Petro Baran[1], Yuriy Varetsky[1,2], Viktor Kidyba[1], Yaroslava Pryshliak[1], Igor Sabadash[1], Oleksandr Franchuk[3]

Lviv Polytechnic National University (1),
AGH University of Science and Technology (2),
Institute of Microprocessor Control Systems for Power System Objects, Lviv, Ukraine (3),

doi:10.15199/48.2022.05.03

VPN-based monitoring power system facilities

Abstract. *Power system substations are usually controlled from a central control point using various telemechanical systems. At most substations in Ukraine without permanent staff, operational maintenance and control are carried out either by operational field teams or remotely using telemechanical systems. Nowadays, all over the world, as well as in newly built substations in Ukraine, operational and dispatching services apply the principle based on wireless digital technologies. The article presents the results of developing a wireless information network based on ALTRA digital recorders using client-server Virtual Private Network technology.*

Streszczenie. *Stacje systemu elektroenergetycznego są zwykle sterowane z centralnego punktu sterowania za pomocą różnych systemów telemechanicznych. Obsługa operacyjna i sterowanie większości stacji elektroenergetycznych na Ukrainie, które nie posiadają stałego personelu, realizowane są przez operacyjne zespoły terenowe lub zdalnie za pomocą systemów telemechanicznych. Obecnie na całym świecie, a także w nowo budowanych stacjach na Ukrainie, służby operacyjne i dyspozytorskie stosują zdalne monitorowanie na podstawie bezprzewodowych technologii cyfrowych. W artykule przedstawiono wyniki opracowania bezprzewodowej sieci informacyjnej opartej na rejestratorach cyfrowych ALTRA z wykorzystaniem Virtual Private Network klient-serwer technologii. (M****onitorowanie obiektów systemu elektroenergetycznego w oparciu na sieć VPN)****.*

Keywords: ALTRA device, power system, information network, Virtual Private Network.
Słowa kluczowe: Urządzenie ALTRA, system elektroenergetyczny, sieć informacyjna, wirtualna sieć prywatna.

Introduction

A feature of the power system is the location of its facilities (power plants, substations, distribution points) over a large area. They are controlled from dispatching points located at a considerable distance from these objects - up to hundreds of kilometers. The second feature of power systems is the lack of permanent maintenance personnel at these facilities. Such conditions are especially typical for substations and distribution points with rated voltages up to 110 kV. Their operation is controlled remotely through telemechanical systems or with the involvement of operational field teams. The exchange of information between control points and objects of electric power systems is traditionally carried out via telemechanical channels. In the world practice of operating electrical systems, wireless wide-area measurement technologies are increasingly being implemented [1-4]. The use of digital technologies in the automation of power system objects (control, relay protection, signalling and measurement) allows replacing traditional telemechanical communications with modern digital wireless ones [5,6].

One of the tasks of dispatching power system objects is measuring electrical quantities at power plants, substations, distribution points. It includes measuring the operating quantities - voltage on the buses, currents in feeder connections, binary outputs of the electrical installation state sensors, etc. For this purpose, special devices - recorders are installed at the facilities of electric power systems.

Description of ALTRA recorder

The Institute of Microprocessor Control Systems for Power System Objects has developed a series of digital devices ALTRA [7, 8], designed to record operating voltages and currents, as well as binary outputs of state sensors of switching equipment and relay protection under normal operating conditions and in case of emergency events. Digital recorders ALTRA are currently operating at many power facilities in Ukraine.

ALTRA devices perform the following functions:

• record the digital oscillograms of the emergency transient electrical quantities;

• control the state of sensor binary outputs of electrical installations;

• save information about emergency events in non-volatile memory;

• calculate and display on the liquid crystal display the RMS values of all recorded quantities;

• allow viewing the characteristics of emergency events on the liquid crystal display.

The ALTRA device contains analog and binary inputs for monitoring external analog signals (voltages, currents) and binary signals of electrical installations. The device's connection to the external circuits to monitor the operating condition of the three lines and the substation bus section is shown in Fig. 1.

The operating condition quantities, which are not directly measured, are calculated based on the discretised instantaneous values of the bus phase voltages and the phase currents of the feeders that are directly monitored by the ALTRA device [9]:

• active, reactive and apparent powers in separate phases;

• power factor for individual phases;

• total active, reactive and apparent powers;

• total power factor.

The root-mean-square value of the Y parameter is calculated based on the discrete values measured within the power frequency cycle by the expression:

$$Y = \sqrt{\frac{1}{T}\cdot\int_0^T y^2(t)dt} \approx \sqrt{\frac{h}{2T}\cdot\sum_{k=0}^{N-1}(y_k^2 + y_{k+1}^2)}\,, \tag{1}$$

where T - is the power frequency cycle (f = 50 Hz); y_k, y_{k+1} – is the instantaneous values of operating condition quantities (voltages, currents) for k and $k+1$ sampling points; N - is the number of sampling intervals per cycle; $h = T/N$ - is the sampling step.

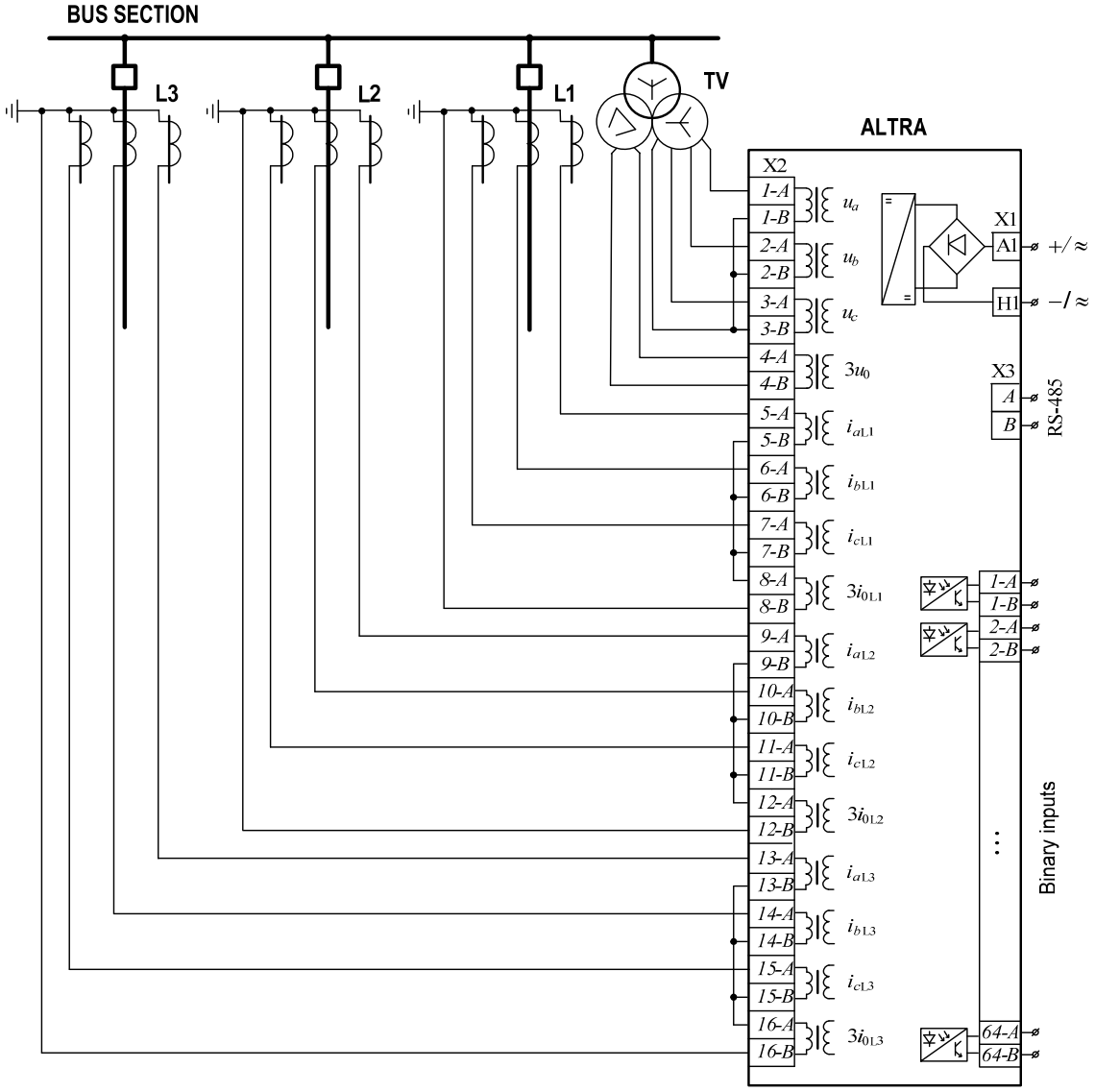

Fig.1. ALTRA connection to the external circuits

The calculation of active and reactive powers is carried out by the harmonic sine and cosine components of phase voltages and currents obtained based on Fourier transform as follows:

$$P = U_0 \cdot I_0 + \sum_{i=1}^{M} \frac{U_{si} \cdot I_{si} + U_{ci} \cdot I_{ci}}{2},$$
$$Q = \sum_{i=1}^{M} \frac{U_{si} \cdot I_{si} - U_{ci} \cdot I_{ci}}{2}. \quad (2)$$

The sine and cosine components of phase voltages and currents of the i-th harmonic $U_{si}, I_{si}, U_{ci}, I_{ci},$ are calculated using the next formulas:

$$Y_{si} = \frac{h}{T} \sum_{k=0}^{N-1} (y_k \sin(i\frac{2\pi kh}{T}) + y_{k+1} \sin(i\frac{2\pi(k+1)h}{T}));$$
$$Y_{ci} = \frac{h}{T} \sum_{k=0}^{N-1} (y_k \cos(i\frac{2\pi kh}{T}) + y_{k+1} \cos(i\frac{2\pi(k+1)h}{T})); \quad (3)$$

$$Y_0 = \frac{h}{2T} \sum_{k=0}^{N-1} (y_k + y_{k+1}).$$

A particular information network has been developed for monitoring the operation and testing of ALTRA devices, promptly changing their configuration during operation, reading and analysing digital oscillograms of emergency events stored in the device memory.

When developing an information network, preference is usually given to wired communication. In the absence of physical of information transmission channels, wireless communication with a GSM-based network is used [10, 11]. Until recently, Circuit Switched Data (CSD) technology was used in such wireless information networks.

VPN-based monitoring system

An information network for wireless communication based on Virtual Private Network (VPN) client-server technology has been developed [8] to replace the existing communication system. Secure Shell (SSH) protocol for remote control is used to protect the information in VPN. The OpenSSH library was used to implement this protocol [13, 14].

The use of VPN technology compared to CSD mode has some advantages: higher connection reliability, speed,

and online (permanent) connection. Moreover, CSD technology will not be supported by mobile operators in the near future. In addition, the quality of communication in the CSD mode is very low nowadays. Wireless communication based on VPN technology is carried out over a GSM network using GPRS, 3G or 4G standards.

The communication system configuration using VPN technology is shown in Fig. 2. The information network has a two-tier structure. The lower level is formed by digital ALTRA devices installed directly on the object.

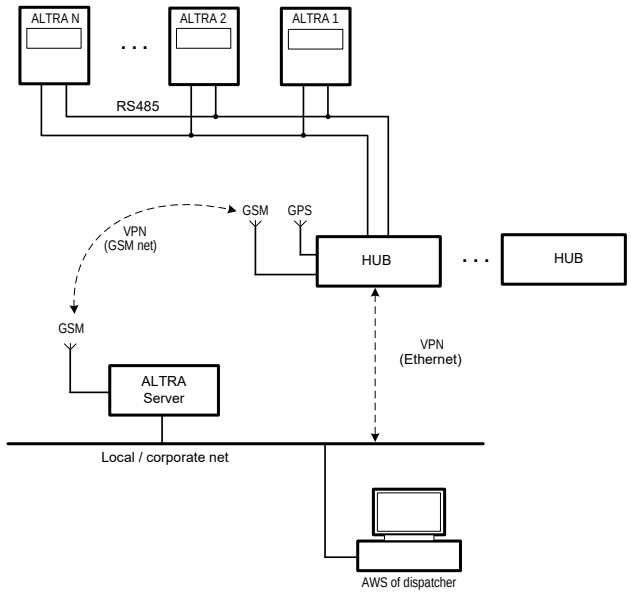

Fig.2. Communication system configuration using VPN technology

These devices are connected to the local network via a two-wire communication line type "twisted pair" using the RS 485 interface.

Access to ALTRA devices is organised based on the Hub. The Hub contains a built-in computer, GPS module and GSM modem. It gathers information from all ALTRA devices installed in the facility, its archiving, time synchronisation, and the transfer of information to the higher level of the control hierarchy.

The upper level of the information network consists of an ALTRA-Server and an automated workstation (AWS) of the power site dispatcher, which are connected to the local computer network.

ALTRA-Server consists of a built-in computer and a GSM modem. It collects information from the Hubs installed on the lower level and transmits it to the operator's AWS for its analysis. ALTRA-Server has a fixed IP address to provide which one can use a SIM-card with a fixed IP address. In terms of controllability, the ALTRA-Server is a passive device. Commands of the Hubs carry out the information transfer to ALTRA-Server, and from the ALTRA-Server device to the operator workstation - by the commands of the workstation.

The operator's AWS is implemented on a personal computer (PC) using special software. It displays the mnemonic diagram of the controlled object (power plant, substation, etc.) on a PC monitor. So, the operator can control ALTRA digital devices, analyse the information registered with them. It is possible to use several operator's AWS in the control system.

Hub and ALTRA-Server are developed on the platform of the Linux operating system and the operator's AWS - on the platform of the Windows operating system.

A secure tunnel is created between Hubs and ALTRA-Server using SSH protocol based on TCP connection for secure access to information. Asymmetric encryption technology, which involves using a key pair (closed and opened), is used to encrypt and decrypt information. Such an organisation ensures high reliability of data transmission and maximum protection against unauthorised access [10].

For additional protection of the local network, access to the ALTRA Server is carried out from the local network only through the specified ports, and access at the command of ALTRA-Server to the site's local network is prohibited.

The chart of information flows of the information network on the platform of ALTRA Server is given in Fig. 3. The Hub reads digital oscillogram files from ALTRA devices. They are then transmitted to the ALTRA Server using the SSH protocol. From there, they are read out at regular intervals by the operator's AWS using the same protocol.

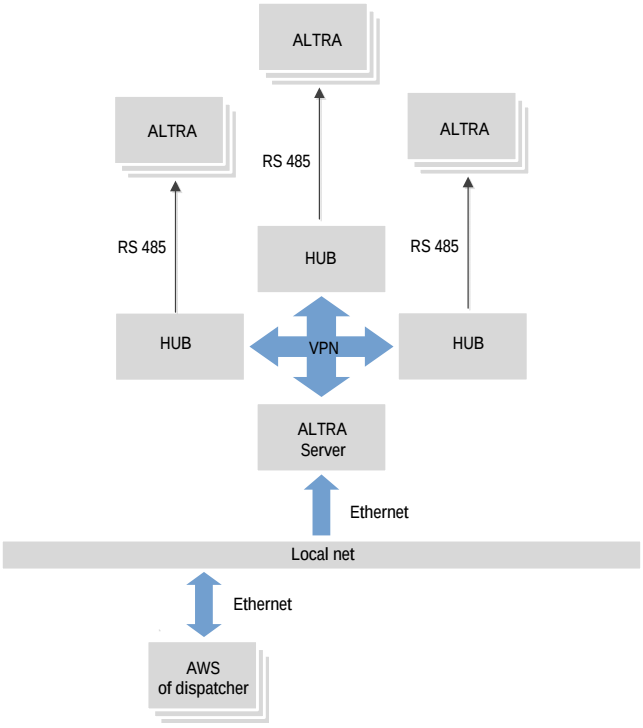

Fig.3. Measurement data flow chart on the ALTRA-Server platform

The possible sampling frequencies of the recording electrical signals in the ALTRA device is set in the device configuration in the range from 1500 Hz to 48000 Hz. From our field experience, the optimal sampling rate of most system transients in terms of aliasing errors, memory using and data transfer rate to the upper level is 3000 Hz or 60 samples for the industrial frequency cycle. However, if there is a need to record high-frequency transients in the power system, one can increase the sampling rate to 48 kHz. Fig. 4 shows an example of the transient behaviour recorded by the ALTRA device under the sampling frequency of 3000 Hz.

Essential functions of ALTRA device control, such as reading/writing configuration, running tests, setting a hub, etc., are executed from the operator's AWS via VPN using commands that provide authentication.

The developed information network of wireless communication on the platform of VPN client-server technology has been commissioned at many power system objects in Ukraine.

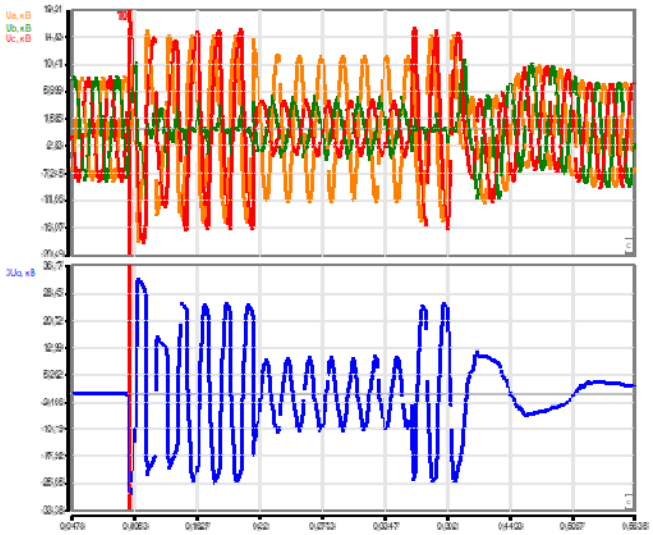

Fig.4. An example of the transient behaviour recorded by the ALTRA device under the sampling frequency of 3000 Hz.

The legal system in Ukraine does not prohibit the use of VPN services, as long as the use of VPN does not violate the rights of third parties and does not pose a threat to national security. VPN service is related to the legislation on personal data protection. Thus, from a legal point of view, the use of VPN data transmission technology in Ukraine is legal. The operation experience of these information networks has approved their high reliability, security and efficiency of data transmission.

Conclusions

The use of ALTRA devices at power facilities provides digital recording operating condition quantities, triggering events of relay protections and circuit breakers, and data transfer to the dispatcher's automated workstation.

Implementing VPN technology into an information network of the power system objects provides high reliability and security of data transmission and does not require additional technical means.

Digital oscillograms of an emergency event are automatically transferred to the PC monitor of the dispatcher's automated workstation, along with complete information about the emergency event.

The commissioning of information networks on the platform of VPN technology for the operational maintenance and control of power system facilities creates the basis for developing digital substations.

Acknowledgments

This research was financially supported by the Polish Ministry of Science and Higher Education (grant AGH 16.16.210.476).

***Authors**: assoc. prof. PhD Petro Baran, Lviv Polytechnic National University, E-mail: petro.m.baran@lpnu.ua; assoc. prof. PhD Viktor Kidyba, Lviv Polytechnic National University, E-mail: viktor.p.kidyba@lpnu.ua; assoc. prof. PhD Yaroslava Pryshliak, Lviv Polytechnic National University, E-mail: yaroslava.d.pryshliak@lpnu.ua; assoc. prof. PhD Igor Sabadash, Lviv Polytechnic National University, E-mail: ihor.o.sabadash@lpnu.ua; Oleksandr Franchuk, Institute of Microprocessor Control Systems for Power System Objects, Lviv, Ukraine, E-mail: olexandr@imskoe.org.ua; prof. DSc Yuriy Varetsky, AGH University of Science and Technology, E-mail: jwarecki@agh.edu.pl*

REFERENCES

[1] F. Salim, K. M. Nor, D. M. Said, "Experience in online power quality monitoring through VPN," IEEE 15th International Conference on Harmonics and Quality of Power, pp.482-485, 2012.

[2] D. Karlsson, M. Hemmingsson, S. Lindahl. Wide Area System Monitoring and Control. IEEE Power & Energy Magazine, no.2(5), pp. 68-76, 2004.

[3] K. E. Holbert, G. T. Heydt, And Hui Ni, "Use of satellite technologies for power system measurements, command, and control," Proceedings of the IEEE, vol. 93, no. 5, pp. 947-955, 2005.

[4] Sun FengJie, QI Qi, Fan JieQing, "Real-time signal time delay analysis of WAMS based on MPLS VPN Technology," The International Conference on Advanced Power System Automation and Protection, pp. 1089-1093, 2011.

[5] V.I. Vasilchenko, O.G. Hryb, and O.V. Leleka, "Digital substation as a component of the Smart Grid system," Electrical engineering and electromechanics, № 6, pp. 72-76, 2014.(in ukr.)

[6] V.G Glovatsky, I.V. Ponomarev, "Modern means of relay protection and automation of electric networks," Energomashvin, 2003, 535 p. (in rus.)

[7] M.V. Bazylevych, R.S. Bozhyk, and I.O. Sabadash, "Microprocessor information-diagnostic system ALTRA for selective identification of grounded phase feeder," Energy engineering and electrification, Kyiv, № 7, ph. 91 – 95, 2003. (in ukr.)

[8] P.M. Baran, V.P. Kidyba, I.O. Sabadash, and M.V. Bazylevych, "Application of digital devices ALTRA in operational and dispatch control of substations," Electric networks and systems, № 4-5, pp. 42–45, 2016. (in ukr.)

[9] M.V. Bazylevych, P.M. Baran, V.P. Kidyba, G.M. Lysiak, and I.O. Sabadash, "Physical model of the telemechanical system for operational and dispatch control of substations," Bulletin of the Lviv Polytechnic National University. Electric Power and Electromechanical Systems, № 870, pp. 3-8, 2017. (in ukr.)

[10] I.V. Gorbaty, A.P. Bondarev, Telecommunication Systems and Networks. Principles of Operation, Technologies and Protocols: textbook. manual, Lviv Polytechnic Publishing House, 2016. (in ukr.)

[11] V.I. Popov, Basics of Cellular Communication of the GSM Standard, M .: Eco-Trends, 2005. (in rus.)

[12] O. Kolesnikov, B. Hatch. Linux: Creating Virtual Private Networks (VPNs): Trasl. with English, M .: Kudic-Obraz, 2004. (in rus.)

[13] D.J. Barrett, R. Silverman, SSH, The Secure Shell: The Definitive Guide, O'Reilly, 2001.

[14] M. W. Lucas, SSH Mastery: OpenSSH, PuTTY, Tunnels and Keys, Tilted Windmill Press; 2nd ed., 2018.