCADA systems is automation. It allows an organization to carefully study and anticipate the optimal responses automatically every time. Relying on precise machine control for monitoring equipment and processes virtually eliminates human error. More importantly, it automates common, tedious, routine tasks once performed by a human, which further increases productivity improves management of critical machine failure in real-time, and minimizes the possibility of controllable environmental disasters.

In addition, SACDA systems are needed to monitor and control a large geographical displacement where an organization may not have enough manpower to cover. Thus, SCADA systems are needed to monitor and control a large geographical displacement where an organization may not have enough manpower to cover. Thus, reliable communication and operability of these areas or sites is critical to profitability.

SCADA Systems Communication

Early SCADA system's data acquisition uses strip chart recorders, panel of meters, and lights. Unlike the modem SCADA systems, there is an operator which manually operates various control knobs exercised supervisory control and data from remote sources by wire or radio or other means. It is also used to send commands, programs and receives monitoring information from these remote locations. SCADA is the combination of telemetry and data acquisition. SCADA is composed of collecting of the information, transferring it to the central site, carrying out any necessary analysis and control and then displaying that on the operator screens. The required control actions are then passed back to the process.

SCADA protocols are very compact in design. Many protocols are designed to send information only when the master station polls the RTU. Typical legacy SCADA protocols include MODBUS RTU, RP-570, PROFIBUS and CONITEL. These communication protocols are all SCADA-vendor specific but are widely adopted and used. Standard protocols are ICE 60870-5-101 or 104, IEC 61850 and DNP3. These protocols are standardized and recognized by all major SCADA vendors. Many of these protocols now contain extensions to operate over TCP/IP, blurs the line between traditional and industrial networking, they each fulfil fundamentally differing requirements. The process of communication over a SCADA system involves several different SCADA system components. These include the sensors and control relays, Remote Terminal Units, SCADA master units, and the overall communication network. Each of these parts is necessary for effectively monitor alarms and status update within the network only when all of these system components function properly. For more complete monitoring of SCADA communications, operators must deploy advanced RTUs. The RTU is where most SCADA communication is gathered within the system. Values from inputs and outputs, referred to as SCADA points are sent from individual sensors to the RTU. The RTU is responsible for forwarding these SCADA communications to the master station, or Human-Machine Interface.



Data acquisition begins at the RTU, IED (Intelligent Electronic Device) or PLC level and includes meter readings and equipment status reports that are communicated to SCADA as required. Then data is 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. Recently, OLE for Process Control (OPC) has become a widely accepted solution for intercommunicating different hardware and software, allowing communication even between devices originally not intended to be part of an industrial network. Central computer of the data acquisition system, located in the hydro power plant, provides measurements performance according to a preset program, the instrumentation existing at this time and remote communications by RS485 bus, using Master-Slave architecture and IEC1107, MODBUS RTU, ASCII protocols.
Communication between the control centre and remote sites could be classified into following categories- Data acquisition-the control centre sends request (poll) message to RTU and RTUs dump data to the control centre. In particular, this includes status scan and measured value scan. The control centre regularly send a status scan request to remote sites to get field devices status and a measured value scan request to get measured values of field devices. The measured values could be ANALOG values or digital coded values and are scaled into engineering format by the front-end processor (FEP) at the control centre.

a.Control function-the control centre sends control commands to a RTU at remote sites. Control functions are grouped into four subclasses-individual device controls, control message to regulating device, sequential control schemes, and automatic control schemes. Firmware download-the control centre sends firmware downloads to remote sites. In this case, the request message is large (large than 64kb) than other cases. Broadcast-the control centre may broadcast message to multiply RTUs. For example, the control centre broadcast an emergent shutdown message or a set-the-clock-time message. Acquired data is automatically monitored at the control centre to ensure that measured and calculated values lie within permissible limits. The measured values monitored with regard to rate-of-change and for continuous trend monitoring. They are also recorded for post-fault analysis. Status indications are monitored at the control centre with regard to changes and time tagged by the RTUs. Existing communication links between the control centre and remote sites operate at very low speeds (300bps to 9600bps).

Protocols of communication

In communication, protocols are needed to be applied to avoid miscommunication, signalling, and other problems. In order for SCADA systems to obtain its functionality, it needs a protocol for transmitting data. Some SCADA protocol includes MODBUS RTU, RP-570, PROFIBUS and CONITEL. These protocols are all SCADA-vendor specific but are widely adopted and used. Standard protocols are IEC 61850 (in which T101 branched out), IEC 60870-5-101 or 104, and DNP3. These protocols are recognized and standardized by all major SCADA vendors. Many protocols are now improved and contain extensions to operate over TCP/IP.

Three most important part of a SCADA system are master station, remote terminal (RTU, PLC, IED) and the communication between them. In order to have good communication between them, there must be a communication protocol. Today most common protocols are DNP3 and T101. It is important to determine which protocol should be applied if you are planning a SCADA system. The two open communication protocols that provide for interoperability between systems for radio-control applications. These are now competing in the world market. IEC 60870-5-101 or T101 is strongly supported in the Europe, while DNP is widely used in North America, South America, South Africa, Asia and Australia.

DNP3 Protocol

The distributed network protocol is a set of communications protocols used between components in process automatic systems. It is mainly used is in utilities such as water and electric companies. It is also technically possible to use it in other utilities. It was specifically developed to facilitate communications between various types of data acquisition and control systems. It plays a crucial role in SCADA system. It is generally used by SCADA master station, RTUs, IEDs. It is primarily used for communications between a master station and RTUs or IEDs. DNP3 supports multiple-slave, peer to peer and multi-master communications. It supports the operational modes of polled and quiescent operation.

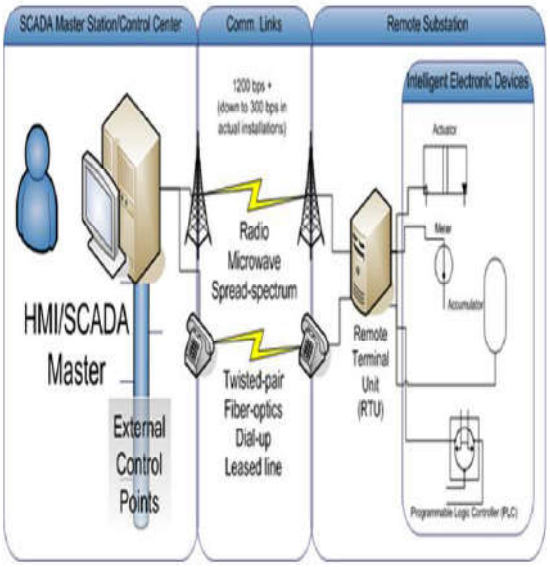


Fig overview of DNP3 protocol

IEC60870-5 Standards

IEC 60870-5 is a collection of standards produced by the international electro-technical commission. It was created to provide an open standard for the transmission of SCADA telemetry control and information. It provides a detailed functional description for TELE-control equipment and systems for controlling geographically widespread processes specifically for SCADA systems. The standard is intended for application in the electrical industries, and has data objects that are specifically intended for such applications. It is also applicable to normal SCADA applications in any industry. But IEC 60870-5 protocol is primarily used in the electrical industries of European countries.

When the IEC 60870-5 was initially completed in 1995 with the publication of the IEC 870-5-101 profile, it covered only transmission over relatively low bandwidth bit-serial communication circuits. With the increasingly widespread use of network communications technology, IEC 60870-5 now also provides for communications over networks using the TCP/IP protocol suite. This same sequence of development occurred for DNP3.

Wireless SCADA Communications

SCADA systems are composed of four major components-

- the master station or the central controller,
- plc/RTU/IED (deployed in remote stations),
- Field bus and
- Sensors.

In Figure, the architecture of SCADA system that replaces the field bus with wireless communication. Along with the field bus, this setup is extended to the Internet. This setup is similar with a private network so that only the central controller can have access to the remote assets. The central controller also has an extension that acts as a web server so that the SCADA users and customers can access the data through the SCADA provider website.

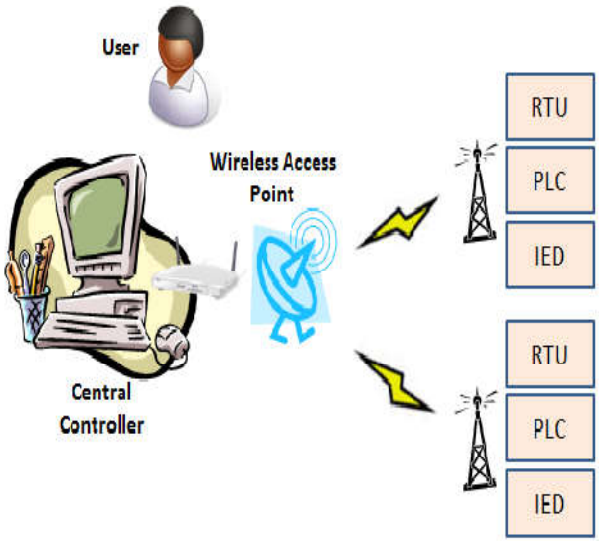


Fig –wireless communication system

Wireless SCADA Control Systems

Free Wave's wireless networking solutions offer advanced flexibility and improved performance for Supervisory Control and Data Acquisition (SCADA) systems. Our wireless SCADA system solutions transmit real-time data reliably and securely across long distances, allowing access from corporate offices anywhere in the world. Free Wave does this with two primary applications-

- Serial and Ethernet communication channels to reach critical infrastructure.
- I/O devices provide industry standard Mod bus access to sensor data with analog and digital inputs and outputs Free Wave solutions connect to your PLC, sensors and remote locations.

Different game of Wireless Instrumentation

SCADA Improves **So** if the business case is that strong and the return on investment is solid, why are some still reluctant to deploy wireless instrumentation in their facilities?
There are three main reasons-

Reliability

In industrial applications, reliability is a major concern. Wireless instrumentation must be as reliable as conventional wired units. Even in simple applications like remote monitoring, users come to expect a certain level of reliability and network availability. Wired systems are much easier to diagnose and trace because the medium, the wire, is physically there or could be dug out. Wireless, on the other hand, uses the invisible free space as a medium. Radio signals are subject to free space attenuation, where the signal loses strength at a rate proportional to the square of the distance travelled. Radio signals are subject to reflection as a result of structure, trees, water bodies and buildings. Furthermore, interference from near-by wireless systems such as cell towers adds more challenges. RF design is getting better in addressing many of these issues. By designing highly sensitive radio receivers, using the transmit power more efficiently and high gain antennas, engineers were able to establish highly reliable RF point-to-multipoint links.

Adaptability

Wireless instrumentation networks are required to adapt to the existing environment. It is not practical to move a well head, a compressor, tank or a separator just to create a reliable wireless link. In long range SCADA networks, it would be much easier to locate a 30 foot tower in the field to allow for line-of-sight consideration. It might also be easier to increase the height of the tower to extend the range and avoid obstruction. Wireless instrumentation networks do not have that luxury. It is sometimes difficult to find a location for an access point or base radio that provides reliable communication with the wireless instruments. Relocating the access point or base radio to improve the RF link with one sensor could result in degrading the links with other sensors in the same network. Adaptability can be addressed by using lower frequency bands, such as the license-free 900 MHz, which tend to provide better coverage, longer range and better propagation characteristics allowing the signal to penetrate obstacles. Also, high gain external antennas that can be mounted as high as possible on a structure allow access to hard-to-reach sensors which could be located at the bottom of a tank. Improved receive sensitivity of radio modules also plays a crucial role in ensuring network.

Integration

Most gas production, processing plants and pipeline facilities have some level of wireless capability in place. Long range proprietary SCADA networks, backhaul point-to-point networks and local wireless area networks are some of the common systems deployed. Each of these networks is being used for a specific purpose such as control data transmission, high bandwidth communication and video surveillance. Engineers and operators are facing the challenge of integrating wireless instrumentation networks with other communication infrastructure available in the field.

Managing and debugging wireless networks presents a new level of complexity to field operators that could deter them from adopting wireless instrumentation despite the exceptional savings. The wireless networks integration dilemma is more apparent in SCADA systems. Since wireless instrumentation networks are supposed to tie into the same SCADA infrastructure available at site in order to relay valuable operating data to the SCADA host, having the ability to manage the complete infrastructure as one network becomes essential. Moreover, having the ability to access hard-to-reach areas and gather new data points that were not economically viable before, gives the operator better visibility into the process and plant operations. However, this data has to end up somewhere in the system in order to be monitored, analyzed and leveraged. SCADA systems are normally designed to handle a certain number of data points or tags. Scaling up the system to handle additional data points and integrate them in trends and reports could be costly.

Despite the abundance of tools to capture process and analyze data in the process control market, ensuring data integration is still a major problem. Some SCADA systems even have a separate historian module that must be purchased as add on to handle the flood of data as a result of adding wireless instrumentation networks. Addressing the Wireless and Data Integration Challenges, a new breed of advanced wireless instrumentation base station radios or gateways is now emerging in the marketplace to address this need. This new generation of gateways integrate both a wireless instrumentation base radio and a long range industrial radio in the same device. The wireless instrumentation base radio has a Mod bus data port, allowing an external Mod bus Master to poll information from the base radio about its own status as well as the status and process values of its field units. It also has a diagnostics port, allowing the connection of the network management software for sensor configuration and diagnostics. Both of these data streams are sent simultaneously through an advanced long range serial or Ethernet radio network. This is how it works in practice-

The wireless instrumentation base radio and all field units must have the RF Channel and Baud Rate set identically.

- Each field unit must then have its RF ID set to a unique value. This value will be used later for Mod bus polling of the data.
- The base radio's Mod bus serial port baud rate must be set to match that of the long range radio.
- The base radio's Device ID must be set. This value will be required later for Mod bus polling of the system. The integrated long range remote radio is configured as remote device relaying information to a Master radio at the main SCADA centre. The available two serial ports on the radio are configured to tunnel Mod bus polling and diagnostic data simultaneously to the wireless instrumentation base radio. This allows operators to manage and diagnose the wireless instrumentation network through the existing long range SCADA infrastructure. Live data and status information for all field units are displayed in a separate view or integrated in the SCADA host. On the data integration front, modern SCADA host software offers a fully integrated environment that includes an integrated and scalable historian to handle more additional data without

going through expensive and sometimes lengthy upgrades. Developing the SCADA screens based on templates allow engineers to add data points easily and rapidly in their systems.

Efficiency

Access to continuous real-time data ensures that operators have the ability to make the most accurate data-driven decisions on how to improve efficiency. Through wireless communication technology for SCADA systems, these crucial decisions are possible and take extensively less time and resources to make. Free-Wave's highly accurate ANALOG I/O solutions allow you to run your operations with tighter tolerances and in turn, greater efficiency. Free-Wave's solutions for SCADA applications improve efficiency and reduce waste, resulting in saved time and money.

Advantages

- Increase Efficiency
- Minimize faults Isolate and precisely locate faults
- Maximize Profitability
- Reduce failures
- Reduce operations overhead
- Reduce man power requirement

Disadvantages

- Initial cost is more to establish SCADA system in real time process.
- Maintenance cost is more in real time process.
- Construction of SCADA is Massive in real time process.
- SCADA system can be damaged by environmental changes

Conclusion

As the adoption of wireless instrumentation networks increases, users will be faced with a number of challenges to ensure the reliability, adaptability and tight integration with their existing infrastructure. New RF and antenna designs help to address reliability and adaptability challenges. This leaves wireless and data integration with the existing SCADA infrastructure as one of the critical challenges to be resolved. Luckily, hybrid gateways, where sensor network base radio and long range radio are integrated, allow users to view, manage and diagnose their dispersed wireless systems from a single point. Similarly, advanced SCADA host software, with an integrated historian and rapid development environment using templates, can facilitate the integration of new data points generated by a growing network of wireless sensors.

Future Works

- Wireless communications for SCADA systems is a practical solution and is required for applications when wired or line communications to the remotely deployed units is prohibitively expensive or it is too time consuming to construct. It can replace or extend the field-bus to the internet and reduce the cost of installation.
- The Researches are being done by electrical engineering scientists in Gujarat and Pune to reduce the cost of SCADA and to implement them in small scale industries and medium scale industries in future.

REFERENCE

Clarke, C., Reynders, D. and Wright, E. 2004. "Practical Modern SCADA Protocols: DNP3, 60870.5 and Related Systems",.

DNP Users Group, "Overview of the DNP3 Protocol", **(2011)**, http://www.dnp.org/About/Default.aspx.

GAO-04-628T, "Critical infrastructure protection; Challenges and efforts to secure control systems", Testimony Before the Subcommittee on Technology Information Policy, Intergovernmental Relations and the Census, House Committee on Government Reform, (2004) March 30, http://www.gao.gov.new.items/d04628t.pdf.

Hildick-Smith, A. 2005. "Security for Critical Infrastructure SCADA Systems," SANS Reading Room, GSEC Practical Assignment, Version 1.4c, Option 1, () February, http://www.sans.org/reading_room/whitepapers/warfare/1644.php.

http://en.wikipedia.org/wiki/DNP3.

Robles, R. J., Choi, M. K. and Kim, T. H. 2005. "The Taxonomy of SCADA Communication Protocols", Proceedings of the 8th KIIT IT based Convergence Service workshop & Summer Conference, Mokpo Maritime University (Mokpo, Korea), ISSN -7334, pp. 23.

Robles, R. J., Choi, M.K. and Kim, T. H. 2005. "The Taxonomy of SCADA Communication Protocols", Proceedings of the 8th KIIT IT based Convergence Service workshop & Summer Conference, Mokpo Maritime University (Mokpo, Korea), ISSN -7334, pp. 23.

Robles, R. J., Seo, K.T. and Kim, T. H. 2010. "Communication Security solution for internet SCADA", Korean Institute of Information Technology 2010 IT Convergence Technology - Summer workshops and Conference Proceedings, May, pp. 461-463.

Wallace, D. 2003. "Control Engineering. How to put SCADA on the Internet",, http://www.controleng.com /article/ CA321065.html.

****