Sophistication of relay protection: good intentions or the road to hell?

by Dr. Vladimir Gurevich, Israel Electric

There was an interesting story in an old science fiction novel. It all started from an innocent thing such as an odd night call to all the phones on planet Earth. The call announced the birth of global intelligence to all people of the Earth.

It turned out that at some stage of development, the proliferation of computers escalated into a new entity: millions of computers, integrated into a single network that controlled everything and everyone on the planet Earth, suddenly became conscious of themselves as a an entity capable of reproducing itself through the automated factories and robots connected to the same network, as well as of defending itself with computerised weapon systems designed to destroy the human race. From the perspective of global intelligence, humanity was nothing but a useless vestige, gobbling up the planet's resources. There are no prizes for guessing about the further development of the action.

Network connected computers already control almost all types of modern industrial production systems, water supply and electricity systems, telecommunications systems and networks. New terms such as smart grid and relay protection with artificial intelligence have emerged in technical literature rather than in science fiction. Today technical literature rather than science fiction refers to the creation of the so-called smart house, where even the refrigerator will analyse the stored products, and, based on the analysis of consumption, will make an order and send it over the network to the nearest supermarket. Today you can find microprocessors everywhere, even the water closet lid [1].

Humanity is moving by leaps and bounds to the creation of all-powerful global intelligence prophesised in the old science-fiction novel. But let's get back to reality.

Reality

And the reality is that major failures in the energy systems that have occurred in America and Europe (USA: 1965, 1977, 2003; France: 1978 Canada: 1982, 2003; Italy: 2003, London: 2003, Sweden: 1983, 2003) were caused by incorrect, or rather, unpredictable actions of relay protection during complex emergency modes due to disabling the wrong sectors of the network. Had the action of relay protection under these specific circumstances been different, the system failures might have been avoided. I am referring to the power systems (USA and Western Europe) that have already been equipped with computers and microprocessor-based protection. For comparison, I should mention that one of the world's largest power systems with a negligible percentage of computerised relay protection devices and the old worn-out equipment has never suffered from such failures. I am referring to the power system of Russia. The answer to the question about the reasons for this can be found in the book of E M Schneerson, and foremost authority in the field of modern relay protection: *"Improvement of the technical level of relay protection devices (RPD) alone does not necessarily lead to the equivalent improvement of efficiency as related to the response to emerging damages. For example, outdated electromechanical and to an extent electronic static RPD, if protection functions and settings are chosen correctly, certainly provides better protection for the network than the microprocessor RPD without rational definitions of the specified parameters"* [2].

In fact, the behavior of electromechanical and electro-static RPD under emergency situations was rigidly determined by their operating principle and settings. Current trends [2-7] in the development of digital protective relays (DPR) are associated with the increase of their "independence" (that is, in fact, unpredictability) in making decisions. It relates to the relay protection self-learning capability peculiar to adaptive neural networks, as well as the use of technologies of artificial intelligence with fuzzy logic, etc.

Complexity

Another clear trend in the development of the modern DPR is the excessive complexity by including extraneous functions not typical for relay protection. Here, for example, the list of functions performed by the a typical "intelligent controller".

IEEE protective functions:

- Sync check
- Under voltage
- Directional power
- Phase balance
- Instantaneous over current
- Inverse time over current
- Over voltage
- Voltage balance
- Directional
- Reclosing
- Under and over frequency
- Lockout
- Differential for transformer protection

Measurement functions:

- Voltage and current RMS values
- Neutral current RMS values
- Power factor measurement (Power factor correction: Capacitor bank switching)
- Total power measurement
- Real and reactive power measurement
- Power quality measurement (FFT for harmonic measurement)
- Frequency measurement
- Total harmonic distortion measurement

Advanced features for protections:

- Coil monitoring for relay failure detection.
- Cold load pickup logic to prevent protective devices from operating when cold load is put on the circuit.
- Voltage constraint with current pickup lowered to increase sensitivity when voltage is also collapsing during the fault.
- Breaker control blocking for coordination with upstream and downstream protective devices via DI or Peer-to-peer communication.
- Directional on over current devices

Add to this the monitoring of external current and voltage circuits, the registration of events, functions of emergency digital oscilloscope, and other routine functions of the DPR.

Then there is the danger of excessive concentration of protective functions in a single terminal, additional relay protection functions, extrinsic to the protection itself, not only lead to the physical complication of the device, consequently reducing its reliability, but also to the complication of its software and user interface. This in its turn leads to a sharp increase in the number

of software errors ("human factors"). Due to such large number of functions, using the same internal resources of DPR and possible conflicts of the embedded logic functions during complex emergency mode accompanied by a transition of one type of damage to another, it is not always possible to predict the behavior of the protection. Damage to one function that is common to all the internal element DPR functions (power supply, watchdog, memory, microprocessor, or its servicing subassemblies, etc.) will result in the instant failure of all protective functions at once.

Despite the obvious problems existing today due to the excessive concentration of protective functions in a single terminal, some leading experts in their philosophizing about the future of relay protection not only advocate additional "adding on" of extraneous functions to relay protection, but even go further.

They put forward the idea of "multi-dimensional relay protection" [6] and "relay protection with proactive functions" [8], acting on the basis of its own experience, its own analysis of the current status of the protected object and prediction of its future state. In essence, this is about the relay protection capability taking completely unpredictable actions, as an independent intelligence making its own (previously not determined) solutions and changing power systems operating modes (through switches) at its own discretion before the emergency mode occurs [9].

It must be emphasised that there is nothing wrong with the development of computer-based diagnostic and prediction methods for electrical equipment, and it could only be welcomed but for the attempts to "intercross" it with the protection relay.

Vulnerability

Apart from the risk of losing control over the relay protection actions, current trends of its development dramatically increase the risk of hacker attacks on the grid as a computerised relay protection system is a good target for changing the state and affecting the modes of power systems. Despite the serious concern of specialists about this problem [10, 11], the trend towards greater susceptibility of power systems to hacker attacks grows.

Another serious threat to the stability of power systems, which is based on current trends in its development, is the development of technologies of artificially produced destructive impacts on electronic and computer equipment [12-18]. The development of these technologies throughout the world contributes to increasing the spread of microprocessor technology and memory elements with high sensitivity to external electromagnetic emission on the one hand, and the tendency of constantly increasing the density of microelectronic components as a result of the reduction of the thickness of the operating and the insulating layers in the crystals, on the other hand. These two tendencies, directed toward each other, form a very dangerous vector of development of modern technologies. Moreover, today, you do not need any special knowledge or equipment in order to create a device capable of destroying all the electronic devices of your neighbour. You can find numerous descriptions on the Internet of such devices based on common microwave ovens, (see Fig. 1) [18].

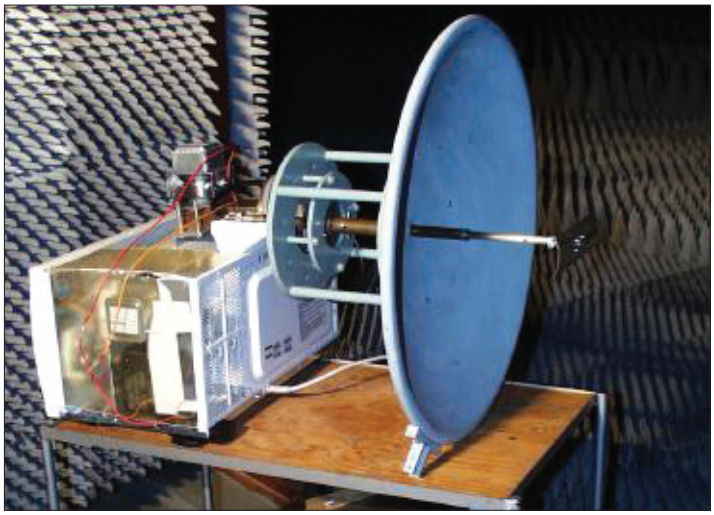

Fig. 1: Electromagnetic weapons based on household microwave oven.

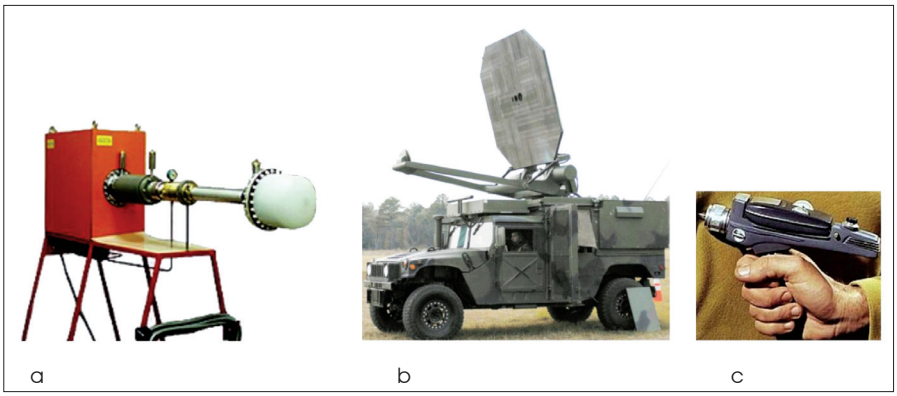

Fig. 2 (a): Super-power ultra-broadband pulse oscillator of directed super-high-frequency electromagnetic emission with output power up to 1000 MW;
Fig 2 (b): A powerful microwave generator mounted on a car;
Fig 2 (c): Hand emitter of powerful electromagnetic pulses, developed by Raytheon.

As for the special "combat" units, there have been very impressive achievements in this field, (Fig. 2). Compact mobile ultra-broadband pulse generators with a capacity of one billion W, portable emitters in the form of pistols and rifles, explosive devices in the form of attaché cases destroying all the electronics within a radius of many hundred meters, special ammunition, and other weapon designed specifically for remote destruction of electronic equipment.

Possible solutions

So, where are we going and to where will we come? Why do the current trends go unnoticed by specialists? Obviously, there is a lot of support for this trend to continue. However, in our opinion, it is not a question of whom to blame, but the question of what to do.

In contrast to isolated measuring and monitoring computer systems, the protective relay is associated directly with the possibility of destructive impact on power system modes. This is the most important and fundamental difference of relay protection from all the other computerised devices and systems used in electric power engineering, preconditioning a need for a different approach to relay protection.

The above thesis, in our opinion, is the answer to this question. What's needed is a different approach in maximising the reliability of relay protection and avoiding features unrelated to relay protection, limiting the number of functions in a single microprocessor terminal, avoiding algorithms with non-deterministic logic allowing the unpredictable action of relay protection, the maximum simplification of the user interface, conducting special research and development providing for the operation of relay protection against intentional destructive electromagnetic

influences, for example, by introducing stand-by emergency relay protection sets. Only electromechanical relays resistant to intentional electromagnetic influences, requiring no live power, and thus being always ready to work can be used as such stand-by RP sets. Therefore, in our opinion, it is too early to dismiss the electromechanical relays. Rather, they should be improved through the new technologies and materials and their range should be updated.

Since the relay protection algorithms are not so complicated (all of them were effectively realised with electromechanical devices which now account for over 90% of all protective relays in Russia), the current protection devices can be as simple as possible. There have been no new functions introduced in the relay protection by DPR, but only some relay protection characteristics were improved. In particular distance protection received polygonal characteristics instead of the circular ones of old electromechanical relays. Therefore in reality there are no objective reasons for today's substantial complication of the relay protection functions.

On the other hand, recently more and more complicated and sophisticated systems for monitoring electrical equipment modes based on the continuous monitoring of the electrical characteristics (tangent of dielectric loss angle, partial discharges in insulation, arrester leakage current, the number and composition of gases dissolved in transformer oil, etc.) have emerged with the ability of predicting the processes progress in time. Automatic process control systems have become more complicated as well as real-time control systems for measuring vector values of current, voltage and power, the systems for registration and oscillographic testing of emergency operation, etc. In contrast to the relay protection all these systems don't have direct influence on the operating mode of power systems and therefore there are no restrictions on the trends of their development.

In our opinion, the only purpose of relay protection should be the relay protection itself (i.e. identification of emergency modes and issuing instructions to the electrical devices changing the operating mode of the protected object in order to exit the emergency mode) and no more. All other problems should be solved by other systems independent of the relay protection. Therefore, further development of microprocessor relay protection and other microprocessor and computer systems in power engineering should take place in independent unrelated parallel courses.

In order to prevent the arbitrariness of manufacturers imposing more and more "advanced" and less reliable DPRs [19,20] to the energy sector, it is necessary, in our opinion, to formulate the basic requirements for the MPD design principles (not for the technical parameters, but for the principles of design) in the relevant standard. The same principles could also include earlier proposals [21] on DPR design as of a set of individual replaceable modules universal in functions, sizes and contact connections (PCBs) by analogy with personal computers.

References

[1] V I Gurevich: "Cost of the progress" – *Components and Technologies,* 2009, N 8.

[2] E M Shneerson : "Digital relay protection." *M Energoatomizdat* 2007.

[3] A Bittencourt, M R de Carvalho, J G Rolim: "Adaptive strategies in power systems protection using artificial intelligence techniques," *The 15th International Conference on Intelligent System Applications to Power Systems,* Curitiba, Brazil November 8 – 12, 2009.

[4] M A Laughton: "Artificial intelligence techniques in power systems", *Artificial intelligence techniques in power systems*, The Institution of Engineering and Technology, 1997, p. 1–18.

[5] R Khosla, T Dillion: "Neuro-expert system applications in power systems" *Artificial intelligence techniques in power systems*, The Institution of Engineering and Technology, 1997, 238 – 258.

[6] U Y Lyamets, D V Kerzhaev, G S Nudelman, U V Romanov: "Multidimensional Relay Protection", *Abstracts of the second International Scientific-Technical Conference on Modern Trends in Development of Power System Protection and Automation,* Moscow September 7-10, 2009.

[7] T S Kamel, M A Hassan, A El-Morshedi, "Application of artificial intelligence in the remote power line protection", *Abstracts of the Second International Scientific Technical Conference on Modern Trends in Development of Power System Relay Protection and Automation,* Moscow September 7-10, 2009.

[8] A Bulychev, G Nudelman: "Relay protection improvement through proactive functions", *News of Electrotechnics,* No. 4 (58), 2009.

[9] V I Gurevich: "Sensational discovery in relay protection", *Energy and industry of Russia,* No. 23-24 (139-140), December 2009.

[10] CIA: "Hacking electrical grids is possible", CNews.ru: Newsline. *24.01.2008,* (www.cnews.ru/news/line/index.shtml?2008/01/24/285018)

[11] V I Gurevich: "Electromagnetic terrorism, The new reality of the 21st century", *The World of Technics and Technologies,* 2005, N 12, c. 14 – 15.

[12] D Daamen: "Avant-garde terrorism", *Intentional Electro Magnetic Interference*, 2002, 23 p.

[13] Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack (www.empcommission.org/docs/empc_exec_rpt.pdf).

[14] A Gannota; "The object of defeat: electronics", *Independent military review.* 2001. № 13.

[15] V Loborev, U Parfionov, V Fortov: "Collapses of noiseless explosion" *Literary Gazette,* N 5 (5865), February 6 -12, 2002.

[16] V Pokrovsky: "Electromagnetic factor", *Independent Gazette*, October 08, 2003.

[17] M Bäckström: "Is intentional EMI a threat against the civilian society?", *SAAB Communication,* 2006.

[18] V Gurevich: "Reliability of microprocessor-based relay protection devices – myths and reality", *EngineerIT*, Part I: 2008, N 5, p. 55 – 59; Part II: 2008, N 7, pp. 56 – 60.

[19] V I Gurevich: "Reliability of microprocessor-based protective devices revisited", *Journal of Electrical Engineering,* Vol. 60, No. 5, 2009.

[20] V I Gurevich: "Microprocessor protective relays: Searching for optimality", *Energy and Industry of Russia*, No. 21 (137), November 2009.

[21] V I Gurevich: "Digital protective relays: It is more questions than answers", *Energetika and TEK*, 2009, N 12, pp. 12 – 16.

Contact Dr. Vladimir Gurevich,
Israel Electric, vladimir.gurevich@gmx.net ❖