Standard Library for Simulation of Communication to 3rd Party devices

ABB

Robin Johansson

Degree thesis for Bachelor of Engineering

Degree program in Electrical Engineering and Automation

Vasa 2020

BACHELOR'S THESIS

Author: Robin Johansson
Degree Programme: Electrical Engineering and Automation, Vaasa
Specialization: Automation Technology
Supervisors: Jan Berglund, Daniel Hummel

Title: Standard Library for Simulation of Communication to 3rd Party Devices

Date: April 22, 2020 Number of pages: 11

Abstract

This thesis was commissioned by ABB Oy Energy Industries department (IAEN) which specializes in power plant control systems. The goal was to develop a standardized procedure for testing communications and as a result increasing the quality of the product. This have been accomplished by creating a plugin for Triangle MicroWorks' Protocol Test Harness which can open a communication channel for a slave or master device. The tool also consists of a library with a few selected devices that are common in the control system.

A big part of this thesis was the programming itself but also a lot of reverse engineering and simulations was carried out to adapt the plugin and communication to already existing methods that are used by the engineers at IAEN.

As a result, the fundamental parts of the plugin work as intended but will still require a bit of programming to allow more devices to be simulated. It was found out that device configuration varies between devices manufacturers which makes is tougher to insert new devices. The plugin functions as a base that can be built upon.

Because this gives ABB an advantage on the market it is regarded as sensitive material and will be placed under secrecy.

Language: English Key words: simulation, power plant, automation, Modbus, DNP3, IEC 60870-5-104

EXAMENSARBETE

Författare: Robin Johansson

Utbildning och ort: El- och automationsteknik, Vasa

Inriktningsalternativ: Automationsteknik

Handledare: Jan Berglund, Daniel Hummel

Titel: Standardbibliotek för simulering av kommunikation till tredje parts enheter

Datum: 22 april 2020 Sidantal: 11

Abstrakt

Examensarbetet är gjort på uppdrag av ABB Oy Energy Industries (IAEN) som specialiserar sig på styrsystem till kraftverk. Målet med detta arbete var att ta fram en standardiserad process för testning av kommunikation och som ett resultat av det öka kvaliteten på produkten. För att åstadkomma det programmerades ett plugin till Triangle MicroWorks Protocol Test Harness som kan öppna kommunikationskanaler för slav- eller masterenheter. Pluginet innehåller även ett bibliotek med enheter som är vanliga i styrsystemet.

En stor del av examensarbetet gick åt till programmering men också simulationer och undersökningar av metoder som redan används av ingenjörerna vid IAEN och hur man kan anpassa pluginet till dessa.

Resultatet blev att de viktigaste delarna av pluginet fungerar som tänkt men kommer kräva lite programmering till så att ännu fler enheter kan simuleras. Det visade sig att konfigurationen mellan enheter skiljer sig mellan tillverkare vilket gör det svårare att inkludera nya enheter. Pluginet kommer fungera som en bas att bygga vidare på.

Eftersom detta examensarbete ger ABB en fördel på marknaden så betraktas detta material som känsligt och kommer att sekretessbeläggas.

Språk: engelska Nyckelord: simulation, kraftverk, automation, Modbus, DNP3, IEC 60870-5-104

OPINNÄYTETYÖ

Tekijä: Robin Johansson
Koulutus ja paikkakunta: Sähkö- ja automaatiotekniikka, Vaasa
Suuntautumisvaihtoehto: Automaatiotekniikka
Ohjaajat: Jan Berglund, Daniel Hummel

Nimike: Vakiokirjasto kommunikaation simulointiin kolmansien osapuolien laitteiden kanssa

Päivämäärä: 22. huhtikuuta 2020 Sivumäärä: 11

Tiivistelmä

Tämä opinnäytetyö on tehty ABB Oy Energy Industriesin (IAEN) toimeksiantona. He ovat erikoistuneet voimalaitoksien ohjausjärjestelmiin. Työn tavoitteena oli kehittää standardoitu prosessi kommunikaation testaamiseen ja näin ollen parantaa tuotteiden laatua. Tätä varten ohjelmoitiin laajennus Triangle MicroWorks Protocol Test Harnessiin, joka voi avata tietoliikennekanavat orja- tai niekkalaitteille. Laajennuksen piti sisältää myös kirjasto ohjausjärjestelmän tavallisista laitteista.

Suuri osa opinnäytetyöstä käsittelee ohjelmointia ja simulaatioita. Lisäksi työssä käsitellään tutkimuksia IAEN:n insinöörien käyttämistä menetelmistä, ja miten laajennus mukautetaan näihin.

Tuloksena on, että laajennuksen tärkeimmät osat toimivat suunnitellusti, mutta vaativat jonkin verran ohjelmointia, jotta useampiakin laitteita voitaisiin simuloida. Kävi myös ilmi, että yksiköiden kokoonpano vaihtelee valmistajien välillä, mikä vaikeuttaa uusien laitteiden sisällyttämistä. Laajennus toimii pohjana, jota voi kehittää edelleen.

Koska tämä opinnäytetyö antaa ABB:lle etua markkinoilla, tätä materiaalia pidetään arkaluontoisena ja luottamuksellisena.

Kieli: englanti Avainsanat: simulaatio, voimalaitos, automaatio, Modbus, DNP3, IEC 60870-5-104

Table of Contents

List of Abbreviations

ADU	Application Data Unit
AVR	Automatic Voltage Regulator
FAT	Factory Acceptance Test
GUI	Graphical user interface
HMI	Human Machine Interface
HV	High voltage
I/O	Input/output
IED	Intelligent Electronic Device
IP	Internet Protocol
MBAP header	Modbus Applicaion Header
OSI	Open systems Interconnection
PDU	Protocol Data Unit
PMU	Power Monitoring Unit
RTU	Remote Terminal Unit
SCADA	Supervisory control and data acquisition
TCP	Transmission Control Protocol
XML	Extensible Markup Language

1 Introduction

This thesis was commissioned by ABB Energy Industries (IAEN) department who specializes in industrial automation. The task consists of programming and testing a software for simulation of industrial communication.

It contains classified material and therefore some chapters are put under secrecy.

1.1 About the company and department

ABB was formed in January 1988 when Sweden’s ASEA and Switzerland’s Brown, Boveri & Cie (BBC) combined their expertise’s into one. That gave ABB control of a third of Europe’s market and 20% of the world’s electric industry market, making them the largest supplier of industrial electric motors, generators and power grids in the world. [1]

As of Q4 2019 ABB has approximately 144,000 employees around the world working in four different business segments. Electrification, Industrial Automation, Motion and Robotics & Discrete Automation. There is a fifth segment named Power Grids that is to be moved over to Hitachi in 2020. [2]

IAEN is a subsegment of Industrial Automation and has four segments of its own. Modular, Hydro, Nuclear & Thermal and Service. Modular department specializes in Make-To-Order gas and diesel engine power plant automation and eBoP which is short for electrical balance of plant. A HV-switchgear is not within IAEN’s scope of delivery. [3]

1.2 Standard electrical panels in a Modular project (Confidential)

1.3 Background and purpose

The idea was developed by IAEN Modular department and introduced by my thesis supervisor Mr. Daniel Hummel.

The purpose of this thesis is to make control system testing more effectively. At the moment when testing a control system, many types of software are used. With this thesis one single software shall be created that is tailored to ABB’s needs.

This software will simulate 3rd party devices before completion and commissioning of the power plant. A device can be anything that is not available at the FAT-area and will be installed later, for example a PMU.

All devices cannot be configured since every project that ABB manufactures is different, but many devices are standard and should have the same device registers in most of the projects. Because of this there must be possibility to adapt the simulation process according to the specifications of the project.

Figure 1 shows a simplified software overview of how the software is to be set up.

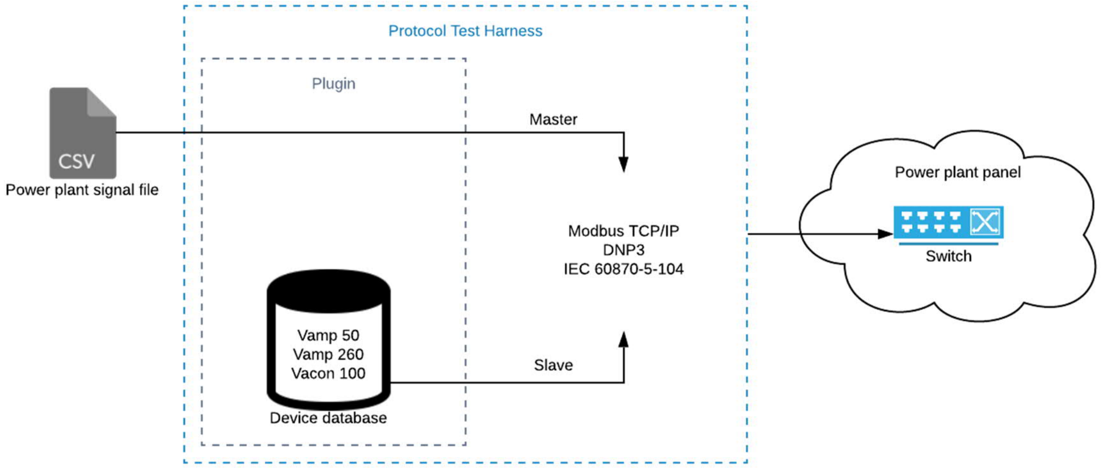

Figure 1 - Software overview

2 Protocols

This thesis demands some knowledge about the communication protocols but only on the surface since the communication software that will be used comes with a large library that is already configured to open a communication channel with a few lines of code.

There are several communication protocols that will be simulated or read. Modbus TCP/IP, DNP3 and IEC 60870-5-104 are the three main ones that will be focused on.

Modbus TCP/IP will be used during both master/client and slave/server communication while DNP3 and IEC 60870-5-104 will only be used for master/client communication.

2.1 Fundamentals of TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) is a collection of protocols originally developed on behalf of the United States Department of Defense under the name NCP (Network Control Protocol). The goal was to establish a protocol that could take alternative routes in a network and still reach its destination. [4]

The four-layer TCP/IP shall not be confused with the seven-layer conceptual OSI model, which is used for designing computer systems and is not used for actual communication but to describe a system architecture. In Figure 2 it is shown how the TCP/IP protocol correlates to the OSI model.

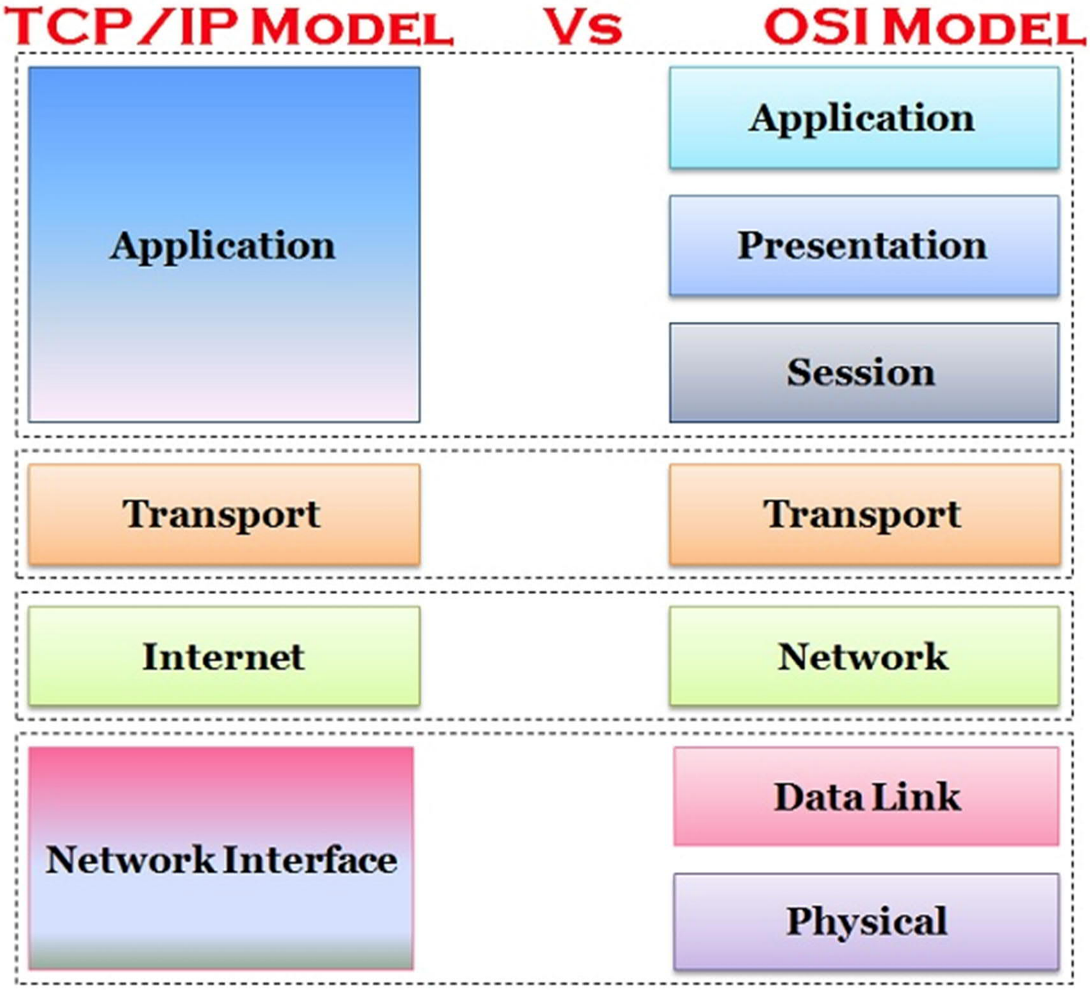

Figure 2 - Diagrammatic Comparison of TCP/IP and OSI [5]

The application layer contains the actual data that is to be sent. The transport layer manages the connection between hosts that communicate, this is where the actual TCP resides. The network (internet) layer handles the routing of the packets over the internet, for this the protocol IP is used. The physical layer (Network Interface) is the component that is used to connect the hosts to the network, mainly an ethernet port. [6] [5]

2.2 Modbus TCP/IP

Modbus is an open-source communication protocol developed by Modicon and released in 1979. At first it was intended for Modicon products, but it was later decided that Modbus should be open to the public. Modicon goes under the name of Schneider Electric today. Schneider Electric assisted in forming the non-profit organization Modbus Organization.

Regular Modbus uses a network of master/slaves where the master sends a command to the slaves. The slaves will not reply the answer if the slave address specified in the command does not target them.

Modbus TCP/IP combines Modbus with the common transport layer of Internet. This is useful because many manufacturers use ethernet ports for interfacing with their devices nowadays.

Modbus TCP/IP forms client/server communication between multiple devices. A client is a master device and server is a slave device. [7]

When sending or receiving a request over TCP/IP the request message is made up of several blocks. These blocks together form the Application Data Unit (ADU) and contain a Modbus Application Protocol (MBAP) header and the Protocol Data Unit (PDU) the MBAP header is added to the start of each Modbus Message followed by a function code and data block.

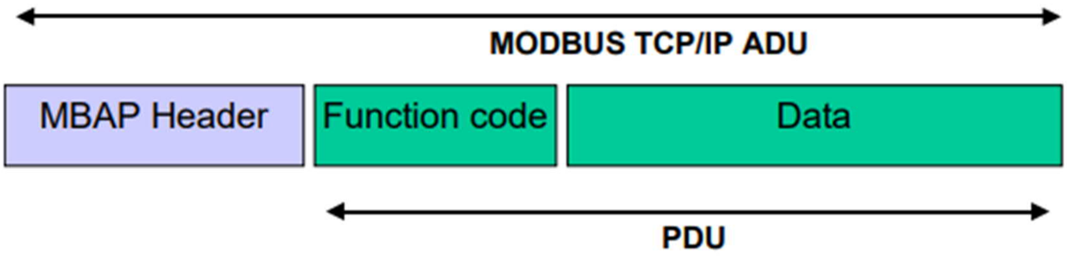

Figure 3 . MODBUS request/response over TCP/IP [8]

The MBAP header contains 7 Bytes.

- 2 bytes: Transaction Identifier. It is an unique identifier that matches the request and response to one another.
- 2 bytes: Protocol Identifier. It will signal what type of protocol is used, will always be set to 0 since that is the identifier for Modbus.
- 2 bytes: Length. The byte count for the rest of the message.
- 1 byte: Unit Identifier. Will identify the device. This is not used for common TCP/IP messages, instead the IP address is used as identification.

[8]

To understand what the function codes are and what they do, some knowledge about the different types of registers used in Modbus communication is needed.

2.2.1 Modbus register types

There are four types of registers used or that can be used in a Modbus enabled device. These are seen in Table 1.

Table 1 - Modbus register types and specification

Type	Size	Access	Address range
Coil	1 bit	Read-Write	00001-09999 000001-065535
Discrete Input	1 bit	Read	10001-19999 100001-165535
Input Register	16 bit	Read	30001-39999 300001-365535
Holding Register	16 bit	Read-Write	40001-49999 400001-465535

[9]

Sometimes using the address range of a Modbus register with format X0001-X9999 is not enough, then using the second address range is a must. The red number marked in the address range marks what type of register it is. [9]

2.2.2 Modbus function codes

A function code is generated by the client and sent to the server. It tells the server what registers the client is interested in and what it wants to do with them. There are three different categories of Modbus function codes, public, user-defined and reserved function codes. Public function codes are for anybody to use and are documented and validated by the Modbus Organization. The function code range is 1-64_{10}, 72-99_{10} and 110-127_{10}. User-defined function codes are an address range from 65-71_{10} and 100-109_{10}. The user can program the desired function code to perform the actions of their choosing. Reserved function codes are codes that are used by manufactures and are not open to the public. In Table 2 the common function codes are seen.

Table 2 - Modbus function codes

Function code	Register Type
1	Read Coil
2	Read Discrete Input
3	Read Holding Registers
4	Read Input Registers
5	Write Single Coil
6	Write Single Holding Register
15	Write Multiple Coils
16	Write Multiple Holding Registers

[9]

2.3 IEC 60870-5-104 and DNP3

IEC 60870-5 is the international standard in electric power SCADA transmission protocols. It was developed by IEC Technical Committee 57 during 1988-2000. IEC 60870-5-104 or T104 which it is also called, is a companion standard of IEC 60870-5 and is the networked version of its sister standard IEC 60870-5-101.

DNP3 is developed from IEC 60870-5 and uses the early design rules. It was developed by Westronic in 1992 and was made public domain in 1993 and is since then maintained by the DNP3 Users group. DNP3 was intended for use in the electric utility industry but has since its introduction been used in other industries as well.

In Europe the most commonly used protocols are T101 or T104 and in North America DNP3 is the preferred protocol.

While Modbus TCP/IP requires a request from the master device, both DNP3 and T104 protocol enables the RTU to send information to the master/controlling station without a request, this results in faster information transmission. To increase efficiency even further, both protocols also based on a report by exception model. This means that only things that have changed will be reported.

The sizes of the messages of the both protocols also vary. T104's messages can only contain one type of data. That can be for example an analog value or a single bit. DNP3 on the other hand can contain multiple types. Because of this T104 will send many smaller messages that are no larger than 250 bytes while DNP3 will send fewer larger messages with sizes up to 2048 bytes.

To identify an object in T104 two identifiers are used. The device identity (ASDU) and information object address (IOA). The device identity shall not be confused with the IP address. The IOA is similar to the Modbus way of addressing an object. It uses type number first to group different types of objects together and then a running number after the initial number. DNP3 objects are identified by the IP address, data type and object index. The index is a unique number for each object of a data type.

T104 includes a unique feature that none of the other protocols has, it includes a cause of transmission (COT) in the message. This COT value represents what has made the event trip. For example, if an operator instructs a breaker to open, it will log that it was opened intentionally instead of saying it has tripped. [10]

3 System setup (Confidential)

4 Software

Two types of software shall be used to make the simulator. The first one already exists and only need familiarizing which is Triangle MicroWorks’ Communication Protocol Test Harness. The other one is Visual Studio Community 2019 which was chosen for the programming.

4.1 Protocol Test Harness

Test Harness is a commonly used term and not just the product name. To make things shorter Test Harness will be shortened to TH in this thesis.

TH can test, monitor and simulate DNP3, IEC 60870-5 and Modbus communication, other protocols are also available but not used in this thesis. This tool also supplies manuals and programming libraries which means it will minimize the workload when programming.

TH will run in the background of the testing and the controlling and setting up of the test will be done via a plugin that can be programmed in a few languages. These are Python, .NET or Tcl/tk scripts. [11]

4.2 Visual Studio Community 2019 and C#

The plugin programmed in this thesis will be made with the programming language C# (C sharp) which is a part of the .NET Framework and will be programmed within the Visual Studio Community 2019 because of its AI-assisted development called IntelliCode. This means it will predict what you will write and give suggestions. It will also make it easier to find errors in the code, which will reduce time in programming. [12]

The .NET Framework is used for various applications, for instance web, Windows and phone. It supports many languages such as C#, F#, VB.NET, etc. [13]

The .NET Framework also allows the programmer to easily create a GUI for the code using Windows Forms for example. It combines code with visual building of a GUI which helps the programmer create a better application. [14]

C# is an object-oriented programming language which means that objects are to be explained in classes. In code example 1 is a class that explains the characteristics of a point in a coordinate system.

Code example 1. A class describing a point

```
public class Point
{
    public int x, y;
    public Point(int x, int y)
    {
        this.x = x;
        this.y = y;
    }
}
```

[15]

5 Programming the plugin (Confidential)

6 Result (Confidential)

7 Discussion (Confidential)

8 References

[1] ABB Ltd, "History," [Online]. Available: https://new.abb.com/about/history. [Accessed 18 November 2019].

[2] ABB Ltd, "Full-year and Q4 2019 results," 5 February 2020. [Online]. Available: https://resources.news.e.abb.com/attachments/published/55793/en-US/5EFEA791DF00/ABB-full-year-and-Q4-2019-results-press-release-English.pdf. [Accessed 21 March 2020].

[3] ABB Oy, "Introducing ABB Energy Industries," ABB Oy, Vaasa, 2019.

[4] H. K. S. J. M. Tittel Ed, "Koncept och planering: TCP/IP och Windows NT 4," in Intensivplugga TCP/IP, Scottsdale, Coriolis Group, 1999, pp. 13-29.

[5] TechDifferences, "Difference Between TCP/IP and OSI Model," 2016 March 2016. [Online]. Available: https://techdifferences.com/difference-between-tcp-ip-and-osi-model.html.

[6] R. L. G. K. Rouse Margaret, "TCP/IP (Transmission Control Protocol/Internet Protocol)," SearchNetworking, February 2020. [Online]. Available: https://searchnetworking.techtarget.com/definition/TCP-IP. [Accessed 22 March 2020].

[7] Modbus Organization, "Modbus FAQ: About The Modbus Organization," Modbus Organization, [Online]. Available: http://www.modbus.org/faq.php. [Accessed 1 March 2020].

[8] Modbus Organization, "MODBUS Messaging on TCP/IP Implementation Guide V1.0b," 24 October 2006. [Online]. Available: http://www.modbus.org/docs/Modbus_Messaging_Implementation_Guide_V1_0b.pdf. [Accessed 1 March 2020].

[9] Control Solutions Minnesota, "Modbus 101 - Introduction to Modbus," [Online]. Available: https://www.csimn.com/CSI_pages/Modbus101.html. [Accessed 6 March 2020].

[10] A. C. West, "DNP3 and IEC 60870-5," in Industrial communication systems, New York, Taylor & Francis Group, 2010, pp. 58:1-58:9.

[11] Triangle MicroWorks, Inc., "Triangle MicroWorks," Triangle MicroWorks, Inc., [Online]. Available: https://products.trianglemicroworks.com/home. [Accessed 8 March 2020].

[12] Microsoft, "Visual Studio IntelliCode," [Online]. Available: https://visualstudio.microsoft.com/services/intellicode/. [Accessed 16 April 2020].

[13] javaTpoint, ".NET Framework," [Online]. Available: https://www.javatpoint.com/net-framework. [Accessed 16 April 2020].

[14] Csharpskolan, "Windows Forms - Del 1," [Online]. Available: https://csharpskolan.se/article/windows-forms-del-1/.

[15] Microsoft, "C# documentation," Microsoft, [Online]. Available: https://docs.microsoft.com/en-us/dotnet/csharp/. [Accessed 8 March 2020].