Protecting power systems from destructive electromagnetic fields

by Vladimir Gurevich, Israel Electric

Modern power systems can be badly affected by intentional destructive electromagnetic impacts (IDEI) and need to be protected from the risks associated with this form of attack. These days, a power system can be made virtually immune to IDEI as a result of new standards, the availability of modern relay protection and automation devices, as well as improved certification and testing procedures.

The problem of intentional destructive electromagnetic impacts (IDEI) on electronic military equipment became apparent a few years after the USA conducted a series of nuclear test explosions coded "Operation Crossroads" on Bikini Atoll in the Marshall Islands (3800 km south-west of Hawaii) in 1946. During those test explosions a new physical phenomenon was discovered: the emergence of a powerful impulse of electromagnetic emission, encompassing an extensive area, which immediately caught the attention of military men.

From 1958 until 1962 both the USA and the Soviet Union conducted a series of high burst tests (40 to 450 km) in order to investigate this phenomenon. It was revealed that the High Altitude Electromagnetic Pulse (HEMP) can destroy electronic equipment, communication systems, radio-stations and radar from a distance of thousands kilometers from the centre of the explosion. At that time information about this phenomenon was kept quiet. Recently, however, it has become known that since the 1980s several countries started to put their efforts into the development of a so-called "super-EMP" nuclear weapon, where the EMP (electro-magnetic pulse) effect is significantly magnified compared to an ordinary nuclear weapon.

Simultaneously, several countries started developing extra-power directional non-nuclear EMP sources as well as electromagnetic bombs, missile reentry vehicles, grenades and other ammunition, which are non-nuclear EMP sources intended to destroy the electronic equipment found at extremely important infrastructure facilities, including communication systems, water and energy supply infrastructure. Powerful portable EMP sources have recently become available on the market. Although these portable devices may not pose a threat of warfare between conflicting countries, they could become implements used by criminal and terrorist organisations.

As the work in this area advanced, information about it became available to the public via various media channels [1-4]. My book, and articles I have written on the topic, pioneered an interest in IDEI in the design of relay protection systems for electrical infrastructure [5-7].

Today, the importance of the IDEI problem in electric power systems is officially recognised all over the world. For example, in the USA there is a special commission of Congress overseeing several large governmental organisations which have been established to investigate solutions to this problem; many private companies offer consultation services in this area, and test equipment and methods of protection have been developed.

Solutions to the problem

The risks to electrical infrastructure can be minimised by considering how military electronic instruments are protected from IDEI. Unfortunately, civil infrastructures cannot be built using the principles of military construction. The reasons for this are obvious from an economical standpoint. So, what do we need to do? Analysis of the situation shows that the problem of protecting a country's power system is comprehensive and cannot be solved by power engineers solely. A country should establish a national programme which is aimed at improving a power system's durability, which would include many participants. Apart from power engineers it should include developers and producers of electronic equipment for the power industry, testing and certifying centres, designers and standardisation organisations.

The electric power industry's contribution

A national programme could start with the selection of the most important power system facilities – those which require protection from the start. These include nodal substations of the most important power plants.

Then, critical types of equipment should be determined at selected facilities, which are the most susceptible to IDEI on the one hand and on the other hand those which are vital for the selected facility of the power industry. For example, digital protection relays, battery chargers of auxiliary DC power systems, and substation control systems.

It is necessary to provide standby sets of critical equipment at selected facilities and to ensure that any electronic module or printed circuit board (PCB), which includes sensitive electronic parts in its design should be taken out. These modules and PCBs should be stored in specially sealed steel containers, which will protect the highly sensitive components, such as memory elements and microprocessors, from the damage which would result from a high-frequency high-strength electromagnetic field. It is not enough, however, to store just a set of spare electronic modules. If electrical equipment, such as a battery charger, is operating under voltage, the IDEI will most likely damage not only the highly sensitive electronic components, but also such assemblies as power transformers, filter capacitors, internal harness of wires and cables, automatic switches, etc. At the same time, if the backup battery charger is not under voltage and the electronic modules and PCBs had been taken out of it, they will survive undamaged.

Spare programmable digital protection relay (DPR) modules which are stored separately should be pre-programmed, configured, marked and prepared for direct installation into a designated DPR.

Critical types of electronic equipment, such as DPRs, should be installed in metal cabinets to protect them from the entry of high-frequency electromagnetic emissions. The structures of these cabinets should be subject to inspection. If they contain glass windows or doors, open blinds or other openings, they need to be altered by putting special reflecting primer on glass windows and doors, filling ventilation blinds with special metal inserts, which resemble a mesh made of steel threads.

If critical types of electronic equipment are installed in open panels, they need to be protected by a steel box from the rear of the cabinet. The front of these panels can be protected by curtains made of a special metalised fabric.

The glass windows in control rooms containing critical types of electronic equipment should be closed and covered by a special transparent reflecting primer. The doors should be metal. The control rooms should be made of reinforced concrete or, alternatively, its walls, ceiling and floor should at least be painted with a special semi-conducting paint, which reflects high-frequency electromagnetic

emission. It is possible to use special protective curtains and carpets containing metal threads, which are also available.

As for external electric circuits, to which the critical items are connected (including power supply, input and output circuits), these should contain sufficient industrial suppressors to provide protection. Varistors are available in single and three-phase designs for AC and DC applications. They can be fitted on a standard DIN-rail and provided with fuses and indicators of the state of the fuses. The more circuits are protected by varistors, the less is the probability that they and the electronic equipment connected to them will be damaged.

Control cables in the circuits of critical types of equipment, which do not have screens, should be replaced by screened cables. At the same time it should be noted that there are many cable screen types, however, only some of them provide protection from IDEI. Cable screens should be grounded on both sides. If the induced alternating current at industrial frequency is present in the screen due to high AC load current running through the cable, grounding of one of the screen's ends is performed through a capacitor.

Control cables connected to critical types of equipment should be provided with filters which suppress induced high-frequency signal in the cable. These filters are especially designed to ensure protection from IDEI. The simplest variant of the high-frequency filter are ferrite rings (cylinders) installed directly on the control cables (but of course, not on the screens). They are cheap and affordable elements, which should be widely used regardless of availability of other forms of protection.

More details on the means for IDEI protection described above are provided in [8].

It is obvious that all the above mentioned measures can be implemented fully only on newly constructed facilities of power supply industry. However, these measures include enough simple and inexpensive technical solutions, which can successfully be realised also in existing facilities.

Concerning standardisation

A lack of standardisation in the field of digital protection relays (both in terms of DPR design and in terms of software) is a serious problem making it difficult to establish measures providing protection of a power industry's facilities from IDEI [9]. The incompatibility of DPR modules from different manufacturers and even different models of the same manufacturer require significant expenditures to purchase and store the sets of standby modules for each separate type of DPR. Incompatibility of software will significantly hinder the check-of-fitness of the modules and restoration of relay protection functioning making it very time consuming.

The lack of standards in the field of DPRs also raises significant problems under normal operation modes of relay protection [9], the need for standardisation in this area becomes especially relevant and requires an urgent solution. Specific solutions to the standardisation problem of modern relay protection are offered in [9].

The problems of standardisation in the field of relay protection are closely related to the problem of the testing of DPR fitness after confirmed IDEI as there is lack of standardisation not only in the field of DPR, but also in the field of testing systems and algorithms implemented in them. However, this problem can also be overcome [9].

Production of relay protection and automation devices

Reducing the vulnerability of DPRs to electromagnetic impacts is the most important element in order to improve the power systems immunity to IDEI. One of the newest and the most effective ways to reduce a relay's vulnerability is the development of hybrid protection relays which combine electromechanical actuators with digital terminals [10 – 12].

This hybrid design of relay protection provides electromechanical devices with high immunity to IDEI, while retaining the broad functionalities of microprocessor based equipment. It also reduces the probability of relay protection faults in the presence of IDEI or cyber impact.

Reducing a DPR's vulnerability can also be achieved by improving the design of input current and voltage transformers; by using special input filters, which reject high-frequency signals and high-voltage pulses; or by adding restrictions on the voltage levels on all inputs and outputs by the use of suppressors; or by improving insulation and the level of galvanic separation between elements of input and output circuits [12]. A special directive should obligate equipping all new types of DPR with a special means of protection from IDEI in the manufacturing stage. To achieve this, typical technical requirements to DPRs should be prepared. They will include a list of standard requirements on electromagnetic compatibility [9] and additional requirements on protection from IDEI [13].

Certification and testing

The need for special technical requirements on DPRs and substation control circuits to provide immunity from IDEI creates the necessity to establish specialised certification and testing centres, which will verify this immunity. The military testing centres available in various countries of the world are not suitable for testing civil equipment. It would be more sensible to use the available testing centres which are designed to deal with the issues of electromagnetic compatibility. This will most probably require the purchasing of equipment and the setting up of such these centres. This equipment is offered on the market by several specialised companies [13]. Apart from the equipment itself, it will also entail the need to develop the procedures of the tests to be undertaken, taking all available experience into consideration [13,14].

Conclusion

The seriousness of IDEI cannot be overlooked. All the necessary precautions should be taken to protect the country's electrical with the aim of improving a power system's immunity to attack. While equipment available for the protection and testing of sensitive instruments is a good start, participation by various organisations under the guidance of a special governmental agency will be required in order to realise all the efforts successfully.

References

[1] WM Wik: "Electromagnetic Terrorism – What are the Risks? What can be Done?", International Product Compliance Magazine, 1997.

[2] J Kappenman, W Radasky, and J Gilbert: "Electric Power Grid Vulnerability to Natural and Intentional Geomagnetic Disturbances", EMC Zurich Symposium, 14 to 18 February 2005.

[3] W Radasky: "The Emerging Threat of Electromagnetic Transients on the Critical Infrastructure", US Department of Homeland Security Conference, 26 to 27 April 2005.

[4] V Gurevich: "The Hazards of Electromagnetic Terrorism", Public Utilities Fortnightly, June 2005.

[5] V Gurevich: "Electromagnetic Terrorism: New Hazards", Electrical Engineering and Electromechanics, 2005.

[6] V Gurevich: "Microprocessor Protection Relays: New Prospects or New Problems?", Electrical Engineering and Electromechanics, 2006.

[7] V Gurevich: "Electromagnetic Terrorism – The New Reality of XXI century", The World of Technics and Technologies, 2005.

[8] V Gurevich: "Cyber and Electromagnetic Threats in Modern Relay Protection" CRC Press, 2014.

[9] V Gurevich: "Problems of Standardisation in Relay Protection", 2014.

[10] V Gurevich: "Reducing the Vulnerability of Digital Protective Relays to Intentional Remote Destructive Impacts", Global Journal of Researches in Engineering : Electrical and Electronics Engineering, 2013.

[11] V Gurevich: "Reducing the Vulnerability of Digital Protective Relays to Intentional Remote Destructive Impacts: Technical-and-Economic Aspects", Global Journal of Researches in Engineering: Electrical and Electronic Engineering, 2014.

[12] V Gurevich: "Reducing the Vulnerability of Digital Protective Relays to Intentional Remote Destructive Impacts: Continuation of the Theme", Global Journal of Researches in Engineering: Electrical and Electronics Engineering, 2014.

[13] V Gurevich: "Problems in Testing Digital Protective Relays for Immunity to Intentional Destructive Electromagnetic Impacts", Global Journal of Advanced Research, 2014.

[14] V Gurevich: "Problems in Testing Digital Protective Relays for Immunity to Intentional Destructive Electromagnetic Impacts", Global Journal of Advanced Research, 2015.

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