1

Technical Progress and Its Consequences

The Philosophy Behind Technical Progress

> *Rational planning in the development of technology more often than not leads to irrational consequences, and technology enters the human consciousness not as a neutral means of meeting our own needs, but as a goal in itself, an alienated force.*
>
> Professor N.V. Popkova, DSc

What is technical progress? The dictionary of philosophy provides this definition:

> *Technical progress – is the interdependent, and mutually stimulating development of science and technology. This concept was introduced in the 20th Century in the context of a basis that made use of a consumerist attitude to nature and a traditional scientific and engineering view of the world. The aim of technical progress is defined as meeting man's ever growing needs; the means by which these demands are met lies in the realisation of achievements in the natural sciences and in technology.*

As N.V. Popkova, Doctor of science in Philosophy wrote in his article 'The Philosophy of Technology' [1.1], technological innovation was indeed introduced by man as a way of improving our daily lives and of meeting our needs: the anthropogenic environment performs this task and enables Earth's ever growing population to obtain the material pre-requisites for life. In recent years, however, ever more profound consequences of technological growth have come to light: the suppression of the inherent biological and humanitarian aspects of human life, and their displacement with anthropogenic values and arrogance. This gives rise to an ambiguous evaluation of the role of the anthropogenic environment: the predominantly positive evaluation that existed in the past and the negative one, which is gaining weight. The main problem lies in the intricacies of managing the anthropogenic environment and in the fact that it is impossible to control its development or even predict how it will react to the introduction of subsequent innovations. The discovery at every stage of technical work of unpredictable and undesirable results shows that: *the anthropogenic environment has always in part been outside the control of the human race that is creating it, which means that it has always possessed autonomy.*

Protection of Substation Critical Equipment Against Intentional Electromagnetic Threats,
First Edition. Vladimir Gurevich.

Thus it is far from the case that the development of technology has always been aimed at 'meeting the ever growing needs of man,' since according to our observations technical progress only began to adopt this characteristic in the second half of the twentieth century.

An old science fiction novel featured an engaging plot, which arose out of something relatively innocent: an unusual night time phone call made to each of the inhabitants of planet Earth. It was in this phone call that the 'Global Mind' announced its' coming to everyone on planet Earth. It turned out that at some stage in its development the proliferation of computers had transformed into something new: millions of computers, which had been combined into an overall network and which controlled everyone and everything on planet Earth had suddenly come to the realization that they represented a single entity capable of reproducing themselves using automated factories and robots that had been integrated into this same network, and of defence with the help of computerized weapons systems designed to destroy mankind. As far as the 'Global Mind' was concerned humanity was nothing more than a rudiment, or ballast that was devouring the planet's resources. You can work out how the plot unfolded from there for yourselves.

Today, almost all modern industrial production methods as well as systems controlling the supply of water, electricity and telecommunications and communications systems, are controlled by computers with a network connection. The terms *Smart Grid* and *Artificial Intelligence based relay protection* have appeared in technical rather than science fiction literature. Issues surrounding the creation of a Smart House, in which even the fridge would be able to assess the levels of the provisions stored inside it and on the basis of this analysis of demand draw up an order and send it via the network to the local supermarket, are being discussed today in technical literature and not in science fiction. Today microprocessors can be found anywhere, even in the toilet seat lid.

Humanity is making huge strides towards the creation of an unpredictable Global Mind, which the old science fiction novel had foreseen. Thus this old plot has long since made the leap from the pages of science fiction novels into the pages of respected philosophical journals and books that illuminate issues in the philosophy of technology. This is a relatively new field of philosophical research, which is aimed at understanding the nature of technology and evaluating its impact on society, culture and man. One school of thought suggests that the philosophy of technology is not, if anything a philosophy in itself but a multidisciplinary intellectual field, in which technology as well as the problems it creates are typically examined as broadly as possible.

At the VISION-21 symposium that was conducted in 1993 by NASA's Lewis Research Centre and the Ohio Aerospace Institute the famous professor of mathematics Vernor Vinge delivered a much talked about speech [1.2]:

> *The acceleration of technical progress – is the key feature of the XX Century. We are on the verge of changes comparable to the emergence of man on Earth. The specific reason for these changes lies in the fact that the development of technology inevitably leads to the creation of beings with an intellect that surpasses that of humans…Large computer networks (and their consolidated users) are able to 'come to the realisation' that they are supernaturally intelligent beings… an event like this would nullify the entire statute book of human laws, possibly in the blink of an eye. An uncontrolled chain reaction would begin to develop exponentially with no hope of regaining control of the situation.*

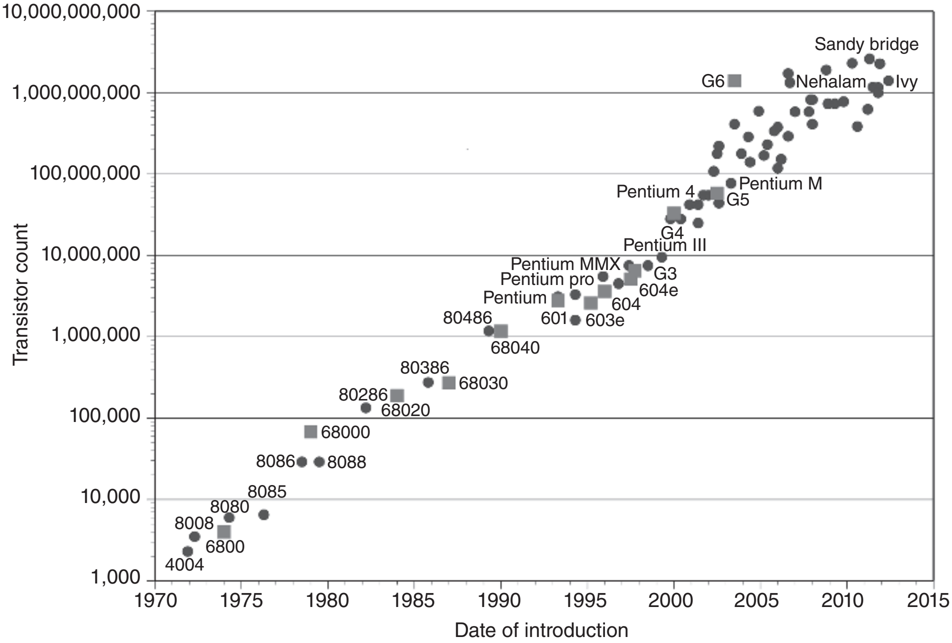


Fig. 1.1 The relationship between time and the number of transistors in microprocessor chips. The vertical axis has a logarithmic scale and the relationship conforms to exponential law.

Vinge proposed a new term for this phenomenon: *Technological singularity*. Normally singularity is understood to mean an isolated point of some kind or a function field, the meaning of which denotes infinity or which demonstrates other behavioural irregularities, it denotes a critical point beyond which the value of a function becomes indefinite and unpredictable. Typical examples of singularity are an avalanche breakdown in semiconductor structures, a tunnelling effect in electrical contacts and in semiconductors, an area of volt-ampere response in a negative resistance diode and so on. Technological singularity implies a certain point in the development of technology as a whole, but specifically the development of computer technology and artificial intelligence beyond which their further development becomes firstly irreversible and independent of humans, and secondly unpredictable.

Naturally, the so-called Moore's law [1.3] would have influenced Vinge's views; this was formulated in 1965 by one of the founders of Intel Gordon Moore. This law states that the number of transistors in microprocessors doubles approximately every 2 years and their productivity grows exponentially as in Fig. 1.1. This law has been valid for 40 years now. Not only do microprocessor and computer technology, which are becoming ever more complex, conform to exponential law but also other types of technology, and with it society. The sociologist M. Sukharev in his work 'An Explosion of Complexity' [1.4] writes:

> *There is another pattern that is visible in the development of society - the acceleration in the growth of complexity over time. Tribal people have lived on the Earth for thousands of years, armed with spears and arrows. In the space of a few*

> *hundred years we have outstripped an industrial and technological civilisation. How long the computer stage will last is not clear, but the speed at which today's society is evolving is unprecedented…*

Many eminent specialists confirm this thinking:
Doctor of Sciences I.A. Negodayev [1.5]:

> *The pattern in the development of technology lies in its subsequent sophistication. This sophistication happens either by increasing the number of elements integrated into a technical system, or by changing its structure.*

The Director and Chief Designer of the Central Scientific and Experimental Design Institute of Robot Technology and Technical Cybernetics, and Associate Member of the Russian Academy of Sciences V.A. Lopot and Doctor of Technical Sciences Professor E.I. Yurevich [1.6]:

> *The overall pattern in the scientific and technical development of all areas of human activity – is the progressive sophistication, integration, and intensification of technology.*

Bezmenov A.E. PhD [1.7]:

> *The trend in the development of technology is characterised by the ever growing sophistication of machines, equipment, and installations. With an increase in the sophistication of these items, their reliability (all other things being equal) diminishes.*

If the 'Explosion of Complexity' in everyday technology is happening to everyone in plain sight and requires no evidence, then the sophistication of technology in industry is not so obvious to the layman. Therefore, we will examine a few concrete examples that confirm this trend.

The Swedish company Programma Electric AB, known all over the world, was founded in 1976 (this company was acquired by General Electric in 2001, and in 2007 it became part of the Megger Group Ltd) and produces a huge nomenclature of equipment and installations to test electrical power engineering equipment: from highly accurate timers and systems testers of protective relays to sources of powerful currents. One of the items this company produces is the B10E equipment pictured in Fig. 1.2, used to measure the minimal pick up voltage in high voltage circuit breaker drives.

In accordance with IEC standard 62271-100 these circuit breakers need to be tested for their compliance with the manufacturer's parameters for the minimal pick up voltage. In general, this refers to a swash that performs a very simple function: a preliminary check on a certain level of voltage controlled by a voltmeter, with the voltage being fed subsequently to the device's output terminals. It is not complicated to develop a diagram for this device, as in Fig. 1.3. In this device the output voltage is set by the variac AT, rectified by a diode bridge, and smoothed by the large capacity (several thousand microfarads) capacitor C. The voltage is fed to one pair of output terminals from a variable alternating current source and to the other from a variable direct voltage source.

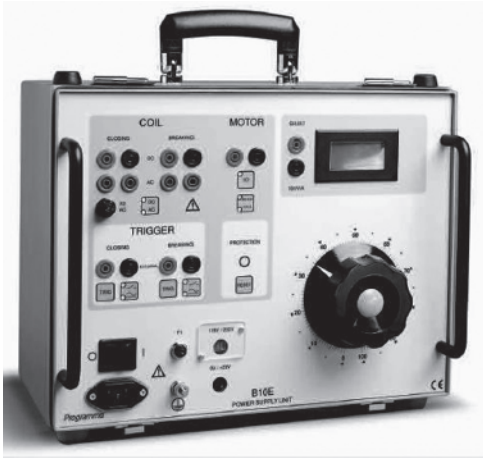


Fig. 1.2 The outside of a B10E type device used to test the minimal pick up voltage in high voltage circuit breaker drives.

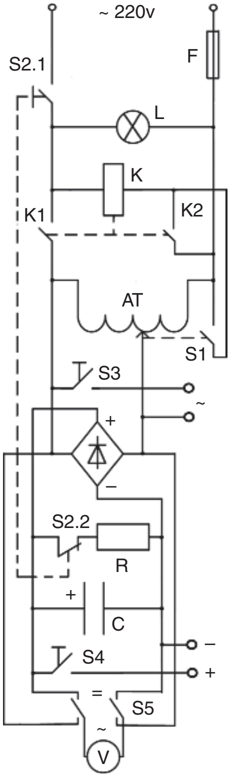


Fig. 1.3 An example of a diagram for a simple device used to test high voltage circuit breakers, which performs all the necessary functions.

The output voltages are monitored with the help of the voltmeter V. In order to prevent any inadvertent high voltage (250 V) feed from the device to the low voltage (24–48 V) coil or to the motor, the S1 micro-switch is fitted to the variac in such a way that its contacts are closed by the movement of the plunger attached to the shaft and only in the neutral position by the variac arm. When the S2 button is pressed the discharge resistor

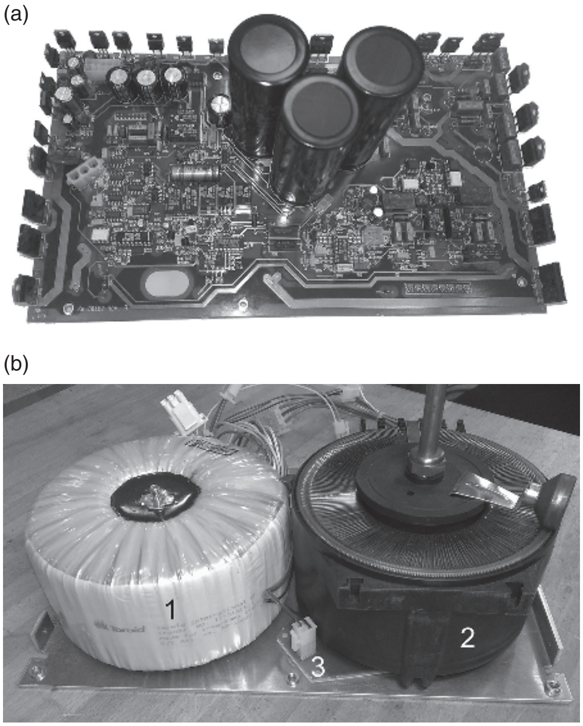


Fig. 1.4 (a) The electronic assembly of the B10E device. The semiconductor elements installed along the edges of the printed board are pressed against the case, which is used as the heatsink for the semiconductor elements during assembly. (b) The power unit in the B10E device: 1 – the multi circuit transformer with a series of different output voltages to feed the device's electronic assemblies; 2 – an adjustable transformer (variac) and 3 – the sensor board for the angle sensor on the variac shaft.

R is cut off from the capacitor C and the voltage is fed to the device's input terminal. In order to feed the circuit breaker coil with the voltage preliminarily supplied with the help of the voltmeter and variac, in addition to the S2 button being pressed, one of the S3 buttons (the alternating current output) or S4 (the direct current output) is pressed. If the circuit breaker does not work, the voltage is increased and the S2 button is held down as one of the S3 or the S4 buttons is pressed once again.

Let us now see how this simplest of algorithms is realized in the B10E device produced by the famous company in Fig. 1.4.

The electronic assembly of the B10E device shown in Fig. 1.4(a) contains 13 electromagnetic relays, 14 different types of integral microcircuits, 10 1A current rectifying diode bridges and 2 powerful 40EPS08 (40A, 800 V) type diodes, 4 high power BUX98AP (24A, 1,000 V) transistors); 3 high power BTA26–400B (25A, 400 V) triacs, 4 high power gate-turn off GTO thyristors (13.5A, 800 V) and 2 precision PBV type current shunts.

To be honest, I admit that when I opened this device with the aim of repairing it, I was completely shocked by what I saw. I was particularly affected by the electronic angle sensor on the variac shaft in place of the simplest micro-switch (as shown in Fig. 1.3). The complete incompatibility of the simplest of functions carried out by this equipment with its technical realization is plain to see. It would be interesting to know what justification the developers of this device used for such an agglomeration of electronics.

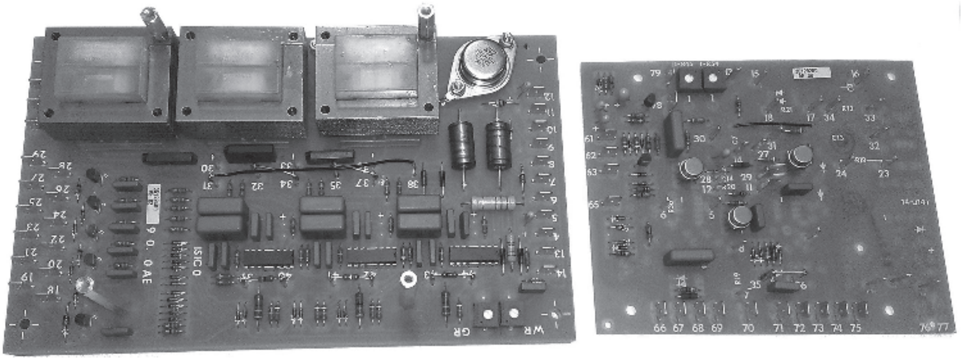
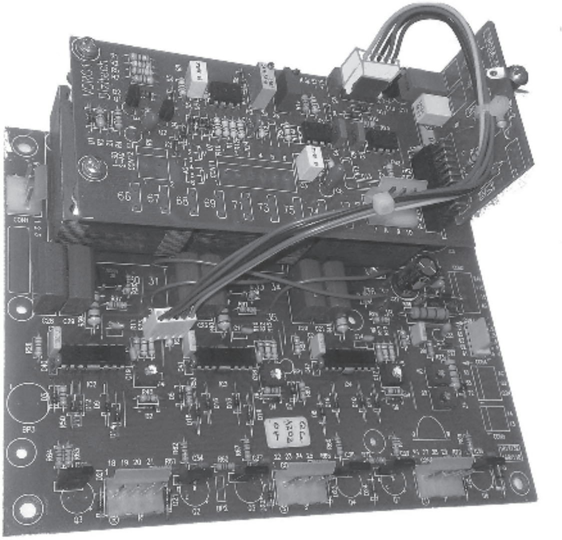


Fig. 1.5 The two modules of the old charger controller that were developed and mass produced in huge numbers in the 1970s by AEG. On the right is the analogue module that controlled the output voltage and current of the charger and which sent a signal to the pulse firing module (on the left) and formed control pulses for the thyristors.

Fig. 1.6 A battery charger's control module produced on a modern element base in accordance with a design developed by AEG in the 1970s.



Here is another example from the field of power stationary battery chargers, widely used in power stations and substations in auxiliary direct current systems. This unit consists of the following principle assemblies: a power transformer, a block of power thyristors and an electronic thyristor control assembly. At the beginning of the 1970s AEG developed a thyristor controlled charger, shown in Fig. 1.5, which proved so successful that it is still used more than 40 years later by different manufacturers in various types of charger unit. Moreover, some manufacturers have copied this control assembly in its entirety, while others have transferred it over to a modern element base, see Fig. 1.6, which in essence does not change the assembly.

Unfortunately, no matter how well analogue technology has proved itself in charger control systems over the course of 45 years both in terms of reliability and ease of repair, at this point it has to be said that it has already been usurped completely by digital devices

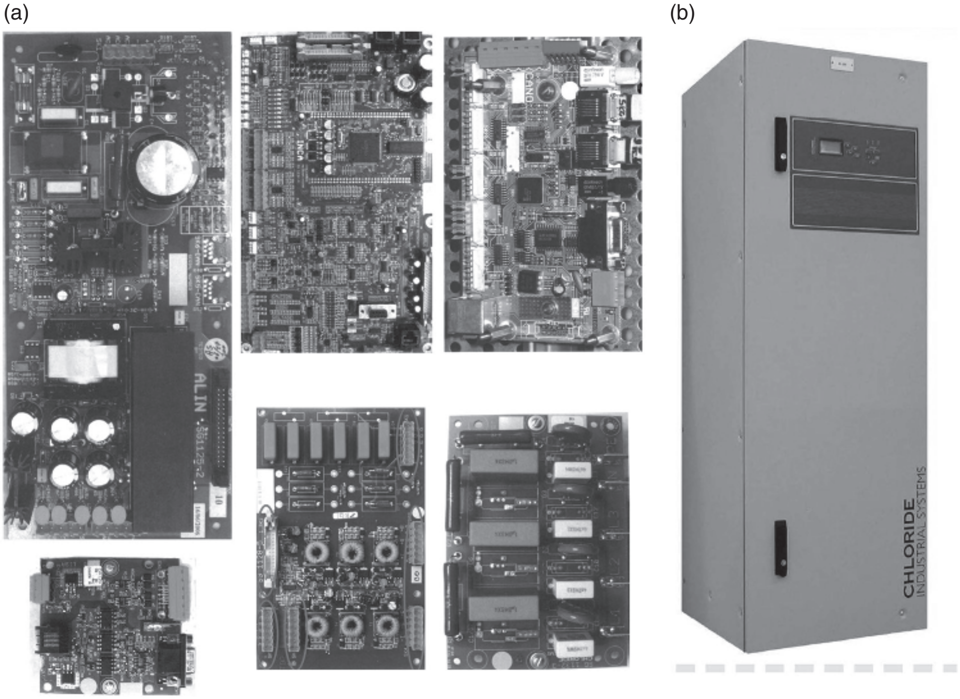


Fig. 1.7 (a) A set of the microprocessor based control modules for the Apodys series battery charger produced by Chloride France S.A. (b) A battery charger from the Apodys series produced by Chloride France S.A., part of the Emerson group.

based on microprocessors. What in terms of new properties have microprocessor controlled battery chargers acquired? (See Fig. 1.7.)

They are as follows: a 'branching' menu in which it is not easy to find the required function in place of the three output voltage control potentiometers and a mode switch; an IP-address and a network connection, which enables hackers to interfere with the operation of the unit; a modern fiber optic connection between the internal modules in place of the traditional copper cables and so on.

One might continue the description of examples that demonstrate 'an explosion of complexity'. For example, in Fig. 1.8 the MCT1600 device, produced by Megger and designed to measure insulating resistance, the transformer ratio and the knee point of the volt-ampere characteristics for the current transformer, which when switched on boots up a full scale VX Works operating system (a 64-byte real time operating system), is a case in point.

As are the insulation resistance meters produced by the same firm, which underwent evolution from a miniature device with a generator that was turned by a handle into extremely complex microprocessor based assemblies, see Fig. 1.9.

A typical example of the 'explosion of complexity' in electrical power engineering is the Smart Grid. It is well known that the Smart Grid concept presupposes the installation of microprocessors in all the elements without exception of the electrical engineering production, distribution and metering system as well as the establishment

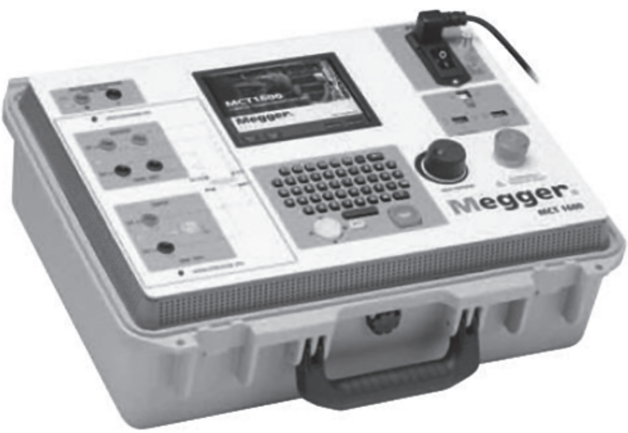
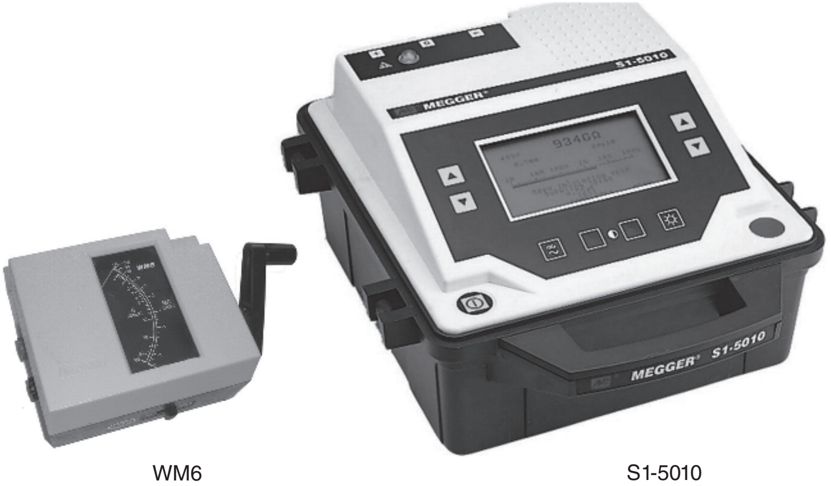


Fig. 1.8 An MCT1600 device produced by Megger to test current transformers.



WM6 S1-5010

Fig. 1.9 Insulation resistance metering equipment produced by Megger: WM6 is the simplest device fitted with a generator and a handle with which to rotate the armature; while the S1-5010 is the most complex microprocessor based device.

of information channels between these elements based on computer networks, predominantly Wi-Fi. The idea of the proponents of Smart Grid was that the energy system of the future should resemble a modern, sophisticated network computer game with thousands of component participants playing a role in the electricity networks. One of the central participants in this 'game' are DPRs with an artificial intelligence and which are self-adaptable, with an indeterministic logic that looks ahead, that is to say it acts independently and at its discretion [1.8].

The affordability and accessibility of microprocessors, industrial control equipment, modern highly integrated electronic components, as well as the huge and ever expanding nomenclature of these components on the market together with the exceptionally high productivity of this equipment, designed for automatic installation and soldering of surface mounting components onto a circuit board and automatic circuit board testing systems – all these remove the restrictions that were once in place on the complexity of electronic systems and their field of application. In connection with this today, microprocessors can be found anywhere. This use of electronic assemblies based on microprocessors, which has expanded with the speed of the Universe in all aspects of technology given their insatiable complexity, is today the defining trend in the development of technology. The proponents of technical progress as we know it today are trying to convince us that technology's unceasing and ever growing complexity is 'technical progress' in itself. Naturally there are some technical and engineering fields that are unable to function without computer operations and microprocessors and microprocessor technology really has made technological leaps forward possible. In far from all cases, however, in which microprocessor technology has been applied have the product specifications provided a reasonable justification and what is more the number of these cases is snowballing and the examples given here are but a poor illustration of this process.

If the growing complexity of technology is often completely unjustified, however, as we have shown previously, then why is technology constantly becoming ever more complicated of itself and moreover at an ever increasing pace? The answer is simple enough: the developers and manufacturers have an interest in technology's growing complexity since it is this constant and determined complication of technology that allows them to achieve certain goals all at once:

- First of all, to raise the effectiveness of their advertising campaigns offering the consumer an ever growing number of new functions in their new products (these are by no means always necessary);
- Secondly to undermine the reliability and service life of their products (which in itself is a natural result of complication), that is to say to force the consumer to purchase a new product more often;
- Thirdly to constantly reduce the serviceability of their manufactured products and to increase the consumer's dependence on the manufacturer. The most modern electronic devices and appliances manufactured using surface mounting technology can only be repaired by replacing entire modules, which are all produced by the same manufacturer.

In many cases the cost of these modules is disproportionately high even though the consumer is forced to purchase them at a clearly inflated price. Thus in many cases the complication of technology has become an artificial process, which often does not change the effective basis initiated by the manufacturer with the aim of further enrichment.

How shameless, however, is this process of technological development?

In the words of Doctor of Technical Sciences and Professor, and head of Central Scientific Research Centre 46 of the Department of Defence of the Russian Federation Major-General V.M. Burenok: a distinguished figure in Russian science [1.9].

> *Technological development conceals within it a multitude of threats, which in terms of their variety and the repercussions of their influence are unpredictable for the fate of civilisation…In the last few years scientific and technological progress has brought the world many technical benefits, but with them a persistent headache. Examples are: computer technology and cyber terrorism, modern*

> *information communication systems and information wars, complex infrastructure and technical asset management systems as well as the serious consequences when they fail, a knowledge of the basis of life as well as genetically modified products, and the advent of the potential for the artificial cultivation of dangerous viruses and so on. Moreover many of these threats that have been generated by new opportunities in technology have not come about straight away and could not have been predicted (either that or those that forecasted them were labelled irrelevant fantasists or eccentrics, that were not worth taking seriously).*

This, however, is what the Academician N.N. Moiseyev wrote on the subject:

> *…scientific and technical progress, and the growth in the power of civilisation does not just bring benefits. The power that this gives people also has to be used wisely. Today man finds himself in Gulliver's position, when he visited the Lilliputian crystal shop. One false move and this whole crystal wonder would turn into a heap of broken glass.*

Knowing that these dangers exist it would most likely be possible to try and prevent them. This, however, is what the distinguished specialist already cited previously had to say on the subject [1.9].

> *Even when the layout of a technical system of some kind has long since been drawn up, but new threats have emerged it seems it is no easy task to predict this situation. Rarely does an analyst for example undertake to predict the consequences of a cyber attack on for example a nuclear power station or a large hydroelectric station's control system or on an air or railway traffic control system. Forecasts such as 'this is going to be awful,' and 'huge and unavoidable losses,' don't suit anyone but assessments such as 'the likelihood of the release of an amount N of radioactive material into the atmosphere will rise to…,' or 'the number of aircraft accidents in airspace with a probability of p will reach the value K' are very hard to make. In order to do this (to make a forecast) a model of the system (or asset) is required, which is almost comparable to the real system, together with a knowledge of how far a hacker's skill has developed, as well as a means of penetrating the system under attack and so on. Firstly, however, this is almost impossible to do, and secondly if this model existed and were to fall into the hands of intruders (hackers) then this makes the chances of the system operating trouble free highly elusive.*

He is supported by the well-known astrophysicist L.M. Gindilis, who wrote in his work [1.10]:

> *The acuteness of the situation lies in the fact that the collapse should come very quickly, in the first few decades of the XXI Century. Therefore, even if humanity were aware of how to 'avert' (or even to stop) this process and had the means and the motive even to turn a corner today – there would still be insufficient time remaining, since all the negative processes possess a certain momentum, which means they cannot be stopped immediately…the global economy is like a heavily*

> *loaded vehicle moving at high speed towards the end of the road, straight to the abyss. Evidently we have already passed the point at which we should have turned to enter a 'turning trajectory'. We won't have time to slow down either. The situation is exacerbated by the fact that nobody knows where the wheel or the brake is. Nevertheless, both the crew and the passengers are very complacent, naively supposing that 'when necessary' they will be able to figure this vehicle out and perform the required manoeuvre.*

In conclusion, we cite the words of the proponent of the theory of technological singularity Vernor Vinge:

> *If 'Technological Singularity' is destined to be, then it will happen. Even if all the nations acknowledge the 'threat' and are scared to death – the progress will not stop. A competitive advantage – be it economic, military, or even in the arts – or any achievement in automation systems would be so overwhelming that a ban on similar technology would merely guarantee that someone else would get there first. I have already expressed my doubt that we will succeed in preventing Singularity, and that its coming is an inevitable consequence of man's natural competitiveness and of the potential inherent in technology.*

The natural (if this term can be used in a technical context) development of technology and engineering was examined previously. There is, though, another side to this problem, which has never been considered in the philosophy of technology. This concerns weapons capable of destroying technology that have developed alongside it. As technology has become more complicated and ever more 'electronic' and 'computerized', so has its vulnerability to intentional remote destructive threats, including cybernetic and electromagnetic threats [1.11]. Therefore, weapons system developers are paying more and more attention to creating new types of weapons aimed at striking technology exclusively, as opposed to humans. This is also a component of 'technical progress', which has been undeservedly excluded from consideration under the philosophy of technology. After all, the sudden destruction of complex electrical systems and the computer networks that branch out from them, and on which modern civilization is founded, could lead to the collapse of that same civilization.

Thus for contemporary society there are not one but two opposing and highly dangerous trends: how uncontrolled development leads to singularity, and the ever growing danger of the sudden and deliberate destruction of this same modern technology using special types of weapons.

1.1 Technical Progress in Relay Protection

Over the course of hundreds of years, electromechanical protective relays (EMPR) have provided solutions to challenges that have arisen in relay protection and, bearing in mind that they comprise around 70–80% of all the protection systems used around the world, then it can be said with some certainty that electromechanical relays today are capable of solving all the challenges facing relay protection. Nevertheless, the last 20–30 years have seen electromechanical relays being replaced universally by Digital

Protective Relays (DPR) and numerous programmable logic controllers (PLC), which control the modes of operation of electrical equipment, have resolutely entered our lives and in many cases it is not possible for electrical power engineering to function properly without them. This is not about certain unique capabilities inherent in microprocessor technology but about the established trend, conditioned by a variety of reasons including bumper profits, obtained through the fully automated production of printed circuit boards (PCB) of DPRs, compared to the production of the previous generation of precision mechanical type relay protection. The search for ways to reduce the production costs and to increase the profitability of production have led to the development of new types of EMPR ceasing some 30–40 years ago and all the efforts of the developers being directed towards the creation to begin with of semiconductor static, and subsequently even microprocessor based digital protective relays (DPR). The first DPR simply copied all the functions and the characteristics of previous generations of relays. New characteristics and scope for DPR only appeared many years later. Therefore, it is doubtful that it can be said that the advent of DPR was conditioned by the actual demand for relay protection. As a result of this technical policy practised by the manufacturers, almost all the world's leading relay protection manufactures completely ceased production of all other types of protection, apart from DPR, and there remained almost no alternative to DPR (one very small exception in this global trend).

The very first examples of DPR, which simply copied the functions of static transistorized semiconductor type relays, see Fig. 1.10, revealed serious problems with the DPR: they would fail on a regular basis and they could not be repaired owing to the presence of a specialized microprocessor and a read only memory (ROM) with a programme written onto it. As a result, if an RXIDF-2H transistorized relay, or one adapted for other discreet components, was repaired relatively quickly and set to work again then their microprocessor analogue: RXIDK-2H would just have been thrown away. As a result, RXIDF-2H DPRs have long since been withdrawn from production, while the RXIDF-2H relays are still in operation. The trend in the reduction of the reliability of relays in connection with the transfer to DPR, that was observed at the very beginning of this process still continues today, despite the fact that the modern generations of DPR have little in common with the very first examples produced several decades ago, see Fig. 1.10. This is testimony to the fact that the problem lies not in the individual technical shortcomings of the early examples of DPR, but is systemic in nature. However, nobody wanted to be known as a retrograde and nobody wanted to talk about the obvious problems that accompanied the introduction of DPR, which had received nothing but a rapturous response. Furthermore, several billions of dollars have been spent on developing ideas and technology linked to the development of DPR over the last few years across the world and the fact that this line of work has become a highly profitable business for thousands of scientists and engineers, and which has fed them over the course of decades, all the discussions concerning the problems and shortcomings of DPR have either nipped a violent rejection in the bud or have had to face one on the part of representatives of the manufacturing enterprises, scientists, developers, project engineers or anyone else involved in this huge business. An attempt by the author in the past to draw attention to the existence of problems with DPRs gave rise to furious allegations of incompetence, of a lack of understanding of the fundamentals of relay protection and even of trying to delay technical progress. In recent years, it is true a realization of the problems with DPR has come about, but this process is reminiscent of an old joke: to

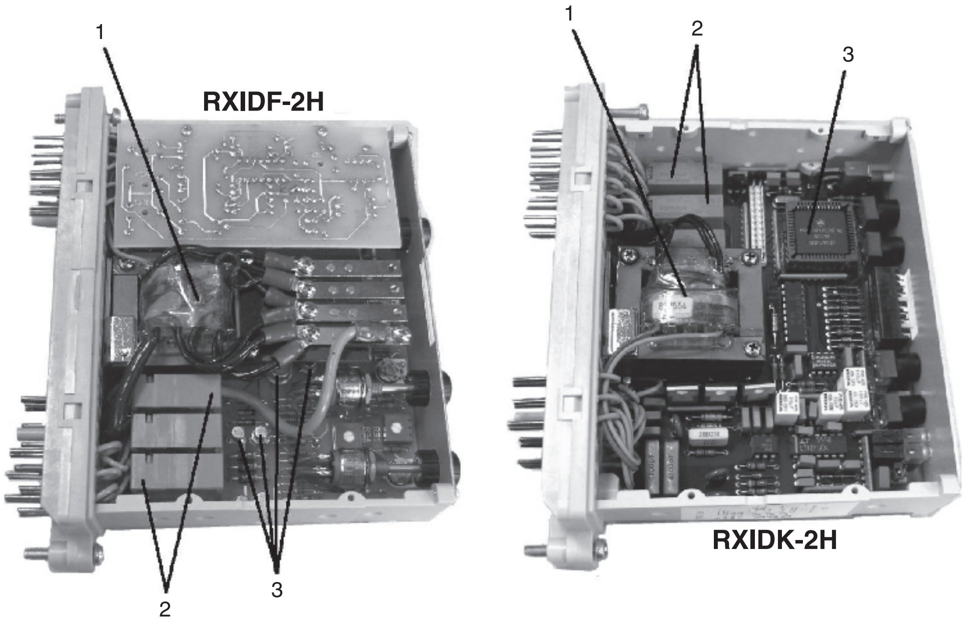


Fig. 1.10 Two dependent time-lag current relays, with identical technical parameters, characteristics, dimensions and manufactured in identical standard COMBIFLEX© casings and produced by the very same company (ABB). On the left is a static semiconductor type RXIDF-2H, while on the right is a microprocessor type RXIDK-2H. 1 – Input current transformer; 2 – electromagnetic output relays and 3 – transistors in a static relay and a specialized microprocessor – in a microprocessor unit.

begin with: ‘this can’t happen because it would never happen’, then ‘there is something in this’ and, finally, ‘could it be any different?’ This is without the middle phrase in this process, however, that it to say without an acknowledgement that the first person to shed light on these problems was right.

Many plagiarists have simply copied whole sections of text from the author’s books and articles and incorporated them into their own articles without adding any links to the source of the information; they report at conferences and even present this work without any alterations at competitions to find the best student dissertations [1.12–1.19].

1.2 Microprocessors – The Basis of the Contemporary Stage of Technical Progress

The affordability and accessibility of microprocessors, industrial sequence controllers and modern electronic components with a high degree of integration, as well as the enormous and ever growing nomenclature of components such as these available on the market, the exceptionally high productivity of equipment designed for automatic installation and soldering of surface mounting elements onto a printed board and automated printed board testing systems – all this removes the barriers that were previously in place to the complexity of electronic systems and the scope of their use. In connection with this today, microprocessors can be found anywhere, up to and including the toilet seat, where they measure the temperature of a corresponding part of the body and set the water heater for the inbuilt shower so that the water temperature matches the temperature of the respective body part. This use of microprocessor based electronic systems, which is growing at speed, in all fields of technology, together with their ever growing complexity is today the defining trend in the development of technology. It has become acceptable to label this trend 'progress' in the development of technology and engineering. Naturally, there are some fields in technology and engineering that that are unable to function without computer operations and microprocessors and microprocessor technology really has made technological leaps forward possible. However, in far from all cases in which microprocessor technology has been applied have the product specifications provided a reasonable justification and, what is more, the number of these cases is snowballing.

Whilst observing this trend not as an onlooker, but as an insider so to speak, that is to say having been involved in the operation and repair of complex electrical devices designed for industrial applications such as relay protection and powerful battery charging equipment, invertors and convertors, as well as uninterruptable power supply (UPS) and so on, doubts creep in about whether the trend described here really represents technical progress. Why? Because the boom that is being observed today that is conditioned by the acute complication of equipment and the ever growing use of microprocessors in all technical fields is not so much linked to actual demand as much as to an intention by the manufacturers to outperform their competitors at any cost, to make something that nobody has made before and to earn bumper profits. In itself, the desire to create something new or to reduce production costs can only be welcomed if the trend in replacing analogue systems that have proved themselves by working faultlessly for dozens of years in discrete electronic components with microprocessors did not lead to the equipment becoming significantly more complex. Also, if it would mean that this equipment would not become unserviceable, or that its reliability would not be reduced and the cost of maintaining it in working order were not so high and it did not require personnel to be so highly trained. When ordering this equipment all these problems remain in the shadows and they are only encountered when the equipment first becomes operational. This is the cost that consumers are forced to pay for so-called 'progress'; that is to say the reckless and irresponsible complication of technology, which is often conducted without any justification and only serves to appease the fashion for technology and to pursue consumers for bumper profits.

1.3 Smart Grid – A Dangerous Vector of 'Technical Progress' in Power Engineering

Today, there is probably not one branch of the media that has not written some kind of rapturous ode in honour of so-called 'Smart Grid', which is touted as the in-thing in technology fashion, bringing us benefits never seen before. Today only the indifferent keep their counsel about their contribution to the development of this new and fashionable direction. It appears that it is not only microprocessor based electricity meters but arc furnace transformers, reactive power compensating equipment and superconducting electrical cables are even electric, as are all elements of a Smart Grid that require money for their production development. Today, targeted state investment programmes are being drawn up and investments running into billions are being allocated. An enormous mechanism is being set in motion to 'draw off' and disperse funds from state budgets for a line of work for which nobody is even able to provide a full, clear and coherent explanation [1.20]. It is common knowledge, however, that the Smart Grid presupposes the installation of microprocessors in all the elements of the production, distribution and metering of electrical power systems without exception, and the establishment of channels of communication based on computer networks, predominantly Wi-Fi. According to the proponents of Smart Grid the energy system of the future should resemble a modern, sophisticated network computer game with thousands of component participants playing a role in the electricity networks. If the millions of domestic electricity meters that have been incorporated into an overall computer network (that is to say millions of potential points of connection for hackers) are added into this then the entire scale as well as the danger of this undertaking, conditioned by a sharp increase in the vulnerability of the electrical power engineering system to attacks by hackers, computer viruses and intentional, destructive remote electromagnetic threats, which are examined in detail later on, becomes even more obvious. An electromagnetic pulse from a high altitude nuclear explosion conducted in near space above the territory of any particular country is today considered an actual variant of a so-called non-lethal weapon, one capable of taking almost the entire microelectronic infrastructure across the entire territory of a country out of action, but sparing the population their lives.

Alas none of these dangers or simply 'horror stories' as they were disdainfully dubbed by some exponents of 'technical progress' in its contemporary sense, are of much concern to scientists and engineers, who are paid from the Smart Grid development funds. Statements such as this are heard frequently: our task is to further technical progress, and any concern for ensuring the security of the nation's electrical power engineering is the prerogative of the Army and of special forces, so let them take this forward. The inferiority of such an ideology is obvious and does not even require an explanation.

1.4 Dangerous Trends in the Development of Relay Protection Equipment

In a series of previous publications, we have drawn attention more than once to the danger of certain trends in the development of relay protection and dismissed as propaganda by microprocessor based protective relay developers and manufacturers. This refers to the following trends:

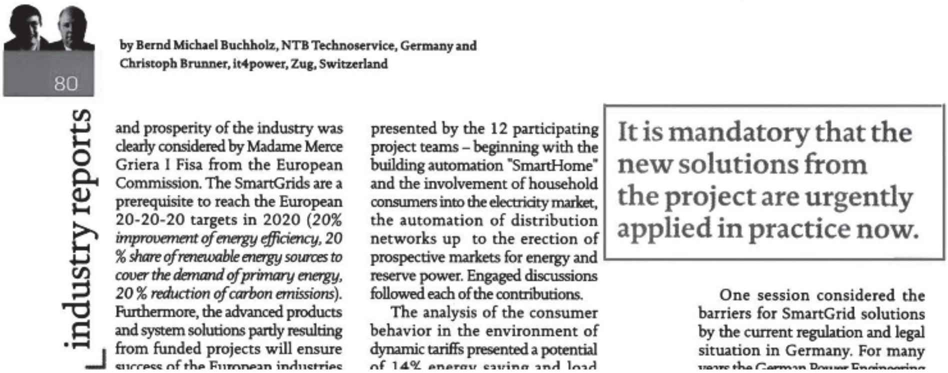
1) The unceasing complication of DPR and an increase in the concentration of protective functions in a single terminal [1.21–1.23].
2) Installing functions onto DPR that do not relate to relay protection such as monitoring electrical equipment, for example [1.24, 1.25].
3) Using indeterministic logic in DPR, as well as so-called 'preventive action', which can give rise to the danger of a loss of control over the relay protection functions [1.24, 1.25].
4) The expanding use of freely programmable logic [1.26] in DPR, accompanied by a significant growth in the ratio of mistakes made by operators and of the protection not functioning properly.

5) Making serviceability checks as well as the operation of relay protection more complicated in general in proportion to the rise in the variety of different types of DPR produced by different manufacturers, which differ both in terms of their design and their software, being used in a single energy system. The lack of standards specifying integrated universal requirements for the design and programming of DPR and increasing the intellectual workload on personnel leads to significant economic losses [1.27]. This situation is compounded every year.
6) A significant weakening in the electromagnetic shielding of protective relays and of the energy system as a whole in proportion with an expansion in the use of DPR [1.28–1.30].
7) An increase in the vulnerability of energy systems to attacks by hackers in proportion with an expansion in the use of microprocessor technology and with the use of cheaper networks such as Ethernet and Wi-Fi in place of comparatively well-protected optoelectronic cables in relay protection systems [1.31].

This complication, both in terms of equipment and programming has come at a price. As references [[1.21–1.22, 1.32–1.35] have shown, the transition to DPR has already led to a significant reduction in the reliability of relay protection. Despite this, however, the proponents of DPR think that it there is no need to stop there, but there is a need to continue to make them more complex, increasing the number of functions carried out by a single terminal; using freely-programmable logic in microprocessor based relay protection; and indeterministic logic based on the theory of neural networks; preventive action algorithms; installing information-measuring systems onto DPR and power equipment monitoring systems; using wireless communication channels (Wi-Fi) between the relays and so on. All these new developments, which are financed by large corporations and often even from the state budget, have turned into a vast business and today nobody wants to be excommunicated from this lucrative 'pie'. The players in this business are not concerned in the least about the future consequences of their activity but they are looking to 'push' their new and fashionable ideas onto the market as soon as possible.

Business is business and its framework acts work differently in different countries and in different fields, including in such a sensitive field as relay protection and control in electrical power engineering. You don't believe this? Then familiarize yourself with the motto of the report on the 'Distribution systems of the future: Novel ICT solutions as the backbone for smart distribution' symposium, published in the journal *PAC World*, see Fig. 1.11. The key words here are 'mandatory' and 'urgent'; that is to say without a careful analysis of the long-term consequences of these innovations and without an unnecessary critique. This was how things were done in countries across the world up until very recently.

After a period of very stormy critical reaction to the authors publications and a complete rejection of the negative consequences of the trends set out here in the development of relay protection, in recent years an understanding has come about of the problems that have been set out before by a number of specialists. For example, B. Morris, R. Moxley and C. Kusch (Schweitzer Engineering Laboratories USA) presented the report: 'Then Versus Now: A Comparison of Total Scheme Complexity' at the Second International Conference 'Contemporary Trends in the Development of Relay Protection Systems and the Automation of Energy Systems' (Moscow, 7–10 September 2009) in



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 success of the European industries 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 of 14% energy saving and load

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 years the German Power Engineering

Fig. 1.11 The motto of one of the publications in a journal that is popular among specialists across the world – *Protection, Automation and Control World* (*PAC World*), September, 2011 (highlighted in a box), reads: 'It is mandatory that the new solutions from the project are urgently applied in practice now.'

which they cast doubt on the need for more and more complexity in protection, arguing their case by using comparative analyses of the reliability of protection based on ever more complicated microprocessor units. V.I. Pulyaev (FGC UES, Russia) also spoke about the poor reliability of DPR at the Third International Conference 'Contemporary Trends in the Development of Relay Protection Systems and the Automation of Energy Systems' (Saint-Petersburg 30 May – 3 June 2011). He noted specifically that a significant proportion of the failures in relay protection occur in microprocessor units (approximately 23% of all cases), which amount overall to around 10% of the total number of protection systems. It goes without saying that this is one of the most important factors that define the need for special measures to be taken to increase the reliability of microprocessor based protection systems. The late Aleksey Shalin (Doctor of Technical Sciences and Professor of the Faculty of Electricity Power Plants at the Novosibirsk State Technical University, and Lead Specialist of the Open Joint Stock Company 'PNP BOLID' in Novosibirsk) wrote openly in his letter responding to one of our publications (see A. Shalin 'Microprocessor Based Relay Protection: The Need for An Analysis of Efficiency and Reliability' in the journal *Electro-technical News*, 2006, No. 2) that the percentage of malfunctions in modern relay protection panels and cabinets often turns out to be significantly higher than for old protection systems based on electromechanical relays, and also that the statistical data confirms the fact of the significant reduction in the effectiveness and reliability during the transition from EMPR to DPR. A. N. Vladimirov (Central Dispatch Administration of Russia's Unified Energy System) also wrote about the reliability problems, as did S. Swain, and D.B. Ghosh (Integrated Electrical Maintenance) among others [1.36].

Stokoe and Gray, in their report 'Development of a Strategy for the Integration of Protection & Control Equipment' at the Seventh International Conference on 'Developments in Power Systems Protection' (Amsterdam, 9–12 April 2001) noted that the old electromechanical relays were durable and long lived systems with a service life of 25 years whereas the service life of modern microprocessor based relays is 15 years or maybe less. They are supported by J. Polimac and A. Rahim (PB Power, United Kingdom) who asserted that the service life of protection systems would decrease from 40 years (for electromechanical systems) to 15–20 years during the transition from electromechanical to microprocessor based relays, and in some cases right down to just a few years following their introduction into service (for microprocessor based systems) [1.36].

The head of the computer division of the Engineering and Technical College at the University of Poona, Maharashtra) Ashok Kumar Tiwari B.E. noted that concentrating a multitude of functions in a single microprocessor terminal reduces the reliability of relay protection sharply, since should this terminal fail a great number of functions would be lost compared to the same scenario if these functions were distributed across several terminals [1.36]. V.A. Yefremov and S.V. Ivanov (of the Engineering Centre 'Bresler') and D.V. Shabanov (FGC UES, Russia) also spoke of the need to limit the number of functions manifested in a single microprocessor based relay protection terminal in their report at the Third International Conference 'Contemporary Trends in the Development of Relay Protection Systems and the Automation of Energy Systems'.

A. Fedosov and E. Pusenkov (who work at a branch of the open Joint Stock Company (SO UES, Siberia) in their article 'Problems arising during the introduction of microprocessor technology in emergency automation' (in the journal *Power Plants*, 2009 No. 12) note the lack of robust, integrated requirements for the material aspects of DPR and their programming. As a result, there is a very high profusion of programmes and algorithms incorporated into DPR, used in a single energy system, leading to problems during operation, and to an increase in the likelihood of the failure of a given device. D. Rayworth and M.A. Rahim (PB Power, UK) [1.36] also wrote about the dramatic rise in the level of complexity in the work of personnel servicing the relay protection during the transfer from electromechanical to DPR, as well as the reasons behind serious accidents involving energy systems. A. Belyaev, V. Shirokov, and A. Yemelyantsev (who work at the Specialized directorate 'Lenorgenergogaz' in St. Petersburg) also wrote about the complexity of the programming interface and the need to introduce an extraordinary number of settings when programming a DPR, in their article: 'Digital Relay Protection and Automation Terminals. The Practice of their Adaptation to Russian Specifications' (in the journal *Electro-technical News*, 2009, No. 5).

Kovalev B.I., Naumkin I.E. (the Siberian Scientific-Research Institute of Power Engineering); Bordachev A.M., (of the Open joint Stock Company 'Institut Energoset'proyekt'); M. Matveyev and M. Kuznetsov (of the Joint Stock Company 'EZOP'); R. Montignies, B. Jover (Schneider Electric, France); V. Nadein ('Arkhenergo'), V. Lopukhov (Sate Unitary Enterprise 'PEO Tatenergo'); A. Yermishkin (of the Joint Stock Company 'Mosenergo'); R. Borisov (of the Research and Production Company 'ELNA' based in Moscow); A.W. Sowa, J. Wiater (Electrical Department, Bialystok Technical University, Poland) and other specialists also noted the unsatisfactory condition of the electromagnetic environment at the majority of the old substations that were designed and built for electromechanical and not DPR, and the failures that occurred in the operation of DPR as a result. Many of them noted the sensitivity to electromagnetic interference in protective relays on a microprocessor element base was higher by several orders of magnitude than on traditional electromechanical analogues and as such in order to ensure the electromagnetic compatibility (EMC) of secondary circuits the level of electromagnetic protection in these relays needs to be increased dramatically. Without a package of work being carried out to ensure EMC it would be impossible to achieve acceptable reliability levels in DPR.

Closely linked to the lack of stability found in DPR in relation to EMC is another more complex and serious problem with respect to intentional remote destructive electromagnetic threats to DPR, which we first brought to the attention of specialists in [1.36]. Today in many countries across the world equipment has already been developed that is capable of taking industrial microprocessor systems of any kind out of action (which naturally includes DPR). Therefore, not only are many publications in technical journals written by well-known specialists such as Manuel. W. Wik (Defence Materiel Administration, Sweden) and William A. Radasky (of the Metatech Corporation, USA) devoted to this topic, but also reports produced by special commissions under the US Congress (see the 'Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse Attack', 2008, for example).

Another new problem, which was previously unknown in relay protection is the problem of the cyber vulnerability of DPR (and consequently in the energy system as a whole) to attacks from hackers. Paralysis of the control system and the large-scale disconnection of entire energy systems, chaos in the monitoring system, as well as the disconnection of the Internet and the mobile communications network – according to American proponents these are the likely consequences of a cyber-attack. Moreover, considering the strategic importance of a target like an energy system it would not be lone hackers that would embark on an attack like this but entire military cyber divisions, which have already been set up in many countries around the world. Just last year a separate Cyber division was founded under the National Security Agency (NSA) in the USA, one of the most powerful and highly classified of the world's secret services, and led by General K. Alexander, which brought together all the Pentagon's cyber protection divisions that existed at the time. Some of them will be ensuring the security of not only of the military and state infrastructure, but also the country's most important commercial assets. Understandably a structure of this magnitude will not only be engaged in defending the country from cyber-attacks but will actually develop attacks of its own (the best defence is offence). The head of Cyber Command and the Director of NSA General K. Alexander announced at Congressional Armed Services Committee hearings that cyber warfare has an effect comparable to the use of a weapon of mass destruction. Cyber warfare is developing at great speed. Many countries such as the USA, Russia, China, Israel, UK, Pakistan, India, North and South Korea have developed complex cyber weaponry, which specialists in cybernetics assert are capable of penetrating computer networks more than once and destroying them. In 2010 the cyber budget of the United States was $8 000 000 000 and in the future this is only set to rise. In 2011 the USA is preparing to set a new doctrine on cyber warfare. The direction of this doctrine can be judged by a programme article published in September and written by the Deputy Head of the Pentagon William Lynne III with the symbolic title of 'Defending a New Space'. The basic premise is that from now on the USA will consider cyberspace as potential a battlefield as land, sea and air. Parallel to this NATO began work to create a concept of collective cyber defence. At an alliance summit held in November 2010 it was decided to develop a 'Plan of action in the field of cyber defence'. This document was to have been published by April 2011 but was signed in June. A great deal of emphasis in this document is placed on the creation of a NATO centre to react to cyber incidents. Initially this was due to be launched in 2015 but on the insistence of the United States the deadline was brought forward by three years. The effectiveness of cyber weaponry can be judged by the widely publicized cyber-attack on the Iranian uranium enrichment centre at Natanz with the help of a Win32/Stuxnet computer worm that destroyed hundreds of centrifuges. A further large-scale attack on the Japanese corporation Mitsubishi Heavy Industries, that produces F-15 aircraft, Patriot anti-aircraft missile systems, submarines, surface ships, rocket engines, ballistic missile guidance and interception systems and other military technology occurred in September 2011.

The corporation's computer equipment (45 closed servers and around 50 personal computers) turned out to be infected with a whole range of viruses that had taken control of them completely. This meant that the computers could be controlled remotely and the information on them could be transferred. There were viruses that enabled built in microphones in the computers as well as cameras to be activated. This enabled the plotters to follow what was happening inside the production and research facilities remotely. Some of the viruses erased the traces of the breach, which made any assessment of the scale of the damage much more difficult. Information on the computers that had been taken over was downloaded onto 14 different sites abroad including in China, Hong Kong, the USA and India.

Modern technology enables viruses to be launched into a computer system remotely in the form of enciphered radio waves with the help of pilotless airborne repeater equipment. Wireless Wi-Fi systems, which it is envisaged Smart Grid systems will be based on, are especially vulnerable to these external attacks. DPR manufactured by leading Western manufacturers are already being fitted with built in modems for Wi-Fi.

In the past several attempts were recorded by Iran to penetrate the Israeli energy system. The Senior Analyst of the United States' Central Intelligence Agency (CIA) Tom Donahue announced at a meeting of government officials and employees of American companies that possessed electrical, water, petroleum, and gas distribution systems, of several attempts known to the CIA to penetrate America's energy systems.

It is very obvious that the trends described here will only increase in proportion with the development of this technology, if the following steps to stop these trends are not taken:

1) In the field of the reliability of relay protection:
   - 1.1. The Introduction of qualified methods of calculating the reliability of DPR [1.37] and a new indicator of their reliability [1.38] that is convenient and practical, and which enables the consumer to submit a complaint to the manufacturer, in place of the current and less than informative indicator 'mean time between failures' (MTBF).
   - 1.2. Limiting and optimising the number of functions in a single DPR module [1.39, 1.40].
   - 1.3. A rejection of the use of non-deterministic logic in DPR [1.24, 1.25, 1.41].
   - 1.4. A considerable restriction on the use of freely programmable logic in DPR – this is a source of human error and of a large number of failures in protective relays [1.24, 1.25, 1.41].
   - 1.5. The introduction of a ban on using DPR for purposes that do not bear any relation to relay protection, such as monitoring the condition of electrical equipment or for so-called 'protection through preventative action'. [1.24, 1.25, 1.41].
   - 1.6. A rejection of the use of wireless network technology in protective relays.
   - 1.7. Forcing DPR manufacturers by law to be concerned with the cyber security of their products and their resilience to intentional destructive electromagnetic threats. This is why standards need to be drawn up and special sections introduced into the technical documentation for DPR, which should reflect the safeguards, and the level of protection in a specific DPR from the attacks

indicated previously, together with its compliance with established standards. Gradual restrictions and then subsequently a complete ban should be introduced on the use of DPR in electrical power engineering that do not conform to the requirements for protection from the threats listed here.

1.8. Publish special bulletins for engineering companies that are engaged in the design of protective relay systems, providing a detailed description of the dangers facing protective relays today, as well as possible preventative measures to protect against them [1.11]. The gradual introduction into design practice of established standards and safeguards initially in newly introduced, and subsequently in existing power systems.

1.9. To assign the development of specific programming and equipment safeguards against the threats listed here to the leading scientific organizations as well as the testing, organization of operational trials and subsequent manufacture of already established, and at the same time inexpensive, equipment safeguards proposed in [1.11, 1.42, 1.43].

2) In the field of the standardization of relay protection:

2.1. Introduce into normative and technical documentation unified definitions for the most important notions in relay protection, such as those proposed in [1.44], for example.

2.2. Develop general technical requirements for microprocessor based protective and automation devices for power systems based on international standards and publish a new document, that uses, for example, the requirements set out in [1.44] as a basis.

2.3. Unify the design as well as the basic software shell for different makes and models of DPR, for which it would be necessary to draw up a set of standards with integrated technical specifications for the design of the functional modules of a DPR, and for the internal communication protocols between them, as well as the basic user software shell.

2.4. Standardize the testing of DPR using modern programmable protective relay testing systems alongside ready-made programming module packages [1.44].

In our opinion, these measures are capable of halting the further development of dangerous trends in the DPR field, and will support a significant increase in the reliability of relay protection, and its resilience to intentional electromagnetic destructive threats as well as reducing running costs.

References

1.1 Popkova N.V. The Philosophy of Technology - the Internet-portal of the Bryansk branch of the Russian Philosophical Society (http://sphil.iipo.tu-bryansk.ru/)

1.2 Vinge V. The coming technological singularity: How to survive in the post-human era. *NASA*. Lewis Research Center, Vision 21: Interdisciplinary Science and Engineering in the Era of Cyberspace pp. 11–22 (SEE N94–27358 07–12), 12/1993.

1.3 Moore G.E. Cramming more components onto integrated circuits - *Electronics*, 19 April, 1965, pp. 114–117.

1.4 Sukharev M. An explosion of complexity - *Computerra*, No. 43, 3 November 1988 (http://offline.computerra.ru/1998/271/1828/).

1.5 Negodayev I.A. The Philosophy of Technology: A textbook/DGTU (textbook)/Rostov on/D, 1998, 319 pp.

1.6 Lopota V.A., Yurevich E.I. Unified mechatronic microsystem modules - the foundation of the intellectual technology of the future - *Artificial Intelligence*, 2002, No. 3, pp. 303–304.

1.7 Bezmenov A.E. *Tolerances, Settings and Technical Metrology. A Textbook for Technical Colleges*. Moskva Mashinostroyenie 1969 322 pp.

1.8 Gurevich V.I. DPR. Equipment, problems, prospects. - M.: *Infra-Inzheneriya*, 2011. - 336 pp.

1.9 Burenok V.M. How can Russia's defensive capabilities be guaranteed in the future? - *The Military Industrial Courier*, No. 39 (507), 9 October 2013.

1.10 Gindiles L.M. Models of civilisations in the SETI problem - *Social Sciences and the Modern World*, 2000, No. 1. pp. 115–123.

1.11 Gurevich V.I. The vulnerabilities of DPR: problems and solutions - M.: *Infra-Inzheneriya*, 2014. 256 pp.

1.12 Grishchuk Yu.S. Timoshenko R.F. An analysis of the reliability of DPR. A Collection of essays 'The NTU Herald': The Problem of Improving Electrical Machinery and Apparatus, No. 16, - *The NTU Herald*, 2010.

1.13 Vnukov A.A. The practice of introducing microprocessor terminals in the modern context - *Electro and Electrical Technology, Electrical Power Engineering, Electro-technical Industry*, 2008, No. 1, pp. 40–41.

1.14 Sapa V.Yu. Electromagnetic compatibility in contemporary electrical power engineering - *Material from the Conference on 'The Achievements of the Higher School. The Technical Sciences'* (the A. Baytursynov Kostanay State University), Kazakhstan, 2011.

1.15 Arynov A.K., Yunus M.E. a comparative analysis of digital protective relays - K.I Satpayev *Kazakh State University Herald*, 2011, No. 83.

1.16 Lint M.G. Mathison V.A., Mikhaylov, A.V. The current state of electro-mechanical protective relay systems and their prospects - *Relay Protection and Automation*, 2013, No. 2, pp. 38–40.

1.17 Kolesnik S.P. The strategic direction of an equipment manufacturer producing power engineering and relay equipment - Abstracts from a Seminar Entitled 'Relay Protection Equipment and Automation, 2013', No. 2, pp. 38–40.

1.18 Grebennikov M. Defining the right path - Russia's Power Engineering and Industry, No. 18 (134) September 2009.

1.19 Iov A.A. and Iov I.A. The reliability of DPR: Myths and Reality - The section entitled 'The Supply of Electrical Power and Electrical Equipment Control Systems in the Mining Industry.' *The All-Russian Scientific and Practical Conference 'The Innovative Development of the Mining and Metallurgical Sector' Irkutsk State Technical University*, Irkutsk 1–2 December 2009.

1.20 Gurevich V.I. Intellectual networks: New prospects or new problems? *The Electro-technical Market*, 2010, No. 6 (part 1); 2011, No 1 (part 2).

1.21 Gurevich V.I. The reliability of DPR: Myths and reality - *Problems in Electrical Power Engineering*, 2008, No. 5–6, pp. 47–62.

1.22 Gurevich V.I. Further thoughts on the reliability of DPR - *Problems in Electrical Power Engineering*, 2009 No. 3 (29), pp. 40–45.

1.23 Gurevich V.I. Is relay protection safe from the point of view of energy security? - *Energy Security and Energy Saving*, 2010, No. 2, pp. 6–8.

1.24 Gurevich V.I. ‘The intellectualisation’ of relay protection: Good intentions or the road to Hell? - *Electrical Networks and Systems*, 2010, No. 5, pp. 63–67.

1.25 Gurevich V.I. Sensational discoveries in the field of relay protection - *Russia’s Power Engineering and Industry*, 2009, No. 23–24, p. 60.

1.26 Gurevich V.I. Logic in free flight - *PRO Electricity*, 2008, No. 1 (25), pp. 28–31.

1.27 Gurevich V.I. Testing DPR - *PRO Electricity*, 2011, No. 2, pp. 28–31.

1.28 Gurevich V.I. Electro-magnetic terrorism - The new reality of the 21st century - *The World of Technology and Engineering*, 2005, No. 12, pp. 14–15.

1.29 Gurevich V.I. The problem of the electromagnetic impact on DPR - *Components and Technology*, 2010, No. 2, pp. 60–64; No. 3, pp. 91–96; No. 4, pp. 46–51.

1.30 Gurevich V.I. The problem of the resilience of DPR and automated systems to intentional destructive electromagnetic threats - *Components and Technology*, 2011, No. 4 (part 1); 2011, No. 5 (part 2).

1.31 Gurevich V.I. The use of cyber weapons against power engineering - *PRO Electricity*, 2011, No. 1, pp. 26–29.

1.32 Gurevich V.I. DPR: New prospects or new problems? - *Electro-technical News*, 2005, No. 6 (36), pp. 26–29.

1.33 Gurevich V.I. On several evaluations of the efficiency and reliability of DPR - *The Electrical Power Engineering News*, 2009, No. 5, pp. 29–32.

1.34 Gurevich V.I. Current problems in relay protection: An alternative view - *The Electro-technical News*, 2010, No. 3, pp. 30–43.

1.35 Gurevich V.I. Criteria for assessing relay protection - Is it worth complicating the situation? - *The Electro-technical News*, 2009, No. 6, pp. 45–48.

1.36 Problems with DPR [in Russian] – Available online at http://digital-relay-problems.tripod.com (accessed August, 2016).

1.37 Gurevich V.I. Problems in assessing the reliability of relay protection - *Electricity*, 2011, No. 2, pp. 28–31.

1.38 Gurevich V.I. New criteria are needed to assess the reliability of DPR - *The Electro-technical Market*, 2011, No. 6, pp. 70–74.

1.39 Gurevich V.I. Current problems of standardisation in the field of relay protection - *The Electro-technical News*, 2012, No. 6, pp. 28–38.

1.40 Gurevich V.I. On the multifunctional protective relay - *PRO Electricity*, 2012, No. 42–43, pp. 45–48.

1.41 Gurevich V.I. Surrealism in relay protection - *EnergoStyle*, 2010, No. 1, pp. 5–7.

1.42 Gurevich V.I. Is protection for relay protection necessary? - *Electrical Energy. Transfer and Distribution*, 2013, No. 2, pp. 94–97.

1.43 Gurevich V.I. Protective relay protection equipment - *Components and Technology*, 2013, No. 5.

1.44 Gurevich V.I. *Problems of Standardisation in Relay Protection*. SPB.: The Publishing House DEAN, 2015, -168 pp.