11TH INTERNATIONAL SCIENTIFIC CONFERENCE ON DEFENSIVE TECHNOLOGIES
OTEH 2024
Serbia, Tara, 9-11 October 2024

DIGITAL RADIO SYSTEM FOR REMOTE MONITORING AND CONTROL ON THE MEDIUM VOLTAGE DISTRIBUTION NETWORK USING THE PDR 300 RADIO DEVICE AS A TRANSMITTER

MARIJA MATOVIĆ
Electrodistribution, Kraljevo, marija.matovic@es.rs

ANA MATOVIĆ
Military Quality Control, Belgrade, ana.matovic4@gmail.com

IVICA MARJANOVIĆ
Military Quality Control, Belgrade, ivicabeogrd@gmail.com

Abstract: *As part of the expansion of the medium-voltage distribution network of the system for remote monitoring and control, the communication connection of the end locations with the control center will be made. For many years, remote monitoring and control systems of the medium-voltage electric distribution network based on digital packet radio communication have been used, using the open protocol DNP3 between remote stations and data concentrators, as well as between data concentrators and SCADA applications. The systems work according to the event, that is, the end stations initiate communication in the event of an event, while the end stations are periodically polled from the concentrator to determine whether the remote station is in communication. Implementation of the DNP3 protocol throughout the system enabled an event logger with time created at remote stations with millisecond resolution. Due to the location expansion of the medium voltage distribution network into a system for remote monitoring and control, the communication connection of the end locations with the control center will be made. The purpose is that all end locations can be managed from the control center, so that from the control center it will be possible to read measurements and signals on the switchgear and issue commands. The remote monitoring and control system consists of a SCADA server, data concentrator, repeater and PDR 300 radio end devices.*

Keywords: *radio device PDR 300, remote monitoring and control, communication protocols.*

1. INTRODUCTION

For the modernization of the existing system of remote monitoring and management of the medium voltage distribution network, for the operation of the monitoring system, the radio device PDR 300 is used, which is a transceiver, which enables the transmission of telemetry data, necessary for the operation of the monitoring and control system over long distances [12]. The field of application of data transmission networks with PDR 300 radio devices is in water/wastewater treatment plants, electricity distribution, gas distribution, oil distribution, wind turbines, industrial process management, remote traffic control, railway communication systems, remote control with assistance PLC elements.

PDR 300 radio PDR 300 supports operation with a wide range of existing communication protocols widely used in remote monitoring and control systems, including DNP3, IEC870, RP570, COMLI, Modbus, Cooper/PG&E 2179, L&G Telegyr 8979, Twacs by DCSI, Turtle by Hunt, Exoline, Cactus, PRIP and Aquacom by ITT Flygt. It also supports the User Defined Protocol option, which provides the ability to use any communication protocol that you define yourself the user [7]. In many modern systems for data transmission, as well as in the system of remote monitoring and management of the medium voltage distribution network, high security is insisted upon. That's why the PDR 300 enables extremely secure encryption of radio messages, namely the 128 bit key XTEA cipher.

This radio device for data transmission is suitable for remote monitoring and management of medium voltage distribution network, which works on the roll call principle, as well as in systems with event-triggered communication. In systems with event-triggered communication, the functionality of the PDR 300 device called Collision Avoidance is used, which prevents the "collision" of radio messages, thereby significantly speeding up communication between devices in the system. The device also supports Peer-To-Peer communication mode.

The PDR 300 radio device system consists of one master device and a maximum of 120 slave devices. Each slave device can work as a signal repeater, an independent device or can be connected to one or more RTU devices (Remote Terminal Unit) or IED devices (Intelligent Electronic Device).

The message can be transmitted to the end radio device via up to six devices, ie. in seven jumps. In this way, the message in the PDR 300 radio device system can be

Corresponding author: M.Matović;
E-mail: marija.matovic@es.rs
DOI: 10.5937/OTEH24078M

transmitted over a distance of over 300 km (190 miles), depending on the specific topography of the terrain of the remote monitoring and control system of the medium voltage distribution network [8]. The data transfer rate can be 4800, 9600 or 19200 bps. Forward Error Correction is a standard function that enables the correction of a very large number of errors in signal transmission, which occur due to the appearance of noise, thereby increasing the sensitivity of the radio device.

The RTU/IED/SCADA system for remote monitoring and control connects to the PDR 300 radio device via a standard RS-232 serial interface. The baud rate of the serial interface is adjustable between 600 and 19200 bps. The configuration of the PDR 300 radio device involves setting a minimum number of parameters, which are easily accessed using a handheld terminal or a personal computer, using a standard terminal program in Windows.

The PDR 300 radio provides non-invasive diagnostics, remote parameter modification and has built-in test and verification functions, easily accessed via a handheld terminal or personal computer, which is achieved using the PDR 300 radio. This radio has two Ethernet ports that use standard RJ45 connector and communication speed from 10Mbps to 100Mbps. It is used for software support and updates. Also, it is intended for future TCP/IP protocols.

The remote monitoring and control system of the medium voltage distribution network uses a data collection device, or the data concentrator GW 502 is a central and communication unit, which provides excellent protocol conversion functions. Available master protocols: IEC60870-5-101, IEC60870-5-103, IEC60870-5-104, IEC61850, DNP3, SPA, (Netcon 8830, 8810), Modbus, Tecoma, ANSI, NPA, Procol, ADLP80, ADLP180, RP570 , RP571, (Felek 400, 4000), etc. As the product is in constant development, the number of supported protocols is constantly increasing.

2. AREA OF APPLICATION

Reasons for using wireless technologies:
- Avoid laying cables in places where it is difficult, expensive or impossible.
- No leased dial-up connections are used, thus reducing costs. Independence from communication service providers is achieved.

Areas of application:
- Water/wastewater treatment plants
- Distribution of electric energy
- Gas distribution
- Oil distribution
- Wind generators
- Management of industrial processes
- Remote traffic control
- Communication systems on railways
- Remote control with the help of PLC elements

Figure 1. Examples of typical data network configurations with PDR 300 radios

Point – to – point

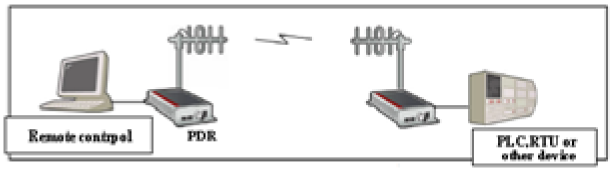

Figure 2. Point-to-point

Point – to – multipoint

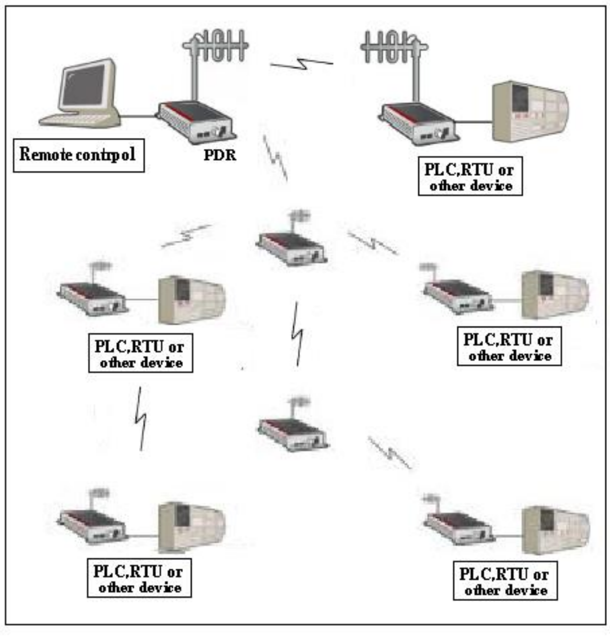

Figure 3. Point-to-multipoint

Distribution of electricity

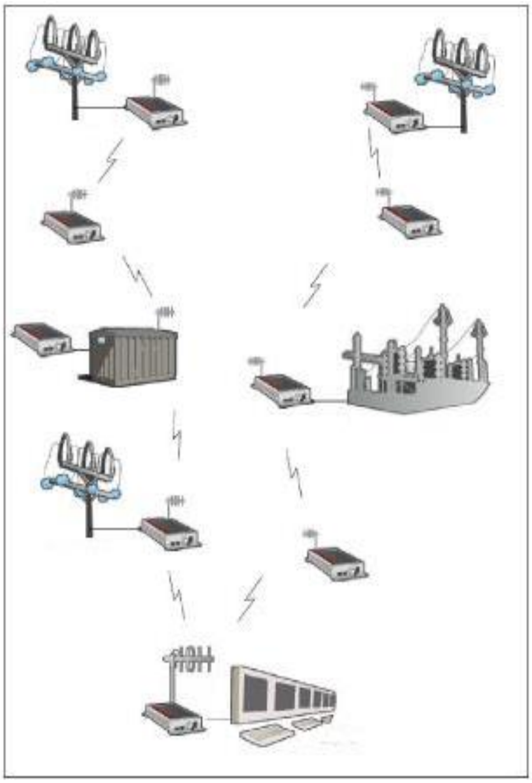

Figure 4. PDR radios in the power distribution network management system

3. FUNCTIONALITY OF THE PDR 300 RADIO DEVICE

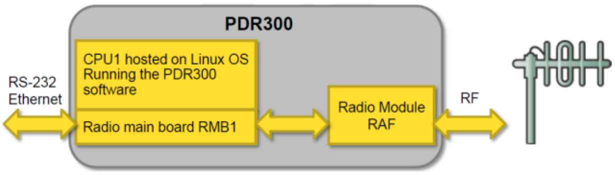

Figure 5. Functional block diagram of the PDR 300 radio device

RS-232 to RF

Serial data comes to the serial port. The MCU (Micro Controller Unit) analyzes the data and frames it, then sends it to the modulation unit. The entire message is temporarily stored in the processor's memory before being forwarded to the modulation unit. The modulation unit converts the sequence of bits into a 4-level baseband signal that is modulated in the radio transmitter.

RF to RS-232

The modulation unit decodes the 4-level baseband signal and forwards it to the MCU. The MCU analyzes the message and sends it to the serial port or forwards it via radio, if the device is working as a repeater in the case of that particular message.

FEC - Forward Error Correction

When sending data, FEC (Forward Error Correction) bits are added to the data being transmitted, before it is converted to a 4-level baseband signal. When receiving data, based on the information from the FEC bits, the FEC algorithm is applied, which corrects errors in signal transmission. A large part of such errors can be corrected using the FEC functionality.

CRC – Cyclic Redundancy Checksum

When sending a signal, at the end of the message, i.e. data string, a CRC byte or bytes is appended. The CRC byte is calculated based on the content of the message. The receiver checks the CRC byte according to the received data and thus detects errors in signal transmission. Corrupted messages are eliminated. If the CRC byte is incorrect, the radio receiving the message does not send back a Non-acknowledgement message (NACK). Any retransmission of the signal should be initiated by the connected IED. This is triggered using a response delay.

Communication

The radio device PDR 300, in the data transmission system, can work as a master or slave/repeater. In each radio device in the system, information about the path for signal transmission, addresses of remote end stations (RTU - Remote Terminal Unit), identification of radio devices and repeaters is configured.

When the control system sends a message to the master device, the master recognizes the address of the message, i.e. its destination. The master checks whether there is a slave device with an identification corresponding to the address from the message in the table of radio devices in the system. If there is, the master checks whether the message should be forwarded through one of the repeaters in the system. Finally, the master transmits the message to the slave device. The response of the slave device is transmitted in the same way.

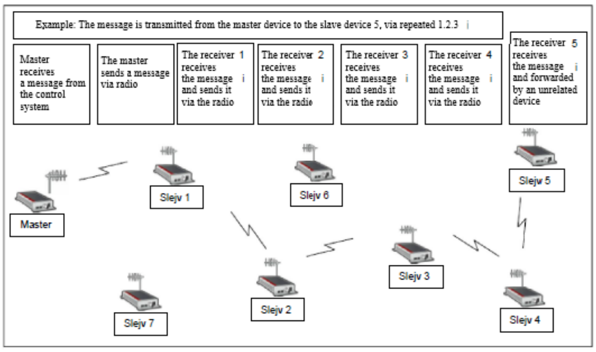

Figure 6. Example of message transmission in the PDR system

Protocols supported by the PDR 300 radio

The radio device PDR 300 currently supports the following protocols for SCADA system communication with the RTU:

- DNP3
- IEC870 (IEC 870-5-1) RP570
- COMLI
- Modbus RTU
- Aquacom
- DCSI
- Hunt 1
- Telegyr 8979
- Cooper/PG&E 2179
- Exoline
- Cactus
- ADJ

These protocols are available as factory settings in the configuration menu of the PDR 300 radio. Protocols not listed can be used using the User Defined Protocol option, which is available in the same configuration menu.

In normal cases, it is only necessary to select the desired protocol in the master radio device. The Direct Routing option is selected in the slave radio, if the message is always forwarded to the same master radio.

User Defined Protocol

The User Defined Protocol option can be applied to any protocol that contains a destination address. The destination address can consist of one or two bytes of data and must always be in the same position in each type of message.

Normally, the User Defined Protocol option is configured only in the master radio. The Direct Routing option is selected in slave radios, if messages are always forwarded to the same master radio.

Direct Routing

The Direct Routing option can be applied in all slave devices of the PDR 300 radio device network, if their messages are always forwarded to the same master devices or to the SCADA system. This eliminates the need to enter addresses of SCADA systems or RTU devices into slave radios. It is only necessary to configure the communication path from the slave device to the master device.

4. ENCRYPTIO – CODING, ENCRYPTION

The radio device PDR 300 has the option of encoding (encrypting) messages. A 128-bit encryption key, called XTEA, is used. The user can define a code key, as a hexadecimal numerical value of 32 characters in length, in each radio device in the network.

XTEA's digital encryption makes the radio network as secure as any other encrypted system or encrypted IP network.

5. SENSITIVITY OF THE PDR 300 RADIO RECEIVER

The sensitivity of the receiver depends on the frequency used, the distance between the channels (12.5 / 25 kHz) and the bit rate (4800, 9600 or 19200 bps). The sensitivity of the receiver is measured by introducing an attenuation to a signal consisting of a known sequence of bits, until a bit error occurs. This is an example of a common way of representing receiver sensitivity:

-110dBm @ BER (Bit Error Rate) < 1x10-6

The value of the sensitivity of the receiver in many cases depends on the known sequence of bits used in its measurement. A series of random bits is used when determining the sensitivity of the receiver, which includes all possible variations in the arrangement of bits in the series and represents the most difficult possible case, which is why it gives very reliable measured values of the sensitivity of the receiver.

Insufficiently good sensitivity of the receiver can be compensated by using antennas with amplification or increasing the power of the output signal. The application of antennas with amplification is the solution most often used in such cases.

It should be noted that the effects of improper antenna installation cannot be compensated by the use of a highly sensitive radio device.

Sensitivity can be used in signal propagation analyzes in radio network planning.

Table 1. PDR 300 radio receiver sensitivity

Model	Frequency range [MHz]	Channel width [kHz]	Data transfe rate [bps]	Sensitivy BER < $1x10^{-6}$
PDR 300	UHF 440 - 470	12.5	4800 / 9600	-116 dBm / - 110 dBm
PDR 300	UHF 440 - 470	25	9600 / 19200	-113 dBm / - 105dBm

6. STRENGTH OF THE TRANSMITTER

Power ranges of radio transmitters are from 0.001 to 5.0 W.

Radios can be set by the user to a certain range of output signal strength. This is achieved by using a suitable configuration interface, and there is also an option for remote control.

7. TRANSMITTER STRENGTH RSSI – RECEIVED SIGNAL STRENGTH INDICATION - INDICATION OF THE POWER OF THE RECEIVED SIGNAL

The value of the RSSI magnitude is used to determine the quality of the radio link. RSSI values can be obtained by running the Radio Link Test from the configuration menu.

The PDR 300 radio device measures RSSI values with the help of an A/D converter. The strength of the received signal is obtained by measuring the voltage and is expressed in volts and translated into a value expressed in dBm.

The following graph shows typical RSSI voltage values given as a function of signal level.

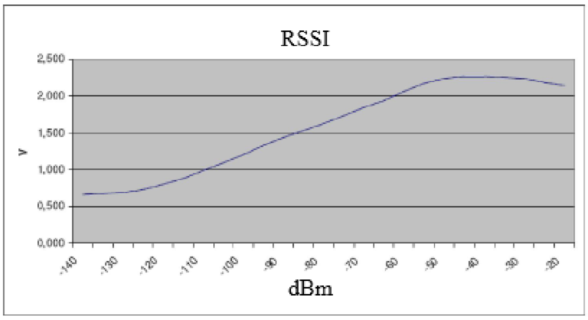

Figure 7. RSSI

7. CONCLUSION

For the implementation of the system for remote monitoring and control, he suggests the radio device PDR 300 due to its good technical characteristics. The main advantage of this device is that it enables the transmission of telemetry data, necessary for the operation of the monitoring and management system, over long distances. The device is intended to work in specific environments that require point-to-multipoint data transmission, which are found in water treatment plants, waste water, industrial plants, power systems, gas extraction plants, oil extraction plants, wind turbine plants, plants for managing industrial processes, plants for remote traffic control, for railway communication systems, plants for remote control with the help of PLC elements.

One of the essential features of the PDR 300 radio device is that it supports work with a wide range of existing communication protocols of wide use, which are used in remote monitoring and control systems, which provides the possibility of using any communication protocol, determined by the user himself.

A very important feature is the reliability of the PDR 300 radio device when transmitting messages in the system, where messages can be transmitted over a distance of over 300 km (190 miles), depending on the specific topography of the terrain. Also, an important application of this radio device is in systems that work on the roll call principle, as well as in systems with event-triggered communication. In systems with event-triggered communication, the functionality of the PDR 300 device called Collision Avoidance is used, which prevents "collision" of radio messages, which significantly speeds up communication between devices in the system.

Simplicity of access using a handheld terminal or personal computer enables non-invasive diagnostics, remote parameter modification and has built-in functions for testing and verification, are the main advantage of this radio device, as well as Forward Error Correction, a standard function that enables the correction of a very large number of errors in signal transmission, which occur due to the appearance of noise, which increases the sensitivity of the radio device.

Literature

[1] S. Stankovski, N. Đukić, S. Tegeltija, R. Kovač and I. Baranovski, “Wireless Parking Access Control,“ 15. International Scientific Conference on Industrial Systems, pp. 136-139, 2011.

[2] E. Ferro and F. Potorti, “Bluetooth and Wi-Fi Wireless protocols: a survey and a comparison,“ Wireless Communications, pp. 12 – 26, 2005.

[3] R. Kovač, S. Horvat, I. Šenk, L. Tarjan and V. Jovanović, “Wi-Fi system for monitoring the student attendance at university lectures,“ 15. International Scientific Conference on Industrial Systems, pp. 160-164, 2011.

[4] Z. Rongbo and Y. Yuhang, “Model-based admission control for IEEE 802.11e enhanced distributed channel access,“ AEU - International Journal of Electronics and Communications, vol. 61, no. 6, pp. 388–397, June 2007.

[5] G. Ostojic, S. Stankovski, M. Lazarevic and V. Jovanovic, “Implementation of RFID technology in parking lot access control system,” Proceedings of the 1st RFID Eurasia Conference in Istanbul, Turkey, pp. 49-53, 2007.

[6] L. Tarjan, I. Šenk, R. Kovač, S. Horvat and G. Ostojić, “Automatic identification based on 2D barcodes,” 15. International Scientific Conference on Industrial Systems, pp. 130-135, 2011.

[7] Akbar A., et al., 2013, Session Initiation Protocol, International Journal of Scientific and Engineering Research Volume 4, ISSN 2229-5518, str. 5.

[8] http://mreze.layer-x.com/ , Septembar, 2014., Eldis Mujarić, dipl. ing., Računalne mreže,

[9] TelecomSpace, Signaling Connection Control Part (SCCP), available at http://telecomspace.com/ss7-sccp.html, 15.7.2014.

[10] A. S. Tanenbaum, Računarske mreže, Микро књига, Београд, 2005.

[11] Комутациони системи, available at http://telekomunikacije.etf.rs/predmeti/te4ks/docs/KS/KS10.docx

[12] D. Mitić, „SYSTEM FOR REMOTE SUPERVISION AND CONTROL OF POWER ELECTRONICS DEVICES ”, 32. Međunarodni skup MIPRO 2009, Zbornik Radova Telekomunikacije i informacije, Vol. II. CTI, ISBN 978-953-233-043-4, Opatija, Hrvatska, Maj 25-29. 2009. god.

[13] Časlav Stefanović, Marija Matović, Danijel Đošić, Srđan Maričić, Ana Matović, "Level crossing rate of the random variables", INFOTEH-JAHORINA, Vol. 10, Ref. B-I-4, ISBN 978-99938-624-6-8, Mart 20-23, 2013.