УДК 621.316.925

V.I. Gurevich

TECHNOLOGICAL ADVANCE IN RELAY PROTECTION: DANGEROUS TENDENCIES

Розглядаються сучасні тенденції розвитку релейного захисту: ускладнення, збільшення кількості виконуваних функцій, застосування недетермінованої та вільно-програмованої логіки, використання Ethernet та WiFi каналів зв'язку, зниження надійності. Визначається небезпека існуючих тенденцій розвитку релейного захисту й необхідність створення незалежного від розробників та виробників реле захисту експертної координаційної ради фахівців для вироблення загальної стратегії та шляхів розвитку релейного захисту.

Рассматриваются современные тенденции в развитии релейной защиты: усложнение, увеличение количества выполняемых функций, применение недетерминированной и свободно-программируемой логики, использование Ethernet и Wi-Fi каналов связи, снижение надежности. Отмечается опасность существующих тенденций развития релейной защиты и необходимость создания независимого от разработчиков и производителей реле защиты экспертного координационного Совета специалистов для выработки общей стратегии и путей развития релейной защиты.

1. EXTRUSION INTO THE HISTORICAL DOMAIN

For over a hundred years all the tasks of relay protection have been performed by electromechanical protection relays (EMR). The fact that EMRs are still widely used in many countries, including Russia (about 80-90% of all types of protections), proves that in general EPRs are capable of solving all the present problems of the relay protection. However, during the past 15-20 years there has been a widespread displacement of EMR by microprocessor-based relay protection devices (MPD). MPD and various programmable logic controllers (PLCs) that control the operating modes of electrical equipment, have become an integral part of our lives and, in many cases, there is no other device available to substitute for them to ensure the normal functioning of the power industry. This is not due to some unique features of microprocessor devices, this is rather a result of the costs of the fully automated production of MPD based on printed circuit boards compared to the production of high-precision mechanics for the relays of the previous generation. 30-40 years ago due to the necessity for cutting production costs and improve profitability of production, the development of the new types of EMRs was stopped and all efforts were focused first on the creation of the static solid-state protections, and then on the development of MPDs. The first types of MPD simply copied all the functions and characteristics of the relays of previous generations. New features and capabilities of MPD have been implemented only many years after. This technical policy of manufacturers has resulted in the complete halting of the production of all other types of protection by all of the world's leading manufacturers of the relay protection, and MPDs have become nearly the only available type of protection.

Even the very first MPDs, which simply copied the functions of the static solid-state transistor-based relays, see Fig. 1, revealed serious problems of the MPDs: more frequent failures and irreparability due to the presence of the special microprocessor and non-volatile memory containing the program. As a result, while the relays of type RXIDF-2H built on transistors and other discrete components were quick to repair and return to operation, their microprocessor-based analogue RXIDK-2H must be discarded. Hence, the microprocessor-based RXIDK-2H have long been taken out of service while RXIDF-2H are still used. The tendency of the relay protection reliability weakening associated with the transition to the MPD and noticed at the beginning of this process can be traced so far, despite the fact that modern generation of the MPDs have little in common with the first samples manufactured a few decades ago, see Fig. 1. This goes to prove that the problem is systemic rather than a result of the single technical defects specific to early MPD models. But no one wanted to gain the character of retrograde and nobody wanted to talk about the obvious problems of MPDs welcomed with such rapturous applause.

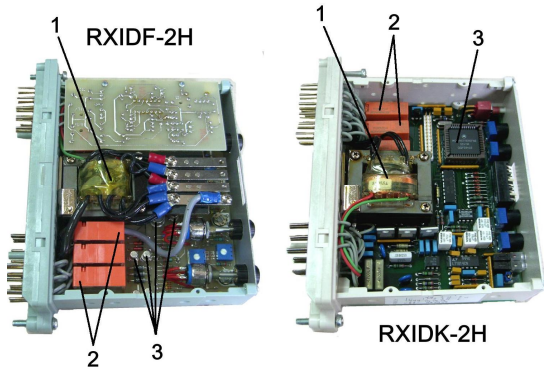

Fig. 1. Two current relays with independent time delay, both with equal technical parameters, dimensions and characteristics made in the identical standard cases COMBIFLEX® manufactured by the same company (ABB), the left – the static solid-state relay RXIDF-2H, the right – microprocessor-based relay RXIDK-2H. 1 – input current transformer; 2 – output electromagnetic relays; 3 – transistors of the static relay and specialized microprocessor of the microprocessor-based one

Moreover, since over the past decades billions of dollars have been invested in the ideas and technologies of the MPDs and as it has become the source of profit for thousands of scientists and engineers all around the world, all discussions about the problems and disadvantages of the MPDs have been nipped in the bud or met with fierce opposition by the representatives of manufacturers, scientists, developers, designers and all other participants of this business.

My past attempts to draw attention to the problems of the MPD [1, 2] caused fierce accusations of incompetence, misunderstanding of the basis of the relay protection, and even of an attempt to slow down the technological progress.

2. ABOUT TECHNOLOGICAL ADVANCE

The cheapness and availability of the highly-integrated microprocessors, industrial controllers and advanced electronic components, a huge and ever expanding range of such components available on the market, extremely high performance of the equipment designed for automatic installation and soldering of the surface mounted components of printed circuit boards, automatic test systems for the ready-made printed boards – all these remove the previous restrictions to the complexity of the electronic systems and their field of application. This is the reason why the microprocessors can now be found everywhere, even in toilet seats, where they measures the temperature of the corresponding part of the body and control the built-in

shower water heater to equalize its temperature with the temperature of the said part of the body [3].

Such an universal expanding usage of microprocessor-based electronic components in all fields of the technology together with their persistent sophistication define the tendency of the technology development. This tendency is what we call an "advance" in the development of engineering and technology. Of course, there are certain fields of engineering and technology where computing and microprocessors are "must haves" and microprocessor technology has really enabled making a technological leap. However, implementation of the microprocessor-based devices is not always required due to the technical requirements to the products, and the number of such cases grows like an avalanche. Nevertheless, if you look at this tendency not as a bystander but as the "insider", in charge in maintenance and repair of complex industrial electrical devices, such as relay protection, high-power battery chargers, inverters and converters, uninterruptible power supplies, etc., you have to ask yourself if the tendency can really help the technical advance. You have to ask "Why?"

Just because the current boom resulted from the sharp sophistication of the devices and ever-widening usage of microprocessors in all fields of technology, and is generated by the intention of the manufacturers to outperform competitors, as well as their rush for innovations and increased profits by any and all means rather than by the real needs.

The aim to create something new or to reduce production costs could only be welcomed if this trend of substituting analog systems on discrete electronic components, which have proved their reliability for tens of years, to microprocessor-based would not lead to the significant sophistication of the equipment, making it irreparable, unreliable and expensive in maintenance in addition to the need for the sharp increase of qualification of the personnel. When you order the equipment, all these problems stay in the background, and you face them only during the maintenance. This is the price that the consumers must pay for the so-called "advance", that is, for the thoughtless and irresponsible complication of the devices, which is often proved only with the "technological fashion" and pursuit of profit. More details on this issue in [3].

3. SMART GRID – ONE MORE DANGEROUS VECTOR OF THE "TECHNOLOGICAL ADVANCE" IN POWER INDUSTRY

You could hardly find a media which did not resound with Smart Grid praises. The so-called "intelligent network" or Smart Grid is the technological "top fashion" promising us unprecedented wealth. Today everyone talks about his or her contribution to the development of this new fashioned trend. It turns out that not only the microprocessor-based power meters, but even electro-furnace transformers, reactive power compensation devices, superconducting power cables, etc., all are the elements of the "Smart Grid", and require investments in manufacture. Thus, governments create targeted investment programs and allocate billions spinning a huge wheel for sucking up and dispersal of the state budgets in the nondescript and unclear direction [4].

As is known, the Smart Grid concept assumes the installation of microprocessors in absolutely all elements of the power production, distribution and metering systems as well as arrangement of data channels between them based on the computer networks, which are generally wireless (Wi-Fi). The apologists of the Smart Grid see the future power system as a fancy modern online game with thousands of participants - the components of the power networks. If we also consider the millions of the household power meters united in a common computer network (i.e., millions of potential points of network access for hackers), the grandeur and the danger of this idea due to the sharp increase in vulnerability of the power systems to hacker attacks, computer viruses and remote intentional destructive electromagnetic impacts (which are detailed in [4]) becomes even more obvious.

Today, the low-power, high-altitude electromagnetic pulse of a nuclear explosion set off in near space over the territory of a country is regarded as a real type of the so-called nonlethal weapons capable of disabling all the microelectronic devices over the whole country while not injuring people [17]. Alas, all these dangers, or "horror stories" as they are disparagingly referred to by some proponents of the "technological advance" in its present form, are hardly considered by scientists and engineers who receive their payrolls from the funds allocated to the development of the Smart Grid. They often say: our task is to advance the technologies, while protection of the national power systems is the "headache" of the army and intelligence agencies. Defectiveness of such an ideology is obvious and does not even require an explanation.

4. DANGEROUS TENDENCIES IN DEVELOPMENT OF THE RELAY PROTECTION

In previous publications we repeatedly drew attention to the dangers of some tendencies in the development of relay protection that is strongly promoted by the developers and manufacturers of the MPDs:

1. Continuous sophistication of the MPDs and increasing the number of protective functions in a single terminal [6, 10].
2. Overloading the MPDs with functions unusual to the relay protection, such as the monitoring of electrical equipment [11, 12].
3. Use of a non-deterministic logic in MPDs, as well as so-called "advance actions" that lead to the risk of the loss of control over the relay protection actions [11, 12].
4. Wide use of free programmable logic [13] in MPDs, resulting in the significant increase in the percentage of staff mistakes and faults of protection.
5. Complication of the serviceability checks and maintenance of the relays, while integrating numerous MPDs of different types and brands with different designs and software in the same power network. The lack of the common standards for the MPD design and software increases the intellectual load on staff and leads to significant economic losses [14]. This situation is exacerbated with every passing year.
6. The dramatic weakening of the electromagnetic immunity of the relay protection and the whole power system in proportion to the usage of the MPDs [15-17].
7. Increased vulnerability of the power systems to hacker attacks resulting from the expansion of the microprocessor-based devices and the usage of the cheap Ethernet and Wi-Fi lines instead of the relatively protected optoelectronic cables in the relay protection systems [18].

This sophistication, of both hardware and software, has not sunk in. As shown in [1, 5-9], even now the transition to the MPDs is accompanied by a significant decline in the reliability of the relay protection. However, the advocates of microprocessor-based relay protection believe that we should not be satisfied with what has already been achieved and must further sophisticate the MPDs by increasing the number of functions performed by a single terminal, by using freely-programmable logic, non-deterministic logic based on the theory of neural networks and algorithms of pre-emptive action, by over-

loading the MPDs with the functions of information-measuring systems and monitoring systems of power equipment and by using the wireless communication channels (Wi-Fi) between relays, etc.

The new-fangled ideas and developments in the field of MPDs are no longer limited only to the functions of relay protection. It is supposed that in the near future not only relay protection, but the whole power systems should correspond to the Smart Grid concept, which implies that all the power equipment of power system elements must be based on microprocessors to manage the exchange of synchronization signals and control commands between such elements via Wi-Fi.

What alluring prospects and inviting horizons! What enormous amounts of money are to be allocated from the government budgets to the new programs in the power systems! So many research and production teams can subsist on these budgets, periodically suggesting more and more improbable, but very "beautiful" ideas, and putting on the market more and more sophisticated but less reliable products.

It's a huge business, and nobody wants to be banned from this sweet "cake". The participants in this business are not concerned about the latest affects of their activities and seek only to quickly "push" their new-fashion ideas to the market.

Business is business and its fundamental laws are the same in all countries and areas, including such sensitive ones as relay protection and power management and control. Do you need a proof? Read the motto to the report on the symposium "Distribution systems of the future: Novel ICT solutions as the backbone for smart distribution" published in the PAC World magazine:


80

by Bernd Michael Buchholz, NTB Technoservice, Germany and Christoph Brunner, it4power, Zug, Switzerland

industry reports

and prosperity of the industry was clearly considered by Madame Merce Griera I Fisa from the European Commission. The SmartGrids are a prerequisite to reach the European 20-20-20 targets in 2020 (20% *improvement of energy efficiency*, 20 % *share of renewable energy sources to cover the demand of primary energy*, 20 % *reduction of carbon emissions*). Furthermore, the advanced products and system solutions partly resulting from funded projects will ensure

presented by the 12 participating project teams – beginning with the building automation "SmartHome" and the involvement of household consumers into the electricity market, the automation of distribution networks up to the erection of prospective markets for energy and reserve power. Engaged discussions followed each of the contributions.

The analysis of the consumer behavior in the environment of dynamic tariffs presented a potential

It is mandatory that the new solutions from the project are urgently applied in practice now.

One session considered the barriers for SmartGrid solutions by the current regulation and legal situation in Germany. For many

Fig. 2. The motto to the one of the articles in the worldwide popular specialized magazine "Protection, Automation and Control Magazine" – PAC World, September, 2011 (in the border)

The keywords in this motto are: "urgently" and "mandatory", that is, without the careful analysis of the remote effects of these innovations and without "unnecessary" criticism. Thus it has worked until today it is worldwide.

There was a period of sharp criticism of my publications and total negation of the non-amenities of the above relay development tendencies. However, in recent years many experts have started to understand the problems I have revealed (and, generally, without any reference to my earlier articles in major technical magazines of Russia, Europe and USA). For example, at the Second International Conference "Actual Trends in Developments of Power System Protection and Automation" (Moscow, September 7-10, 2009) B. Morris, R. Moxley, C. Kusch (Schweitzer Engineering Laboratories, USA) submitted a report: "Then Versus Now: A Comparison of Total Scheme Complexity", where they questioned the need for further sophistication of the protection and appealed to the comparative assessment of the reliability of the simple electromechanical relay protection and multifunction microprocessor-based protection systems. They stated that they have identified a trend of downward reliability of the relay protection systems built on sophisticated microprocessor-based devices.

The unreliability of MPDs was also raised by V.I. Pulyaev (FSK UES, Russia) at the Third International Conference "Actual Trends in Developments of Power System Protection and Automation" (St. Petersburg, May 30 – June 3, 2011). He particularly noted that the significant failure rate of relaying accounts for microprocessor units (approximately 23 % of all cases), which constitute only about 10% of the total number of protection devices. This is definitely one of the most important factors determining the need for special measures to enhance the reliability of the MPDs.

Now late Alexey Shalin (Ph.D., a professor of Electric Power Stations Department of the Novosibirsk State Technical University, leading specialist of LLC "PNP BOLID", Novosibirsk), in his article responding to one of my publications (see A. Shalin, "Microprocessor-based relay protection: analysis of the efficiency and reliability is required," in "News of Electrical Engineering", 2006, No. 2) commented that the percentage of malfunctions of the modern relay panels and cabinets often was significantly higher than of the old defenses based on electromechanical relays. He also presented statistical data confirming that the transition from the defenses based on electromechanical relays to microprocessor terminals was accompanied with the significant reduction in the efficiency and reliability.

The unreliability of current MPDs was the focus of the articles by A.N. Vladimirov (Central Dispatch Administration of UES of Russia); S. Swain, D. B. Ghosh (Integrated Electrical Maintenance) and others [19].

J. Stokoe and J. Gray. in their report "Development of a Strategy for the Integration of Protection & Control Equipment" submitted at the 7th International Conference "Developments in Power Systems Protection" (Amsterdam, 9-12-th April 2001) pointed out that the old electromechanical relays were strong and durable devices with a lifetime of 25 years, whereas the life of modern microprocessor-based protection is 15 years or less.

They echoed by J. Polimac and A. Rahim (PB Power, United Kingdom) who declared that the transition from electromechanical relays to microprocessor-based ones reduced the lifetime of protection from 40 years (EMR) to 15-20 years, and sometimes even to only a few years after commissioning (MPD) [19].

The Head of Computer Department of Engineering and Technology College (University of Poona, Maharashtra, India) Ashok Kumar Tiwari B. E. noted that the integration of numerous functions in a single microprocessor terminal significantly reduced the reliability of the relay protection, since the failure of the terminal will result in the loss of too many features, compared to the system where these functions are distributed among several terminals [19].

The necessity to limit the number of functions combined in a single MPD terminal was also mentioned in the report by V.A. Efremov, S.V. Ivanov (IC "Bresler") and D.V. Shabanov (Russia FGC) "Actual Trends in Developments of Power System Protection and Automation" also submitted at the same Third International Conference, mentioned above.

A. Fedosov and E. Pusenkov, (a subsidiary of OAO "SO UES" ODE Siberia) in their article "Problems arising from the introduction of microprocessor technology in the emergency control systems" ("Power Stations", 2009, No. 12) noted the lack of the strict standards on the MPD hardware and software has resulted in too great a variety of programs and algorithms built in the power system MPDs, which has lead to the faulty operations and increased the likelihood of faults of such devices.

The sharp vertical growth of the tasks performed by the personnel servicing the relay protection after the tran-

sition from EMR to MPD was referenced as the cause of severe accidents in power systems by D. Rayworth and M. A. Rahim (PB Power, UK) [19].

A. Belyaev, V. Shirokov and A. Emelyantsev (Specialized Department "Lenorgenergogaz", St. Petersburg) in their article "Digital terminals of RPA. Adapting to Russian conditions" ("News of Electrical Engineering", 2009, No. 5) also considered the complexity of program interface and the necessity for inputting numerous set points during the programming of MPDs.

The poor electromagnetic environment in the most of the old substations designed and built for the electromechanical relay protection, and not for microprocessor-based devices, as well as the resulting numerous MPD faults were noted by B.I. Kovalev, I.E. Naumkin (Siberian Energy Research Institute); A.M. Bordachev (JSC "Institute Energosetproject"), M. Matveev and M. Kuznetsov (OOO "Aesop"); P. Montignies, B. Jover (Schneider Electric, France); V. Nadein ("Arkhenergo"); V. Lopukhov (SUE "Tatenergo PEO"); A. Ermishkin (JSC "Mosenergo"), R. Borisov (NPF "ELNAP", Moscow); A. W. Sowa, J. Wiater (Electrical Department, Białystok Technical University, Poland) and others.

Many experts noted that the vulnerability of MPD to the electromagnetic interference is several orders higher than that of traditional electromechanical counterparts, and therefore to ensure the electromagnetic compatibility (EMC) of the secondary circuit their level of electromagnetic protection has to be significantly higher. Thus an acceptable level of MPD reliability can be reached only after providing for their EMC. Low EMC survivability of the MPDs is closely related to the deeper and more dangerous problem of remote intentional destructive electromagnetic impacts on the MPD, which we first considered in [15].

Many countries have already developed the devices that can remotely disable any microprocessor-based industrial systems (including the MPD, of course), so this problem was the focus of the numerous articles in technical magazines written by such well-known experts like Manuel W. Wik (Defense Materiel Administration, Sweden) and William A. Radasky (Metatech Corporation, USA), and also it was included in the reports of special committees of the U.S. Congress (e.g., see: "Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack", 2008).

Another previously unknown challenge of the relay protection is the so-called cyber vulnerability of the MPDs (and, consequently, of the whole grid), or exposure to hacker attacks.

The paralysis of control systems, major outage of whole power systems, chaos within control systems, disconnection of Internet and cellular phones are all in the scenario of cyber war in the American apologists' opinion. Moreover, considering the strategic importance of such objects as power systems such attacks will rather be organized by special military cybernetic units than by single hackers. And such units have already been established in many countries of the world.

Last year the US Cyber Command started its operations. Being a part of the National Security Agency (NSA), the top secret and one of the most powerful intelligent agencies of the world, under the command of General Keith Alexander, the organization has united all previously existing cyber safety departments of the Pentagon. A year ago Cyber Command had about 1,000 employees, but the military had announced its initiation of a major hiring plan for particular specialists to increase the number of employees of this unit of NSA to 10,000 people.

Some of them will be in charge of the protection of military and state infrastructures as well as of the most important commercial properties of the state. It's obvious that such a large structure will not only protect from the hacker attacks, but will also develop hacker attacks (after all, attack is the best defense). The current Head of Cyber Command, and Director of NSA General K. Alexander has declared at hearings of the Military Service Committee of House of the USA that the effect of cyber weapons is comparable to the effect of mass destruction weapons.

Cyber weapons are on the fast track. Experts say that many countries - including the USA, Russia, China, Israel, Great Britain, Pakistan, India, Northern and South Korea - have developed sophisticated cyber weapons which can repeatedly get into computer networks and are capable of destroying them. In 2010 the cyber budget of USA reached 8 billion USD, and in the future this amount will further grow. In 2011, USA plans to embrace a new doctrine of cyber safety. Its aims were revealed in a policy paper by Deputy Head of the Pentagon William Linn III under the symbolic name "New Space Protection". The main idea of the paper is that from now on the USA considers cyber space as the potential battlefield along with land, sea and air. In parallel, NATO has started to work on the development of a collective cyber safety concept. At an Alliance Summit held in November 2010, it was decided to develop a Cyber Safety Action Plan. The document should be ready by April 2011 and signed in June. The main concept of the document centers around the creation of a NATO Cyber Accident Response Center. Initially the Center was planned to be commissioned in 2015 but on the insistence of the USA this has been reduced by three years.

Effectiveness of cyber weapon was proved by the widely known cyber attack on the uranium enrichment plant in Natanz, Iran, with Win32/Stuxnet worm which destroyed hundreds of centrifuges.

Another massive attack was mounted in September 2011 on the Japanese corporation Mitsubishi Heavy Industries, engaged in the production of important parts of the F-15 jets, Patriot missile complexes, submarines, surface ships, rocket engines, guidance and intercept ballistic missiles systems, and other military equipment. Computer equipment of the corporation (45 private servers and around 50 PCs) was infected with a set of viruses, which took complete control over it. The viruses allowed controlling the computers from the outside and transfer the available data. Some viruses were aimed to activate the built-in computer microphones and cameras. This allowed the attackers to keep an eye on what's happening in the production and research facilities. Other viruses erased signs of cracking, which seriously complicated the assessment of the damage. Information from the computers was transferred to 14 websites located in other countries, including China, Hong Kong, USA and India.

Modern technologies allow infecting the computer system remotely through the encoded radio signals sent by unmanned aerial re-transmitters. Wi-Fi systems, which are planned to be the basis for Smart Grid, are particularly exposed to such infections. Built-in Wi-Fi modems have already been built into the MPDs by the leading Western manufacturers.

In the past there were attempts of computer penetration into the power system of Israel made by Iran. Senior CIA analyst Tom Donahue at a meeting between government officials and employees of USA companies from the power, water, oil and gas supply sector mentioned that CIA identified numerous attempts to penetrate the US power grid. Obviously, we can state that the cyber wars have already started and while they will intensify over time, the vulnerability of power systems will continue to increase too due to the current tendencies, thus forming a

very dangerous vector.

So today, we should stop turning a blind eye to the tangle of problems associated with the proliferation of the MPDs, disparagingly calling them "scary stories from Gurevich", since already today dozens of experts from many countries state that there are serious problems that need to be addressed.

5. WHAT TO DO?

In my opinion, it's time to put an end to the uncontrolled development of unproven and dangerous trends in the relay protection and automation systems, including the Smart Grid.

This requires the establishment of the National Coordinating Councils for the relay protection and intelligent networks, which must analyze current trends, develop national strategies and coordinate the standardization in these areas.

The Councils should include independent experts and specialists in the field of relay protection, microelectronics, data protection and electromagnetic compatibility, who do not have economic ties with the development and production of the MPDs or the elements of the Smart Grid. It should be noted that a purely mercantile financial interests of individuals and even entire scientific and industrial groups, interested in the funding of any new digital technologies in the power sector and, in particular, in the field of the relay protection, regardless of the long-term effects of such technologies and not limited to any frameworks, may result in national disasters in the near future.

New technologies in the field of relay protection, automation, communication and data transfer systems should not be introduced into service until the possible negative consequences of their wide distribution is fully considered in the light of accumulated experience, and until the effective measures to protect against remote intentional destructive impacts, whether intentional electromagnetic impacts or hacker attacks, is developed. Development of measures to protect sensitive electronic equipment of power systems against intentional destructive impacts should be considered as one of the main targets and it should be funded by amounts not less than those spent for the development of new technologies, such as the Smart Grid. Development of any new technology, based on digital microelectronics, should be considered as complete and ready for use in power industry only after the development of measures to protect it from the intentional destructive impacts.

New standards on microprocessor-based relay protection, which are required according to [20, 21], must include the requirements for the protection against intentional destructive impacts, as the current standards on electromagnetic compatibility (EMC) consider only the stability of the equipment against natural effects, rather than against intentional destructive electromagnetic impacts.

I must carefully examine the ways to improve the reliability of the MPDs by means of the modern redundancy hybrid relays [22, 23].

I am sure that it is the only acceptable direction of the technical advance in such an important and basic sector of any national infrastructure as power industry.

REFERENCES

1. Gurevich V. Microprocessor Protection Relays: New Prospects or New Problems? – "Electr. Engineering News", 2005, № 6 (36), p. 57-60.
2. Gurevich V. Microprocessor Protection Relays: alternating view. – Electro-info, 2006, № 4 (30), p. 40-46.
3. Gurevich V.I. Price for "the progress". – Components and Technologies, 2009, № 8.
4. Gurevich V.I. Smart Grid: New Perspectives or New Problems? – "Electrotech. Complexes and Control Systems", 2011, № 1, (Part I), 2011, № 3 (Part II).
5. Gurevich V. Reliability of Microprocessor-Based Relay Protection Devices – Myths and Reality. – Engineer IT, Part I: 2008, № 5, p. 55-59; Part II: 2008, № 7, p. 56-60.
6. Gurevich V. I. Reliability of Microprocessor-Based Protective Devices – Revisited. – Journal of Electrical Engineering, Vol. 60, № 5, 2009.
7. Gurevich V.I. Some Performance and Reliability Estimations for Microprocessor Based Protection Devices. – Electric Power's News, 2009, № 5, p. 29-32.
8. Gurevich V.I. How to Rebuild Relaying? – Energize, 2010, № 4, p. 36-39.
9. Gurevich V.I. Criteria of estimation for a relaying: Whether it is necessary to complicate a situation? – Electric Power's News, 2009, № 6, p. 45-48.
10. Gurevich V.I. Whether the Relay Protection is Safe? – Energy-Safety and Energy-Economy Magazine, 2010, № 2, p. 6-8.
11. Gurevich V. Sophistication of Relay Protection: Good Intentions or the Road to Hell? – Energize, 2010, Jan/Feb, p. 44-46.
12. Gurevich V.I. Sensational "Discovery" in the Relay Protection. – Power and Industry of Russia", 2009, p. 23-24.
13. Gurevich V. I. Logic in Free Flight. – "PRO Electrichestvo", 2011, № 2. p. 28-31.
14. Gurevich V. Tests of Microprocessor-Based Protection Devices. "PRO Electricity", 2008, № 1, p. 41-43.
15. Gurevich V. The Hazards of Electromagnetic Terrorism. – Public Utilities Fortnightly, 2005, June, p. 84-86.
16. Gurevich V.I. Problems of Electromagnetic Impacts on Digital Protective Relays. – "Components and Technologies", 2010, № 2, p. 60-64; № 3, p. 91-96; № 4, p. 46-51.
17. Gurevich V.I. Stability of Microprocessor Relay Protection and Automation Systems Against Intentional Destructive Electromagnetic Impacts. – Electrical Engineering & Electromechanics, 2011, № 5 (Part I); 2011, № 6 (Part II).
18. Gurevich V.I. Cyber Weapon Against of Power Industry. – Energize, 2011, № 10.
19. Problems of Microprocessor-based Relay Protection. http://digital-relay-problems.tripod.com.
20. Gurevich V.I. The Standardization in the Field of Microprocessor Protection Relays is Necessary. Electric Power's News, 2011, № 2, p. 34-42.
21. Gurevich V.I. The New Concept of Digital Protective Relays Design. – "Serbian Journal of Electr. Engineering", 2010, vol. 7, № 1, p. 143-151.
22. Gurevich V.I. Perspectives for Hybrid Technology in Relay Protection and Automation. – Components and Technologies, 2011, № 10, p. 70-73.
23. Gurevich V. Hybrid Reed-Solid-State Devices are a New Generation of Protective Relays. – Serbian Journal of Electr. Engineering, 2007, v.4, № 1, p. 85-94.

Received 24.11.2011

Gurevich Vladimir, Ph. D., Honorable Professor
Central Electrical Laboratory of Israel Electric Corp.
POB 10, Haifa 31000, Israel
e-mail: vladimir.gurevich@gmx.net

Gurevich V.I.
Technological advance in relay protection: dangerous tendencies.
In the article, the modern lines in the development of relay protection are considered: complication, increasing number of functions, use of non-determined and free-programmed logic, use of Ethernet and Wi-Fi communications channels, decreasing reliability. The article highlights the danger of the existing tendencies in relay protection development and the necessity for creation of new lines of relay protection that are independent of the current developers and manufacturers. The article calls for creation of an Expert Coordination Council of specialists for development of the general strategy and ways of relay protection.
Key words – **relay protection, tendency, evolution.**