

引信软件安全性与引信安全系统 软件安全性探讨

秦栋泽

(中北大学 机电工程学院, 太原 030051)

摘要: 首先结合相关标准探讨了引信软件安全性与引信安全系统软件安全性的概念以及内涵, 讨论了引信软件安全性的不同维度。进而对引信安全系统软件安全性进行了分析, 明确了引信安全系统软件主要特点。最后对当前引信系统软件安全性存在的部分问题给出了建议与改进措施。

关键词: 兵器科学与技术; 引信; 安全性; 引信软件; 引信软件安全性; 引信安全系统软件安全性

中图分类号: TJ43 **文献标志码:** A **文章编号:** 1672-9242(2024)08-0025-07

DOI: 10.7643/issn.1672-9242.2024.08.004

Fuze Software Security and Fuze Safety System Software Security

QIN Dongze

(School of Mechanical and Electrical Engineering, North University of China, Taiyuan 030051, China)

ABSTRACT: The concept and connotation of the fuze software security and fuze safety system software security were discussed and the different dimensions of the fuze software security were expounded. On this basis, the fuze safety system software security was analyzed. Meanwhile, the main characteristics of the fuze safety system software were defined. Finally, several suggestions and improvements were put forward to some problems in the current fuze system software security. The research results can provide a reference for setting standards of the fuze software security.

KEY WORDS: ordnance science and technology; fuze; security; fuze software; fuze software security; fuze safety system software security

随着弹药引信向小型化、引弹一体化、导引一体化等“三化”方向发展, 以及灵巧化、智能化水平的提高, 软件在引信中的重要性越来越突出。虽然引信软件没有它其中的硬件(如雷管、传爆管等)所具有的物理属性和化学属性, 对周围人员和物体不会造成直接的危害, 但是引信所涉及的信息交联、环境敏感、实时处理、精确控制等技术都与其软件息息相关, 引信软件有可能通过硬、软件的接口使得硬件发生误动或失效, 从而造成严重的安全事故^[1-3]。文献[4-8]

对引信软件的安全性测试进行了研究。文献[9-15]对引信软件的可靠性进行了研究。对于引信软件安全性与引信安全系统软件安全性的区别, 引信安全系统软件与其他嵌入式软件相比较的显著特点, 相关文献较少。本文主要针对上述问题展开研究。

1 国内外相关军用标准分析

美军的 MIL-STD-1316F 指出, 如在软件能直接

收稿日期: 2024-06-03; 修订日期: 2024-07-31

Received: 2024-06-03; Revised: 2024-07-31

引文格式: 秦栋泽. 引信软件安全性与引信安全系统软件安全性探讨[J]. 装备环境工程, 2024, 21(8): 25-31.

QIN Dongze. Fuze Software Security and Fuze Safety System Software Security[J]. Equipment Environmental Engineering, 2024, 21(8): 25-31.

控制或启动引信安全系统元件的情况下,可参照 AOP-52^[16-18]。AOP-52 是一份北约文件,为弹药相关软件安全提供指导。“Joint Software Systems Safety Engineering Handbook”是美国国防部的一份出版物,其目的是提供指导方针,以实现合理水平的保证,即软

件将在可接受的风险水平内执行。与软件相关的另一份重要文献是 MIL-STD-882E,该文献是国防部系统安全标准实践文件,其中包含关于软件系统安全和分析的附录 B^[19]。国内对引信安全性、软件安全性也有相关军用标准,相关内容见表 1。

表 1 引信安全性、软件安全性相关军用标准^[20-29]
Tab.1 Military standards related to fuze security and software security^[20-29]

序号	标准名称及编号	主题内容	适用范围	备注
1	GJB 373B—2019《引信安全性设计准则》	引信及作为引信子系统的安 全与解除隔离装置的安全性 设计要求	引信及弹药战斗部起爆控制 装置的安全性设计	
2	GJB 1244A—2019《电引信 和电子引信安全设计准则》	电引信和电子引信的安全设 计要求	炮弹、航空炸弹、火箭弹、导 弹等配用电引信和电子引信 的设计。不适用于全电子引信 的设计	引信的软件设计应按照 GJB/Z 102A—2012 的要 求进行安全性设计
3	GJB 346A—2019《引信安 全失效率计算方法》	引信安全失效率的计算方法	引信的安全性分析和计算	未给出软件安全失效率 计算方法
4	GJB 6456—2008《引信电子 安全与解除保险装置设计 准则》	引信电子安全与解除保险装 置的安全性设计准则	无隔爆爆炸序列且以电子或 部分以电子方式完成解除保 险和发火的引信	
5	GJB 10157—2021《军用可 编程逻辑器件软件 Verilog 语言编程安全子集》	严于语法规定的可综合 Verilog 语言编程安全子集	军用可编程逻辑器件安全关 键软件	
6	GJB 8114—2013《C/C++语 言编程安全子集》	C/C++语言严于语法规定的 编程安全子集	C/C++语言编写的军用安全 关键软件	
7	GJB 102A—2012《军用软 件安全性设计指南》	规定了军用软件安全性设计 实施指南	军用软件需求分析、设计和实 现时的软件安全性设计	
8	GJB 5369—2005《航天型号 软件 C 语言安全子集》	C 语言软件的编程准则	航天型号 C 语言软件	
9	GJB/Z 142—2004《军用软 件安全性分析指南》	软件生存周期中实施软件安 全性分析的指南	安全相关软件的获取、供应、 开发、运行和维护	
10	GJB/Z 102—97《软件可靠 性和安全性设计准则》	给出了计算机软件可靠性和 安全性设计的准则和要求	武器装备嵌入式软件的需求 分析、设计和实现	

上述军用标准从引信、软件各自角度出发,为保证安全性制定了相关的措施。GJB 373B—2019《引信安全性设计准则》附录 A 提出了实现安全控制的逻辑装置使用要求,GJB 1244A—2019《电引信和电子引信安全设计准则》提出了软件设计参考 GJB/Z 102A—2012《军用软件安全性设计指南》。要实现 GJB 373B—2019《引信安全性设计准则》附录 A 要求,是不是完全采用 GJB/Z 102A—2012《军用软件安全性设计指南》中的措施即可,是否需要针对引信特点进行必要的裁剪与增补,以便于引信软件研发人员的使用。在展开该项工作以前,本文首先对引信软件、引信软件安全性、引信安全系统软件安全性等相关概念、内涵以及特点进行探讨,为上述问题以及后续引信软件安全性的相关标准研究提供参考。

2 相关概念及内涵探讨

2.1 引信软件

由于目前尚未见明确的引信软件、引信软件安全性、引信安全系统软件安全性定义,笔者结合相关标准对上述概念进行探讨。

对于引信的相关定义,笔者主要参考 GJB 373B—2019《引信安全性设计准则》。该标准对引信(引信系统)的定义为:“用于感知环境和目标,或响应飞行时间、压力、指令等预定条件,并引发弹药战斗部装药的实体系统。引信(引信系统)可由单个独立实体或多个分布式独立实体构成。在预定的位置或时间之前,引信(引信系统)的主要功能是保证安全和向

待发状态转换^[20]”。

对于软件的相关定义,笔者主要参考了 GB/T 11457—2006《信息技术-软件术语》。该标准对软件的定义为“与计算机系统操作有关的计算机程序、规程和可能相关的文档”,对硬件定义为“用于处理、存储或传送计算机程序或数据的物理设备”,嵌入式软件定义为“大的系统的一部分,并能执行其某些需求的软件,如用于航天器或快速传输线系统中的软件;嵌入式计算机系统所用的软件^[30]”。

GB/T 11457—2006《信息技术-软件术语》中对软件的定义是从技术特点角度入手进行定义的。引信的定义是从产品功能角度入手进行定义的。在引信产品设计中,感知环境和目标,或响应飞行时间、压力、指令等预定条件,保证安全和向待发状态转换,引发弹药战斗部装药的策略或方法类问题可以由软件来实现,通过接口控制硬件完成相关功能。

结合上述2个标准的相关定义,笔者认为引信软件指:用于处理被各种传感器感知的环境和目标信息,或响应飞行时间、压力、指令等预定条件信号,在预定的位置或时间之前,保证安全和向待发状态转换,并引发弹药战斗部装药实体系统中的程序。该程序通过接口控制硬件完成上述的功能,具有配合性、协同性特点,属于嵌入式软件。

2.2 引信软件安全性

在英文中,“safety”和“security”2个词翻译过来都是安全性,但内涵不一样。“safety”指功能安全性,安全功能性,内安全;“security”指保密安全性,安全保密性,外安全等。“safety”主要为了防止系统给生命财产及生态环境造成灾难性破坏,主要威胁来源于系统设计缺陷或操作人员对关键设备的误操作,危害性是从系统内流向系统外。“security”主要是防止未授权用户非法访问系统的敏感数据或信息,主要威胁来源于外界(黑客或病毒)对系统的故意攻击,危害性是从系统外流向系统内,所指的非事物本身,而是外来的不安全影响因素。

GB/T 11457—2006《信息技术-软件术语》没有对“safety”的安全性进行定义,而是将“security”安全(性)与保密(性)放在一起定义和解释:“对计算机硬件、软件进行的保护,以防止其受到意外的或蓄意的存取、使用、修改、毁坏或泄密。安全性也涉及对人体、数据、通信以及计算机安装的物理保护^[30]”。更多强调的是保密安全性。

现阶段多数军用软件运行环境相对封闭,各种军用软件的安全性多指的是功能安全性。例如 GJB/Z 161—2012《军用软件安全性设计指南》中安全性采用的是“safety”一词,软件安全性定义:“软件运行不引起系统事故的能力^[26]”。GJB/Z 142—2004《军用软件安全性分析指南》中安全性采用的也是“safety”

一词,软件安全性定义:“软件具有的不导致事故发生的能”^[28]GJB 373B—2019《引信安全性设计准则》中安全用的也是“safety”一词,主要指的是引信的功能安全性,对于保密安全性考虑得比较少。GJB 373B7—2019《引信安全性设计准则》中所规定的条款主要是防止系统对人员或外界环境造成危害,较少关注软件本身及其要使用的数据不会被非授权代理(软件或人员)篡改等一类问题。从引信技术的发展角度看,通过引信与卫星、网络、指挥及引信间的信息交联,实现信息共享,是引信未来的一个重要发展方向^[31-42]。引信功能拓展增加通讯、组网后也面临“security”保密安全问题。

结合上述的分析,笔者认为引信软件安全性包括了功能安全性与保密安全性。功能安全性第一层面是通用的软件安全问题,第二层面是引信产品重点关注的功能性需求与软件相关的问题。保密安全性即引信软件防止其受到意外的或蓄意的存取、使用、修改、毁坏或泄密的能力。结合引信产品现阶段的技术水平,本文主要探讨的引信软件安全性是功能安全性的第二个层面,即引信产品特有的软件安全性问题。对于引信软件的可靠性以及测试性,相关文献研究得较多。软件的运行可靠是安全的基础,对于测试性,GJB 373B7—2019《引信安全性设计准则》附录中规定了保险装置(应该是指保险装置)中的逻辑装置在战时不可重复编程,未明确规定引信其他装置软件是不是可以重新编程。

2.3 引信安全系统软件安全性

现阶段引信的功能安全性主要靠引信安全系统保证,因此引信软件特有安全性问题主要体现在引信安全系统软件安全性需求中。

GJB 373B7—2019《引信安全性设计准则》中对引信安全系统的定义:“引信中用以防止解除隔离与作用的装置的集合。可包括环境敏感装置、指令执行装置、安全控制电路、保险装置、隔离装置等^[20]”。该定义非常全面,覆盖了与安全相关的装置(包括了发火控制系统的保险装置、电起爆器短路装置、延迟接电装置等),同时还强调了集合,说明安全是整个引信安全系统的属性,而不是任何给定的子组件。安全系统的核心部分安全与解除隔离装置定义域比安全系统窄,不包括发火控制系统的保险装置。一般设计中采用软件的有环境敏感装置、指令执行装置、安全与解除隔离装置的保险装置、隔离装置的动态能量开关等。

引信安全系统软件安全性指:引信中用以防止解除隔离与作用装置的集合所采用软件运行不引起系统事故的能力。安全与解除隔离装置软件安全性指:引信中用以防止解除隔离的集合所采用软件运行不引起安全系统提前解除隔离事故的能力。

引信安全系统软件安全性重点关注软件设计不当可能导致对保险装置、隔离装置等失去控制,或者是无法监控,或未能针对检测到的危险条件提供相应的缓解措施。如安全与解除隔离装置的保险装置、隔离装置动态能量开关的软件对产生危险事件的接口有直接影响。基于软件控制类别,引信安全系统软件安全应用功能可分为安全关键功能或安全相关功能,初步分析如下。

1) 安全-关键控制功能。直接控制危险硬件或事件的标称路径的软件功能(如程序初始化时控制接口处于安全状态;提供系统资源、数据库、定时、中断和一般操作的系统功能,错误处理、内存保护和防止未经认证的接口控制;在通过接口传输之前和之后,提供安全关键数据、对象或消息的打包和解包服务;将系统恢复到已知的未损坏状态所需的事件和过程等)。

2) 安全-关键监控功能。监控标称控制路径异常或监控危险硬件条件的软件功能(例如:看门狗)。

3) 安全-关键危险缓解功能。软件功能,作用于监控功能,直接缓解危险状况(例如,陷入死循环后复位)。

4) 安全-关键显示功能。软件功能,为危险硬件或事件提供显示,必须采取行动以减轻潜在的灾难风险,显示不正确的信息或未能在规定时间内提供正确的显示会导致事故(如地雷引信起爆计时显示)。

3 引信安全系统软件特点分析

3.1 典型软件架构

架构设计是软件设计中非常重要的一个环节,引信安全系统架构设计要考虑软硬件功能分配的问题。由于开发成功后软件成本比硬件更低,在满足安全性需求时,引信安全系统设计优先采用软件。引信安全系统软件架构常见的有以下几种。

1) 引信安全系统软件是独立的,此种架构安全性比较容易保证。

2) 将一个装置连接到另一个装置(如环境敏感装置与安全解除隔离装置软件各自独立),创建一个安全监控和控制分散的引信安全系统软件。此种架构时,环境敏感装置可能服务于弹药系统,也服务于引信安全系统。GJB 373B7—2019《引信安全性设计准则》的4.2.8条款指出,需要在不可逆的预定发射前,对安全系统使用性能进行状态检查。目前,随着技术的进步,高价值制导弹药在长期贮存后有软件状态检测,甚至软件更新的需求,大多数的制导类弹药环境敏感装置不仅仅服务于引信安全系统。但是引信安全系统的软件要求固化,对于该种架构环境敏感装置硬件信息直接传递给引信安全系统,引信安全系统宜编写专用的软件,不与弹药系统的环境敏感装置共用软件。

3) 各装置硬件独立,软件整合到一个MCU中(如环境敏感装置软件、指令执行装置软件、安全与解除隔离装置的保险装置整合到一个软件中,为了降低硬件成本甚至还包括探测与起爆信号处理软件,形成一个引信软件)。此种架构下,接口和计时问题就比较突出,安全性不容易保证。该种架构软件设计时,要进行全面的安全性分析以及深入的测试。

4) 通过无线通信将引信安全系统集成在一起,此时就存在保密安全性问题(如卫星定位模块服务弹药系统,也服务引信安全系统,制导弹药的GPS设备作为指令输入装置,在运行过程中GPS设备经历了短暂的电源中断或者干扰,重启后可能导致输入数据紊乱,提前给出解除保险的指令),该种架构安全性隐患较大。

3.2 特点分析

1) 软硬件耦合性强,软件受硬件接口影响大。引信安全系统硬件起额外辅助功能的组件较少(为了保证可靠性),在引信安全系统软件中实际的核心通信、控制和保护功能所需的代码,与实现这些功能额外所需的代码相比,是比较少的。引信安全系统软件的安全需求主要体现在功能需求(如提供正确的控制功能、实现所需的硬件诊断),有些是引信安全系统软件设计要实现的目标(如可容忍的失败率、最坏情况下时间响应)。因此,在引信安全系统中,不能孤立地考虑硬件和软件元素。例如,引信安全系统软件会依赖于单独的检查硬件(如外部看门狗),而硬件状态有时也会被软件监视,软件选择特定的微处理器和存储单元会产生特定的接口、时间和容量要求等。

导致引信产生安全问题的危害可能是一个单一因素,也可能是多个因素的组合。在引信安全系统中,由于最终的危害通过输出接口响应体现,对于是硬件还是软件因素导致的危害,不太容易很清晰地区分。引信硬件经过多年的工程实践,有可参考的底事件数据库,而软件应用的功能模块不同时与之相关的参数不能以与硬件相同的方式进行估计,而且要确定单个软件功能的故障概率非常困难。因此,要依据潜在的风险严重性和软件对硬件的控制程度进行研究,不能仅仅依赖于软件风险的严重性和概率。

2) 工作环境恶劣,供电不稳定。由于引信安全系统要求使用寿命内必须保持安全,因此系统设计和相关的安全参数应该考虑潜力及在生命周期内对设计完整性的“攻击”(如通过正常上电操作、维护、产品改进、升级和更换)。引信中常用的MCU芯片都存在一个稳定运行的供电电压区间,当MCU实际供电电压超出此区间时,MCU软件就可能运行异常,出现“跑飞”或者“死机”的现象,甚至同一个型号,不同批次的MCU芯片的稳定工作电压范围都有所差异。在引信安全系统中,软件一旦“跑飞”到安全关

键控制模块中, 将造成严重后果。

通常在引信上电的初始阶段、安全系统解保、起爆时容易发生电路欠压(瞬时掉电)问题。例如, 某子弹药机电引信, 该子弹药被抛撒后, 自身的涡轮发电机开始工作, 抛撒初期子弹药姿态不稳定, 转速不稳定, 导致引信供电不稳定, 容易发生电路欠压、浪涌(尖峰)问题。当引信安全系统采用火工品保险解保时, 可能会使电源瞬时断路, 导致软件重启, 此时 MCU 会自动进行硬件复位, 原先 RAM 中的数据被强制清除, 电源重新恢复后, 软件从头执行, 各个 I/O 接口输出信号也重新回归初始状态。由于电路重新上电可能造成个别 I/O 信号的异常翻转, 引起引信安全功能的混乱与错误。起爆时, 对于全电子安全系统, 工作状态切换时间间隔短, 系统的功率需求不稳定, 会引起电源输出电压的振荡波动, 软件跑飞风险增大。

3) 面临强电磁干扰, 通讯不可靠。引信模式装定、信号传输以及依靠电平触发的外部中断往往不采用标准的通信接口设计, 而是使用特定数量、特定组合的高低电平通过 MCU 的 I/O 接口发送信息。这种设计较好地降低了电路结构与软件设计复杂度, 减少了成本, 但这种信息传输方式的物理线路缺乏标准通信接口所具备的电气抗干扰特性, 易受噪声和毛刺的干扰, 导致软件对电平信号的采样误判, 特别是当电平信号的电压值较低时, 信噪比减低, 信号淹没在噪声中, 信号传输失真。例如, 引信机电安全系统中常用 MCU 输出电平使储能电容放电电路导通驱动电推解保, 全电子安全系统中利用 MCU 的 I/O 接口引脚输出 PWM 波使升压电路为起爆电容充电等。如果此信号传输线路上被电磁干扰出现强噪声, 可控硅器件可能被噪声电压所导通, 根据可控硅的特性, 一旦被导通一次, 即使后续线路上噪声消失导通状态也会一直保持, 如果软件中不进行必要的容错、避错设计, 有可能出现安全关键执行电路绕过软件的安全逻辑控制而误动作的风险。

4) 软件测试要点尚未明确规范。GJB 273B7—2019 对引信安全系统在各任务剖面的失效率进行了定义, 但是没有明确引信安全系统软件的失效率, 因为目前还没有公认的方法来测量软件的失效率, 特别是对于软件组态中的特定功能。现有的通用嵌入式软件测试技术较少考虑引信特殊的安全性需求, 主要面向的是软件通用安全性问题。由于引信软件设计总是包含缺陷, 而且缺陷越多, 那么在引信软件运行的过程中出现失效的可能性就越大。当然缺陷是否会导致严重到足以导致安全失效的错误, 则是另一个问题。引信软件失效与硬件失效的一个重要区别是没有随机行为。例如, 给定一个具有一定组合的输入的测试历程, 引信软件总是失效, 相反在另一组不同的测试历程中, 它从不失效。测试时可以人为制造单个安全特征(保险逻辑)到不安全状态, 每个安全特征依次

被破坏, 然后评估设计的性能。该方法在暴露单点故障机制和弱点方面有效, 但是如果引信软件代码量较大时, 所有代码都依次人为制造到不安全状态工作量较大, 也不一定有此必要。为了提升测试效率, 测试时, 设计人员与测试人员拟针对引信软件功能进行区分, 确定测试方法以及测试用例和可容忍的故障率。对于安全关键功能或安全相关功能宜进行详细的测试以及代码级分析。在传统的黑盒测试基础上进行白盒测试, 查看代码结构、与安全相关功能的实现、内存管理、异常或中断处理等相关的特定功能, 跟踪处理器中的功能以及它的寄存器、缓存内存、地址和数据总线等。需要注意的是引信的软件测试必须是在模拟工作开始到结束的各个环节、信号特征以及允许的极限条件。例如, 制导炸弹还要模拟全弹流程测试。

4 结语

本文针对引信软件安全性问题展开了研究, 结合相关标准探讨了引信软件、引信软件安全性与引信安全系统软件安全性的概念以及内涵, 讨论了引信软件安全性的不同维度。引信软件主要由安全系统软件和发火控制系统软件组成, 结合引信产品现阶段的技术水平, 本文主要对引信安全系统软件安全性进行了分析, 讨论明确了引信安全系统软件特点主要包括软硬件耦合性强, 软件受硬件接口影响大; 工作环境恶劣, 供电不稳定; 面临强电磁干扰, 通讯不可靠; 软件测试要点尚未明确规范等。对于部分问题初步给出了解决的建议与措施, 上述的研究成果可为引信软件安全性相关标准的制定或 GJB 373B7—2019《引信安全性设计准则》附录 A 部分后续版本的补充完善提供参考。

参考文献:

- [1] 杨辉, 高敏. 引信软件安全性概念及分析方法[J]. 现代引信, 1998, 20(4): 1-5.
YANG H, GAO M. Concept and Analysis Methods of the Software Safety of a Fuze[J]. Journal of Detection & Control, 1998, 20(4): 1-5.
- [2] 崔俊杰, 周春桂, 张明荣. 环境对引信软件安全性接口影响研究[J]. 火箭与制导学报, 2007, 27(2): 401-403.
CUI J J, ZHOU C G, ZHANG M R. The Study of the Environmental Effect on the Safety of Interface about Software of Fuze[J]. Journal of Projectiles, Rockets, Missiles and Guidance, 2007, 27(2): 401-403.
- [3] 董成基, 齐杏林, 吕静, 等. 引信软件失效模式影响分析研究[J]. 装备环境工程, 2012, 9(5): 92-97.
DONG C J, QI X L, LYU J, et al. Software Failure Modes and Effects Analysis of Fuze[J]. Equipment Environmental Engineering, 2012, 9(5): 92-97.
- [4] 高聪杰, 齐杏林, 杜力民. 引信软件安全性和可靠性仿

- 真测试系统研究[J]. 微计算机信息, 2005, 21(22): 70-71.
- GAO C J, QI X L, DU L M. Study on Safety and Reliability Simulation Testing System for Fuze Software[J]. Control & Automation, 2005, 21(22): 70-71.
- [5] 王静, 齐杏林, 郭丽华. 基于虚拟仪器技术的引信软件安全性测试系统[J]. 微计算机信息, 2005, 21(4): 164-165.
- WANG J, QI X L, GUO L H. The Testing System of Fuze Software Safety Based on Visual Instrument[J]. Control & Automation, 2005, 21(4): 164-165.
- [6] 曹营军, 杜仕国, 田春雷, 等. 引信软件的安全性[J]. 测试技术学报, 2000, 14(4): 247-251.
- CAO Y J, DU S G, TIAN C L, et al. Safety Criteria in Fuze Softwares[J]. Journal of Test and Measurement Technology, 2000, 14(4): 247-251.
- [7] STUART A W, BOOZ A H. Software Safety Functionality Hazard Assessment Focusing Level of Rigor (LOR) on the Safety-Critical Software Decision Points[C]// 18th Annual NDIA Systems Engineering Conference. Springfield: [s. n.], 2015.
- [8] DAVID A. Geremia Software Quality Assurance Applied towards the Development of VHDL - Based Safety Critical Hardware[C]// 61st NDIA Annual Fuze Conference. San Diego: [s. n.], 2018.
- [9] 娄文忠, 马宝华. 引信软件可靠性的关键问题与对策研究[J]. 探测与控制学报, 2002, 24(2): 1-4.
- LOU W Z, MA B H. Study on the Key Problem of the Fuze Software Reliability and It's Solution[J]. Journal of Detection & Control, 2002, 24(2): 1-4.
- [10] 吴奇, 王亚斌. 破甲弹机电引信嵌入式软件架构[J]. 探测与控制学报, 2021, 43(3): 12-15.
- WU Q, WANG Y B. Embedded Software Architecture for Electromechanical Armor-Breaking Projectile Fuze[J]. Journal of Detection & Control, 2021, 43(3): 12-15.
- [11] 高聪杰, 齐杏林. 引信软件可靠性测试用例生成研究[J]. 四川兵工学报, 2006, 27(1): 36-37.
- GAO C J, QI X L. Study on Case Generation of Fuze Software Reliability Test[J]. Sichuan Ordnance Journal, 2006, 27(1): 36-37.
- [12] 李湛, 娄文忠. 引信软件测试模型分析与实践[J]. 探测与控制学报, 2003, 25(S1): 59-62.
- LI Z, LOU W Z. An Analysis and Practice of Fuze Software Testing Model[J]. Journal of Detection & Control, 2003, 25(S1): 59-62.
- [13] 马少杰, 张河, 王雨时. 引信软件可靠性设计技术研究[J]. 南京理工大学学报(自然科学版), 2003, 27(4): 439-441.
- MA S J, ZHANG H, WANG Y S. Research on Reliability Design Techniques for Fuze Software[J]. Journal of Nanjing University of Science and Technology, 2003, 27(4): 439-441.
- [14] 张飞云, 李长福. 引信软件可靠性测试与评估的工程技术研究[J]. 制导与引信, 2002, 23(4): 52-57.
- ZHANG F Y, LI C F. The Reliability Test and Evaluation Study of Fuze Software[J]. Guidance and Fuze, 2002, 23(4): 52-57.
- [15] 闻泉. 基于多版本编程的软件引信滤波程序可靠性设计[J]. 电子测量技术, 2009, 32(1): 13-16.
- WEN Q. Reliability Design for Filtering Program of Software Fuze Based on N-Version Program Frame[J]. Electronic Measurement Technology, 2009, 32(1): 13-16.
- [16] Fuze Design, Safety Criteria for: MIL-STD-1316F[S]. Department of Defense .
- [17] Guidance on Software Safety Design Andassessment of Munition-Related Computing Systems: Aop-52[S]. 2008.
- [18] DOD. Joint Software Systems Safety Engineering Handbook[S]. 1999.
- [19] Department of Defense Standard Practice System Safety: MIL-STD-882E[S]. 2012.
- [20] 中央军委装备发展部. 引信安全性设计准则: GJB 373B—2019[S]. 北京: 国家军用标准出版发行部, 2019.
- General Equipment Development Department of the Central Military Commission. Fuze Design, Safety Criteria for: GJB 373B—2019[S]. Beijing: National Military Standard Publishing Department, 2019.
- [21] 中央军委装备发展部. 电引信和电子引信安全性设计准则: GJB 1244A—2019[S]. 北京: 国家军用标准出版发行部, 2019.
- General Equipment Development Department of the Central Military Commission. Guidelines for Safety Design of Electrical and Electronic Fuzes: GJB 1244A—2019 [S]. Beijing: National Military Standard Publishing Department, 2019.
- [22] 中央军委装备发展部. 引信安全失效率计算方法: GJB 346A—2019[S]. 北京: 国家军用标准出版发行部, 2019.
- General Equipment Development Department of the Central Military Commission. Method of Calculation for Fuze Safety Failure Rate: GJB 346A—2019[S]. Beijing: National Military Standard Publishing Department, 2019.
- [23] 国防科学技术工业委员会. 引信电子安全与解除保险装置设计准则: GJB 6456—2008[S]. 北京: 国防科工委军标出版发行部, 2008.
- Science and Technology Industry Committee of the National Defense. Fuze Design, Electronic Safety and Arming Devices Criteria for: GJB 6456—2008[S]. Beijing: Military Standard Publishing Department of the National Defense Science and Technology Commission, 2008.
- [24] 中央军委装备发展部. 军用可编程逻辑器件软件 Verilog 语言编程安全子集: GJB 10157—2021[S]. 北京: 国家军用标准出版发行部, 2021.
- General Equipment Development Department of the Central Military Commission. Safe Subset of Verilog Language Programming Formilitary Programmable Logic Devices: GJB 10157—2021[S]. Beijing: National Military Standard Publishing Department, 2021.

- [25] 中国人民解放军总装备部. C/C++语言编程安全子集: GJB 8114—2013[S]. 北京: 总装备部军标出版发行部, 2013.
General Equipment Department of the Chinese People's Liberation Army. Safe Subset of C/C++ Language Programming: GJB 8114—2013[S]. Beijing: Military Standard Publishing Department of the General Equipment Department, 2013.
- [26] 中国人民解放军总装备部. 军用软件安全性设计指南: GJB/Z 102A—2012[S]. 北京: 总装备部军标出版发行部, 2012.
General Equipment Department of the Chinese People's Liberation Army. Guide for Military Software Safety Design: GJB/Z 102A—2012[S]. Beijing: Military Standard Publishing Department of the General Equipment Department, 2012.
- [27] 国防科学技术工业委员会. 航天型号软件 C 语言安全子集: GJB 5369—2005KGW[S]. 北京: 国防科工委军标出版发行部, 2005.
Science and Technology Industry Committee of National Defense. Safe Subset of C Language for Space Armament Software: GJB 5369—2005KGW [S]. Beijing: Military Standard Publishing Department of the Science and Technology Industry Committee of National Defense, 2005.
- [28] 中国人民解放军总装备部. 军用软件安全性分析指南: GJB/Z 142—2004[S]. 北京: 总装备部军标出版发行部, 2004.
General Equipment Department of the Chinese People's Liberation Army. Guide for Military Software Safety Design: GJB/Z 142—2004[S]. Beijing: Military Standard Publishing Department of the General Equipment Department, 2004.
- [29] 国防科学技术工业委员会. 软件可靠性和安全性设计准则: GJB/Z 102—97[S]. 北京: 国防科工委军标出版发行部, 1997.
Science and Technology Industry Committee of National Defense. Software Reliability and Safety Design Criteria: GJB/Z 102—97[S]. Beijing: Military Standard Publishing Department of the Science and Technology Industry Committee of National Defense, 1997.
- [30] 中华人民共和国国家质量监督检验检疫总局, 中国国家标准化管理委员会. 信息技术 软件工程术语: GB/T 11457—2006[S]. 北京: 中国国家标准管理委员会出版发行部, 2006.
General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China, Standardization Administration of China. Information Technology—Software Engineering Terminology: GB/T 11457—2006[S]. Beijing: Publishing Department of the Standardization Administration of China, 2006.
- [31] 张合. 引信的过去、现在与未来[J]. 探测与控制学报, 2023, 45(5): 1-6.
ZHANG H. The Past, Present and Future of Fuze[J]. Journal of Detection & Control, 2023, 45(5): 1-6.
- [32] 张合. 灵巧引用三元级联控制方法研究[J]. 中国科学: 技术科学, 2023, 53(9): 1449-1464.
ZHANG H. "Three-Element" Cascade Control Method of a Smart Fuze[J]. Scientia Sinica (Technologica), 2023, 53(9): 1449-1464.
- [33] 张合. 引信与环境[J]. 探测与控制学报, 2019, 41(1): 1-5.
ZHANG H. Fuze and Environment[J]. Journal of Detection & Control, 2019, 41(1): 1-5.
- [34] 马宝华, 游宁, 李杰, 等. 云弹药引信的技术命题[J]. 探测与控制学报, 2017, 39(6): 1-5.
MA B H, YOU N, LI J, et al. Technical Propositions of Cloud Ammunition Fuze[J]. Journal of Detection & Control, 2017, 39(6): 1-5.
- [35] 马宝华. 现代引信的控制功能及特征[J]. 探测与控制学报, 2008, 30(1): 1-5.
MA B H. Control Function and Characteristics of Modern Fuzes[J]. Journal of Detection & Control, 2008, 30(1): 1-5.
- [36] 马宝华. 战争、技术与引信——关于引信及引信技术的发展[J]. 探测与控制学报, 2001, 23(1): 1-6.
MA B H. War, Technology and Fuze-about Fuze and Fuze Technology Development[J]. Journal of Detection & Control, 2001, 23(1): 1-6.
- [37] 马宝华. 网络技术时代的引信[J]. 探测与控制学报, 2006, 28(6): 1-6.
MA B H. Fuze in Networked Technology Era[J]. Journal of Detection & Control, 2006, 28(6): 1-6.
- [38] 施坤林, 黄峥, 马宝华, 等. 国外引信技术发展趋势分析与加速发展我国引信技术的必要性[J]. 探测与控制学报, 2005, 27(3): 1-5.
SHI K L, HUANG Z, MA B H, et al. The Analysis of the Characteristics and Trend of the Foreign Fuze Technology and the Necessary of the Rapid Developing of Our Fuze Technology[J]. Journal of Detection & Control, 2005, 27(3): 1-5.
- [39] 施坤林, 黄峥, 牛兰杰, 等. 引信的三大基础技术与发展要求[J]. 探测与控制学报, 2018, 40(1): 1-4.
SHI K L, HUANG Z, NIU L J, et al. Three Underlying Technologies and Developing Requirements of Fuze[J]. Journal of Detection & Control, 2018, 40(1): 1-4.
- [40] 汪仪林, 马秋华, 张龙山, 等. 引信智能化发展构想[J]. 探测与控制学报, 2018, 40(3): 1-5.
WANG Y L, MA Q H, ZHANG L S, et al. The Development Visualization of Fuze Intelligentize[J]. Journal of Detection & Control, 2018, 40(3): 1-5.
- [41] 汪仪林, 张龙山, 马秋华. 从美军标看我国引信安全性的差距[J]. 探测与控制学报, 2019, 41(3): 1-5.
WANG Y L, ZHANG L S, MA Q H. The Deficiencies of Domestic Fuze Safety Referring to U.S. Military Standards[J]. Journal of Detection & Control, 2019, 41(3): 1-5.
- [42] 崔占忠. 引信发展若干问题[J]. 探测与控制学报, 2008, 30(2): 1-4.
CUI Z Z. Some Issues on the Fuze Development[J]. Journal of Detection & Control, 2008, 30(2): 1-4.