VLADIMIR GUREVICH

EMP PROTECTION OF CIVILIAN CRITICAL INFRASTRUCTURE

OPINIONS

PROBLEMS

STRATEGY

SOLUTIONS

THIRD EDITION

2023

ANNOTATION

Gurevich V. EMP Protection of Civilian Critical Infrastructure: Opinions, Problems, Strategy, Solutions. Third Edition. – Haifa, 2023, 30 p.

The problem of the destructive effects of High-Altitude Electromagnetic Pulse (HEMP or EMP) on electronic and electrical equipment has been well known for more than 50 years. All military equipment and critical equipment of special governmental services are reliably protected from such influences. There are many companies on the market that manufactures numerous EMP protection means that meet the requirements of military standards. It would seem that in such a situation, critical civilian infrastructure facilities (electrical power systems, water supply systems, communications, large medical centers, banks, etc.) should also be protected against EMP. But it turns out that this is not the case! Nowhere in the world are critical civilian infrastructure still protected from such impacts! Why?

The main reason is an attempt to use well-known military strategies, methods and protection means for protecting civilian infrastructure.

This brochure analyses the reasons why critical civilian infrastructure has been unprotected for more than 50 years, proposes new protection strategies and methods, as well as new protections means designed especially for the civilian sector.

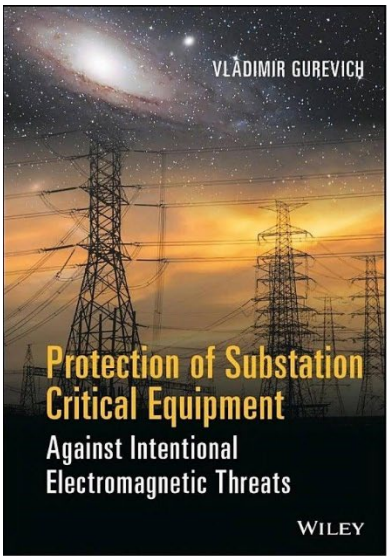
The brochure is intended for managers and technical staff of civil infrastructure facilities, specialists in the field of EMP, university teachers and students.

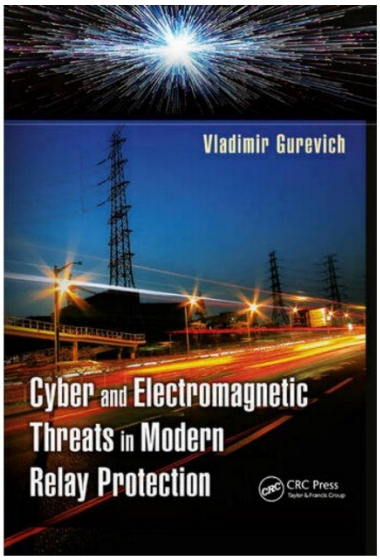
---

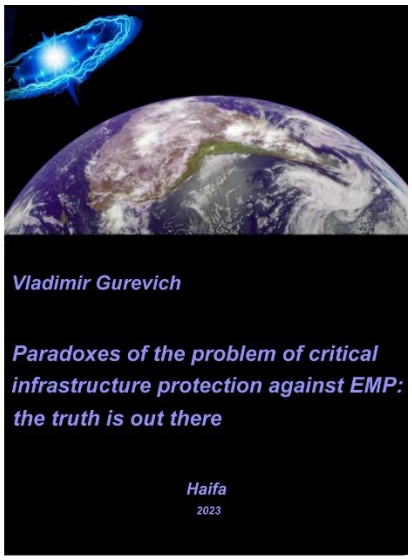
vladimir.gurevich@outlook.com

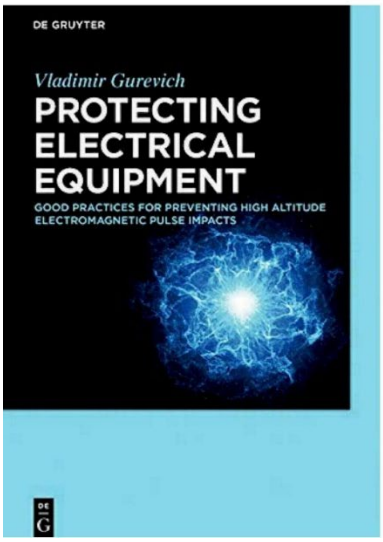
EMP Protection of Civilian Critical Infrastructure: Opinions, Problems, Strategy, Solutions

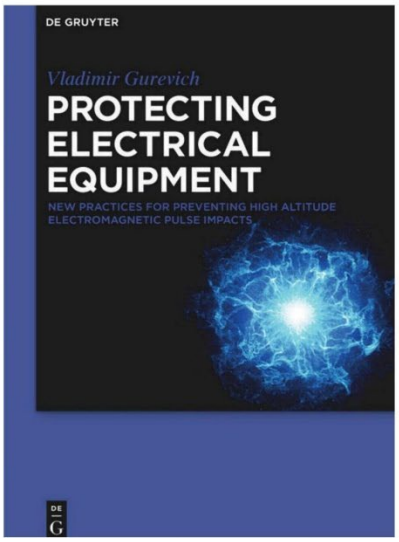
Dr. Vladimir Gurevich, Prof. Emeritus

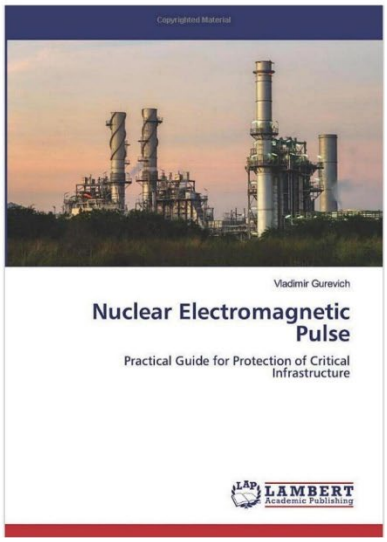












1. INTRODUCTION

The ability of the powerful electromagnetic pulse, generated upon the HEMP to destroy all electronics, has been known to nuclear physicists since the first nuclear explosion was performed in 1945 on the Alamogordo range, New Mexico (project “Trinity”). Upon the explosion, all apparatus that was meant to monitor the explosion parameters became inoperative. Upon all further test explosions performed in all countries, that electromagnetic pulse was registered precisely and was followed with the analysis and study of the parameters.

Beginning in the 1970s (50 years ago), that subject has been unclassified. At that time, dozens of Western scientific and technical reports, prepared by numerous military and civilian organizations (working at the military request), were devoted to different aspects of HEMP impact on electrical equipment and electronics. Since then, the electromagnetic pulse had been officially recognized as one of the damage effects of nuclear weapons, along with the detonation wave, the temperature, the light and the radioactive emission. At the same time, the first recommendations for the protection of electronic and electrical equipment from HEMP appeared, which, of course, were primarily intended for military equipment [1, 2].

Well, what about civilian critical infrastructure protection? Today, at least a hundred organizations around the world are dealing with this problem (there are more than 50 of them in the United States only), dozens of detailed reports have been published on this topic, which are freely available on the Internet [3], as well as hundreds of articles and books. Dozens of standards (civilian and military) describe how to protect critical infrastructure equipment against HEMP [3].

But if everything is so good, then why is critical civilian infrastructure still unprotected anywhere in the world? Why, after 50 years of careful study of the problem and hundreds of recommendations, is the Department of Homeland Security asking Congress for tens of millions of dollars to "*improve understanding*", Fig. 1?

Critical Infrastructure Security and Resilience Research, Development, Test, and Evaluation Spend Plan

April 25, 2022
Fiscal Year 2022 Report to Congress

Homeland Security *Science and Technology Directorate*

S&T Project	Purpose	Funding ($)	Funds Obligation Timeline
Focus Area 2: Electromagnetic Pulse and Geomagnetic Disturbance Resilience Capabilities			
CISRR - EMP and GMD Resiliency	Improve our understanding of the effects of EMP/GMD events on communications infrastructure (and other critical infrastructure) and drive research activities to provide practical, data-driven, specific, and actionable information, concepts, techniques, technologies, and tools to critical infrastructure owners and operators to implement to protect their current and future communication systems from the impacts of an EMP event.	$22,750,000	FY 2022-2025

Fig. 1. The budget of the Department of Homeland Security to "improve understanding" of the problem of critical infrastructure resilience after 50 years of careful study.

And this is just one organization out of many dozens "studying" this problem in the United States alone! One can only imagine how much money from the budget is "sawn" under the guise of this problem…

2. OPINIONS

To date, we have three opposing concepts on the problem of protecting the civil critical infrastructure, which are reflected in the statements of the apologists of these three concepts:

A. Everything has been known for a long time, there are no technological problems:

"The problem is not the technology. We know how to protect against it. It's not the money, it doesn't cost that much. The problem is the politics. It always seems to be the politics that gets in the way".

Dr. Peter Vincent Pry,
Executive Director of the Task Force on National and Homeland Security

"The U.S. military already has EMP protection approaches that are practical, affordable, tested and well understood that can be translated directly to electric power grid control facilities and supervisory control and data acquisition electronics and networks."

Dr. George H. Baker,
Prof. Emeritus James Madison University, Director Foundation for Resilient Societies

---

B. We have neither the knowledge nor the resources to protect infrastructures:

"*Much of the available information is not specifically applied to electric utilities, making it very difficult for utilities and regulators to understand effective options for protecting energy infrastructure".*

Robin Manning,
Vice president for transmission and distribution for the Electric Power Research Institute (EPRI)

"Managing that kind of threat right now — no one really has the resources to do that"

Richard Mroz,
President of the New Jersey Board of Public Utilities

C. There are no solutions to the problem, so you need to leave everything as it is

"I don't mean to be so flippant, but there really aren't any solutions to THIS, so I would just leave it at that".

General M. V. Hayden
Ex-Director of the National Security Agency (NSA);
Ex-Director of the Central Intelligence Agency (CIA)

Which of them is really right?

Yes, all three, if try to use military technologies to protect civilian infrastructure! Here's just one problem: such an attempt is doomed to failure ...

The representatives of the powerful Military-Industrial Complex (MIC) also did their bit to slow down the process of implementing concrete measures, which were already well known, to protect systems from HEMP. They insist that the only effective defenses against HEMP is a national anti-missile defense system, into which more budgetary funds should be invested. This position, which was adopted by the representatives of the MIC, would be completely understandable if the

relatively low cost of defensive measures to protect the most important elements of the country's infrastructure and its systems from HEMP were compared with the cost of developing and producing an effective multi-layered antimissile shield that would protect the entire country. However, it appears that it is not that simple and that missile systems have been in existence for some time that an anti-missile system is not capable of defending against, that is to say it is not possible to protect the national infrastructure from HEMP attacks. What sort of systems are these then? First of all, these are theatre ballistic missile (TBM) systems which can be equipped with a nuclear warhead, Fig. 2.

Fig. 2. Soviet/Russian theatre ballistic missile (TBM) systems which can be equipped with a nuclear warhead (explosion yield up to 200 kt).

Fig. 3. A conventional shipping container (left) and a LORA missile system container (right)

The danger of such systems is that they can be as close as possible to the borders of any country. With a small area of a country (for example, such as Israel), the flight time of such a missile can be

so small that the missile defense system will not be able to effectively counteract. Especially dangerous are modern container-type missile systems, which are made in the form of an ordinary container with missiles hidden inside. Such a system is, for example, the Israeli LORA system (Long-Range Artillery Weapon System). The launcher of such a system differs very little from a conventional shipping container, Fig. 3. Today there are hundreds of millions of sea containers in circulation across the world, Fig. 4. Nobody knows which of them are genuine and which are filled with missiles…

Fig. 4. An ordinary civilian container ship loaded with hundreds of standard containers and a LORA rocket, launched from a ship with containers during a test launch.

Developed by IAI's MALAM division, LORA is a sea-to-ground and ground-to-ground system which comprises a long-range ballistic missile, a unique launcher, a command-and-control system, and a ground/marine support system. LORA missile has a length of 5.2 m, a diameter of 625 mm and weight of 1,600 kg. It can engage targets at a short range of 90 km and at long ranges up to 430 km. High explosive (HE) warhead (up to 600 kg) can be equipped with a nuclear charge. This rocket is capable of going up to an altitude of 45 km and above, that is, to an altitude optimal for the production of HEMP.

No missile defense system is capable of neutralizing a missile that unexpectedly launches vertically from one of the hundreds of containers standing in the cargo port of a container ship, Fig. 3.

The LORA missile system is not entirely unique. Similar systems are also being developed and manufactured by other countries. That is the actual situation is such that the Army is not in a position to provide a sufficiently reliable defense of the civilian infrastructure facilities and population centers from HEMP and as such it is the electrical engineering specialists themselves that need to be concerned with this defense ahead of time.

3. THE PROBLEMS

Today, indeed, there is all the data on how and how critical infrastructure can be protected. However, the means of protection against HEMP available on the market, made according to military standards, are not suitable for the protection of civilian infrastructure. Therefore, no one does anything in practice to protect civilian infrastructure. That is everyone is right and everything is correct, but this does not interfere with the situation that for 50 years not a single substation in the world has been protected as it should be (two substations in USA, partially protected do not count).

But where is the way out of this paradoxical situation?

There can be only one way out of this situation: the development of protective equipment specifically designed for civilian infrastructure. But for this it is necessary to know well the structure and features of civilian infrastructure, including control cabinets with electronic equipment, relay protection, power transformers, DC power auxiliary supply system, grounding systems, Ethernet networks and much more. Therefore, it is not easy to develop protection for such a diverse range of equipment. In addition, in order to understand what means of protection are needed for civilian infrastructure, ***it is necessary to understand why the known military means of protection are not suitable***.

There are several very important problems detailed in [4, 5]. Here are some of them:

Problem 1. Unlike the civilian systems, over the last few decades, all critical military systems vulnerable to HEMP have been designed with HEMP protection. It is much easier and cheaper to include HEMP protection means in the design stage than try to protect the existing critical civilian equipment, such as digital protection relay cabinets used in the electric power industry. Such cabinets, sometimes overstuffed with apparatus, have dozens of inputs and output multicore cables and each separate core requires protection. Who will attend to this?

Problem 2. Internal electrical wiring of military systems (tanks, airplanes, ships, missiles) are made with preassembled wire harnesses or with separate wires in strict adherence to drawings and sizes. Thus, the electrical characteristics of such wiring at high frequencies (HEMP frequencies) are identical to the equipment of the same type. It means that it is sufficient to test the HEMP immunity of one finished typical sample in order to be sure that all other units will have the same characteristics. In the electrical power industry, it is hardly possible to find two identical cabinets with electronics having absolutely identical internal wiring.

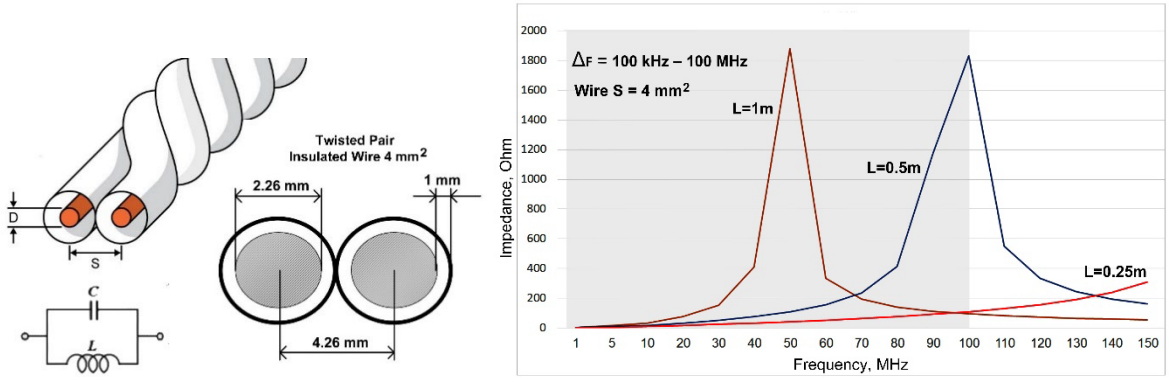
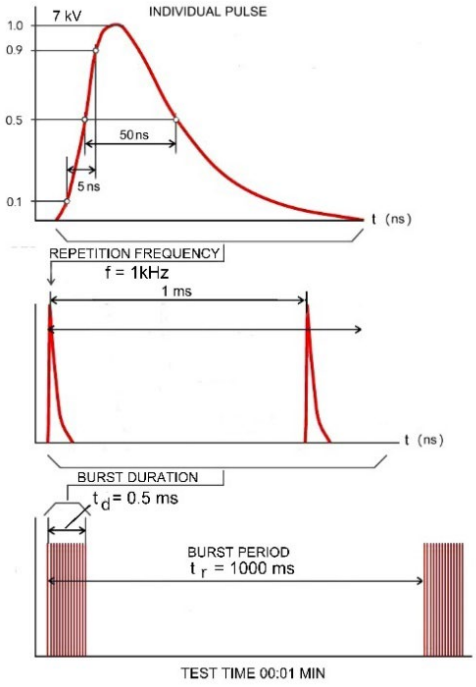


Fig. 5. Estimation model for a twisted pair of conductors and impedance of a twisted pair of mounting wires of different lengths (1 m; 0.5 m; 0.25 m) as a function of frequency.

Author's study [4], confirming that in the frequency range of 100 kHz - 100 MHz, the resonant frequency and impedance of the most common twisted pair of wires changes very significantly when the length of these wires' changes (0.25 m; 0.5 m; 1 m), Fig. 5, and as results a dramatic change of cabinet internal apparatus vulnerability to HEMP [4]. Therefore, a typical test model for civilian control cabinets does not exist.

Thus, the results of testing any individual cabinet for very short electromagnetic pulse impact cannot be extrapolated over other cabinets, i.e., in practice, there is no "typical" cabinet for such tests. Based on conclusions made in [4 - 6], it is not feasible to conduct such tests for this type of equipment.



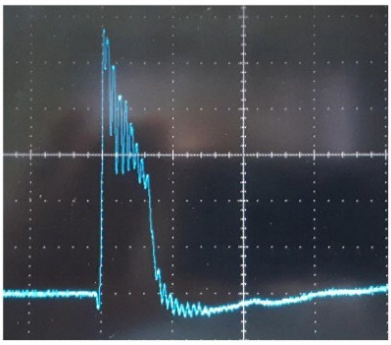


Fig. 6. Testing equipment and set-up of the Electrical Fast Transient (EFT) pulse generator (EFT is very close in shape and duration to HEMP) to test compliance with IEC 61000-4-25 and oscillogram of the real pulse.
1 – DOBLE F2253 simulator of relay protection modes (as an external power source); 2 – MIG0603 standard HV pulse generator; 3 – 500N EFT pulse generator; 4 – Tektronix MSO 4034 pulse oscillograph; 5 – test object (digital protection relay - DPR).

Another study of the unpredictability of the resilience level of civilian equipment to HEMP was carried out by the author personally on the example of power supplies for microprocessor-based digital protection relays (DPR). A DPR is a critical kind of equipment which ensures sustainability of power systems' operation. Thus, it is of utmost importance that DPRs are resilient to HEMP. The most important part of a DPR is its internal power supply. Thus, efficiency of other functional modules of a DPR largely depends on its integrity. On the other hand, external circuits to which it is directly connected may be a powerful source of electromagnetic impact for a DPR. This is the reason why DPR's power sources have been selected as the target of author research, Fig. 6.

The following DPRs (various types, various manufacturers and various time of manufacturing) were used for testing purposes:

- SPAD330C (ABB)
- 7S5115 (Siemens)
- REC316 (ABB)
- Siprotec 7SJ62 (Siemens)
- F650 (General Electric)

Power supplies of all these DPRs available in the market are of a switching type. This means that they feature a typical design, which includes an input filter, rectifier, converter of DC input voltage into high-frequency voltage, small-size step-down high-frequency transformer with a ferrite core, secondary rectifier with filters, a circuit for output voltage stabilization and adjustment (there are several circuits like this in each switching power supply). Regardless of shared mode of action, these power sources are significantly different from each other in terms of design, complexity, number of elements and size.

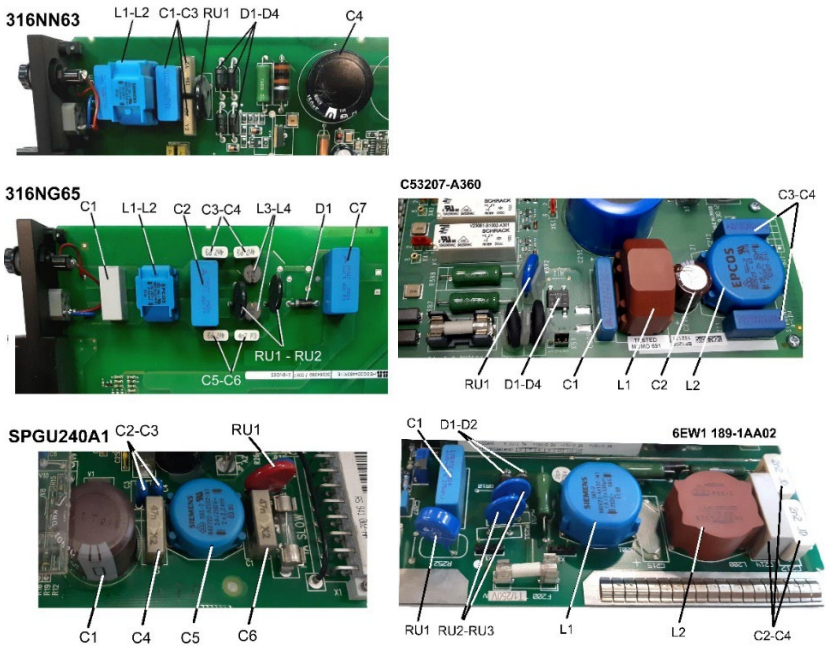


Fig. 7. Various types of input filters on DPR's power supplies, a) manufactured by ABB; b) manufactured by Siemens. In addition to capacitors C_N and chokes L_N of the filters, also include varistors RU_N.

Since DPRs are always subject to pulse noise under a real operating environment, all power supplies are compulsory equipped with input filters LC (Fig. 7). As a rule, these filters include high-frequency chokes L_N and capacitors C_N (designed to suppress a high-frequency noise) as well as

varistors RU_N, which limited the noise's amplitude. Since all the power supplies contained rather complicated filters, the tests were expected to be formal and all DPRs would successfully pass them.

Different power supplies reacted differently to the test pulses [4], and one of them showed a very strange feature. When exposing this power supply to a standard 1.2/50 μs lightning pulse (6 kV amplitude), there was no response at all, but it switching off as it was affected by very short EFT (5/50 ns) with the amplitude of 1 kV. Lack of detectable response of the DPR to a pulse with high amplitude and high energy and loss of efficiency (though temporarily) upon the impact of a shorter pulse with low amplitude (low energy) was an unexpected finding of this experiment.

Single EFT pulse with the amplitude of 7 kV impacting the DPR resulted in power loss in all circuits. However, several seconds later the DPR rebooted and returned into a normal state. Impact of standard pulse bursts (1.2/50 μs) with the increased amplitude (up to 7 kV) resulted in permanent damage in the power supply (breakdown of the key element – powerful MOSFET transistor BUZ80 type with maximal operating voltage 800V and maximal impulse current 13A) and further blowing of a current-limiting resistor. These Power supplies were also tested with additional EMI filters and surge arresters at its inputs [4].

Testing of a mentioned DPR fitted with 316NN63 power supply revealed that the faults during DPR's operation occurred:

a) when delivering an EFT pulse with 1kV (and more) amplitude to the power supply's input;
b) when delivering an EFT pulse with 2.6 kV (and more) amplitude to the input of the power supply with an NBM-06-471 filter connected in series;
c) when delivering an EFT pulse with 4 kV (and more) amplitude to the input of the power source with an NBM-06-471 filter fitted with a varistor at the input.

Conclusion for this research: The electromagnetic filters connected before the power supply, may significantly improve electronic equipment's resistance to EFT and HEMP when fitted with a varistor at the input. But, «*significantly improve electronic equipment's resistance*» does not mean to completely protect against the effects of HEMP. That is, for civilian infrastructure there will always be a danger of damage to certain types of equipment, while other types of equipment will be reliably protected by the proposed (non-military) means of protection. And due to the huge variety of kinds and types of equipment used even at one separate civilian facility, it is simply not possible to check and establish the real level of stability of each of these types of equipment. In addition, these individual specimens of the electronic devices do not work on their own, in isolation from others, but are closely connected with them by electrical and functional connections into a common system, which makes even a very approximate assessment of the resilience of such a system unrealistic.

PROCESSOR (INTEL)	CLOCK RATE MHz	STRUCTURE SIZE micrometer	CPU VOLTAGE, V	NUMBER OF TRANSISTORS
8088	5	>1,5	12	28 000
80286	10	1,5	5	130 000
80386DX20	20	1,5	5	275 000
80486DX25	25	1	5	1 200 000
80486DX33	33	1	5	1 200 000
P80486DX266	66	0,6	5	1 200 000
Pentium I	75	0,6	3,3	3 300 000
Pentium I	100	0,6	3,3	3 300 000
Pentium MMX	200	0,35	2,8	4 500 000
Pentium II	266	0,28	2,5	7 500 000
Pentium III	450	0,25	2	9 500 000
Pentium III	500	0,18	2	28 000 000

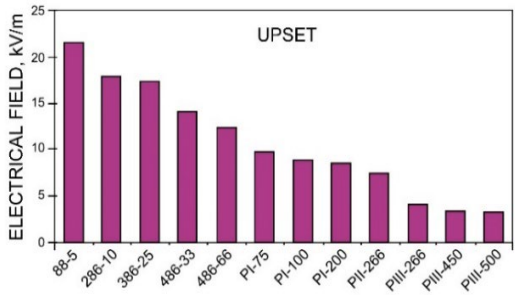


Fig. 8. Information on microprocessors (up to Pentium III inclusive) and the levels of pulse electric field resulting in their malfunctions.

The data presented in [4] regarding the resilience of different electronic components, computers and computer networks also confirm an extremely large scattering of test results, depending on the influence of a very large number of almost unpredictable factors and the inability to transfer the results of single tests of specific devices and systems to other devices and systems. Only two examples from [4]: Fig. 8 and Fig. 9.

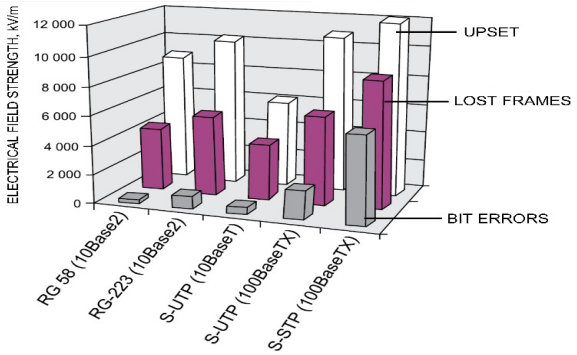


Fig. 9. The level of susceptibility (failures) of the simplest computer network for various network and cables configurations.

Problem 3. The military apparatus is protected within the electromagnetic range both from HEMP and Intentional Electromagnetic Interferences (IEMI), as well as from data leak through the electromagnetic fields (TEMPEST). The higher frequency range of IEMI and TEMPEST is far beyond the HEMP range (20 GHz–40 GHz). However, such means must ensure at least 80 dB – 100 dB attenuation of an electromagnetic interference (signal), Fig. 10.

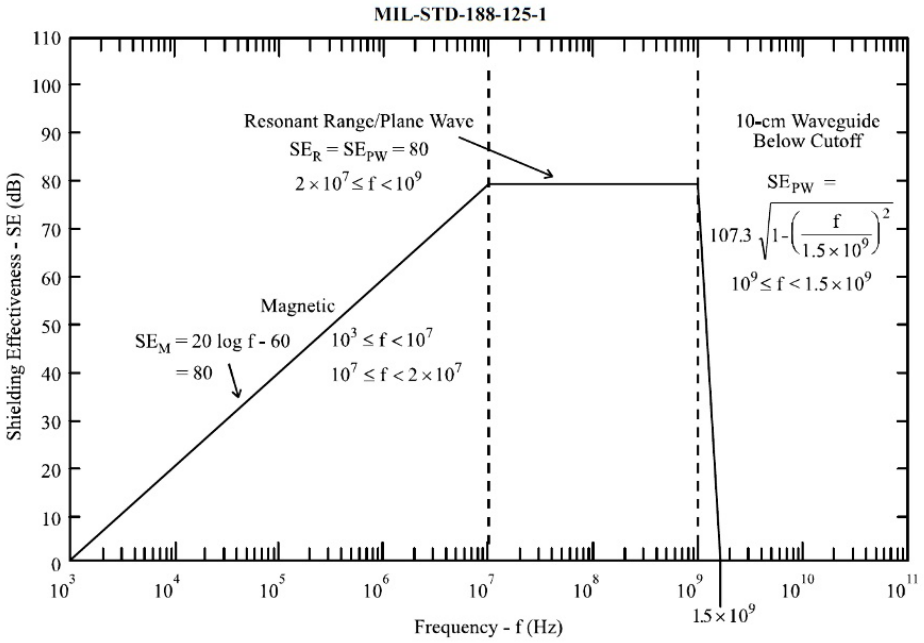


Fig. 10. Minimum HEMP shielding effectiveness requirement according to MIL-STD-188-125-1 [7].

Many manufacturers want to be holier than the Pope and offer on the market EMP filters with parameters that exceed the requirements of this standard, Fig. 11.

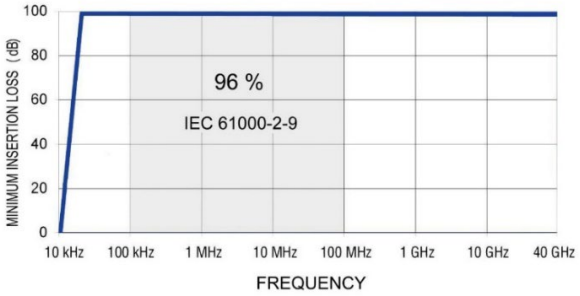


Fig. 11. Typical amplitude and frequency features of HEMP filters represented in ETS-Lindgren's promotional materials.

Even single-phase two-line filters (the simplest) designed for installation into a DC or single-phase AC supply circuit featuring 3–10 A costs 1.500 – 2.500 US Dollars. Weight and dimensions of these filters (Table 1) worsen the situation.

Fig. 12. HEMP filters (left) and control cabinets (right). For size comparison.

The first question that surfaces upon receiving the cost information is: what is special about them? The answer can be found in specifications of these filters. The frequency range of such filters spans from dozens of kilo-hertz to as high as 20-40 GHz and the noise signal attenuation achievable within this range is up to 100 dB (i.e. 100,000 times in respect to amplitude!), Fig. 11. It is clear that such high-quality filters with such an ultra-wide range of operating frequencies cannot be small, simple and cheap, Fig. 12, Table 1.

Does anyone really believe that equipment of the civil infrastructure can use the same filters simulating the ones used in the underground military bunker? The answer to this question can be obtained from the results of a study carried out by the National Coordinating Center for Communications (USA) [8], Table 2.

Table1. Weight and dimensions of HEMP filters from various manufacturers

Type	Nominal Current, A	Manufacturer	Dimensions, mm	Weight, kg
EEP16SPN	16	European EMC Products	560 x 200 x 112	15
LRX-2005-S2 LRX-2010-S2	5 10	ETS-Lindgren	940 x 229 x 127	27.2
8080-2-16	16	Holland Shielding Systems BV	720 x 90 x 130	-
A-10543	10	Captor Corp.	762 x 229 x 140	-
DS33330	6	MPE Ltd.	420 x 200 x 120	10

DS33331	16			
FH1960-2W FH1970-2W	20	LCR Electronics (Astrodyne)	762 x 305 x 127	-
MF420-CF	10	EMI Solutions (EMIS)	750 x 150 x 110	-
GPF271C-16	16	Changzhou Noordin Etech. Co.	800 x 200 x 125	-
CDSUX20210A6	10	Corcon (TE Connectivity)	533 x 203 x 127	13.6

From the presented table, one can see the inexpediency of applying the requirements of military standards to the means of protecting civil equipment. It appears that it is quite enough to attenuate HEMP by 20 - 30 dB only. This significantly changes the attitude towards the problem of protecting civilian equipment.

Table 2. HEMP modeling results of damage and upset mitigation for nuclear burst 100 kT at a height of 400 km over the territory of the United States.

Equipment	Protection level, dB	Damage and upset area, sq. km	Damage and upset equipment, %
Ethernet with 30 m cable	0	~5.000.000	69.7
	10	~3.000.000	40.8
	20	~600.000	8.2
	30	0	0
Ordinary telephone system for analog signal transmission over twisted pair (POTS Telephone)	0	~4.000.000	51.5
	10	~900.000	12.9
	20	0	0
	30	0	0
Cordless telephone	0	~6.000.000	78.0
	10	~2.500.000	32.8
	20	~300.000	4.4
	30	0	0

Such a conclusion is also confirmed in [9], where it is shown that even for military equipment, the requirements of the basic standard MIL-STD-188-125 [7] should not be applied directly to military facilities of all echelons:

"If shielding facilities applying the MIL-STD-188-125 standard are installed in all national infrastructures, it is estimated that a huge budget will be required. MIL-STD-188-125 does not consider the blocking and attenuation characteristics of regular buildings or underground facilities in terms of EMP protection. Furthermore, it requires the use of a huge amount of concrete, rebar, and steel plates in heavyweight structures to disallow even a single failure in mission-critical facilities. Hence, there is no need to apply MIL-STD-188-125 to military facilities of all echelons… Therefore, it was confirmed that EMP protection measures could be changed from the current shielding room-oriented, fixed-type protection facilities to mobile lightweight protection facilities using shielding fabrics, shielding racks, redundant equipment, spare equipment, and failure recovery."

Accordingly, what should be said about civilian equipment?! Do we really need such a broad range of the frequencies for HEMP protection, if according to IEC 61000-2-9 [10] 96% of HEMP's energy is emitted in 100 kHz–100 MHz range and 70% of the energy – in 100 kHz–10 MHz range, Fig. 11 and Fig. 13?!

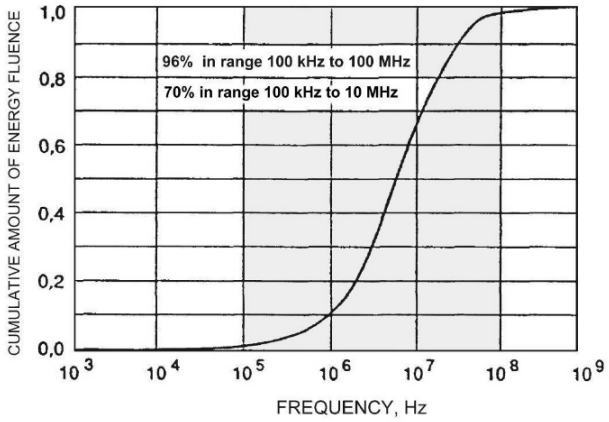


Fig. 13. HEMP energy distribution over the frequency range (see IEC 61000-2-9 [10])

Answer yes, for military installation. The military apparatus is protected within the electromagnetic range both from HEMP and Intentional Electromagnetic Interferences (IEMI), as well as from data leak through the electromagnetic fields (TEMPEST). The higher frequency range of IEMI and TEMPEST is far beyond the HEMP range (20 GHz–40 GHz). But what regarding of civilian installation? Do we need IEMI and TEMPEST protection for civilian infrastructure?

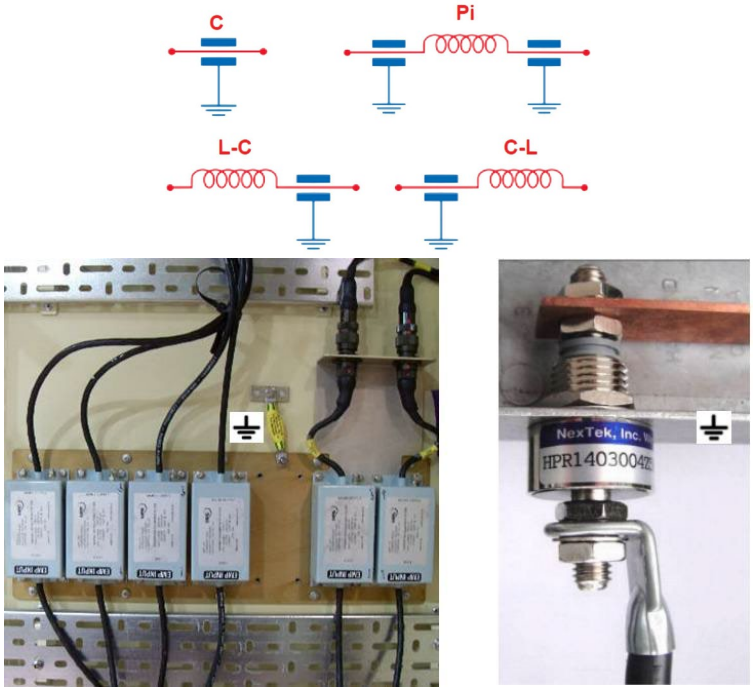


Fig. 14. Simplified design and appearance of various LC-filters against HEMP with parallel capacitive elements that divert impulse energy from the input to the ground

Of course, there are smaller filters (although also not cheap at all), but they all use the ground as an energy absorber for HEMP, Fig. 14. But in fact, the ground is not such an absorber moreover, the grounding system itself is a huge antenna that collects energy from a large area and brings it directly to the grounded electronic equipment [4-6].

In addition, a many of these filters are not protected against the high amplitude of the EMP input pulses and therefore require the installation of additional surge arresters at the input, as required by the standard MIL-STD-188-125 [7], Fig. 15.

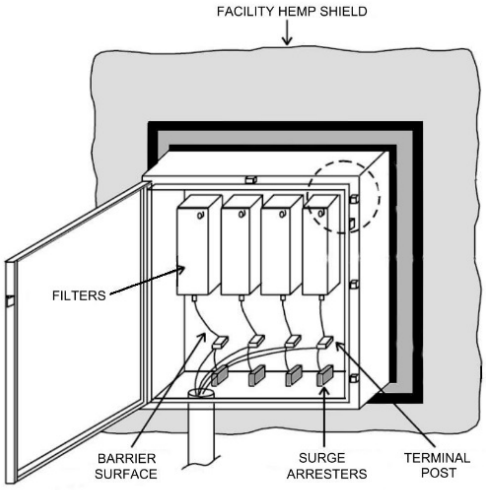


Fig. 15. Design of inlet box for connecting of external cable to a unit protected from HEMP (according to MIL-STD-188-125)

Special circuit diagrams for connecting the current and voltage circuits of microprocessor-based protection relays installed in cabinets require the use of HEMP filters also with special internal circuit diagrams [6].

Fig. 16. The author in the process of testing the optical multiplexer (left) type FOCUS (Fiber Optic Communications for Utility Systems) for compliance with IEC standards for electromagnetic compatibility

The transition to optical communication cables between cabinets with electronic equipment is sometimes presented as a panacea for all ills. Unfortunately, this is far from the case, since all the same electronic equipment remains inside the cabinets, connected to external power supply circuits and to external power actuators such as solenoids, high-voltage circuit breakers, disconnectors,

motors, etc. If through these external circuits HEMP penetrates into the cabinet, then it is likely to damage internal telecommunications equipment, despite the fact that the external communication lines are made on optical fiber. Moreover, multi-channel equipment that converts electrical signals into optical signals and vice versa, restores electrical signals from optical signals (the so-called multiplexers) are very complex devices containing a large number of microelectronic components and microprocessors. That is, the presence of such devices can further increase the vulnerability of infrastructure objects. Sometimes these very complex and sensitive electronic devices do not withstand even standard pulse effects when tested for standard electromagnetic compatibility, Fig. 16.

Problem 4. This problem is related to the test benches simulating HEMP. Within such a test bench, such as the guided-wave type HEMP simulator, Fig. 17, that has been primarily developed for testing pieces of military equipment), the bottom part of the antenna is embedded into a concrete base and has ground potential, Fig. 17.

As is well known, lightning is an electrical discharge that occurs due to the high potency difference between the cloud and the ground. As is well known, all electrical equipment must be grounded, so when lightning strikes it, the charge is discharged into the ground through the grounding system.

In the EMP simulator of the guided-wave type a high-voltage pulse of the generator is applied between the grounded grid (low-potential electrode) and the antenna (high-potential electrode), that is, in terms of potentials, it is a complete analogue of the cloud-ground system. Grounding the EUT located on the test bench means connecting it to the lower, low-potential electrode of the test bench. In this case, the EUT will be exposed to the same pulse high potential as when the lightning potential hits it.

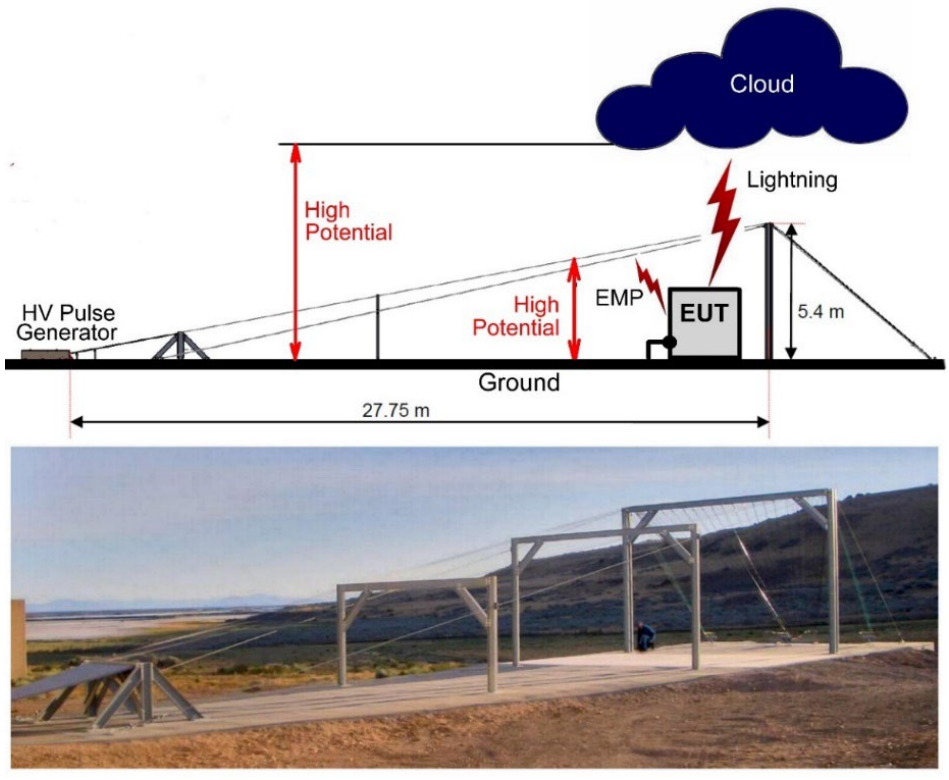


Fig. 17. The antenna system of the military test bench simulating HEMP.
EUT – equipment under test.

Of course, EMP is not a breakdown in air between two big "electrodes" like lightning. This is an electromagnetic wave incident on the EUT. But inside the EUT, it transforms into the same effect on the EUT as lightning, that is, into an overcurrent pulse and into an overvoltage pulse. Therefore, the grounding of the EUT on the test bench will perform the same protective function.

However, a real EMP creates a potential difference into the EUT that has nothing to do with the potential of the ground and therefore the grounding of the EUT on the test bench will completely change the picture compared to the real one.

It is not a problem for tanks, airplanes, missiles, or other military equipment. However, in the case of civilian equipment, such as cabinets with digital protective relays with grounded zero potential points of internal electronic circuits (i.e. connected directly to the antenna bottom part), the test bench pulse impact on such a cabinet will differ from the real HEMP.

From the foregoing, it follows that the test of a grounded EUT on a such type test bench does not correspond to the real conditions for exposure to HEMP. Therefore, it remains unclear what the real impact of real EMP on grounded electronic equipment will be. At the same time, it should also be taken into account, that the branched grounding system itself is a huge antenna that absorbs the energy of EMP from a large area (for example, on the test bench, Fig.17)

One other problem of the HEMP simulators. Electronics cabinets used in the power generation industry have dozens of input and output cables, tens and hundreds of meters long. The cables act as antennas absorbing electromagnetic energy over the large area, delivering it directly to the sensitive electronics inside the cabinets. The findings of computer simulation reported by Lawrence Livermore National Laboratory [11] suggest that the amplitude on the ends of 45 and 65-meter-long control cables can reach as high as 100-120 kV at an established rating of E1 HEMP's electric field of 50 kV/m. How can such long cables be modeled on a very compact test space, which is available even on large test benches. For example, on the test bench 28 meters long (Fig. 17) the test area is only 2m x 2m. Only within this small area the parameters of the test pulse will meet the standard.

As noted above, these test benches were developed for testing military equipment, and therefore the requirements for testing on these test benches are set out in military standards, for example in MIL-STD-461G [12]. This standard provides separate test procedures and verification methods for equipment located in protected sheaths and separately for cables. That is, the testing of such a type of equipment as control cabinets with cables extending to the outside is not provided at all. However, in real conditions, the electronic equipment located inside such cabinets is exposed to the simultaneous complex effects of HEMP on both: the cables and the cabinet itself. And such a complex effect is not the same as a separate effect on the sheath (cabinet) and a separate effect on the cables coming out of it. In any case, if the standard requires such separate tests, then for civilian equipment they can be carried out without the use of a huge and very expensive military test bench (Fig. 17).

Today, there are a huge number of devices on the market for measuring the attenuation of electromagnetic radiation with protective shells (cabinets) and screens; for direct (contact) impact on the equipment of short high-voltage pulses (EFT- electrical fast transiens); for impact of such pulses on long cables (with capacitive coupling clamp); to measure the filters attenuation, etc., Fig. 18.

The author of this brochure widely used such devices in the process of developing and researching new means of protection for critical civilian equipment and did not feel the need to use a military test bench.

Fig. 18. Instruments sufficient to test civilian equipment for resistance to HEMP.

As shown in [5-6] most existing test benches, even on large, are of little help for testing cabinet-type equipment, which is used in the civil power industry and the results of these tests will be meaningless and useless.

Problem 5. Despite a large number of civil and military standards, including the still classified standard [13], describing the parameters of HEMP that affect equipment, the real values of these parameters remain completely unpredictable due to objective reasons.

For example, all HEMP-related standards define a field strength of 50 kV/m as a factor affecting the equipment. But in fact, this field strength can be completely different, both much more and much less.

Much more:

"On 3 September 2017, immediately after the sixth nuclear test, North Korea claimed that they were capable of attacking with an ultra-powerful EMP by detonating a hydrogen bomb high in the atmosphere" [9].

"*Russia has "Super-EMP" weapons specialized for HEMP attack that potentially generate 100,000 volts/meter or higher, greatly exceeding the U.S. military hardening standard (50,000 volts/meter)…Super-EMP is a…first-strike weapon," according to Aleksey Vaschenko, who describes Russian nuclear weapons specially designed to make extraordinarily powerful HEMP fields as Russia's means for defeating the United States"* [14].

Much less:

"Through calculations we found that, early-time HEMP has the property of a steep rise time and a slightly slower trailing time; the maximum electric field on ground is located in the area of 1–2 explosion heights to the south of the burst point on the ground; the area of minimum electric field is located at 50 km to the north of the burst point on the ground, about one magnitude smaller than the maximum value, as shown in Table I. This depends upon the inclined angle between the motion trail of the Compton electrons in the transmission direction and the geomagnetic field. If the inclined angle is smaller, the incited Compton currents will be smaller, and the field intensity will be smaller; if the inclined angle is bigger, the field intensity will be bigger" [15].

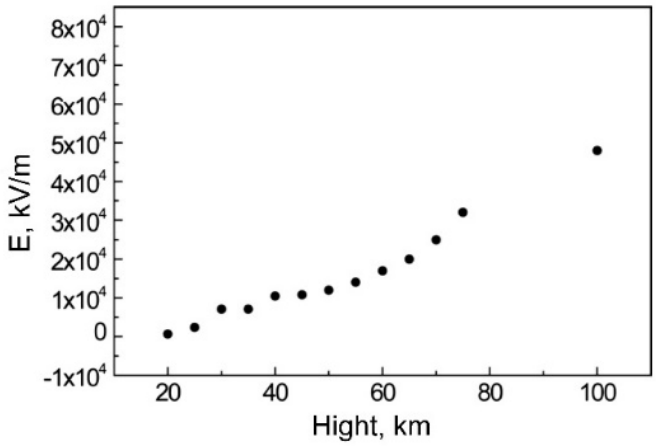


Fig. 19. Changes of the electric field intensity at different HOBs over the explosion center for 1Mt yield [15].

Table. 3 and Fig. 19 show only some of the possible variations of the HEMP field strength depending on external conditions, which cannot be predetermined.

There is also a nonlinear relationship between the power of the nuclear charge and the strength of the electric field:

"The power of the 100 kT explosion is 10 times less than that of the 1 MT nuclear explosion, with the electric field intensity peak down by 2.5 times; the power of 500 kT explosion is two times less than that of the 1 MT nuclear explosion, with the field intensity peak down by 15% only" [15].

"Due to a limiting atmospheric saturation effect in the EMP generation process, low yield weapons produce peak E1 fields of the same order of magnitude as large yield weapons if they are detonated at altitudes in the 50-80 km range. The advantage of high yield weapons is that their field on the ground is attenuated less significantly at larger heights of burst (that expose larger areas of the Earth's surface)." [16].

As can be seen, unpredictable variations in the intensity of HEMP exposure to equipment are possible over a very wide range, Fig. 20, 21 [16].

Table 3. Electric field peak value distributed on the ground from a 100 km height of burst (HOB), 1Mt yield burst [15].

Location on the ground (Projection point on the ground from the explosion center)	Peak electric field, V/m
50 km to the north	2866
26 to the north	11447
ground zero	20777
57.7 km to the south	35494
100 km to the south	40042
173 km to the south	40227
247 km to the south	37071
290 km to the south	34802
514 km to the south	30796

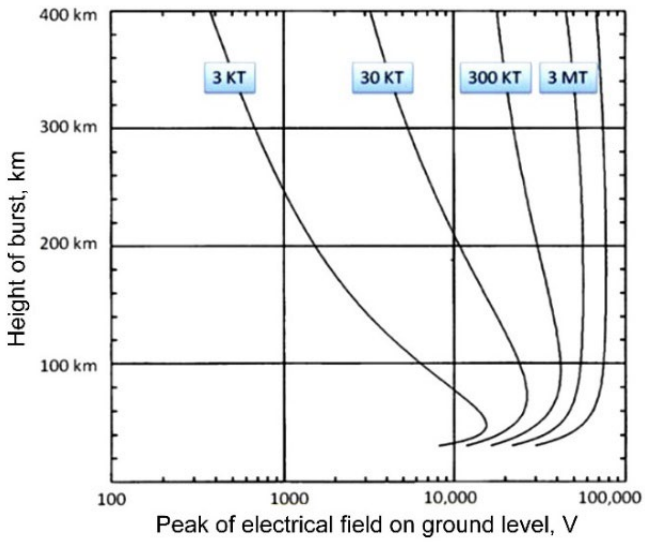


Fig. 20. Variations in the intensity of HEMP exposure.

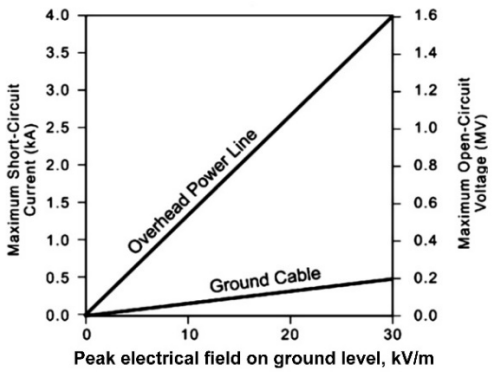


Fig. 21. Voltage and current induced in long overhead lines and ground cables by E1component of HEMP from kiloton-class yield weapons.

Problem 6. The next problem is using the requirements of the MIL-STD-188-125-1 [7] concerning injection of current pulse at testing resilience of electronic equipment to HEMP. Table B-I in section B "Pulsed Current Injection (PCI) Test Procedures" of this standard stipulates technical requirements for testing equipment, particularly for a high-voltage pulse generator. This device should generate a current pulse with an amplitude of up to 5,000 A with the source impedance of 60 Ω. According to the standard: "source impedance is the ratio of the generator peak open-circuit voltage to the peak short circuit current", i.e.: $R_{SOURCE} = U_{OPEN}/I_{Sh.C}$. Thus, the requirement to "open-circuit voltage" can be determined as: $U_{OPEN} = R_{SOURCE}$ x $I_{Sh.C.}$ = 60Ω x 5,000 A = 300,000 V. The generator providing such parameters really exist on the market. For example, the Marx type generator, manufactured by Montena EMC company.

In other words, output voltage of the generator, the output terminal which is connected to a circuit with high source impedance, (such as inputs/outputs of low-voltage electronic equipment) can reach as high as hundreds of thousands of volts! Which electronic circuits could sustain this voltage? Why should this voltage be applied to these circuits as they are subject to civil standards [17] restricting voltage at 8 kV (level EC8) or 16 kV (level EC9), depending on specific placement of equipment?

These simple calculations, multiple references in the standard to "conductive circuits" and "short-circuit currents", as well as lack of tests for "differential mode", imply that the requirements of this standard are not applicable for electronic equipment. They are rather suitable for testing of conductive protection devices, such as filters, which are connected into a "common mode", and grounded cable shields. Author assumed this previously [4 - 6] and thus he did not mention pulse current tests as a recommended method of HEMP-resilience testing of electronic equipment. However, some specialist dealing with these tests insists on adhering to requirements of this section of MIL-STD-188-125-1 when testing electronic equipment. It is globally true that HEMP simulators are usually maintained by military men or military industry representatives. These representatives used to work with military standards and often have no idea about existing sets of civil standards. When civil specialists test civil equipment on military test benches, they have no choice but to accept the rules established by the owners of the testing equipment. Hence, a supposed necessity of testing civil equipment based on MIL-STD-188-125-1 is also suggested in various scientific and technical papers. This is the reason why this discussion was necessary to challenge a common opinion.

Consequently, my conclusion is: requirements of section B "Pulsed Current Injection (PCI) Test Procedures" of MIL-STD-188-125-1 are not suitable for testing civil electronic equipment by supplying test pulses to its input and output terminals. Thus, these tests should be excluded from the

testing schedule of this equipment to HEMP-resilience. Industrial electronic equipment, meeting the requirements of standards on electromagnetic compatibility, will also be resilient to current pulse flowing through additional input-placed transient suppression protecting elements upon HEMP impact, and thus requires no additional tests to be carried out on special testing equipment stipulated by MIL-STD-188-125-1.

Problem 7. The inability to consider the specific conditions in which thousands of specific types of equipment are located: types of buildings; the location of rooms with interior equipment; the presence of windows; cables, their length, depth in the soil; specific soil properties (which, moreover, change significantly depending on weather conditions), etc. Specifically, the inability to consider the weakening properties of the environment surrounding the equipment in order to assess what additional protective equipment and with what properties are needed. There are thousands of options here.

4. AUTHOR's STRATEGY

From the foregoing, we can conclude that military strategies, means and technologies for protecting against HEMP are too expensive for the civilian sector, and suitable strategies and technologies for the civilian sector simply do not exist now. Therefore, a new absolute different strategy and means are required for the protection of the civilian infrastructure.

The main principles of the author's strategy:

- *It is fundamentally impossible to formulate clear technical requirements for HEMP protection of equipment that would be universal for all types of civilian facilities and equipment;*
- *it is impossible to ensure absolute protection for every piece of electronic equipment employed at civilian critical facilities;*
- *any available level of protection which can attenuate (at least partially) HEMP impact on electronic and electrical equipment is useful for civilian critical infrastructure.*
- *The cost of protection devices budgeted during the design stage (in case of new equipment and facilities) will be much lower compared to upgrading the existing equipment.*
- *Due to technical and economic reasons, protection should only be provided to the most important (critical) types of electronic equipment installed at critical facilities of the power industry, rather than to any and all types of equipment employed at the power industry.*
- *Critical types may include equipment which is directly involved in electrical energy generation and transmission, as well as main types of relay protection, control and automation systems, AC and DC power supply systems.*
- *Consequently, measuring systems, communication (but not telecommunications used by digital relay protection devices), remote control and remote signaling systems do not belong to equipment without which temporary generation and distribution of electrical energy will be hampered in emergency situations.*
- *HEMP protection of equipment is multi-layered:*
  - *The first (top) layer includes protected buildings and structures.*
  - *The second layer includes protected rooms (halls) where equipment is installed.*
  - *The third layer includes protected cabinets with electronic equipment.*

- *The fourth layer includes protection input and output terminals of the equipment itself placed into control cabinets.*
- *Some additional "layers" of protection may include means for attenuation electromagnetic interferences penetrating into the equipment through the input and output cables (grounding, control and power).*

However, the use of all these "layers" in any situation is not feasible. In some cases, it is feasible to use just some of the "layers" in various combinations.

- *Instead of protecting specific types of employed electronic equipment, it is sometimes feasible to use back-up equipment of the same type stored in a metal container directly at the facility being protected.*

- *Existing HEMP-simulating test benches provide insufficient information at immunity testing of the power system's electronic equipment and thus testing such equipment (e.g. each cabinet with electronic equipment) on such test-benches is not feasible.*

In other words, the **general strategy** should be based on maximum use of maximum amount of known nonmilitary protection means (selected based on the above-mentioned strategy), with restrictions to be determined by technical and economic capabilities of a specific infrastructure object, only because any level of protection which can attenuate (at least partially) HEMP impact on electronic equipment is useful.

5. SOLUTIONS FROM THE AUTHOR

In accordance with the specific strategy for the protection of civilian infrastructure previously proposed by the author, he also developed specific means of protection, which are installed in trial operation and have already been tested in real operation during 2 – 3 years.

On Fig. 22 shows special HEMP filters intended for installation in current and voltage circuits of microprocessor-based protection relays.

Fig. 22. Special HEMP filters designed by author for installation in current and voltage circuits of microprocessor-based protection relays

In the group of these filters, there are also constructions intended to be inserting in the grounding circuits of the control cabinet and protection relays that do not violate the safety requirements for grounding circuits. These filters are designed to limit the influence of voltages induced in the grounding system under the action of HEMP.

Some filters are designed to be included in the power supply circuits of microprocessor-based protection relays inside the control cabinet, Fig. 23.

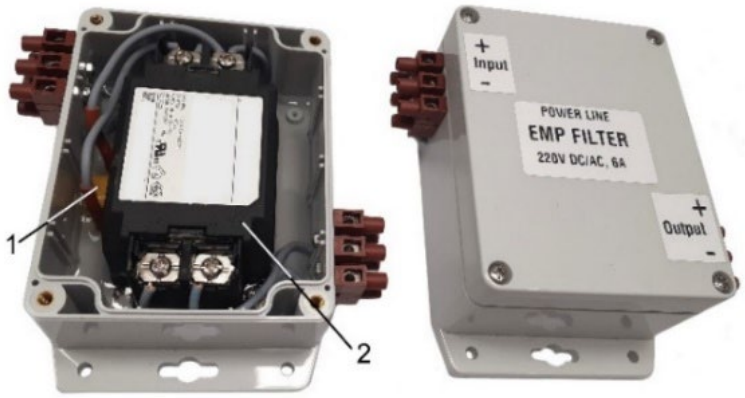


Fig. 23. HEMP power line filter for microprocessor-based protection relays inside the control cabinet. 1 – special high-efficiency surge arrester; 2 – electromagnetic two stage filter.

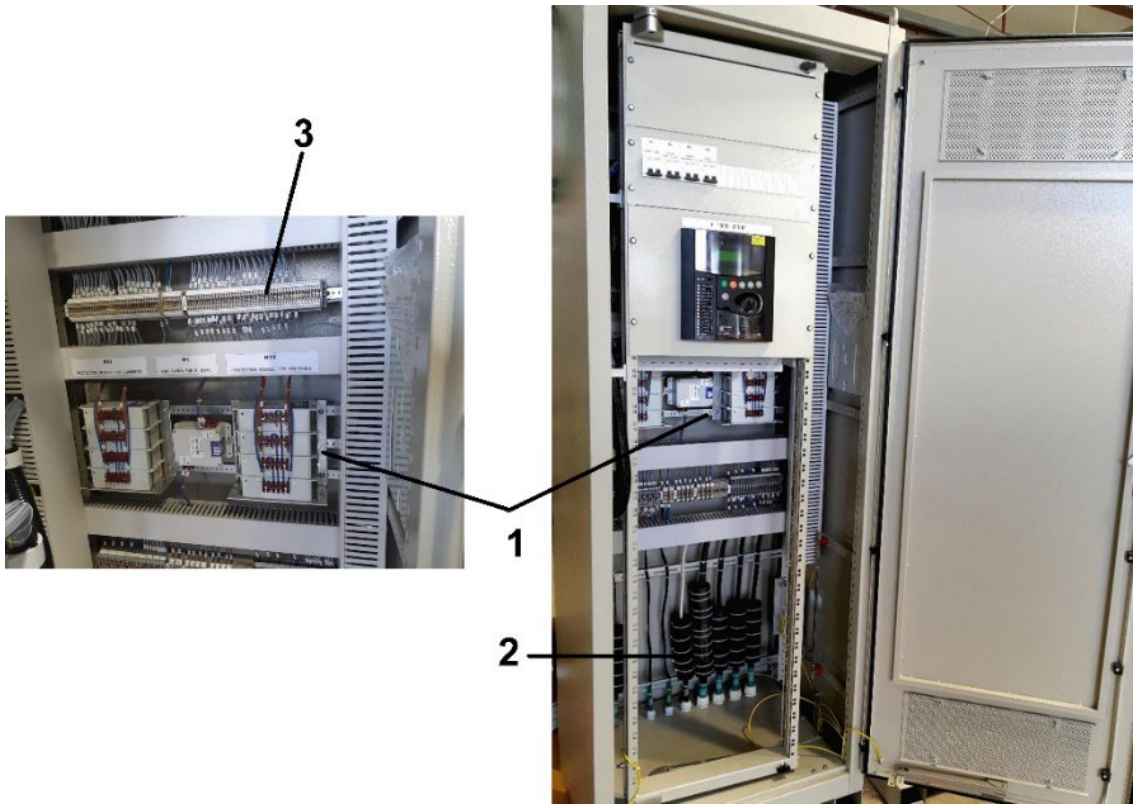


Fig. 24. Complete control cabinet with a microprocessor-based protection relay, filters and DIN-rail surge arresters. 1 - described above filters; 2 – addition filters; 3 – special surge arresters

A prototype of the control cabinet with a microprocessor-based protection relay, equipped with filters and special surge arresters, is shown in Fig. 24.

For high-power transformers of all voltage classes, the author has developed a new protection system that consist a set of small and inexpensive components, Fig. 25, as well as a simple device for periodic monitoring of the serviceability of this system during exploitation, Fig. 26.

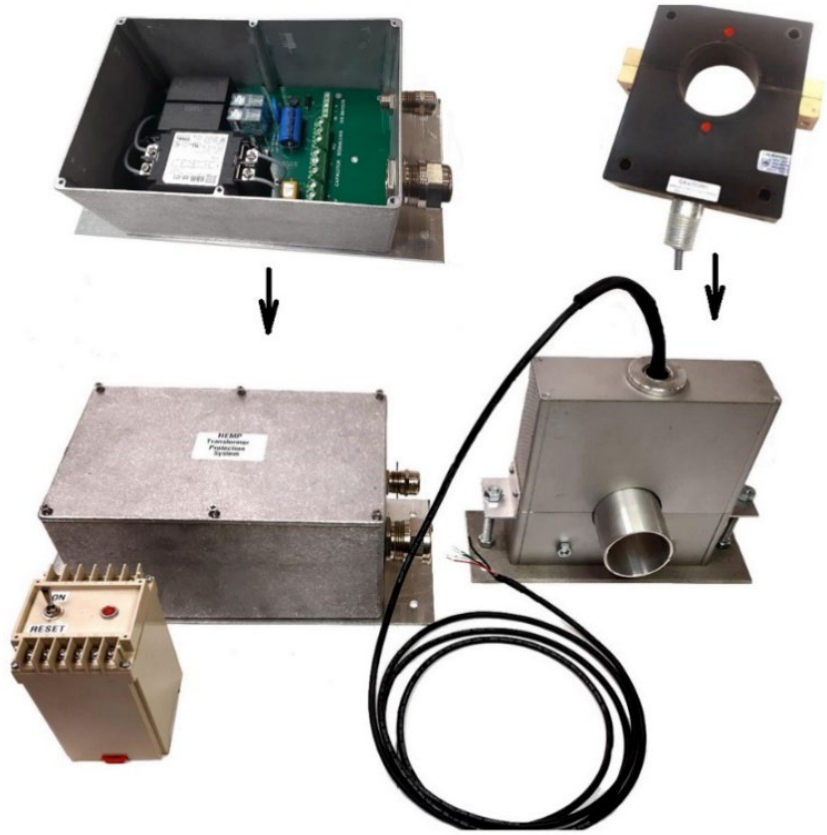


Fig. 25. Simple system for protection of high-power transformer against E3 component of HEMP

Fig. 26. Simple E3 component simulator for testing serviceability of the system for protection of high-power transformer

As known, for the operation of electronic systems of critical infrastructure, an extensive DC power auxiliary supply system is used, including large accumulator batteries and chargers. To ensure the operability of this system, the author has developed three different devices. The first of these is an automatic charger that maintains the batteries in good condition when the charger is damaged under the HEMP action, Fig. 27. This device constantly monitors the serviceability of the main charger and automatically turns on in case of damage of the main charger.

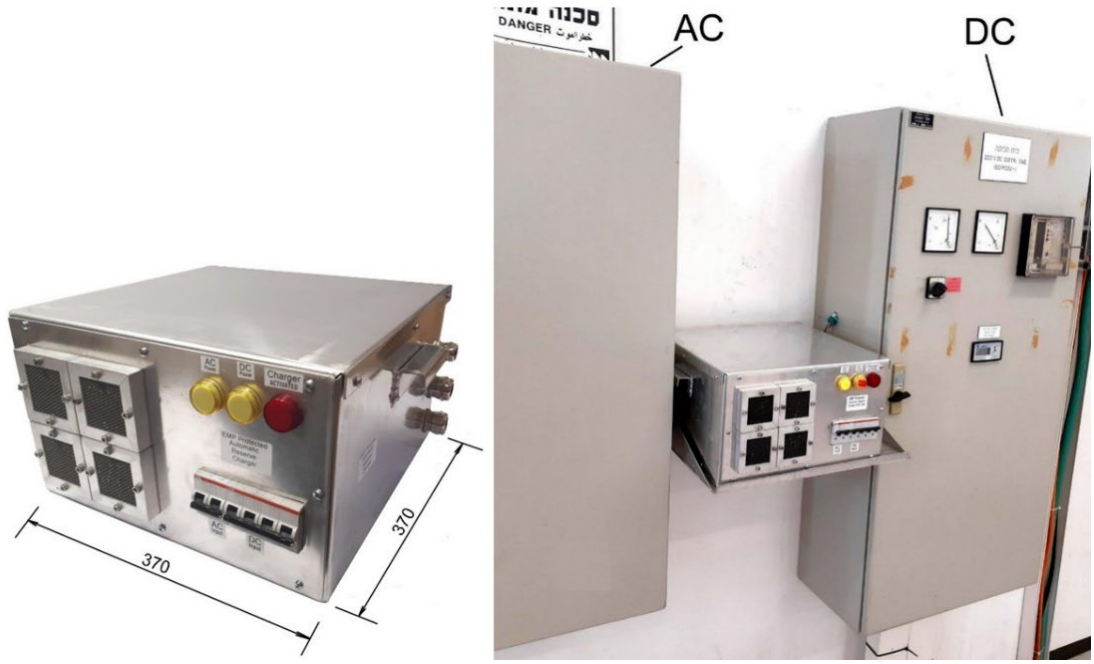


Fig. 27. Automatic HEMP protected charger for auxiliary DC power supply systems of critical infrastructures

Unfortunately, sometimes damage to the charger does not lead to the disappearance of its output voltage, but on the contrary, in the supply of too high voltage to the auxiliary power supply system of electronic equipment. For example, instead of the usual voltage of 237 V in the power supply system, such a damaged charger can produce a voltage of 260 - 270 V, which is dangerous for both electronic equipment and battery.

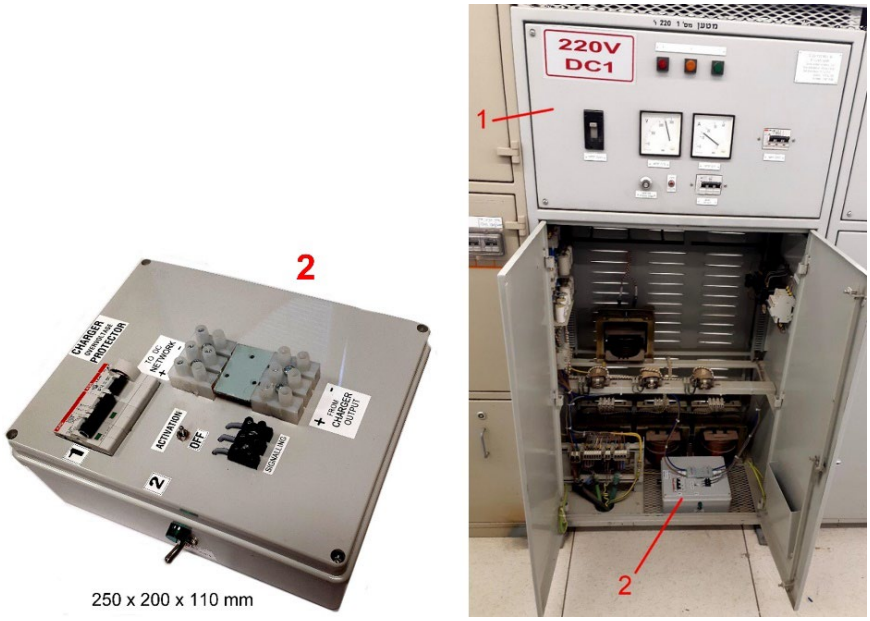


Fig. 28. Charger disconnection module

To prevent such a mode of the charger when it is damaged, the author has developed a small protective module that automatically disconnects such a damaged charger from the DC auxiliary

supply network, Fig. 28. This module is also protected from the effects of HEMP. Such a module can be combined in a common design with the automatic charger described above.

Fig. 29. HEMP protected backup power supply for electronic equipment testing after HEMP impact

Automatic chargers will not be installed everywhere. And after exposure to HEMP, there is a need to check the serviceability of electronic equipment before actuating. To do this, we need a power supply that simulates a conventional auxiliary DC power system. Such a backup power supply-simulator protected from HEMP is shown in Fig. 29.

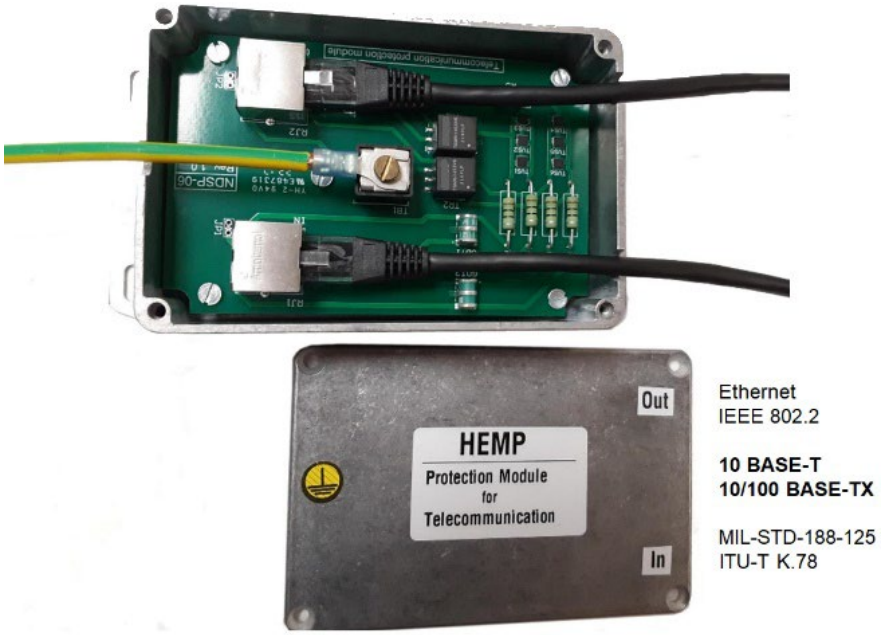


Fig. 30. HEMP protection module for telecommunications

Telecommunications are widely used in relay protection systems and other important systems at substations, power stations, and water supply systems. As a rule, it is based on 10 Base-T and 10/100

Base-TX Ethernet. This is the most vulnerable part of the infrastructure, which requires special high-effective protection. Moreover, such protection should not affect the work of telecommunication. Such a protective module was developed by the author, Fig. 30, and tested for compliance with standard ITU K.78 [18].

Another important type of electrical equipment at critical infrastructure facilities is uninterruptible power supply units (UPS). To protect such type of electrical equipment, the author has developed a protection system, Fig. 31.

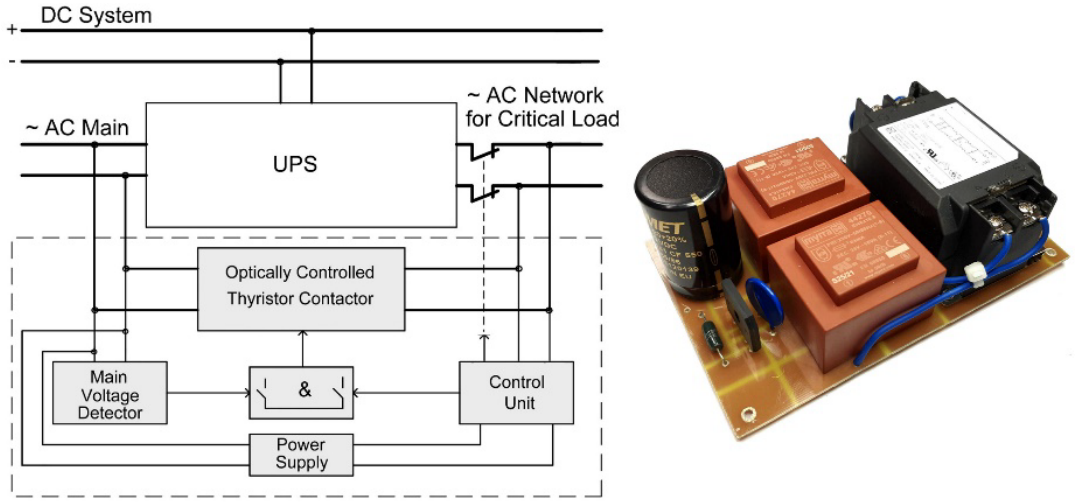


Fig. 31. UPS protection system and it's voltage detector

Unfortunately, not all UPS units will be protected at critical infrastructure facilities, but only the most important of them. For the rest of the UPS, a special tester (Fig. 32) has been developed that allows to very easily and quickly determine the serviceability of the UPS units, exposed to HEMP.

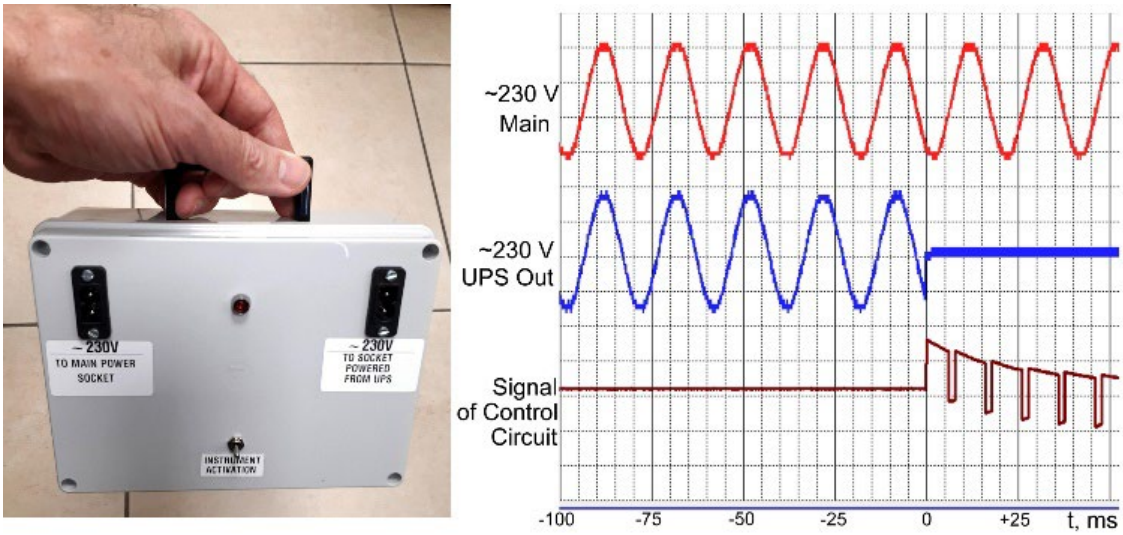


Fig. 32. Simple tester for express verification of the serviceability of the UPS unit after the HEMP impact.

Modern diesel generators with a capacity of 500 kW and above are often used as a backup power source at critical infrastructure facilities. Such diesel generators have a powerful electronic controller that controls all modes of operation of the diesel generator.

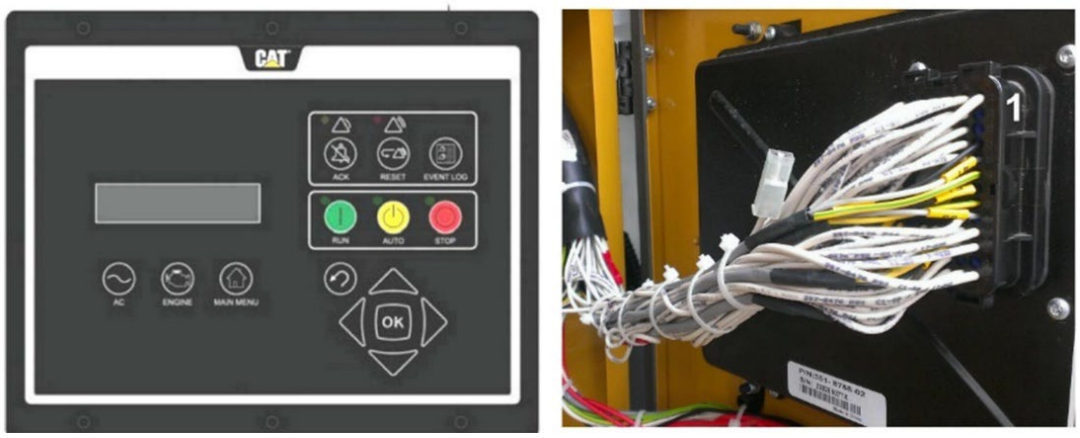


Fig. 33. Main controller of diesel generator

If this controller is damaged, the diesel generator cannot be started and operated. Moreover, this controller is made absolutely unprotected and dozens of wires are connected to it that do not have electromagnetic shielding, Fig. 33. Such a “backup power supply” of critical infrastructure is not really such, since it will be disabled immediately when exposed to HEMP.

So, what to do?

For backup diesel generators, a solution was also found, Fig. 34, including protection against the penetration of the electromagnetic wave through the open frames of air cooling, as well as through the power wires of the internal charger, Fig. 34.

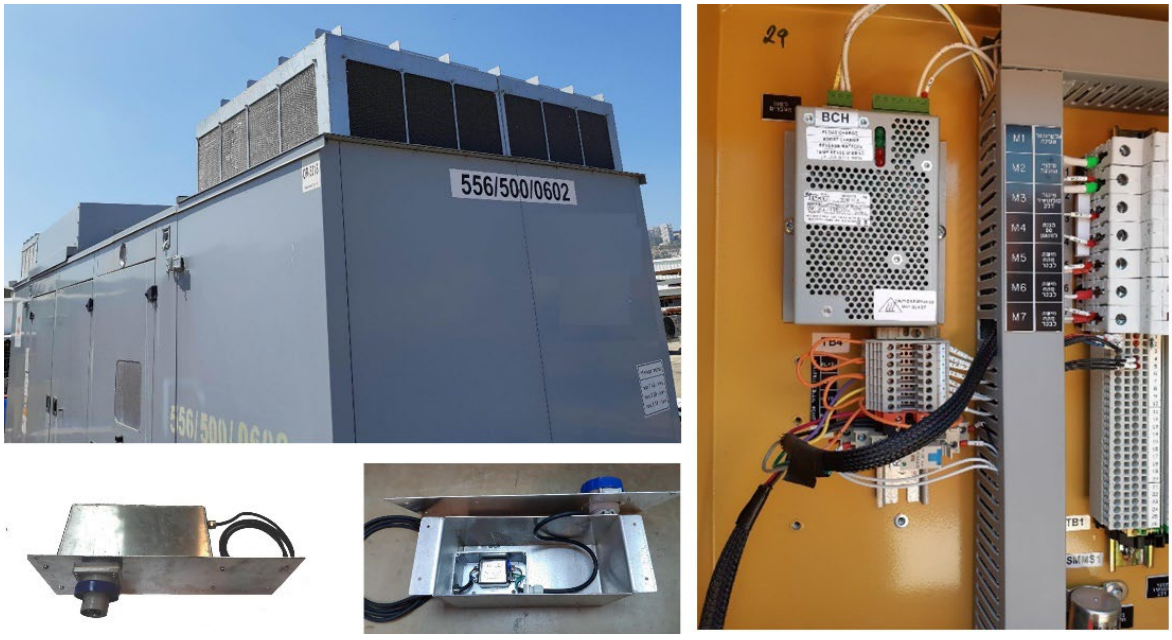


Fig. 34. Protection elements of the backup diesel generator, developed by the author.

The devices described above are designed specifically to protect critical civilian infrastructure, built by the author and tested. It remains only to start mass production of the developed means of protection.

KEY FINDINGS

1. The actual situation is such that the Army is not in a position to provide a sufficiently reliable defense of the civilian infrastructure facilities and population centers from HEMP and as such it is the electrical engineering specialists themselves that need to be concerned with this defense ahead of time.
2. The HEMP parameters affecting civilian infrastructure equipment depend on so many factors that they should be considered as uncertain.
3. The difference in the constructions, properties and characteristics of various types of civilian equipment used in critical infrastructure facilities, their different location inside the buildings, the differences in the buildings themselves, the presence of long cables connecting different types of equipment, make their levels of resilience to HEMP (and therefore the required levels of their protection) completely uncertain.
4. The real level of HEMP protection and the real level of resilience will be determined by the technical and economic capabilities allocated for a particular infrastructure. But, based on paragraphs 1 and 2, it follows that any level of protection is desirable and any level of resilience increases the resistance of critical infrastructure to HEMP. Naturally, with this approach, some of the equipment may be damaged when exposed to HEMP, but most of the equipment will remain in good condition and will be able to continue to function. The more protective means is installed on a particular infrastructure object, the higher its degree of protection will be. This approach to the problem differs significantly from the requirements for military equipment.
5. Military standards should not be used to determine the requirements for the level of protection of civilian infrastructure equipment.
6. The numerous HEMP protection means available on the market, made according to military standards, are not suitable for use in civilian equipment. For civilian equipment, other HEMP protection means should be used, such as those described in this brochure.
7. For civilian infrastructure, it is necessary to use a completely different strategy and different principles of protection than for military equipment. Such a strategy and such methods of protection are described in this brochure.
8. The most common types of test benches - EMP simulators (guided-wave type) designed for testing military equipment according to military standards, are not suitable for testing civilian equipment. Therefore (and on the basis of paragraphs 1 and 2 above), it can be concluded that there is no point in such tests at all and no significant conclusions can be drawn from the results of such tests.
9. The transition to fiber optical communication lines for the transmission of telecommunication commands between cabinets with electronic equipment is not a panacea and, in some cases, only exacerbates the situation.
10. To the frequently asked question: "*Is it possible to consider an infrastructure object completely protected from HEMP if the recommendations described above are followed?*" - the answer is NO! But it can be assumed that this object will be much more resistant to HEMR, and the probability of its damage will be much lower.

REFERENCES

[1] Gurevich V. Cyber and Electromagnetic Threats in Modern Relay Protection. – CRC Press, 2015, 205 p.
[2] Gurevich V. Protection of Substation Critical Equipment Against Intentional Electromagnetic Threats. – Wiley, 2017, 228 p.
[3] Gurevich V. EMP and Its Impact on Electrical Power System: Standards and Reports. - "International Journal of Research and Innovation in Applied Science (IJRIAS)", 2016, Vol I, Issue VI, pp. 5 – 10.
[4] Gurevich V. Protecting Electrical Equipment: GOOD Practices for Preventing High Altitude Electromagnetic Pulse Impacts. – De Gruyter, 2019, 386 p.

[5] Gurevich V. Protecting Electrical Equipment: NEW Practices for Preventing High Altitude Electromagnetic Pulse Impacts. – De Gruyter, 2021, 204 p.
[6] Gurevich V. Nuclear Electromagnetic Pulse: Practical Guide for Protection of Critical Infrastructure. – Lambert Academic Publisher, 2023, 462 p.
[7] MIL-STD-188-125-1 High –Altitude Electromagnetic Pulse (HEMP) Protection for Ground Based C^4I Facilities Performing Critical. Time-Urgent Mission. Part 1 Fixed Facilities, 2005.
[8] Electromagnetic Pulse (EMP) Protection and Resilience Guidelines for Critical Infrastructure and Equipment. National Cybersecurity and Communications Integration Center, Arlington, Virginia, 2019.
[9] Kukjoo K. at al. Development of Decision-Making Factors to Determine EMP Protection Level: A Case Study of a Brigade-Level EMP Protection Facility. - Applied Science, 2021, No. 11, 2921. MDPI.
[10] IEC 61000-2-9 Electromagnetic compatibility (EMC) - Part 2: Environment - Section 9: Description of HEMP environment - Radiated disturbance. Basic EMC publication, 1996.
[11] Technical Report LLNL-TR-741344, Lawrence Livermore national Laboratory, 2017.
[12] MIL-STD-461G. Requirements for the Control of Electromagnetic Interference Characteristics of Subsystems and Equipment. Department of Defense, 2015.
[13] MIL-STD-2169B. High Altitude Electromagnetic Pulse (HEMP) Environmental. Department of Defense, 2012.
[14] Pry P. Russia: EMP Threat. The Russian Federation's Military Doctrine, Plans, and Capabilities for Electromagnetic Pulse (EMP) Attack. EMP Task Force on National and Homeland Security, 2021.
[15] Cui M. Numerical Simulation of the HEMP Environmental. - IEEE Transactions on Electromagnetic Compatibility, 2013, Vol. 55, No. 3.
[16] Smith K., at al. Numerical Fits for Estimating High-Altitude EMP from Unclassified Gamma Ray Pulse Sources. Metatech Technical Note, 1990.
[17] IEC 61000-4-25. Electromagnetic compatibility (EMC) Part 4-25: Testing and measurement techniques – HEMP immunity test methods for equipment and systems, 2002.
[18] ITU K.78. High Altitude Electromagnetic Pulse Immunity Guide for Telecommunication Centers. - International Telecommunication Union, 2016.