A Statistical Approach to Analyze the Risk of HPEM Attacks on Electronic Systems

Torsten Teichert, Lars Ole Fichte, Marcus Stiemer
Helmut-Schmidt-University,
Faculty of Electric Engineering
Hamburg, Germany
torsten.teichert@hsu-hh.de

Stefan Potthast, Frank Sabath
Bundeswehr Reseach Institute for Protective Technologies
and NBC Protection
Munster, Germany
frank.sabath@ieee.org

***Abstract*— Risk analysis of complex electronic systems against radiated interferences is an evident part of the design phase, especially in modern military environments, and is vital for later operation. Since affordable high power electromagnetic (HPEM) sources become more and more available, risk analysis against such threats has to keep pace with these changing circumstances. In this paper a method consisting of computational electromagnetic (CEM) simulations combined with statistical methods based on [1],[2] will be presented. The novel method is then applied to a generic missile.**

***Keywords*— HPEM sources, statistical methods, numerical simulation**

I. INTRODUCTION

As electromagnetic compatibility (EMC) problems are cost drivers for engineering projects, a trade-off between risk reduction and depth of analysis has to be found. Ideally, a worst-case-scenario is estimated, but, since an electronic system consists of many parts that respond differently on an electromagnetic (EM) interference (EMI) and interact in a complicated way, it is crucial that typically a whole class of critical scenarios has to be considered, whose parameters are a priori unknown. To overcome this problem, a statistical framework has been derived in [1] based on a statistical model of the whole EMI at system level. The risk analysis is performed by a Monte-Carlo-simulation of this model. Aiming at a reduction of the system and, thus, of simulation time, we propose an alternative version, where only the electronic system is statistically modeled as in [1], but the interfering EM field is computed via CEM simulations. The basic idea is employing the reciprocity theorem, to obtain a guess for parameters of critical scenarios after the vulnerable points of the system under consideration (SuC) have been identified with the help of the statistical model. The methodology is exemplarily applied to a generic missile as a SuC. An alternative approach to reduction of costs would be the use of a reverberation chamber, which is also beneficial to figure out thresholds for critical scenarios, but information about cause and effects which lead to an interference is lost.

II. ANALYTIC PROCEDURE

The threat environment and the electronic system are individually analyzed. The electronic system is then statistically modeled as described in [1], while the EMI is treated via CEM simulation. The link between the two different sub-models is established by an application of the reciprocity theorem.

A. Analysis of electromagnetic interference

As a first step, the EM environment is described. In the example SuC, the radiating source is located on the ground, the SuC is airborne, and there is a line of sight between source and SuC. Different source types may be taken into account.

B. EMI propagation

Based on the knowledge of the source type and the distance to object, the coupling paths into the SuC are analyzed. In this special case, there is an intended EMI (IEMI) source radiating directly on the target. No walls or zone models are considered. The target is decomposed into several volumes, which are partly filled with dielectric material and interconnected via a cable harness. Moreover, it is assumed that the SuC has no retroactive effect on the incident field.

C. System characteristics

To identify the most vulnerable points of the SuC, a statistical model according to [1] is constructed. To this end, the inner conditions of the systems are observed and a fault tree analysis is performed. With this model, the mission critical states of the system are identified.

D. CEM-Simulation of an inverse problem

In this step, broadband sources are placed at the vulnerable components of the system and the resulting field is computed with a CEM simulation to identify the SuC's points of weak shielding. From the resulting field pattern the critical parameters of the IEMI are identified. This procedure leads to all critical scenarios, if the system can be assumed sufficiently close to a linear one. If not, an iterative improvement of the guess is possible.

E. EM-Simulation of the native problem

Finally, a CEM simulation with the critical IEMI-parameters identified in the preceding step is performed and the electronic system is set in the resulting state. For additional reduction of costs, the correlation matrix for the representative parameters can additionally be taken into account to deduce the system state from the IEMI parameters.

III. CONCLUSION

Risk analysis on the system level basically requires a statistical paradigm such as elaborated in [1]. A hybrid version linking a statistical model for the electronic system and a CEM simulation for the IEMI as proposed in this paper is may be more efficient, since the parameter space for a Monte-Carlo-simulation is drastically reduced. Moreover, a reduction of probabilistic parameters increases certainty.

REFERENCES

[1] Genender, E.; Garbe, H.; Sabath, F., "Probabilistic Risk Analysis Technique of Intentional Electromagnetic Interference at System Level," IEEE Transactions on Electromagnetic Compatibility, vol.56, no.1, pp.200-207, Feb. 2014

[2] Genender, E., „Risikoanalyse von Systemen bei elektromagnetischer Störbeaufschlagung,“ Shaker-Verlag, 2012