Proceedings Paper:
Simio, Francesca De, Cillis, Francesca De, Fumagalli, Giustino et al. (2016) Strategies to improve Critical Infrastructures Robustness against the IEMI threat:a Review of relevant Standards and Guidelines on the topic. In: Critical Information Infrastructures Security:10th International Conference, CRITIS 2015, Berlin, Germany, October 5-7, 2015, Revised Selected Papers. 10th International Conference, CRITIS 2015, 05-07 Oct 2015 Lecture Notes in Computer Science. Springer, DEU, pp. 251-254.

https://doi.org/10.1007/978-3-319-33331-1_22

Strategies to improve Critical Infrastructures Robustness against the IEMI threat: a Review of relevant Standards and Guidelines on the topic

Francesca De Simio[1], Francesca De Cillis[1], Giustino Fumagalli[1], Maria Carla De Maggio[1], Stefan van de Beek[2], John Dawson[3], Linda Dawson[3], and Roberto Setola[1]

[1]Complex Systems & Security Lab, Università Campus Bio-Medico di Roma
Via Álvaro del Portillo 21, 00128 Rome, Italy
f.desimio@unicampus.it,f.decillis@unicampus.it
giustinofumagalli@yahoo.it,m.demaggio@unicampus.it
r.setola@unicampus.it
[2] Telecommunication Engineering Group, University of Twente, 7522 NB Enschede, The Netherlands
g.s.vandebeek@utwente.nl
[3]Department of Electronics, University of York, Heslington, York, YO10 5DD, UK
john.dawson@york.ac.uk,l.dawson@york.ac.uk

Abstract. This paper aims to provide a brief overview of relevant standards, procedures and guidelines to standard bodies to manage the impact of the Intentional ElectroMagnetic Interference (IEMI) threat. It also provides guidelines for CI operators on how to reduce their exposure on IEMI hazards.

Keywords: IEMI, Standards, Guidelines, Critical Infrastructures Protection

1 Introduction

Attacks by Intentional ElectroMagnetic Interference (IEMI) on Critical Infrastructure (CI) have become a significant threat in recent years due to the availability of suitable interference sources at low cost. Intentional ElectroMagnetic Interference (IEMI), is in general defined as *the intentional malicious generation of electromagnetic energy introducing noise or signals into electrical and electronic systems, thus disrupting, confusing or damaging these systems for terrorist or criminal purposes* [1–3].

Recent years have seen the development of several international and European programs for CI Protection (CIP) such as the STRUCTURES [4] HIPOW [5], and SECRET [6] projects to raise awareness among the community on CIP and to support CI providers in the definition of specific and effective countermeasures for CIP [7, 8]. This paper describes work undertaken as part of the FP7 European project STRUCTURES (Strategies for The impRovement of critical

infrastrUCTUre Resilience to Electromagnetic attackS) [9]: Section 2 provides a brief overview about the standards in the fields of Business Continuity Management (BCM), Risk Management (RM), Information Technology (IT) Security and Information and Communication Technology (ICT) Security related to IEMI threat. Section 3 presents the most relevant aspects to be taken into account for providing guidelines to CI operators to reduce their exposures on IEMI hazards.

2 IEMI Threats and Standardization: the state of the art

#	Standard	Scope	Impacted by introduction of IEMI threat	Note
1	ISO/IEC 27001:2013	IT Security	×	
2	ISO/IEC 27002:2013	IT Security	√	
3	ISO/IEC 27005:2011	Risk Management	√	
4	ISO/IEC 27011:2008	IT Security	√	Specific for telecommunication
5	ISO/IEC 27019:2013	IT Security	√	Specific for Energy sector
6	ISO/IEC 27031:2011	BC Disaster Recovery	√	
7	ISO/IEC 27033:2011	ICT Security	×	
8	ISO/IEC 27035:2011	BC Disaster Recovery	×	
9	ISO 27799:2008	IT Security	√	Specific for Health sector
10	ISO/IEC 24762:2008	BC Disaster Recovery	×	
11	ISO 31000: 2009	Risk Management	×	
12	ISO/IEC 31010:2009	Risk Management	√	
13	ISO 22301:2012	BC Disaster Recovery	×	
14	ISO 22313:2012	BC Disaster Recovery	×	
15	ISO/PAS 22399:2007	BC Disaster Recovery	×	
16	ITSEC 1.2	ICT security	×	Critical equipments and applications should be certified for security characteristics against IEMI attack through these standards.
17	ISO 15408: 1999	ICT security	√	Note: ITSEC has been broadly replaced by Common Criteria
18	ISO 13335-1:2004	ICT Security	×	
19	ISO 13335-4:2000	ICT Security	√	
20	BSI (Bundesamt fur Sicherheit in der Informationstechnik) Standard 100-3	Risk Management	√	DE only
21	TIA-942	IT Security	√	USA standard (ANSI) and Electronic Industries Alliance (private sector).
22	ITU-K81:2009	IT Security	√	Reference document on intentional EM threats protection

Table 1. List of Relevant Standards to IEMI threat for a CI.

Table 1 summarises European standards relevant to the protection of CI. As part of complex standards framework, not all relevant documents listed in Table 1 mention to the IEMI threat. In a top-down approach, higher level documents

usually refer to standardized management systems (such as IT Security Management Systems - ISO27001 or BCM System - ISO22301) or define generic models to be use in a broad context or are not related to a specific threat. It is our opinion that all documents listed in Table 1 should devote specific sections to the IEMI threat topic.

For completeness we also mention that the International Electrotechnical Comission (IEC) produces a series of standards and technical reports on the effects of electromagnetic interference on electronic systems in the IEC 61000 series such as the IEC61000-1-5 technical report on "High power electromagnetic (HPEM) effects on civil systems" [10].

3 Guidelines for CI operators

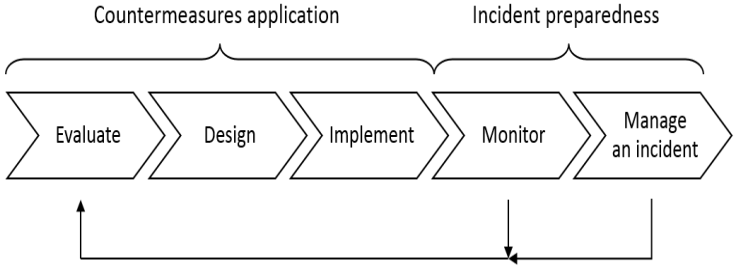

Fig. 1. The BC and ISM cyclical process

In general, BC and Information Security Management (ISM) usually rely on a cyclical process, which is arranged into several steps as described in Fig. 1. Countermeasures such as physical separation of critical electronics from possible sites for an attack, can be complemented by additional electromagnetic shielding of buildings, equipment and cables depending on the assessment of risk and evaluation of the levels of susceptibility and criticality of each sub-system. Wireless communications and navigation (e.g. GPS) systems which are becoming widely used in infrastructure systems are particularly vulnerable to IEMI and difficult to protect due to the low levels of signals at the receiver. Incident preparedness should include some means of detecting an IEMI attack [11], otherwise system failures may be incorrectly blamed on hardware failure or software errors. Detection of an attack also means that prompt action can be taken to detect the source of the attack and manage other aspects of the incident. Savage and Radasky [12, 13] provide a more detailed view of the problem and possible solutions.

4 Conclusions

In this short paper we have been able to give only a brief overview of the available standards and guidelines for to improve the robustness of CI. More information and other relevant material can be found on the STRUCTURES project web site [4].

Acknowledgment. The research leading to these results has been implemented in the framework of the Project STRUCTURES co-funded by the European Union Seventh Framework Programme under grant agreement n 285257.

References

1. Sérafin, D., Critical infrastructures are at risk under electromagnetic attacks, European CIIP Newsletter, vol. 9, i. 1 (2015)
2. The Threat of Radio Frequency Weapons to Critical Infrastructures Facilities, TSWG & DETO Publication, August 2015
3. Parfenov, Y.V.; Zdoukhov, L.N.; Radasky, W.A.; Ianoz, M., "Conducted IEMI threats for commercial buildings," in Electromagnetic Compatibility, IEEE Transactions on , vol.46, no.3, pp.404-411, Aug. 2004
4. STRUCTURES Strategies for The impRovement of critical infrastrUCTUre Resilience to Electromagnetic attackS, `http://www.structures-project.eu/` (access on May 4, 2015)
5. HIPOW Protection of Critical Infrastructure against High Power Microwave Threats, `http://www.hipow-project.eu/hipow/` (access on Sep 8, 2015)
6. SECRET - SECurity of the Railway network against Electromagnetic ATtacks, `http://www.secret-project.eu/` (access on Sep 8, 2015)
7. European Commission, `http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm` (access on May 4, 2015)
8. Flammini, F., Setola, S., Franceschetti, G., Effective Surveillance for Homeland Security: Balancing Technology and Social Issues, Chapman and Hall/CRC, (2013)
9. van de Beek, S., Dawson, J., Flintoft, I., Leferink, F., Mora, N., Rachidi, F., Righero, M., Overview of the European project STRUCTURES, Electromagnetic Compatibility Magazine, IEEE , vol.3, no.4, pp.70,79, (2014)
10. International Electrotechnical Commission, IEC Technical Report, 61000-1-5, Electromagnetic compatibility (EMC) - Part 1-5: General - High power electromagnetic (HPEM) effects on civil systems, IEC 2004.
11. Dawson, J.F., Flintoft, I.D., Kortoci, P., Dawson, L., Marvin, A.C., Robinson, M.P., Stojilovic, M., Rubinstein, M., Menssen, B., Garbe, H., Hirschi, W., Rouiller, L., A Cost-Efficient System for Detecting an Intentional Electromagnetic Interference (IEMI) attack, Electromagnetic Compatibility (EMC Europe), 2014 International Symposium on , vol., no., pp.1252,1256, (2014)
12. Savage, E., Radasky, W. , Overview of the threat of IEMI (intentional electromagnetic interference), Electromagnetic Compatibility (EMC), 2012 IEEE International Symposium on, 317-322, Aug 2012.
13. Radasky, W. , Fear of frying electromagnetic weapons threaten our data networks. Here's how to stop them , Spectrum, IEEE , vol. 51, no. 9, 46-51, Sept 2014.

Simio, F. D.; Cillis, F. D.; Fumagalli, G.; Maggio, M. C. D.; van de Beek, S.; Dawson, J.; Dawson, L. & Setola, R. , "Strategies to improve Critical Infrastructures Robustness against IEMI threats: Review of relevant Standards and Guidelines" , Proceedings of The 10th International Conference on Critical Information Infrastructures Security , October 5-7 2015.

The final publication is available at Springer via http://link.springer.com/ as:
Simio, F. D.; Cillis, F. D.; Fumagalli, G.; Maggio, M. C. D.; van de Beek, S.; Dawson, J.; Dawson, L. & Setola, R. , Rome, Erich and Theocharidou, M. W. S. (ed.) , "Critical Information Infrastructures Security: 10th International Conference, CRITIS 2015, Berlin, Germany, October 5-7, 2015, Revised Selected Papers" , Strategies to Improve Critical Infrastructures Robustness Against the IEMI Threat: A Review of Relevant Standards and Guidelines on the Topic , Critical Information Infrastructures Security , Springer International Publishing , 251-254 , 2016. , DOI: 10.1007/978-3-319-33331-1_22 , Available: http://dx.doi.org/10.1007/978-3-319-33331-1_22