IEMI Classification of Facilities

Daniel Månsson [#1], Rajeev Thottappillil [*2], Mats Bäckström [+3]

[#]*High Voltage Valley*
AB Samarkand2015, Box 832, 771 28, Ludvika, Sweden
[1]Daniel.mansson@highvoltagevalley.org

[*]*Royal Institute of Technology (KTH)*
Teknikringen 33,SE-10044 Stockholm, Sweden
[2]*Rajeev.Thottappillil@ee.kth.se*

[+]*Saab Systems*
SE-581 88 Linköping ▪ Sweden
[3]*Mats.Backstrom@saabgroup.com*

***Abstract*—Determination of shielding efficiency in combination with knowledge of the susceptibility of the equipment located inside the shield is not sufficient for estimating the threat from intentional electromagnetic interference towards a facility or distributed system. In addition, shielding efficiency is a concept more suitable for enclosures. The physical distribution, the complexity of the system and the intent behind the disturbance call for alternative methods of classification for distributed systems. One such method, based on three key terms; Accessibility, Susceptibility and Consequence, is proposed here.**
Key words: Intentional electromagnetic interference (IEMI), security, classification, shielding effectiveness.

I. Introduction

Since the beginning of the 1980's the inherent vulnerability of the technical infrastructures to electromagnetic interference (EMI) has steadily increased. However, this is not to say that the knowledge and technology of how to mitigate electromagnetic disturbance has not increased, it has. Nevertheless, the evolution of our society and how technology is used has changed the prerequisites for electromagnetic compatibility. A number of reasons can be given for why the threat from intentional electromagnetic interference (IEMI) has increased:

1. The overall increase in the use of sophisticated and sensitive electronics. Commercial-off-the-shelf (COTS) equipment such as computers, communication systems, etc., may be used in electromagnetic environments that they were originally not intended for.
2. Miniaturization of systems which results in weaker disturbances being able to interfere with or damage systems.
3. Increased use of the electromagnetic spectrum which leads to more open ports (antennas) that can be used for front-door coupling of intentional disturbances.
4. Commercial high power sources of different characteristics [1] exist today, alongside standardized sources for EMC and lightning induced effects tests as well as commercial radars. The legislation of ownership of these types of sources is not clear today.
5. The large amount of available and legal components that can be assembled to form more or less crude high power electromagnetic (HPEM) sources.
6. The openness of today's modern society may tempt certain groups, as IEMI attacks can be performed covertly and anonymously (compared to, e.g., an explosion which will immediately identify the cause of disruption in the infrastructure).

As can be seen IEMI has some inherent difficulties compared to unintentional EMI that has to be kept in mind when assessing the threat to a facility. However, additional problems arise. Normal praxis for assessing the susceptibility of a system is to use shielding effectiveness in combination with knowledge of the susceptibility of the equipment located inside the shield, see Fig. 1. (In this paper the term shielding efficiency denotes protection against both radiated and conducted disturbances). However, for large distributed systems, or a facility, this creates problems. For instance, where in the facility should the fields be measured? The room or compartment containing the most critical equipment is one option, but then the interdependencies of the internal system and the transfer function of the facility have to be fully understood. Also, from where should the fields originate (source point)? The facility is not a closed system, thus, radiating from the exterior or from within (e.g., a lobby) can greatly differ. In addition, conducted transients may be a larger threat than radiated fields as suggested in [2] and [3] as readily available ports for injecting electromagnetic disturbances are available and for the most part not considered as a risk.

Even if the electromagnetic topology principle (zoning) is implemented in the facility an attacker could circumvent this by entering through the outer zone (as access control may not be present in most civilian facilities) and then radiate or inject a disturbance. Even worse, transient mitigation, in a facility, in the form of surge protection or filters are for the majority positioned on the exterior of the outer zone boundary, in the form of lightning protection, and thus the, e.g., power sockets are uncontrolled paths from one point to several connected systems, especially for fast impulses.

In should be clear now that the methodology of determination of shielding effectiveness together with equipment susceptibility will not fully represent facilities vulnerability to IEMI.

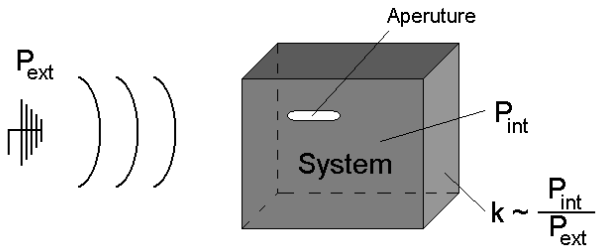

Fig. 1 The shielding effectiveness is derived from the ratio of two measured quantities, one external and one internal value, using, e.g., the electric- or magnetic field,.

II. IEMI CUBE

As stated above, the physical distribution and complexity of a facility renders the shielding effectiveness concept almost useless for determining whether the facility is vulnerable from IEMI attacks. Therefore, an alternate method, based on the variables *accessibility*, *consequence*, and *susceptibility*, is suggested. These three variables form a *vulnerability vector* in the variable space spanned by the IEMI/ASC-cube (see Fig. 2). The scaling of these variables is best not to follow a numbered scale, but should rather be a form similar to the grading of "very limited", "limited", "severe", "very severe" and "catastrophic". The three variables can be collectively be weighted and the vulnerability estimated by forming the IEMI/ASC-cube. The variables are described in the section below and highlighted by an example at the end.

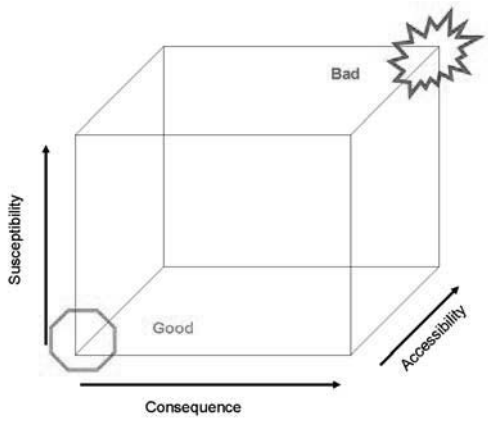

Fig. 2 The IEMI/ASC cube.

Observe that a facility is still considered vulnerable if the consequence term is low but the accessibility and susceptibility are high. If the consequence of an attack is also high the facility is considered to be critically vulnerable.

A. Accessibility

Imagine a facility that has fences that creates a minimal distance between any susceptible system and source. Along with a good surveillance this creates less vulnerability from IEMI attacks than a facility that does not have fences. Existence of fences is an example where the *accessibility* (A) is lowered and thus diminishes the threat from an attacker. The accessibility term should also consider the ability to reach suitable ports for injecting transients, e.g., power-, network or lamp sockets. The accessibility term should thus be related to the ability of gaining access to "points" (both in space and in a network) suitable for injecting or radiating an electromagnetic disturbance.

B. Consequence

Consider a hypothetical successful attack on a nuclear power plant or a successful attack on a postal office. The *consequence* (C) of the attack will greatly differ between the two facilities. It is vital that the consequence term is deduced in cooperation with the system owner or operator as they will have intricate knowledge of the system not available to an outside engineer. Past experience of fault incidents from, e.g., lightning induced incidents, will give an indication on the consequence of an IEMI attack. System simulations might also provide some information on how different upset events would affect connected systems and how the obstruction of the operation of the original system would spread to other facilities or distributed systems.

C. Susceptibility

Finally, consider a facility that has fully implemented the zoning principle with shielded compartments and correctly installed filters and surge protective devices. If compared to a facilities that has not, the *susceptibility* (S) of the last facility is much greater than the first. A facility, viewed upon as a complete system, is very complex, but it would be advantageous to still keep the IEC definition of system susceptibility [4] (see below):

"Inability of a device, equipment or system to perform without degradation in the presence of an electromagnetic disturbance".

Standard EMC susceptibility tests are made by irradiating the object under test and noting the, e.g., field levels for different situation (e.g., frequency, polarization, etc.) and their corresponding upset events (e.g., interference, crash, or permanent damage). However, it is often impossible to irradiate a whole facility (or a large distributed system such as a power grid or railway system) and the interpretation of the results would be difficult. Therefore the susceptibility term for the suggested IEMI investigation method is divided into three terms:

1. *Receptivity*, the degree of the facility's ability to mitigate disturbances between points and/or ports (a

description of transfer functions). For instance, shielding or filters would affect this, but also, e.g., different network layouts.

2. *Sensitivity*, the threshold levels for different upset events of the equipment and subsystems inside the facility (as traditionally defined as "susceptibility", see above)
3. *Redundancy*, the existence of backup systems and ability to "degrade gracefully" [5], that is to continue the operation of the facility or system even though the main subsystems are being interfered with or perhaps permanently damaged.

The sensitivity can be estimated from susceptibility tests performed on subsystem or equipment either considered critical for the operation of the facility or easily accessible by an electromagnetic disturbance through, e.g., ports. The receptivity can be derived from both simulations (as [6]), calculations (as [7]), and low level experiments (as [3]), in which estimates of the transfer functions from likely points of irradiation or ports of injection, to system that are critical to the operation, are made. The redundancy can be estimated (with the system owner or operator) from past experience, in which the facilities continued operation has been put to the test, by, e.g., power outages or lightning induced incidents.

III. SIMPLE COMPARISON OF TWO FACILITIES

Let us now apply this method in an attempt to compare and classify two different facilities (see Fig 3 and 4). These two facilities help supervise and, to some extent, control the railway infrastructure and therefore it is of interest to investigate the vulnerability from IEMI. Two special EMC audits with IEMI in mind were performed [8] at the facilities to identify accessibility, risks and mitigation procedures installed (e.g., shields, filters, etc.).

Fig. 3 An older generation of control facility (hereby called CF1). Some important points have been marked.

Fig. 4 A newer design of control facility (hereby called CF2). Some important points have been marked.

Both facilities have surge protective devices installed at the power distribution central to mitigate lightning type disturbances or other "common" disturbances that could be expected in the power grid. For obvious reasons the exact location, purpose and consequence of a successful IEMI attack on the facility can not be given here.

A. Accessibility

Both of the control facilities are built close to public roads and the locations can be reached completely unhindered. Also, both facilities have relatively sturdy doors, however some differences exist. The newer facility, called CF2, is metal clad inside and has been built with fences, which, at first glance, is good, however the fence is not of a sturdy design and is more to stop "children and berry pickers". There is also some gap between the fence and the ground. It should also be noted that the distance between the fence and CF2 is small and the free-space attenuation of electromagnetic fields would be practically of no relevance for a likely radiating IEMI source. The older design, called CF1, did not have any fence surrounding the control facility. In addition, CF1 has windows (marked in Fig. 1) that CF2 did not. At both sites accessible ports (some marked in Fig. 1 and 2) could be found, that could be used to inject transients into the different networks. Also, cables could be easily accessed underneath CF2 (which stands on concrete pillars) and used for injecting disturbances into the system. Accessing the cables connected to CF1 was not obvious, but could be done.

Due to existence of some form of physical obstacle in CF2 (fence) and the windows in CF1 the accessibility is concluded to be slightly higher for CF1.

B. Susceptibility

1) Receptivity

Control facility CF2, was designed with some EMC in mind, as it is made out of metal plates (covered with wood), however the quality of the joints were not known to the operator and may not be adequate. In addition, the air-intakes are not EMC proof and thus the attenuation of radiated fields may not be sufficient for higher frequencies. CF1 was made out of concrete (with the possible existence of the odd reinforcement bar) and thus very transparent for

electromagnetic fields. Thus the ability to deliver disturbances into the facilities, considering radiated and injected disturbances, was found to be very high. In addition, surge mitigation was only found at respective power distribution central of the facilities, not at the external ports.

2) Sensitivity

The equipment inside both control facilities was of similar type, however CF1 utilized slightly older systems. Also the systems inside were of COTS (commercial-off-the-shelf) nature and, thus, not expressly hardened against HPEM. Over the last decade, open literature on threshold levels for different upset events have be published which can serve as an indication on the level of immunity for common equipment and of use for a first rough estimate, before immunity tests are performed.

3) Redundancy

Both facilities had backup power in some form or another.

Considering these three terms, the susceptibility is concluded to be a higher for CF1, mainly due to the lack of any shielding.

C. Consequence

The consequence of a successful IEMI attack on these facilities will not be reviewed here.

D. Conclusion of comparison

It was clear that even though the control facilities handle "day to day" EMC issues such as disturbance from power networks relevantly unhindered, the classification, from an IEMI perspective, would be poor. This is mainly due to a high accessibility, high receptivity of the facilities and high sensitivity of the equipment and subsystem inside that could be disturbed or permanently damaged by many available HPEM sources. However, it also shows that steps taken to improve the traditional electromagnetic compatibility provided some improvement also for the IEMI protection.

IV. Conclusion

In this paper an alternative method for EMC classification is suggested. The method was developed to classify the vulnerability of facilities and large distributed system from IEMI. The vulnerability vector is formed, in the variable space spanned by the IEMI/ASC-cube, by estimating the accessibility and susceptibility of the facility, as well as the consequence of a successful IEMI attack. Due to the complexity of a facility the susceptibility is subdivided into three terms; the receptivity, sensitivity and redundancy.

Acknowledgments

The Swedish Rail Administration is greatly acknowledged for the help and funding of these investigations.

References

[1] D.V. Giri and F.M. Tesche. "Classification of intentional electromagnetic environments (IEMI)", *IEEE Trans. EMC*, vol 46, No. 3, pp 322-328, August 2004.

[2] D. Månsson, T. Nilsson, R. Thottappillil, M. Bäckström, "Propagation of UWB transients in low-voltage installation power cables", *IEEE Trans. EMC*, Vol. 49, No. 3, pp 585-592, August 2007.

[3] D. Månsson, R. Thottappillil and M. Bäckström, "Propagation of UWB transients in low-voltage power installation networks", *IEEE Trans. EMC*, Vol. 50, No. 3, pp. 619-629, August 2008

[4] *Electromagnetic compatibility (EMC) - Part 2-13: Environment - High-power electromagnetic (HPEM) environments - Radiated and conducted*, IEC Standard 61000-2-13 Ed. 1, 2005.

[5] Rawashdeh, O.A.; Lumpp, J.E., "A technique for specifying dynamically reconfigurable embedded Systems", in *Proc. IEEE Aerospace Conference*, pp. 1-11, 5-12 March, 2005.

[6] J. Carlsson, T. Karlsson and G. Undén "EMEC-an em simulator based on topology", *IEEE Trans. EMC*, vol. 46, pp. 353-358, August 2004.

[7] W. Radasky, C.E. Baum, M.W. Wik, "Introduction to the special issue on high-power electromagnetics (HPEM) and intentional electromagnetic interference (IEMI)", Vol. 46, No. 3, pp. 314 – 321, Aug. 2004.

[8] R. Thottappillil , Daniel Månsson, Nelson Theethayi, Mats Bäckström, Tony Nilsson, Göran Undén, Barbro Nordström, Per Bohlin, Per Anders Lindeberg, Ulf Hellström, Peter Lindeberg, Georg Bohlin, Mihael Zitnik, Lise Ekenberg, "Response of Civilian Facilities to Intentional Electromagnetic Interference (IEMI), with Emphasis on the Swedish Railway Network", *EMC Europe Workshop*, Rome , Sept. 19-21, 2005