고출력 전자파 대책 기술 연구 동향
- 유럽 EMP 대책 기술 관련 프로젝트 중심 -

권 종 화* · 정 연 춘**

*한국전자통신연구원,
**서경대학교

Ⅰ. 개 요

전력망, 통신망 등 국가 주요 기간 망과 더불어 원자력 발전 시설과 같은 주요 국가 시설에 대해 고출력 전자파 펄스에 대한 방호 평가 및 대책 기술에 대한 관심과 요구가 높아지고 있는 실정이다. 현재 민수용 전기·전자 및 통신 장비에는 고출력 전자파 펄스(HPEM/IEMI)에 대한 시험 요구가 국제적으로 전혀 이루어지지 않고 있으며, 단지 개별 기기 상호간의 전자파장해 방지를 위해 전자파적합성(EMC) 시험만을 적용하고 있다. 또한 군용 장비에 대해서도 MIL 규격(MIL-STD-461F, MIL-STD-464A 등)에서 민수용 기기보다 엄격한 내성 규격을 적용하고 있으나, 여전히 HPEM/IEMI와 같은 고출력 전자파 펄스에 대한 내성은 고려되고 있지 않은 실정이다. 미국, 러시아, 일본, 독일, 영국, 스웨덴, 노르웨이 등 각 국가에서는 HEMP는 물론 HPEM/IEMI에 대한 방호 대책 관련 지침(Guideline) 및 실무 매뉴얼을 가지고 있는 것으로 알려져 있으나, 대부분이 각국의 국사 보안과 관련된 부분이 많고, 관련 기술 기준 등이 비밀문서(Classified document)로 분류되어 확인이 불가능한 경우가 많다.

국내에서도 국가 주요 기반 시설인 전력망 및 통신망 등은 컴퓨터와 각종 IT 기기를 이용해 제어 및 통제되고 있으며, 이러한 제어·통제 시스템은 고출력 전자기파에 매우 취약한 것으로 알려져 있다. 따라서 이러한 기기들이 고출력 전자기 폭탄이나 핵폭발에 의한 전자파 펄스 등에 노출되어 오동작하면 사회 기반 시스템에 문제를 일으키게 되어 사회적으로 큰 혼란을 발생시킬 가능성이 높아지고 있다. 따라서 고출력 전자기파를 이용한 전자파 테러와 같은 잠재적인 위협은 중요한 보안 이슈로 대두되고 있는 실정이다.

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 전자파 펄스에 대한 연구가 주로 군을 중심으로 진행되어, 연구 내용이나 결과들이 대부분의 국가에서 비밀로 취급하여 공개된 자료가 미비한 실정이다 최근 군 시설뿐만 아니라, 주요 민간 시설들도 전기·전자 시스템에 의해 유지·관리되고 있어 고출력 전자기파 펄스에 의한 영향이 커져 민간 분야에서도 고출력 전자파 펄스에 대한 연구를 진행 중인 것으로 알려져 있다.

본 고에서는 유럽에서 진행되었거나 현재 진행중인 고출력 전자기파 관련 연구 프로젝트에 대해 기술하고자 한다.

Ⅱ. 고출력 전자기파

고출력 전자기파라 함은 고고도 핵 전자기파와 고출력 비핵 전자기파를 총칭하며, 고고도 핵 전자기파(High Altitude Electromagnetic Pulse: HEMP)는 지상 30 km 이상에서 핵폭발에 의해 생성되는 펄스형 전자기파를, 고출력 비핵 전자기파(High Power Elec-

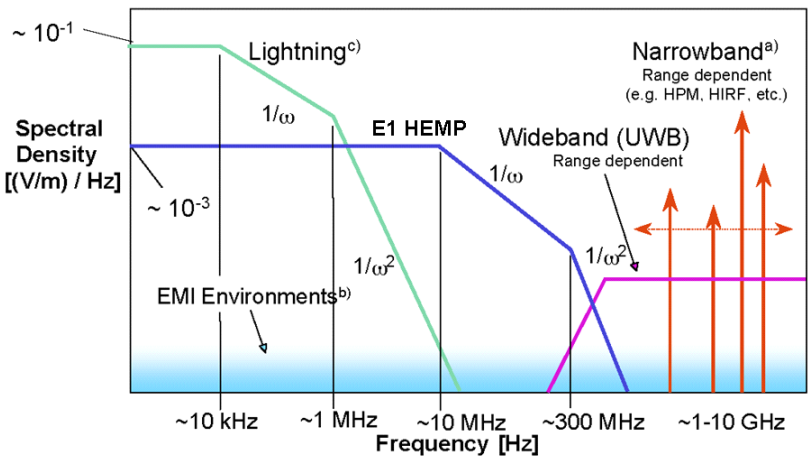
tromagnetics: HPEM)는 정보기기 등을 손상시키거나, 오동작을 유발할 수 있는 의도적으로 복사・전도된 전자기파를 각각 의미한다. 고출력 전자기파 펄스는 강력한 에너지를 가진 순간적인 전자기 충격파로, 전자기기의 오동작 또는 물리적 파괴를 유발하는 것으로 EMP의 종류는 핵 폭발에 의해 발생하는 핵(nuclear) EMP와 핵 이외의 원인에 의해 발생하는 비핵(non-nuclear) EMP로 구분한다. <표 1>과 [그림 1]에서는 고출력 전자기파와 기존 전자파 장해(EMI)의 특성을 비교하였다.

철도, 항공을 비롯한 많은 국가 주요 인프라(critical infrastructures) 및 시설은 정보통신기술(ICT) 기술의 발전과 더불어 전기・전자회로 및 유・무선 전파통신에 의해 제어되고, 운용되는 상황에서 100 V/m 이상의 고출력 전자기파 펄스에 노출된 경우, 큰 피해가 우려된다. 특히, 데이터 센터(Internet Data Center: IDC) 등 대부분의 주요 통신 시설은 현재 고출력 전자기파 펄스 공격에 거의 무방비 상태이므로, 이에 대한 평가 및 대책 기술 개발이 시급한 실정이다. 아래 [그림 2]는 고출력 전자기파에 노출되어 손상된 전기전자 부품의 예를 보여준다.

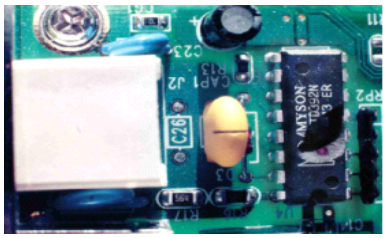
[그림 3]에서와 같이 초고주파공학 및 소재・부품 기술의 발전을 기반으로 소형화된 고출력 전자파 발생 장치를 개발하기 위한 연구가 군을 중심으로 진행 중이며, 민수 영역에서도 RF 기술의 발전으로 소형화된 고출력 전자파 발생 장치의 개발이 용이하고,

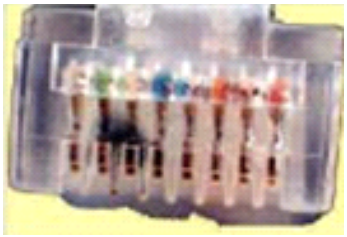
<표 1> 고출력 전자기파(HEMP/HPEM)과 전자파 장해 특성 비교

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

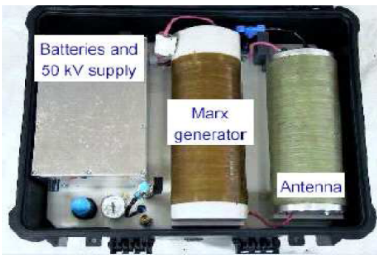


[그림 1] 고출력 전자기파(HEMP/HPEM) 주파수별 특성 비교


500 V 신호 인가에 따른 주요 칩 손상



4.5 kV 신호 인가에 따른 커넥터 손상

[그림 2] 고출력 전자파 영향 시험 결과, IC 칩 및 Ethernet 커넥터 영향



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] 고출력 전자기파 발생 장치

인터넷 등에서 쉽게 획득 가능함에 따라, 고출력 전자기파에 의한 문제 발생의 가능성은 증가하고 있다.

Ⅲ. 고출력 전자기파 관련 EU 프로젝트

고출력 전자기파에 의한 기기 및 시스템, 그리고 주요 인프라를 보호하기 위한 다양한 연구들이 유럽은 물론 미국, 일본, 중국 등 기술 선진국을 중심으로 전 세계적으로 진행되고 있다.

유럽에서는 FP7 RTD(7^{th} Framework Program for Research and Technological Development) 프로젝트의 일환으로 국가 간 혹은 관련 산업간 컨소시엄을 구성하여 2000년대 중반부터 고출력 전자파 관련 다양한 프로젝트가 수행되고 있으며, 대표적인 프로젝트는 〈표 2〉에서 기술한 바와 같이 HIRF-SE, HIPOW, STRUCTURES, SECRET 등이 있다.

3-1 HIRF-SE 프로젝트

최근 항공기 외부에서 발생된 위협은 물론 비행 중 기체 내부에서 다양한 형태의 수많은 전기·전자 장비들이 사용됨에 따라 항공기가 작동해야 하는 전자파 환경은 점점 더 복잡해지고 있다. 또한 항공기의 전자기적 측면을 고려하는 작업의 대부분은 측정 단계에서 이루어지고 있으며, 전자파 관련 문제가 발생했을 경우 상당한 추가 비용이 필요하므로 설계 단계에서 이를 고려할 필요가 있다.

HIRF-SE(High Intensity Radiated Field-Synthetic Environment) 프로젝트의 목적은 항공기를 대상으로 설계 프로세스의 초기 단계에서 기체 설계의 전자기적 측면이 고려될 수 있도록 개발 단계에서 사용할 수 있는 계산 시스템을 유럽 항공기 산업을 제공하는 것이다. 따라서 HIRF-SE 연구 결과의 적용은

〈표 2〉 고출력 전자기파 관련 주요 연구 프로젝트

프로젝트명	주요 대상 기기 및 시설	연구 기간 및 비용	Web Site
HIRF-SE	· 항공기 · 항공기 설계 단계에서 전자파적합성 고려	2008. 12.~2012. 12. 26.5 M€	www.hirf-se.eu
SECRET	· 철도 시스템 · GSM-R 철도시스템에 대한 방해 위협에 대응	2012. 8.~2015. 7. 26 M€	www.secret-project.eu
STRUCTURES	· IEMI 검출용 '필드 프로브' 개발 · IEMI 위협의 발생 이전 검출에 대한 작업	2012. 7.~2015. 6. -	www.structures-project.eu
HIPOW	· 전자파 위협으로부터 주요 인프라 보호를 위한 포괄적인 제도 개발 · 주요 인프라 보호에 관한 유럽 정책 지원 · EMP/HPM 위협에 대한 주요 인프라의 취약점 강화	2012. 6.~2015. 5. 4,756,371 EURO	www.hipow-project.eu

상당한 경제적 이익을 줄 수 있다. 더욱이 항공기에 필요한 인증 및 자격시험에서 상당한 절감 효과를 제공할 수 있다.

HIRF-SE 프로젝트에 대한 기본 정보는 다음과 같다.

- Project Name: High Intensity Radiated Field-Synthetic Environment(HIRF-SE)
- Project No: 205294(FP7)
- Project Manager: Prof. Frank B. J. Leferink(Univ. of Twente, NL)
- Project website: www.hirf-se.eu
- Project duration: 2008.12.1~2012.12.1.
- Project budget: 28.8 M€ /19.3 M€ funding
- Number of person/years: 2510 man/months
- Project Coordinator: ALENIA AERONAUTICA S.p.A.

HIRF-SE 프로젝트는 전자기학의 항공 분야 응용에서 중요한 전문성을 갖춘 모든 항공기 제조업체, 연구 기관 및 대학 등 대규모 커뮤니티에 의해 제안되었다.

HIRF-SE 프로젝트에서 계산 프레임 워크 결과는 다음과 같다.

- 항공기 기체 산업에 있어서 복합 재료 및 구조의 사용 증가에 대처하기 위한 능력: HIRF-SE 프레임 워크는 전자기장 특성과 복합 재료의 성능 수치 시뮬레이션을 위한 가장 진보된 계산 모델이 포함됨.
- 내부 및 외부 전체 전자파 환경(현재 및 미래)에 대처하기 위한 능력: HIRF-SE 프레임워크는 다양한 토폴로지와 (내부 및 외부) 전자파 간섭원에 대한 시뮬레이션을 할 수 있음.

HIRF-SE 프로젝트를 통행 개발된 방법론 및 도구는 인증기관에 따라 민간 항공 커뮤니티 내에서 잘 인식되었다. 따라서 HIRF-SE 프레임워크 결과의 적용은 항공 산업에 상당한 경제적 이익을 줄 수 있을 뿐만 아니라, 항공기에 필요한 인증 및 자격시험에서 상당한 절감 효과를 제공할 것이다.

3-2 SECRET 프로젝트

3-2-1 개요

SECRET(SECurity of Railways against Electromagnetic aTtacks) 프로젝트는 유럽 공동체에서 추진하고 있는 FP7 RTD(Research and Technological Development)

의 일환으로 GSM 기반 철도 시설에서의 전자파 공격에 대한 대응책을 마련하기 위해 2012년 8월 1일부터 3년간 수행 중인 프로젝트이다. SECRET 프로젝트에는 유럽 5개국(독일, 벨기에, 이탈리아, 프랑스, 스페인)에 위치하고 있는 총 11개의 산학연 단체가 참여하고 있다.

SECRET 프로젝트에 대한 기본 정보는 다음과 같다.

- Project Name: SECurity of Railways against Electromagnetic aTtacks('SECRET')
- Mainly concentrating on Jammer threats to the GSM-R system(FP7-SST-2011-RTD1)
- Website: www.secret-project.eu
- Duration: August 2012~July 2015(36 month)
- Project Leader: EU Transport Authority(EUROPE RESEARCH TRANSPORT)
- Cost: 26 M€

3-2-2 프로젝트 목적

SECRET 프로젝트의 주요 목적은 수많은 지휘 통제, 제어, 통신 및 신호 시스템에 방해를 일으킬 수 있는 의도성 전자파 장해(Intentional Electromagnetic Interference: IEMI)와 관련하여 철도 인프라에 전자파 공격의 위험과 영향을 평가함과 동시에 예방 및 복구 조치를 확인하기 위함이며, 또한 철도 네트워크에 대한 보안을 확보하기 위한 방호 솔루션을 개발하는 것이다.

SECRET 프로젝트의 목적은 다음과 같다.

- EM 공격의 중요한 시나리오를 파악하고, 철도 인프라의 위험 분석 및 공격 실험에 영향 평가
- 공격의 효과를 완전히 무력화시키거나 정상 상태로의 복귀가 용의하도록 하기 위해 EM 공격이나 관리 프로세스 탐지 장치를 포함 같은 공격에 장비의 보호 및 탄력 명령 제어 및 통신 체계 개발
- 철도 인프라를 강화하기 위한 기술적인 권고사항을 제시

3-2-3 연구 내용

SECRET 프로젝트는 인프라를 강화함과 동시에 유럽 전체 철도 시스템의 표준화 과정에서 발생되는 전자파 취약점으로부터 유럽 철도를 방호하기 위한 혁신적인 솔루션을 개발한다. 이것은 유럽 철도 교통 관리 시스템(European Rail Traffic Management System: ERTMS)에 따른 기술 개발과 유럽 표준화 및 철도 인프라의 탄력성을 향상시키는 기술적인 권고의 생산이 필요하다.

3-2-4 프로젝트 구성

SECRET 프로젝트의 총 기간은 36 개월이며, 기술적 작업 분야와 행정적 작업 분야를 담당하는 총 8개의 Working Package(WG)로 구성되어 있습니다.

WP1은 전자파 공격 시나리오 및 영향, 그리고 전자파 공격 장치와 관련하여 위협 분석(threat analysis) 및 위험 평가(risk assessment)에 전념하고 있다. WG1의 결과물은 정책 결정권자의 철도 인프라의 중요성에 대한 명확한 인식을 제공하는 것을 목표로 한다. WP2, WP3과 WP4는 전자파 공격으로부터 철도를 보호하기 위해 구현된 혁신적인 솔루션에 초점을 맞추고 있다. WP5은 유럽의 표준화 기구에 적합한 요구 규격과 기술적 권고사항을 마련하는 것을 목표로 한다. WP6, WP7과 WP8는 프로젝트 결과에 대한 보급과 기술적인 관리, 관리 및 재무 관리를 각각 담당한다.

① WP1: 철도를 위한 전자파(EM) 공격 시나리오의 위협 분석 및 위험 평가
- 공격용 장치(전자파 공격을 발생시키는데 사용될 수 있는 공공 부분에서 가능한 증폭 시스템 및 방출)의 식별에 전념
- 철도 인프라에 대한 시스템적 분석을 통해 피

해 시스템에 초점
- 전자파 공격 시나리오는 철도 인프라의 실질적인 전자파 취약성을 평가하기 위해 구현될 것임.

② WP2: 철도 인프라 강화를 위해 정적 보호, 위상학적(Topologic) 솔루션
- 철도 인프라 및 네트워크의 위상학적 구조(topologic architecture)에 집중
- 위상학적 구조는 유선 전송 링크, 케이블, 전기·전자 기기를 포함한 유선 네트워크에 대응

③ WP3: 전자파 환경 감시 및 전자파 공격 탐지
- 통상의 전자파 환경 조건과 전자파 공격 조건을 구별하기 위한 센서와 프로세스를 포함하는 전자파 공격 탐지 솔루션을 담당
- WP3에서 개발하는 결과물 정보 데이터는 WP4에서 진단 시스템과 동적 보호를 제공 기능을 제공

④ WP4: 동적 방호: 탄력적 구조를 위한 검출 시스템
- 탄력성 있는 통신 구조물에 탄력성을 갖는 공격 관리 서브시스템을 결합한 동적 방호 솔루션과 시뮬레이션 평가를 통한 요구사항과 개념 구현의 증거에 대한 평가에 집중

⑤ WP5: 전자파 공격에 강건한 철도 인프라에 대한 제안
- 정책 결정권자, 운용자, 철도 산업의 권고에 초점을 두고 있으며, 유럽 표준화 향상에 기여

⑥ WP6: 개발 및 보급
- 프로젝트를 수행하는 동안 수집된 성과의 보급과 사용을 관리한다. 이것은 공공 분야의 다른 결과와는 별도로 보안에 민감할지도 모르는 결과를 처리

⑦ WP7: 기술적 관리
- 고품질의 결과를 달성함과 동시에 프로젝트 전체를 통해 프로젝트 관련 행위에 대한 체계적이고 과학적인 모니터링을 보장할 수 있음을 확신

⑧ WP8: 행정 및 재무 관리
- 프로젝트 행정 및 재무 관리를 담당

3-3 STRUCTURES 프로젝트

3-3-1 개요

선진국에서 생활의 안전과 품질은 주요 인프라(critical infrastructures: CI)로 정의될 수 있는 일련의 인프라(에너지 시스템, 정보통신기술 시스템, 교통 등)의 연속적이고 협력적인 성능에 의존한다.

STRUCTURES 프로젝트는 주요 인프라(CI)에 대한 전자파 공격, 특히 의도성 전자파장해(IEMI)에 대한 주요 인프라에 미치는 가능성 있는 영향을 분석하고, 유럽의 국방과 경제 안보를 위한 전자파 공격(의도성 전자파 장해 포함)을 평가하며, 혁신적인 인식과 방호 전략을 식별하고, 전자파 공격의 가능성 있는 결과에 대해 정책 결정권자에 대한 정보 및 개념을 제공하는 것을 그 목적으로 한다. EMC(전자파적합성), LEMP/NEMP/HEMP(낙뢰/핵폭발/고고도 핵 전자기파 펄스)는 관련 기존의 연구 결과는 IEMI 문제에 대한 효과적인 해결책을 찾는 데 가능성 있는 출발점으로 고려될 수 있다. 위상학적(topological) 방법, 위험 분석 및 3D 모델링 시뮬레이터는 주로 기본적 구성에 대한 포괄적인 세트를 분석하는 데 적용될 수 있다. STRUCTURES 프로젝트에는 유럽 6개국(이탈리아, 독일, 스위스, 영국, 독일, 네덜란드)에 위치하고 있는 총 13개의 산학연 단체가 참여하고 있다. STRUCTURES 프로젝트의 기본 정보는 다음과 같다.
- Project Name: Strategies for The impRovement of critical infrastrUCTUre Resilience to Electromagnetic

attackS(STRUCTURES)

- Website: www.structures-project.eu
- Project Leader: IDS Italy
- Sponsored by the EC - DG Enterprise and Industry
- Call: FP7-SEC-2011-1 / Grant Agreement : FP7-SEC-2011-285257
- Duration: 1 July 2012～30 June 2015 (36 months)
- No. of partners : 12

고출력 전자파 장해, 특히 핵폭발로부터 발생된 고고도 핵 전자기 펄스(HEMP)와 번개로부터 발생된 전자파 펄스(LEMP)에 대한 전기・전자 시스템의 취약성은 수십 년 전부터 알려져 있다. 매우 낮은 주파수 범위를 특징으로 하는 이러한 간섭에 대한 대책은 표준과 가이드라인 핸드북에서 연구되고, 증명되어 보고되었다.

그러나 대응 능력과 규제 프레임워크 사이의 갭은 의도성 전자파 장해를 고려해야 한다. 의도성 전자파 장해(IEMI)는 매우 높은 주파수, 낮은 비용, 작은 크기에서 높은 전력 EM 전원의 증가하는 가능성, 민감한 시스템에 대한 시민 사회의 증가하는 의존성, 그리고 테러의 증가 현상 때문에 점점 더 발생할 가능성이 높은 위협이 되고 있다.

에너지 시스템, 은행, 운수 등의 민간 인프라와 서비스는 표준과 가이드라인의 부족 때문에, 그리고 높은 주파수 장해에 대응하도록 설계되거나, 시험되지 않은 상용 전자 기기의 사용은 물론, 수많은 안테나와 같은 의도적 인입점(POE) 혹은 케이블 상의 불완전한 차폐와 같은 비의도적 인입점(POE) 등으로 인하여 IEMI의 주요 가능성 있는 대상이다.

그런 맥락에서, IEMI 주요 인프라의 실제 취약점을 이해하고, 그 보호를 위한 일련의 지침을 제공하는 매우 중요하다.

3-3-2 프로젝트 목적

선진국에서의 생활 안전과 품질 인프라(에너지 시스템, ICT 시스템, 교통 등) 세트를 연속으로 좌표의 성능에 의존한다. 선진국에서 생활의 안전과 품질은 주요 인프라(CI)로 정의될 수 있는 일련의 인프라(에너지 시스템, 정보통신기술 시스템, 교통 등)의 연속적이고 협력적인 성능에 의존한다. 그래서 그러한 인프라를 “주요 인프라”(CI)로 불린다.

STRUCTURES 프로젝트의 목적은 다음과 같다.

- 주요 인프라(CI)에 대한 의도적 전자파 공격에 대한 가능성 있는 영향을 분석
- 유럽의 국방과 경제 안전 보장을 위해 의도적 전자파 공격에 의한 영향을 평가
- 혁신적인 인식과 방호 전략을 식별
- 가능성 있는 결과에 대해 정책 결정권자를 위한 정보 및 개념을 제공

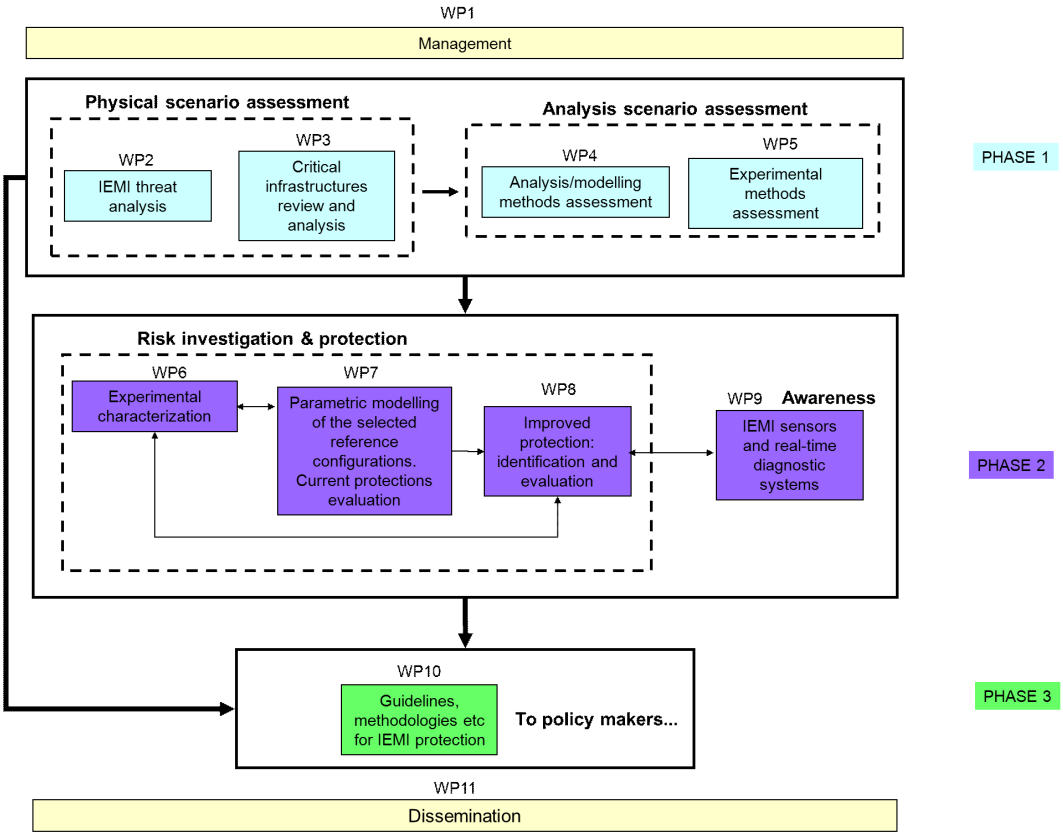
3-3-3 프로젝트 구성

STRUCTURES 프로젝트는 [그림 4]에서와 같이 3단계(phase)로 구성되어 있으며, 세부 주제별로 총 11개의 Working Package(WP)가 운영되고 있다.

WP1은 프로젝트에 대한 관리를 담당하고, WG11은 도출된 프로젝트 결과를 효율적인 보급을 담당하고 있다. WG2와 WG3는 의도성 전자파 장해(IEMI) 공격에 대한 물리적 시나리오 평가를, WG4와 WG5에서는 해석 및 분석 시나리오 평가를 각각 담당한다. WG6～8은 위험 조사 및 방호를, WG9는 위협에 대한 인식을 다룬다. 마지막으로 WG10에서는 IEMI 방호를 위한 지침과 방법론을 다룬다. 본 절에서는 각 단계별, WP별 담당 업무에 대해 보다 자세히 기술하고 한다.

① 단계 1(Phase 1)

1 단계는 물리적 관점에서 관심 있는 시나리오(IEMI 위협 및 중요 인프라)의 평가와 2 단계에서 필요한 모델링 및 측정 문제를 검토하는데 집중한다.



[그림 4] STRUCTURES 프로젝트 조직 구성 및 임무

1 단계의 끝에 관심이 있는 모든 시나리오가 식별되어야 하며, 모든 측면이 논의되고, 분류되어 논리적으로 구성되어야 한다. 조사 및 설계의 다음 단계는 그 이후에 시작될 수 있습니다.

- WP2(IEMI Threat Analysis): 특징적 파라미터(전원/EIRP, 넓은/좁은 대역, 연속/펄스, PRF, 복사/전도, 편파, 기술 수준 등)와 각 파라미터의 범위를 식별하기 위해 IEMI 발생원에 대한 검토
- WP3(Critical Infrastructures Review and Analysis): 취약성과 전략적・경제적 중요성 때문에 중요한 것으로 분리된 사전에 선택된 일련의 인프라와 하위 시스템, 그리고 그 기능들에 대한 검토와 분석
- WP4(Analysis/Modeling Methods Assessment): WP7 "조사"와 관련된 2 단계를 위한 분석 및 모델링 방법론을 식별하고 준비하는 임무를 담당
- WP5(Experimental Methods Assessment): WP7 "조사"와 관련된 2 단계를 위한 실험적인 기법을 식별하고 준비하는 임무를 담당

② 단계 2(Phase 2)

2 단계는 1 단계에서 식별된 주요 인프라, 서브시스템 및 기능에 대한 IEMI에 의한 영향에 대한 연구와 그에 따른 인프라의 회복력을 향상시킬 수 있는 비용 대비 효율적인 기술의 식별에 집중한다. WP4와

WP5에서 준비된 수치 해석 및 실험적인 방법론이 검토되며, 이를 WP2와 WP3에서 확인된 전자파 환경에 적용한다. 2 단계의 마지막에는 “위험 평가, 모델링, 영향 저감”과 “상황 인식과 평가”와 관련된 모든 요소들이 이용 가능하며, 문서화되어야 한다. 즉, 2단계에서 얻어지는 결과들은 내용을 검토하여, 3 단계에서 마련될 IEMI 방호 지침에 포함한다.

- WP6(Experimental Characterization): WP3에서 식별되지 않은 경우, IEMI에 대한 내성 임계값을 특성화함과 동시에 모델링 절차가 입증될 많은 시험 케이스를 제공하기 위해 다양한 실험이 수행됨.
- WP7(Parametric modeling of the selected reference configurations): 파라미터 분석 모델링을 통해 WP3에서 설정한 주요 인프라 기본 구성에 대한 분석을 담당
- WP8(Improved protection): 알려진 IEMI의 유해한 효과에 대해 혁신적인 방호 기술과 전략에 대한 조사, 식별 및 증명을 담당, 이러한 경우 비용 대비 효율적인 기술이 우선되어야 함.
- WP9(IEMI Sources and real-time diagnostic systems): 인프라 환경을 24시간 전천후로 모니터링할 수 있는 IEMI 센서와 센서 네트워크 조사를 통하여 “상황 인식과 평가”라는 기능 담당

③ 3 단계(Phase 3)

2 단계의 끝에서 시작하여 3 단계에서는 “WP10-IEMI 방호를 위한 지침 및 방법론 등”을 개발한다. 정책 결정권자 및 이해 관계자에게 (가이드라인, 방법론, 해석 툴, 권고사항, 최적의 평가기준 등으로 구성된) 해결 방안을 제공하기 위해 이전 단계의 결과들은 검토되고, 기존 규격과의 비교되어야 한다. 이는 인프라에 대한 IEMI 위협을 정밀하게 평가하고, 인프라의 내성을 강화하고, 기기 및 시스템의 차폐효과를 증가시키고, IEMI 위험에 대한 인프라 관리에 대한 적절한 전략을 계획하기 위해 필수적이다. 외부 전자파 위협으로부터 중요한 시스템의 안전성을 확보하기 위한 포괄적인 규칙과 방호 전략을 얻기 위해서 STRURCTURES 프로젝트에 의해 제안된 절차(낙뢰, NEMP 등)와 유사한 응용 분야에서 이미 사용 중인 표준 사이의 호환성은 검증될 것이다.

3-4 HIPOW 프로젝트

3-4-1 개요

HIPOW 프로젝트에서는 주요 인프라의 일부를 구성하는 시스템에 대한 실제 실험과 시험을 실시할 것이고, 전자파 복사를 제거할 수 있는 프로토 타입의 센서를 개발하며, 고출력 전자파를 검출하고, 방호할 수 있는 방법을 권고한다. HIPOW 프로젝트의 기본 정보는 다음과 같다.

- Project Name: “Protection of Critical Infrastructure against High Power Microwave Threats”
- Website: www.hipow-project.eu
- Duration: 2012-06-01～2015-05-31(36 months)
- Project Reference: 284802
- Project Cost/Funding: 4.756.371 EURO/3.373.578 EURO
- Program Acronym: FP7-SECURITY

HIPOW 컨소시엄은 14개의 파트너와 9회원을 갖는 최종 사용자 그룹으로 구성되어 있다. 컨소시엄 구성원들은 유럽 전역 10개국에 분포되어 있으며, 이는 수행해야 할 작업 및 결과물의 품질에 유리하다. 주요 인프라의 구조와 기술적 구현은 물론 주요 인프라의 구현을 위한 규제 기준은 국가마다 다르다. 그로 인하여 다양한 국가에서의 참여는 현재 유럽 내 주요 인프라 분석을 용이하게 진행할 수 있다.

유럽에서 진행되는 보안에 민감한 프로젝트에 대한 파트너로서의 경험을 바탕으로, 프로젝트 결과의 대규모 배포를 위해서도 가장 적합한 방법이다. 컨소

시엄의 크기와 구성은 다음을 고려하여 정의되었다.

- 관리 가능성
- 프로젝트를 위해 최종 사용자의 실제적 참여의 보장
- 프로젝트 목적 달성을 위해 여러 국가에서의 경험을 축적

3-4-2 프로젝트 목적

HIPOW 프로젝트는 전자파 위협으로부터 주요 인프라를 보호하기 위한 포괄적인 제도의 개발을 목표로 하고 있습니다. 포괄적인 제도에는 전자파 위협에 강화된 대책과 강력한 구조 관련 지침, 조직 수준에서 적용 가능하도록 제안된 위험 관리 절차, 그리고 유럽 및 각국의 주요 인프라에 적용할 수 있는 표준이나 지침 등이 포함된다. HIPOW 프로젝트에서는 실제 실험을 기반으로 한 탐지 및 방호 대책을 권고할 것이다.

HIPOW 프로젝트의 목표는 다음과 같다.

- 전자기장 복사 위협으로부터 중요 인프라 보호를 위한 포괄적인 제도 개발
- 성숙 중요 인프라 보호에 관한 배아 유럽의 정책 지원
- EMP / HPM 위협에 대한 중요 인프라의 취약점을 감소

3-4-3 프로젝트 주요 내용

고출력 마이크로웨이브(HPM) 무기 및 기타 무선 주파수(RF) 장치로부터의 잠재적 위협은 현재 우려해야 할 수준으로 증가하고 있다. EM 테러와 같은 저비용 및 낮은 수준의 기기에 의한 위해 공격은 언제 어디서나 발생 가능하며, 치명적인 결과를 수반하는 가능성 있는 방해는 현실적으로 고려될 수 있다. 유럽연합에서는 제한된 수의 프로젝트가 전자파 위협을 다루고 있다.

과도 전자기장에 의한 유해한 영향과 관련된 물리현상을 잘 이해하고 있지만, 그러한 영향들은 근본적으로 컴퓨터 시뮬레이션에 의해 정확히 모의하거나 예측하기 어렵다. 현재 효율적인 전자기장 3D 수치해석 모델링 도구들을 활용할 수 있는 다양하며 빠르고 강력한 컴퓨터들이 존재함에도 불구하고, 대형 시스템 및 인프라에 대한 문제를 시뮬레이션을 통해 해석하는 것은 여전히 어려운 문제로 알려져 있다.

전자기장 해석과 관련된 두 개의 큰 이슈는 다음과 같다.

- 해석 구조 내부에 고려해야 하는 구조물의 최대-최소 크기의 비가 커지는 문제
- 효과 예측에 영향을 줄 수 있는 비선형 문제

3-4-4 프로젝트 결과

HIPOW 프로젝트의 결과는 유럽 전역에 대해 NNEMP/HPM 공격에 대한 인지와 준비에 있어서 현재의 고도로 단편화된 상황을 개선한다. HIPOW 프로젝트는 NNEMP/HPM 위협에 대한 포괄적인 답변뿐만 아니라, 주요 인프라에 대한 위협에 대해 정책 결정권자를 위한 명확한 관점을 제공한다. 다음으로 HIPOW 프로젝트는 NNEMP/HPM 공격에 대한 유럽의 회복력을 개선함과 동시에 기존의 불충분한 상황을 상당 부분 개선시킨다.

위험 관리 절차, 감지, 강화와 강건을 위한 권고, 정책 결정권자와 주요 인프라 조직에 대한 지침, 그리고 미래 표준에 대한 반영 등 HIPOW 프로젝트에 의해 제공되는 NNEMP/HPM에 대한 주요 인프라의 방호를 위한 포괄적인 제도는 공공 기관과 주요 인프라에 의해 사용될 것이다.

구현되어 사용될 때, HIPOW 제도는 NNEMP/HPM 위협에 대한 취약성에 대해 주요 인프라의 소유자와 정책 결정권자의 인식을 높일 수 있다. 더욱이 HIPOW 프로젝트는 NNEMP/HPM 위협으로부터 중요 인프라 보호를 강화하고 개선할 것이며, 이후 여러 분야에 긍정적인 영향을 미칠 것이다.

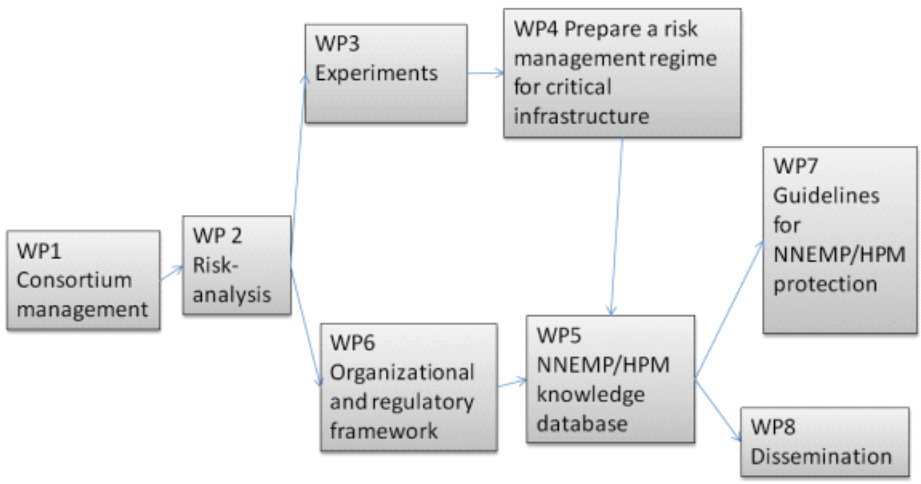
3-4-5 프로젝트 구조

프로젝트는 14개의 컨소시엄 회원사와 전문적인 기술을 갖는 전문가, 그리고 최종 사용자(사용자, 인프라 소유자 및 정부 기관)에 의해서 수행된다. 최종 사용자는 서명된 계약 의향서(Letter of Intent; 契約意向書)를 통해 프로젝트에 참여한다. 프로젝트 공동 연구자들은 여러 형태의 조직, 즉 연구 기관, 학계, 산업계, 정부, 엔지니어링, 사용자 또는 인프라의 소유자들이다. 이러한 프로젝트 참여 구성원의 다양한 조합은 긴밀히 협력하고, 프로젝트의 성공을 위해서는 긴밀한 프로젝트의 관리가 필요하다.

[그림 5]에서의 퍼트(PERT: Program Evaluation and Review Technique) 다이어그램은 다른 워크 패키지 간의 관계를 보여준다. WP6는 WP2에서 수행된 결과에 어느 정도 의존하지만, WP2가 완료되기 전에 시작될 수 있다. WP6의 결과는 NNEMP/HPM 데이터베이스를 담당하는 WP5에 제공된다. 실험을 담당하는 WP3는 보다 중요한 주요 대상물에 대해 적절한 실험을 위해 WG2로부터의 예비 조사 결과를 기반으로 해야 한다. 실험하는 동안 실패의 위험을 줄이기 위해 실험에 대한 계획은 초기에 수립되어야 한다. WP4는 WP3에 부분적으로 의존하지만, WP3이 끝나기 전에 시작할 수도 있다. 모든 비밀이 아닌 정보는 데이터베이스에 저장된다. 데이터베이스(WP5)는 지침을 개발하고 일반적으로 보급하기 위한 중요한 소스가 된다.

① WP1: 컨소시움 관리(Consortium management)
- 프로젝트의 행정적 및 기술적 관리의 조정을 포함하여 프로젝트의 전 주기 동안 전체 프로젝트를 관리하고 제어
- 프로젝트 작업에 대한 과학적/기술적 품질 모니터링
- EU 담당 위원회와의 좋은 관계를 유지하고, 주변 사회 및 대중에게 프로젝트를 제시

② WP2: 위험 분석(Risk-analysis)
- NNEMP/HPM 공격의 가능성이나 그러한 위협을 줄이기 위한 관련 국제, EU 및 국가 차원의 프레임워크를 조사
- 의도적이거나 자연적으로 발생된 유해한 과도 전자기장의 영향에 대해 준비하여, 대응하고, 회복하기 위해 유럽에서 사용되는 운용상의 기능



[그림 5] HIPOW 프로젝트 내 Work Package의 Pert 다이어그램

과 실천, 교육 개념, 그리고 표준을 식별
- EU 회원국과 관련국들은 위험한 전자기장 발생으로부터 전자 시스템이나 인프라의 피해를 방지하기 위한 시도하는 방법과 그들이 전자기장 발생을 어떻게 감지하는지, 그리고 그들이 실제 전자기장 공격과 자연 현상을 어떻게 구분하는지 등에 대한 식별

③ WP3: 실험(Experiments)
- 첨단 전자기기 및 주요 인프라의 전형적인 감응성 및 취약점에 대한 정보를 개선
- 사용 가능한 방호 대책과 방법론을 확장하고 개선
- 기준 시험을 수행하고 감응성 임계값을 설정
- 각 시험 대상과 관측된 효과에 대한 원인과 결합 메커니즘을 식별
- 강화된 절차적 방법을 사용하여 방호 대책 설계
- 제안된 방호 대책에 대해 관측된 영향 평가

④ WP4: 주요 인프라에 대한 위험 관리 방법 준비(Prepare as risk management regime for critical infrastructure)
- NNEMP/HPM 공격의 검출과 진단 방법을 위한 기술 조사
- 위험 관리 절차를 위한 중요한 도구로 EM 공격을 모니터링 하기 위한 진단 시스템 개발
- 위험 완화 방법에 대한 연구 및 제안
- 다른 조직에도 적용 가능한 위험 관리 프로세스 설정

⑤ WP5: NNEMP/HPM 정보 데이터베이스화(NNEMP/HPM knowledge database)
- 중요 인프라에 대한 NNEMP/HPM 위험과 방호 대책 관련 정보를 포함하는 데이터베이스를 생성. 데이터베이스는 정책 결정권자와 같은 주요 이해 관계자들에게 NNEMP/HPM 공격에 대하여 회복력(resilience)을 향상시킬 수 있는 위험 및 비용 데이터, 가능한 도구 및 재료와 강화된 대책 기법 등 NNEMP/HPM에 대한 특정 정보를 찾을 수 있는 능력을 줄 것임.
- 일반 대중을 위해 공개된 결과를 보급하는데 사용될 수 있는 Web-site를 생성, 웹 사이트는 또한 HIPOW 컨소시엄과 외부 이해 관계자가 비밀이 아닌 정보의 공유 지점으로 사용될 수 있도록 설계될 수 있음.
- WP5 내에서 개발된 애플리케이션의 유지 보수를 보장하기 위한 개발 계획을 상세히 설명

⑥ WP6: 구조적 혹은 규범적 프레임워크(Organizational and regulatory framework)
- 윤리적 혹은 법적 문제에 초점을 맞춘 NNEMP/HPM 방호와 관련된 전체 유럽 내 기존 법률, 규정, 표준 및 감독 관행의 재검토
- NNEMP/HPM 방호 및 사회에 미치는 영향에 관한 규제의 윤리적 혹은 법적 문제와 관련된 문제를 확인
- NNEMP/HPM에 대한 방호와 준비를 작업하고, 감독하기 위한 조직적・제도적 틀을 개발

⑦ WP7: NNEMP/HPM 방호를 위한 지침(Guidelines for NNEM/HPM protection)
- 일반적으로 최종 사용자와 유럽 사회를 위해 HIPOW 프로젝트로부터 얻어진 결과의 직접 적용 가능성을 확보
- EU를 비롯한 이해 관계자에 지속적인 영향을 제공하고, 이해 관계자들로 하여금 프로젝트 결과를 사용할 수 있도록 독려
- 전자 장비와 시스템에 대한 NNEMP/HPM 내성과 방호 관련 EU 및 국제 산업 표준 초안 마련
- 권장 방호 대책 등의 직접적인 최종 사용자 적

용이 가능하게 하기 위해 핸드북 및 다른 참고 자료 개발

⑧ WP8: Description: Dissemination

- HIPOW 프로젝트의 결과에서 발생한 지적 재산권을 보호
- 보안 담당자에 의한 결과의 적절한 이용을 보장
- 최첨단 NNEMP/HPM 공격과 방호 지정
- 최소 하나 이상의 비밀이 아닌 워크숍의 조직은 물론 학술대회 참석과 논문의 제출, 회의에서의 발표 및 데모 등 프로젝트 결과에 대한 지속적인 보급 활동 실시
- EU와 관련 국가에서의 HIPOW 도구, 절차 및 참고 자료의 이용을 촉진
- EU 관계자에 지속적인 영향을 부여하고, 이해관계자가 결과를 사용할 수 있도록 독려

참 고 문 헌

[1] 정연춘, “전자파 보안 기술 동향,” 한국전자파학회 전자파기술, 제21권 제1호, 2010년 1월

[2] 미국 하원 전자파 펄스위원회, 전자파 펄스 공격에 대한 위협 평가 보고서, 2008.

[3] MIL-STD-188-125-1/2, HEMP Protection for Ground-based C4I Facilities Performing Critical, Time-urgent Missions, 1998.

[4] MIL-HDBK-423, High Altitude Electromagnetic Pulse (HEMP) Protection for Fixed and Transportable Ground-based C4I Facilities.

[5] ITU-T K.78, High altitude electromagnetic pulse (HEMP) immunity guide or telecommunication centers, 6. 2009.

[6] ITU-T K.81, High-power electromagnetic (HPEM) immunity guide for telecommunication systems, 11. 2009.

[7] IEC/TR61000-1-5 Ed.1.0, EMC – Part1-5 General – High power electromagnetic (HPEM) effects on civil systems

[8] HIRF-SE Website, www.hirf-se.eu

[9] HIPOW Website, www.hipow-project.eu

[10] STRUCTURES Website, www.structures-project.eu

[11] SECRET Website, www.secret-project.eu

[12] EU FP7 TRD 프로젝트 Website, cordis.europa.eu/fp7

≡ 필자소개 ≡

권 종 화

1994년 2월: 충남대학교 전자공학과 (공학사)
1999년 2월: 충남대학교 전파공학과 (공학석사)
2010년 2월: 연세대학교 전기전자공학(공학박사)
1999년 1월~현재: 한국전자통신연구원 방송통신미디어연구소 전파기술연구부 전자파환경연구실 실장/책임연구원
[주 관심분야] SI/PI 및 EMC 대책 기술 및 표준화, 고출력 전자기파 펄스 대책 및 측정기술

정 연 춘

1984년 2월: 경북대학교 물리학과 (이학사)
1986년 2월: 경북대학교 물리학과 (이학석사)
1999년 8월: 충남대학교 전자공학과 (공학박사)
1985년 12월~2001년 5월: 한국표준과학연구원 전자기환경그룹 그룹장, 책임연구원
2000년 3월~2001년 2월: Univ. of York, Visiting Academics
2001년 6월~2002년 2월: (주)익스팬전자 중앙연구소장
2002년 2월~현재: 서경대학교 전자공학과 교수
[주 관심분야] EMI/EMC 측정 및 대책 기술, 전자파 재료