远程多管火箭炮火控系统的软件安全性测试分析

庞红彪 李之博 高小雅
(中国兵器工业信息中心 北京 100089)

摘 要 简单介绍了远程多管火箭炮火控系统的软件组成、功能、典型任务剖面和软件安全性测试的基本内涵;然后根据火控系统的典型任务剖面分析了不同阶段的软件安全性测试,系统解决了远程多管火箭炮火控系统软件安全性测试"难""杂""多"问题,有效提高了测试效率和质量,进一步确保了远程多管火箭炮火控系统的安全性。

关键词 远程多管火箭炮,火控系统,典型任务剖面,软件安全性测试,软件质量
中图法分类号 TP311.5 **文献标识码** A

Software Safety Test Analysis for Fire Control System of Remote Multi-barrel Rocket

PANG Hong-biao LI Zhi-bo GAO Xiao-ya
(Information Central of China North Industries Group Corp, Beijing 100089, China)

Abstract The fire control system's software composition, function and typical task profile of remote multi-barrel rocket were introduced briefly. And the basic connotation of the software safety test was introduced briefly. Then according to the typical task profile of the fire control system, the software safety test in the various stages was analyzed, and the " difficult" " Miscellaneous " " multiple " problems in the course of the fire control system's software safety test were solved systematically. The test efficiency and quality are improved effectively, and the fire control system's safty of remote multi-barrel rocket is ensured further.

Keywords Remote multi-barrel rocket, Fire control system, Typical task profile, Software safety test, Software quality

1 引言

远程多管火箭炮是我军口径最大、射程最远和首次采用控制技术的新型火箭炮,是我军炮兵重点发展的装备。随着火箭炮武器信息化的发展,赋予软件的功能越来越强大,造成软件规模越来越庞大,越来越复杂。但是由于重功能、性能,轻效能的传统观念,忽视可靠性、维修性、保障性、安全性等设计,造成装备使用寿命短、故障严重、维修效率低、安全风险高,尤其是安全性,对于武器装备来说,虽然发生概率低,但一旦发生安全事故,轻则装备损坏,重则危及人员生命;同时由于很多研制单位不重视软件,加上国内软件工程化起步较晚,软件研发人员对标准的理解有差异,导致在编制软件需求时连软件功能性能需求都有可能描述不清,软件安全性更无从谈起,致使软件安全性测试几乎没有,存在巨大的安全隐患。因此本文从多年多管远程火箭炮火控系统(以下简称火控系统)软件实际测试经验出发,以火控系统工作任务剖面为基础,对火控系统软件的安全性测试进行分析,以提高火控系统软件安全性测试的效率和质量,同时供软件研发人员参考。

2 火箭炮火控系统典型任务剖面

2.1 火控系统软件组成

远程多管火箭武器系统由火控系统、无人机侦察系统、指挥系统和保障装备组成。火控系统是火箭炮自动控制和火箭弹发射控制的核心,是火箭炮部队承担战斗任务的主要装备,一般由远程多管火箭炮、火箭弹、弹药装填车等组成,其主要功能包括指挥通信、信息处理、导航、寻北、弹道解算、调炮、火箭弹的参数装定和发射控制等。火控系统软件一般包括弹载计算机软件、组合导航软件、卫星定位软件、GNSS 定位装置软件、地面发控装置软件、火控操控台软件、惯导软件、随动控制软件、火控计算机软件、炮长显控台软件和药温装置软件,其软件组成及相互关系如图 1 所示。

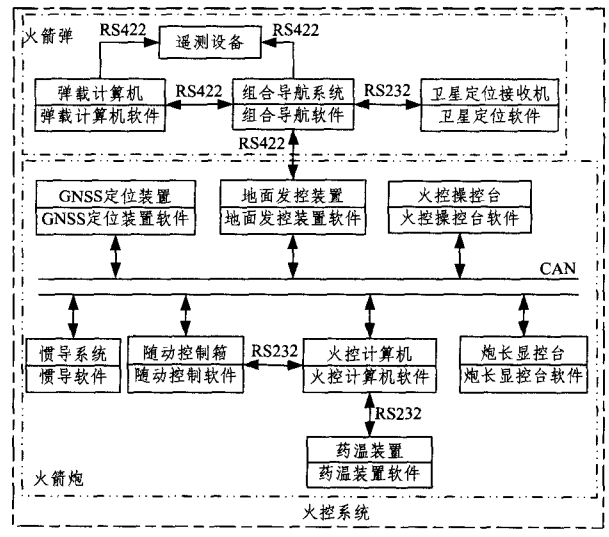

图 1 远程多管火箭炮火控系统软件组成示意图

庞红彪(1977—),男,硕士生,高级工程师,主要研究方向为软件可靠性与软件测评、软件工程,E-mail:li19ly@126.com;李之博(1984—),女,工程师,主要研究方向为软件可靠性与软件测评、软件工程;高小雅(1981—),女,工程师,主要研究方向为软件可靠性与软件测评、软件工程。

2.2 火控系统典型任务剖面

在作战使用时，火控系统有“导航”、“自主”和“非自主”3种工作模式。“导航”模式主要在行军时使用；“非自主”模式是指火控系统在营(连)射击指挥系统指挥下工作；“自主”模式是指火控系统“脱离”营(连)射击指挥系统的指挥独立作战，与“非自主”的主要区别在于火控系统得到目标信息和气象资料后，根据本炮定位定向导航装置测得的炮阵地坐标，由炮长显控台自动解算出射击装定诸元及飞行任务参数，其它的工作原理和操作过程基本与“非自主”作战方式相同。典型作战发射任务剖面如图2所示。

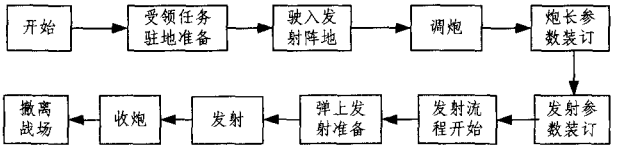

图2 远程多管火箭炮发射剖面示意图

3 软件安全性测试基本内涵

软件安全性测试是验证软件安全性等级和识别潜在安全性缺陷的过程，包括安全性和保密性两个方面，除了检验软件中已存在的安全性、安全保密性措施外，还应识别潜在软件安全性缺陷。对于非嵌入式软件，软件安全性是软件在受到恶意攻击时依旧能提供所需功能的能力，更多关注的是软件的失效安全性；对于嵌入式软件，软件安全性是在系统发生错误、产生故障或异常时能够容错的能力，更多关注的是在错误、故障或异常条件下软件对设备、人员和环境的保护。火控系统软件是嵌入式软件。根据GJB2725A附加指南的要求，嵌入式软件安全性测试策略包括以下几个方面：

1)对安全性关键的软件部件，必须单独测试安全性需求；

2)在测试中全面检验防止危险状态措施的有效性和每个危险状态下的反映；

3)对设计中用于提高安全性的结构、算法、容错、冗余、中断处理等方案，必须进行针对性测试；

4)应进行对异常条件下系统/软件的处理和保护能力的测试(以表明不会因为可能的单个或多个输入错误而导致不安全状态)；

5)对输入故障模式的测试；

6)必须包含边界、界外及边界结合部的测试；

7)对“0”、穿越“0”以及从两个方向趋近于“0”的输入值的测试；

8)测试安全性关键的操作错误测试。

4 火控系统软件安全性测试分析

根据远程多管火箭炮火控系统典型任务剖面，火控系统软件安全性主要包括以下几个方面：第一，出厂验收及驻地准备过程中的软件安全性，直接影响着火控系统的调炮精度；第二，行军过程中的软件安全性；第三，调炮过程中的软件安全性，直接影响着火控系统的调炮安全；第四，发射过程中的软件安全性，影响火箭弹能否安全发射，完成最终的发射任务；第五，其它安全性要求。

4.1 出厂验收及驻地准备过程中的软件安全性测试

火箭炮在出厂前都要进行出厂验收，以对各种安装误差和系统误差进行校正，在校正后才能交付。

在接收到作战任务后，炮长获取目标坐标、阵地坐标、气象文件和射击口令后上报弹药条件、当前位置、开始诸元以及完成情况，然后命令火控台。

火控台收到命令后给火控计算机、随动系统、惯导、药温装置、GNSS和地面发控装置上电，在确认上电完成后发送自检命令，自检正常后向车载惯导发送校正点坐标，待惯导寻北完成提示后自动用炮。其任务剖面如图3所示。

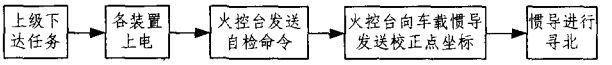

图3 驻地准备任务剖面

1)软件对重要数据的保护安全性测试

火箭炮在出厂时要对一些重要参数进行校正，包括对姿态角传感器进行修正，获取惯导安装误差、惯导里程系数、弹性变形数据、炮口偏移量以及对随动进行归零操作；对这些数据的修改必须有权限控制，但是由于火控系统都是嵌入式软件，并且没有连接互联网，相对对立，因此密码安全性远比连接互联网软件的密码安全性简单得多，因此只要验证密码安全性的有效性即可。软件密码安全性包括密码登录和密码设置/更改两个方面，其安全性测试设计如表1、表2所列。

表1 密码登录安全性测试设计表

密码元素设计长度		小于	等于	大于	为空
密码登陆输入密码情况	密码长度	×	√	×	×
	输错次数	√	×	×	——

表2 密码设置/更改安全性测试设计表

密码设置/更改情况	纯数字	纯字母	纯特殊字符	数字字母组合	数字字符组合	字母字符组合	数字字母字符组合
有效性	√	√	√	√	√	√	√

2)零位校正与调炮安全性测试

零位校正目的是修正炮零位与车体位置之间的偏差。但是零位校正后使得炮相对于原来的车体位置存在偏差，而调炮就是相对于零位的运动，其范围在输入时是一个绝对值(比如方位范围：$[-a,a]$mil，高低范围：$[b,c]$mil)，并不随着炮的零位变化而相应变化。这时如果还按照原来的正常调炮范围进行调炮，可能导致以下两种情形：一是无法调炮；二是因超界导致设备损坏，在火箭炮实际测试过程中出现过零位重新校正后而引发的安全性事故，因此必须对零位校正与调炮范围之间的逻辑关系进行测试，设Δ=零位校正量(包括高低和方位)，其安全性测试设计如表2所列。

表3 零位校正与调炮范围之间的逻辑安全性测试设计表

调炮范围 \ Δ	<下边界	≥下边界	<0	=0	>0	≤上边界	>上边界
高低下边界	×	b−Δ	b−Δ	b	b+Δ	b+Δ	×
高低上边界	×	c−Δ	c−Δ	c	c+Δ	c+Δ	×
方位下边界	×	−a−Δ	−a−Δ	−a	−a+Δ	−a+Δ	×
方位上边界	×	a+Δ	a+Δ	a	a+Δ	a+Δ	×

3)惯导寻北与调炮安全性测试

惯导寻北是保证调炮精度的前提条件，因此在寻北过程中不允许调炮，否则将会影响调炮精度。

4)与安全相关的故障处理情况测试

在整个火箭炮中与安全相关的单体包括火控计算机、随动控制箱、弹载计算机和地面发控装置，因此要测试在各个单体发生故障时软件的处理能力，其总体测试策略如下。

a)对每个单体的故障要有针对性测试。对于火控计算机，自检包括各单体通信自检和药温装置；对于随动控制系统，它是调炮操作的执行者，保证了调炮的安全性，而保证随动控制系统准确调炮的是高低姿态采集器和方位姿态采集器，因而随动控制系统在进行自检时，必须对高低姿态和方位姿态采集的正确性进行自检，确保正常，同时必要时可以通过命令自检方式对调炮精度进行自检；对于弹载计算机，它是控制炮弹飞行的核心部件，其自检包括关键内存单元自检、DA/AD检测、通信检测、引信初始状态检测、舵机检测、二次电源检测；对于地面发控装置，自检包括火箭弹检测、地面发控参数装定板检测、地面发控弹上控制板检测和地面发控弹上供电板检测。

b)对每个故障的确认要有防虚报测试，需要软件进行多次确认；

c)对每个单体的报故时间要有超时处理测试；

d)要对各个状态信号的脉宽和幅度进行测试。

4.2 行军过程中的软件安全性测试

在驻地准备完成后，火箭炮按照指令驶入发射阵地。一般说来，在行军状态时火控系统全部关闭电源。需要导航时由GPS定位定向导航装置或惯性定位定向导航装置进行导航，这时火控操控台、惯性定位定向导航装置、炮长显控台需要开机，从软件安全性来讲只要保证导航状态下不允许操作调炮即可，因此只要验证导航状态下软件是否限制调炮操作即可。

4.3 调炮收炮操作过程中的软件安全性测试

远程多管火箭炮的调炮有3种方式，包括分步调炮、操瞄调炮和随动调炮。其中分步调炮由人工输入高低和方位后按照调炮流程一步一步地进行；操瞄调炮是由人工输入装定方位和装定表尺后软件自动进行操瞄解算，然后将操瞄解算结果发送给火控计算机，火控计算机再转发给随动进行调炮；随动调炮是火控计算机将调炮参数发给随动进行调炮。调炮的一般流程如图4所示。

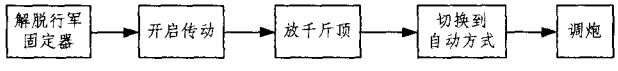

图4 调炮流程

分步收炮的一般流程如图5所示。

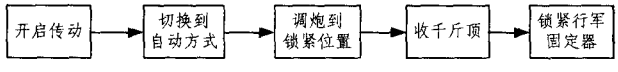

图5 收炮流程

1)操作流程安全性测试

从调炮收炮的流程可以看出，在调炮收炮过程中行军固定器和千斤顶是保证调炮收炮安全性的关键部件，因此必须在二者出现异常情况下对软件进行安全性测试，其测试设计如表4所列。

表4 调炮收炮操作流程安全性测试设计表

行军固定器 \ 千斤顶	下放过程中	下放到位	收起过程中	收起到位
解脱过程中	×	×	×	×
解脱到位	×	√	×	×
锁紧过程中	×	×	×	×
锁紧到位	×	×	×	×

2)调炮过程中出现断电

一般情况下，在调炮过程中，火控系统不允许断电，因此要测试在调炮过程中断电后软件的处理情况。

3)调炮边界安全性测试

调炮边界安全性测试是对高低方位处于边界或等于“0”、穿越“0”以及趋近于“0”时软件的处理情况进行测试。其安全性测试设计如表5、表6所列。

表5 调炮边界安全性测试设计表

	小于	等于	大于	最小值	最大值
高低下边界	×	√	√	——	——
高低上边界	√	√	×	——	——
方位下边界	×	√	√	——	——
方位上边界	√	√	×	——	——
高低方位组合	——	——	——	√	√

表6 调炮在“0”值附近的安全性测试设计表

高低/方位 \ 取值	−0.1mil	=0mil	0.1mil
高低	√	√	√
方位	√	√	√
高低方位组合	√	√	√

4)调炮方式切换安全性测试

为保证调炮安全，在调炮过程中不能随意切换调炮方式，其安全性测试设计如表7所列。

表7 调炮方式切换安全性测试设计表

调炮方式切换 \ 调炮过程中	分步调炮过程中	操瞄调炮过程中	随动调炮过程中
分步调炮	——	√	√
操瞄调炮	√	——	×
随动调炮	√	×	——

5)调炮误差安全性测试

在发送调炮指令后，火控计算机将调炮位置发送给随动系统，随动系统经过处理后将调炮位置返回给火控计算机。火控计算机对发送的调炮位置量与返回的调炮位置量进行对比，如果二者的误差在允许范围内则允许调炮，否则不允许调炮，这个误差要求非常严格，仅为0.1mil，因此必须进行安全性测试，设Δ=发送的调炮位置量−返回的调炮位置量，其安全性测试设计如表8所列。

表8 调炮误差安全性测试设计表

有效性 \ Δ	<−0.1	=−0.1	>−0.1	<0.1	=0.1	>0.1
是否能调炮	×	√	√	√	√	×

6)调炮过程中异常操作安全性测试

在调炮过程中，由于整个车体都承受着巨大的冲击，因此调炮过程中首先必须保持车体的平稳，另外要保证调炮精度，必须保证车体位置的准确性，因此其组合操作和异常操作是必须要进行测试的。

4.4 发射过程中的软件安全性

1)炮口查询的安全测试

炮口查询是非常重要的功能，通过炮口查询，确定整个发射时序的时间零点，如果时间零点错误，可能导致整个发射时序混乱，引起误发射。其安全性测试设计如下：

a)要对弹架分离信号的脉宽和幅度进行测试；

b)防抖动滤波处理测试，测试软件抗干扰滤波处理能力，要模拟出一定宽度和幅度的干扰信号进行测试；

c)对炮口查询的确认要有防虚报测试,需要软件多次确认,比如连续采集弹架分离信号多次,如果采集信号一致,则确认弹架分离成功。

2)发射方式安全性测试

远程多管火箭炮火控系统发射方式分为车内发射和车外发射,其安全性测试设计如下:

a)在发射准备工作完成之前,车内车外发射按钮都不能起作用;

b)两种发射方式互斥,在发射方式为车内时,车外发射按钮不起作用;在发射方式为车外时,车内发射按钮不起作用;

c)对发射方式按钮信号的处理要具备消抖能力,测试发射方式按钮信号为干扰信号时软件的处理能力。

3)引信安全性测试

引信作为弹药战斗部的起爆控制系统,它的安全性和可靠性对战斗部效能的发挥和人机安全性起着至关重要的作用。引信解保包括安保机构解保、安保机构充电和引信热电池激活3部分。其安全性测试设计策略如下:

a)要逐一对各个信号的脉宽、幅度和时序进行测试。包括安保机构解保信号、热电池检测信号、热电池激活信号;

b)防抖动滤波处理测试,测试软件抗干扰滤波处理能力,要模拟出一定宽度和幅度的干扰信号进行测试;

c)对各个信号的确认要有防虚报测试,需要软件多次确认,比如连续采集热电池激活信号多次,如果采集信号一致,则确认热电池激活成功。

4.5 其它安全性测试

1)要对与安全相关的关键信息的表示方式进行测试。要求关键信息必须采用多位、非全0或非全1的独特模式表示,比如弹种信号。

2)与安全相关的中断处理情况测试。为了防止软件出现异常,一般弹载计算机软件都具有看门狗功能,其测试设计如下:

a)喂狗时间测试,设T=规定的喂狗时间。

表9 喂狗时间安全性测试设计表

喂狗时间	<T	=T	>T
t	√	√	×

b)程序异常时,比如让程序跑飞时,进行测试。

3)要对通信过程中的可靠性和安全性进行测试。要求软件必须对帧头、字节长度、命令码、数据范围、校验和以及多字节或少字节的非法数据进行判断和处理。

4)要对与启动相关的关键信号的受控情况进行测试。要求受控于两个完全独立的输入控制,比如安保机构解保由两个独立的安全保险执行机构闭锁控制。

5)要对与安全相关的按钮的消抖能力进行测试。要求软件能够识别按钮由于抖动产生的干扰信号。

4.6 测试方法的有效性和充分性

以火控系统典型任务剖面为基础,分析每一个工作阶段软件存在及可能存在的安全隐患点,然后针对每个软件安全需求点,采取不同的测试策略或设计方法设计出安全性测试用例,解决了火控系统软件安全性测试"难""杂""多"问题。首先,以任务剖面为基础按阶段系统地去分析中每个操作的软件安全性,从系统操作本身出发,大大降低了仅仅依靠软件需求规格说明和测试人员工程经验来获取软件安全性的不确定性和不充分性,有效解决了火控系统软件安全性测试"杂"而"多"的问题,确保了测试的充分性。比如根据兵器软件评测中心实际测试来看,调炮范围与零位校正之间逻辑关系、对发射按钮的防抖滤波处理、炮口查询确认的防虚报需求等等在软件需求规格说明中根本没有体现,这时如果仅仅依靠测试人员工程经验,可能导致测试不充分;其次,针对每个安全点,文中都给出了具体的测试策略和设计方法,有效解决了火控系统软件安全性测试"难"问题。

影响本文安全性测试充分性的因素包括两点:一是火控系统软件组成发生变化,可能导致某些软件安全性需求发生变化;二是任务剖面和工作方式发生变化,可能导致遗漏某些软件安全性需求。

4.7 测试实验

统计兵器软件评测中心2005年至今所有火控系统软件测试情况,可知2011年以前,也就是在没有采用本文描述的方法之前,由于火控系统软件安全性需求的不明确、不系统,导致火控系统软件安全性测试主要依靠软件测试人员的工程经验,其问题主要体现在密码登录和通信处理等;从2011年以后,即采用基于任务剖面的分析方法后,火控系统软件安全性测试的广度和深度大幅提高,其软件安全性问题主要体现在安全条件的互锁处理、干扰的处理、工作流程的处理等方面,有效降低了火控系统软件的安全隐患。

结束语 综上所述,远程多管火箭炮火控系统软件安全性测试就是按照远程多管火箭炮典型任务剖面逐一分析、归纳和总结影响安全性的因素并加以测试的过程。同时借鉴其它火控系统软件测试中收集的各种安全性数据,发现远程多管火箭炮火控系统软件已存在或潜在的安全性问题并提出解决措施,为远程多管火箭炮火控系统的研制提供参考,从而在周而复始的、不断的测评-研制相互促进过程中提升远程多管火箭炮火控系统软件的安全性。

参 考 文 献

[1] 吕金和. 软件安全性测试研究[J]. 计算机安全,2010(8):48-52

[2] 王军,等. 某型多管火箭炮火控系统可靠性Nelson模型[J]. 火力与指挥控制,2007(10)

[3] 王雨时. 引信安全系统及安全性现状与发展对策[J]. 探测与控制学报,2008,30(6)

[4] 冯广斌. 远程火箭炮武器系统可靠性研究[D]. 南京:南京理工大学,2004

[5] 测试实验室和校准实验室通用要求的附加指南[S]. GJB2725B-2009. 北京:中国人民解放军总装备部技术管理中心,2009

[6] 火炮火控系统安全性试验方法[S]. GJB 2697-1996. 北京:科工委司令部,1996

[7] 许聚常,朱国庆,尹平,等. 军用软件测试指南[S]. GJB/Z141-2004. 北京:中国人民解放军总装备部,2004

[8] 软件可靠性和安全性设计准则[S]. GJB/Z 102-1997. 北京:航天工业总公司,1997