A new strategy is needed to solve the 50-year-old problem - EMP protection of critical civilian infrastructure

Dr. Vladimir Gurevich, Prof. Emeritus
Industrial EMP Solutions, CEO

Annotation: 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 article proposes new protection strategies and methods for the civilian sector.

Keywords: high-altitude electromagnetic pulse, EMP, HEMP, critical infrastructure, protection means

1. INTRODUCTION

The ability of the powerful electromagnetic pulse, generated upon the high-altitude electromagnetic pulse - HEMP (or simplified EMP) 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.

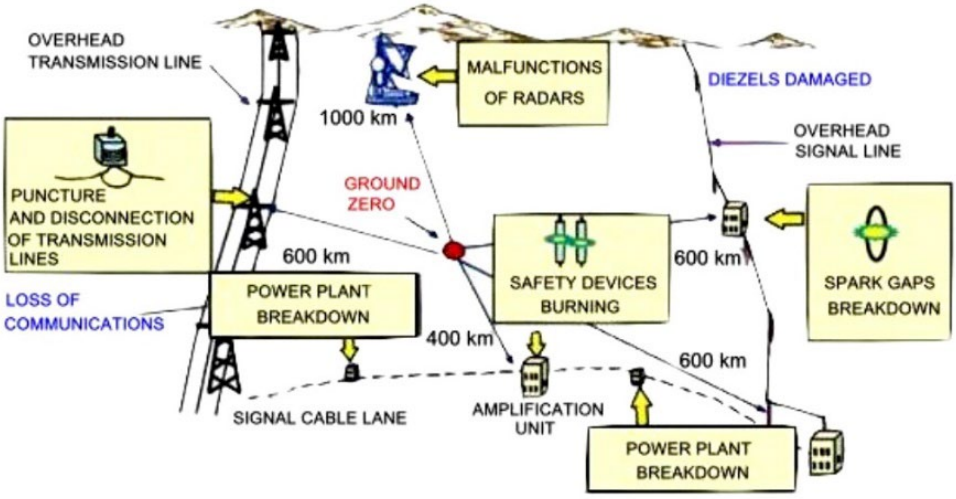

Fig. 1. Damaged electric equipment affected by HEMP during nuclear high-altitude test explosion performed under "K-3" project in Kazakhstan in 1962 (based on data published in V. M. Loborev's report presented at EUROEM International conference in France in 1994).

Additional experimental high altitude nuclear explosion named "K-3" was performed in the Soviet Union (at Kazakhstan, 180 km west of Dzhezkazgan town) on October 22, 1962 (300 kt yield, at altitude 290 km). According to data, published by V. M. Loborev [1], Fig. 1. EMP impact caused failures in the operation of Air Defense radar located about 1,000 km away. An underground power cable with a length of 1,000 km, passing at a depth of about 1 m and connecting towns Tselinograd and Alma-Ata, was put out of action. Breakdowns of ceramic insulators resulting in short-circuit were observed on 35 kV electric overhead power lines, in some areas. The insulators were so damaged that the wires fell to the

ground. Electromagnetic pulse caused fires due to short-circuit in electric appliances. A power generator which was connected to an underground power cable was knocked out of service at one of power plants in Karaganda town, relay protection (even old electromechanical type, not modern EMP sensitive microprocessor based!) was triggered resulting in switching the power generator off at another power plant. A slow geomagnetic component of EMP induced a short current pulse with an amplitude of several thousand Amps, as well as a long (more than 20 sec) current pulse, rated 4 Amps. This led to diesel-generator damage and triggering of protection devices mounted over a 570 km above-ground telephone line. There is also information about some breakages of electronic equipment, occurred at Baikonur Cosmodrome. At the same time, it should be taken into account that the level of electronics in the USSR in 1962 was incomparably lower than in the West today. That is, the breadth of application of electronics, its sensitivity (i.e., susceptibility to EMP) were incommensurate with today. If such a test were carried out today, it would lead to the complete collapse of a large part of the country.

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 EMP 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 [2, 3].

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 [4], as well as hundreds of articles and books. Dozens of standards (civilian and military) describe how to protect critical infrastructure equipment against HEMP [4].

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

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. 2?

And this is just one organization out of many dozens (more than 50!) "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…

1. OPINIONS

To date, we have four opposing concepts on the problem of protecting the civil critical infrastructure, which are reflected in the statements of the apologists of these three concepts [5]:

Concept 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

---

Concept 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

Concept 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)

Concept D: Effective defenses against HEMP are a national anti-missile defense system only into which more budgetary funds should be invested

Representatives of Military-Industrial Complex (MIC)

This last concept seems to be quite effective. After all, the military and representatives of the military-industrial complex should know this problem better than anyone else. But, let's understand this concept.

First, this concept, which was adopted by representatives of the military-industrial complex, would be quite understandable if the cost of developing and producing an effective multi-layer anti-missile shield that would protect the entire country would be lower than the cost of defensive measures to protect critical elements of the country's infrastructure and its systems against EMP. But this is not so, but quite the opposite!

Secondly, 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. 3.

Fig. 3. 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. 4. 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. 4.

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.

The lack of clear, understandable, technical-effective and cost-effective solutions to the problem of protecting civilian critical infrastructure, suitable for practical application (and not for scientific reports only) for more than 50 years, indicates the existence of a very serious problem.

2. THE PROBLEM

Today, indeed, there is all the data on how and how critical infrastructure can be protected. Therefore, no one does anything in practice to develop new protection means specially for civilian infrastructure. And why, if everything has long been known and the market is full of all kinds of protective equipment (EMP filters, shelters, etc.)? That is, everyone is right and everything is correct, but this does not prevent the situation that for 50 years not a single substation in the world has been protected as it should be (two substations in the United States, partially protected do not count).

Well, the problem exists or does not exist, that is the question?

In the previous section, the author points out the existence of a serious problem, and in this section, he writes that everything has been known for a long time and the market is full of protective equipment! The author only confused the situation and made it completely incomprehensible!

Alas, it is precisely such kind of confusion that exists in the protection of civilian infrastructure. After all, it is not for nothing that one of the leading experts in this field, Dr., Prof. Emeritus of James Madison University writes: "*The current state of EMP protection is random, disoriented and uncoordinated".*

But what is the reason for all this confusion and lack of solution to the problem for more than 50 years?!

The main and only problem is the attempts to use military technology to protect civilian critical infrastructure for all these 50 years.

The author argues that the well-known concepts of protection of military equipment and the means of protection against EMP available on the market, made according to military standards, are not suitable for the protection of civilian infrastructure.

But where is the way out of this paradoxical situation?

There can be **only one way out of this situation: the development of new protection strategy and new 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.

Unfortunately, it is not possible to describe within the framework of this article the problems that arise when trying to apply military technology to civilian equipment without resorting to very specific technical details and features of electronic and electrical equipment. But all these technical details are described by the author in [7] and are intended for technical specialists.

It is important to reiterate here that this is not only a question of new means of protection, but also of a new strategy for the protection of civilian infrastructure against EMP.

3. AUTHOR's STRATEGY

From the foregoing, we can conclude that suitable strategies and technologies intended for the civilian sector 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 (reviewed in detail and substantiated in [7] with all technical and scientific evidence) are:

- *It is fundamentally impossible to formulate clear technical requirements for EMP 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) EMP 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.*

- *EMP 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 EMP-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) EMP impact on electronic and electric equipment is useful.

4. SOLUTIONS FOR PROTECTIVE MEANS 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 several electrical substations during 2 – 3 years, Fig. 5.

Fig. 5. EMP protective means developed by author: power transformer protection, power main DC simulator, protection of control cabinets with electronic digital equipment, special EMP filters for civil equipment, automatic reserve EMP protected battery charger for electrical substations, Ethernet telecommunication protective module, and even protective means for high power backup diesel generators.

5. 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 EMP and as such it is the electrical engineering specialists themselves that need to be concerned with this defense ahead of time.
2. The EMP 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 EMP (and therefore the required levels of their protection) completely uncertain.

4. The real level of EMP protection and the real level of resilience will be determined by the technical and economic capabilities allocated for a particular infrastructure. But, based on research described in [7], it follows that any level of protection is desirable and any level of resilience increases the resistance of critical infrastructure to EMP. Naturally, with this approach, some of the equipment may be damaged when exposed to EMP, 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 EMP protection means available on the market, made according to military standards, are not suitable for use in civilian equipment. For civilian equipment, other EMP protection means should be used, such as those described in this article.
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 article.
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 [7]), 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 EMP 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 EMP, and the probability of its damage will be much lower.

6. EPILOGUE

It is quite obvious that one person, even such a specialist as the author of this publication, who has many years of experience in the field of EMP protection of civilian infrastructure, is physically unable to provide protection for an entire energy system, or a water supply company, communications system, large medical centers, banks, etc.

The country needs a production center that would be engaged in the development and production (and not research, consulting and "study of the problem"!) of protective means especially for civilian infrastructure. It can be a small manufacturing company or even a technical laboratory that develops protective equipment for civilian infrastructure, produces technical documentation, manufactures prototypes, tests them and orders their mass production at large manufacturing companies. 5 - 10 engineers and technicians under the guidance of an experienced specialist could finally solve a 50-year-old problem and ensure the protection of the country's infrastructure from nuclear EMP.

"… should not wait for the federal government to take action, we need to take action now to protect our portion of the grid."

David Gregory,
Chairman of the Special Committee on Government Accountability,
member of the Missouri House of Representatives

"The time for research is running out; we have the data we need. It's time for bold action"

R. James Woosley, former Director Central Intelligence Agency (CIA)

REFERENCES

[1] Loborev V. Up to Date State of the NEMP Problems and Topical Research Directions. - Electromagnetic Environments and Consequences: Proceedings of the EUROEM 94 International Symposium, Bordeaux, France, 30 May – 3 June 1994, pp. 15-21.

[2] Gurevich V. Cyber and Electromagnetic Threats in Modern Relay Protection. – CRC Press, 2015, 205 p.

[3] Gurevich V. Protection of Substation Critical Equipment Against Intentional Electromagnetic Threats. – Wiley, 2017, 228 p.

[4] 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.

[5] Gurevich V. Protecting Electrical Equipment: GOOD Practices for Preventing High Altitude Electromagnetic Pulse Impacts. – De Gruyter, 2019, 386 p.

[6] Gurevich V. Protecting Electrical Equipment: NEW Practices for Preventing High Altitude Electromagnetic Pulse Impacts. – De Gruyter, 2021, 204 p.

[7] Gurevich V. EMP Protection of Civilian Critical Infrastructure: Opinions, Problems, Strategy, Solutions. Third Edition. Haifa, 2023. (www.best-empsolutions.com/emp_prot_civil_infrastructure.PDF)