International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.03, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

Study and Preparation of Test Automation System for IEC-60870-5-104 Communication Protocol and Support for Data Analysis

Shubham D. Naik[1], Prof. Palhavi Kerkar[2]

[1,2]*Department of Electronics and Telecommunication, Goa College of Engineering -Goa, (India)*

ABSTRACT

In today's world, Automation is the need of the hour. The throughput of a company is directly proportional to the demand of the customers. In order to meet the desired demands automation of systems is of utmost importance. This paper focuses on the importance of the IEC-60870-5-104 protocol for Industrial automation. It highlights the design and implementation of Test Automation System for IEC-60870-5-104 using the TMW .Net Protocol Components and proposes the validation of data using automation capability of Microsoft Excel.

Keywords: IEC-60870-5-104 protocol, Industrial Automation, Test Automation System, TMW .Net Protocol Components, Validation of data;

I.INTRODUCTION

Industrial automation is defined as a set of technologies that results in operation of machines and systems without significant human intervention and achieves performance superior to manual operation. In any plant the purpose of automation is to maintain the product quality, achieve higher output, increased productivity, efficient use of materials, reduce startup time, increase speed of operation and human safety [1].

The main objective of automation is to improve processes to be more predictable, more sustainable and more precise. One such domain where there is a lot of scope for automation is the Electronic industry. Automation can be carried out during the testing phase of a product i.e. Test automation can be carried out.

Test Automation is the use of an automation tool to control the execution of tests and the comparison of actual outcomes with predicted outcomes. It can automate some repetitive but necessary tasks in a formalized testing process already in place or perform additional testing that would be difficult to do manually [2]. Protocols are defined as formal standards and policies which comprise of rules, procedures and formats that define communication between two or more devices over a network. protocols determine how data are transmitted between computing devices and over networks. Modbus, DNP3, IEC-60870-5 are some of the protocols used by industrial devices to communicate with one another.

Devices such as the Remote Terminal Unit (RTU), Protection Relays are used for applications like Smart grids, substation automation etc. Substation automation in power industry enables the development of remote monitoring, control and electronic devices coordination [3].

Thus, it is of utmost importance that the devices are tested in all aspects before employing them in the field. One such testing technique is Protocol Conformance Testing. Protocol Conformance Testing is basically a technique used to ensure that a product or process meets predefined standards.

This paper highlights the development and use of an Automation Test setup to carry out the validation of a IEC-60870-5-104 protocol.

II.PRELIMINARIES

2.1. IEC-60870-5-104 Standard

IEC 60870-5-104 is a companion standard of IEC 60870-5 that provides a communication profile for sending basic telecontrol messages between two systems in electrical engineering and power system automation. Telecontrol means transmitting supervisory data and data acquisition requests for controlling power transmission grids.

It is a standard for telecontrol equipment and systems with coded bit serial data transmission in TCP/IP based networks for monitoring and controlling geographically widespread processes. It provides the network access to IEC 60870-5-101 using standard transport profiles. That is, it delivers IEC 60870-5-101 messages as application data over TCP, port 2404. IEC 104 enables communication between control station and a substation via a standard TCP/IP network. The communication is based on the client-server model [4].

The client-server model is a software architecture model which is made up of two parts client system and server system both communicating over a computer network or on the same network. A client server application provides an efficient way to share the communication workload. The client process always initiates a connection to the server, while the server process always waits for request from client. On the field, the client and server are known as master and slave respectively.

IEC 60870-5-104 is also known as Supervisory Control and Data Acquisition (SCADA) protocol. It is used in power, petrochemical, water treatment, and oil and gas production industries. IEC 60870-5-104 is often used in power systems as a SCADA protocol between control stations and substations.

2.2. TMW .Net Protocol Components

The TMW .Net Protocol Component is a library which is available for the development of communications applications on the Microsoft .Net framework [5].It is highly flexible and easy to use in the communications protocol sector. These components support a number of different communication protocols such as IEC 60870-5, DNP3 and Modbus. These protocols can be configured as Master or Slave implementations

III.DESIGN AND IMPLEMENTATION

For developing any software application selecting the right programming language is of prime importance. Programming languages are building blocks for all computer software. The proposed Automation tool is designed in Microsoft Visual Studio 2010, using the C# programming language. C# is a modern, general-purpose, object-oriented programming language developed by Microsoft. It is a widely used professional language as it is object oriented and can be compiled on a wide variety of platforms. C# is a part of .NET framework and is used for writing .NET applications. The .NET framework is a revolutionary platform that helps programs to write windows applications, web application, web services to name a few.

The designed test tool is a Windows Forms Application, having three forms as shown in Fig.1. The first form is a splash screen which is basically a control element which appears during launching of program. The next form is the User Input Interface in which the relevant TCP parameters are initialized by the user. Finally, the Main form comprises of different control elements like buttons, checkboxes which enables the user to communicate with the DUT (Device Under Test). From the communication point of view, the Automation Test Tool is configured as an IEC104 master and the DUT is an IEC104 slave. A LAN cable is the communication medium between the master and slave.

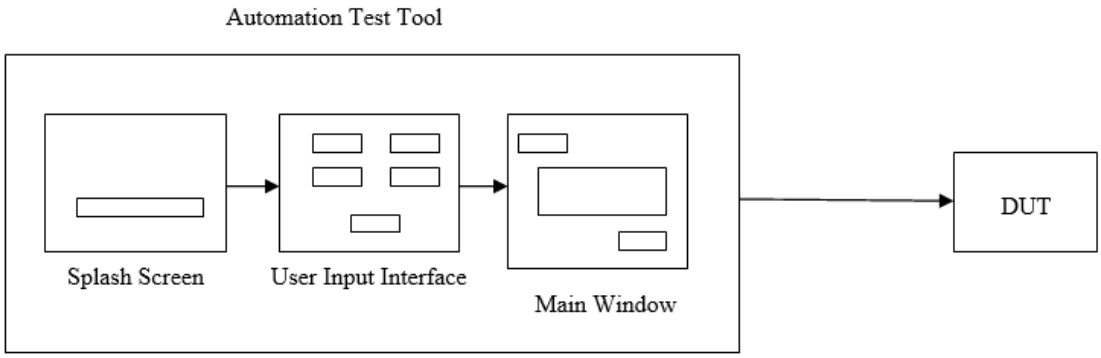

Fig1. schematic diagram of the test tool

In a TCP\IP network connection is established using three-way handshake. In this approach the master and slave devices exchange acknowledgement and synchronization packets before actual data communication. Currently, the Test tool is being run using the simulator-to-simulator approach i.e. the DUT is replaced by a TMW Protocol Test Harness Simulator configured as an IEC104 slave. It should be noted that the simulator is initialized in the same computer in which the Test tool is running. The loopback address (127.0.0.1) is used to facilitate communication between the tool and simulator.

The commands transmitted are as follows:

1. Single Point Information Command: This is a digital command using which digital values On and Off are transmitted to the slave.

2. General Interrogation Command: This command checks whether slave is online and requests subset or all data points from the slave.
3. Scaled Floating Point Command: This is an analog command using which floating analog values are transmitted to the slave.

The commands described above are some of the commands which are mentioned in the IEC-60870-5-104 standard. These commands are transmitted to the specific Information Object Addresses (IOA's) designated to each type of Information (i.e. Single Point, Scaled Floating Point etc.). The responses received by the master for each of the commands are stored in Microsoft Excel for future analysis. This capability is incorporated in the test tool by exploiting the automation capability of Microsoft Excel.

A protocol analyzer is integrated with the test tool. Protocol analyzer is defined as a tool (hardware or software) which is used to capture and analyze signals and data traffic over a communication channel. The protocol analyzer log is saved after the termination of the test tool.

IV.OBSERVATION AND RESULTS

This section shows the observed readings and results of the Test Tool when it was implemented in a simulator to simulator environment. A simple test case was implemented in which:

1. A GI command was transmitted.
2. Digital On (single point command) to IOA's 100 to 101.
3. Digital Off (single point command) to IOA's 100 to 101.
4. Scaled values to IOA 700 (value =15.8) and 702 (value=456.5).

The outputs and the results of the test case are shown below:

Fig. 2.user input interface

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.03, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

The User Input Interface shown in Fig.2. enables the user to enter the initialization parameters like IP addresses, Check ping status etc. When the "OK" button is pressed the Automation Test Tool shown in Fig.3. is displayed on the screen.A save file dialog box prompts the user to enter the file name in which the command responses will be saved. This file is saved in .csv format (Fig.6.).Clicking on the "Start Master" button initiates communication between the master and slave. The labels " Connected"and "Online " indicate the status of the connection between the master and slave.The data traffc observed in the protocol analyzer is saved in .txt format (Fig.5.) for future reference.

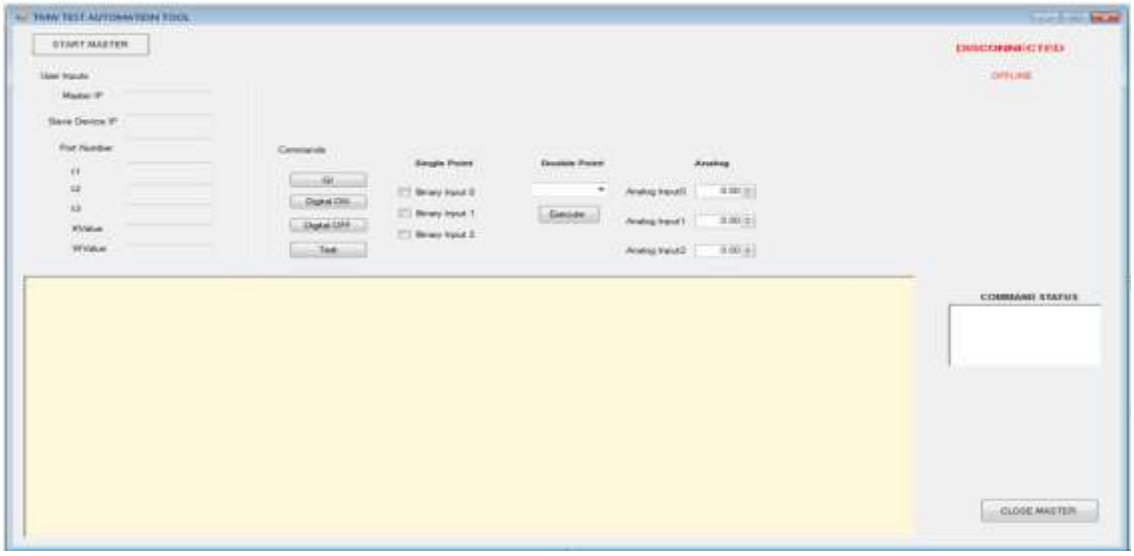

Fig. 3.automation test tool disabled

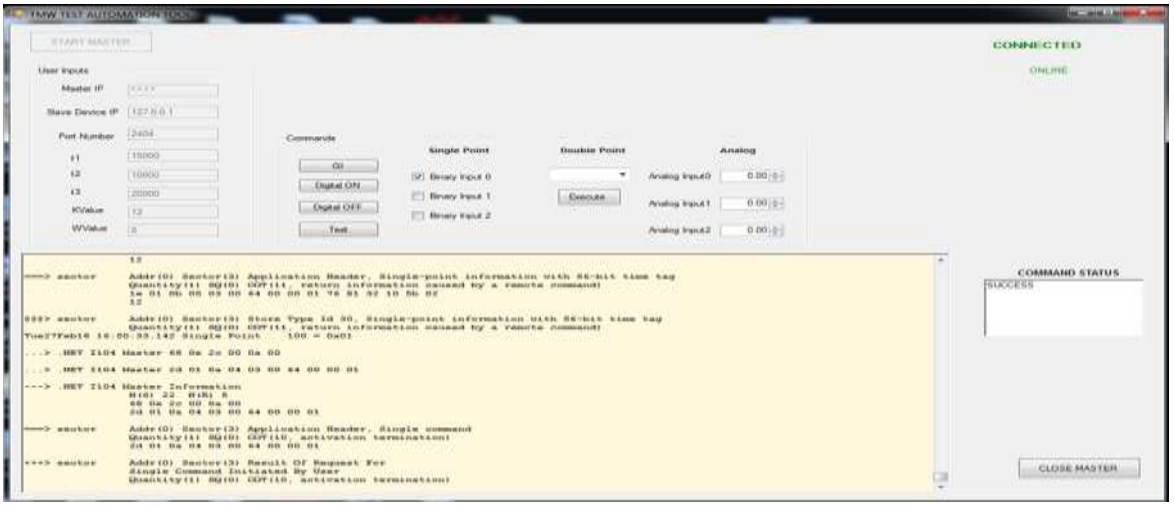

Fig. 4.automation test tool enabled

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.03, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

Fig. 5.the protocol analyzer log autosaved as text file

	A	B	C	D
1	IOA	COT	Value	Timestamp
2	100	20	0	16:34:13
3	101	20	0	16:34:13
4	102	20	0	16:34:13
5	103	20	0	16:34:13
6	104	20	0	16:34:13
7	105	20	0	16:34:13
8	106	20	0	16:34:13
9	107	20	0	16:34:13
10	108	20	0	16:34:13
11	109	20	0	16:34:13
12	100	11	1	16:34:17
13	101	11	1	16:34:17
14	102	11	1	16:34:17
15	100	11	0	16:34:19
16	101	11	0	16:34:20
17	102	11	0	16:34:20
18	100	11	1	16:34:23
19	101	11	1	16:34:23
20	102	11	1	16:34:24
21	100	11	1	16:34:24
22	101	11	1	16:34:25
23	700	1	15.8	16:34:26
24	701	1	0	16:34:26
25	702	1	456.5	16:34:26
26	100	11	1	16:34:26
27	100	11	1	16:34:26
28	101	11	1	16:34:26
29	102	11	1	16:34:27

Fig.6. command response outputs

The “GI” button sends a General Interrogation command to the DUT (simulator in this case),“Digital ON” when clicked sends a ON command to IOAs 100 to 102 and vice versa for “Digital OFF”. “Test”executes the Test case. The floating point analog inputs to the designated IOA’s are take through the numeicupdown boxes.

Fig.5. shows the response outputs of the test case. The Cause of Transmission (COT) column indicates what caused the slave to respond to the master. The COT codes obtained in the output are shown in Table.1.

Table 1. Cause of Transmission

COT code	**Cause of Transmission**
20	Interrogated by station interrogation
11	Return information caused by remote command.
1	Periodic, cyclic

V.CONCLUSION

This paper presents the implementation of a basic IEC104 test automation tool for protocol conformance testing. From the command response output results (Fig.6.) it is concluded that the COT and timestamp are the important parameters which can be analyzed to verify the correctness and latency of the transmitted values.

VI.FUTURE WORK

The work presented in this paper leads to the following lines of future work:

1. Incorporating all the IEC104 Information types in the Test Tool.
2. Using the Test Automation Tool to carry out Conformance Testing of a DUT (example: RTU).
3. Increasing the functionality of the Test Tool to support all protocols listed in Table I.
4. Creating test cases to check correctness of analog values in a user specified time interval.

VII. ACKNOWLEDGMENT

This work was done at the R&D center of Siemens- Energy Automation Verna Goa-India. Author is thankful to the Head of Department and faculty, Department of Electronics and Telecommunication Engineering, Goa College of Engineering, Farmagudi, Ponda -Goa, for constant support and encouragement.

REFERENCES

[1] Abdu Idris Omer Taleb M.M., PhD, *Architecture of Industrial Automation Systems*,European Scientific Journal,*vol.10.*,edition 2014.

[2] Kolawa, Adam; Huizinga, Dorota, a*utomated defect prevention:best practices in software management*.Wiley-IEEE Computer Society Press,2007,.p. 74

[3] J.Horalek, J.Matyska,V.Sobeslav, *communication protocols in substation automation and IEC-61850 based proposal*, 14th IEEE International Symposium on Computational Intelligence and Informatics, November 2013.

[4] Faculty of Information Technology Brno University of Technology ,Brno, Czech Republic, *Description and analysis of IEC 104 Protocol , Technical Report*, December , 2017.

[5] Triangle MicroWorks, Inc. .Net Protocol Components User Manual , January 11 2016.