Use of C-UAS System and Its EM Effect Analysis

Tae Heon Jang
RF Application Technology Center
Korea Testing Laboratory (KTL)
Ansan-si, Gyeonggi-do, Korea
thjang@ktl.re.kr

Jeong Ju Bang
Aerospace EM Technology Center
Korea Testing Laboratory (KTL)
Jinju-si, Gyeongsangnam-do, Korea
jjbang@ktl.re.kr

Jeong Min Kim
Aerospace EM Technology Center
Korea Testing Laboratory (KTL)
Jinju-si, Gyeongsangnam-do, Korea
jmkim@ktl.re.kr

Abstract—Counter UAS(C-UAS) system is protection system for infrastructure against UAS threats. Most of C-UAS systems use radar and RF jammer for detection and neutralization of UAS respectively. C-UAS system is installing in critical facilities such like airport, nuclear power plant and energy infrastructures in many countries for security against UAS threats. However these EM sources may affect to the existing critical system, subsystem or equipment around them. It needs to assess EM vulnerability before installation of them for safety in the aspect of EMC. This paper investigates how to assess EM vulnerability according to IEC standards and others and proposes the necessity of a new standard to deal with it.

Keywords- C-UAS, EM, Vulnerability, Assessment

I. INTRODUCTION

UAS is considered a threat when its operation has, or indicates, the potential to harm life, information, operations, environment and/or property. Counter UAS system refers to a set of technological tools to monitor, detect, identify, record and enable response to unauthorized UAS activities; C-UAS may also include countermeasures capable to neutralize, or limit, potential risks. Different types of deployment can be considered: C-UAS system placed in fixed positions, mounted on vehicles or drones, or portable. Most of C-UAS systems use radar and RF jammer for detection and neutralization of UAS. C-UAS system is installing in critical facilities such like airport and nuclear power plant for security against UAS threats. However these EM or HPEM source may affect to the existing critical system, subsystem or equipment around them. It needs to assess EM vulnerability before installation of them for safety in the aspect of EMC. This paper investigated IEC standards and other standards on the assessment of EM vulnerability in civil critical infrastructures due to EM or HPEM sources.

II. USE of COUNTER UAS SYSTEM

Figure 1 shows examples of C-UAS introduced at infrastructures. Some of C-UAS use radars for detecting UAS and RF jammer for neutralizing UAS. In future, C-UAS system may introduce HPEM sources to counter the threat of UAS swams. The use of C-UAS system render that HPEM compatibility is getting more important in the existing system.

(a) C-UAS for nuclear power plant

(b) C-UAS for airport

Figure 1. Examples of C-UAS system used at infrastructures.

III. EM EFFECT ANALYSIS AND ASSESSMENT

IEC/TS 61000-5-9 discusses methods for the assessment of systems to the effects of HPEM.

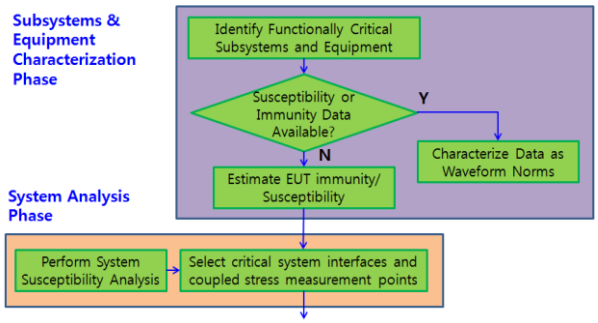

Figure 2. Assessment methodology flow chart in IEC 61000-5-9

From ITU-T K.81, Vulnerability level (VL) of a system for infrastructure can be derived from equation (1).

III. CONCLUSION

The near use of HPEM sources will drive IEC TC77 SC C to establish the method of analysis and assessment for HPEM vulnerability, hazard and risk.

REFERENCES

[1] IEC/TS 61000-5-9, System-level susceptibility assessments for HEMP and HPEM, August 2009
[2] ITU-T K.81, High-power electromagnetic immunity guide for telecommunication systems, June 2016