American Journal of Applied Sciences 11 (8): 1418-1425, 2014
ISSN: 1546-9239

doi:10.3844/ajassp.2014.1418.1425 Published Online 11 (8) 2014 (http://www.thescipub.com/ajas.toc)

THE SCADA REVIEW: SYSTEM COMPONENTS, ARCHITECTURE, PROTOCOLS AND FUTURE SECURITY TRENDS

[1]Shahzad, A., [1]S. Musa, [1]A. Aborujilah and [2]M. Irfan

[1]Malaysian Institute of Information Technology (MIIT), University Kuala Lumpur, Malaysia
[2]Windfield College, Kuala Lumpur, Malaysia

Received 2014-01-15; Revised 2014-05-13; Accepted 2014-05-27

ABSTRACT

The Supervisory Control and Data Acquisition (SCADA) system has prominent place and play important roles within real time industrial communication included “electric stations, oil stations and water purification plants”. In this study; the SCADA System main components, architecture and important protocols, which have been used in SCADA message transmission are reviewed. After review, the current research changes the direction (Section: Future Work) to the security of SCADA system and the existing methods or security methods that have been deployed within the SCADA system. This review also gives directions to secure SCADA network communication.

Keywords: Supervisory Control and Data Acquisition (SCADA) System, Protocols, Security Trends

1. INTRODUCTION

1.1. SCADA System Components

The SCADA system is based on hardware included “Master Terminal Unit (MTU), Remote Terminal Units (RTUs)” or/and actuators and sensors and software included Human Machine Interface (HMI) or other user software that provides communication interface between SCADA hardware and software. Human Machine Interface (HMI) also provides facility to visualized entire SCADA communication included controlling and monitoring. Master Terminal Unit (MTU) is located at control center or perform the services of control station and connected with one or more Remote Terminal Units (RTUs), that may geographically distributed over remote sites (wide area network) or within Local Area Network (LAN) using communication link/media such as radio signals, telephone line, cable connection, satellite and micro waves media. Typically, physical environment is connected with actuators or/and sensors and actuators/sensors are connected with Remote Terminal Units (RTUs). The RTUs have been collecting data/information from actuators/sensors and then process to Master Terminal Station (MTU) for monitoring and controlling the entire SCADA system. Usually, SCADA system is divided into five main components/parts (illustrated in **Fig. 1**) “included Master Terminal Unit (MTU), Remote Terminal Unit (RTU) and Human Machine Interface (HMI) historian” and SCADA communication media or link (Stouffer and Kent, 2006; Musa *et al*., 2013b). More detail related with SCADA components is following below.

1.2. Master Terminal Unit (MTU)

The center controller or master terminal unit is may form of a server (computer) or/and group of sub servers connected directly or indirectly with main server, through communication link such as “Local Area Network (LAN) or/and Wide Area Network (WAN)”. Human Machine Interface (HMI) is typically installed in Master Terminal Unit (MTU) or control center and provide facility to visualized the information coming from remote terminal units. The information is displayed in understand able form such as in the form of textual and graphical, that will easily understood able for SCADA user/operators during communication.

Corresponding Author: Shahzad, A., Malaysian Institute of Information Technology (MIIT), University Kuala Lumpur, Malaysia

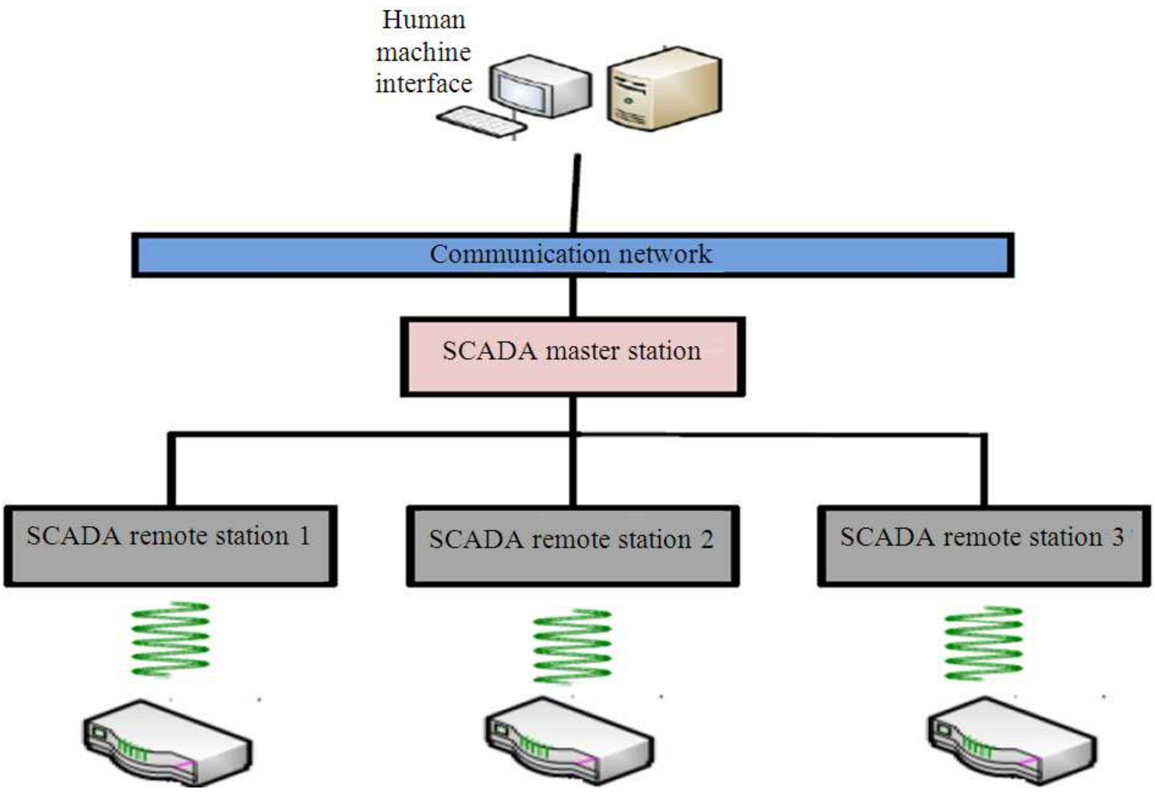

Fig. 1. SCADA communication component

So, each user terminals or sub terminals will visualize associated information on display screen by connected with main server through communication media.

Few years before, SCADA system has many incompatibilities in the terms of software/hardware connectivity and information/data visualization, but with great revolution in DCS (distributed control system), now SCADA provides high resolution display (screen). Therefore, SCADA operators can easy view the site map or remote station operational view in high resolution and also successfully resolved the compatibilities issues during hardware/software configuration and installation. So, any SCADA software/hardware will easily install and operate, while connecting with simple server (computer) included home computer or office computer having Microsoft windows (XP, window 7 or 8).

With the SCADA advance software compatibilities and connectivity, open new ways to install SCADA system applications included SCADA modeling and simulation application, hydraulic modeling, geographical information system, drawing applications and data bases within a single computer as home or office computer (Stouffer and Kent, 2006; Musa *et al*., 2013b). Main services performed by Master Terminal Unit (MTU) are follows below:

- Monitor and control entire SCADA communication through communication link such as LAN/WAN (radio signals, telephone line, cable connection, satellite and micro waves media)
- Using human machine software; visualized the data/information related with SCADA communication in the forms of text and graph
- Send request data/message to RTUs included current status of RTUs, information collection from RTUs, check communication link and upon receiving information/data from RTUs, perform acquisition

1.3. Remote Terminal Unit (RTU)

Substations or Remote Terminal Units (RTUs) are act as slave stations in SCADA architecture. Typically, Remote Terminal Units (RTUs) are connected with physical environment through actuators or sensors. RTUs have been collecting real time information from sensors and transmit back to master terminal station, usually depend upon the request send from master station. In few cases, remote terminal station is also able to send request to master station such as in case of disaster, disaster recovery, actuators or sensors functions off and other critical issues. Main services performed by Remote Terminal Unit (RTU) are follows below.

Remote terminal stations are responsible to collect information/data from sensors or actuators that are connected with physical environment and process information back to master station (depending on master request).

Remote Terminal Units (RTUs) are geographically distributed over different sites, collecting and processing the real time information to master station using link LAN/WAN (radio signals, telephone line, cable connection, satellite and micro waves media,). Remote Terminal Units (RTUs) are also responsible to deliver the current status information of physically devices connected with network included devices are configured properly and working (operation) in right directions (Stouffer and Kent, 2006; Musa *et al*., 2013b).

1.4. Human Machine Interface (HMI)

Human Machine Interface (HMI) or SCADA user interface is most important part of SCADA system. This provides interface between hardware and software within SCADA communication. SCADA system deployment and performance are depending on software (Human Machine Interface) specifications such as testing, checked and compatible with numbers of nodes within SCADA network. Usually, Human Machine Interface (HMI) has been designed according to SCADA network structure needs and specification. Some proprietary software’s are available (in market or online) and uses for specific SCADA hardware configuration. Often does not provide interface or compatibilities for other vendors”hardware”. Commercial “Off-The-Shelf (COTS) products are available and provide flexible and compatible interface between several types of SCADA hardware and software. Usually, proprietary software’s are based on SCADA processes and controlling operations, while software’s such as Commercial Off-The-Shelf (COTS) are based (focusing) on several types of SCADA compatible hardware’s or equipments and Instruments. Therfore, COTS are more flexible and reliable in hardware compatibilities as comparison with proprietary software. As conclusion; must be ensuring that which of software is appropriate for SCADA system design that compatible with hardware, while installation of new system (Stouffer and Kent, 2006; Musa *et al*., 2013b). Main services performed by Human Machine Interface (HMI) are follows below:

- Provide interface for SCADA communication between hardware and software
- Display all SCADA operational information such as controlling and monitoring and communication status between Master Terminal Unit (MTU) and Remote Terminal Units (RTUs) or/and Remote Terminal Units (RTUs) and Master Terminal Unit (MTU) in the form textual or graph or/and other human readable text
- Also provides conversion between several data types such as analog to digital, digital to analog, digital/analog to human readable text and text to digital/analog

Some of typical software's uses by SCADA system (Stouffer and Kent, 2006) are following below:

- “Master station (computer) operating node” is based on UNIX platform and uses for controlling master station hardware
- “Terminal station operating node” is uses for controlling terminal station hardware and usually, master station operating node functionality is same as terminal station operating node
- “Master station software (Application)”; provides user interface or graphical user interface and operate/control “communication between master terminal unit (MTU) and Remote Terminal Units (RTUs) or/and Remote Terminal Units (RTUs) and Master Terminal Unit (MTU)”. At other side, “Terminal station software (Application)”, is basically part of master station software and used to access information/data, that is available on master station software (Application)
- “Protocol drivers” are usually situated in both master station and terminal station communication and used to control data translation and interpretation “between Master Terminal Unit (MTU) and Remote Terminal Units (RTUs) or/and Remote Terminal Units (RTUs) and Master Terminal Unit (MTU)
- “Tool for network management” is used for SCADA network communication control and monitoring purposes such as checking the network performance results. At other side, “Automation tools for remote terminal station” is uses by SCADA operators to make configuration and maintain remote terminal station applications

1.5. Historian

The term historian is used to store incoming and outgoing processing/processes from/to SCADA control center. Historian is just same as database, which is centralized located within SCADA server or/and as separate located server (database server). All communication such as monitoring and control information "between Master Terminal Unit (MTU) and Remote Terminal Units (RTUs) or/and Remote Terminal Units (RTUs) and Master Terminal Unit (MTU)" have been stored within historian. SCADA system will fetch information from historian according to the requirements of process being executed include information/data analysis, report generationand time management of storage between processes and query generation and execution, (Stouffer and Kent, 2006; Musa *et al*., 2013b).

1.6. SCADA Communication

The communication network provides services for communication between nodes in SCADA network system. Using transmission medium facility; data/message has been able to transmitted "between Master Terminal Unit (MTU) and Remote Terminal Units (RTUs) or/and Remote Terminal Units (RTUs) and Master Terminal Unit (MTU)" included radio signals, telephone line, cable connection, satellite and micro waves media. Cable connection is uses for small type of networks usually, within industry or small industry, because this connection is inconvenient for large distance. With the growing demand of industry and larger connectivity of SCADA nodes with LANs/WANs; based on network demands powerful radio signals, satellite and microwaves media have been often used for SCADA communication.

Usually, SCADA system uses "point to point or PTP, point to multipoint or PTM" and multipoint to multipoint or MTM topologies and communication procedures included half-duplex and full-duplex for communication (Stouffer and Kent, 2006; Musa *et al*., 2013b).

2. SCADA COMMUNICATION ARCHITECTURE

Traditionally, SCADA systems have been connected within limited networks but growing demand of SCADA over the world and uses of modern networks architectures, SCADA also replace from Monolithic to Networked. SCADA communication architecture is usually divided into three main generations such as First Generation: Monolithic, Second Generation: Distributed, Third Generation: Networked. More detail related with SCADA system generation is following:

2.1. First Generation: Monolithic

First generation of SCADA architecture development was based on idea similar with main frame system. Mean that network communication was not exit at all and each station was worked as single centralized station. More detail related with first generation of SCADA system is following below:

- The concept of Wide Area Network (WAN), for connectivity between master station and remote station was developed (concept based on remote terminal communication in SCADA field only) and WAN protocols (current protocols) were unknown in first generation
- Few proprietary protocols were developed for SCADA communication with limited functionalities; that don't fulfill the requirements of communication such as infeasible for handling several traffic communications with remote station over network
- Field devices connectivity with the master station was fairly limited and deployed at bus level using proprietary. Primary and backup systems were used for the purposes of limited redundancy check and monitoring and failure detection or event operations were performed by standby system

2.2. Second Generation: Distributed

The significant improvements have been done in second generation and several processes were distributed across stations within Local Area Network (LAN). Each station has specific operation/function and send/receive real time information/data between the stations connected within LAN. More detail related with second generation of SCADA system is following below:

- In distributed environment, some of stations are uses for communication such as master station communication with the remote stations and other stations utilized as human machine interface or HMI for monitoring and controlling purposes and remaining uses for database/historian storage
- Usually, LAN protocols have been used for communication between the nodes within distributed

environment, where the functions have been resisting as distribution of SCADA system function across several multiple systems

- Distribution of SCADA functionalities across several systems connected within LAN, would increase processing power and improve the system redundancy and reliability
- The system failure ratio in second generation will deceased while comparison with first generation. In first generation; only one primary station was used but in second generation all stations are communicating simultaneously within LAN. If one of system fails with network, then other stations are still in processing states
- Wide Area Network (WAN) technology has been also deployed and used for "communication between master station and remote station or/and remote station and master station" WAN communication is fairy same as current technology (LAN/WAN), but communication functions were limited for remote station protocols usage such as incompatible/unavailability for several network traffic (Stouffer and Kent, 2006)

2.3. Third Generation: Networked

Third generation of SCADA is approximately same as second generation architecture but difference in architecture uses. Current generation uses open architecture but second generation was based on proprietary architecture. More detail related with Third generation of SCADA systems is depicted below.

Like second generation; master station is centralized and accessible from several remote stations, several networks are deployed for communication and single application functions are distributed/share between several types of systems in SCADA network architecture and proprietary protocols are also used by remote stations to communication with master station.

Current generation has been deployed open architecture for SCADA communication across LANs/WANs by using several types of open standard protocols. These open standards completely minimize the limitations suffered by SCADA communication in second generation and open new ways to connect several types of input/output devices or off-the-shelf systems with SCADA network.

The main development done in third generation is uses of WAN technology for SCADA network using Internet Protocol (IP) or/and Transport Control Protocol (TCP). SCADA uses TCP/IP for communication between the fields devices which are located across multiple stations. Few companies, also developing Remote Terminal Units (RTUs) to communicate with master station through Ethernet.

SCADA distribution system over WAN, functionalities also enhanced in this generation. SCADA operations are distributed across several physical stations through WAN for the purposes of disaster issues handling and provides more reliability and scalability. If any station crash or fail, this will not effect on entire SCADA system because replicated copies are store over several locations. In second generation, SCADA processing were distributed across several systems within LAN for increases the reliability in communication. But if master station fail/crash or/and LAN connectivity fail, this was affect the entire SCADA system. SCADA system connectivity with several types of protocols and networks over internet; make SCADA system more vulnerable from several types of attacks and threads (Stouffer and Kent, 2006).

3. SCADA COMMUNICATION PROTOCOLS

"The SCADA system communication between Master Terminal Unit (MTU) and Remote Terminal Units (RTUs)" are implemented by uses of SCADA protocols. Each SCADA protocol provides rules and procedures of communication between field devices and other functions included MTU/RTU command generation, MTU/RTU status information, data/information accumulation, data presentation and conversation, assignment of MTU/RTU addresses, system monitoring and controlling. Usually, each SCADA protocol is proves two types of communication ways/sets. Fist communication set; is used by master station, to initial the communication with allocated Remote Terminal Units (RTUs) and further response back to Remote Terminal Units (RTUs). Second communication set; is used by remote station, to initial the communication with allocated Master Terminal Unit (MTU) (in few critical cases, Remote Terminal Units (RTUs) are also able to send response or unsolicited response to master station) (Reynders *et al*., 2004; Krutz, 2005).

Some of most famous/popular protocols used within SCADA communication (industrial communication) are following below.

3.1. Modbus Protocol

SCADA system uses Modbus protocol for application layer communication or real time communication over OSI layer seven between field devices connected with several network lines. Basically; Modbus protocol has been provided architecture of master station/remote station communication for the purposes of message/data request/response to/from master station and remote station. Modbus has been used four types of communication modes between master station and remote station communication such as request message to master station, response message from master station, message/process acknowledgment or confirmation (upon message received by remote station) and master station received request message from remote station. Usually, Modbus protocol is provides communication services "between Master Terminal Unit (MTU) and Remote Terminal Units (RTUs) or/and Remote Terminal Units (RTUs) and Master Terminal Unit (MTU)" or/and between fields devices and Human Machine Interface (HMI).

In SCADA system, when remote station initial the communication and send request message to master station Modbus protocol will assemble this message (request) from remote station into Protocol Data Unit (PDU), usually PDU is combination of Function Code (FC) and data request, or by adding function code with requested data, also known as Protocol Data Unit (PDU). By addiang fields at OSI layer 2, the constructed Protocol Data Unit (PDU) will convert into an Application Data Unit (ADU). Upon receiving, master station will generate the request message and then send back to remote station.

Traditionally, Modbus protocol is uses RS-232/485 or other modem for serial communication between master station and remote station, but uses of TCP/IP protocol with modbus, a new layer has been established for modbus message transmission (PDU encapsulation), over "transport control protocol/ internet protocol or TCP/IP and Ethernet" (Reynders *et al*., 2004).

3.2. DNP3 Protocol

In terms of SCADA communication, "Enhanced Performance Architecture (EPA) model is simplified form of OSI seven layer "model". The International Electro Technical Commission (IEC) creates the EPA model and DNP protocol is based on EPA model.

Distributed Network Protocol (DNP3) is one of important open protocol has been used in SCADA communication between master terminal station and remote terminal stations or out stations. Usually master terminal station initial the command or send data/message to remote terminal station and remote terminal station response according to master terminal station request. DNP protocol is used for serial or Internet Protocol (IP) communication between master terminal station and remote terminal stations (Shahzad *et al*., 2014a). Using TCP/IP protocol, DNP3 provides communication over internet between devices connected in Wide Area Networks (WAN) and DNP3 protocol is situated above than TCP/IP protocol suite in communication hierarchy for fairly communication over internet (Reynders *et al*., 2004; Musa *et al*., 2013a; 2013b).

3.3. IEC 60870-5 Protocol

In SCADA system, "Enhanced Performance Architecture (EPA) model" is a simplified form of OSI seven layer model. The "International Electro Technical Commission (IEC)" has been developed the EPA model and "IEC 60870-5-101 protocol" is also based on EPA model. Usually, one special purpose layer is added on the top of EPA model, known as application layer. This user layer is specify the functions and operations related with telecontrol system and provides interaction between SCADA field devices, which are fully supported with telecontrol system.

Several frame formats and services are specified for each layer in IEC 60870-5 protocol and several functions are also defined for user program (layer), located between application layer (OSI model) and user interface. According to the needs of protocol enhancement within SCADA industry, IEC 60870-5-101 protocol standards will also change from 60870-5-101 to 60870-5-104 or telecontrol standard profiles (such as T101, T102, T103, T104). Each protocol standard define different specifications, data objects and functions codes at application protocol level within SCADA communication system.

International Electrotechnical Commission (IEC) has been developed first complete protocol known as 60870-5-101 for SCADA communication, that fulfill the all necessary requirements, included define data objects and functions, across geographical area, through Wide Area Network (WAN) technology. 60870-5-101 protocol also specifies the basic requirements such as generic data types and general services for remote stations. Usually, standards 60870-5-101 to 60870-5-103 are uses for electrical industries operation, while standard 60870-5-104 also provides services for SCADA communication, through Transport Control Protocol (TCP) and Internet Protocol (IP) by adding two additional layers such as transport and network layer of OSI seven layer model (Reynders *et al*., 2004).

3.4. Profibus Protocol

Profibus is stand for "process field bus". Profibus is network standard usually, uses within industrial control systems such as SCADA, DCS and PLC, Including Controlling, assembling and handling of field devices (ICS). Profibus has been mostly used in Europe and also famous in other continent of world, included Asia, America and Australia, Profibus is supported, communication between fields devices (with bus controller/access) or "between Master Terminal Unit (MTU) and Remote Terminal Units (RTUs) or/and Remote Terminal Units (RTUs) and Master Terminal Unit (MTU)", with some specifications (requirements) such as connector type D, 127 point, 24 km distance (supported), speed up to 12 Mbps and message size up to 244 bytes per node (Reynders *et al*., 2004).

Typically, Profibus protocol have three version such as Distributed Peripheral (DP), Field bus Message Specification (FMS) and PA. More detail is given below.

In Distributed Peripheral (DP), master station takes request message (read input) from remote station and then generate response message (write information) back to remote station. Distributed Peripheral (DP) is also supported, more than one master station (multiply stations) read information/data from field devices and then main controller (master) will able to send response back to remote station.

Field bus Message Specification (FMS), only support peer-to-peer communication between master stations; such that each master station is authorized to send/receive message from other master stations within communication system. FMS communication (message) has contained more loads as comparison with DP communication.

When FMS and DP versions are used simultaneously within one network, than called COMBI mode. The PA protocol working is same as Distributed Peripheral (DP), only has difference in voltage level.

Profibus protocol is also based on OSI model seven layer, with extra layer on the top of OSI model, known as called application layer. Data link layer has same specification for FMS, DP and PA (Profibus variations), while IEC 61158-2 standard is uses by PA and RS-485 is uses by DP and PA as physical layer implementation (Reynders *et al*., 2004).

3.5. Foundation Fieldbus

Foundation Fieldbus has four layers such as "user layer, application layer, data link layer, physical layer" within protocol stack and these all layers are based on OSI seven layer model, with extra layer on the top of OSI model known as called user application layer. Which provides specific (standard) user interface between software and fields devices. Fieldbus has number of benefits/advantages, while connecting with modern or smart field devices and communication networks, included easy processes integration, decrease heavy wire cost,session minimized, enhancement in field devices control and monitoring, multifunctional devices, open standard and interoperability among vendors, enhancement in data integrity and availability.

Another achievement of Fieldbus is HART (Highway Addressable Remote Transducer) Protocol, which is supported both analog and digital communication of industrial processing and automation. The most important advantage of HART protocol is same existing wiring 4-20 mA structure is used for receiving both analog and digital information on same cable (Reynders *et al*., 2004).

3.6. Modbus Plus Protocol

Modbus plus Protocol is based on standard Modbus protocol limitation. Modbus plus protocol (not open standard) is designed to overcome the master station limitation over modbus protocol, such that field devices connectivity with master station through several modbus networks or networks. Modbus plus is "token" base protocol and allow the field devices to exchange information/data from master station and master station is also able to control and monitor all communication at remote site. The network addresses range 1--64 are utilized and each field device has its own unique address. Each field device is able to communicate with other device in network, with specified route as information inside message. Mostly, Modbus II is not used within real time communication, because of extra wire (cable) and other difficulties related with communication (Reynders *et al*., 2004).

3.7. Data Highway Plus/Dh-485 Protocol

Allen Bradley uses three main protocol standards such as the highway protocol, the highway plus protocol and DH-485 for communication. The highway protocol provides peer-to-peer half duplex communication within Local Area Network (LAN) and systems range and data rate are up to 64 nodes and 56.7 Kbaud.

The highway plus protocol communication is same as the highway protocol, with limitation of systems and utilization of token system, also called floating master. The highway plus protocol also utilize three layers such as application layer, data link layer, physical layer) of OSI model. DH-485 is a proprietary protocol and provides communication between system (computer) and field devices within local area network, with RS-485 support medium (Reynders *et al*., 2004).

4. CONCLUSION

In this study, the SCADA system details included the components "such as Master Terminal Unit or MTU, Remote Terminal Unit or RTU, Human Machine Interface or HMI, Historian and SCADA Communication", the architecture "such as First Generation: Monolithic; Second Generation: Distributed; and Third Generation: Networked" and the important protocols "such as Modbus Protocol, DNP3 Protocol, IEC 60870-5 Protocol, Profibus Protocol, Foundation Fieldbus, Modbus Plus Protocol and Data Highway Plus/DH-485 Protocol" with their specifications, which are using in current age, have been reviewed.

5. FUTURE WORK

Several generic security solutions included SSL/TSL, TCP, IPSec, security pattern and most important cryptography have been deployed in the area of Industrial control systems or ICSs security and implementation. Almost, all solutions are based on end-to-end communication and provide security mechanisms for SCADA system protection are also based on end-to-end.

After conducting and analyzed; the detail literature survey on SCADA/protocols security issues and its potential vulnerabilities (Shahzad *et al*., 2013; 2014b; Musa *et al*., 2013a), a solution has been proposed to secure the SCADA communication, by deploying cryptography solution within Distributed Network Protocol version 3 (DNP3) and/or other SCADA protocols as part of Industrial Control Systems (ICSs).

6. ACKNOWLEDGMENT

I would like to thank to my parents and my friend, M. Irfan boosted me morally and provided me great information resources.

7. REFERENCES

Krutz, R.L., 2005. Securing SCADA Systems. 1st Edn., illustrated, Hoboken, John Wiley Publishing, ISBN-10: 047178768X, pp: 218.

Musa, A.S., A. Shahzad and A. Aborujilah, 2013a. Simulation base implementation for placement of security services in real time environment. Proceedings of the 7th International Conference on Ubiquitous Information, (CUI' 13), New York, USA, DOI: 10.1145/2448556.2448587

Musa, A.S., A. Shahzad and A. Aborujilah, 2013b. 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 on Ubiquitous Information Management and Communication, (IMC' 13). DOI:10.1145/2448556.2448588

Reynders, D., S. Mackay and E. Wright, 2004. Practical Industrial Data Communications: Best Practice Techniques. 1st Edn., Butterworth-Heinemann, Elsevier, ISBN-10: 0080480136, pp: 432.

Shahzad, S., A. Aborujilah, M.N. Ismail and M. Irfan, 2013. Conceptual model of real time infrastructure within cloud computing environment. Int. J. Comput. Networks, 5: 18-24.

Shahzad, S., A. Aborujilah, S. Musa and M. Irfan, 2014a. Industrial Control Systems (ICSs) vulnerabilities analysis and SCADA security enhancement using testbed encryption. Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication, (IMC' 14), New York, USA. DOI: 10.1145/2557977.2558061

Shahzad, S., A. Aborujilah, S. Musa and M. Irfan, 2014b. A new cloud based supervisory control and data acquisition implementation to enhance the level of security using testbed. J. Comput. Sci., 10: 652-659. DOI: 10.3844/jcssp.2014.652.659

Stouffer, J. and K. Kent, 2006. Guide to Supervisory Control and Data Acquisition (SCADA) and industrial control systems security. Recommendations of the National Institute of Standards and Technology.