URSI AP-RASC 2019, New Delhi, India, 09 - 15 March 2019

Intentional Electromagnetic Interference and Critical Infrastructure

Rajeev Thottappillil[(1)], Mats Bäckström[(2)]
(1) KTH Royal Institute of Technology, Stockholm, Sweden, e-mail: Rajeev@kth.se
(2) SAAB Aeronautics, SAAB AB, Linköping, Sweden; e-mail: mats.backstrom@saabgroup.com

Intentional Electromagnetic Interference or IEMI is the result of maliciously created electromagnetic disturbances in sensitive electronic systems. Modern infrastructure such as power supply, wireless communication networks, banking system, and transportation networks are dependent on civilian-off-the-shelf (COTS) equipment for its uninterrupted and reliable operations. Even though COTS equipment are tested for electromagnetic compatibility as per pre-defined un-intentional electromagnetic environment and test methods, intentionally created electromagnetic disturbances creates a lot of uncertainty in the proper functioning of critical COTS elements of the infrastructure. Infrastructure is interconnected widely distributed systems and there are several ports where substantial electromagnetic energy can be coupled intentionally by saboteurs and once coupled these disturbances travel through the interconnected system and cause breakdown at one or more weak links. It is probable that some of these breakdowns may lead to widespread disruption of critical infrastructure, such as power supply blackouts, financial service shutdown or disruption in railway network due to signal failures. Due to its inherent nature, EM attacks to civilian infrastructure may happen anonymously and repeatedly without detection. Protection of civilian critical infrastructure against the effects of IEMI has received a lot of attention recently from the EMC community. This article reviews the work done around the world with special emphasis on the work done in Sweden [e.g; 1-5].

1. B. Oakes, L. Mattsson, P. Näsman, and A. Glazunov, ”A Systems‐Based Risk Assessment Framework for Intentional Electromagnetic Interference (IEMI) on Critical Infrastructures”, *Risk Analysis*, **38, 6**, June 2018, pp. 1279-1305. DOI: 10.1111/risa.12945.

2. N. Mora, I. D. Flintoft, L. Dawson, J. F. Dawson, F. Rachidi, M. Rubinstein, A. C. Marvin, P. Bertholet, M. Nyffeler, “Experimental Characterization of the Response of an Electrical and Communication Raceway to IEMI”, *IEEE Transactions on Electromagnetic Compatibility*, **58, 2**, April 2016, pp. 494-505. DOI: 10.1109/TEMC.2015.2510423.

3. D. Månsson, R. Thottappillil, and M. Bäckström, “Methodology for Classifying Facilities With Respect to Intentional EMI”, *IEEE Transactions on Electromagnetic Compatibility*, **51**, **1**, February 2009, pp. 46-52. DOI: 10.1109/TEMC.2008.2010327.

4. D. Månsson, R. Thottappillil, M. Bäckström, and O. Lundén, “Vulnerability of European Rail Traffic Management System to Radiated Intentional EMI", *IEEE Transactions On Electromagnetic Compatibility*, **50**, **1**, February. 2008, pp. 101-109. DOI: 10.1109/TEMC.2007.915281

5. M. Bäckström, and K. G. Lövstrand, ”Susceptibility of electronic systems to high-power microwaves: Summary of test experience”. *IEEE Transactions on Electromagnetic Compatibility*, **46**, **3**, August 2004, pp. 396-403. DOI: 10.1109/TEMC.2004.831814.