doi: 10.3969/j.issn.1001－893x.2013.01.020

军用电子设备安全性设计*

生建友**

（总参第六十三研究所，南京 210007）

摘 要：安全性作为武器装备质量特性中的一项重要内容越来越受到人们的重视。由于组成结构越来越复杂、自动化程度越来越高以及工作时产生的电磁波可能被截获等原因，军用电子设备发生安全事故的可能性越来越大。介绍了安全性的定义，强调了安全性的作用。结合国军标要求和军用电子设备的使用实际，分析了设备安全性设计的定性、定量要求，提出了安全性设计的主要内容，详细讨论了军用电子设备人员、设备的安全性设计和电磁信息安全设计的具体措施，可供该领域从事设计、管理和维修的人员借鉴。

关键词：军用电子设备；安全性设计；人员安全；设备安全；电磁信息安全
中图分类号：TN805　　文献标志码：A　　文章编号：1001－893X(2013)01－0099－06

Safety Design of Military Electronic Equipment

SHENG Jian-you

(The 63rd Research Institute of the General Staff Headquarters, Nanjing 210007, China)

Abstract: Safety is attracting more and more attention as an important part of quality characteristics for weapons and equipment. Due to the more complex composition structure, the higher automatic level and the intercepted probability of electromagnetic wave produced in operation, the possibility of safety accidents occurrence on military electronic equipment is becoming higher and higher. This paper introduces the safety concept and emphasizes the functions of safety. According to the requirements of GJB and the practice experience of military electronic equipment, it analyzes the qualitative and quantitative requirements for safety design, proposes the main contents, finally discusses the concrete measures of safety design for personnel, equipment and electromagnetic information for military electronic equipment in detail. The methods presented herein can be useful for those who are engaged in designing, managing and maintaining in this field.

Key words: military electronic equipment; safety design; personnel safety; equipment safety; electromagnetic information safety

1 引 言

系统安全起源于 20 世纪 50 年代到 60 年代美国研制民兵式洲际导弹的过程中，美军于 1969 年颁布了安全性军用标准 MIL-STD-882，从此，系统安全的思想与技术在各个行业得到广泛应用[1]。我国武器装备的安全性工作是在借鉴外军先进经验基础上开展的，也相继颁布了一系列有关安全的标准、规范，对提高装备的安全性水平发挥了重要作用[1]。由于承制单位对装备的安全性不重视，装备研制过程中较少系统性地开展安全性工作，导致一些装备存在先天性安全缺陷，并因此发生事故，造成重大损失。电子装备作为现代信息化战争的核心装备，功能越来越多，组成结构越来越复杂，自动化程度越来越高，设备发生安全事故的可能性不断增大，而且，随着信息侦收技术的发展，电子设备运行过程中由于电磁辐射而泄露的信息被截获的风险也是越来越

* 收稿日期：2012－06－21；修回日期：2012－09－04　Received date: 2012－06－21; Revised date: 2012－09－04
** 通讯作者：shjy668@sohu.com　**Corresponding author**: shjy668@sohu.com

高[2-3]，加强安全性的研究与设计显得尤为迫切。

基于上述国内外现状分析，本文针对军用电子设备的使用实际，研究并提出了军用电子设备的安全性设计内容和具体对策，以全面提高设备的安全性水平。

2 安全性的概念及作用

2.1 安全性概念

安全是指不发生可能造成人员伤亡、职业病、设备损坏、财产损失或环境损害的状态。该定义是指产品在寿命周期内某一时刻安全与否的状态，表征产品的瞬态特性和使用特性。安全性是指产品所具有的不导致人员伤亡、系统损坏、重大财产损失或不危及人员健康和环境的能力[4]。同可靠性、保障性等一样，是通过设计赋予的一种固有的装备属性，是保障使用安全的能力体现，是可度量与比较的。

2.2 安全性的作用意义

军用电子设备要完成其规定的任务，其作战性能、功能固然重要，但是，如果设备不安全，经常发生事故，再好的作战效能也难以发挥。安全性作为设备的重要特性，其作用主要表现在以下三方面。

(1)有利于提高设备的作战能力。设备安全性好，其发生事故的次数就少，平时能经常处于安全可用状态，战时能长时间安全作战，设备的作战能力自然很强。

(2)有利于提高产品的市场竞争力，部队的生存能力，节约保障资源。和平时期，设备质量高，安全性好，信誉度就好，市场竞争力就强；战争时期，可有效减少机毁人亡的事故发生，必然减少保障人员和设施等保障资源，从而相对缩小部队规模，提高部队的机动性和生存能力。

(3)电子设备的电磁信息安全事关国家安危、战争胜负。设备电磁信息安全性不好，容易造成信息泄漏，被敌对势力侦收后，就会掌握我方的装备参数、方位及通信、指挥、控制等关键信息，从而给敌方有可乘之机，一旦有战事，势必造成更大范围的人员伤亡、装备损毁，进而影响战局。

3 安全性设计的要求与内容

3.1 安全性设计要求

安全性要求是设备研制过程中进行安全性设计、分析与评价的依据。应将顾客对产品的安全性要求和有关法规、标准、设计手册规定的要求转化为设备的安全性设计要求，包括定性要求和定量要求，使事故风险在可接受的范围内。

3.1.1 定性要求

按照GJB367A 和GJB900 的要求，在项目研制任务书中，应提出以下几项要求[1,5]。

(1)减少危险品要求。设计师通过设计、选材等手段，尽量减少设备对危险品的使用。

(2)危险品隔离要求。将设备中的危险元器件隔离起来，如高压器件、高辐射器件等。

(3)安全保护要求。将设备中的关键零部件、元器件保护起来。

(4)监测、报警要求。设计具有控制或监测功能的软件和安全报警装置，随时检测、监视设备的危险状况，并通过设备的显示器、指示灯或扬声器给出信号或发出声音。

(5)警告信号要求。警告信号应明显，以减少操作人员对该类信号的漏判与误判。

(6)警告标志要求。通过设计不能消除的危险，应在装配、使用、维护说明书中给出警告和注意事项，并在危险零部件的醒目位置做标记。

(7)预防差错要求。在结构设计中采用防差错措施，尽量减少设备在使用、保障中由人为差错造成的危险。

(8)风险最小化要求。通过设计，设备在各种约束条件下，达到人员伤亡、设备损坏、信息泄露和环境破坏的风险最小化。

(9)电磁信息防护要求。通过设计、选材等手段，尽量减少设备的电磁信息泄露。

(10)报废处理要求。电子设备中通常有一些会对环境造成污染的器件和电池，大批量列装的设备，应要求考虑退役后设备的处置安全问题。

3.1.2 定量要求

表征安全性的参数主要有事故率/概率、安全可靠度、事故风险等。国内外最常用的安全性度量方法是事故风险评价[1,5]。GJB900 给出了两种风险评价事例，具体的定量指标可根据设备的具体情况和实际需求而定。GJB376A 根据电子设备的特点，对设备的绝缘电阻、介电强度、泄漏电流等安全性指标规定了具体的量值，具体值参见文献[6]。目前，这两个国军标还都没有对电磁信息安全规定明确的定量指标。

3.2 安全性设计内容

按照安全性定义及 GJB900 的要求，安全性设计

主要是人员、设备的安全设计及环境的防护设计。电子设备的使用、保障中不会对环境造成破坏, 即便是设备损坏一般也不会损害环境, 但是, 设备工作时会发出电磁波, 如果被敌方截获则容易造成信息泄密, 设备的电磁信息安全应值得重视, 因此, 军用电子设备的安全性设计主要包括人员、设备及电磁信息的安全设计等 3 部分内容。

4　安全性设计

安全性水平的高低由设计决定的, 如果"先天"设计不足靠"后天"弥补, 不但费事而且费钱, 得不偿失。安全性设计应在项目研制之初就开始进行, 并贯穿于研制全过程, 通过设计来实现设备的安全性要求。

安全性设计是通过各种设计措施来消除和控制各种危险, 提高设备的安全性。安全性设计的指导思想是为设备的操作使用、维修保障人员提供可接受的保护措施, 避免在使用、保障过程中, 由于设计缺陷或误操作而导致人身伤害、财产损失, 避免设备工作时的电磁信息泄露。在安全性和成本等其他因素发生冲突时, 应该优先考虑安全性的要求。

4.1　人员、设备的安全性设计

人员、设备的安全性设计主要从防电击、防高温、防静电、防着火、防辐射以及结构设计、告警标志等方面采取措施。

4.1.1　防电击措施

电击是由于电流通过人体而造成的, 其引起的病理、生理反应取决于电流的大小和持续的时间以及通过人体的路径[7]。通常毫安级电流就会对人体产生危害, 大电流甚至会造成人员死亡, 防触电保护是电子设备安全性设计的重要内容。可采取以下措施防止电击伤害。

(1)在满足功能要求的基础上, 限制电路输出的电压或电流, 使操作者可接触到的电压和电流都是安全的。工作电压超过 30 V(均方根值或直流)的部位应加防护装置(如绝缘套管、防护隔板等), 以防操作、维修时碰到被电击。

(2)设备应装有能切断设备电源的总开关, 高压电路应有自动放电电路, 以保证断电后在2 s内放电至30 V以下[1]。

(3)综合考虑电气间隙、爬电距离等因素优化电路设计, 优化线缆的走线设计与固定安装, 减少线缆的松动和表面绝缘层损坏的可能性, 并采取有效绝缘和安全接地措施, 确保设备电源输入端与机箱之间的介电强度满足 GJB367A 的要求, 绝缘电阻在正常大气条件下不小于 100 MΩ, 潮湿环境下不小于 2 MΩ, 机箱与地之间的泄漏电流不大于5 mA。

(4)安全接地措施。机箱上应设计接地装置, 设备内需要接地的零部件都应通过它连接到保护大地上。当地线作为线路的一部分时, 任何电缆在其两端的接线端应有一条地线, 接地线应通过电连接器上的接线端接到机箱或机座上, 电源回线不能作为接地线用。屏蔽电缆或金属编织覆盖层的屏蔽层、电连接器金属外壳应有效连接到机箱上。安全接地措施应兼顾电磁信息安全设计和防静电设计需要。

4.1.2　防高温和着火措施

电子设备工作时会产生热量, 如果缺少热绝缘或散热能力不足, 则会使设备产生高温; 设备由于过载、短路、元器件故障、绝缘击穿等原因也会产生高温, 过高的温度会烫伤人, 会导致着火危险。针对高温、着火危险, 应采取以下措施。

(1)选择使用耐火、耐高温性能好、不自然的材料、元器件, 且不释放出可燃或有毒气体, 并尽可能满足军用性能要求。

(2)根据设备的使用要求对元器件进行降额设计, 减少功耗; 采用熔断器或断路器, 为设备提供过流过载保护; 设计过流、过压保护装置, 防止电路过热[8]。

(3)对发热量大的器件单独采取传热措施, 同时, 对整机综合采取增加散热面积、表面涂深色涂料、机箱上增加散热孔或外加风冷、液冷模块等措施, 确保使用人员可触及的设备表面温度限制在允许的范围内。机箱上开孔要考虑电磁信息的安全性要求。

(4)电源线与插头之间连接牢靠, 导线截面积与电流匹配, 连接线缆在机箱内要固定等。

4.1.3　防静电和辐射措施

静电放电(ESD)会导致电子元器件、电子设备严重损坏, 被称为现代高技术工业中的病毒[8]。防静电的关键就是防止静电荷的产生与积累, 使物体表面绝缘, 阻隔静电放电效应发生的路径, 避免对电路的干扰。可采用如下措施。

(1)选用内部有静电保护电路的器件、对静电不敏感的器件。

(2)对静电敏感的器件设计保护电路; I/O 端口加装 ESD 专用滤波器; 隔离 ESD 敏感电路, 并单独设计屏蔽盒。

(3)PCB 上下两层大面积敷铜并多点接地;选用多层 PCB;在 PCB 板的顶层与底层周边设计保护带镶边(镶边不同于地线)[9]。

辐射包括电离辐射(如 χ 射线、γ 射线等)和非电离辐射(包括红外、射频、微波以及激光辐射等)。防辐射主要是控制设备辐射出来的电磁能量或射线剂量,采取的措施主要是屏蔽、接地与隔离。具体措施与电磁信息的安全设计类似。

4.1.4 结构防护措施

为进一步确保军用电子设备安全性,在结构设计上也应同步采取防护措施。

(1)结构件要具有足够的强度和刚度,为电路单元的连接和固定提供安全可靠的支撑。结构设计应确保设备重心在下,以防倾倒,避免造成人机伤害。

(2)操作、维修人员接触到的结构件要避免出现锐角和锐边,结构件外露的锐边应打圆。

(3)设计防误插装置,确保电连接器不会因误接而造成设备损坏,同时采取措施,确保连接器在分离前后工作人员不致受到电击。

(4)设备面板上的显示装置、调节机构及操作部件应按人机工程学的要求进行设计。设备的结构应为维修人员提供最大的方便和安全[10]:一是看得见;二是够得着,维修人员的手直接或借助于工具能够接触到维修部位;三是有足够的操作空间。

(5)对于抽屉式结构的机箱或安装在机架上的设备应有限位和固定装置,以防其从机架上跌落,而对设备和人员造成不必要的伤害。

(6)设备外露的电连接器座、波导口等应配有防护盖,以防运输、贮存中损坏,或杂物、虫子、灰尘、雨、雪进入。

(7)连接用螺钉(螺栓)的螺纹拧入长度不少于 1.2 倍的螺纹直径,并保证在振动环境中不松动,冲击环境中不断裂。

(8)设计的机箱应满足设备特定的使用环境,且必须与保护接地连接。

4.1.5 安全性说明与标记

如果上述防护措施不能消除某项危险的可能性时,则应考虑提示性安全措施,即文件和标记,可以通过装配说明书、用户使用手册进行描述,简要说明在什么情况下采取何种措施才能安全使用,出现什么危险时应采取的相应措施等,也可以在相应危险零部件、器材、设备上设计醒目标记,避免设备在操作、安装、维修、运输等过程中引起危险。标记应包括文字、颜色和图样,告警标记应符合 GB2894-1996《安全标志》的规定[7-8]。根据电子设备的特点,以下几点必须在设备的相应位置进行标记:

(1)电气插座旁必须标出供电的电压、相位及频率等特性参数,熔断器座旁必须标出额定电流值;

(2)非电气连接器座旁必须印有插座的用途名称(如数据、话音、天线等)和插座位号(如 XS01),名称与位号应与用户使用手册的内容相一致;

(3)印制板上的接地点和设备上的接地装置旁必须有接地标记,开关旁应有"通—断"标记;

(4)可触及的零部件表面温度由于功能原因或环境温度过高超过允许的限值,必须有"小心烫伤"的标记。

标记作为确保设备安全的措施之一,应是耐久、清晰、容易辨认的,标记的位置应是人容易看到和阅读的地方。

4.2 电磁信息的安全性设计

电磁信息安全性设计就是根据电磁信息泄露机理,采取电磁信息泄露防护技术,使电路单元及设备的电磁发射水平限制在不易被截获的范围内。电磁信息泄露防护技术开始是作为电磁兼容(EMC)的一部分,现在已发展成为一门独立的学科和技术[2]。

电磁信息泄露防护技术主要有 3 种:一是物理抑制技术,分为包容法和抑源法两种[3];二是伪辐射技术,伪辐射技术就是使设备产生不带信息的伪噪声,以淹没设备中的有用信息,使敌方侦收到的信息是虚假信息;三是 Soft-TEMPEST 技术[2]。该技术诞生于 20 世纪末,用软件的方法通过改变设备的工作状态和信号特征达到抑制电磁泄露的目的。伪辐射技术和 Soft-TEMPEST 技术可参考其他有关文献,本文主要讨论物理抑制技术。

4.2.1 分区隔离设计

根据信息泄露的可能性和防护要求,对设备的各组成单元进行区域划分,凡是只载有或处理非保密信息的电路依据防护要求标定为黑区,而载有或处理未经加密的机密信息的电路标定为红区,红区与黑区之间实施电磁隔离,且红、黑区分别供电。对红区严格实施屏蔽、滤波、接地等电磁信息泄露防护措施,而黑区则可以放宽要求。

4.2.2 抑源法

抑源法从元器件、线路和印制板(PCB)入手,消除产生强电磁波的根源。主要有以下 5 种措施。

(1)合理选用元器件

元器件是影响设备电磁辐射能量的主要因素之

一。选用元器件时应综合考虑以下因素[9]: 外形尺寸小的 SMT 或者 BGA 封装; 芯片内部 PCB 有多层电源层和接地层; 耗散功率很小; 功能满足要求的前提下, 运行速率尽可能低; 电源和接地管脚位于封装中央; IC 封装内使用高频去耦电容的芯片; 具有金属外壳; 散热性能好。

(2)选用多层印制电路板

资料表明: 如果增加一个接地层, 就会提高 PCB 板的信号完整性和电磁兼容能力, 如对双层板增加两个或多个电源层和接地层, 就可以获得 10 ~ 20 dB 辐射性能的改进[9]。因此, 应选用有多个电源层和接地层的多层印制板, 当然, 应兼顾费用问题。

(3)优化印制板的布局与布线

布局与布线的好坏直接影响到 PCB 板的电磁辐射水平。布局时应注意: 强信号、弱信号、高电压信号和低电压信号完全分开; 同时包含高速、中速、低速逻辑电路时, 高速电路应紧靠边缘连接器, 中、低速电路依次远离连接器; 时钟电路远离输入输出端; 使用同一种电源供电的元器件尽量放在一起; 集成电路的去耦电容尽量靠近芯片的电源脚。布线时应注意: 输入输出端的连线避免平行走线; 所有连线尽可能短, 关键信号线最短; 线宽合理, 且电源线、地线尽量宽, 地线 > 电源线 > 信号线; 电源线与地线尽可能靠近; 布线宽度不要突变, 不要突然拐角。具体的布局与布线参见文献[3, 9]。

(4)滤波与吸收

滤波是抑制信息传导泄漏的有效措施。对设备中的电源线、信号传输线、公共地线等选用相应的滤波器, 以阻隔电磁波传播。设计电路板时, 印制板上电源线与地线之间的滤波也应重视, 要适当加些滤波电容。

(5)接地

良好的接地是抑制电磁信息泄漏的有效途径, 它既可以解决传导泄漏又可以解决辐射泄漏。设计时, 将信号地与噪声地、高电平信号与低电平信号地线、数字信号与模拟信号地线分开敷设, 接地线都应尽可能短、粗、直。屏蔽盒、屏蔽窗、电缆屏蔽层以及晶体、滤波器的外壳等都要良好接地。

4.2.3 包容法

包容法主要从材料、结构和工艺等方面采取措施对电路单元和设备进行屏蔽设计, 屏蔽是抑制电磁辐射最有效的手段。主要包括以下 5 方面措施[3]。

(1)机箱屏蔽

金属材料的机箱屏蔽效果好, 是首选。如果是工程塑料制成的机箱, 则应采用真空沉积、电涂、粘贴等工艺技术在机箱内壁粘附一层导电薄膜, 使其具有屏蔽效果。

(2)电路局部屏蔽

对设备内部电磁辐射能量较大的单元单独制作屏蔽盒进行局部屏蔽, 这样和机箱一起就起到了双重屏蔽效果。

(3)缝隙屏蔽

由于装配、维修的需要, 机箱上都有缝隙, 为防止缝隙电磁泄露, 应在缝隙处加装导电衬垫, 以保持机箱电气上的连续性, 提高设备的屏蔽效能。导电衬垫的种类、结构形式很多, 应根据机箱的具体结构选用、安装相应的导电衬垫, 具体见文献[11]。

(4)孔、窗屏蔽

如机箱上有散热通风孔, 则在通风孔处安装截止波导窗, 它在抑制电磁泄露、提高屏蔽效能的同时还能保证良好的通风能力。机箱上指示灯孔的屏蔽也可以采取这种方法。显示器是军用电子设备的常用模块, 由于窗口面积较大, 需要安装屏蔽窗, 屏蔽窗既能屏蔽电场, 也能屏蔽磁场和平面电磁波, 能很好地防止电磁信息从显示窗口泄漏出去。

(5)保险丝座屏蔽

保险丝是电子设备的常用器件, 单个保险丝座则用金属帽把它覆盖起来, 帽盖内装弹性簧片使其与机箱有良好的电接触。多个保险丝座则将它们集中在一起, 专门设计屏蔽罩将其盖住。

5 结束语

安全性作为武器装备的通用质量特性之一, 其设计应和其他特性设计、性能设计、功能设计结合起来, 统筹考虑。军用电子设备的安全性设计涉及面广, 是一门综合性较强的专业, 同时也是一项实践性很强的工作, 没有一个固定的格式可套。不同类型的产品, 不同的使用场合, 会有不完全相同的安全要求和设计方法。设计人员应牢固树立新的质量观, 重视安全性设计工作, 积极跟踪并采用国内外有关安全性分析设计的理论和技术, 努力提高我国军用电子设备的安全性水平。

参考文献:

[1] 赵廷弟. 安全性设计分析与验证[M]. 北京: 国防工业出版社, 2008.

ZHAO Ting-di. Safety Design Analysis and Verification[M]. Beijing: National Defense Industry Press, 2008. (in Chinese)

[2] 阎慧, 董正宏, 韩伟杰. 军用网络电磁信息安全技术[M]. 北京: 国防工业出版社, 2010.
YAN Hui, DONG Zheng-hong, HAN Wei-jie. Safety Technique of Electromagnetic Information for Military Net[M]. Beijing: National Defense Industry Press, 2010. (in Chinese)

[3] 生建友. 通信设备的电磁信息泄露及对策[J]. 无线电工程, 2000, 30(3): 35—37.
SHENG Jian-you. Communication Equipment's Electromagnetic Signal Leakage and Its Counter-measure[J]. Radio Engineering of China, 2000, 30(3): 35—37. (in Chinese)

[4] GJB900—90, 系统安全性通用大纲[S].
GJB900—90, System Safety General outline[S]. (in Chinese)

[5] 王自力. 可靠性维修性保障性要求总论[M]. 北京: 国防工业出版社, 2011.
WANG Zi-li. Demonstration of Reliability, Maintainability and Supportability Requirements[M]. Beijing: National Defense Industry Press, 2010. (in Chinese)

[6] GJB367A—2001, 军用通信设备通用规范[S].
GJB367A—2001, General Specifications for Military Communication Equipment[S]. (in Chinese)

[7] GJB/Z150.1—2007, 军用电子设备安全设计指南(电击部分)[S].
GJB/Z150.1—2007, Safe Design Guide for Military Electronic Equipment, Part1: Protection against Electric Shock[S]. (in Chinese)

[8] GJB/Z99—97, 系统安全工程手册[S].
GJB/Z99—97, Engineering Handbook for System Safety[S]. (in Chinese)

[9] 邵小桃. 电磁兼容与 PCB 设计[M]. 北京: 清华大学出版社, 2009.
SHAO Xiao-tao. EMC and PCB Design[M]. Beijing: Tsinghua University Press, 2009. (in Chinese)

[10] 莫世禹. 舰艇通信设备安全性设计[C]//第六届电子产品防护技术研讨会论文集. 安顺, 贵州: 电子学会可靠性分会, 2008: 176—179.
MO Shi-yu. Safety Design for Communication Equipment in Warship[C]//Proceedings of the sixth Electronic Product Protection Technical Seminar Analects. Anshun, Guizhou: Reliability Branch of the Chinese Institute of Electronics, 2008: 176—179. (in Chinese)

[11] 生建友. 舰载电子设备的缝隙泄露与导电衬垫[J]. 舰船电子工程, 2000, 20(6): 51—55.
SHENG Jian-you. Shipborne Electronic Equipment's aperture Leakage and Conductive gaskets[J]. Ship Electronic Engineering, 2000, 20(6): 51—55. (in Chinese)

作者简介:

生建友(1968—), 男, 江苏泰兴人, 硕士, 高级工程师, 主要从事军用电子设备结构、工艺、可靠性的研究与设计工作, 已发表论文 50 余篇。

SHENG Jian-you was born in Taixing, Jiangsu Province, in 1968. He is now a senior engineer with the M. S. degree. His research concerns the design of structure, technology and reliability of military electronic equipment. He has published more than 50 papers.

Email: shjy668@sohu.com