

## MICROPROCESSOR PROTECTION RELAYS: NEW PROSPECTS OR NEW PROBLEMS?

Gurevich Vladimir, Ph.D  
Israel Electric Corp., Central Electric Laboratory  
POB10, Haifa 31000, Israel  
fax: (++1) 603-308-5909, e-mail: gurevich2@bezeqint.net

*Внутрішня архітектура і принцип дії мікропроцесорних реле захисту мають мало загального з пристроями, званими "електричними реле". Але такі реле захисту на основі мікропроцесора поступово витісняють традиційні електромеханічні і навіть електронні реле захисту практично у всіх областях енергетики: це стало модною тенденцією. Проте, при найближчому розгляді виявляється, що переваги засобів захисту на основі мікропроцесора насправді не так вже і очевидні, зате вони мають істотні недоліки. У цій статті обговорюються деякі з цих проблем.*

*Внутренняя архитектура и принцип действия микропроцессорных реле защиты имеют мало общего с устройствами, называемыми "электрическими реле". Но такие реле защиты на основе микропроцессора постепенно вытесняют традиционные электромеханические и даже электронные реле защиты практически во всех областях энергетики: это стало модной тенденцией. Однако, при ближайшем рассмотрении оказывается, что преимущества средств защиты на основе микропроцессора в действительности не так уж и очевидны, зато они имеют существенные недостатки. В этой статье обсуждаются некоторые из этих проблем.*

### I. INTRODUCTION

Microprocessor systems are similar to simple digital computer systems (Fig. 1), in which the microprocessor performs the timing and control of the system and carries out all arithmetic and logical operations. The system memory may be Read Only Memory (ROM) for dedicated applications or Random Access Memory (RAM) for the storage of data and programs, or a combination of both. System memory stores the program to be executed and the data relevant to the specific task.

The microprocessor communicates with the system memory by means of a bus system. The same bus system permits communication of the microprocessor with the interface adaptor, or Input/Output (I/O) unit, which makes possible the transfer of data and control signals to and from the system. As it can be seen from Fig. 1, the microprocessor is quite a complex device with specific terminology and principles of operation that have nothing in common with the protective relays considered above. The question arises if the "microprocessor-based protection device" is a "relay" in the full sense of the word. On closer examination it turns out that the "microprocessor-based relay" is a small computer in which the output circuits (usually built-in CT or VT - Fig. 2) have matched parameters with external current and voltage transformers, with a program stored in memory, allowing processing of input signals in such a way that operation of this or that type of protective relays can be modeled. With the help of a basic universal microprocessor one can create any relay by just making certain changes in the program, at least that is how it used to be at the initial stage of development of microprocessor-based equipment. Opinions are sometimes expressed that protective devices now available on the market are in fact only single-purpose devices designed for execution of a limited set of functions, typical of relays of some particular type.

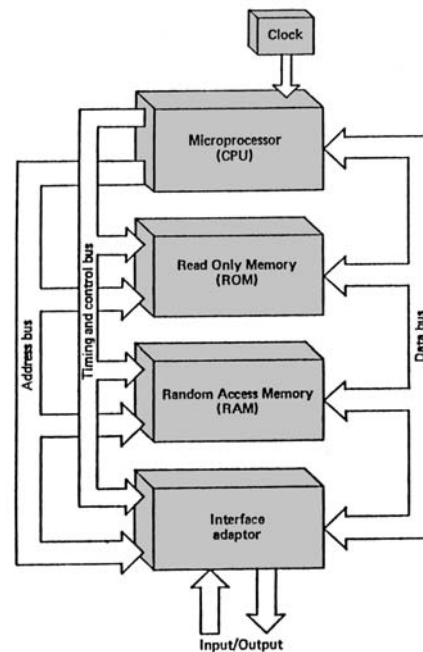


Fig. 1. Typical structure of microprocessor system.

Such devices have names corresponding to the name of a relay of a particular type, like Frequency Relays for instance, and one can communicate with such a device only with the help of a special program which specially created for this particular device, taking into account all of its peculiarities.

Actually the relay is programmed by inputting certain pick-up thresholds, time intervals, and algorithms of choosing of the proper type, among all possible types of working characteristics, but in this case, limitations are set not for the microprocessor (for which it is all the same, whatever signals to process), but for ROM containing the program of this microprocessor and the number of input and output channels.

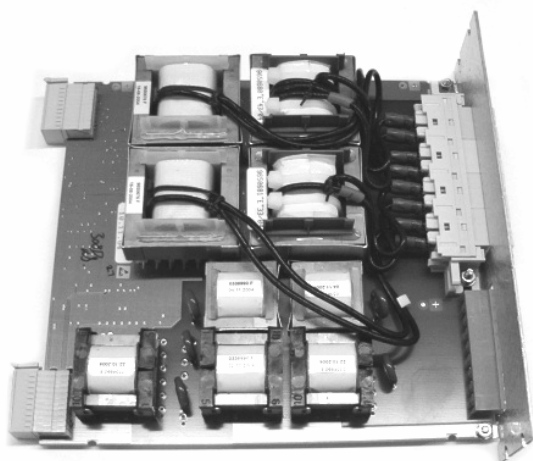


Fig. 2. Input unit with built-in CT's and VT's

If in devices performing the function of protective relays one uses not ROM (Read-Only Memory), but EPROM (Erasable Programmable Read-Only Memory) or EEPROM (Electrically Erasable Programmable Read-Only Memory) and a pocket programmer that allows recording to ROM of any algorithm of a microprocessor operation, one will obtain a Universal Protective Relay instead of a Frequency relay. It won't differ practically from modern universal Programmable Logic Controllers with digital and analog inputs such as Modicon® family (Gould Modicon) or SIMATIC® family (Siemens) and many others. Each such device may contain tens of input modules for transformation of signals to Boolean or hexadecimal code, tens of virtual timers of different types, comparators, counters of different configurations, different types of triggers, univibrators, a great number of memory registers used for recording of intermediate results, powerful output modules, etc. Using this set of virtual elements in a computer program running in Windows®, one can draw very complex automation systems (much like in graphics editors) which are then loaded to the controller. Having chosen the option "simulation", one can see on the display how this automation system works in real-time operation modes, or in emergency modes modeled purposely. Today a special computer program is used for work with each type of such controllers; however scientists are trying to create a universal program allowing work with controllers of different types.

Apparently the internal architecture and principles of operation of microprocessor-based devices have little in common with devices called "electric relays". To illustrate this fact one can mention a well-known complex universal microprocessor-based relay of the REL-316 type (ABB), designed for distance protection of power lines and for differential protection. This relay appears to be used quite often as a substation controller and not as a protective relay, since it is based on a powerful universal microprocessor supplied with a great number of logical inputs and relay outputs.

As follows from the facts considered above, in the author's opinion microprocessor-based devices, including so-called "microprocessor protective relays", should be

considered not in a literature devoted to electrical relays, but in technical computer literature, however, since these virtual microprocessor-based devices are widely used as protective relays it is still worthwhile to consider some important aspects of practical use of these devices.

First, we'll consider those numerous advantages of micro-processor-based "relays" which are usually indicated in advertisements and numerous publications of engineers from companies-manufacturers of such relays.

## II. ADVANTAGES OF MICROPROCESSOR-BASED RELAYS

1. *Many microprocessor-based relays allow us to record and then replay modes preceding and functioning during failures, for analysis of emergency situations.*

Well, were power-engineering specialists really deprived of this possibility before? Aren't there a great number of various loggers of emergency modes and of relay pick-ups? The ABB, Siemens, Areva, NxtPhase, RiS, Dewetron GmbH, etc., alone offers tens of variants of loggers and analyzers of various different emergency modes.

2. *Microprocessor-based relays allow us to change pick-up settings with the help of a computer and to turn from one characteristic to the other using only software tools.*

This is really more convenient than to adjust the relay with the help of potentiometers and a screwdriver, but how often does one have to adjust setting modes of the relay during 20 - 25 years? Two times? Three times?

3. *Microprocessor-based relays allow us to provide all the information regarding their state to remote dispatching centers through special communication channels.*

Hadn't remote multi-channel systems of data transmission (SCADA, for instance), transmitting information about the pick-up of every electromechanical relay to the dispatching desk, been used before microprocessor-based relays appeared?

4. *Microprocessor-based relays allow us to change configuration of the relay protection set: to switch some functions ON or OFF (that is to switch ON or switch OFF some relays) by software means with the help of an external computer.*

This is really much more convenient than to install separate relays and remake the assemblage in relay protection boards, but again the same question arises: How often does one actually need to resort to such operations? Once (or twice under the most adverse conditions) for the whole service term of the relay (20-25 years)?

5. *Microprocessor relays are less prone to dust, increased humidity, aggressive gas and vapors than electromechanical relays.*

The author wonders if the author of this thesis has ever been to modern halls (or rooms) of relay protection in power stations or substations. It seems that he hasn't, otherwise he would have been aware that, first, electromechanical protective relays have been produced

for decades in heavy hermetic cases of metal and glass that are well protected from dust and other negative environmental factors. Secondly, modern halls of relay protection are separate clean enclosed spaces equipped with air-conditioners maintaining stable conditions regardless of conditions outside. Microprocessor based relays are installed in similar halls.

6. *A small microprocessor-based relay can replace a whole set of standard electromechanical relays. In the first place this applies to complex distance protections. Thus you can save expensive space occupied by cabinets with relay protection.*

It is true that complex microprocessor relays occupy smaller areas of mounting by 5-10 times less than a set of standard relays with similar functions. It is also true that boards with microprocessor-based protections occupy less space by several times than conventional ones, but the tricky question is: What part of space of the power station or substation can one actually save if one replaces electromechanical relays with microprocessor-based ones? One hundred thousandth? Or one millionth?

7. *Microprocessor-based relays are more sensitive to emergency modes than electromechanical ones.*

This is also absolutely true, as all the arguments considered above given by advocates of microprocessor-based relays. The question is whether such high sensitivity and accuracy are really required in relay protection of power units. For example, let's take microprocessor-based frequency relays picking up when frequency diverts by 0.005 Hz, and standard analog electronic relays with a pick-up accuracy of 0.01-0.05 Hz (for different models). The author wonders if anywhere in the world there is a power station or substation with frequency relays performing some operations in the power system at a frequency error of 0.005 Hz from the nominal value? In many cases, even sensitivity of standard electromechanical or analog electronic relays is excessive and one has to coarsen it artificially. Can relay protection of power units face the problem of low sensitivities of the relay?

8. *Higher reliability of static microprocessor-based relays in comparison with electromagnetic relays containing elements moving mechanically.*

At first sight it may really seem uncontestable that a static device without movable elements is much more reliable than a complex mechanism with numerous interacting elements, but only on the face of it. On closer examination it appears that things are not so simple.

8.1. First, the number of pick-ups (that is the movements of movable elements) of electromechanical protective relays is paltry in comparison with their service life. Referring to his personal experience, the author can say that he has come across such cases when relays with original (factory) defects have been exploited for more than 10 years.

The fact that these defects have not been discovered for 10 years proves that during all this time the relay never picked up (and also that it is inadmissible to check relays so rarely!). Is it really worth speaking about mechanical wear in such cases?

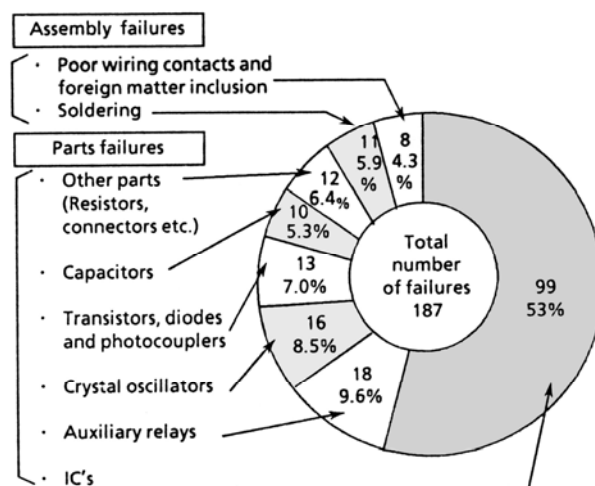


Fig. 3. Statistics of malfunctions of 378 microprocessor-based relays, produced by leading Japan companies

8.2. Secondly, the number of elements from which a microprocessor-based relay is constructed is by hundreds and thousands times more than the number of elements from which an electromechanical relay is made. The reliability theory says that there is an inversely proportional dependence between the number of elements and the reliability of complex systems. As far as reliability of the elements is concerned, everything is also not as simple as that. In the electromechanical relay affected by external factors capable of causing damage, there are only coils of electromagnets and insulation of internal installation wires. These are very reliable and stable elements, but if it was a question of improving their reliability the coils could be impregnated with epoxide resin in vacuum and internal wiring in Teflon insulation could have been used. In microprocessor-based relays practically all electronic elements are affected by the supply voltage, and a part of them by input current or voltage. Some elements are constantly in the mode of generating signals. Some components (electrolytic capacitors, for example) wear considerably under constant exposure to working voltage. As far as integral circuits (IC – basic active elements of microprocessor-based relays) are concerned, they are the main cause of relay malfunctions (Fig. 3), [1]. One of the major problems of complex electronic devices is aging of their components, bringing on changes in their parameters, during their lifetime. As a rule the lifetime of such devices usually does not exceed 10-15 years. At about that time we begin to encounter various failures, malfunctions and disturbances that are sometimes very difficult to locate in such complex devices such as in the microprocessor relays, and even if we do successfully diagnose a malfunction it is not always possible to repair it (continuing with the above example, printed circuit boards on the surface mounting microelements for instance - standard technology for microprocessor relays). In such situation it is possible to replace damaged PCB only entirely, which cost sometimes makes a significant part of relay cost. With all due respect to our new and modern technologies, it should be noted here that previously far more "simple" electromechanical protection relays, some produced as many as 40 and 50

years ago from materials and according to technologies of that time, continue to work reliably today in many power systems (in Russia, for example).

Mass maintenance of microprocessor relays presents many problems, with their built-in switching power supply. Such power supplies re-complex devices (see Fig. 4, for example) and with the addition heavy duty, continuous work, and exposure to spikes, harmonics, etc., they often fail.



Fig. 4. Built-in switching power supply.

Power supplies of microprocessor devices frequently create problems that designers did not foresee at all when developing these devices. The author experienced such a problem when a breakdown of one of the minor elements of a microprocessor device produced a short circuit of power supply. The microprocessor instantly gave a set of uncoordinated commands, which led to simultaneous disconnecting of all the power transformers of a large class 161 kV substation. Analysis of the reasons for this failure established that the short circuit of the power supply had come in the current limiting mode, as is necessary for high-grade power supplies. Current limitation is provided by fast decrease of output voltage level so that the output current does not exceed the maximal value allowed for the power supply. In the presence of large-capacity capacitors in the power supply, this voltage reduction occurred relatively slowly: during 0.5-1 second. During this time the microprocessor, whose voltage supply had essentially been reduced, started to "go around the bend" and have sufficient lengthy time to give out complete commands, causing and leading to the serious failures.

In order to prevent this, in our opinion, power supplies for microprocessor devices must be completed with so-called "crowbar protection" – a simple circuit (a thyristor, for example) which provides instantaneous short circuiting of the output of the power supply, whenever the emergency mode is enacted.

8.3. Protection functions of the important object (high-voltage line, power transformer, bus bar system and generator on power plant) have been divided between 5 - 6 separate relays till an era of microprocessor devices. Failure of one relay yet did not lead to malfunction of all protection system completely. In one microprocessor device functions of many relays are concentrated. For

example, one only the microprocessor device such as REG-216 carries out functions: differential protection; inverse-time overcurrent; negative phase-sequence; over voltage; distance protection; underimpedance; overload; overtemperature; frequency; rate-of-change frequency; overexcitation, etc. In such device failure of any common element, for example, the power supply, the microprocessor or its auxiliary elements leads to malfunction of protection system completely.

8.4. One of the serious problems which have been found out by the author [2] that discrepancy between switching capabilities of subminiature electromagnetic relays (using as output elements in microprocessor protection devices, Fig. 5) and real conditions. Researches executed by the author have shown, that as output elements of the microprocessor protection devices produced by all leading companies are used subminiature electromagnetic relays which are not intended for switching inductive loading with currents about 2 - 5 A (coils trip of high-voltage circuit breakers or auxiliary lockout relay) at 125 and the more so 250 V DC. These subminiature relays work with a huge overload and can be damaged at any moment.

8.5. Internal constant monitoring of condition (self-diagnostic, self-testing) of main units, even separate important elements of microprocessor protection device promoted by manufacturers as great progress in protection technique which allowed the maximum protection reliability [3].

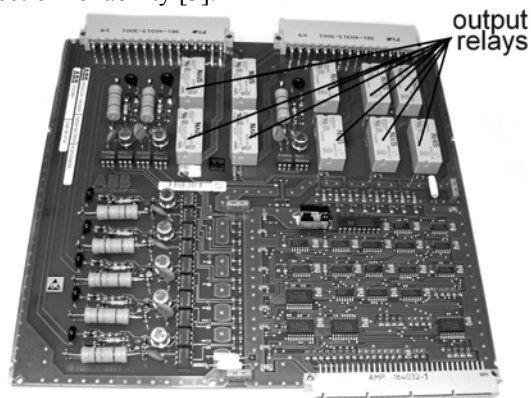


Fig. 5. I/O module with subminiature output relays

Actually, the statement that internal self-diagnostics of microprocessor relays allows increasing reliability of relay protection is not correctly. There is no connection between failure intensity of elements of microprocessor relays and the information on the happened failures. In actual fact appears no more, than an advertising gimmick. For example, in protection device MiCOM P437 constant monitoring serviceability of each of output electromagnetic relays (so, anyway, the manufacturer asserts) is available. But who can explain, how (even, only theoretically) it is possible to supervise serviceability relay (that is ability to closing normally open contacts at coil energizing or absence welding of normally closed contact of the relay) without its pickups? At more detailed consideration of this question it appears, that continuity of the coil is constantly supervised only (by passing through them of weak pulses of a current which are not causing

operations of the relay). What can happen with not energized coil? For what such monitoring is necessary?

8.6. That is why research performed in [4] led to the following conclusion:

*"Microprocessor relay reliability is lower than that of electromechanical and static relays: Microprocessor relay components tend to fail more often than those of conventional relays. This disadvantage is not compensated by a self-monitoring function, especially in unmanned substations. Maloperation or a failure to operate as a result of an internal relay failure may occur before the arrival of staff, after receiving an alarm signal".*

The experience in this area of such a huge country as the former Soviet Union and present Russia is very interesting. More than 1.6 million relay protection and automation devices, mostly Russian made electromechanical relays (Electrical Devices Plant in Cheboksary), are installed in the Russian power supply system which is one of the oldest and biggest in the world. Of those, microprocessor protection systems constitute less than one per cent. Even in the Moscow power system, one of the most advanced and well provided power systems, microprocessor devices amount to only 3 thousand out of a total of 170 thousand relay protection devices used there, which is at most 2%.

Moreover, according to specialists' evaluations, about 80% of the relay protection devices in Russia have been operating for 20 years, and some relays even for over 50 years, while their service life should not exceed 15 years [5]. It is worth mentioning that with all of this going on, the true response factor of this protection remains stable, and is over 99%! This fact suggests that Russian electromechanical protection relays are highly reliable and that even in the 21<sup>st</sup> century such protection can be successfully used in the world's largest power supply system. Such situation is characteristic not only for Russia, but also for other old power systems. In spite of the fact that microprocessor relays exist in the market any more first ten years, rates of replacement of electromechanical or old static relays remain, on the average, very low. According to [3] it will take about 70 years to replace all the predecessor relays with modern microprocessor. Yet it is clear that the life-time of the major part of the electromechanical protection relays has expired and they are called for replacement. Because of aging of bronze and brass subjected to permanent mechanical stress, and peeling of the insulation material of relay wires, they are only microns far from short circuit. At the same time in the opinion of many Russian specialists in the field of power engineering, total replacement of traditional Russian electromechanical relays by compatible digital parts made in Europe and USA will result in a drastic increase of emergency cases in power supply systems. Moreover, unlike their Western colleagues, the Russian manufacturers of low voltage equipment advance a sound belief in rational implementation of technical innovations in such specific fields as relay protection. They believe that in the next three to five years all of the obsolete equipment should be

replaced *with traditional time-proved* electric equipment, and only then should carefully planned installation of digital devices begin in power installations. This should be done selectively rather than totally, and moreover that the microprocessor relays be backed up with new generation electromechanical protection systems.

Leading manufacturers of microprocessor devices, such as ABB, Siemens, and Alstom have successively penetrated the Russian market, however at the moment even they show certain caution, taking into account the scale of the Russian power system and the possible loss in case of a major crash. ABB for example, purchased in Russia sets of microprocessor protection relays for its project at one of the biggest power stations in Kyrgyz, and then connected them in parallel with its own (Russian) electromechanical relays. A similar solution was used in some other objects, for example at the Zubkovsky substation at the center of Moscow. In spite of such very careful treatment of microprocessor protection devices in Russia and their very limited use, the rate of these device failures in the Russian power supply system still turned out to be twice as high as that of the traditional protection devices. The following data were brought up: Within three years, from 1999 to 2001, 100 out of 23264 operations of relay protection devices at the Novosibirsk power system were false responses. Part of these false responses occurred with modern equipment that was only lately put into operation. In another case false responses of Siemens microprocessor devices at one of the thermal power stations of the Moscow power system "Mosenergo" resulted in disconnection of all of these protection systems, which remained unconnected for more than two years. At another substation of the same power system microprocessor relays were damaged by a stroke of lightning. At a power station in Kostroma microprocessor device failures were triggered by... static voltage from synthetic carpets.

Taking into account that safe operation of the entire power supply system depends on the relay protection system, the above-mentioned cases are more than just unfortunate incidents. This is a problem that needs to be immediately addressed. Moreover, it is clear that as a result of such incidents which occurred within the last few years, the excitement about implementation of intellectual digital technology in Russia has declined. At present 70% of the Russian low voltage industrial equipment market (which also includes relay protection devices) belongs to foreign companies. Because of serious accidents that occurred in the Western power supply systems this fact does not inspire the Russian specialists: They "do not want to repeat somebody else's mistakes", as mentioned in one the publications.

These were some of the so-called "advantages" of microprocessor-based protective relays. Let's take a look at their disadvantages.

### III. DISADVANTAGES OF MICROPROCESSOR-BASED RELAYS

3.1. *Impact of electromagnetic disturbances from the power supply network on operation of the relay: blackouts, sags, spikes, surges, (Fig. 6). These impacts can enter electronic equipment through AC network,*

serial or communication lines and damage or destroy components, data will be lost.



Fig. 6. Fragment of I/O module with numerous damages elements and breakdown tracks on printed circuits.

Many cases of malfunctions and even damages of microprocessors caused by spikes and surges are described in literature. For example, mass malfunctions of microprocessor-based time relays occurred in nuclear power plants in the USA. A review of these events indicated that the microprocessor-based timer/relay failed as a result of voltage spikes that were generated by the auxiliary relay coil controlled by the timer/relay. The voltage spikes, also referred to as "inductive kicks," were generated when the time-delay contacts interrupted the current to the auxiliary relay coil. These spikes then arced across the time relay contacts. This arcing, in conjunction with the inductance and wiring capacitance generated fast electrical noise transients called "arc showering" (electromagnetic interference). The peak voltage noise transient changed as a function of the breakdown voltage of the contact gap, which changed as the contacts moved apart and/or bounced. These noise transients caused the microprocessor in the time relay to fail.

The organization of the supply system of relay protection is also very important. Power units are supplied by powerful accumulator batteries with a constantly connected charger, or by an *uninterrupted power supply* (UPS) cushioning the negative impact of the factors listed above, however the same system supplies driving gears of power switches and many other devices, causing spikes. Besides, investigations of UPS systems [6, 7] have shown that at certain conditions noise spikes and high harmonics can get into microprocessors through grounded circuits and neither UPS nor filters can prevent this. Thereupon, another aspect of the problem gains our attention: suspensions and malfunctions of operation of the own microprocessor of the UPS in emergency modes on high-voltage circuits.

When the control microprocessor malfunctions, alternation of switching-ON and switching-OFF of power semiconductor elements of the inventor may be disturb and short circuit loop making, followed by automatic switching-OFF of the input circuit breaker of the UPS. This same phenomenon can happen to automatic chargers whose microprocessors are supplied from an external auxiliary UPS. Such incidents quite often occur in practice, but nobody yet has concerned himself with a serious analysis of the reasons. It is quite possible that the reasons for such emergency switching of USP, and of the chargers, are similar to those for the case considered above.

*3.2. Microprocessor-based relay protections, especially complex ones such as distance protections, do not always operate adequately in complex failures or on*

boundaries of protection zones and can not always trace transient processes correctly and in proper time. In practice one often comes across breakdowns and malfunctioning of complex microprocessor-based protections in exploitation conditions. If the relay is tested on a standard laboratory test bench with standard signals at its inputs, it will operate precisely and reliably. The problem is that it is impossible to simulate all possible combinations and signal distortions that may take place in real situations on a test bench. It is also impossible to foresee all such situations when the relay is designed. This situation is similar to when a properly functioning powerful PC equipped with an undamaged powerful software shell (such as Windows®) suddenly buzzes at a certain instruction set, or if several programs run simultaneously. In most cases it is impossible to foresee and prevent such situations. The working group of the USA and Canada has published the report on the reasons of well known accident (August 14, 2003) in which it is ascertained, that one of the reasons of occurrence of computer "suspension" of control system and occurrence of emergencies in a power supply system of the company "First Energy" in USA. In electromechanical relays such situations are impossible. Therefore a many researchers insist that at the further wide introduction of digital techniques in protective relaying it is necessary to provide additional independent (reserved) not digital protection relays for emergency modes.

*3.3. A strange phenomenon exist whereby high-speed microprocessor-based protections respond to the emergency mode much more slowly then electromechanically ones.* In some of the power systems for reliability improvement microprocessor-based and electromechanical distance relays are switched in parallel. When emergency situations were analyzed, more than once it turned out that the electromechanical relay had picked up and tripped the circuit breaker *before* the microprocessor-based relay responded. This may be explained by the fact that unlike an electromechanical or analog electronic relay, the microprocessor-based relay operates with input values discretely. It "picks" current values of input quantities and copies them into the buffer, then picks another set of input values in a certain time interval and compares them with those stored in the buffer. If the second set is identical to the first, the input values are directed to the microprocessor for processing. In general, for pick-up of an electromechanical or instantaneous electronic relay 10-15 milliseconds are enough, while for a microprocessor-based relay 30-40 milliseconds are required (theoretically). Actually full operating time of microprocessor relay frequently reaches up to 50-80 ms for complex failures. So it often turns out that the superior performance of the microprocessor-based relay indicated in the advertisement of the producer is not provided in practice. In transient emergency modes the microprocessor has to process great sets of information in a real time mode, accompanied by quick and considerable changing of input signals. For this it requires certain time (sometimes hundreds of milliseconds). Moreover, if after the starting of the microprocessor the situation changes (for example, a

single phase short circuit to the ground turned to the two-phase and then to the three-phase one), the starting process of calculation is interrupted and all calculations must be performed from the very beginning.

*3.4. There are essential differences in operation of electromechanical and microprocessor-based relays caused by their different susceptibility to harmonics, saturation, and other wave distortions.*

It is well known that at great ratios of short circuit currents, current transformers considerably distort the curve of the output current applied to the relay. The problem of deterioration of accuracy is relevant for all types of relays, including electromechanical ones. Electromechanical relays produce torque that is proportional to the square of the flux produced by the current. These relays respond to the current squared or to the product of the currents produced by the input quantities. Since root-mean-square (rms) is defined as the average of the integral of the square of the current, these relays are said to be rms responsive. For most microprocessor relays, all quantities other than the fundamental component are noise. These relays used digital filters to extract only the fundamental and either attenuate or eliminate harmonics [8]. The Fast Fourier Transformation (FFT) is a very useful tool for analyzing the frequency content of stationary processes in microprocessor relays. Protection algorithms based on FFT have serious disadvantages including the neglecting of high frequency harmonics, when dealing with non-stationary processes (magnetizing inrush and fault currents) for determining the frequency content. Furthermore, different windowing techniques should be applied to calculate the current and voltage phasors and this causes significant time delay for the protection relay. In this case, accuracy is not assured completely [9]. For example, in cases of influence of inrush current on transformer differential relay with harmonic restraint, the relaying information is contained in the system fundamental and the harmonics only interfered. It is somewhat surprising that the digital filter will faithfully extract the fundamental from any waveform that is periodic at system frequency. The distance elements, in another example, did not operate because no voltage depression accompanied the high current signal. However, sensitive settings caused the negative-sequence directional to identify a forward fault.

*3.5. Considerable complication of exploitation of the protective relay* apparently: testing and adjustment of microprocessor-based protections with the help of a computer (or even without it) require some new level of training of specialists and more time (what we mean here is that a technician or an engineer doesn't have to adjust the same relay every day, but they have to learn everything about it from the very beginning and to gain an understanding of testing methods). It is enough to look through Instruction Manuals of these devices, which are looks as thick book, to realize this, and as far as trouble tracing and repair of such devices go, this is practically impossible during the exploitation. An article [10] tackles the problems arising during testing of microprocessor-based relays. The acceptance test is a step-by-step

procedure published in the relay's instruction manual that checks that the relay's measuring elements, timing elements, status inputs, contact outputs, and logic processing system are functional, and that relay performance is within the manufacturer's intended specifications, using settings and logic defined by the manufacturer's test procedure. The test will include calibration checks involving secondary current and voltage injection. The relay is not field calibrated since, generally, only factory processes can calibrate numerical relays. In the process of working through these tests, one will learn a bit about the relay and will perform the value of showing that the relay is functioning correctly. The acceptance test does not make one completely knowledgeable of the relay, so some time should still be set aside for further investigation of the relay as the commissioning program proceeds.

Modern microprocessor-based systems (as line current differential protection, for example) are complex devices that include sophisticated protection algorithms and intense communications. As a result, performance testing of such complex systems may create a problem particularly because expensive and specialized equipment is required. Basic validation testing may be performed using phasors and test sets as far as the protection functions are considered; and a local loop-back procedure as far as the communications are considered. True performance testing requires either a real-time digital simulator or a playback system capable of driving several sets of three-phase currents and voltages (2- and 3-terminal testing). Testing the communication channels for high noise, bursts, channel asymmetry, channel delay, etc. is a field that does not belong to traditional relay testing. This requires new expertise and specialized test equipment. Due to complexity of modern current differential relays, it is highly beneficial, if not crucial, to conduct performance tests involving both protection and communication functions particularly if difficult system conditions or poor communication channels are anticipated.

*3.6. The increasingly large weight of the "human factor"* in the operation of microprocessor relays created many more opportunities for additional mistakes, particularly during the programming and testing stages of the relay. Many interrelated functions and parameters controlled by one microprocessor-based relay lead to the necessity of artificial coarsening and even to entire disabling of some functions to test the other ones. After testing, one shouldn't forget to input the previous settings of the relay. Such problems don't exist in electromechanical relays. In instruction manuals for many such relays it is indicated that the settings of the relay may be changed during testing of the relay, which is why after that one should carefully check them.

In addition, the interfaces of many modern programs can often not too friendly, and the internal logic that works with them can sometimes be arrant anguish! Many new programs (including from some very well-known companies!!) are simply "raw" and contain a lot of bugs. Who can know what will occur if even one bug starts to control relay protection?

3.7. *Information redundancy.* Many digital relays have too many variants of parameters for setting such which are not unequivocally necessary for relay functioning. Especially it concerns the devices with complex functions, such as distance protection with their one hundred set parameters. A functions for 15 - 20 the light-emitting diodes located on the forward panel of the relay; a degree of brightness of the screen; color of a luminescence of the screen; color of the reports of information display; time of preservation of the data on the screen; and many other parameters with numerous variants which can be chosen from library of parameters. Frequently, these variants are superfluous. For example, in microprocessor protection device MiCOM P437 only the fuse supervision algorithm for voltage transformer can be chosen on four different variants! Such obvious redundancy leads to great number of settings variants passes for the protection device with complex functions. It increases of a mistake probability because "the human factor". The problems pertinent to the human factor grow repeatedly if the same group of people should serve the relay of the different manufacturers having various programs with different interfaces, different principles of a parameters choice, at times adjustments, even different names and designations of the same main parameters.

3.8. *Possibility of intentional remote actions to break the normal operation of the microprocessor-based relay protection (Electromagnetic Weapons, Electromagnetic Terrorism).*

Intensive investigations in electromagnetic weapons field are being carried out in Russia, the USA, England, Germany, and China. In the USA such research is carried out by the biggest companies of the military-industrial establishment, such as TWR, Raytheon, Lockheed Martin, Los Alamos National Laboratories, the Air Force Research Laboratory at Kirtland Air Force Base, New Mexico, and many civil organizations and universities. The German company "Rheinmetall Weapons and Munitions" has also been researching E-weapons for years and has test versions. The EMP shell was designed following revelations that Russia was well ahead of the West in the development of so-called radio-frequency weapons. A paper given at a conference in Bordeaux in 1994 made it clear that the Russians believed it possible to use such weapons to disable all of an enemy's electronic equipment. Written by Dr. A. B. Prishchepko, Deputy Director of Scientific Center "Sirius", Member-correspondent of the Russian Academy of Military Sciences and entitled "Radio Frequency Weapons on the Future Battlefield", it described Soviet research dating back to the late forties, provoking near panic among western military planners [11]. It gave credence to the nightmare scenario of a high-technology war in which all the radio, radar and computer systems on which their weapons depended would be disabled, leaving them completely defenseless. As of late, many projects of past age have been declassified and are freely sold today. For example, the Institute of High Current Electronics of the Russian Academy of Sciences in Tomsk (HCEI SB RAS) offers at free sale ultra-wideband high-power sources of directional electromagnetic radiation (Fig. 7).

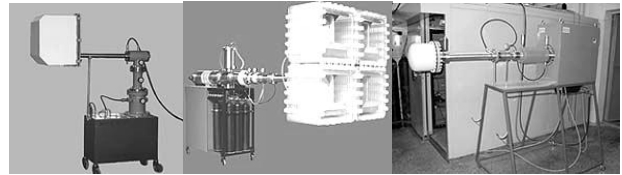


Fig. 7. Compact ultra-wideband generators of directional pulse electromagnetic radiation with power output up to 1 GW (Institute of High Current Electronics, Russia)

As the technology of military RF weapons matures, such weaponry also becomes affordable and usable by criminals and terrorists [12]. Both cheap low-tech and expensive high-tech weapons exist. High-power sources and other components to build EM weapons are available on the open market and proliferate around the globe. Electronic components and circuits, such as microprocessors, are working at increasingly higher frequencies and lower voltages and thus are increasingly more susceptible to electromagnetic interference (EMI). At the same time, there have been rapid advances in radio frequency (RF) sources and antennae and there is an increasing variety of equipment capable of generating very short RF pulses that can disrupt sophisticated electronics. Intentional electromagnetic interference (EMI) poses a significant threat worldwide.

In addition, it turns out that "electromagnetic terrorism" is not the only form of modern remote terrorism to which microprocessor-based relays are prone. There are also electronic intrusions called *cyber-attacks*.

A cyber intrusion is a form of electronic intrusion where the attacker uses a computer to invade electronic assets to which he or she does not have authorized access. The IEEE defines electronic intrusions as:

*"Entry into the substation via telephone lines or other electronic-based media for the manipulation or disturbance of electronic devices. These devices include digital relays, fault recorders, equipment diagnostic packages, automation equipment, computers, PLC's, and communication interfaces".*

A cyber-attack can be an intrusion as described above, or a *denial of service attack* (DOS) where the attacker floods the victim with nuisance requests and/or messages to the extent that normal services and functions cannot be maintained. A DOS attack is also called a *flood attack*. A *distributed DOS attack* (D-DOS) is a flood attack launched simultaneously from multiple sites. More full and in detail this problem is described in author's publication [13].

#### IV. CONCLUSIONS

1. Did microprocessor-based relays introduce any new functions for relay protection that were unknown before or impossible to implement with the help of traditional relays? On closer examination it appears that the answer is NO. Microprocessor-based relays only combined features of some relays adding some functions that used to be carried out by registration devices.

2. Do microprocessor-based relays provide a higher level of reliability of power supply? NO!

3. Did microprocessor-based relays make the work of the maintenance staff simpler? Obviously NO!



4. Do microprocessor-based relays have any uncontested advantages? Again the answer would appear to be NO! Microprocessor relays have appeared as a result of developments in microcontrollers and not in order to improve conventional (static or electromechanical) relays. The behavior of conventional relays in operation continues to be excellent. Why do we need to make our life more complicated by using microprocessor based relays, which on the one hand have no essential advantages in comparison with traditional ones, and on the other hand have many of their own unsolved problems? It turns out that there is an important reason to use microprocessor-based relays, however it doesn't lie in the power industry field, but in the field of...relay production [14]. It appears that it is much more profitable to produce microprocessor-based relays than electromechanical or even analog electronic ones. The structure of microprocessor relays is extreme simple: a box with sockets (slots) and the set of printed circuit boards. This is explained by the possibility of complete automation of all technological processes and production and control of parameters of microprocessor-based relays. The following question is to the point here: Where do problems of manufacturer's concern development of correct technical politics in the power industry field? In fact, the largest international concerns, such as ABB, General Electric, Siemens, Alstom have become "trendsetters" in the power industry and now determine main tracks of development not only of relay protection, but also of the whole power industry. If in some years these companies stop producing all other types of relays except for microprocessor-based ones (and this is the main tendency today), this fact won't justify uncontested advantages of such relays from the point of view of interests of power suppliers and of the whole society.

5. The transition to microprocessor relays (if inevitable!) should be complete, that is excluding teamwork with electromechanical relays, such transition should be carried out together with the replacement of traditional instrument transformers to optical, and full replacement of all electric wires connected to the relay to isolated optical wires. Microprocessor relays should be mounted in closed metal cases made with use of high-frequency technology. Relay power supplies should be carried out through the unit's "motor-generator".

To neglect these requirements could lead to serious problems in the electric power industry in the near future.

So we can see that indeed there are many new problems still not known in world of electromechanical relays.

#### V. REFERENCES

- [1] T. Matsuda, et al., "Experience with Maintenance and Improvement in Reliability of Microprocessor-Based Digital Protection Equipment for Power Transmission Systems". Report 34-104. SIGRE Session, 30 August – 5 September 1992, Paris.
- [2] V. Gurevich, Nonconformance in Electromechanical Output Relays of Microprocessor-Based Protection Devices under Actual Operating Conditions//Electrical Engineering and Electromechanics, 2006, 1.
- [3] G. Johnson and M. Thomson, "Reliability Considerations of Multifunction Protection". – Basler Electric Co.
- [4] "Aspects of Digital Protective Relaying". Report RE-626. IEC, Israel, 1991.
- [5] Material of the 15<sup>th</sup> Scientific and Technical Conference, "Relay protection and automation of power supply systems, 2002".
- [6] The Power Protection Handbook. – APC, 1994.
- [7] B.D. Dshochov, Features of power supply of computer network elements // Industrial Power Engineering", 1996, N2, p.17-24.
- [8] S.E. Zocholl and G. Benmouyal, "How Microprocessor Relays Respond to Harmonics, Saturation, and Other Wave Distortions". Schweitzer Engineering Laboratories, Inc. Summer 2003.
- [9] N. Neneş O.O., Onbilgin G., Kocaman C. Transformer Protection Using the Wavelet Transform //Turkish Journal of Electrical Engineering & Computer Sciences, Vol.13, No.1, 2005.
- [10] J. Reason, Realistic relay tests need fault reconstruction //Electr. World, 1991, v. 205, N 5, pp. 41-42.
- [11] A. B. Prishchepenko, V. V. Kiseljov, and I. S. Kudimov, "Radio Frequency Weapon at the Future Battlefield", "Electromagnetic environment and consequences", Proceedings of the EUROEM94, Bordeaux, France, May 30-June 3, 1994, part 1, p. 266-271.
- [12] Gurevich V. The Hazards of Electromagnetic Terrorism //Public Utilities Fortnightly, June 2005.
- [13] V. Gurevich, Electromagnetic Terrorism: New Hazards // Electrical Engineering and Electromechanics, 2005, 4.
- [14] F.S. Schleithoff, Statischer Schutz im Mittelspannungsnetz //Elektrizitätswirtschaft, 1986, v. 85, No. 4, pp. 121-124.

*Поступила 15.11.2005*