ISSN 1392 – 1215

ELECTRONICS AND ELECTRICAL ENGINEERING

ELEKTRONIKA IR ELEKTROTECHNIKA

2012. No. 7(123)

TELECOMMUNICATIONS ENGINEERING

TELEKOMUNIKACIJŲ INŽINERIJA

Migration of the IT Technologies to the Smart Grids

L. Cepa, Z. Kocur, Z. Muller

Faculty of Electrical Engineering, Czech Technical University in Prague, Technicka 2, 166 27 Praha 6, Czech Republic, phone: +420 22435 2083, e-mails: cepaluka@fel.cvut.cz, zbynek.kocur@fel.cvut.cz

crossref http://dx.doi.org/10.5755/j01.eee.123.7.2390

Introduction

The Smart Grids are the electrical and communications networks that allow regulating the production and consumption of electricity in real time. This technology introduces a sophisticated and effective management at the level of resources into the power grid. There is necessary to propose a sufficiently dimensioned data network to ensure the effective management.

The main goal of this paper is to provide an introduction to industrial control networks. The paper also describes the current situation of these networks and the gradual migration of IT technologies from ICT networks to industrial control networks. Finally, the last goal of this paper is to perform a view of the possible future development of data networks in industrial control networks.

Characteristics of industrial control networks

The basic function of industrial control networks (ICN) is to provide communication between the control systems and their subordinate subsystems such as sensors, actuators, etc. The ICN networks can be divided, among others, according to the branches of industry in which they are used: power and utilities (water and gas) called ICNPG, automated production lines, refineries, breweries, intelligent buildings, airplanes, cars, etc.

Each subgroup has specific requirements and demands on the operated services. This paper will further describe only ICNPG networks, namely the Smart Grids. There are following services for ICNPG networks: control (local or remote), optimization, supervision, and remote reading of data from electricity meter called AMM (Automated Meter Management).

ICNPG networks are typically used in two or three purpose-built plans in the power grids:

- Global control including SCADA (Supervisory Control And Data Acquisition) systems, main process servers, etc.;
- Process bus including PLC (Power Line Communication) links and RTU (Remote Terminal Unit);
- field bus including digital sensors, actuators, IED (Intelligent Electronic Devices).

The different proprietary technology is still used for each level of ICNPG network. Modern ICNPG networks use a standardized protocol IEC 61850 series for communication between sensors, actuators and local control system in the power grids. This protocol is based on the automated, data- and network-oriented principles of management at the level of substation. A standardized protocol IEC 60870-5-104 is used for communication between the dispatching center and different substations or dispatching center and other power systems of the distribution power grid (switching substations, transformer substations, etc.). This protocol is based on the TCP/IP (Transmission Control Protocol/Internet Protocol) family of protocols. This whole system is generally known as SCADA and includes a core network that uses IP. The goal of SCADA system is the superior central monitoring (data collection) and control of power systems or processes.

The specific requirements for the ICNPG network can be summarized as follows:

- Support of deterministic real-time communications;
- Availability 24 hours a day, 7 days a week;
- High level of data traffic safety;
- Sufficient reserve of bandwidth;
- Simple implementation and easy management;
- Easy detection of problems and their rapid elimination;
- Easy segmentation, scalability and expandability;
- Support for standardized solutions and compatibility of device manufactures;
- Accurate defined emergency plan of solving the problems.

The fundamental features that should respect each ICNPG network can be summarized as follows: availability, quality, integrity, and authenticity.

Differences between ICNPG and ICT

The ICNPG network components must be designed with the regard to the difficult conditions which they are used in practice.

The certain parts of ICNPG network are an integral part of management processes in real time seen from the perspective of applications. Therefore, the strict requirements for timely and deterministic delivery of the data units (segments, packets and frames) are required, particularly at the lowest levels. The applications of the ICT network are related to the customer and his own understanding of the specific quality of the application.

The size of delay can range from 1s for slow processes, 10-100ms for faster processes up to the values less than 1ms for the control of various time-consuming processes. Therefore, the required maximum delay is necessary to be known for proposal of the specific ICNPG network.

The ICNPG networks require guaranteed QoS (Quality of Service) of transported data units between the terminals regarding the minimum delay and jitter. These requirements are not required for the most services of the ICT networks, except VoIP (Voice over IP), see [6,7]. The non-compliance with the quality of transmission may inflict negative impact either operational for ICNPG networks or economic and security.

Both networks are different seen from the perspective of data traffic character. The ICNPG networks are characterized by sending the short data maybe of a large amount. The ICT networks have the burst character of data traffic in the total large volume.

Another important difference is the topology of node interconnections. The extended star without redundancy that is commonly used in the ICT networks is entirely insufficient in most of the ICNPG networks because of the lack of redundancy. It must also respect the resistance against the communication failure. This topology is depicted in the Fig. 1a. There are several redundant topologies in the ICNPG networks as described in the section Topology.

Definition of availability and reliability

The availability and reliability performs an important characteristic of the ICNPG network. The availability of the ICNPG network must meet more strict requirements in comparison with ordinary ICT network. The inability to meet these criteria can result into errors during the control sequence. It can result into disastrous situations related to loss of profits and shutdown of the production process in some cases. The strict requirements for the ICNPG networks result into more rigorous philosophy of the design, construction and management than usual in the ICT network. Despite the fact that some components of ICT networks are used in the ICNPG networks.

The basic parameters of availability and reliability of the ICNPG network can be summarized as follows:

1. Appropriate QoS with respect of the transmission parameters which include:
   a. required bit rate,
   b. required maximal bit error rate,
   c. maximum size of the delay with preserved the maximum dispersion of incoming times of the data units.
2. Ensurance of the required availability of services.

The reliability is often used as an extent of trouble-free system function. It can be quantified as the mean time between failures (MTBF) expressed in hours or as the failure rate expressed in hours of -1. The failure rate defines the number of failures per unit time. The parameter called availability (A) is used to express the trouble-free state of the system in practice that takes into account the time needed to repair the failure. The mean time to repair (MTTR) that is expressed in hours is present in the definition of availability. The availability is given by

$$A = \frac{MTBF}{MTBF + MTTR}. \qquad (1)$$

The availability is a dimensionless value that ranges from 0 to 1. The value 0 represents a permanently malfunctioning system. The value 1 represents a failure-free system. The value of availability for real systems is approximately 1. The maximum time of failure for year, month and week is shown in the Table 1. Table 1 shows the concrete values of availability expressed in % (i.e. A% = A*100).

Current trends of information technology in ICNPG

The Ethernet technology that was designed for the ICT networks with non-guaranteed delay and random access to the media gets to the forefront in the ICNPG network today.

Table 1. The maximum time of failures for year, month and week [1]

Availability %	Total time of failure per year	Total time of failure per month	Total time of failure per week
90	36,5 days	72 hours	16,8 hours
95	18,25 days	36 hours	8,4 hours
98	7,3 days	14,4 hours	3,36 hours
99	3,65 days	7,2 hours	1,68 hours
99,5	1,83 days	3,6 hours	50,4 minutes
99,8	17,52 hours	86,23 minutes	20,16 minutes
99,9	8,76 hours	43,2 minutes	10,1 minutes
99,95	4,38 hours	21,56 minutes	5,04 minutes
99,99	52,6 minutes	4,32 minutes	1,01 minutes
99,999	5,26 minutes	25,9 seconds	6,05 seconds
99,9999	31,5 seconds	2,59 seconds	0,605 seconds

The Ethernet technology is a fully standardized technology that is widely used in the practice in the ICT networks This technology is gradually spreading to the ICNPG networks thanks to good price of Ethernet and with the coming of full-duplex variations that allows to guarantee the required QoS.

The same fact is true for TCP/IP family of protocols. It is often rather software expandability of this family of protocols. There are many possibilities of their implementation to end industrial devices due to the large expansion of this family of protocols.

Finally, there are applications that can be advantageously used in the ICNPG networks such as the database systems and operating systems that are needed for control applications. The advantage of the existing operating systems is fact that the systems are constantly evolving.

Smart Grid technology

There are many definitions of Smart Grids today. The purely technical interpretation respecting the true nature of smart power grids is one of them: “The Smart Grids are electrical and communication networks allowing the regulation of the production as well as consumption of electricity in real time”. The Smart Grid technology is based on a large number of scattered sources such as power plants with capacity of hundreds of MW or even smaller sources with power capacities of hundreds of kW coupled to MW units.

This technology introduces a sophisticated and effective management at the level of resources into the power grid. The goal of Smart Grid technology is to reconfiguration of the power grid on the basis of information about current consumption of electric energy in order to achieve the smallest energy losses in energy transmission path. The goal of reconfiguration is also effective use of all sources. The scattered sources and smart management allow very efficient solution of critical situations that may occur in failure of the power grid due to failures of resources or control system.

The effective control of Smart Grids is critically dependent on the type and quantity of information gathered from resources and consumers. There is necessary to propose a sufficiently dimensioned data network between the resources/consumers, data center and dispatching center control to ensure the effective control.

Network technologies

The appropriate transmission technology can be chosen being based on the required availability and reliability parameters (Service Level Agreement, SLA), especially the maximum delay that can be determined from the most widely used standards in the ICNPG network and technical studies dealing with these issues [2, 3]. The summarized availability and reliability parameters are shown in Table 2. These values are recommended and their size depends on internal processes in the ICNPG network of given company.

The systems of autonomous control for actuators that are located at substations, transformer substations and switching substations are the most challenging part of the power grids. These systems require a maximum delay approximately 4ms [3]. The SDH (Synchronous Digital Hierarchy) technology or industrial Ethernet meet these requirements. In addition, the Ethernet also allows a better connection to the rest of the data network in the Smart Grid technology.

Table 2. The required availability and reliability parameters for Smart Girds [2, 3]

Priorities of the management requirements			
Low priority	Control level of energy flow direction and optimization of power grid		
	Availability	Delay	Downtime
	>99,9%	<1s	<9 hours per year
Middle priority	Local and remote control level of actuators		
	Availability	Delay	Downtime
	>99,99%	<1s	<1 hours per year
High priority	Autonomous control level of actuators		
	Availability	Delay	Downtime
	>99,999%	<4ms	<1 minutes per year
Priorities of the supervisory activities			
Low priority	Supervision level of non-critical systems (optimization of power grid, EZS)		
	Availability	Delay	Downtime
	>99,9%	<10s	<9 hours per year
High priority	Supervision level of technology (monitoring power grid)		
	Availability	Delay	Downtime
	>99,9%	<1s	<1 hours per year

The requirements and commands are less challenging parts of the power grids. There are following commands in the ICNPG networks: the control of actuators, optimization of power grid, collection of system information for monitoring, etc. In the case of failure, these commands do not require an immediate response. Above mentioned activity can be performed locally or remotely from a dispatching center via the WAN (Wide Area Network). The combination of Ethernet and TCP/IP family of protocols is recommended here.

These two transmission technologies are appropriate only. SDH has a constant delay, high data rate and allows a rapid data transmission recovery after a failure (of the order in units of milliseconds). The disadvantage of SDH is worse integration into the networks based on Ethernet, poor scalability and higher CAPEX than the Ethernet technology.

Ethernet is universal technology and is available in various data rates. Gigabit Ethernet (GE) is the most widely used version of Ethernet today. Ethernet has a typical delay in units of milliseconds. The disadvantage of Ethernet is the dependence of delay on the load of transmission path. The delay increases with heavier loads. There is necessary to propose the sufficiently dimensioned data network, implement QoS or time synchronization for this reason. The implementation of QoS requires the support of all active nodes.

There are two methods for ensuring synchronization of Ethernet technology. The first method is called synchronous Ethernet or also network synchronization. It uses an external clock signal according to the recommendation ITU-T G.8261 and each node retrieves this signal. Therefore, the network nodes must support this recommendation. The advantage of this technology is the independence on the total load of the line. The second method is called packet synchronization and it is defined by the IEEE 1588v2. This method does not depend on the physical layer but it can be influenced by characteristics of the transmission chain (jitter). Both methods of synchronization can be combined.

In the case of communication failure, the Ethernet allows to create a redundant connection using STP (Spanning Tree Protocol), RSTP (Rapid STP) or MSTP (Multiple STP). These protocols are normally designed for the ICT networks and enable the data transmission recovery after a failure in the order of hundreds to units of seconds. The special protocols based on STP protocol achieve the data transmission recovery after a failure in the order of units of milliseconds. These protocols are usually proprietary and they can be found only with device manufacturers for industrial Ethernet (Bosch, Hirschmann, RuggedCom, Moxa, etc.). Other manufacturers often use a modified RTSP protocol by themselves. These protocols are usually incompatible with the protocols of other manufactures. The disadvantage of these protocols is the dependence of data transmission recovery after a failure to the size of the data network. This disadvantage of STP protocols should be eliminated using a new TRILL (Transparent Interconnection of Lots of Links) protocol [4].

The reduction of response time of failures in the data network, VLAN (Virtual Local Area Network) technology can be used as depicted in the Fig. 1c or the data network can be divided into the smaller parts using routers as depicted in the Fig. 1d. The routers work at the network layer (L3) of ISO/OSI model. These smaller routed networks are usually of local character and the redundancy is secured using a dynamic routing protocol, typically OSPF (Open Shortest Path First), or MPLS (MultiProtocol Label Switching) protocol. MPLS protocol is used for large network, but, contemporary, due to convergence, and, multi-service access, it begins to assert into smaller networks. The speed of data transmission recovery after a failure is in the order of hundreds of milliseconds to seconds in layer 3 networks. It depends a lot on the technical solutions of routers, configuring of OSPF process and the size of data network. Ethernet directly supports higher layer protocols (IEC 61850 and IEC 60870-5-104 based on TCP/IP family of protocols), which are commonly used for control and monitoring of the power grids.

Therefore only Ethernet is used as a transmission technology for the Smart Grids. There is necessary to use Ethernet from an industrial series in the case of lowest levels of the Smart Grids in order to meet the requirements for fast data transmission recovery after a failure in the order of units of milliseconds.

Availability and reliability of the Smart Grids are solved using duplication (redundancy) of nodes and links in Ethernet with TCP/IP family of protocols. The appropriate standardized protocols such as MSTP, VRRP (Virtual Router Redundancy Protocol) and OSPF, that ensure the forwarding of data traffic through the remaining functional part of network, when a node or link fails, are used to secure it. Using the priority of certain types of packets (or frames), which contain the data applications requiring the strict requirements respecting the minimum delay and jitter is also solved.

Data network segments

Ethernet and TCP/IP family of protocols provide a flexible and scalable network architecture that allows optimizing the network regarding to the transmission capacity and reliability. There is necessary to respect the hierarchy arrangement of nodes within the network topology. The data network can be divided into three segments in the Smart Grids. Each segment requires a specific bandwidth requirements, reliability and availability. They are described in the following sections.

Core network

The core network allows mutual connecting of the different sites (distribution and access networks) in any geographic area. It uses the high-speed Ethernet (mostly GE or 10GE), IP and MPLS technologies. Typical data rate ranges from 1 Gbps and optimally 10 Gbps to 100 Gbps. The core network connects the tens to hundreds of nodes. It does not intend for direct connection of end terminal and users. The optical fiber is commonly used medium in the modern core networks.

The core network is designed to be able to transfer large amounts of data from different resources with different QoS. The SLA ranges from 99,9% to 99,999% in the core network, see Table 2.

Distribution network

The distribution network typically provides a connection of a large number of access networks to the core network. The geographic distance of distribution network is given by the distance between the access network and core network. There may be used a wide range of transmission technologies in distribution networks than in the core network. It is given by the type of medium. In the case of optical fiber, it can be used the high-speed Ethernet (typically GE). In the case of metallic cables, it can be used the Fast Ethernet (FE). The GE or xDSL (Digital Subscriber Line) can be used regarding the limit parameters. The wireless transmission systems based on WLAN (Wireless Local Area Network) or FWA (Fixed Wireless Access) or GSM (Global System for Mobile Communications) or via radio modems are used in places where there are no metallic cables or optical fibers. The use of transmission technologies is also dependent on the type of service or services that will exploit these networks. For instance, the control, supervision and optimization require stricter requirements for availability and reliability. Therefore more reliable Ethernet is used for these processes than GSM technology. GSM is used only for gathering information (for instance, in the AMM technology). The data rate ranges from the tens of kbps to units of Gbps.

The distribution networks must also support the QoS. However, the QoS is not supported in the data networks of mobile operators, so the type of transmitted data must conform to this fact. The SLA ranges from 99,5% to 99,999%, see Table 2. These values result from the differences of used transmission technologies.

Access network

The goal of access network is to provide a connection of end terminals and users to the distribution network or core network. The topology and technology of access networks is directly related to their purpose (Smart Grid, management of power grids, etc.). Therefore, it is necessary to count with deploying large amounts of proprietary technologies that are not standardized. The access networks connect end terminals in the order of units to tens. The data rate ranges from the tens of kbps to hundreds of Mbps.

The QoS is quite difficult to implement in the access networks, because some nodes and technologies do not support QoS. It is common that today's industrial nodes only support VLAN technology. The industrial nodes are developmentally delayed for several years compared to the ICT nodes. The SLA ranges from 99,9% to 99,999% and more, see Table 2. The situation is more complex with regard to the SLA in the access networks. The access networks that are intended for control and monitoring of power grids are not recommended to use for the transmission of other services. Other services can be operated only with the transmission technologies that allow keeping the desired SLA.

Data Network Hierarchies

The hierarchy of data network defines a way to connections between the segments. It is recommended to keep the following two hierarchical arrangements that can be combined due to good scalability in networks based on TCP/IP:

- Full hierarchy. It is used when the access network are not in direct reach of the core network. The distribution network is used to span the distance between access network and core network. Typically, the core network can be finished in the main transformer substation in given location and the access networks can be finished in secondary substations;
- Reduced hierarchy. It can be used in locations where the access network is in direct reach of the core network.

Topology

There are several types of network topologies in the Smart Grids. The most commonly used topology that is realized at link layer (L2) of ISO/OSI model is the extended star with redundancy. This topology is shown in the Fig. 1b. There is important to use STP, RSTP or MSTP protocol in all switches in the L2 network to keep a redundancy. The proprietary protocols of manufacturers of industrial switches can also be used in layer 2 networks. The disadvantage of these protocols is in the incompatibility with similar protocols from other manufacturers.

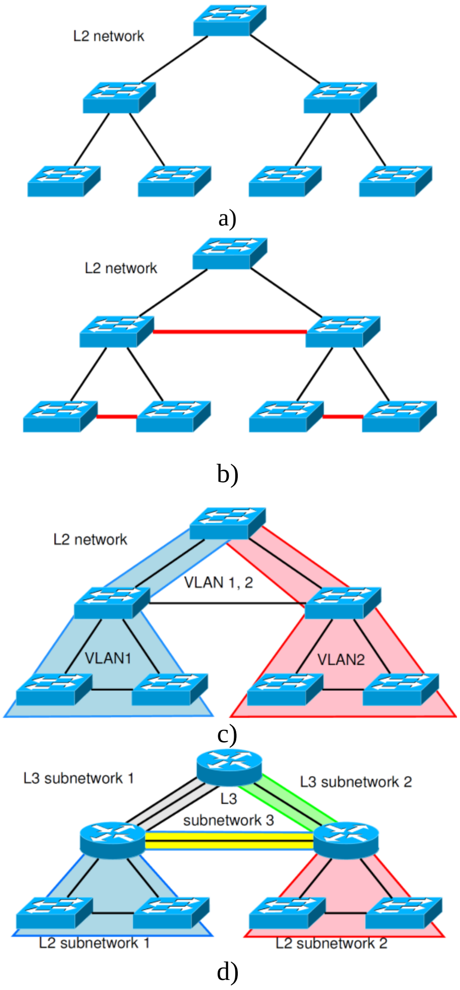

Fig. 1. ICT technologies in Smart Grids: a – extended star without redundancy; b – extended star with redundancy; c – VLAN technology; d – routed network

IP Support

The IP (Internet Protocol) works at network layer (L3) of ISO/OSI model. Therefore, it is technologically independent. The IP version 4 (IPv4) is the most widely used in modern ICT networks. But IP version 6 (IPv6) is starting to replace it, especially in the core networks. There are several reasons for the transition from IPv4 to IPv6.

The main reason is the near exhaustion of IPv4 address space (2^{32}). The number of IPv6 addresses is 2^{128}. IPv6 is an extension of IPv4 [5]. From the perspective of Smart Grids, the biggest advantage of IPv6 is a direct support of multicast and anycast. IPv6 multicast is a more sophisticated solution in comparison with IPv4 multicast. So it could replace the HDO (mass remote control) system that is important for Smart Metering (AMM technology). HDO system is a set of technical resources (such as transmitters, receivers, central automation, transmission line, etc.) enabling to broadcast the commands or signals over the distribution grids of energy companies in order to turn on and off the consumers and switching the tariffs.

In addition to larger IPv6 address space and a direct support of multicast and anycast, QoS support, direct security support, fast routing and auto-configuration are interesting for the Smart Grids.

It is necessary to think about the interconnection of Smart Grids to the Internet or other networks (e.g. enterprise network) due to the IPv6 deployment in these networks. It considers a hypothetical Smart Grids of an energy company, with the Smart Metering, which uses the IPv4 protocol. These Smart Grids have over 4 billion addresses and the IPv4 address space is basically inexhaustible. Therefore, it is necessary to consider the other advantages of IPv6.

The IPv6 deployment is not a problem with regard to the SCADA system. Most of the transmission and application layer of protocols require little or no changes to work with IPv6. The application protocols that include IPv6 addresses are the only exception.

IPv4 and IPv6 are incompatible. There is necessary to use the transition mechanisms for simultaneous operate IPv4 and IPv6 operation. These mechanisms are not appropriate due to the large requirements for the availability and reliability of Smart Grids. Thus, both protocols should not work together in the Smart Grids.

The IPv6 support is constantly improving in the ICT networks. It is expected that the IPv6 support will be improved in the Smart Grids too.

Conclusions

This paper describes the migration of traditional IT technologies to the Smart Grids and compares them with ICT networks. This comparison shows that the utilization rate of ICT technologies must be determined in Smart Grids with regard to the required criteria, especially the maximum delay of data transmission. The appropriate transmission technology can be chosen based on the required availability and reliability parameters. The combination of Ethernet or industrial Ethernet, TCP/IP family of protocols and other auxiliary protocols (RSTP, VRRP, OSPF and MPLS) are recommended in the Smart Grids because it best meets the strict requirements (availability and reliability) for the design of industrial networks.

Acknowledgements

This work was supported by the grant MSM6840770038.

References

1. **Marcus E., Stern H.** Blueprints for High Availability, 2nd ed. – Wiley, 2003. – 624 p.
2. **Alcatel/Lucent**. Smart Choices for the Smart Grid (Technology White Paper). – 11 p. Online: http://enterprise.alcatel–lucent.com/private/images/public/si/pdf_smartChoice.pdf
3. **Jensen M., Sel C., Franke U., Holm H., Nordström L.** Availability of a SCADA/OMS/DMS System – a Case Study // IEEE PES Conference on Innovative Smart Grid Technologies Europe, October, 2010. – P. 1–8.
4. **Touch J., Perlman R.** RFC 5556 Transparent Interconnection of Lots of Links (TRILL): Problem and Applicability Statement (standard). Online: http://www.ietf.org/rfc/rfc5556.txt.
5. **Deering S., Hiden R.** RFC 2460 Internet Protocol, Version 6 (IPv6), Specification (standard). Online: http://www.ietf.org/rfc/rfc2460.txt.
6. **Pravda I., Vodrazka J.** Voice quality planning for NGN including mobile networks //12th International Conference on Personal Wireless Communications (PWC'2007). – Prague, 2007.
7. **Kovac A., Halas M., Voznak M.** Impact of Jitter on Speech Quality Estimation in Modified E–model // Conference proceedings of RTT'2010. – Velke Losiny, 2010.

Received 2012 01 04
Accepted after revision 2012 02 09

L. Cepa, Z. Kocur, Z. Muller. Migration of the IT Technologies to the Smart Grids // Electronics and Electrical Engineering. – Kaunas: Technologija, 2012. – No. 7(123). – P. 123–128.

This paper describes the migration of the traditional IT technologies to the Industrial Control Networks for Power Grids (ICNPG), characteristics of the typical ICNPG network and the differences between them and ICT network. We define the availability and reliability of the ICT networks and describe the current trends of the IT technologies in the ICNPG network with regarding its use in the Smart Grids. Finally, we describe the Smart Grid technology and summarize the availability and reliability of the ICNPG networks from technical studies. The comparison of ICNPG and ICT networks show that the utilization rate of ICT technologies must be determined in the Smart Grids with regard to the required availability and reliability. Ill. 1, bibl. 7, tabl. 2 (in English; abstracts in English and Lithuanian).

L. Cepa, Z. Kocur, Z. Muller. IT technologijų migracija į išmaniuosius tinklus // Elektronika ir elektrotechnika. – Kaunas: Technologija, 2012. – Nr. 7(123). – P. 123–128.

Aprašoma tradicinių IT technologijų migracija į elektros tinklų industrinius valdymo tinklus. Pateikiamos tipinio ETIVT tinklo charakteristikos ir jo skirtumai nuo IRT tinklo. Nustatytas IRT tinklų tinkamumas ir patikimumas bei šiuolaikinės IT technologijų ETIVT tinkluose tendencijos. Apibrėžta išmaniųjų tinklų technologija ir apibendrintas ETIVT tinklų tinkamumas ir patikimumas. Tinklų palyginimas parodė, kad IRT technologijų panaudojimo išmaniuosiuose tinkluose koeficientas turi būti nustatytas atsižvelgiant į reikiamą tinkamumą ir patikimumą. Il. 1, bibl. 7, lent. 2 (anglų kalba; santraukos anglų ir lietuvių k.).