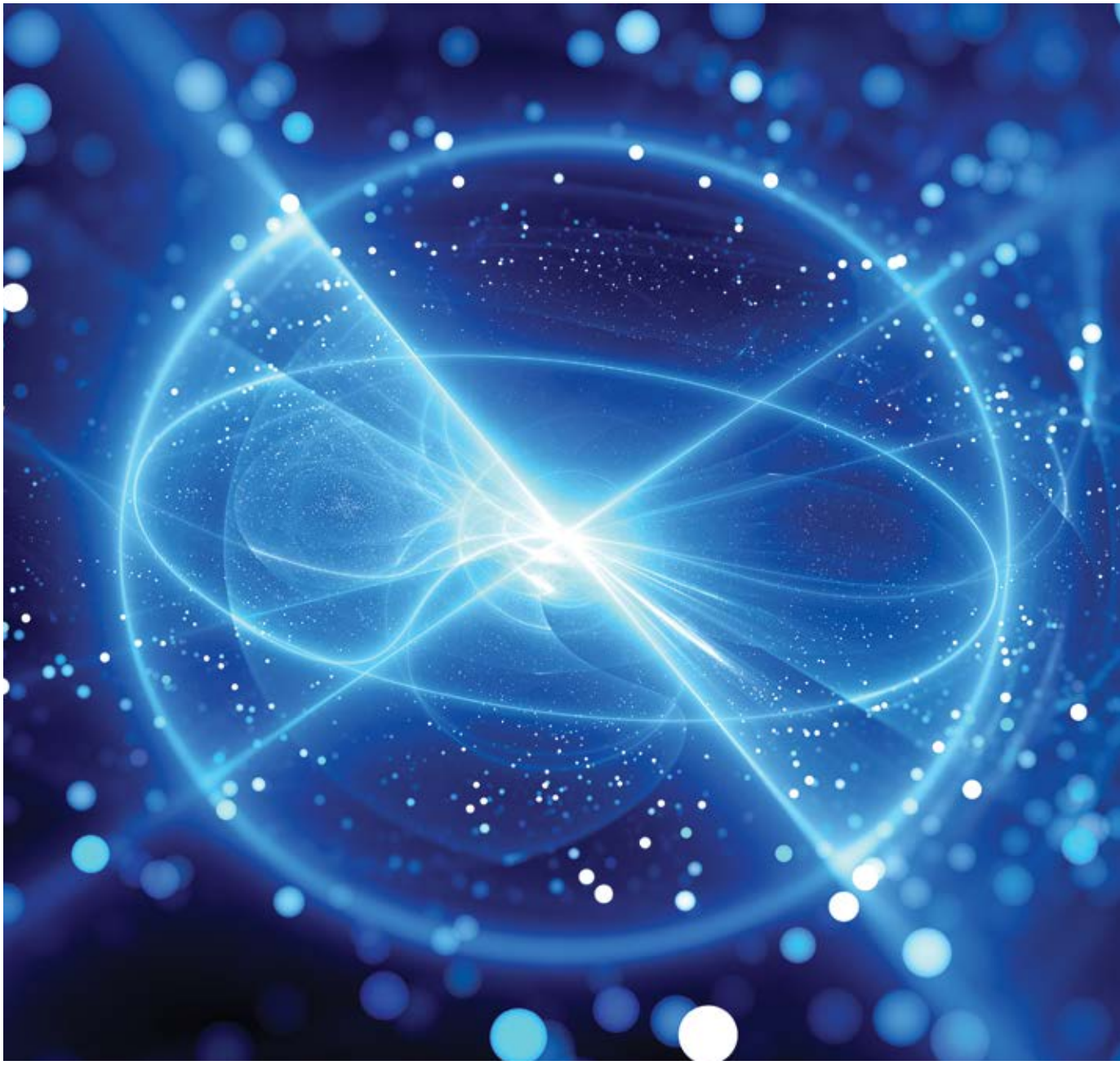
ADDRESSING THE GLOBAL THREAT OF EMP EVENTS

The Impact on Business and Life as We Know It

By Michael Caruso, Janet O'Neil and Bob Piemonte



Maintaining the resilience of all critical infrastructure segments, including the electric grid, sensitive data centers and vital communication channels, has become a growing concern globally as electromagnetic pulse (EMP) events continue to threaten society and the operation of business and life as we know it. EMP events include high altitude electromagnetic pulse (HEMP) and intentional electromagnetic interference (IEMI). HEMP can occur from a nuclear weapon being detonated in outer space (higher than 29 kilometers/18 miles). IEMI threats can easily be created by terrorists and criminals utilizing high power electromagnetic weapons to attack power system assets.

In Europe, the STRUCTURES and SECRET consortiums have been formed to address EMP events. SECRET [1] addresses the security of railways against electromagnetic attacks. STRUCTURES [2] classifies IEMI threats according to their availability, their technical characteristics (such as bandwidth) and their portability. Critical infrastructures are identified and their most characteristic aspects are addressed.

In the United States concern over protection against EMP events has been spearheaded by InfraGard, a partnership between the Federal Bureau of Investigation (FBI) and members of the private sector. EMP protection has become an especially high priority for electric utilities and financial institutions. As further evidence of the evolving concern over HEMP and IEMI (from this point jointly referred to as "EMP"), the White House signed the 2017 National Defense Authorization Act (NDAA) on December 23, 2016. The NDAA includes the complete language of H.R. 1073/S. 1846, Critical Infrastructure Protection Act (CIPA). The CIPA amends The Homeland Security Act of 2002 and addresses the need for electromagnetic pulse (EMP) and geomagnetic disturbance (GMD) protection of all 16 critical infrastructure segments.

GROWING GLOBAL CONCERN

Numerous experts have warned about the growing threat of EMP events. No longer is it a question of if it will happen, but when. In a recent issue of Financial Sense®, Dr. Peter Vincent Pry, executive director of the U.S. Congressional EMP Commission, discussed the potential of an EMP catastrophe and the danger inherent in being reliant on a constant source of power. "The very technological revolution that is feeding our prosperity is also making us more vulnerable," Pry said. "As electronics get smaller and faster, and operate on lower energy levels, they also become proportionally more vulnerable to EMPs."[3]

As noted in the article by F. Michael Maloof that appeared in WORLDNETDAILY, "Modern financial services utilities have transformed the national economy from a paper system into an electronic system," the [U.S. Congressional] EMP Commission said. "Examples of some key industry utilities include FEDNET, Fedwire, ACH, Clearing House Interbank Payments System (CHIPS), the Society for Worldwide Interbank Financial Telecommunications (SWIFT), the National Association of Securities Dealers' Automated Quotation System (NASDAQ), the NYSE (New York Stock Exchange), the New York Mercantile

Michael A. Caruso is an independent consultant, formerly Director, Government & Specialty Business Development for ETS-Lindgren. He is a recognized leader in the RF shielded enclosure/ EMP protection/anechoic test chamber industry with 33 years' experience in project management, engineering, technical applications and business development. Caruso has testified before the U.S. Congress on the need for EMP protection of the critical infrastructure. He can be reached at carusomi54@gmail.com.

Janet O'Neil is a customer relations specialist with ETS-Lindgren, and has over 30 years of experience in the RF microwave and electromagnetic compatibility (EMC) industries. She is a member of the Board of Directors of the IEEE Electromagnetic Compatibility (EMC) Society, and a member of Subcommittee 1 (Techniques and Development) of ANSI ASC C63®. O'Neil can be reached at janet.oneil@ets-lindgren.com.

Bob Piemonte is the Director of Government/General Purpose Shielding for ETS-Lindgren and coordinates the company's Building Information Modeling (BIM) manufacturing, engineering and project management teams. Piemonte has more than 30 years of experience in the engineering and installation of RF shielding systems, and can be reached at bob.piemonte@ets-lindgren.com.

Exchange (NYMEX) and the Depository Trust and Clearing Corporation (DTCC)." [4]

In a recent letter to investors, billionaire hedge-fund manager Paul Singer warned that an electromagnetic pulse, or EMP, is "the most significant threat" to the U.S. and its allies in the world. [5]

Contributor Kevin D. Freeman notes in his article published in TheBlaze, "World War III: The Coming Cyber-Financial Attack that will Shock America", that "every day, there are hacking attempts originating in Moscow, Beijing, and cities throughout the Middle East and North Korea."[6]

In other articles, Iran is reported to have endorsed a nuclear EMP attack on the United States [7] and two, preeminent U.S. national security experts explain how to prevent the worst damage from an EMP event. [8]

In short, financial institutions, countries and governments are becoming educated and aware of EMP threats.

CRITICAL INFRASTRUCTURE SEGMENTS IMPACTED BY THE 2017 NATIONAL DEFENSE AUTHORIZATION ACT

In May 2015, Dr. Pry, Dr. George Baker, Professor Emeritus at James Madison University and CEO of BAYCOR, and Michael Caruso from ETS-Lindgren testified in hearings before the U.S. Congress on CIPA H.R. 1073 that EMP protection is available and cost effective, and that several businesses have already voluntarily implemented this protection. [9] This testimony along with that of other experts provided the rationale and feasibility for enacting the CIPA. All 16 critical infrastructure segments are shown in Table 1 below. Any entity that is part of any one of these critical infrastructure segments is now required by law in the U.S. to address EMP protection of their facilities and services.

Several of these critical infrastructure segments are also included in the European STRUCTURES consortium scope of work.

EMP PROTECTION SYSTEMS

EMP protection systems typically involve radio frequency (RF) shielding of a structure's walls, ceiling

Power sources are especially vulnerable to EMP and IEMI events. The resulting indefinite loss of power and communication will be catastrophic to government and society.

Energy Sector (electricity, petroleum, and natural gas)
Defense Industrial Base Sector
Communications Sector
Healthcare and Public Health Sector
Emergency Services Sector
Water and Wastewater Systems Sector
Transportation Systems Sector
Food and Agriculture Sector
Information Technology Sector
Financial Services Sector
Nuclear Reactors, Materials, and Waste Sector
Chemical Sector
Commercial Facilities Sector
Critical Manufacturing Sector
Dams Sector
Government Facilities Sector

Table 1: Critical infrastructure segments in the U.S.

and floor as well as specialized penetrations to allow the protected transfer of power, air, water, cables, etc. into the shielded environment without degradation of shielding performance.

The RF shielding industry has provided EMP protection systems and services for over 30 years for government and military facilities. Over the past five years, industry leaders have designed and constructed EMP protected facilities for several Fortune 1,000 companies that have decided to develop command-and-control operations centers in support of their growing businesses. One of these companies required over 100,000 square-feet of their facility to be protected against an electromagnetic pulse.

It is critical that a recognized expert organization be heavily involved from project concept through completion, supporting the EMP infrastructure design for the company's data processing, system control, and data acquisition - all designed with a "concurrently maintainable model." This means that the facility design is capable of maintaining fully redundant infrastructure services while performing maintenance, without sacrificing backup system availability during any primary system's unplanned failures.

The various operations centers are self-dependent and maintain continuous operations with outside corporate facilities and data-generating equipment during emergencies, natural disasters, or other major disruptions. In addition, many of the designs included kitchens, showers, and offices that enabled continuous occupancy. These types of facilities are also designed to mirror other corporate data centers, providing back-up capabilities and rapid recovery due to any loss in the corporation's regional network.

EMP PROTECTION RECOMMENDATIONS

EMP protection of any critical infrastructure entity, whether related to the energy, defense or financial institution sectors, is not an easy task. Recognizing the growing need for EMP protection for the non-military/non-government critical infrastructure segments, the RF shielding industry has responded by developing innovative and cost-effective EMP protection solutions that meet and exceed the protection required by both MIL-STD-188-125 (versions 1&2) and current guidance of the IEC SC-

EMP and IEMI events threaten business as we know it by causing unrecoverable damage to data centers serving financial, public utility, and IT markets, among others.

77C Committee. Currently available EMP protection approaches include:

- An all welded on-site built solution. Considered the most expensive and time consuming solution, this application is generally reserved for government and military applications required to comply with the strictest requirements of MIL-STD-188-125 1&2. It is also an effective solution for portable or mobile EMP structures, such as those mounted on a flat-bed truck.
- A more conventional type modular bolt-together, hardness critical item (HCI) certified system designed to be assembled as a liner to new or existing structures. This solution is particularly effective for use in control center and data center applications.
- A factory-built welded "container like" solution that can accommodate multiple modules joined together at the site to create large protected facilities. This application is particularly well-suited to energy service providers and utilities due to its ability to be fitted off-site with much of the control and SCADA equipment. Assembly time on site is also considerably shortened with this approach.
- A conductive concrete solution that utilizes various ferrous/magnetic materials into the concrete mix as aggregate and is applied as "shotcrete" (a sprayed application). The conductive concrete solution can be deployed as prefabricated panels that are assembled on-site or completely fabricated on-site. This relatively new approach can be used as a complete solution or as part of a hybrid solution

when used with an HCI-certified modular bolt together system.

- In addition, there are new techniques available for the subfloor treatment. For example, using a subfloor of steel-reinforced conductive concrete can be cost-effective for large projects as the installation time for the project can be reduced significantly. With careful planning, the RF shielding panels can then be attached to the subfloor.
- Some metal building suppliers have modified their designs to provide up to 40 dB attenuation (the lower end of the current guidance of the IEC SC-77C Committee). This is an application that some utilities are considering for protection of remote service facilities.
- The most important point of entry (POE) is the filters and surge arresters. These must be HCI certified and installed on all electrical conductors that penetrate the EMP shielded enclosure. These conductors include, but are not limited to, power circuits, data lines, video and communications lines, alarm circuits, lighting circuits, and signal lines such as telephone lines, antenna lines, HVAC control lines, security and fire alarms. Filters must be built and labeled by a nationally registered test lab (NRTL) to fully conform to UL 1283 and have standard short circuit withstand ratings in accordance with UL 1283. It is best practice to have short circuit ratings greater than or equal to the short circuit withstand ratings of the switchboards or panel boards feeding the filters.

(In all cases listed above, it is imperative to address all points of entry (POEs) with HCI components such as doors, power filters, control filters, waveguide vents and waveguide penetrations.)

Considering the extreme consequences of a failure in EMP protection, great care must be taken to select a consultant or company that is a documented, experienced provider in the detection, measurement and management of electromagnetic energy. It is helpful to engage a company whose EMP capabilities and services include design, consulting, manufacturing and installation for a turn-key system approach to any project. This approach guarantees all components of the project work together seamlessly to meet or exceed performance requirements.

photo courtesy ETS-Lindgren

Independently tested and certified EMP protection solutions ensure continuation of service should an EMP event occur. Solutions include shielding of walls, floor and ceiling, plus protective entry points for air, water, and power.

For large projects, a certified building information modeling (BIM) team can also provide a key advantage. BIM is used to plan, design and construct buildings and infrastructure as the first step in any large project. The use of BIM tools results in cost-effective and well-managed project execution. Many large companies have this capability today.

Documentation or test reports that verify that EMP shielding panels, filters, specialty penetrations for secure air, water, and power transfer have been tested as a system (working together) by an independent test laboratory should also be requested. If a consultant or company cannot provide an independent test report for the manufacturer's complete EMP test system, this should raise concern. Again, should an EMP protection system fail, it would be difficult to put a price on the consequences of lost data or, in a worst-case scenario, lost lives. Neither scenario is acceptable since high quality, and reliable, EMP protection is available.

FUTURE ACTIVITY

In recognition of the growing concern and impending new U.S. legislative requirements, several electric power industry leaders have requested reports detailing the EMP vulnerability of substation control houses and the current available options for the construction of future EMP protected substation control houses. In addition, some report requests seek more extensive information on EMP protection of data centers, command and control centers and research facilities for the remaining critical infrastructure segments. These reports typically identify the potential issues in each of the current

designs as it relates to the EMP protection of critical electronic equipment, expected EMP impact on the critical components, mitigation opportunities for existing facilities and recommendations for planned facilities.

The guiding specification for the EMP protection recommendations are often a modified version of MIL-STD 188-125-1, *High-Altitude Electromagnetic Pulse (HEMP) Protection for Ground-Based C4I Facilities Performing Critical, Time-Urgent Missions*. The modifications to this specification will frequently include a relaxation of material, construction methodology and verification testing, but not overall performance.
While the MIL-STD 188-125-1 specification is not the only currently published standard for the construction of an EMP protected facility, it is preferred by many. Since the application related to substation control houses is not officially classified as "time-urgent," modifications for economic considerations are appropriate. In accordance with these considerations, an EMP protection guide is available through the IEC as standard IEC 61000-5-10 for commercial applications or installations that are not necessarily time urgent. The overall EMP protection evaluation and recommendations not only address the six-sided shielded enclosure, but also address and treat all points of entry and infrastructure critical systems. In addition to MIL-STD- 188-125, this standard incorporates the current guidance of the IEC SC-77C Committee that establishes the high-end limit of 10 GHz for IEMI threats.

CONCLUSION

Global threats posed to society and business from nuclear weapons, geomagnetic disturbances and terrorists or criminals utilizing high power electromagnetic weapons are a recognized concern of European consortiums, the U.S. government and non-government critical infrastructure entities. Cost-effective EMP protection options are available that can help both critical infrastructure entities and other concerned businesses to protect themselves from the EMP threat.

The authors would like to thank Martha Hallman and Sergio Longoria of ETS-Lindgren for their invaluable contributions to this article.

REFERENCES:

1. "Overview of the European Project Security of Railways in Europe against Electromagnetic Attacks (SECRET)", *IEEE EMC Magazine*, Vol 3, Issue 4, January 27, 2015, http://ieeexplore.ieee.org/document/7023203
2. "Overview of the European Project STRUCTURES", *IEEE EMC Magazine*, Vol 3, Issue 4, January 27, 2015, http://ieeexplore.ieee.org/document/7023202
3. Financial Sense, February 2, 2017, http://www.financialsense.com/contributors/dr-peter-vincent-pry/emp-threat
4. WORLDNETDAILY, February 2013, "EMP Would Hit Banks at Speed-of-Light", http://www.wnd.com/2013/02/emp-would-hit-banks-at-speed-of-light/
5. The Wall Street Journal, August 12, 2014, https://www.wsj.com/articles/james-woolsey-and-peter-vincent-pry-the-growing-threat-from-an-emp-attack-1407885281
6. The Blaze, February 20, 2014, http://www.theblaze.com/contributions/world-war-iii-the-coming-cyber-financial-attack-that-will-shock-america/
7. Washington Examiner, December 28, 2016, http://www.washingtonexaminer.com/iran-endorses-nuclear-emp-attack-on-united-states/article/2561733
8. The Backgrounder #2491, National Security and Defense, November17, 2010, http://www.heritage.org/research/reports/2010/11/emp-attacks-what-the-us-must-do-now
9. Due to the sensitive nature of these projects, ETS-Lindgren signs a non-disclosure agreement with its customers. Hence, while capabilities, methodologies and project objectives may be shared, the identity of the customer and location cannot legally be shared.