International Journal on
"Technical and Physical Problems of Engineering"
(IJTPE)
Published by International Organization of IOTPE

ISSN 2077-3528
IJTPE Journal
www.iotpe.com
ijtpe@iotpe.com

December 2019 | Issue 41 | Volume 11 | Number 4 | Pages 22-27

DUAL CHANNEL SCANNING IN COMMUNICATION PROTOCOL IN INDUSTRIAL CONTROL SYSTEMS FOR HIGH AVAILABILITY OF THE SYSTEM

L. Rajesh P. Satyanarayana

Department of Electronics and Communications, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Andhra Pradesh, India, locharalarajesh@gmail.com, satece@kluniversity.in

Abstract- Now a days Industrial Control Systems (ICS) plays a very important role in process plants or Critical Infrastructures. An ICS system used for monitoring and controlling a process plant or a pipeline or an industry. Basically, it consists of an intelligent device like PLC (Programmable Logic Controller) or RTU (Remote Telemetry Unit) for scanning the field sensor devices and a server to process the data and an MMI system to display the data on a Graphical User Interface (GUI) in different ways like alarms, trends, and reports. All RTUs will be connected to Master Station through Optical Fiber Communication (OFC) and scanning using communication protocols like MODBUS, DNP (Distributed Network Protocol), IEC 101/104 protocol. Each RTU will have two communication channels for providing redundant connectivity to Master Station. But both these channels will be connecting to a single aster station. If there is a break in OFC communication after some Intermediate Station or repeater station in the pipe line network, then all RTUs will be failed state and data from the field will not be available at the Master station after that particular station. To resolve this condition or problem, dual master stations with multiple scan paths will be proposed to enhance the redundancy of scanning through Master control station and hence the availability of the SCADA system increased.

Keywords: SCADA, RTU, PLC, Communication Protocol, MODBUS, DNP, Master Station.

I. INTRODUCTION

Industrial Control Systems (ICS) are using for monitoring and controlling various critical infrastructures. SCADA systems are generally used in ICS systems. SCADA stands for supervisory control and data acquisition which is used for monitoring and control of a process plant like pipeline operations or industry to reduce manual intervention and speed up the activities and increase production efficiency [1]. It consists of servers, PLCs, RTUs, HMI (Human Machine Interface) systems, routers, and other network elements. It can be used for all types of industry which require automation like Oil & Gas, Steel, Power generation & transmission, cement factories, etc. Intelligent SCADA is required for secure operations of power plants [2]. In recent years smart grid is the new concept for reliable and quality distribution of power [3]. Using SCADA the plant can be run with high efficiency, productivity with safe & secure operations [4]. Various protocols will be used for scanning the RTUs/PLCs from SCADA Servers. Different types of instruments will be connected to PLC/RTU. Now a day SCADA data can be displayed on web or mobile applications also. SCADA data can be displayed in various forms like graphics, reports, trends, alarms, etc. [5].

The SCADA data can be used for higher levels of management like Enterprise Resource Planning (ERP) etc also. This data can also be used for further processing for applications like leak detection, batch tracking, pig tracking in pipeline applications, islanding in level two automation in steel plants and smart grid automation in power sector applications [6]. The SCADA systems are vulnerable to security attacks [7]. The system should be protected from attacks for integrity, confidentiality, availability of the system. The availability of the system is one of the key parameters for the performance of SCADA systems [8].

II. SCADA SYSTEM COMPONENTS

A SCADA system contains the following components in the network [4].

A. Filed Instruments

Field instruments are basically transducers or sensors, used for measuring the field values like pressure, flow, density, etc. These devices convert the physical quantity to electrical quantity and send the data to PLC/RTU. Monitoring and maintaining process variables at the appropriate levels is extremely critical in industrial automation and process control. A sensor in the industrial environment is either continuously or periodically measuring critical parameters such as density, temperature, pressure, flow, etc. The primary challenge of sensing in industrial environments is conditioning low signal levels in the presence of high noise and high-surge voltage [9].

B. RTU or PLC

Programmable Logic Controller or Remote Telemetry Unit used for scanning the I/O and executing interlocks and logics for industry field operations. The basic units have a CPU (a computer processor) that is dedicated to run one program that monitors a series of different inputs and logically manipulates the outputs for the desired control. They are meant to be very flexible in how they can be programmed while also providing the advantages of high reliability compact and economical over traditional control systems. The I/O system provides the physical connection between the equipment and the RTU/PLC. The PLC/RTU will be connected to main SCADA Server through LAN or WAN. The PLC/RTU will have a communication module for interfacing with SCADA Server through Serial or Ethernet communication [10].

C. DAQ Servers and IT Hardware

SCADA Server will be used for processing the received data from PLC/RTU and logging of the data for further future analysis. The Client will be used to display the data in different formats and sending the controls to PLC/RTU. SCADA package will be loaded in Server and protocol driver like MODBUS, DNP will be running in this server [11]. The main functionality of SCADA Servers is scanning the RTUs, time synchronization, database management, alarms triggering, report generation, control command execution, etc. [12].

D. Network Components

The network consists of Lan switches to connect the various nodes. Routers also are used for WAN interface i.e. to connect various stations. Redundancy is an important factor in SCADA networks. In pipeline applications, the RTUs are geographically spread throughout the pipeline. Optical Fiber Communication will be used for bi-directional data transfer between main master station and RTUs.

III. EXISTING SINGLE MASTER STATION

We took pipeline application project as an example where SCADA will be used [13]. In pipeline automation, SCADA system is using for safe and secure operations of oil and gas product dispatch and delivery. The main master station will be residing at one place and RTUs will be distributed along the pipeline to cater the control operations. All RTUs will be connected to local communication panel and will be connected to master station though OFC communication [14]. Each RTU will have two communication paths. They are called Port A and Port B. The RTUs will be polled by DNP protocol and data will be exchanged between SCADA Server and RTU using this protocol. Each RTU will have dual power supplies, CPU card, and communication module. Figure 1 displays the normal connectivity without multiple path scanning and DMS concept. One SCADA Server and One MMI were connected in dual LAN and the two LANs are connected to a Router for WAN interface. Two RTUs are connected in the network. The scanning methodology will be as follows:

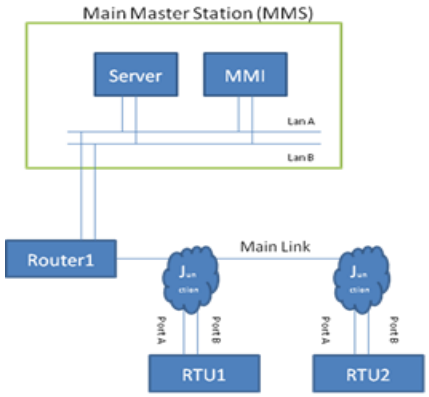

Figure 1. Single master station with dual channels

A. The communication channel is healthy between RTU and Main Master Station (MMS)

The Master SCADA Server will poll the RTU through Port A of the RTU.

B. When there Is a Break in Port A

If the communication between SCADA Server and RTU Port A failed because of cable problem or communication channel problem or RTU module problem, the SCADA Server starts polling through Port B using OFC or Back Up Communication Link.

C. When There Will Be Total Communication Break between SCADA Server and RTU

But if there is a total communication break between SCADA Server at MMS and RTU, there was data loss and SCADA Server cannot monitor or control the field after that affected RTU. Figure 2 shows the failed condition. There is a total communication break after RTU1 and before RTU2. SCADA Server cannot connect RTUs after RTU1. There is no connectivity between RTU2 and SCADA Server at MMS. If there is break between RTU1 and RTU2 locations, then RTU 1 will be polled by MMS Server but there was no connectivity between RTU2 and MMS Server. The Server cannot get data from RTU2 and cannot monitor and control the pipeline after RTU2 locations. This is the problem with existing or old architecture. To resolve this condition multiple scan paths with dual master station support is proposed. This will increase the redundancy of the master station and system availability. Each RTU has two paths to reach MMS i.e. one path directly MMS connectivity and another path connects MMS through DMS (Dual Master Station). MMS and DMS also connected by two redundant paths i.e. OFC and back up link secured MPLS/VPN dedicated line.

IV. MULTIPLE SCAN PATHS WITH DUAL MASTER SUPPORT

Each RTU was configured with two numbers of communication ports. One port was configured to communicate with Main Master Station (MMS) in one direction and the other was configured to communicate with the RTU in the second direction. Communication channel switch over of an RTU occurs if:

a) The corresponding communication port fails or when there is a failure in the communication path to reach that port.
b) Operator request.

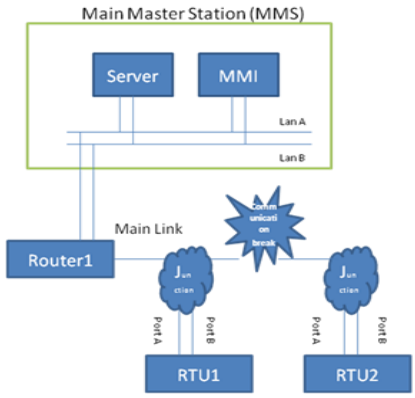

Figure 2. Communications break after RTU1 in the network

We installed another Master station at other end of the project set up and is called Emergency Master Station (EMS) or Dual Master Station (DMS) and it was normally in slave mode to master station i.e. if RTU is healthy and communicated to Main master station, then this DMS will be running in slave mode i.e. sit idle. The MMS and DMS were connected by WAN routers by two paths one is OFC and another one is Back Up communication link (BCL). The connectivity diagram was shown in Figure 3. For Lab Test purpose the two paths were connected using two back to back LAN cables only. One number of SCADA servers and a MMI connected in MMS. One window-based SCADA server and an MMI connected in DMS. Two RTUs were connected in the network. Now we will see the failed conditions.

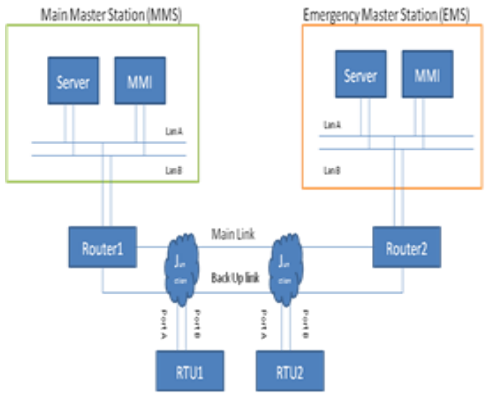

Figure 3. Multiple paths between MMS and DMS

A. Communication Is Healthy

It the communication between the RTU and Main master station is healthy then the RTU was polled with Port A only. Port B was communicated to DMS and only health messages were transferred. Generally, Port A will be high priority path due to high bandwidth provided by OFC.

B. Communication Breaks between Port A of RTU and MMS

If there is a break between Port A of RTU and MMS due to communication module of RTU or OFC break or WAN router failure, then MMS sent the port A fail message to DMS. Then DMS started the polling to the effected RTU and sent the data to MMS through OFC line.

C. Communication Break between Port A of RTU and MMS and OFC Failure between DMS and MMS

If there is a break between Port A of RTU and MMS due to communication module of RTU or OFC break or WAN router failure, then MMS sent the port A fail message to DMS. Then DMS started the polling to the effected RTU and sent the data to MMS through Back Up Link.

D. Total Communication Break between MMS and DMS

If there was a total communication break between MMS and DMS, then the RTUs which were accessible to MMS were polled by the MMS Server. The RTUs which were not accessible to MMS but accessible to DMS were polled by DMS Server. DMS Server identified the total commendation break between MMS and DMS and started scanning the available RTUs. The data was processed by DMS Server and displaced on MMI which were connected to it. The logged data was stored in DMS Servers in form of files and sent to MMS after communication restoration, for maintaining proper synchronization of data and used for leak detection and other upper layer applications [5].

V. CALCULATION OF SYSTEM AVAILABILITY

High availability can be achieved by fault-tolerant systems. The term fault tolerant means a system can work in the presence of hardware component failures. A single component failure in a fault-tolerant system should not make a system interruption because the alternate component will take over the task transparently [15]. Generally, the availability of the control system will be mentioned in %. For example, if plant availability is mentioned as 99%, the system is not available for 3.65 days out of 365 days in a year.

Availability is generally measured by uptime ratio which represents % of time the system is available.

$$\text{Downtime Per Year } (\text{minutes}) = \\ = (1 - \text{Uptime Ratio}) \times 365 \times 24 \times 60 \quad (1)$$

Equation (1) represents another way to represent the system availability in % of downtime [16]. Table 1 describes the % availability and corresponding down time in days and hours per year using Equation (1) [15]. For example, 99.9% availability represents

$$(1 - 99.9/100) \times 365 \times 24 = \\ = 8.76 \text{ hours} = 8 \text{ hours}, 45.6 \text{ min}$$

Table 1. Availability % in terms of days and hours

Availability in %	Downtime in annual
90%	36 days, 12 hours
99%	87 hours, 36 minutes
99.9%	8 hours, 45.6 minutes
99.99%	52 minutes, 33.6 seconds
99.999%	5 minutes, 15.4 seconds
99.9999%	31.5 seconds

The availability can also measure by below described Equations (2) or (3) [16]:

$$Availability\ of\ the\ System = \\ = time(up)/(time(up)+time(down)) \quad (2)$$

$$Availability\ of\ the\ System = (MTBF)/(MTBF+MTTR) \quad (3)$$

where, *MTBF* = Mean Time Between Failures and *MTTR* = Mean Time to Repair.

The availability of the system can be calculated by down time and uptime as shown in Equation (2). The same can also calculated using Equation (3). Availability of serial and parallel component blocks can be calculated as follows described in Equation (4) [17]:

$$A_{serial} = \prod_{i=1}^{n} A_i$$
$$A_{parallel} = (1-\prod_{i=1}^{n}(1-A_i)) \quad (4)$$

where, A_i is availability of *i*th device. Equation (4) can be useful for calculation of availability of a system contains several sub-blocks. We can use the below block diagrams for calculation of system availability for above system.

Figure 4 shows the block diagram for single master station and Figure 5 displays the block diagram used for calculation of system availability of dual master station. In DMS station the RTU contains two paths to SCADA Server for scanning or polling the data.

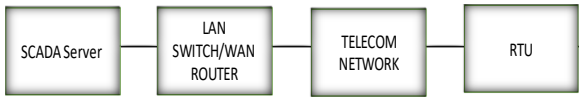

Figure. 4 Block diagram for single master station

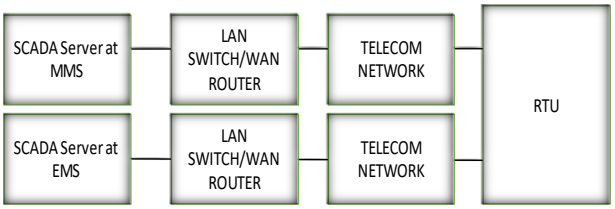

Figure. 5 Block diagram for dual master station

VI. RESULTS AND DISCUSSION

Using Equation (4), we calculated the availability of the control system with single master station and dual master station with dual scanning of RTU. Here we assumed system availability of SCADA Servers, LAN/WAN device is 99.95% and Telecom panel is 99%.

Anyhow these components are fixed on both the calculations it is not affect the calculations. We used above formulae for calculation of system availability. The results are tabulated in Table 2 and graphical form as shown in Figure 6.

Table 2 displays the % availability for single master station and dual master stations using various % of availability of components in the network. The same table can be represented as graphical form as shown in Figure 6. The graph is an x-y plot between components availability and Total system availability for SMS and DMS stations. For each pair of server availability and other components availability, the availability of DMS station is more than SMS station. From Table 2 and graph in Figure 6, it was concluded that dual master station achieves high availability than single master station.

Another advantage of high availability can be achieved by physical connectivity of the dual scanning paths. One of the connections can be connected in Path A direction and Second connection can be accessed in Path B through station B. It is required to provide same parameters on both the channels and paths.

As the DMS system has two parallel scanning paths between SCADA Server and RTU, it has high availability of the system. Hence the system is more reliable and safer for critical operations.

Table 2. System availability calculations

Server % Availability	Switch % Availability	Telecom % Availability	RTU % Availability	SMS % Availability	DMS % Availability
99.0000	99.0000	99.0000	99.0000	96.0596	97.0299
99.1000	99.1000	99.0000	99.1000	96.3510	97.2260
99.2000	99.2000	99.0000	99.2000	96.6430	97.4223
99.3000	99.3000	99.0000	99.3000	96.9355	97.6189
99.4000	99.4000	99.0000	99.4000	97.2287	97.8156
99.5000	99.5000	99.0000	99.5000	97.5224	98.0125
99.6000	99.6000	99.0000	99.6000	97.8167	98.2096
99.7000	99.7000	99.0000	99.7000	98.1117	98.4069
99.8000	99.8000	99.0000	99.8000	98.4072	98.6044
99.9000	99.9000	99.0000	99.9000	98.7033	98.8021
99.9500	99.9500	99.0000	99.9500	98.8516	98.9010
99.9900	99.9900	99.0000	99.9900	98.9703	98.9802

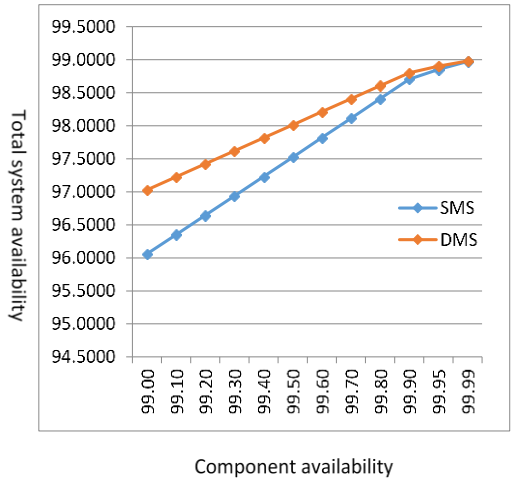

Figure 6. Graph between system availability versus component availability

VII. CONCLUSIONS

The availability of the control system for monitoring and controlling is very crucial parameter for safe and secure operations of the process plants. The system should available to the operators at 99.95%. The existing SCADA architecture does not provide dual master support and redundancy. Therefore, there was no monitoring and control of the plant if there was a total communication break between SV station and Master station (MMS). Using multiple scan methodology, there is a provision for dual master station and RTUs were polled to this master station whenever there was a total break in communication. All RTUs which are not accessible to main Master station (MMS) due to communication break were polled by this new emergency master station or Dual Master Station. The availability of system was enhanced and hence the safety & productivity will also be enhanced.

NOMENCLATURES

SMS	Single Master Station
SCADA	Supervisory Control and Data Acquisition
RTU	Remote Telemetry Unit
PLC	Programmable Logic Controllers
DMS	Dual Master Station
EMS	Emergency Master Station

ACKNOWLEDGEMENTS

The authors are very thankful to Koneru Lakshmaiah Education Foundation (Deemed) University, India to allow and conduct the research.

REFERENCES

[1] A. Daneels, W. Salter, "What is SCADA?", International Conference on Accelerator and Large Experimental Physics Control Systems, pp. 339-343, 1999.

[2] A.M. Hashimov, F.T. Rzayev, T.H. Dostalizade, "Intelligent Power Supply of Industrial Plants", International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue 12, Vol. 4, No. 3, pp. 149-151, Sep. 2012.

[3] H. Shelaf, H. Gozde, M. Ari, M.C. Taplamacioglu, "Investigation of Requirements Transform to Smart Grid", International Journal on Technical and Physical Problems of Engineering (IJTPE), Issue 24, Vol. 7, No. 3, pp. 27-31, Sep. 2015.

[4] J. Figueiredo, J. Sa da Costa, "A SCADA System for Energy Management in Intelligent Buildings", Energy and Buildings, Vol. 49, pp. 85-98, 2012.

[5] H.L. Smith, W.R. Block, "RTUs Slave for Supervisory Systems (Power Systems)", IEEE Computer Applications in Power, Vol. 6, No. 1, pp. 27-32, Jan. 1993.

[6] T. Mecham, B. Wilkerson, B. Templeton, "Full Integration of SCADA, Field Control Systems and High Speed Hydraulic Models: Application Pacific Pipeline System", 3rd International Pipeline Conference, American Society of Mechanical Engineers Digital Collection, 2016.

[7] L. Rajesh, P. Satyanarayana, "Communication Protocol Security in Industrial Control Systems to Protect National Critical Infrastructure", Journal of Advanced Research in Dynamical and Control Systems, pp. 290-304, 2017.

[8] L. Rajesh, P. Satyanarayana, "Vulnerability Analysis and Enhancement of Security of Communication Protocol in Industrial Control Systems", Helix - The Scientific Explorer, Vol. 9, No. 04, pp. 5122-5127, 2019.

[9] K.A. Stouffer, J.A. Falco, K.A. Scarfone, "Guide to Industrial Control Systems (ICS) Security: Supervisory Control and Data Acquisition (SCADA) Systems, Distributed Control Systems (DCS), and other Control System Configurations such as Programmable Logic Controllers (PLC)", pp. 800-882, Jun. 2011.

[10] E. Byres, J. Lowe, "The Myths and Facts Behind Cyber Security Risks for Industrial Control Systems", VDE Congress, Vol. 116, 2004.

[11] M. Majdalawieh, F. Parisi Presicce, D. Wijesekera, "DNPSec: Distributed Network Protocol Version 3 (DNP3) Security Framework", Advances in Computer, Information, and Systems Sciences, and Engineering, Springer, Dordrecht, pp. 227-234, 2007.

[12] R.L. Krutz, "Securing SCADA Systems", John Wiley & Sons, 2005.

[13] Duong Trung, "Modern SCADA Systems for Oil Pipelines", Industry Applications Society 42nd Annual Petroleum and Chemical Industry Conference, pp. 299-305, Denver, CO, USA, 1995.

[14] M. Liu, J. Shimin, Y. Mancang, "Design Replica Consistency Maintenance Policy for the Oil and Gas Pipeline Clouding SCADA Multiple Data Centers Storage System", International Conference on Intelligent and Interactive Systems and Applications, Springer, Cham, 2017.

[15] E. Vargas, "High Availability Fundamentals", Sun Blueprints Series, Nov. 2000.

[16] C. Engelmann, "Symmetric Active/Active High Availability for High Performance Computing System Services", Ph.D. Thesis, Department of Computer Science, University of Reading, UK, 2008.

[17] C. Engelmann, H.H. Ong, S.L. Scott, "The Case for Modular Redundancy in Large-Scale High Performance Computing Systems", 27th IASTED International Conference on Parallel and Distributed Computing and Networks (PDCN), pp. 189-194, Innsbruck, Austria, 16-18 Feb. 2009.

BIOGRAPHIES

Locharala Rajesh was born in Andhra Pradesh, India in 1983. He completed B.Tech. degree in Electronics and Communication Engineering in 2004 and M.Tech. degree in 2011 from Jawaharlal Nehru Technological University, Hyderabad, India. He is currently pursuing the Ph.D. degree in Electronics and Communication Engineering Department at Koneru Lakshmaiah Education Foundation (Deemed) University, Andhra Pradesh, India. He is a member of international association of Engineers (IAENG). He published two papers in international journals and attended conferences.

Penke Satyanarayana was born in Andhra Pradesh, India. He received his B.Tech. degree in Electronics and Communication Engineering from Koneru Lakshmaiah College of Engineering, India in 2000. He completed M.Tech. degree in 2004 and Ph.D. degree from Jawaharlal Nehru Technological University, India in 2015. Presently he is working as Professor and Head of the Department in Koneru Lakshmaiah Education Foundation (Deemed) University, Andhra Pradesh, India. He published several articles in reputed international and national journals and attended conferences. Presently he is guiding six research scholars.