

Simulator of IEC 60870 communication

1st Tomáš Calábek

Department of Telecommunications
Brno University of Technology
Brno, Czech Republic
237881@vutbr.cz

2nd Antonín Boháčik

Department of Telecommunications
Brno University of Technology
Brno, Czech Republic
Antonin.Bohacik@vut.cz

Abstract—The power industry’s evolution hinges on efficient and reliable transmission, distribution, and control of electricity, increasingly facilitated by remote monitoring and control systems. Among these, SCADA technologies stand out, enabling centralized supervision and management of energy infrastructure. Central to these systems are communication protocols such as protocols from IEC 60870 standard, facilitating data exchange within power networks. This paper introduces a communication simulator based on IEC 60870-5-101/103/104 protocols. Our simulator for IEC 60870 is capable of simulating all three mentioned protocols on the client-server principle. It can simulate both balanced and unbalanced transmissions, adjust transmitted data, set quality bits, and much more. Our simulator was tested in a virtual environment.

I. INTRODUCTION

Today, the power industry is a key sector that is constantly evolving to ensure efficient and reliable transmission, distribution, and control of electricity [1]. With the development of technology and automation in the power sector, the remote control is becoming an increasingly important system, enabling centralized monitoring and control of power equipment, including distribution networks [2]. In the field of remote control of power systems, modern technologies such as SCADA (Supervisory Control and Data Acquisition) are used, which enables operators to efficiently monitor and control energy equipment remotely [3]. These controls are key to ensuring the safe and optimized operation of power plants, transmission networks, and distribution systems [4]. In the context of remote control and SCADA systems, communications play a key role. Protocols that enable the transfer of information between devices in a power system. These protocols include the IEC 60870 standard, which defines the communication method between devices in the energy sector [5].

The aim of this paper was the presentation of the communication simulator based on IEC 60870-5-101/103/104 protocols. This simulator provides a variety of functions such as changing the transmitted data, the period of sent messages, or communication protocol, also sending various queries, or creating communication datasets. The simulator also includes a user interface that makes it easier to work with our developed simulator. The final simulator was tested in a virtual environment using 4 VMs (Virtual Machine), where 3 were individual servers of the mentioned protocols and one VM where all clients were stored.

A. State of the Art

In the domain of operational communication generators/simulators, a diversity of manufacturers and services is evident. While the generators generate almost random data, simulators generate data with a sort of logic behind them. Numerous companies engage in the development of such tools, each offering its unique solution. Examples of these manufacturers include National Instruments with their NI VeriStand software, Doble Engineering Company with their simulators, and OPAL-RT Technologies with their Real-Time Simulator.

However, it is crucial to note that not all these products sufficiently cover a broad spectrum of ICS (Industrial Control Systems) protocols. Some companies focus solely on specific protocols or provide limited support for various industrial control standards. Examples of companies specializing in ICS protocol simulators include ABB Group with their System 800xA simulator, Honeywell International Inc. with their Experion PKS simulator, and Schneider Electric with their EcoStruxure Control Expert simulator.

Particular attention must be paid to simulators operating with the standard 60870 protocol, which is crucial for many industrial applications, especially in the energy sector. Unfortunately, only a limited number of companies offer protocol generators of this specification. Among them are Siemens AG with their SIMATIC WinCC simulator for the 60870 protocol and ABB Group with their RTU500 series, which supports the 60870 protocol.

The following Table I provides a concise overview of companies involved in communication data generation and analyzes the solutions they offer, including their protocol coverage and other key functionalities.

TABLE I
OVERVIEW OF COMPANIES ENGAGED IN DATA GENERATION AND ANALYSIS OF PROVIDED SOLUTIONS.

Offered solution	Supported protocols	Price
NI VeriStand	Modbus, CANopen	Unspecified
Simulators ICS	DNP3, IEC 61850	275 €
EE Power RTS	IEC 60870, IEC 61850, DNP3	18.300 €
ABB System 800	IEC 61850, DNP3, Modbus	Unspecified
Experion PKS	IEC 61850, Modbus, PROFIBUS	155 €
EcoStruxure	IEC 61850, Modbus, PROFINET	6.510 €
SIMATIC WinCC	IEC 60870, Modbus, PROFINET	1.000 €
Our IEC 60870 Sim.	IEC 60870-5-101/103/104	< 100 €

II. SCADA

The standard provides functionality for remote controlling SCADA systems. The term SCADA refers to a set of software and equipment used to monitor and control technical or industrial equipment. The SCADA system works on the principle of control and server stations. In this respect, IEC 60870 provides SCADA systems with support for the implementation of functions that are crucial for the proper functioning of SCADA systems. The most important functions that IEC 60870 provides to SCADA systems include the following [4]:

- Ensuring interoperability – IEC 60870 is designed to ensure interoperability between the various components of SCADA, facilitating seamless communication across different devices and systems.
- Improving reliability and safety – IEC 60870 makes SCADA systems implement an authentication and access control process, preventing unauthorized access to critical control points. At the same time, IEC 60870.
- Real-time communication – IEC 60870 can handle requests. communication in real-time. By using efficient communication protocols the standard facilitates the rapid exchange of data between field devices and the central SCADA control center, enabling rapid decision-making

A. IEC 60870

IEC 60870 is a set of international standards, developed by the IEC (International Electrotechnical Commission), which addresses the need for efficient and reliable communication in power systems [4]. IEC 60870 is referred to in the Czech Republic as CSN EN 60870. It is the name for the whole group of standards called *Remote control systems and equipment*. These standards were originally developed to support systems for SCADA in the energy sector. The IEC 60870 standard is based on the EPA architecture, as well as protocol DNP3 [5].

B. IEC 60870-5

IEC 60870-5 also referred to as *Communication Protocols* defines detailed descriptions of the useful functions of systems for remote control and the control of geographically extensive processes. These functions include three of the most important – Polling, Report by Exception, and time stamp assignment [6]. Polling involves the master unit in a communication system sending requests to multiple server units, each responding as required, while Report by Exception allows server stations to communicate with the master independently, transmitting crucial information promptly. Timestamps, automatically attached to events, help identify the initial event amidst subsequent occurrences, requiring accurate time synchronization between the master and server units for effective usage.

The IEC 60870-5 standard provides information on a set of information elements that are suitable for a wide range of SCADA applications, especially for power distribution system applications [4]. This data is transmitted within ASDUs (Application Service Data Units) carrying application data, which may contain one or more information, see Fig. 1 [7]. Each

data unit has a unique type identification number. Only one data type is included in each ASDU, located in the first field of the ASDU. The types of information elements are defined by the standard and grouped by direction, either monitoring or control, and by the type of information that is transmitted, such as process information, system information, or file transfer parameters. Furthermore, messages can be classified according to the actual reason that caused the message to be sent, referred to as COT (Cause Of Transmission). This classification serves to improve clarity when processing received messages. The next section in the ASDU message header is the sequence number SQ (Sequence number), which indicates the order of the messages received. It also contains the sender address of the message known as OA (Object Address) and an information element, which is a key element for the transmission of information.

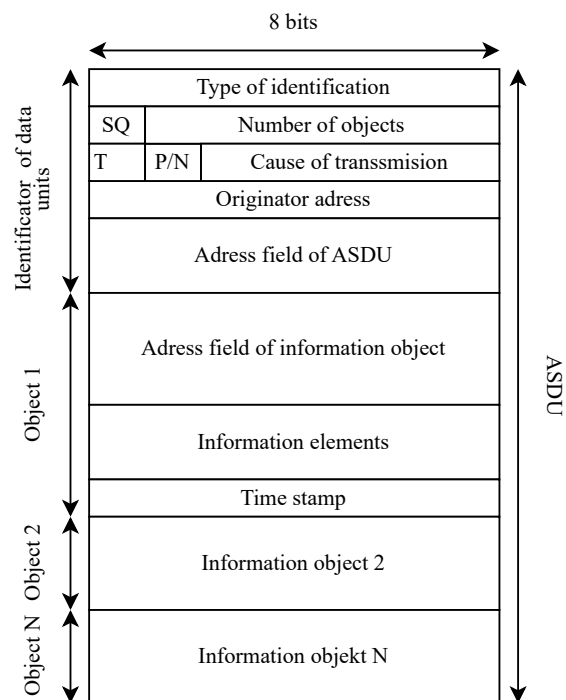


Fig. 1. Structure of ASDU format [7]

1) *IEC 60870-5-101*: This is a companion standard known as *Transmission Protocols – Companion standard especially for basic telecontrol tasks* that defines a communication profile for the transmission of basic messages of remote control messages between the central control station (client) and the remotely controlled stations (server) [8]. The companion standard works on the 2nd layer, i.e. link layer data. IEC 60870-5-101 allows two basic ways of transmitting communication: (1) unbalanced transmission and (2) balanced transmission [7].

In unbalanced transmission, the control station initiates all communication by polling the controlled outputs, supporting services such as SEND/NO REPLY for global messages and cyclic commands, SEND/CONFIRM for control commands and setup commands, and REQUEST/RESPOND for calling data from controlled stations.

On the other hand balanced transmission, each station can initiate message transmission, acting as both control and controlled stations, with supported services like SEND/CONFIRM and SEND/NO REPLY limited to point-to-point and multi-point configurations. IEC 101 is used in telecontrolling power systems, electric power systems, teleprotection, etc. It also serves as the basis for the IEC 104 standard, which is an extension of it that can communicate via TCP/IP protocol, i.e. wirelessly.

2) *IEC 60870-5-103*: This standard specifies the information interface of protection systems in the field of automation and control of power systems. This standard aims to ensure compatibility between protection devices and control system devices in server stations [9]. The VDEW protocol, incorporated into the IEC 60870-5 protocol suite, specifically the discussed IEC 60870-5-103, is a five-tone selcall mode defined by the German Verband der Elektrizitätswirtschaft. Within IEC 60870-5-103 there are two methods of information exchange. First, it uses standardized messages and application procedures to transfer standardized ASDUs. The second method uses generic services to transfer a wide range of information. The standardized messages cover only a limited set of protection functions, meaning that protection devices can only support a subset of the functions defined by this standard. Predefined messages and application procedures are mandatorily used where possible, and generic services are used otherwise. Overall, IEC 60870-5-103 and the VDEW protocol provide a framework for efficient communication and information exchange between protection devices and control systems in power systems, with an emphasis on compatibility and the ability to use different transmission protocols, including TCP/IP.

3) *IEC 60870-5-104*: As mentioned before IEC 104 is an extension standard that expands IEC 101 with a TCP/IP interface so it's able to suit complete network access [7]. The application layers of these two standards are the same with the difference that some of the data types are not implemented so they cannot be used. The IEC 104 data contain mechanisms for synchronization. One of the most common devices where IEC 104 is used is the MT-151 which is a telemetry mobile controller.

III. IEC 60870 COMMUNICATION SIMULATOR

While existing solutions cater to specific protocols or lack comprehensive support, our simulator fills a critical void by offering a versatile platform encompassing the full spectrum of ICS protocols, particularly IEC 60870. Featuring a modular architecture and user-friendly interface, our simulator facilitates testing, research, and education in the energy and automation sectors. Its capabilities extend to simulating diverse communication models, enhancing its applicability for developers, researchers, and practitioners. Furthermore, its potential integration into physical devices bridges the gap between theoretical exploration and practical implementation. In summary, our IEC 60870 communication simulator represents a significant advancement, addressing the challenges of

communication protocol testing and development in the power industry. For implementation purposes, the practical part will focus on the analysis and verification of the functionality of the IEC 60870-5-104 protocol. This part focuses on the protocol implementation. The communication simulator will serve as testing software for people working with telecommunication protocols in the energy industry, but also as a kind of insight into this standard for any non-expert user.

The simulator for the IEC 60870 communication standard significantly enhances scientific research and development in the energy and automation sectors through diverse approaches. It serves as an important tool for testing and validating implementations by providing a simulated environment that aligns with the standards outlined in IEC 60870. Developers can thoroughly test various device and system implementations, facilitating error identification, resolution, and performance optimization. Additionally, the simulator supports research and development efforts by providing a platform for experimentation without the constraints of physical deployment, thereby reducing both the time and costs associated with developing new technologies or refining existing systems. Moreover, the simulator is pivotal in education and training initiatives within the energy and automation domains. It furnishes students, technicians, and professionals with a practical environment for hands-on work and experimentation with communication protocols and devices, fostering deeper understanding and proficiency without the risks associated with real-world deployment. In discussing the IEC 60870 communication standard simulator, it's crucial to highlight its potential for implementation within real, physical devices. This feature not only ensures seamless integration between virtual simulations and hardware but also extends the utility of the simulator in the context of practical use.

A. Software design

The simulator comprises two core components: (1) client and (2) server. Each component is intricately crafted to adhere to the nuances of the protocol version, facilitating seamless extension with additional protocols via modular add-ons. The client module not only accommodates interaction with simulated servers but also interacts with real-world energy or industry devices. This integration offers distinct advantages, including the ability to test and validate device behavior, as well as generate datasets from live equipment. Such versatility enhances the utility of the simulator for both testing and real-world application scenarios.

B. Simulator Design

Fig 2 illustrates the testing topology of the created IEC 60870 communication simulator. The implementation of this simulator involves modular architecture, utilizing appropriate programming languages and frameworks for protocol handling and message parsing. Key components include modules for protocol handling, message parsing, data simulation, and a GUI (Graphical User Interface). The GUI provides users with intuitive interaction, allowing configuration of simulation

parameters, monitoring of communication traffic, and analysis of protocol behavior. It will offer features such as configuration settings, message monitoring, simulation controls, data visualization, and error handling.

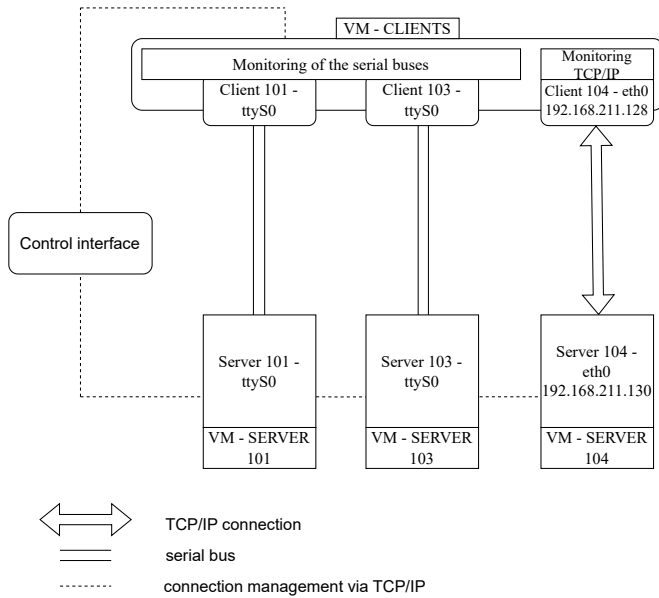


Fig. 2. Test scheme of the IEC 60870 protocol simulator

Figure shows a diagram of the operation of the communication simulator. This diagram meets all the objectives, as it contains 4 virtual stations – 1 virtual station where clients of all mentioned protocols run, and 3 virtual stations, where one of the servers operates in each of them. These virtual stations are shown in the diagram as VM – CLIENTS, VM – SERVER 101, etc. Servers are shown in the diagram as Server 101, Server 103, etc. They also described which communication interface they are working on. All protocol clients are running on the VM – CLIENTS virtual station. At the same time, network monitoring is connected to the clients, but for the IEC 60870-5-101/103 protocol, the monitoring of serial buses is involved, whereas, for the IEC 60870-5-104, it is monitoring TCP/IP connection. For clients, as well as for servers, it is also noted on which communication interface they operate. Here only exception is Client 104, which operates on the *eth0* interface. For better and clearer functionality, a *Control Interface* is also added, which will subsequently manage all simulators of each protocol and will be the GUI of the simulator. The double-sided arrow indicates a TCP/IP connection, the two parallel lines mark the serial bus connection, and the dashed line is used to connect the Control Interface to the individual clients and servers.

The GUI will provide features such as configuration settings where the user will be able to specify parameters such as communication modes (client/server), message types, data objects, and network settings. It will also provide data visualization where the GUI will offer graphical representations of simulated data, such as charts, tables, and plots, to facilitate

data analysis and interpretation. The last important thing is going to be error handling where will GUI provide feedback on simulation errors and issues, helping users troubleshoot and debug their implementations.

IV. CONCLUSION

In the realm of operational communication generators and simulators, numerous manufacturers offer a variety of solutions. While companies provide unique tools, not all adequately cover a broad spectrum of ICS protocols. Some focus solely on specific protocols or offer limited support for various industrial control standards. Few companies specialize in simulating the IEC 60870 protocol, crucial for many industrial applications, especially in the energy sector.

In this paper, we introduced the concept of an IEC 60870 communication simulator. This simulator offers a versatile platform for testing, research, and education in the energy and automation sectors. Its modular architecture, with components for protocol handling, message parsing, data simulation, and a user-friendly graphical interface, ensures flexibility and usability. Our simulator represents a significant contribution to the field a comprehensive solution to the challenges of communication protocol testing and development. Our simulator’s potential for implementation in industry devices enhances its utility, bridging the gap between theoretical exploration and practical deployment. In the context of future development, the communication simulator will be optimized for better performance and efficiency. Additionally, support for communication protocols such as IEC 61850, DNP3, Profinet, EtherNet/IP will be expanded to enable communication simulation across various devices, including ABB REC615 and PQ monitor MEG44PAN. The simulator’s GUI will be enhanced with new features such as data visualization, communication statistics, and interactive elements for scenario creation.

REFERENCES

- [1] C. Rohmingtuanga, S. Datta, N. Sinha, and T. S. Ustun, “Scada based intake monitoring for improving energy management plan: Case study,” *Energy Reports*, vol. 9, pp. 402–410, 2023.
- [2] T. Cherifi and L. Hamami, “A practical implementation of unconditional security for the iec 60780-5-101 scada protocol,” *International Journal of Critical Infrastructure Protection*, vol. 20, pp. 68–84, 2018.
- [3] G. Cheng, Y. Lin, A. Abur, A. Gómez-Expósito, and W. Wu, “A survey of power system state estimation using multiple data sources: Pmus, scada, ami, and beyond,” *IEEE Transactions on Smart Grid*, 2023.
- [4] G. Clarke and D. Reynnders, *Practical modern SCADA protocols*. Oxford: Newnes, 2004.
- [5] V. Skoko, B. Atlagic, and N. Isakov, “Comparative realization of iec 60870-5 industrial protocol standards,” in *2014 22nd Telecommunications Forum Telfor (TELFOR)*. IEEE, 2014, pp. 987–990.
- [6] Y. RUDZINSKI and P. VLADYKA, “Komunikační protokoly pro dálkové ovládání iec/iso 60870-5,” 2010.
- [7] P. Matoušek, *Description and analysis of IEC 104 Protocol*. Faculty of Information Technology BUT, 2017. [Online]. Available: <https://www.fit.vut.cz/research/publication/11570>
- [8] M. Uzair, “Communication methods (protocols, format & language) for the substation automation & control.”
- [9] A. Sudhakar, R. C, and A. S, “Implementation architecture of iec 60870-5-103 communication protocol on arm platform running on rtos for industrial ieds,” in *2022 4th International Conference on Inventive Research in Computing Applications (ICIRCA)*, 2022, pp. 80–86.