

고출력 비핵 전자파 대책기술 연구개발 동향

권 중 화

한국전자통신연구원(ETRI)

I. 개 요

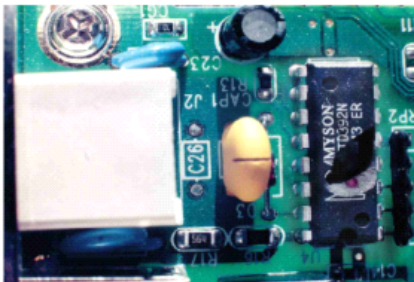
전력망, 통신망 등 국가 주요 인프라와 더불어 원자력 발전시설과 같은 주요 국가시설에 대해 고출력 전자파에 대한 위협이 높아지고 있고, 이에 대한 방호 평가 및 대책기술에 대한 관심과 요구가 높아지고 있는 실정이다. 미국 EMP 위원회에서는 2008년 보고서에서 고출력 전자파 등에 의해서 전력망이 피해를 입어 전국적인 단전 사고가 발생하면 1년 이내 미국 국민의 90%가 기아, 질병, 사회범죄 등으로 목숨을 잃을 것으로 추산하고 있으며, 특히 북한이 미국 상공 궤도에서 핵탄두를 폭발시켜 발생하는 고출력 전자파로 미국을 공격한다면 미국의 전력망이 완전히 파괴돼 복구에 1년 6개월이 필요하며, 수백만 명이 목숨을 잃을 수 있다는 보도 등이 나오고 있는 실정이다.

국내에서도 국가 주요 기반시설인 전력망 및 통신망 등은 컴퓨터와 각종 IT 기기를 이용해 제어 및 통제되고 있으며, 이러한 제어 통제 시스템은 고출력 전자파에 매우 취약한 것으로 알려져 있다. 따라서 이러한 기기들이 고출력 전자파 폭발이나 핵폭발에 의한 전자파 펄스 등에 노출되어

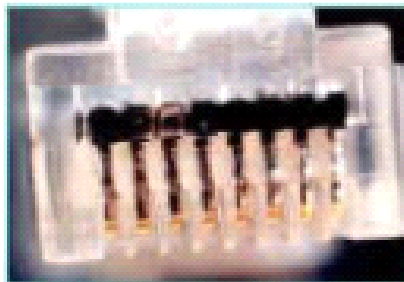
오동작하면, 사회기반 시스템에 문제를 일으키게 되어, 사회적으로 큰 혼란을 야기할 가능성이 높아지고 있다. 따라서 고출력 전자파를 이용한 전자파 테러와 같은 잠재적인 위협은 중요한 보안 이슈로 대두되고 있는 실정이다.

철도, 항공을 비롯한 많은 국가 주요 인프라(critical infrastructures) 및 시설은 ICT 기술의 발전과 더불어 전기·전자 회로 및 유무선 전파통신에 의해 제어되고 운용되는 상황에서 100 V/m 이상의 고출력 전자파 펄스에 노출된 경우, 큰 피해가 우려된다. 특히, 데이터 센터(Internet Data Center) 등 대부분의 주요 통신시설은 현재 고출력 전자파 펄스 공격에 거의 무방비 상태이므로, 이에 대한 평가 및 대책기술 개발이 시급한 실정이다. [그림 1]은 고출력 전자파에 노출되어 손상된 전기전자 부품의 예를 보여준다.

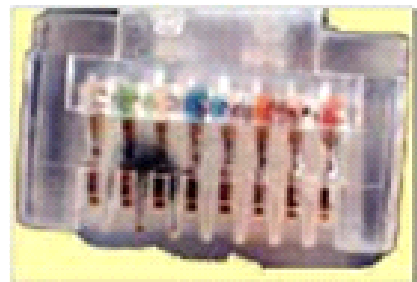
고출력 전자파로부터 기기 및 시스템, 그리고 이를 포함한 주요 시설을 보호하기 위한 연구가 미국과 일본, 유럽연합 등을 중심으로 활발히 진행 중에 있다. 핵폭발에 의한 전자파 펄스 등 고출력 전자파에 대한 연구가 주로 군을 중심으로 진행되어, 연구 내용이나 결과들이 대부분의 국가에서 비밀로 취급하여 공개된 자료가 미비한 실정이다. 최근 군



500 V 신호 인가에 따른 칩 손상



4.5 kV 신호 인가에 따른 커넥터 손상



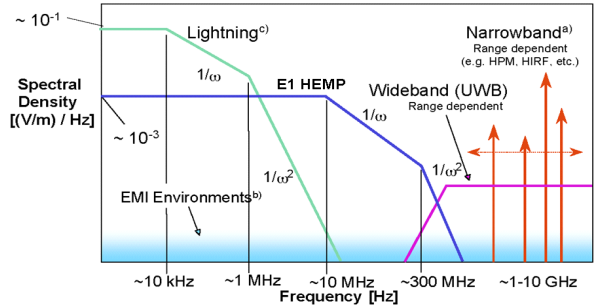
[그림 1] 고출력 전자파 영향 시험 결과: IC 칩 및 Ethernet 커넥터 영향

「본 연구는 미래창조과학부 및 정보통신기술연구진흥센터의 정보통신·방송 연구개발사업의 일환으로 수행하였음. (B0194-16-1001, 전자파 잔향실 기반 실환경 전파 측정 및 평가 기술 연구)」

시설뿐만 아니라, 주요 민간 시설들도 전기·전자시스템에 의해 유지·관리되고 있어, 고출력 전자파에 의한 영향이 커져 민간 분야에서도 고출력 비핵 전자파에 대한 연구를 진행 중인 것으로 알려져 있다. 본 고에서는 고출력 비핵 전자파에 대한 이해를 높이기 위해 고출력 비핵 전자파의 특성 및 대책기술 등에 대해 기술하고자 한다.

II. 고출력 비핵 전자파 특성

낙뢰(lightning strikes)나 정전기 방전(ESD) 근처에서의 전자파, 핵폭발에 의한 전자파, 그리고 레이더 시스템 근처에 전자파 등 고출력 전자파는 통상 높은 세기의 과도 전기장 및 자기장을 갖는 펄스 형태의 전자파로서 전력·통신·금융 서비스 망 등의 다양한 전기·전자시스템을 일시에 파괴 또는 오동작을 유발할 위험이 있다. 고출력 전자파는 강력한 에너지를 가진 순간적인 전자기 충격파로, 전자기기의 오동작 또는 물리적 파괴를 유발하는 것으로, 고출력 전자파의 종류는 핵폭발에 의해 발생하는 핵(nuclear) 고출력 전자파와 핵 이외의 원인에 의해 발생하는 고출력 비핵(non-nuclear) 고출력 전자파로 구분한다. 고고도 핵 전자파(High Altitude Electromagnetic Pulse: HEMP)는 지상 30 km 이상에서 핵폭발에 의해 생성되는 펄스형 전자파를, 고출력 비핵 전자파(High Power Electromagnetics: HPEM)는 정보기기 등을 손상시키거나, 오동작을 유발할 수 있는 의도적으로 복사·전도된 전자파를 각각 의미한다. <표 1>과 [그림 2]에서는 고출



[그림 2] 고출력 전자파 주파수별 특성 비교

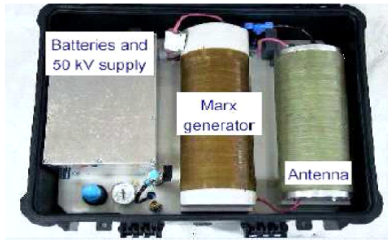
력 전자파와 기존 전자파 장애(EMI)의 특성을 비교하였다. HEMP는 핵폭발에 의해 발생되므로, HEMP에 대한 대책은 군사 시설 및 전시에 국가 운영이 반드시 필요한 주요 시설에 주로 적용되고 있다. RF 및 ICT 기술이 발전함에 따라 민간 시설에 대해서는 핵에 의한 고출력 전자파보다는 고출력 비핵 전자파에 의한 위협의 가능성이 높으며, 이에 대한 90년대 이후 연구들이 많이 진행되고 있다. 고출력 비핵 전자파에 대해서는 HPEM, 전자파 테러(EM Terrorism) 등 다양한 용어들이 사용되었으나, 1999년 2월 스위스 취리히에서 개최된 전자파적합성(EMC) 분야 국제학회에서 고출력 비핵 전자파를 의도성 전자파 장애(Intentional Electromagnetic Interference: IEMI)로 통일하여 사용하기로 하고, 다음과 같이 정의하였다.

IEMI 정의: 테러나 범죄를 목적으로 전기·전자 시스템에 중단, 혼란 혹은 피해를 가하기 위해 노이즈나 신호를 인가하기 위한 의도적이고 악의적인 전자파 에너지 발생(intentional malicious generation of electromagnetic energy introducing noise or signals into electric and electronic systems, thus disrupting, confusing or damaging these systems for terrorist or criminal purposes)

의도성 전자파 장애(IEMI)에 대한 우려와 관심이 높아지는 이유는 다음과 같다. 우선 높은 에너지의 RF 발생원과 효율 높은 안테나 등 고출력 전자파 관련 전자파 기술이 발전됨에 따라서 IEMI 발생원의 급속한 확산이 가능하다는 점이다. [그림 3]은 군 혹은 민간에서 개발된 다양한 고출력 전자파 발생장치와 100 m 거리에서의 전기장 세기를 보여

<표 1> 고출력 전자파 및 전자파장애 특성 비교^[5]

비교 항목	EMI	HEMP	HPEM(IEMI)
주파수 대역	30 MHz~6 GHz (RE) 9 kHz~30 MHz (CE)	~500 MHz	100 MHz~10 GHz
전자파 세기	3 V/m (50 V/m)	50 kV/m	수백 V/m~수백 kV/m
영향 범위	~수십 m	~수백 km	~수백 m
	전기·전자기기	전력/통신망	IDC, 원전 등 주요 건물
발생원	전기·전자기기	핵폭발, 낙뢰 등	E-bomb 등 고출력 복사체



휴대용(man-portable)
전기장: 1.2 kV/m @ 100 m



차량용(transportable)
전기장: 3.3 kV/m @ 100 m



차량용(transportable)
전기장: 500 kV/m @100 m

[그림 3] 군 및 민간에서 개발된 고출력 전자파 발생장치 및 전기장 세기

준다. RF 기술의 발전을 기반으로 소형화된 고출력 전자파 발생장치를 개발하기 위한 연구가 군을 중심으로 진행 중이며, 민수 영역에서도 RF 기술의 발전으로 소형화된 고출력 전자파 발생장치의 개발이 용이하고, 인터넷 등에서 쉽게 획득 가능함에 따라 고출력 전자파에 의한 문제 발생의 가능성은 증가하고 있다. 두 번째로는, ICT 기술이 급속히 발전함에 따라 주요 기반 시설에서 Mission-critical 혹은 Safety-critical 전기전자 시스템들에 대한 사회적 의존의 커지고 있어, 전자파 위협(EM threat)에 대한 사회 시스템의 취약성이 증가하고 있다는 점이다. 특히, 기기 및 시스템의 효율을 높이기 위해 높은 주파수 및 낮은 전압에서 동작하는 IT 시스템의 전자파 내성(EMS) 수준이 낮아지고 있어, 의도성 전자파 장애에 의한 취약성은 높아지고 있는 실정이다. 마지막으로 세계적으로 테러에 대한 위협이 증가하고 있으며, 고출력 전자파 발생원 개발의 용이성, 공격 대상 시설의 전자파 취약성, 그리고 전자파 특성상 물리적 경계 밖에서의 은밀한 공격이 가능하다는 점들 때문에 의도성 전자파 장애(IEMI)가 테러에 사용될 가능성이 높다고 할 수 있다. 이러한 이유로 고출력 비핵 전자파에 대한 세계적인 우려와 관심이 높아지고 있으며, 사회 기반 시설을 보호하고, 사회 안전성을 높이기 위한 다양한 연구들이 미국과 유럽을 중심으로 대부분 보안과제로 수행되었으며, 연구 결과들은 해당 국가에서 정책으로 반영되고 있는 것으로 파악된다.

또한 RF 분야에서의 주요 학술단체인 URSI(International Radio Scientific Union)에서는 이러한 전자파 공격의 가능성을 일반 대중에게 알리고, 그로 인한 사회적 피해를 줄이기 위해 “전자파를 이용한 범죄 행위에 대한 결의문(Resolution of Criminal Activities using Electromagnetic Tools)”을 1999년

8월에 발표하였다. 결의문에서 고출력 전자파와 관련하여 일반인들에게 알리기 위해 다음의 내용들을 기술되어 있다.

- 전자파를 이용한 범죄 행위의 존재
- 물리적 경계를 전자파가 관통하므로, 전자파 기반 범죄는 은밀하고 익명으로 수행 가능성
- 교통, 통신, 보안 및 의약품과 같은 주요 인프라 및 사회의 중요한 기능에 전자파를 사용하는 범죄 행위가 가지는 잠재적인 심각한 영향 가능성
- 전자파 기반 범죄 행위에 의한 국가의 건강한 경제 활동의 잠재적인 중단은 중대한 결과를 초래 가능성

또한 URSI 위원회에서는 전자파를 이용한 공격 및 위협을 고려하고, 다음의 조치를 취할 것을 전자파 적합성(EMC)을 포함한 과학자 그룹에게 권고하였다.

- 취약성 제고를 위해 IEMI를 포함한 HPEM 관련 연구를 수행
- IEMI에 의한 공공시설/주요 인프라를 보호하기 위한 적절한 대책기술 연구
- IEMI에 대한 기기 및 시스템 취약성 평가를 위한 시험 및 평가방법 개발
- 보호 표준 수립에 관한 자료 제공 및 표준화 작업 지원

전기·전자 기기에 대한 고출력 전자파 위협을 이해하기 위해서는, 노출된 기기에 대한 운영상의 문제를 야기할 수 있는 발생 가능한 다양한 유형의 전자파 환경을 이해해야 한다. 고출력 비핵 전자파에 대한 전자파 환경은 신호의 주

파수 특성, 에너지 전달 메커니즘, 그리고 전달 경로에 따라 다음과 같이 구분한다.

- 주파수 특성: 협대역(narrow band) 및 광대역(wideband/broadband)
- 전달 메커니즘: 복사성(radiated) 및 전도성(conducted)
- 전달 경로: Front-door Coupling 및 Back-door Coupling

일반적으로 통신에서 사용되는 분류에서는 Fractional BW와 Percent BW를 근거로 분류한다. 즉, Percent BW가 1% 미만이면, 협대역, 25% 이상이면 광대역으로 분류한다.

$$\text{Fractional bandwidth} = \frac{2(f_h - f_l)}{(f_h + f_l)} \quad (1)$$

$$\text{Percent bandwidth} = \frac{2(f_h - f_l)}{(f_h + f_l)} \times 100 \quad (2)$$

여기서 f_h 와 f_l 는 각각 신호 대역폭의 상한 및 하한 주파수이다.

그러나 통신용 신호에 적용되는 PBW(Percent Bandwidth) 정의는 고출력 전자파의 경우, 190% 이상인 경우가 많아서 적합하지 않아 고출력 전자파 분야에서는 Bandratio(br) 및 PBW(Percent Bandwidth)에 기반한 다음 <표 2>의 분류 방식을 따른다. 즉, br이 1.01보다 적으면 Hypoband(narrowband), 1.01보다 크고 3보다 작으면 Mesoband, 3보다 크고 10보다 작으면 Sub-Hyperband, 그리고 10보다 크면 Hyperband라고 한다.

$$\text{br(Bandratio)} = \frac{f_h}{f_l} \quad (3)$$

$$\text{PBW(Percent Bandwidth)} = 200 \frac{(br - 1)}{(br + 1)} \quad (4)$$

고출력 전자파에서 일반적으로 협대역 파형(Narrowband Waveform)이라 함은 고정된 시간(100 ns ~ 1 ms) 동안 전달되는 거의 단일 주파수(일반적으로 중심 주파수의 1% 미만의 대역폭)이다. 시스템 취약성과 관련하여 협대역 위협은 일반적으로 전기 에너지가 좁은 주파수 대역으로 전달되므

<표 2> 대역폭에 근거한 고출력 전자파 분류

구분	Percent bandwidth(PBW)	Bandratio(br)
Hypoband 혹은 narrowband	$pbw \leq 1\%$	$br \leq 1.01$
Mesoband	$1\% < pbw \leq 100\%$	$1.01 < br \leq 3$
Sub-hyperband	$100\% < pbw \leq 163.64\%$	$3 < br \leq 10$
Hyperband	$163.64\% < pbw \leq 200\%$	$Br > 10$

로, 매우 높은 전력(수천 V/m)을 갖는다. 시험 중인 각 시스템은 각기 다른 취약한 주파수를 가질 수 있으며, 협대역 파형을 가진 시험 장비에서 관찰되는 오작동은 영구적인 손상일 경우가 많다. [그림 4]는 IEC61000-4-35에서 제시된 협대역 시험에 사용되는 시험 설비들이다.

UWB 혹은 SP(Short Pulse) 등 광대역 파형은 시간 영역 펄스가 반복적으로 전달되는 경우가 일반적이다. 광대역 특성은 파형의 에너지가 중심 주파수와 관련하여 상당한 주파수 범위에서 생성됨을 나타낸다. 시간 영역 펄스는 동시에 여러 주파수에서 에너지를 생성하기 때문에, 단일 주파수에서의 에너지 밀도는 훨씬 적으며, 따라서 협대역 신호의 경우만큼 피해가 크지 않다. 그러나 많은 주파수가 동시에 적용되기 때문에, 시스템의 취약점을 찾는 것이 더 적절한 것으로 알려져 있다. [그림 5]는 IEC61000-4-35에서 제시된 광대역의 고출력 전자파 파형을 발생하는 시험 설비들이다.

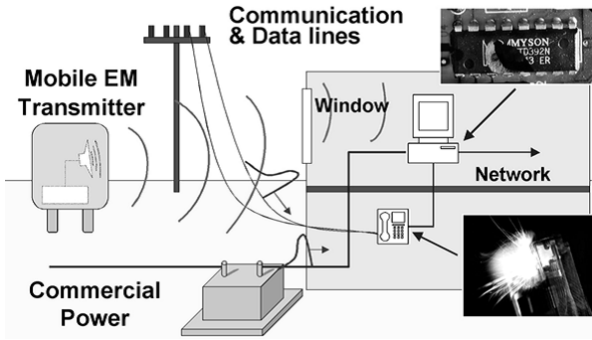
고출력 전자파는 [그림 6]에서와 같이 전자파가 전달되는



[그림 4] 협대역 파형(narrowband/hypoband waveforms)을 갖는 고출력 전자파 시험 시설



[그림 5] 광대역 파형(wideband waveforms)을 갖는 고출력 전자파 시험 시설



[그림 6] 고출력 전자파 전달 메커니즘: 복사성 결합 및 전도성 결합

방식에 따라 공기 중을 통해 전달되는 복사성 결합(radiated coupling)과 전력선이나 통신제어선 등 도선에 유기되어 전달되는 전도성 결합(conducted coupling)으로 구분할 수 있다. 일반적으로 복사성 전자파에 대해서는 보호 구역에 대해 도전성 물질로 만들어진 차폐재를 이용하여 방호하고, 전도성 전자파에 대해서는 다양한 필터를 이용하여 전자파 대책을 수립한다. 또한 고출력 전자파가 전달되는 경로에 따라 Front-door coupling과 Back-door coupling으로 구분되는데, Front-door coupling은 방송통신 등 대상 시설이 의도적으로 사용되는 주파수 대역에 대해 공격하는 방식이고, Back-door coupling은 대상 시설의 의도적으로 사용하지 않는 주파수 대역을 사용하는 방식이다. 일반적으로 Front-door coupling은 대상 시스템의 주파수 대역에 해당되는 협대역 파형을, Back-door coupling은 대상 시스템의 취약 주파수를 알지 못하므로 광대역 파형을 이용한다.

III. 전자파 방호 기술

고출력 비핵 전자파는 핵폭발에 의한 고출력 전자파와는 달리 전자파 발생원으로부터의 거리에 따라 전자파의 세기가 달라진다. 따라서 보호하고자 하는 시설로부터 발생원의 접근을 제어하는 것도 IEMI에 대한 방호 기법 중 하나이다. 이와 같이 고출력 비핵 전자파에 대한 방호기술은 전자파 관점에서의 방호기술과 더불어 보안 관점에서의 방법도 중요한 요소이다.

고출력 비핵 전자파에 대해 보안 관점에서의 방호기술

(security approach)은 다음과 같으며, 이러한 조치만으로도 IEMI의 위협을 상당 부분 줄일 수 있다.

- 보호 대상 기기 및 시스템 주변에 접근이 제한된 보안 구역 설정
- 시설로 들어오는 모든 전력 및 통신에 대한 무단 접근 방지
- 중요 기기 및 시스템을 시설 외벽에서 멀리 배치
- 중요 배선에 대해서는 추가적으로 배치
- 중요 기기 및 시스템에 백업 전원 사용

전자파 관점에서 기본적으로 적용 가능한 고출력 비핵 전자파 대책기술은 다음과 같다.

- 중요 기기 및 시스템에 전자파 차폐 적용
- 중요 기기 및 시스템에 사용되는 케이블에 대한 서지 보호 및 필터 적용
- 가능한 비금속 광섬유 케이블 사용
- 비정상적인 과도 상태에 대한 시스템 및 배선 모니터링, 보안 요원에게 경고 제공
- 시스템 내성을 주기적으로 시험 및 검증

보호하고자 하는 전기·전자 시스템의 기능에 강한 외부 전자파가 어떻게 영향을 주는지를 정확히 이해한 후에 시스템에 대한 보호를 설계할 수 있다. 고출력 비핵 전자파로부터 기기 및 시스템을 보호하기 위한 다양한 방법들이 적용된다. [그림 7]은 고출력 전자파에 대한 복사성 및 전도성 방호기술이 적용된 예를 보여준다.

우선 전술한 바와 같이 일반적으로 고출력 전자파 발생원을 보호 대상 기기 및 시스템으로부터 멀리 떨어지게 함으로써, 시스템에 입사하는 전자파를 줄일 수 있다. 즉, 원거리 영역에서 전자파는 거리에 반비례한다. 이러한 조치는 보호 대상 구역 주변에 물리적 장벽(울타리, 벽)을 구축하여 적용할 수 있다.

기기 및 시스템에 도달되는 복사성 형태의 전자파는 도전성 물질로 만들어진 차폐(shield)로 방호할 수 있다. 일반적으로 전도성이 높은 금속의 두께는 중요하지 않으며, 의



[그림 7] 고출력 전자파에 대한 복사성 및 전도성 방호기술

도적이거나 비의도적 개구부 등 차폐 구조물에 있는 불연속성이 중요하다. 상용 시스템을 IEMI로부터 보호하려면 건물 내부의 중요 장비를 통합하고, 작은 기기실 또는 랙을 이용하여 장비를 보호하는 것으로 충분할 수 있다. 외부와 전기적으로 연결(안테나, 통신 회선, 전력선)될 필요가 있는 경우, 고출력 전자파의 전도성 결합을 줄이기 위한 조치가 모든 선로에 반드시 필요하며, 높은 수준의 IEMI 방해를 줄이기 위해서 서지 파괴기와 필터가 필요하다. (금속 도체가 없는) 광섬유 케이블을 사용할 수도 있으며, 이러한 경우, 적절한 크기의 도파관을 사용하여 차폐 구조물 통해 올바르게 삽입되어야 한다.

IV. 표준화 동향

민수용 기기 및 시스템에 대해 고출력 전자파 표준은 국제전기기술위원회(IEC)에서 군용 표준과 기존의 전자파 적합성(EMC) 표준을 근거로 하여 1980년대부터 고출력 전자파에 대한 표준을 제정하고 있다. IEC에서 고출력 전자파에 대한 표준을 담당하는 위원회인 TC77 산하 SC77C에서는 고고도 핵폭발에 의한 전자파를 포함한 인위적인 고출력 과도 현상에 의한 위협으로부터 민수용 기기, 시스템 및 시설을 보호하기 위한 전자파적합성 분야에서의 표준화를 담당한다.

IEC에서는 EMC 표준과의 차별화와 더불어 다양한 실험 결과를 기반으로 100 V/m를 초과하는 침투치 전기장을 고출력 전자파로 정의하고 있다. 1989년부터 HEMP에 대한 민수용 시설 및 전기·전자기기 내성평가 및 보호대책 관련 표준을 제정하여 현재 거의 완료된 상태이며, 1999년 6월부터

는 IEMI를 포함한 HPEM에 대한 내성평가 및 보호 관련 국제 표준을 제정하고 있다. IEC에서는 고출력 전자파 관련 20개의 표준을 발행하였으며, 현재 기기 및 시스템에 대해 IEMI 내성평가 방법에 대한 IEC61000-4-36을 제정하였으며, 기존 시설 및 신규 시설에 대해 HEMP 및 IEMI 방호 대책 수립을 위한 지침과 IEC 표준을 적용하기 위한 방법을 제공하기 위한 새로운 프로젝트가 진행 중에 있으며, IEC61000-5-10으로 제정될 예정이다. IEC TC77에서 제정한 고출력 전자파 관련 표준 및 기술보고서는 [그림 8]과 같다.

통신시설 및 시스템에 대해 전자파 문제를 다루는 ITU-T SG5에서도 고출력 전자파 관련 표준을 담당한다. ITU-T SG5에서는 IEC 관련 규격을 근거로 통신시설 및 시스템을 고출력 전자파로부터 보호하기 위해 내성 확보를 위한 권고서를 마련하여 제공하고 있다. ITU-T에서 제정한 고출력 전자파 관련 권고서는 <표 3>에서와 같다.

ITU-T K.78 권고서는 고고도 핵 전자파(HEMP)로 인한 손상 및 파괴로부터 교환, 유·무선 통신 및 신호 전송, 그리고 전력 분배를 위해 통신센터 내에서 사용되는 기기의 보호에 대한 지침을 제공한다. ITU-T K.81 권고서는 의도성 전자파 장해(IEMI)를 포함한 HPEM에 의해 초래되는 위협 레벨에 대해 정의하고, 고출력 전자파에 대한 통신센터 내 기기 및 시스템의 취약성에 대해 기술한다. 또한, 고출력 전자파에 의한 위협이 통신시스템에 미치는 영향을 최소화하는 데 사용될 수 있는 물리적인 보안 조치의 마련에 대한 지침을 제시한다. ITU-T K.81에서 고려되는 HPEM 발생원은 IEC 61000-2-13에서 제시하는 정보를 근거로 하였다. ITU-T K.115 권고서는 주요 통신망에 대한 생존성과 신뢰성을 높이기 위해 고고도 핵 전자파 펄스(HEMP), 의도성 전자파 장해(IEMI)를 포함한 고출력 비핵 전자파(HPEM), 정보 누출(TEMPEST) 및 낙뢰(lightning) 등과 같은 전자파 보안 위협(Electromagnetic security threat)에 의한 주요 통신센터 및 내부 설치 기기의 영향을 최소화하기 위한 방법이 제시되어 있다.

V. 맺음말

전기·전자공학 및 RF 기술이 급속히 발전함에 따라 고출

IEC61000-1 General	-3: The Effects of High-Altitude EMP (HEMP) on Civil Equipment and Systems		-5: High power electromagnetic (HPEM) effects on civil systems	
IEC61000-2 EM Environment	-9: Description of HEMP Environment – Radiated Disturbance	-10: Description of HEMP Environment – Conducted Disturbance	-11: Classification of HEMP Environments	-13: High-power electromagnetic (HPEM) environments - Radiated & conducted
IEC61000-4 Testing and Measuring Techniques	-23: Test Methods for Protective Devices for HEMP and Other Radiated Disturbances	-24: Test Methods for Protective Devices for HEMP Conducted Disturbance	-33: Measurement Methods for High-Power Transient Parameters	-35: HPEM Simulator Compendium
	-25: HEMP Immunity Test Methods for Equipment and Systems	-32: High-Altitude Electromagnetic Pulse (HEMP) Simulator Compendium	-36: IEMI Immunity Test Methods for Equipment & Systems	
IEC61000-5 Installation and Mitigation Guidelines	-3: HEMP Protection Concepts	-4: Specifications for Protective Devices against HEMP Radiated Disturbance	-5: Specification of Protective Devices for HEMP Conducted Disturbance	-6: Mitigation of External EM Influences
	-7: Degrees of Protection Provided by Enclosures Against EM Disturbances	-8: HEMP Protection Methods for the Distributed Infrastructure	-9: System-level susceptibility assessments for HEMP and HPEM	-10: Guide to the Application of HEMP and IEMI Publications (In Preparing)
IEC61000-6 Generic Std.	-6: HEMP immunity for indoor equipment			

[그림 8] IEC/TC77에서 발행된 고출력 전자파 관련 표준

<표 3> ITU-T SG5 담당 고출력 전자파 펄스 관련 권고서

번호	표준명	발행일
ITU-T K.78	High altitude electromagnetic pulse(HEMP) immunity guide or telecommunication centers	2016. 6
ITU-T K.81	High-power electromagnetic(HPEM) immunity guide for telecommunication systems	2016. 6
ITU-T K.115	Mitigation methods against electromagnetic security threats	2015. 11

력 전자파를 발생할 수 있는 발생원을 손쉽게 개발할 수 있으며, 국가 주요 기반시설인 전력망 및 통신망 등은 컴퓨터와 각종 IT 기기를 이용해 제어 및 통제되고, 이러한 제어 통제 시스템은 고출력 전자파에 매우 취약한 것으로 알려져 있다. 또한 다양한 이해관계가 충돌하는 현대 사회에서 이러한 고출력 전자파를 테러와 같이 악의적인 용도로 사용할 가능성이 높아지고 있는 실정이다. 따라서 주요 기반 시설 내 제어 통제용 기기 및 시스템이 고출력 전자파 폭탄이나 의도성 전자파 장애(IEMI) 등에 노출되어 오동작하면

사회기반 시스템에 문제를 일으키게 되어 사회적으로 큰 혼란을 야기할 가능성이 높아지고 있다. 따라서 고출력 전자파를 이용한 위협은 중요한 보안 이슈로 대두되고 있는 실정이다.

본 고에서는 고출력 비핵 전자파의 특징과 이로부터 주요 기기 및 시스템을 보호하기 위한 전자파 저감 및 보호대책에 대해 기술하였으며, IEC 및 ITU-T에서 진행 중인 표준에 대해서도 간단히 기술하였다.

첨단 ICT 기술을 기반으로 제어 및 관리되는 주요 시설 및 인프라를 안정적으로 관리하고 이를 통해 안전하고 지속 가능한 사회를 구현하기 위해 고출력 전자파를 전자적 침해행위로 포함하고, 이에 대한 국가적 대책을 세우고 지속적으로 적용해야 할 것이다.

참 고 문 헌

[1] EMP Commission, Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, 2008.

- [2] The San Diego Union-Tribune, "North Korea amps up worries about potential threat to the U.S. power grid", Mar. 2017.
- [3] The Wall Street Journal, "Don't Under- estimate North Korea's Nuclear Arsenal", Feb. 2017.
- [4] 연합뉴스, "올시 전 CIA 국장 경고...북한 핵능력 과소 평가 말라.", 2017년 3월.
- [5] W. A. Radasky, C. E. Baum, and M. W. Wik, "Introduction to the special issue on high-power electromagnetics (HEMP) and intentional electromagnetic interference (IEMI)", *IEEE Trans. EMC*, vol. 46, no. 3, pp. 314-321, Aug. 2004.
- [6] 권종화, 정연춘, "고출력 전자파 대책 기술 연구 동향: 유럽 EMP 대책 기술 관련 프로젝트 중심", 한국전자파 학회지 전자파기술, 25(3), pp. 34-47, 2014년 5월.
- [7] 권종화, "고출력 전자기파 표준 현황 및 동향", 대한전자공학회지, 41(7), pp. 34-47, 82-87, 2014년 7월
- [8] D. V. Giri, F. M. Tesche, "Classification of intentional electromagnetic environments (IEME)", *IEEE Trans. EMC*, vol. 46, no. 3, pp. 322-328, Aug. 2004.
- [9] IEC Website, www.iec.ch
- [10] IEC61000-4-35 Ed. 1.0, Electromagnetic compatibility (EMC) -Part 4-35: Testing and measurement techniques- HPEM simulator compendium environment, Jul. 2007.
- [11] Recommendation ITU-T K.78, "High altitude electromagnetic pulse immunity guide for telecommunication centers", Jun. 2016.
- [12] Recommendation ITU-T K.81, "High-power electromagnetic (HPEM) immunity guide for telecommunication systems", Jun. 2016.
- [13] Recommendation ITU-T K.115, "Mitigation methods against electromagnetic security threats", Jan. 2011.

≡ 필자소개 ≡

권 종 화



1994년 2월: 충남대학교 전자공학과 (공학사)
 1999년 2월: 충남대학교 전파공학과 (공학석사)
 2010년 2월: 연세대학교 전기전자공학 (공학박사)
 1999년 1월~현재: 한국전자통신연구원 방송·미디어연구소 전파·위성연구본부 전파환경·감시연구그룹 Project Leader (PL)/책임연구원
 [주 관심분야] SI/PI 및 EMC 대책 기술 및 표준화, 고출력 전자파 펄스 대책 및 측정기술