A simplified methodology for IEMI risk assessment.

Odd Harry Arnesen
Comprehensive Defense Division
Norwegian Defense Research Establishment (FFI)
Kjeller, Norway
Odd-harry.arnesen@ffi.no

Abstract— We develop a simplified methodology for IEMI risk assessment, intended for Critical Infrastructure (CI) owners, operators and designers. The objective is to provide robust and simple procedures that may enable people to perform a first order risk assessment, without much previous IEMI experience. This will result in a generalized indication of their exposure and vulnerability to deliberate radio frequency attacks. Hopefully the methodology will provide the users with (1) an overall risk assessment, (2) increased awareness of IEMI, (3) an overview of common mitigation techniques, and (4) an incentive to perform a more thorough risk assessment to get the full picture. The work expands on the Risk Assessment Guide [1] developed under the EU FP7 project "HIPOW". Several other approaches have recently been published as well [2][3].

Keywords-IEMI; risk assessment; vulnerability; critical infrastructure

I. INTRODUCTION

The basic idea is to adapt a general standard for risk assessment, NS5832:2014, aka. "the Tri-Factor Model", to cover the issues pertinent to IEMI vulnerabilities. The three factors in NS5832:2014 are Threat, Susceptibility and Consequence. One noteworthy feature of this standard is that it does not rely on any probability estimates, neither for attack nor effects. Only a set of selected values and the consequences of their loss in several threat scenarios are considered.

We see this standard as particularly appropriate for low probability, high impact threats. There are obvious advantages in using a standard commonly used for CI risk assessment in general. One disadvantage for this particular choice is that it is a national Norwegian standard, so far not internationally adopted.

II. ADAPTATION TO IEMI

The standard's methodology is based on a set of scenarios, to be defined by the user according to the situation and threats in question. What we have done in order to adapt the methodology to is simply to provide a predefined set of 7 scenarios, covering various aspects of the threat.

This paper builds on results from the EU FP7 project "HIPOW", grant number 284802.

These scenarios cover the following "Threats":

1. Small jammers, WLAN, GPS, GSM etc.
2. Hand held small IEMI and injection devices.
3. Portable (suitcase type) IEMI devices.
4. Large, vehicle carried IEMI devices.
5. Offsite attack, on links or required infrastructure.
6. Military attack, compact, sophisticated IEMI devices.
7. Nuclear Electromagnetic Pulse.

All the tricky issues of e.g. the vast parameter spaces, target susceptibility statistics, perceived aggressor capabilities and competence, as well as the classified issues are hidden in the scenarios. Obviously, this may be an oversimplification, however though not perfect it is good enough for the intended purpose; a DIY first order IEMI risk assessment.

III. ANALYSIS METHODOLOGY

The actual analysis starts with the compilation of a prioritized list of the various functions the unit under analysis is expected to maintain. These are the "Values" to protect. Along with this is a corresponding list of "Consequences", i.e. the impact of failing functions.

Then there is a survey of the electronic systems and sub-, support-, backup- etc. systems as well as external links that are required to perform the critical functions. From the previous lists a corresponding ranking of the technical hardware is performed.

Next, there is a survey of any protective measures already implemented, such as extra shielding, general EMI measures, access control, surveillance, backup and recovery routines etc.

The various hardware are indicated on one or more maps of the physical layout of unit under analysis. Also shown on the map are the protective measures, and access zones for the general public, visitors, employee categories etc., as well as adjacent vehicle access zones.

The maps are analyzed for each of the scenarios, in order to establish the likely impacts of the corresponding RF-attacks.

In general this boils down to distances, modified by whatever protective measures they have implemented. The aggressor's ability to identify, locate and observe the target systems are also emphasized.

IV. SUMMARY

It is hoped that the Risk Analysis will make the users aware of the likely consequences of IEMI, and demonstrate the value of implementing even basic protective measures.

REFERENCES

[1] O.H. Arnesen, J. Godø, M. Maal, "HPM/NNEMP Risk Assesment Guide", Deliverable 7.3, EU FP7 Grant number 284802, Jan. 2016.

[2] E. Genender, H. Garbe, F. Sabath "Probabilistic Risk Analysis Technique of Intentional Electromagnetic Interference at System Level", IEEE Trans. on EMC Vol. 56, No.1 Feb 2014, 200-207.

[3] Fortifikasjonsverket (Sweden), "Vägledning för skydd mot avsiktiga EM-hot", IEMI mitigaton guide, Nov. 2017.