Maintaining Functional Safety under an Intentional Electromagnetic Interference (IEMI) Attack.

Per Ängskog[a,b] and Ben Oakes[a]
[a]KTH – Royal Institute of Technology, Stockholm, Sweden
[b]University of Gävle, Gävle, Sweden

Abstract—**The importance of protection against IEMI effects in civilian applications is growing rapidly as more and more societal infrastructure is equipped with electronic devices. This paper discusses methods to help maintaining functional safety in the event of an IEMI attack.**

I. Introduction

Today the societal infrastructure is becoming increasingly dependent on electronic communications and electrical control systems, e.g. the so called SCADA (Supervisory, Control and Data Acquisition) systems. These systems and communications solutions are often installed with the intent to modernize and facilitate operations or to protect against unauthorized access to buildings and vehicles, etcetera. Commonly, the functional benefits of the installation are prioritized, while security aspects are considered secondary issues. When discussed, it is mainly information security and data encryption that are addressed.

The security against intentional electromagnetic interference – robustness – is, in most cases, nonexistent. Criminals have already taken advantage of this weakness and the threat increases as the knowledge of vulnerability becomes widely spread amongst the common public, and that the IEMI sources are readily accessible at affordable prices [1]. To mitigate the effects of an IEMI attack it is necessary to decrease the risks and potential effects on the system in question. This is discussed extensively by Månsson et al in [2]. Even if a device is tested and verified against the appropriate EMC directive regulations, it will not necessarily survive and maintain functionality in the case of an attack[3].

II. IEMI and Functional Safety

The intention of an attack could be anything ranging from pranks to sabotage or terrorism and the resulting effect may be very limited or catastrophic. The Institution of Engineering and Technology (IET) are presenting a new 'Guidance' on how to achieve cost-effective EMC for Functional Safety compliance [4] based on the IEC standard 61508 focusing on functional safety due to EMI. Clearly, functional safety requires a much higher resilience to EMI in general and IEMI in particular since the normal EMC standards mainly are focused upon achieving interoperability between devices. The 'Guidance' points out several techniques and measures to achieve a higher level of functional safety, for example:

a. Separation of safety & non-safety functions
b. System design and development including malfunction and diversity
c. Fault monitoring, recording, analysis and integrity

The physical separation of safety and non-safety functions should be made already in the initial design phase or it will prove very costly. Interfaces between safety and non-safety functions must be clearly specified to avoid unintentional coupling mechanisms between the two. Documentation of all measures must be meticulously maintained to avoid mistakes in any subsequent redesign.

To obtain high 'Safety Integrity Levels' (SILs), IEMI related malfunctions must be possible to detect and counteract. The strategy to achieve high SILs primarily includes prevention, secondly mitigation and eventually accommodation. Technological diversity is required to reduce the vulnerability and avoid undetected failures resulting from IEMI attacks. The last resort should be a graceful degradation where a minimum functionality is maintained instead of a total break-down.

An IEMI attack leaves no traces unless it causes physical damage. Therefore it is important to have clever Event Data Recorders (EDRs) that not only record detected EMI but also other unexpected events and anomalies in the system, allowing immediate appropriate action as well as facilitating post-event analysis.

The authors of this paper are members of the project "Protection against IEMI threats" initiated at KTH in 2013. The issue of functional safety is of great importance to the project, a mission from Fortifikationsverket, the Swedish Fortifications Agency, the primary funder of the operation.

III. Summary and Conclusions

Utilizing structured techniques and measures when designing a system or equipment, catastrophic errors can be evaded in the case of an IEMI attack. EDRs should be installed to avoid denial-of-service due to IEMI by moving the system into a state of graceful degradation. The same EDRs may also help to identify the approach of attack.

References

[1] E. Savage and W Radasky, "Overview of the threat of IEMI (intentional electromagnetic interference)," Proc. of the *2012 IEEE Int. Symp. on EMC*, Pittsburgh (PA), USA, August 2012, pp. 317–322

[2] D. Månsson, R. Thottappillil and M. Bäckström, "Methodology for Classifying Facilities with Respect to Intentional EMI," IEEE *Trans. Electromagn. Compat*., vol. 51 , no. 1, pp 46–52 Feb. 2009.

[3] D. Imeson, B. Lytollis, B. Kirk and K. Armstrong, "Workshop on EMC for Functional Safety for EMC-Europe 2013"

[4] 'Overview of techniques and measures related to EMC for Functional Safety', The Institution of Engineering and Technology, 2013. Available online: www.theiet.org/factfiles