

IEMI 복사에 의한 네트워크 통신 장비의 취약성 분석

서창수, 허창수^a, 이성우, 진인영

인하대학교 전기공학과

Vulnerability Analysis of Network Communication Device by Intentional Electromagnetic Interference Radiation

Chang-Su Seo, Chang-Su Huh^a, Sung-Woo Lee, and In-Young Jin
 Department of Electrical Engineering, Inha University, Incheon 22212, Korea

(Received October 10, 2017; Revised October 16, 2017; Accepted October 17, 2017)

Abstract: This study analyzed the Vulnerability of Network Communication devices when IEMI is coupled with the Network System. An Ultra Wide Band Generator (180 kV, 700 MHz) was used as the IEMI source. The EUTs are the Switch Hub and Workstation, which are used to configure the network system. The network system was monitored through the LAN system configuration, to confirm a malfunction of the network device. The results of the experiment indicate that a malfunction of the network occurs as the electric field increases. The data loss rate increases proportionally with increasing radiating time. In the case of the Switch Hub, the threshold electric field value was 10 kV/m for all conditions used in this experiment. The threshold point causing malfunction was influenced only by the electric field value. The correlation between the threshold point and pulse repetition rate was not found. However, in case of the Workstation, it was found that as the pulse repetition rate increases, the equipment responds weakly and the threshold value decreases. To verify the electrical coupling of the EUT by IEMI, current sensors were used to measure the PCB line inside the EUT and network line coupling current. As a result of the measurement, it can be inferred that when the coupling current due to IEMI exceeds the threshold value, it flows through the internal equipment line, causing a malfunction and subsequent failure. The results of this study can be applied to basic data for equipment protection, and effect analysis of intentional electromagnetic interference.

Keywords: Ultra wide band electromagnetic radiation, Vulnerability analysis, IEMI (intentional electromagnetic interference), Network device

1. 서론

정보화 시대의 발전으로 인하여, 인터넷과 통신기술을 이용하여 컴퓨터들끼리 서로 네트워크망을 구성하며 다량의 데이터를 주고받도록 진화하였다. 이러한 통

신 네트워크는 의사소통의 가장 중요한 부분이 되어 현대 사회에서 필수적인 요소로 자리 잡았다. 이와 같이, 정보화 시대에 있어서 네트워크 시스템에 대한 의존도가 점점 더 증대되고 있다. 이러한 네트워크 시스템 장비는 외부의 과도 전자기파에 의해 고장 또는 파손될 수 있으며, 네트워크 연결에서 원치 않은 신호를 수신하는 오동작을 일으킬 수 있다 [1,2]. 따라서 본 연구에서는 네트워크 시스템에 대한 전자기 펄스 영향을 평가하기 위해 근거리 네트워크에서 주로 이용되고 있는 switch hub와 workstation에 대한 전자기 펄스

a. Corresponding author; cshuh@inha.ac.kr

Copyright ©2018 KIEEME. All rights reserved.
 This is an Open-Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (<http://creativecommons.org/licenses/by-nc/3.0>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

노출의 취약성을 비교·분석하였다. 또한 각 장비별 오동작 임계치 측정과 실시간 네트워크 상태 분석을 통하여 데이터 손실률을 관찰하였다.

2. 실험 구성

2.1 실험 Source

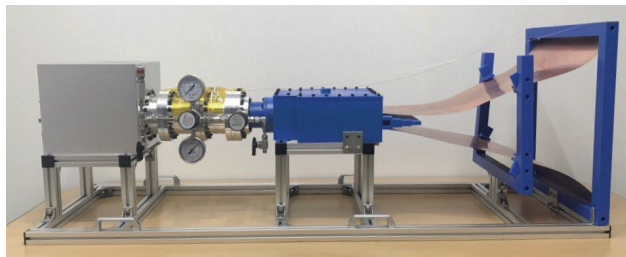
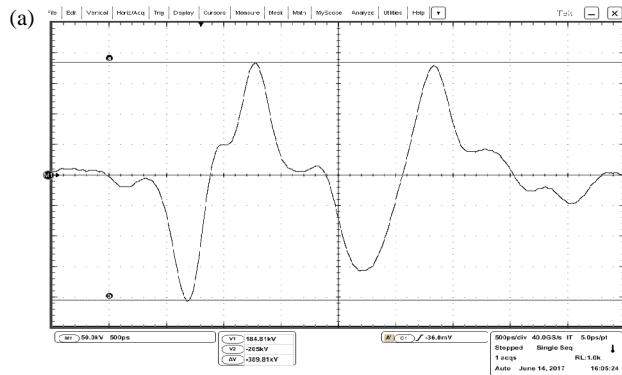


Fig. 1. IEMI source (UWB Generator).



Contents		Value
Power supply	Output voltage	≥ 500 V
High voltage generator	Output voltage	≥ 200 kV
Pulse generation	Output voltage	≥ 180 kV
Antenna	Frequency	500 MHz
	bandwidth	~ 2 GHz
System	Waveform	Bipolar
	Pulse rise time	≤ 200 ps
	FWHM	≤ 2 ns
	PRF	1~100 Hz
	V_{far} (rE)	≥ 180 kV

Fig. 2. (a) Measurement waveform and (b) UWB generator specification.

IEMI 복사 시험 source로 사용된 UWB 발생 장치는 매우 짧은 시간의 펄스로 낮은 에너지를 가지므로 매우 작은 크기로 구성될 수 있기에 위험한 무기로 사용될 수 있다 [3]. UWB 발생 장치는 그림 1과 같이 왼쪽은 전원장치, 고전압발생기, 펄스 성형망, 오른쪽은 초광대역 안테나로 구성되며 700 MHz의 중심 주파수를 가지며 최대 180 kV의 출력 전압을 가진다. 이 장치에 의한 복사 펄스를 6 m 거리에서 측정하였을 때 그림 2(a)와 같은 이중 지수 형태를 가지며 상승시간은 200 ps이고, 펄스폭은 2 ns이다. 파형의 측정된 전계 값은 6 m 거리에서 약 30 kV/m 전계 크기를 갖는다. 시험에 사용된 장비는 출력 전압이 가변 불가능하므로 장비와 EUT의 거리에 따라 복사 세기로 조절하였다.

2.2 시험대상기기(EUT)

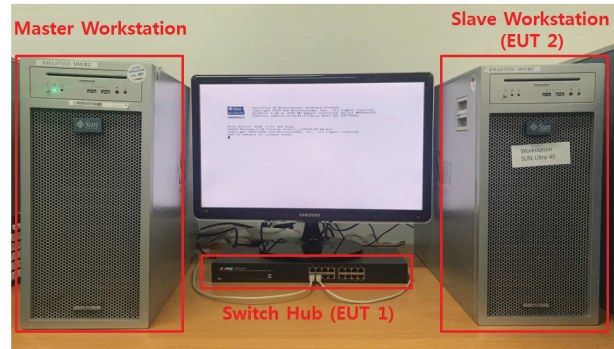


Fig. 3. EUT local area network system.

EUT 1은 네트워크 분야에서 LAN (근거리 네트워크)을 구성할 때 필수적인 요소 중의 하나인 switch hub이다. 버스 형태로 접속되는 LAN에서 분기하여 컴퓨터들을 LAN에 접속시키는 집선 장치로, 각 노드를 LAN에 연결해 주는 것은 물론 각 노드에서 발송되는 데이터를 바탕으로 수신 노드의 주소를 판독하여 수신 노드로 데이터를 전송한다. 전원은 100~240 VAC이며 16개의 port를 지원한다.

EUT 2는 특수한 분야에 사용되는 목적으로 만들어진 고성능의 컴퓨터인 workstation이다. 실험에 사용된 workstation은 전력 계통에서 클라이언트/서버 네

트위크를 제어하는 다중 사용자 시스템으로 사용된다. 이 장비는 유닉스를 기반으로 한 solaris 10 운영체제를 사용한다.

실험에 사용될 시스템은 그림 3과 같이 switch hub와 두 대의 workstation을 이용하여 근거리 네트워크로 구성하였다. 네트워크 신호를 주고받는 경로는 master workstation-hub-slave workstation-hub-master workstation 방식으로 ping 보내 다시 응답을 받는 과정을 정상 동작 범주로 정의하였다. EUT 2는 slave workstation을 대상으로 하였다.

2.3 실험 조건 및 방법

실험은 근거리 네트워크 유지한 상태에서 표 1과 같이 3개의 pulse type으로 최대 거리 20 m부터 최소 far field 거리인 4 m까지 단계별로 실험하였다. 실험 방식은 40개의 ping을 주고받는 도중에 복사 환경에 노출하여 네트워크 동작 형태를 관찰하였다. 외부 환경에 대한 영향을 최소화시키기 위하여 네트워크 케이블은 STP를 사용하였으며 오실로스코프 및 모니터링 시스템은 외부에 위치시켰다. 실험 장소는 정보통신산업진흥원 내부 무반사실에서 이루어졌다.

그림 4는 EUT 1 복사 내성 시험과 EUT 2 복사 내성 시험에 관한 구성도이다. 시험대상 기기만을 펄스 전자기파에 노출시키고, 복사되는 동안 발생하는 동작 유형 및 커플링 신호를 모니터링 시스템과 오실로스코프를 통해 확인하였다 [4,5]. IEMI에 가장 취약한 상태를 고려하기 위하여 복사 방향은 port 부분이 노출된 정면을 향하여 실험을 수행하였다. 오실로스코프를 통해 EUT 내부 PCB의 3.3 VDC 전원선로(channel 1), AC 전원 접지단자와 내부 PCB 접지 단자 선로(channel 3)와 STP 케이블 선로(channel 4) 커플링 전류를 관찰하였다.

Table 1. Pulse type used in radiation experiments.

Pulse type	Execution time (s)	Pulse repetition frequency (Hz)	Num. of total pulse
Pulse A	20	1	20
Pulse B	10	10	100
Pulse C	5	20	100

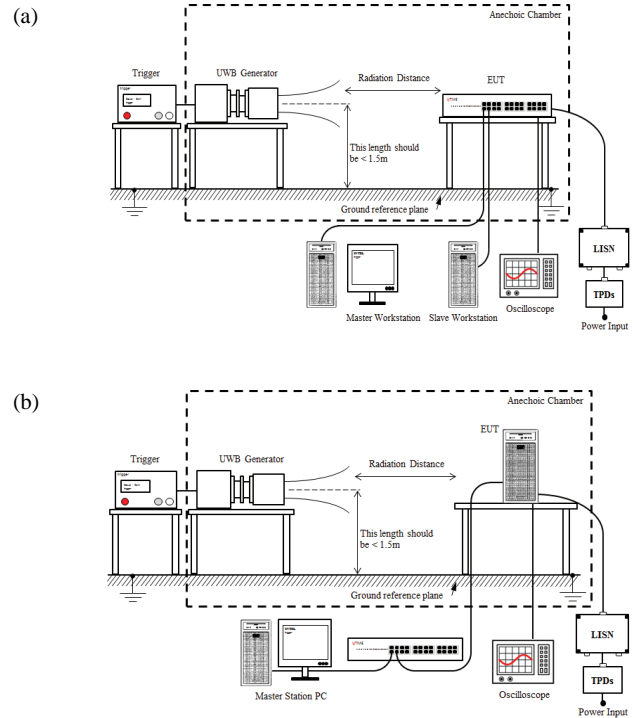


Fig. 4. (a) EUT 1 experiment setup and (b) EUT 2 experiment setup.

3. 결과 및 고찰

3.1 EUT 1 실험 결과

실험 결과는 네트워크 시스템 동작 형태와 커플링 신호로 구분하여 분석하였다 [6]. 표 2는 광대역 전자기파 복사에 대한 network hub 내성 결과를 요약한 것이다. 표에 의하면 20~18 m의 조건에서는 hub가 정상 동작하며 네트워크 연결상의 문제가 없다는 것을 알 수 있다. 하지만 18 m 이하의 거리, 즉 전계 세기 10 kV/m 이상부터 네트워크 연결상의 오동작이 발생함을 알 수 있다. 오동작의 유형은 방사가 시작됨과 동시에 네트워크 연결이 끊어지게 되고 방사 시간 동안 네트워크 데이터 손실이 생긴다. 그리고 방사 시간이 끝난 후 대략 4초 동안 self-recovery가 진행된다. Self-recovery란 전자기파가 방사하는 동안에 오동작이 발생하지만, 방사가 완료된 후 장비 스스로 제 기능을 회복하는 것을 말한다. 임계치 이후 최대 far field 거리인 5 m까지 오동작 현상만 발생하고 파괴 현상을 나타내지 않았다. 그림 5는 광대역 전자기파 펄스 조건에 따라 데이터 손실률을 그래프로 나타낸 것이

Table 2. Switch hub immunity results for UWB radiation.

Power (kV/m) /distance (m)	Pulse type	Network operation	Data loss (%)
10/20	A	Normal	0
	B		0
	C		0
10.3/17.5	A	Malfuntion	53
	B		30
	C		13
12/15	A	Malfuntion	60
	B		40
	C		23
18/10	A	Malfuntion	53
	B		38
	C		22
38/5	A	Malfuntion	51
	B		38
	C		28

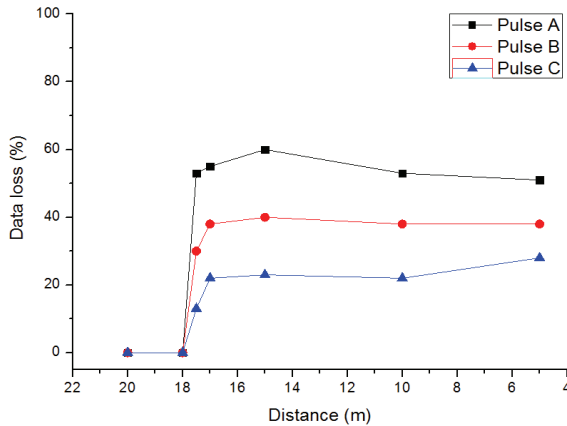


Fig. 5. Data loss rate according to pulse type by distance EUT 1 experiment.

다. Pulse type A의 데이터 손실률은 임계 지점 이상에서는 전계 세기와 상관없이 약 55%로 나타났다. Pulse type B, C 또한 임계 지점 이상에서는 전계 세기와 상관없이 각각 38%, 20%의 데이터 손실률을 나타낸다. 이를 통해 전계 세기는 오직 오동작 현상을 유발하며 데이터 손실률과는 상관관계가 없음을 확인할 수 있다. 각각의 펄스 조건과 데이터 손실률을 비교하여 보았을 때 다음과 같은 결론을 얻을 수 있다.

$$Data\ loss\ (\%) = \frac{Radiating\ Time + Self\ Recovery\ Time}{\neq\ twork\ Connect\ Time} \quad (1)$$

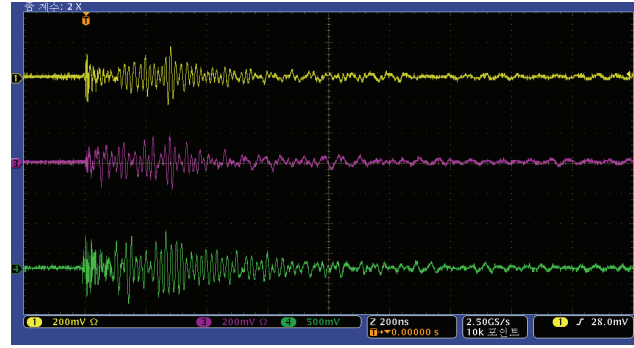


Fig. 6. EUT's coupling current waveform in case of UWB 10 kV/m exposure.

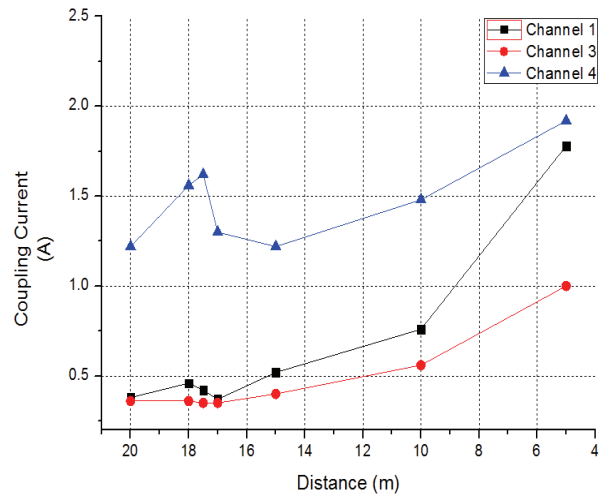


Fig. 7. Peak value of coupling current according to distance in pulse type B.

데이터 손실률은 방사 시간과 self-recovery 시간을 합한 값을 전체 네트워크 연결 시간으로 나누어 백분율로 환산한 값이다. 이는 데이터 손실률은 EUT가 전자기파에 노출되는 시간에 매우 큰 영향을 받는다는 것을 알 수 있다.

그림 6은 광대역 전자기파 전계 10 kV/m에 노출되었을 때 EUT 내부에 커플링 되는 전류의 파형이다. 그림 7은 거리에 따른 EUT 내부 커플링 전류 피크 값을 그래프로 나타낸 것이다. 광대역 전자기파 3개의 pulse type 모두 위의 그래프와 유사한 현상을 나타냈다. EUT의 임계치 지점인 18 m 전에는 비교적 EUT 내부 라인(channel 1, 3)보다 외부 네트워크 라인(channel 4)을 통해 많은 전류가 커플링 된다. 임계치를 넘어서게 되면 외부 네트워크 라인에 커플링 되

는 전류는 1.6 A에 도달하게 되고 EUT 내부 라인 전류가 증가하기 시작한다. 이때부터 네트워크 오동작 현상이 일어나게 되는데, 이는 전자기파 방사에 의해 커플링 된 신호가 장비 외부로 빠져나가지 못하고 기기 자체에 교란을 일으키는 것으로 사료된다. 임계치를 넘어선 이후부터는 각 채널 모두가 전계 세기가 증가할수록 전류가 증가하였다. Pulse type에 관계없이 커플링 되는 전류 효과가 비슷한 결과를 통해 펄스 반복률과 커플링 되는 전류의 세기와는 연관이 없음을 알 수 있으며 오직 펄스 피크 전계 세기가 영향을 준다는 것을 알 수 있다.

3.2 EUT 2 실험 결과

표 3은 workstation에 대한 광대역 전자기파 복사 내성 결과를 요약한 것이다. 표에 의하면 7~20 m 거리에서는 pulse type과 상관없이 모든 조건에서 workstation이 정상 동작하며 네트워크 연결상의 문제가 없다는 것을 알 수 있다. 하지만 6.5 m 이하의 거리, 즉 전계 세기 27.7 kV/m 이상부터 pulse type B, C에서 네트워크 연결상의 오동작이 발생함을 알 수 있다. Pulse type B에서는 방사 시간 동안 일시적으로 네트워크 연결이 끊겼다가 다시 복구되는 반면, pulse type C에서는 방사 시간 동안 지속적으로 네트워크 연결이 끊겼다가 방사 시간이 끝난 후 대략 1분 동안 self-recovery가

Table 3. Workstation immunity results for UWB radiation.

Power (kV/m) /distance (m)	Pulse type	Network operation	Data loss (%)
10/20	A	Normal	0
	B		0
	C		0
25.7/7	A	Normal	0
	B		0
	C		0
27.7/6.5	A	Normal	0
	B	Temporary MalfunTION	15
	C	MalfunTION	6
30/6	A	Temporary MalfunTION	6
	B	MalfunTION	32
	C	MalfunTION	12
45/4	A	MalfunTION	47
	B	MalfunTION	34
	C	MalfunTION	13

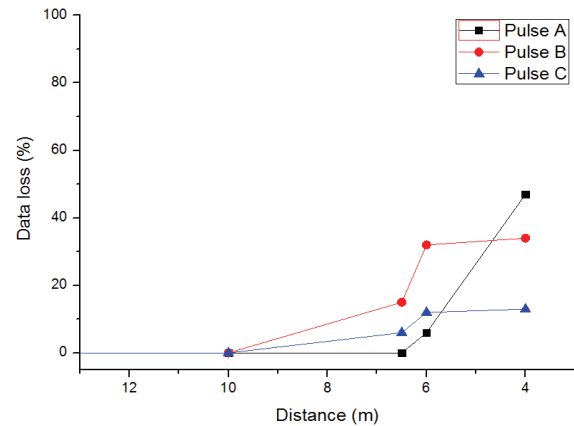


Fig. 8. Data loss rate according to pulse type by distance in EUT 2 experiment.

진행된다. 6 m 거리에서는 pulse type A에서도 일시적인 오동작을 보이며 pulse type B, C는 방사 시간 동안 오동작을 보인다.

그림 8은 광대역 전자기파 펄스 조건에 따라 데이터 손실률을 그래프로 나타낸 것이다. 기존 hub 실험과 다르게 workstation 실험의 경우 일시적인 오동작 현상이 일어나는데 이는 hub 장치보다 workstation의 내부 PCB 구조가 복잡하기 때문으로 유추할 수 있다. 또한, 펄스 조건에 따라 임계지점이 다른 것을 보았을 때 복잡한 회로의 경우 펄스 반복률과 상관관계가 있음을 알 수 있다. 펄스 반복률이 높아짐에 따라 같은 전계에 있어서 장비가 민감하게 반응함을 알 수 있다. 데이터 손실률의 경우 hub 실험과 마찬가지로 방사 시간에 비례하였다.

4. 결론

본 논문에서는 광대역 전자기파 복사에 의한 2종류의 통신 네트워크 장비를 EUT 대상을 선정하여 피해 효과를 수행하고 실험 결과를 통해 다음과 같은 결론이 도출되었다.

- 1) 광대역 전자기파로 인한 통신 네트워크 장비의 오동작은 장비 유형에 따라 다르게 나타났다. Switch hub의 경우 정상 동작, 오동작(네트워크 손실)으로 2개의 동작 형태를 보였다. 위의 오동작은 전계 세기가 증가함에 따라 발생하였으며 임계 전계치는 10 kV/m 이상이였다. 오동작 발

생 시 데이터 손실률은 방사 시간에만 비례하여 증가하였으며 펄스 반복률과의 상관관계를 찾지 못하였다.

Workstation의 경우 정상 동작, 일시적인 오동작, 오동작으로 3개의 동작 형태를 가졌다. 위의 동작 형태는 전계 세기가 증가함에 따라 순차적으로 발생하였으며 임계 전계치는 Hub 실험과 달리 펄스 조건에 따라 다르게 나타났다. 펄스 반복률이 높아질수록 장비가 취약하게 반응하여 임계치가 낮아짐을 확인하였다. 두 장비에 대한 실험 모두 파괴 현상은 일어나지 않았는데, 이는 광대역 전자기파 복사 신호가 펄스 형태로 매우 짧은 시간에 복사되어 에너지 측면에서 매우 낮은 양을 가지기 때문임을 유추할 수 있다.

- 2) 본 논문에서는 장비의 오동작 이유를 추정하기 위하여, 방사되는 동안 내부 커플링 전류를 측정하였다. 측정 결과, 임계치 이전에는 장비 내부 라인보다는 외부 네트워크 라인을 통해 많은 전류가 커플링 되었다. 하지만 오동작이 일어나는 임계 지점 이후, 외부 네트워크 라인에 커플링 되는 전류가 갑자기 감소하고 장비 내부 라인에 커플링 되는 전류가 상승하기 시작하였다. 이는 광대역 전자기파 복사에 의한 커플링 전류가 외부로 빠져나가다가 임계치 이상을 넘어서게 되면 내부 장비 라인을 통해서 흐르게 되어 오동작 및 고장이 발생하게 됨을 유추할 수 있다.

감사의 글

본 연구는 산업통상자원부(MOTIE)와 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구 과제입니다(No.20161015201550).

REFERENCES

- [1] D. Nitsch, M. Camp, F. Sabath, J. L. ter Haseborg, and H. Garbe, *IEEE Trans. Electromagn. Compat.*, **46**, 380 (2004). [DOI: <https://doi.org/10.1109/TEMC.2004.831842>]
- [2] IEC, *IEC 61000-2-13: Electromagnetic compatibility (EMC) - Part 2-13: Environment - High-power electromagnetic (HPEM) environments - Radiated and conducted* (IEC, Geneva, 2005) p. 27.
- [3] M. Camp, H. Garbe, and D. Nitsch, *Proc. 2001 IEEE EMC International Symposium. Symposium Record. International Symposium on Electromagnetic Compatibility (Cat. No.01CH37161)* (IEEE, Montreal, Canada, 2001) p. 1015. [DOI: <https://doi.org/10.1109/IEMC.2001.950538>]
- [4] R. T. Tientcheu and D. Pouchè, *Proc. 2015 International Conference on Electromagnetics in Advanced Applications (ICEAA)* (IEEE, Turin, Italy, 2015) p. 1357. [DOI: <https://doi.org/10.1109/ICEAA.2015.7297339>]
- [5] IEC, *IEC 61000-4-36: Electromagnetic compatibility (EMC) - Part 4-36: Testing and measurement techniques - IEMI immunity test methods for equipment and systems* (IEC, Geneva, 2014) p. 20.
- [6] W. S. Cho, P. K. Kwak, C. Y. Park, J. K. Yang, and H. S. Geum, *J. Korean Inst. Electromagn. Eng. Sci.*, **22**, 220 (2011). [DOI: <https://doi.org/10.5515/KJKIEES.2011.22.2.220>]