Electromagnetic Security: Risks Management Improvement using Statistics

Robert L. Gardner, Consultant
6152 Manchester Park Alexandria,
VA 22310, USA
Robert.L.Gardner@verizon.net

Chaouki Kasmi*, Muriel Darces and Marc Hélier
Sorbonne Universités
UPMC Univ Paris 06, UR2, L2E,
F-75005, Paris, France
*chaouki.kasmi@ssi.gouv.fr

Abstract—**The hardening of critical infrastructures against threats of intentional electromagnetic interference is mandatory in order to improve their *safety* and *security*. We propose in this paper to demonstrate how the extreme value statistics can be involved in risks management procedures for the estimation of appropriate protections thanks to the evaluation of a safe margin.**

Keywords-component: Electromagnetic security; Risk management; Extreme Values statistics;

I. CONTEXT

Intentional electromagnetic interference (IEMI) poses unacceptable risks for the security and safety of critical infrastructures. The hardening of these structures has been enhanced thanks to risk management procedures. In the same time, the complexity of systems and networks imposes to lay aside experimental tests for a combined use of simulation tools and statistics [1]. The use of models imposes to take into account the uncertainty and the variability of input modeling parameters. This has been achieved by the introduction of stochastic methods, such as the Monte-Carlo approach, which allows estimating the variability of a physical quantity under study.

In *Electromagnetic Compatibility* studies, the *Gaussian* model (computation of the mean and variance of the physical quantity under study) is mainly applied, even if it is known for failing in accurately modeling the probability of *outliers*. We propose to highlight the benefit of extreme value statistics [2] for an accurate design of protective devices.

II. VULNERABILITIES AND PROTECTIONS ANALYSIS

The risk has been formulated [3] as a function of the *Exposure* of the target, its *Vulnerability* and its *Criticality* as follows:

$$Risk = \alpha\{Exposure, Vulnerability, Criticality\}$$

Based on the estimated risk, additional protective devices should be inserted in the infrastructure.

In order to define the appropriate protection line (*PL*), it is necessary to estimate accurately the following parameters [4]:

- *Threat Level* (TL), provided by standards;
- *Immunity level* (IL) of the device to be protected;
- *Safe margin* (SM) in order to introduce the parameters uncertainty and variability.

As soon as we focus on the *security* and *safety* of critical system, it is necessary to manage the *worst-case* scenario (as depicted in Fig. 1) where the tails of distributions overlap. It has been shown [2] that the extreme values statistic, and more specifically the *excess model*, is a well-founded methodology for the analysis of highly improbable events.

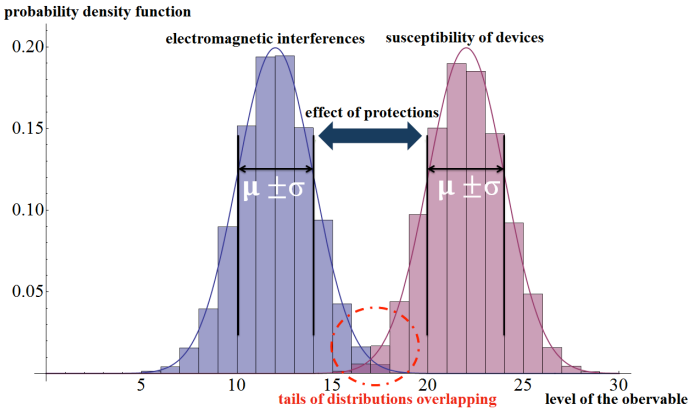

Figure 1. Probability density function of IEMI vs. Device susceptibility

By adjusting the extreme values thanks to the generalized *Pareto* distribution [2], the TL, IL and SM levels can be computed for a given probability.

III. RISKS MANAGEMENT

During the presentation, it will be demonstrated how we can capitalize on the prediction of the extreme values statistics of the devices immunity (IL), IEMI level (TL) and protections performance for the design of appropriate protective systems (SM).

REFERENCES

[1] R. L. Gardner and Christopher W. Jones, "System Lethality: Perspective on High Power Microwaves", System Design and Assessment Note 34, July, 1995.

[2] C. Kasmi, M. Darces, M. Hélier, and E. Prouff, "Generalised Pareto distribution for extreme value modelling in electromagnetic compatibility", Electronics Letters, Vol. 49, pp. 334–335, 2013.

[3] E. F. Vance, "The Relation of Cost to Evaluation and Monitoring of Electromagnetic Protection", System Design and Assessment Note, Note 33, January, 1994.

[4] A. W. Kaelin and M. Nyffler, "Pass/Fail Criteria for HPEM-Protection devices", Proc. Of EUROEM 2012, pp. 89, Toulouse, France, July, 2012.