引信软件失效模式影响分析研究

董成基，齐杏林，吕静，于毅成，赵志宁
（军械工程学院，石家庄 050003）

摘要：可编程器件在新型引信中的应用，使得软件安全性成为影响整个引信系统安全性的重要因素，软件失效后可能通过软硬件界面使硬件发生误动，并可能导致严重的事故。软件安全性分析是保证软件安全性的有效方法之一。将软件失效模式影响分析法（SFMEA）应用于引信软件分析中，从弹药存储至清理全过程分析可能由引信软件导致的风险，给出了分析的关键步骤、常见的失效模式和原因。结合某型基于双微处理器的引信进行了实例分析，发现了其中一个风险未被降低至可接受水平，证明了该方法的有效性。

关键词：引信软件；SFMEA；软件安全性；风险
中图分类号：TP311.5；TJ430　　**文献标识码：**A
文章编号：1672－9242(2012)05－0092－06

Software Failure Modes and Effects Analysis of Fuze

DONG Cheng-ji, *QI Xing-lin*, *LYU Jing*, *YU Yi-cheng*, *ZHAO Zhi-ning*
(Ordnance Engineering College, Shijiazhuang 050003, China)

Abstract: The using of Programmable Logic Devices (PLD) in new type fuzes makes software safety becoming a fatal factor influencing whole system′s safety. The software failures may cause hardware action abnormally through interface between software and hardware, and the abnormal action may cause mishap. Software safety analysis is an effective way to assure software safety. Software Failure Modes and Effects Analysis technique was applied to analyze fuze software safety, including lifecycle risks that may caused by software from ammunition handling to disposal. The key steps of analysis as well as the general software failure modes and the exact causes were given. A case study on analyzing a double micro-controllers based fuze system found an unacceptable risk which isn′t being controlled, which proved the effectiveness of SFEMA technique.

Key words: fuze software; SFMEA; software safety; risk

引信是保证弹药安全性的关键装置，近年来微处理器、微控制器、可编程序逻辑控制器等可编程器件应用在新型引信中，软件安全性也成为影响整个引信系统安全性的重要因素，其失效可能通过软硬件界面使硬件发生误动，从而导致严重的事故，损害装备或危及生命。如何保证引信软件的安全性是一

收稿日期：2012-05-26
作者简介：董成基（1988—），男，四川人，硕士研究生，研究方向为嵌入式软件测试、软件可靠性、软件安全性。

个亟待解决的问题。

北大西洋公约组织已经制定了针对引信软件安全性的标准AOP-52,但是引信软件安全性仍然存在诸多挑战,包括分析技术、设计技术、测试和验证标准等都是人们面临的难题[1]。20世纪90年代初我国相继对全电子安全系统及其软件展开了研究,在GJB 373A—97和GJB 6456—2008中都要求对含有嵌入内置式微处理器、控制器或其他计算装置的安全与解除保险系统分析确定软件对启动保险件所起的作用,并确认任何单点失效或可信失效类型。国内对引信软件安全性的研究涉及概念定义、分析和测试等方面。概念定义方面主要对软件可靠性、保密安全性与事故安全性做了区分[2];分析技术包括故障树、Petri网[2—4]、失效模式影响分析[5]和引信软硬件界面分析[6];测试领域通常通过分析引信软件中的安全关键软件,然后采用半实物仿真技术对其进行测试[7]。

上述研究对引信软件安全性保证提供了基本思路,奠定了较好的基础,但是尚不能满足军标中提出能确认单点失效或可信失效类型的要求,而且没有在引信处理至清理的全过程考虑引信软件安全性。故障树和Petri网都属于模型,使用有限制,要对引信软件存储至清理的全过程进行安全性分析,显然不适用。因此采用SFMEA对引信软件进行分析,为引信软件安全性设计和测试提供依据。

1　引信存储至清理全过程的安全性需求

在美国第54届引信年会上,提出了现代战争中对引信安全性的新要求[8],如图1所示。传统的引信安全性需求只包括安全距离之前的安全性,而新的需求则增加了飞行阶段和战斗之后的安全性需求,全面涵盖了引信处理、使用和战场清理等全过程。

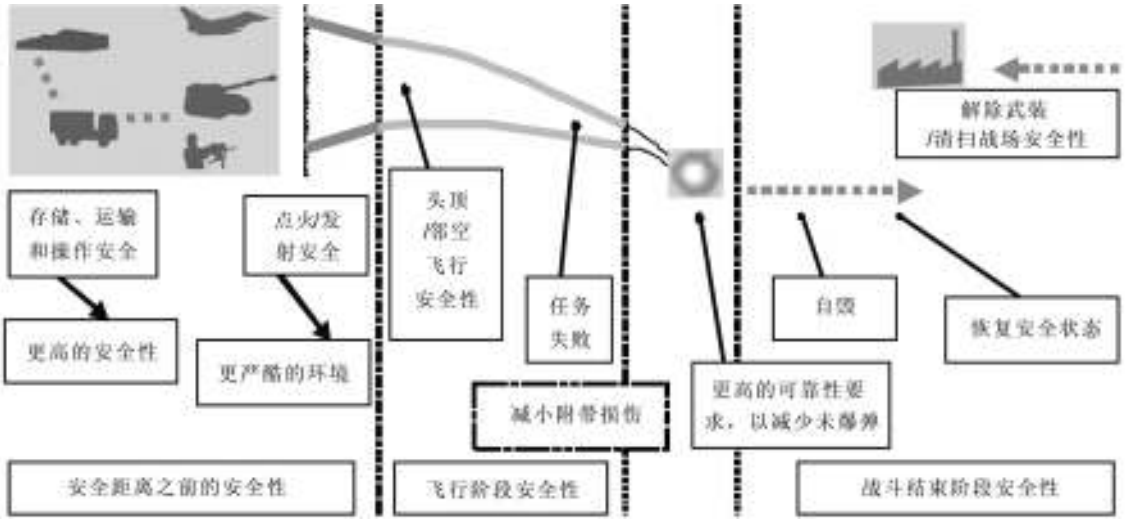

图1　现代战争对引信安全性的新需求

Fig. 1　New requirement of fuze safety for modern warfare

引信软件失效模式和影响分析也应该在引信存储至清理的全过程中来考虑。一方面是为了全面掌握引信失效或误操作可能产生的事故。另外,虽然引信软件导致的安全性问题是由于引信软件的设计缺陷或编码中引入缺陷导致的,软件缺陷不会像硬件那样因遭遇恶劣环境和随时间的推移而增多,但是使用环境会对硬件产生影响,硬件是软件运行的平台,一旦硬件失效,软件也有可能失效,全过程的考虑有助于全面分析导致软件失效的原因。

2　软件失效模式影响分析简介

2.1　软件失效模式影响分析方法及步骤

SFMEA用于分析软件系统中软件失效对系统可能造成的影响。首先进行系统风险分析,建立系统可能进入的危险状态与系统风险之间的映射,然后分析输入变量和软件逻辑的失效模式,变量输入

和软件逻辑的失效模式被映射到对输出的影响上，再将输出的失效映射到风险分析阶段确定的系统风险状态，风险状态由软件的变量标示[9]，如图2所示。连接风险分析和失效模式影响的纽带是确定系统状态为风险状态的软件中所有变量的取值和时序，所以变量是SFMEA的核心和着力点。然而，由于软件的封装性，获取软件的源代码比较困难，在不能获得源代码的情况下只能考虑外部的输入和输出变量。

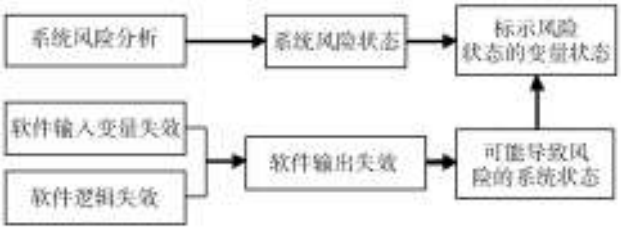

图2 SFMEA过程

Fig. 2 The process of SFMEA

2.2 软件失效模式的确定

软件系统的种类繁多，不同类别的软件其失效模式各有其特点。国内外对通用类软件的失效模式做过很多研究，概括了很多种软件失效模式。在提取软件失效模式时，基于《通用软件失效模式分类表》[10]，结合目标软件的特点，分析当前关注软件所有可能的失效模式，有取舍地利用、细化。

3 引信软件失效模式影响分析

3.1 弹药系统风险分析

考虑现代战争中对引信安全性的新要求，应在弹药储存至清理的全过程中对引信系统风险进行分析。弹药在储存、运输和处理阶段的风险包括电、火、潮、跌落和撞击等因素导致的弹药引爆；在弹药从发射到安全距离这一阶段的风险有发火时间误差、弹丸留膛、膛炸、炮口早炸等；在飞行阶段的风险包括射程过短、误识别目标造成误攻击等；在作用阶段的风险有提前作用、延后作用和伤及无辜；战斗结束后的风险主要是未爆弹被意外引爆。

对应弹药各阶段的风险，引信系统在储存、运输、处理、使用和清理各个阶段也存在可能由引信软件导致的风险。在储存、运输和处理阶段，由于弹上可编程器件不供电，即使有静电等因素影响，因软件失效而使引信系统进入风险状态的可能性也非常小，故不予分析；从发射到安全距离阶段的风险主要是过早解除保险；飞行阶段的风险是引信提前作用，出现异常，不能使弹药进入安全状态；作用阶段的风险有引信作用模式选择错误而伤及无辜；战斗结束后的风险是未绝火或泄能。引信在弹药处理及使用各阶段的风险分析见表1，为了与失效模式分析结合，列出了各阶段风险涉及的软件变量。

表1 引信各阶段可能由软件导致的风险

Table 1 The risks that may be caused by software in each phase

阶段	风险	相关软件变量
储存、运输、处理	无	无
从发射到安全距离	过早解除保险等	解除保险信号、计时器
飞行阶段	提前作用、出现异常，不能使弹药进入安全状态等	起爆信号
作用阶段	引信作用模式选择错误而伤及无辜	起爆模式选择信号、起爆信号
战斗结束后	未绝火或泄能	自毁信号、绝火信号、泄能信号

3.2 引信软件失效模式的确定

按照2.2节中介绍的方法，确定引信软件的失效模式。软件通用失效模式分为12大类。引信软件属于嵌入式软件，故其失效模式分析可以借鉴嵌入式系统的结构来分析。一个典型的嵌入式安全关键软件中，系统先自检，然后读入传感器信号，验证传感器信号的值，计算控制信号，验证控制信号和硬件状况，如果硬件状况良好则允许输出，所有的验证都正确才输出控制信号到执行机构[11]。在无法获取源代码的情况下，只能分析软件的输入和输出，而对于中间处理过程只能根据软件设计的相关文档进行分析。中间处理包括对数据的处理和控制信号的计算等操作，中间处理的失效包括数据处理计算不正确和软件本身失败两类，两者都可以视为软件逻辑失效，所以从输入和软件逻辑的失效模式到输出映射的角度来对引

信软件的失效模式进行分类分析,分析注重从数值和　　时间两个方面展开,分析结果见表2。

表2　软件失效模式到对输出影响的映射

Table 2　The map from software failure modes to outputs

失效模式		对输出的影响	
		无输入错误检测	有输入错误检测
输入的失效模式	正确的输入不被接受	无输出	无输出
	输入值超出有效范围	输出值错误	无输出
	在有效范围内的错误输入值	输出值错误	无输出
	输入不完整	输出错误	无输出
	输入时刻超时	输出时刻超时	无输出
软件逻辑的失效模式	程序无法启动	无输出	
	程序非正常终止	无输出或输出不完整	
	程序不能终止	无输出或输出不完整	
	程序运行超时	输出超时	
	程序运行时机超前或滞后	输出时机提前或滞后	
	中断处理错误	输出错误或时序错误	
	数值计算错误	输出值错误	
	数值计算精度不满足要求	输出精度不满足要求	
	功能不完整	输出不完整	
	多余的功能	输出多余	

3.3　引信软件失效模式原因分析

找到软件失效的原因才能从根源上杜绝失效的产生。按照输入和软件逻辑两大类失效模式展开分析,分析结果见表3。引信软件的输入来源是传感器,其失效可以简单处理为数值失效和时刻失效。软件逻辑失效则有计算相关的失效和程序本身失败两类。

表3　软件失效的原因分析

Table 3　Software failure causes analysis

失效模式分类	失效原因
输入数值错误	传感器数据丢失
	传感器数据错误
输入时刻错误	I/O接口时序错误
	外围电路与接口不同步
程序无法启动	无法正常初始化
程序非正常终止	功能运行的前提条件不满足
程序不能终止	死循环或死锁
程序运行超时	处理时间过长
程序运行时机超前或滞后	提前或滞后触发软件,处理器时序紊乱
中断处理错误	中断阻塞或中断返回错误
数值计算错误	设计不符合需求、表达式不完整或不正确
数值计算精度不满足要求	舍入或舍去错误、混合类型计算
功能不完整	缺失计算
多余的功能	多余的计算及输出

3.4 引信软件失效模式影响分析实例

失效模式对系统的影响分析需要将失效模式对应到软件系统的风险状态，但是失效模式只有与具体的引信软件实例结合起来才能确定风险状态的映射。例如数值计算错误这个失效模式可能发生在软件中的多个地方，不同变量的取值计算错误造成的影响不一样，对应的风险也不同，所以应结合软件实例具体分析。以某基于双微控制器的引信为例进行分析如下。

该型引信为双微控制器电子安全结构，主控制器的软件流程如图3所示，第一和第二环境信息由引信的加速度传感器和转速传感器传送至微控制器。环境信号识别、解除保险和发火这些安全关键操作都必须由主控制器和安全控制器共同决策。解除保险和起爆决策示意如图4所示，解除保险（拔销点火）信号输出的条件是后座开关信号、离心力信号以及固定的远距离解除保险时间都正常，而且这3个信号的时序必须正确，起爆信号的输出条件与此类似。

根据表1，该引信中可能由软件导致的风险只涉及前3个阶段，风险包括过早解除保险和提前作用。风险由输出问题导致，根据表2和表3中的失效

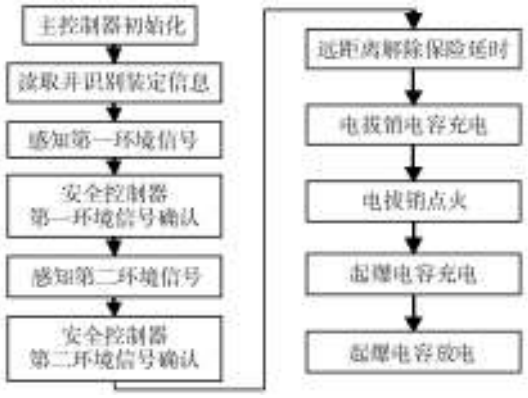

图3 某型引信主控制器软件流程

Fig. 3 Main controller software flow of a fuze

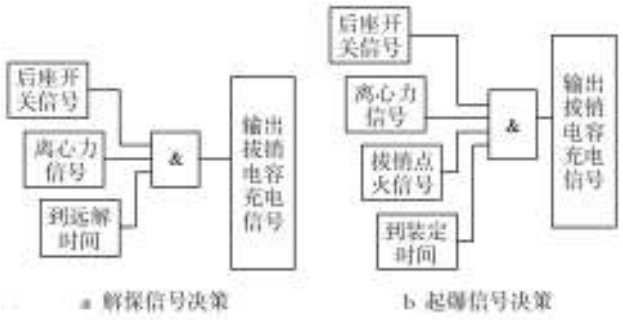

图4 某型引信软件关键信号输出决策

Fig. 4 Output signals decision-making of the fuze

表4 某基于双微控制器的引信软件失效模式影响分析

Table 4 The SFMEA of a double micro-controllers based fuze software

软件单元	失效模式	失效原因	影响		危害等级
			局部影响	系统影响	
初始化	变量未初始化	设计忽略或遗漏	计算值错误	输出控制信号错误	严重
子程序	未控制不使用的内存	设计时忽略或遗漏	程序“跳飞”读入“脏”数据	程序失败或“非法”动作	严重
读写EEPROM	写EEPROM错误	地址错误或数值错误	无法读取正确装定时间	早炸、作用时间长或瞎火	非常严重
子程序	读EEPROM错误	地址错误或传输错误	无法读取正确装定时间	早炸、作用时间长或瞎火	非常严重
判断第	信号早到	加速度传感器或I/O接口时序错误	解保逻辑判断错误	提前解保或无法解保	非常严重
一环境	信号晚到	加速度传感器或I/O接口时序错误	解保逻辑判断错误	无法解除保险	非常严重
子程序	信号值错误	加速度传感器错误或传输错误	解保逻辑无法正常判断	无法解除保险	严重
SPI通信	主控制器和安全	同步机制受阻	解保逻辑无法正常判断	无法解除保险和发火	严重
子程序	控制器时间不同步				
远距离解	解保信号早输出	两个环境信号都发生早到	提前解除保险	早炸	非常严重
除保险	解保信号晚输出	计算超时或时序错误	无法解保	瞎火	严重
子程序	解保信号值错误	计算错误或传输错误	无法解保	瞎火	严重
	发火信号早输出	时间装定错误	引信提前作用	造成安全事故	严重
发火子程序	发火信号晚输出	时间装定错误或时序错误	引信作用时间长或无法作用	弹药清除存在危险	严重
	发火信号值错误	计算错误	发火电路无法正常导通	引信无法作用	严重

模式对输出的影响,确定导致引信进入风险状态的失效模式,再根据表3分析相关的失效原因,分析结果见表4,判断第二环境力子程序与判断第一环境力子程序类似,故未给出。

通过分析发现读写EEPROM等几个影响非常严重的失效模式,但在引信设计中这些失效模式对应的风险都得到了较好的控制。在引信处理及使用的全过程中发现,该引信中没有设计绝火和泄能,其相应的风险未得到良好的控制。美国军用引信手册MIL-HDBK-757中提出能量泄漏的需求是存在的,以便在弹药瞎火时,爆炸物处理队能够在电发火电路安全有保障的条件下回收或移动弹药。故通过分析,应在该引信中增设绝火和泄能功能,以便在引信出现异常状态时,能使弹药进入安全状态。

4　总结

将软件失效模式影响分析技术用于对引信软件安全性的分析,总结了引信软件常见的失效模式,并在引信存储至清理的全过程中对某基于双微控制器的引信软件进行分析,发现了其中安全性设计中欠考虑的一个安全性问题。证明该方法的有效性,为引信软件安全性保证提供了一种可行的方法。

参考文献:

[1] FORNOFF Jeffrey M. Scalable Software Evaluation Method-ology and Tools[C]// UT:55th Annual Fuze Conference. Salt Lake City,2011.(余不详)

[2] 杨辉,高敏. 引信软件安全性概念及分析方法[J]. 现代引信,1998(4):1—5.

[3] 王卫民,陈亚旭,齐杏林. SFAT和PETRI网在引信软件安全性分析中的应用[C]// 第十三届引信学术年会. 重庆,2003.(余不详)

[4] 王卫民,陈亚旭,齐杏林. 基于PETRI网的引信软件安全性分析实例研究[C]// 第六届国际可靠性、维修性、安全性会议. 西安,2004.(余不详)

[5] 李世中,张亚,赵河明. 引信软件安全性分析方法初探[C]// 第六届国际可靠性、维修性、安全性会议. 西安,2004.(余不详)

[6] 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]. 弹箭与制导学报,2007,27(2):505—507.

[7] 王静,齐杏林,吕静. 引信软件安全性仿真测试系统研究[J]. 军械工程学院学报,2005,17(3):18—20.

[8] PERRIN Max. New Safety Requirements Fuzing System Sol-utions[C]// MO:54th Annual Fuze Conference. Kansas City,2010.(余不详)

[9] GODDARD P L. Validating the Safety of Embedded Real-Time Control Systems Using FMEA[C]// Reliability and Maintainability Symposium. Atlanta,1993.(余不详)

[10] 王丙磊. 系统级软件FMEA方法及辅助分析工具的研究[D]. 长沙:国防科学技术大学,2009.

[11] GODDARD P L. Software FMEA Techniques[C]// Reliability and Maintainability Symposium. Los Angeles,California U-SA,2000.

(上接第61页)

浙江大学,2006:7—9.

[13] 梁宝平. 干燥设备设计选型与应用实用手册[M]. 北京:北方工业出版社,2006.

[14] JOHNSON AJ,PETERSEN RD,SWANSON SD. Microwave Heating Apparatus and Method:USP,4940865[P].1990-07-10.

[15] DIXON D,ERLE R,ESCHEN V,et al. Microwave Solidific-ation Development for Rocky Flats Waste[EB/OL]. [1994-04-01]. http://www.osti.gov/bridge/servlets/purl/120869-OncrNF/webviewable/120869. pdf.

[16] Sprenger G S,Petersen R D. Microwave Waste Processing T-echnology Overview[EB/OL]. [1995-04-01]. http://www.os-ti.gov/bridge/servlets/purl/120869-OncrNF/webviewable/120869. pdf.

[17] WHITE T L,BERRY J B. Microwave Processing of Radioa-ctive Materials-1[R]. Dallas,Texas:American Chemical So-ciety,1989.

[18] WHITE TL. Microwave Applicator for In-drum Processing of Radioactive Waste Slurry:USP,5324485[P]. 1994-06-28.

[19] ERLE R R,ESCHEN V G,SPRENGER G S. Optimization of Microwave Heating in an Existing Cubicle Cavity by Incorp-orating Additional Wave Guide and Control Components[R]. USDOE,1995.