

文章编号: 1671-0576(2020)01-0048-06

电子信息系统对高功率微波武器防护措施研究

高伟伟¹, 江志东¹, 曲家庆², 贺伟炜²

(1. 海军航空大学青岛校区, 山东 青岛 266041; 2. 上海无线电设备研究所, 上海 201109)

摘 要: 在阐述高功率微波(High Power Microwave, HPM)武器对电子信息系统毁伤影响基础上,分析 HPM 武器的毁伤途径及方式。从技术层面提出当前应对 HPM 武器毁伤的新技术和新材料研究热点,从战术层面提出应对 HPM 武器毁伤需要加强的战术措施。研究结果对新型电子信息系统的研制和战术防护措施的选择提供了一定的参考。

关键词: 电子信息系统; 高功率微波; 防护措施

中图分类号: TN974; TN975 **文献标志码:** A

DOI: 10.3969/j.issn.1671-0576.2020.01.010

Research on the Protective Measures of Electronic Information System Against HPM Weapons

GAO Wei-wei¹, JIANG Zhi-dong¹, QU Jia-qing², HE Wei-wei²

(1. Qingdao Branch, Navy Aviation University, Qingdao 266041, Shandong China;
2. Shanghai Radio Equipment Research Institute, Shanghai 201109, China)

Abstract: The threat of High Power Microwave (HPM) weapons to electronic information systems is becoming more and more serious. On the basis of expounding the damage effect of HPM weapon on electronic information system, this paper analyzes the damage ways and modes of HPM weapon, puts forward the research hotspots of new technologies and new materials to deal with HPM weapon damage from the technical level, and puts forward the tactical measures to be strengthened to deal with HPM weapon damage from the tactical level, provides some reference for the development of new electronic information system and the selection of tactical protection measures in combat.

Key words: electronic information system; HPM; protective measures

0 引言

高功率微波(High Power Microwave, HPM)

是一种强电磁脉冲,其频段范围为 1 GHz ~ 300 GHz,峰值功率高于 100 MW^[1]。高功率微波武器是一种应用高功率微波技术的新型定向能武器,又称为电磁脉冲武器。其原理是将高功率微波能量通过定向天线进行辐射,产生高功率窄带微波波束,运用电、热等毁伤效应,对敌方的通

收稿日期: 2019-12-27

作者简介: 高伟伟(1985—),女,硕士,讲师,主要从事新概念武器研究。E-mail: 315397708@qq.com

信设备、雷达、导弹、导航设备等电子信息系统造成干扰或毁伤^[2-4]。因此,加强 HPM 武器的防护措施研究对制胜未来战场有着非常重要的意义。

1 毁伤机理

随着 HPM 武器相关技术的飞速发展,HPM 武器对电子信息系统的毁伤影响日益严重,其毁伤途径和方式往往使电子信息系统“无所遁形”。

1.1 毁伤影响

HPM 武器通过电效应、热效应等方式对电子信息系统甚至人畜进行杀伤,既具有“软”杀伤能力,又具有“硬”杀伤能力^[5]。文章仅针对电子信息系统进行研究分析,表 1 列出了不同功率密度的微波辐射对电子信息系统产生的影响^[6]。

表 1 微波辐射对电子信息系统的影响

| 辐射功率密度/ ($\mu\text{W}/\text{cm}^2$) | 对电子信息系统的影响 |
|--|---|
| 0.01~1 | 通信、雷达、导航及计算机网络等电子信息系统受到干扰,不能正常工作。 |
| 0.01~1 | 通信、雷达、导航及计算机网络等电子信息系统的电子器件性能降低甚至失效,严重的会烧毁集成电路芯片。 |
| 10~100 | 在系统金属壳体表面感应出强大电流,通过天线、金属开口或缝隙等处进入系统内部,造成电子器件功能紊乱甚至烧毁。 |
| 1~10 | 产生强场,作用于导弹、炸弹或燃料库等设备设施天线或内部电子器件,引爆或引燃设备设施。 |

1.2 毁伤途径

HPM 武器对电子信息系统的毁伤途径主要是“前门”、“后门”耦合^[7-8]。若 HPM 武器的辐射能量通过电子信息系统设备的天线或传输线等直接耦合到其内部,进而对电子信息系统产生干扰或毁伤,称为“前门”耦合。若辐射能量通过电子信息系统设备的表面孔洞、缝隙、线缆或壳体等耦合进入设备内部,对其电子器件造成干扰甚至导致器件失效,则称为“后门”耦合。对于电子信息系统,HPM 可通过天线耦合、线缆耦合、孔洞或

缝隙耦合、壳体感应、微波穿透、回路耦合等六种方式^[5-6,9-10]进入系统内部。

(1) 天线耦合

HPM 武器辐射出高功率电磁波,在目标电子信息系统附近形成强电磁场。理论上,只要处于此电磁场范围内的导体,均可认定为电磁波的接收天线,包括电子信息系统接收天线、传输线及裸露在外的金属导线或引线等。处于电磁场内的接收天线将会感应产生很高的场强,从而导致电子信息系统内部产生高电压或大电流,干扰甚至毁伤系统。

(2) 线缆耦合

如果电子信息系统的电源线缆、信号线缆或系统设备间连接部位未做好防护处理,且处于 HPM 照射范围内,由于强电磁场作用,这些部位会感应产生较强的电压或电流,感应电压或电流会对电子信息系统造成不可估量的损伤。

(3) 孔洞和缝隙耦合

电子信息系统因散热等要求,通常在其设备表面留有一定的孔洞,此外由于系统设备组装、连接等因素可能会留有一定的表面缝隙。而 HPM 的波长一般在厘米或毫米量级,若孔洞或缝隙尺寸大于 HPM 的半波长,电磁波进入设备内部会产生驻波,影响设备的正常工作。

(4) 壳体感应

一般情况下,雷达、通信设备等电子设备的壳体是由金属材质制成的。在 HPM 产生的强电磁场范围内,由于电磁能量的作用,金属壳体必然会产生感应电动势。一方面,设备的接地端一般会连接壳体,感应电动势可能导致设备内部部分电子元器件遭到干扰甚至毁伤;另一方面,设备的电源线缆、信号线缆及天线馈线等各类线缆均会穿过壳体进入设备内部,在 HPM 作用下,很有可能产生电磁谐振,影响设备内部线路及器件的正常工作。

(5) 微波穿透

HPM 覆盖的频谱一般较宽。根据 HPM 的功率、频谱范围、极化类型和电子信息系统设备的尺寸大小、设备间连接情形等因素的不同,HPM 对各类导电介质均有不同程度的穿透能力,即便是地下的电子信息系统都有可能受到影响。

(6) 回路耦合

根据麦克斯韦电磁理论,在 HPM 作用下,电子信息系统与周围潮湿的空气和大地等会形成回路,产生电磁耦合,干扰设备的正常运行。

1.3 毁伤方式

随着科技的进步,电子信息系统使用的电子器件数量越来越多,变相降低了系统的抗 HPM 毁伤能力。HPM 对电子设备或其内部电子器件的毁伤方式主要有高压击穿、器件烧毁、微波加温、瞬时干扰、浪涌冲击等^[11-12]。

(1) 高压击穿

若 HPM 被电子信息系统接收,将被转换为高电压或大电流,由此引起系统内部节点或部件损伤甚至回路的击穿。

(2) 器件烧毁

由于高电压或大电流的作用,导致系统内部电子器件的烧毁或保险丝、金属连接线等的熔断。

(3) 微波加温

任何电子器件都有限定的工作温度阈值。HPM 属于微波,微波照射对电子器件会产生一定的加温作用,若温度超过电子器件的工作温度阈值,电子器件将无法正常工作甚至烧毁。

(4) 瞬时干扰

若 HPM 辐射进入电子信息系统内部的功率较低,虽不足以毁坏系统,但由于感应瞬时电压或电流的作用,仍会对系统造成干扰,影响其正常工作。

(5) 浪涌冲击

若 HPM 由于电子信息系统的屏蔽措施未能直接进入系统内部,仍有可能在设备壳体上感应出高电压或大电流。高电压和大电流通过设备的孔洞、缝隙等进入系统内部,会导致一些敏感器件受到干扰甚至毁坏。

2 技术防护措施

为提高电子信息系统对 HPM 武器毁伤的防护能力,在明确设备的“前门”、“后门”和 HPM 毁伤途径及方式的基础上,应对防护措施加以重视并进行深入研究。

2.1 基本防护措施

基本的防护措施有屏蔽、滤波和接地等。针对 HPM 武器和电子信息系统的特性,应对其进行合理设计。

(1) 屏蔽

屏蔽是指利用合适的屏蔽材料并进行合理的设计,以达到电磁防护目的的手段。对于电子信息系统来说,屏蔽包括线缆屏蔽、孔洞屏蔽和缝隙屏蔽等,屏蔽是预防“后门”耦合的重要措施。

(2) 滤波

滤波是从频域角度进行电磁防护的方法。在分析电子信息系统频率特性基础上,将从天线或传输线等耦合进入系统的非有用信号滤除。滤波器一般有反射滤波器和损耗滤波器两种,在实际应用中,经常将两者结合起来以达到更好的效果。

(3) 接地

接地是将电子信息系统设备通过合理途径与大地相接,将 HPM 感应产生的电流导出至大地。良好的接地措施是抑制噪声和抵抗干扰的有效保证,能够很大程度上提高系统的工作稳定性。

以上是最基本的电磁防护措施,除此之外,较常见的还有接收限幅、浪涌保护等防护措施,均可有效降低 HPM 对电子信息系统的危害。

2.2 防护新技术

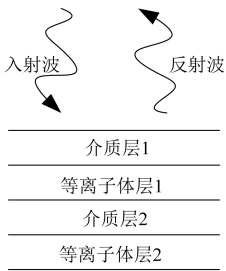
除上述基本的防护措施外,近年来新的防护技术相继被提出,主要有等离子体防护技术、基于能量选择表面的防护技术、仿生电磁防护技术等。

(1) 等离子体防护技术

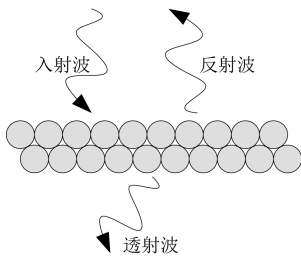
等离子体是自然界中除固态、液态、气态之外的另一种物质形态,其内部含有大量载流子,因此具有很好的导电性,且对电磁场有很强的反应。国内外关于等离子体与 HPM 相互作用的研究有很多。常规的限幅器,如 PIN 二极管限幅器、变容二极管限幅器、肖特基势垒二极管限幅器等,很容易被 HPM 毁伤。根据等离子体对电磁场的反应原理制成的等离子体限幅器,相比常规限幅器具有更高的功率容限,对 HPM 具有更好的防护效果。

图 1 是两种等离子体防护结构^[13-14]。其中:图 1(a)是一种介质层与等离子体层间隔分布的防护结构,通过介质层的反射和等离子体层的吸收以及层间的反射对 HPM 进行衰减;图 1(b)是

两层圆柱状等离子体结构,HPM 通过该结构时,经过两层离子体的反射和吸收,同样达到了衰减 HPM 的效果。



(a) 混合等离子体层结构



(b) 双层柱等离子体结构
(等离子体圆柱阵列)

图 1 等离子体防护结构

(2) 基于能量选择表面的防护技术

基于能量选择表面 (Energy Selective Surface, ESS) 材料的防护技术是运用压控导电材料或电磁敏感材料进行设计的电磁防护技术。ESS 材料具有电磁环境的自适应特性,可根据空间中电磁能量的强弱,实时变化自身对电磁波的传输特性,从而改变空间的电磁分布,以实现电磁能量的低通特性。

图 2 为一种较为典型的 ESS 电磁防护材料结构^[15],该结构是由导电交叉金属贴片和反向并联二极管组成的二维周期性网格阵列。为保证屏蔽效果,网格间距应远小于入射电磁波波长。由于二极管的压控特性,入射电磁脉冲的强度不同,二极管的感应电压也会不同,因此防护结构是可变的。当入射信号能量较小时,二极管两端电压低于其导通电压,此时所有二极管都处于截止状态,该结构为导电网格阵列,几乎不会影响电磁信号的传输;反之,当入射信号能量增大,二极管两端电压大于其导通电压时,所有二极管都处于导

通状态,该结构为金属屏蔽网,可以阻止强电磁脉冲进入设备内部。

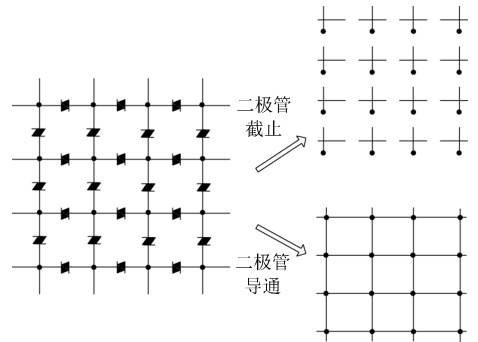


图 2 典型的 ESS 电磁防护材料结构

(3) 仿生电磁防护技术

仿生电磁防护主要是学习生物系统的构造和活动的过程、机理,并进行合适的提取后将其应用到电磁防护领域^[16],是电磁仿生学的新生分支。目前,关于此方面的研究方兴未艾。

2.3 防护新材料/新器件

伴随着新型防护技术的研究,各类新材料和新器件在 HPM 防护中也得到越来越多的应用。

(1) 纳米材料

纳米材料是指在三维空间中至少有一维处于纳米尺度或以此为基元构成的材料。由于材料的尺度远小于电磁波波长以及小尺度所带来的大表面效应,使得纳米材料可以对电磁波进行有效的屏蔽防护^[17]。以纳米技术为基础的新型复合电磁防护材料研究已成为重要的研究热点。据报道,美国 IBM 公司已研制出以多层石墨烯为主的新型防护材料,可以对微波辐射进行有效的防护^[18]。文献^[19]提出了一种纳米聚苯胺-镀镍碳纤维复合材料,具有良好的力学性能、电磁屏蔽性能和吸波性能。一定工艺条件下,其在 10 kHz~4 GHz 频率范围内的电磁屏蔽效能最高可达 72 dB。

(2) 智能防护材料

智能防护材料是一种能够感知外界变化,并根据变化情况做出适当反应的新型材料,是继石器材料、钢铁材料、合金高分子材料及人工设计材料之后的第五代材料。相比于传统电磁防护材料,智能防护材料电磁调节速度更快、电场敏感度

更高、相变前后的电导率变化范围更大、相变时间更短且相变可逆^[20],具有更好的电磁防护性能。广义上,应用于等离子体技术和能量表面选择技术的材料都可以看作是智能防护材料。

(3) 新型器件

现有电子信息系统中的器件大部分不具有抵抗 HPM 的能力。在研究新型电磁防护技术和材料的同时,需加强对新型强电磁防护器件的研究。目前,美俄等国已研制出可以抵抗一定功率强度 HPM 脉冲的集成芯片,相对于常规芯片,其抗强电磁脉冲能力提高了 8~10 倍^[6]。运用石墨烯材料制成的晶体管相比常规晶体管具有更高的迁移率和开关比,理论上可以突破传统晶体管对亚阈值斜率的限制^[21]。

除此之外,由于光信号的传输受电磁脉冲的干扰较小,可以考虑用光纤替换现有电子信息系统中传输信号的线缆,以减少线缆耦合的影响。

3 战术防护措施

从技术上提升电子信息系统 HPM 防护能力的同时,还应从战术上考虑如何降低 HPM 武器对电子信息系统的危害。参考美国国防机构对电磁防御问题的分析与应对策略^[22],应从以下方面考虑电子信息系统的 HPM 防护。

3.1 加强电子信息系统的主动干扰和伪装欺骗能力

敌方 HPM 武器必然要事先得到我方电子信息系统可靠信息才可进行电磁攻击,所以加强对敌方探测设备的主动干扰和欺骗,并对我方设备进行合适的伪装,将极大地降低敌方打击效果。有经验表明,在雷达阵地附近布置假阵地,随着伪装级别的提升,敌方以假当真的概率将大为增加。不同伪装级别下目标的发现概率及摧毁概率如表 2 所示^[23]。

表 2 不同伪装级别下目标的发现概率及摧毁概率

| 技术参数 | 未施加伪装 | 施加三级伪装 | 施加二级伪装 | 施加一级伪装 |
|--------|-------|--------|--------|--------|
| 发现概率/% | 100 | 95 | 86 | 33 |
| 摧毁概率/% | 80 | 74 | 67 | 25 |

3.2 加强对 HPM 武器或平台的主动攻击

最好的防御就是进攻。应加强对我方探测设备的重视与应用,提升探测设备的协作能力;加强区域甚至整体的探测感知能力,积极主动探测敌方 HPM 武器及其平台所在;合理部署针对 HPM 武器的打击部队并加强其机动能力,遇有状况及时响应,力争先于敌方攻击。

3.3 提升安全保密能力

对电子信息系统的电磁信息要加强保密,严防电磁信号频率、制式、功率等重要信息的泄露。同时应结合电子信息系统部署地点的实际情况,制定严格的安全保密规章,甚至将电磁安全保密措施扩展至“声”、“光”等领域。

4 结束语

文章对 HPM 武器的毁伤机理进行了简要阐述,并在此基础上探讨了未来进行 HPM 武器防护的新技术和战术防护要求。随着科技的进步,电子信息设备和 HPM 都在快速发展,未来战争中,电子战必然是重中之重。防护好己方电子信息系统免受敌方 HPM 武器的攻击可能是未来战场制胜的关键。

参考文献

- [1] BENFORD J, SWEGLE J, SCHAMILOGLU E. 高功率微波 [M]. 江伟华, 张弛, 译. 2 版. 北京: 国防工业出版社, 2009: 1-3.
- [2] 陈凯柏, 周晓东, 高敏. 高功率微波技术研究进展及应用[J]. 飞航导弹, 2019 (6): 1-6.
- [3] 祝民鹏. 高功率微波作用下雷达装备效能评估[D]. 郑州: 战略支援部队信息工程大学, 2018: 1-2.
- [4] 唐鑫, 杨建军, 严聪, 等. HPM 武器电子毁伤效能评估方法[J]. 系统工程与电子技术, 2016, 38 (10): 2317-2323.
- [5] 李海山. 高功率微波武器攻击电子信息设备影响因素分析及防护方法研究[M]. 长沙: 国防科技大学出版社, 2011: 6-8.
- [6] 余世里. 高功率微波武器效应及防护[J]. 微波学报, 2014(6): 147-150.
- [7] TESCHE F M, BULTER C M. On the addition of EM field propagation and coupling effects in the

- BLT equation [J]. Interaction Notes, 2003, 558 (7): 1-43.
- [8] TESCHE F M, KEEN J M, BUTLER C M. Example of the use of the BLT equation for EM Field propagation and coupling calculation [J]. URSI Radio Science Bulletin, 2005(312): 32-47.
- [9] GEDNEY S D. An anisotropic perfectly matched layer-absorbing medium for truncation of FDTD lattices[J]. IEEE Transactions on Antennas and Propagation, 1996, 44(12): 1630-1639.
- [10] 周鹏. 用于接收机高功率微波防护的 ESS 技术研究[D]. 西安: 西安电子科技大学, 2018: 15-17.
- [11] KIRAWANICH P, KRANTHI N S, ISLAM N E. Modeling external interference on system using electromagnetic topology technique [C]// 2004 International Symposium on Electromagnetic Compatibility, Silicon Valley, California. New York: IEEE, 2004: 804-808.
- [12] TAYLOR C D, YOUNAN N H. Effects from high-power microwave illumination [J]. Microwave, 1992, 35(6): 50-96.
- [13] 杨耿, 谭吉春, 盛定仪, 等. 等离子体对高功率微波的防护[J]. 核聚变与等离子体物理, 2008, 28 (1): 90-93.
- [14] 刘洋, 时家明, 程立, 等. 双层等离子体对 6 GHz 高功率微波防护实验[J]. 红外与激光工程, 2017, 46(9): 1-5.
- [15] YANG C, LIU P G, HUANG X J. A novel method of energy selective surface for adaptive HPM/EMP protection [J]. IEEE Antennas and Wireless Propagation Letters, 2013, 32(12): 112-115.
- [16] 刘尚合, 原亮, 褚杰. 电磁仿生学—电磁防护研究的新领域[J]. 自然杂志, 2009, 31(1): 1-7.
- [17] 祝民鹏, 侯德亭, 陈丹. 国外高功率微波技术发展及应用[J]. 飞航导弹, 2018(2): 67-71.
- [18] 刘洋, 程立. 电磁脉冲防护技术研究现状[J]. 材料导报, 2016, 30(28): 272-275.
- [19] 王东红, 李克训, 姜晓东, 等. 纳米聚苯胺-镀镍碳纤维复合材料屏蔽/吸波性能[J]. 安全与电磁兼容, 2016, 15(3): 47-50.
- [20] 成伟, 王妍, 王赟, 等. 自适应智能电磁防护材料测试方法研究[J]. 装备环境工程, 2017, 14(4): 32-35.
- [21] 田禾. 基于石墨烯的新型微纳电子器件研究[D]. 北京: 清华大学, 2015: 43-54.
- [22] STUKENBERG M D, WOOLSEY A J, DEMAIO C D. Electromagnetic defense task force (EDTF): 2018 report [R/OL]. Alabama: Air University Press, 2018. https://media.defense.gov/2018/Nov/28/2002067172/-1/-1/0/LP_0002_DEMAIO_ELECTROMAGNETIC_DEFENSE_TASK_FORCE.PDF.
- [23] 王远, 郭宜忠, 宫迅勋, 等. 电磁脉冲武器对雷达的损伤效应及防护措施[J]. 航天电子对抗, 2016, 22(6): 17-19, 61.

~~~~~  
(上接第 47 页)

- [2] 徐贵贤. 1553B 总线简介及其实现[J]. 通信技术, 2011, 44(5): 166-168.
- [3] 茅飞, 朱昊, 朱兴华, 等. 基于 FPGA 的曼彻斯特码功能实现技术[J]. 机电产品开发与创新, 2011, 24(6): 148-150.
- [4] 董毅, 何刚强, 梁汉文, 等. 基于 FPGA 的曼彻斯特编解码器的设计[J]. 电子设计工程, 2019, 27 (10): 15-18, 23.
- [5] LI J, CHAI M. Design of 1553B avionics bus interface chip based on FPGA [C]// 2011 International Conference on Electronics, Communications and Control, Ningbo. New York: IEEE, 2011: 3642-3645.
- [6] 汤晓曦, 尹蕾, 许晏, 等. 基于 FPGA 的曼彻斯特编解码器设计[J]. 电子设计工程, 2011, 19(23): 171-173, 177.
- [7] 黄家平, 王明皓, 谢慧玲, 等. 1553B 总线通信系统可靠性分析[J]. 飞机设计, 2010, 30(2): 57-61.