PROTECTION CIVILIAN INFRASTRUCTURE AGAINST HIGH ALTITUDE ELECTROMAGNETIC PULSE (HEMP): THE PROBLEMS AND STRATEGY

Vladimir Gurevich
•
Israel Electric Corp.
vladimir.gurevich@outlook.com

Abstract

Since the devastating effect of HEMP on electronics in the military field has been known for a long time, all military systems are equipped with efficient protection against the impact of HEMP. However, HEMP is equally dangerous for all civil electronics used in almost every section of today's most important infrastructure of any country, for instance the power industry. Therefore, the opinion that all technical problems have long been solved by the military and you just need to use their solutions and their experience in the civilian sector can be heard often. It is a very common and very dangerous illusion in the author opinion. The article describes the problems associated with the use of military technology in the civilian sector and proposes an author's strategy for protecting the civilian infrastructure.

Keywords: HEMP, electromagnetic pulse, electronic equipment, infrastructure protection, power industry, protection strategy

I. Introduction

The ability of the powerful electromagnetic pulse, generated upon the nuclear explosion at high altitude (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. This has been mentioned in all open sources, including booklets and recommendations on protection against the massive weapon distributed amongst the population during the "cold war" between the USA and the USSR. However, at that time only a few people understood. Not only average people, but also engineers and technicians working in power generation, electrical engineering and electronics, and even military specialists who are not experts in nuclear physics were not aware of the problem. Unfortunately, the situation has not changed a lot despite hundreds of reports, presentations, articles and books, as well as dozens of open military and civilian standards on this subject. At least in the USA this subject is in the spotlight of many dozens of organizations listed in [1], including numerous Congress Panels created especially for this. Many years have been spent

researching this subject which has been funded prevalently by the government. However, civil engineers working in the field of electrical power supply, water supply, sewage systems, telecommunication, banking, etc., are bewildered about this massive data so far.

But why?

II. The Problems

The problem is that all such numerous organizations which are fed on massaging the HEMP issue and periodically frightening the laymen with the fatal disaster resulting from the HEMP impact are not interested in an early solution to this issue and are discontinuing. Conversely, all of them are interested in keeping this problem afloat and continuation of prolonged funding. And the proposed specific technical solutions for protecting civilian infrastructure elements against HEMP encounter reluctance to even discuss these solutions, since, supposedly, all technical problems have long been resolved.

The opinion that all technical problems have long been solved by the military and you just need to use their solutions and their experience in the civilian sector can be heard often. Here is what Dr. George H. Baker, Prof. Emeritus James Madison University, Director Foundation for Resilient Societies says in his testimony before the Senate Homeland Security Committeein of Congress [2]:

> *"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."*

In his numerous publications Dr. Peter Vincent Pry, Executive Director of the Task Force on National and Homeland Security, has said the same thing many times:

> *"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".*

The same idea, but in different words, is repeated by Ambassador Henry F. Cooper, Chairman of High Frontier, and an acknowledged expert on strategic and space national security issues [3]:

> *"Moreover, I emphasized that we have the technical know-how to accomplish this objective; actually, have known how for decades but have not done so for political — not technical or financial reasons".*

Unfortunately, this is a very common and very dangerous illusion that is replicated by people who are very far from the real technical problems of the civil infrastructure sector. Instead of involving technical experts for solving technical problems, such statements only replicate empty talks and delay the practical solutions of the problem. It is clear that the more such empty talk and the fewer specific technical solutions suitable for the civilian sector, the longer the problem will remain afloat and the more money can be obtained for this problem.

Why military HEMP protection means are not suitable for the civilian sector?

There are several very important problems and 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 power generation industry. Such cabinets, sometimes overstuffed with apparatus, have dozens of inputs and output multicore cables and each separate core requires protection. Who will do it?

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 enough 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 power generation industry, it is hardly possible to find two identical cabinets with electronics having absolutely identical internal wiring. Since at HEMP frequencies range (100 kHz to 100 MHz) the minor change of wire length, even to 20 cm - 30 cm, or in its placement inside the cabinet, results in a dramatic change of cabinet internal apparatus vulnerability to HEMP (Gurevich, V., 2021), a typical test model 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 [1] and [4] it is not feasible to conduct such tests for this type of equipment. The data presented in [1] regarding the resilience of 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.

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). According to MIL-STD -188-125-1 such means must ensure at least 80 dB attenuation of an electromagnetic interference in the frequency range up to 1 GHz. Many manufacturers want to be holier than the Pope and offer on the market HEMP filters with parameters that exceed the requirements of this standard. For example, the typical attenuation features of HEMP filters described in ETS-Lindgren's promotion materials reach 100 dB in the frequency range up to 40 GHz, and this despite the fact that 96% of the total HEMP energy is released in the frequency range up to 100 MHz (in accordance with the standard IEC 61000-2-9). It is clear why a such low power filter (for example LRX-2005-52 type, for a current of 5A) of this company has dimensions of 940 x 229 x 127 mm and a weight of more than 27 kg. Similar parameters are available for filters from other manufacturers. The costs $US 1,500-2,500 worsen the situation. Does anyone really believe that civil power engineering 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) (*Electromagnetic Pulse (EMP) Protection and Resilience Guidelines*, 2019). From the presented data, 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.

Such conclusion is also confirmed in [5], where it is shown that even for military equipment, the requirements of the basic standard MIL-STD-188-125 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."*

So, what to say about civilian equipment?!

Problem 4. This problem is related to the test benches simulating HEMP.

Within such a test bench like the guided-wave type HEMP simulator 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. 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 internal electronic circuit (i.e. connected directly to the antenna bottom part), the test bench pulse impact on such a cabinet will differ from the real HEMP, since it will not be related to Earth potential in any way.

One another 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 and delivering it directly to the sensitive electronics inside the cabinets. How can such long cables be modeled on a compact test bench (the above image on Fig. 1.4 shows one of the very big benches not available in every country)?

As shown in [1], [4] most existing test benches are of little help for testing cabinet-type equipment, which is used in the civil power industry and the results of these tests are illogical.

Problem 5. Despite a large number of civil and military standards, including the still classified standard [6], 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 equipment. But in fact, this field strength can be completely different, both much more (100 kV/m for Super-EMP) and much less (5 – 10 kV/m for some environmental).

Table 1: *Electric field peak value distributed on the ground from a 100 km height of burst (HOB), 1Mt yield burst [7].*

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

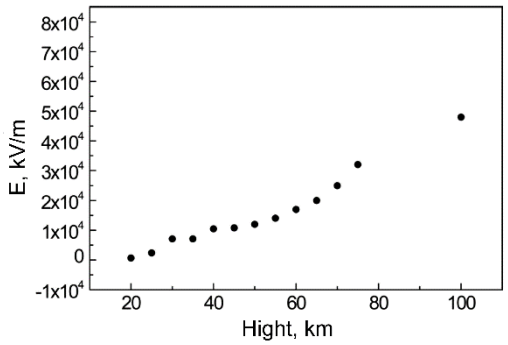

Figure 1: *Changes of the electric field intensity at different heights of burst over the explosion center for 1Mt yield [7].*

In Table. 1 in Fig. 1. shows 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"* [7].

As can be seen, unpredictable variations in the intensity of HEMP exposure to equipment are possible over a very wide range.

Problem 6. 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 equipment inside them; the presence of windows; cables, their length, depth in the soil; specific soil properties (which, moreover, change significantly depending on weather conditions), etc. That is, 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.

This raises a very important question regarding assessment of efficiency of applied protection measures and protection means. In this situation I rely on three rationales:

- it is fundamentally impossible to formulate clear technical requirements for HEMP protection of equipment that would be universal for all types of civilian equipment;
- it is impossible to ensure absolute protection for every piece of electronic equipment employed at power facilities;
- any level of protection which can attenuate (at least partially) HEMP impact on electronic equipment is useful.

Based on this, the general strategy should be based on ***maximum use of maximum amount of known protection means with restrictions to be determined by technical and economic capabilities of specific power system only.***

This approach makes testing of complete protected equipment on simulation test benches absolutely senseless, even if we forget about downsides of guided wave-type simulators. Nevertheless, some tests are necessary and important. They include testing of specific means (elements) selected for protection, such as varistors, filters, cabinets, cables, etc. The purpose of these tests is to check parameters declared by the manufacturer and to select the most efficient protection elements from the diversity offered in the market. These tests can be performed using generally accessible instruments, manufactured by companies described in [1].

All these problems have been detailed in my previous books on this subject [1], [4].

But what is the status in terms of drawing the government's and society's attention to this problem? Just as bad as in terms of technical problems! US bureaucrats and officials have managed to convert the renowned Directive of former President D. Trump "Executive Order on Coordinating National Resilience to Electromagnetic Pulses" into another example of bureaucratic sophistry and verbosity. It was detailed in my previous book [1]. As a consequence, nothing essential was made in this regard, and "*the current state of EMP protection is random, disoriented and uncoordinated*", - according to Dr. George H. Baker, Prof. Emeritus James Madison University. Regarding that situation, there is a big range of views amongst different specialists in this field, including the very opposite ones [1]. For example, Dr. Peter Vincent Pry, Executive Director of the Task Force on National and Homeland Security mentions: "*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*". However, other experts take great issue with it. "*I don't think we have an illusion we will prevent it. That's really the government's job*", - says Mike

Bryson, Vice president of operations for the Valley Forge, Pennsylvania-based operator. His words are echoed by another representative of the US electrical energy sector, Richard Mroz, President of the New Jersey Board of Public Utilities: "*Managing that kind of threat right now — no one really has the resources to do that*" [1]. General M. V. Hayden, Ex-Director of the National Security Agency (NSA), Ex-Director of the Central Intelligence Agency (CIA) sums up: "*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*" [1].

"*…leave it at that*"? So, let us forget and do nothing... Brilliant strategy, isn't it? Nonetheless, the developers of the new weaponry from all countries clearly understand the chosen strategy and the present situation and relentlessly work on the new electromagnetic weapon types, including a super-EMP bomb – nuclear explosive with a manifold magnification of pulsed electromagnetic radiation, while understanding that there is no protection against it and it will not be available in the near future.

It should be noted here that opponents to any measures on protection of infrastructure against HEMP often say that such protection does not make sense, since any nuclear explosion initiated by any side will immediately result in a massive attack with all nuclear weaponry and a single electromagnetic pulse will be meaningless. In fact, this is not true. Recently, nuclear weapon strategy and tactics have evolved. It is not just a strategic deterrent weapon anymore. For example, there are programs on creating new tiny nuclear warheads for tactical cannon shots actively developed in many countries. Here it should be noted that in order to generate a powerful EMP, the nuclear warhead must be activated at a high altitude (more than 30 km), therefore such a warhead is not a mass lethal weapon. This fact should be deemed as an important motivation to apply such weapons. If the weapon will cause no direct human losses, the opponent will hardly initiate the regular overland nuclear attack resulting in millions of deaths. The response will likely be symmetric. That is why it is very important to protect the infrastructure against HEMP, and this problem will evolve over time.

Digital protective relays and automatic control systems built on microprocessors, distributed power generation controlled with the artificial intelligence devices, digital substations, etc., all these great and most advanced systems are particularly vulnerable to HEMP. A very dangerous modern phenomenon in the electrical power industry called "digital substation" should be mentioned here. No, of course, it is not dangerous in itself, but in the way it is "implanted" into the power electrical industry. However, no threats stop the digital substation apologists. The development and implementation of artificial intelligence systems in the electric power industry continues without any limitations and without regard to the increasing significantly vulnerability of the electric power industry to HEMP with such development trends. Thus, the modern electrical power industry's development tendency is accompanied by its increasing vulnerability. Is it progress? There is rather a strange situation – while everyone is concerned with the cyber security of today's civil electrical power industry, no one thinks about its protection against HEMP. This position of the leading power engineering experts, and all-around appeals to fasten the power engineering sector digitalization by any and all means, without any consideration of the problem or intention to simultaneously develop measures on protection of all those digital technologies against HEMP, are hair-raising.

However, this does not eliminate the need to search for and select the most effective means of protection of the civilian infrastructure from those offered on the market, which have the best price-performance ratio.

Despite the seemingly routine and simplicity of the problem, for a number of reasons this becomes a very difficult task in this specific field of technology. One of the problems is that civilian sectors of the economy have not yet started real work anywhere in the world to protect civilian infrastructure from HEMP, and therefore these sectors are not consumers of protective equipment. For this reason, manufacturers of this protective equipment are primarily focused on military orders and produce products according to military standards that meet the requirements of the military. As a result, the means of protection offered on the market today have parameters

that are excessively high for the needs of civilian infrastructure and, accordingly, a high cost that is completely unacceptable for civilian needs. Specifically, even if in some country, in some sector of the economy, they decide to deal with the problem of protection against HEMP, they will not find anything suitable on the market.

In this regard, the only solution may be to conduct research and development of protective equipment specifically designed for civilian infrastructure with the new strategies and methods for their application. It can be stated that today these tasks have not yet been solved, and numerous reports and recommendations published by dozens of organizations are too vague, not specific, and do not help to solve the problem of protecting civilian infrastructure. They create only a background noise and the illusion that all technical problems have already been resolved and it is only a matter of government decisions.

It is a pity that the authors of the report do not understand that the most important for protection against HEMP parameters of "*thousands of diverse infrastructure installations*"[8], are not determined in fact and any "*EMP-related intelligence gathering*" not will help here.

III. The 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 this strategy:

- It is impossible to ensure protection of any and all types of electronic equipment in the power systems.
- It is impossible to ensure absolute protection even for the most important types of equipment being used.
- 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.
- 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 power system's electronic equipment and thus testing such equipment (e.g. each cabinet with electronic equipment) on such test-benches is not feasible.
- 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.

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 power system, only because any level of protection which can attenuate (at least partially) HEMP impact on electronic equipment is useful.**

References

[1] Gurevich V. Protecting Electrical Equipment: GOOD Practices for Preventing High Altitude Electromagnetic Pulse Impacts. DeGruyter, Berlin, 2019, 386 pp.

[2] Testimony of Dr. George H. Baker before the Senate Homeland Security Committee. *Senate Committee on Homeland Security and Governmental Affairs, February* 27, 2019.

[3] Cooper H. F. Will Biden Improve Trump's Cyber and EMP Initiatives? – *NewsMax*, 29 January 2021.

[4] Gurevich V. "Protecting Electrical Equipment: NEW Practices for Preventing High Altitude Electromagnetic Pulse Impacts. DeGruyter, Berlin, 2021, 204 pp.

[5] Kukjoo, K, at al, 2021. "Development of Decision-Making Factors to Determine EMP Protection Level: A Case Study of a Brigade-Level EMP Protection Facility". *Applied Science,* No. 11, 2921. MDPI.

[6] MIL-STD-2169B, 2012. High Altitude Electromagnetic Pulse (HEMP) Environmental.

[7] Cui, M., 2013. "Numerical Simulation of the HEMP Environmental". *IEEE Transactions on Electromagnetic Compatibility, Vol. 55, No. 3, June 2013.*

[8] Electromagnetic Pulse (EMP) Protection and Resilience Guidelines for Critical Infrastructure and Equipment. National Cybersecurity and Communications Integration Center, Arlington, Virginia, 2019.