

防空武器系统软件可靠性定量分析方法研究

赵 勇 车建国 郭晓东

郑州防空兵学院火力控制工程系, 河南郑州 450052

摘要 针对防空武器系统软件可靠性特点, 主要从软件开发中的可靠性指标分配以及可靠性增长试验两个环节入手, 较为详细地阐述了对其实定量分析的方法, 为防空武器系统软件可靠性设计提供了定量分析的依据。

关键词 防空武器 软件 可靠性 定量 方法

Study On Quantitative Analysis Method Of Software Reliability for Aerial Defence Weapon System

Zhao Yong, Che Jian-guo, Guo Xiao-dong

Zhenzhou Air Defence Forces Academy, Zhenzhou 450052, China

Abstract: According to the characteristic of software reliability of aerial defence weapon system, the article mainly analyzes about the reliability distribution and its growth test, and expatiates on the quantitative analysis method, and provides quantitative analysis basis for the software reliability design of aerial defence weapon system.

Key words: Aerial Defence Weapon, Software, Reliability, Quantification, Method

0 引言

可靠性对于武器系统是非常重要的。战场环境下, 每一个小小的不可靠因素所带来的损失都可能是不可估量的。硬件如此, 软件也一样。航天飞机的飞行软件达 50 万行源代码, 而 F-22 战斗机的源代码竟然达到 150 多万行, 软件失效已成为系统瘫痪的主要原因。根据美国国防部和 NASA 的统计, 当今武器系统中的软件可靠性比硬件系统大约低一个数量级。因软件故障而造成的重大事故也不乏其例, 如 F-18 战斗机在海湾战争中, 飞行控制软件共发生了 500 多次故障, 爱国者导弹因软件问题误伤了 28 名美国士兵。由此可见, 软件可靠性在武器系统中的重要性。

1 防空武器系统软件可靠性分析

依据软件可靠性的定义, 可知防空武器系统软件的可靠性是指: 在规定的条件下, 规定的时间内软件完成赋予的特定功能, 不引起防空武器系统失效的概率。软件可靠性对于防空武器系统也是至关重要的。防空导弹以及高炮火控系统都必须在可靠软件的支持下才能充分发挥其应有的功能, 因此对防空武器的软件可靠性进行定量的研究显得非常重要。防空武器系统的软件种类比较多, 但往往最注重的是各种相关控制软件, 如导弹系统中测试软件、发射控制软件、导弹飞行控制软件的可靠性就对整个系统软件可靠度起决定性作用。若以上三种软件的可靠度分别为:

赵 勇: 郑州防空兵学院火力控制工程系在读硕士研究生, 研究方向: 防空兵技术装备作战运用。

E-mail: qingfengxzh2@vip.sina.com

R_C 、 R_L 、 R_F ，则系统整体的软件可靠度 R_S 为：

$$R_S = R_C \times R_L \times R_F$$

但对导弹软件可靠性的定量分析，却不能仅仅以这三种软件之间类似于串联的关系进行定量研究，软件可靠性的定量分析应该是在软件设计的各个阶段展开。在软件设计的各个阶段，除了软件设计方法的运用外，正确实施软件可靠性指标定量分配以及定量地研究软件可靠性增长试验，对软件可靠性的实现更显得更为重要。

2 软件可靠度定量分配方法

软件可靠性最明显的体现就是平均故障间隔时间 (MTBF) 的大小，也就是其失效率的大小。因此，在软件设计中，合理地确定软件的平均故障间隔时间以及相应各个部分的指标分配就是软件设计阶段定量分析重点探讨的问题。美国国际标准 ANSI/AIAA R-103-1992 中指出：软件最合理的失效率大约在 $10^{-3}/h$ 和 $10^{-4}/h$ 左右。另据统计，国外一般民用软件的 MTBF 一般在 $10^3 h$ 左右。因此，防空武器软件的 MTBF 应该在 1000h 到 10000h 之间是较为恰当的。

软件可靠性指标的分配随着对软件可靠性预计的进展要进行不断的调整和细化。传统的分配方法往往只能获取一个经验上的估计值，这一估计值对于软件设计初期有一定的效果。但随着软件的深入开发对软件建立必要的预测模型，通过预测模型对软件可靠性指标进行分配，并进行验证，则是一种更有效完成软件可靠性指标分配的定量分析方法。

预测模型通常可以由下式给出：

$$Y = A + \sum_{i=2}^9 (b_i \times x_i) \quad (1)$$

其中， $Y = \text{Log } N$ ， N ——预测的软件缺陷数；

A, b_i ——待定系数；

x_i ——影响软件的特定因素。

在防空武器系统软件开发过程中，经过对实际软件开发积累的数据以及软件运行的情况进行统计，可以获取在相应影响软件的特定因素下，软件出现缺陷情况的数据资料。对这些数据资料进行处理，采用最小二乘法对 (1) 式进行拟合，

就可以确定 A 和 b_i 。在现有的软件开发过程中，在影响软件的特定因素 (如表 1 所示) 确定以后，便可根据 (1) 式对本次开发软件潜在的缺陷数进行预测，然后采用相应的软件模型和必要的经验数据来初步确定软件的寿命曲线，这样对不同软件进行了缺陷数的确定，这些缺陷数就可以作为防空武器系统软件定量指标分配的依据。

表 1 影响软件的特定因素

序号	影响因素	具体取值定义
x_2	开发规模	用 KLOG (千行) 表示，不包括注释语言
x_3	评审程度	功能设计步骤评审程度=根据评审结果修改功能说明书次数/说明页数； 编码步骤的代码检查程度=通过代码检查修改程序的处数/程序的规模
x_4	改造差异	改造：-1；新开发：0；挪用 (或移植)：1。
x_5	开发工具语言	简易语言：-2；高级语言：-1；系统描述语言：0；宏汇编语言：1；汇编语言：2。
x_6	与操作系统的接口	无外部接口：-2；标准接口：1；接口多：0；复杂接口：1；新接口：2。
x_7	成员从事开发的时间	>8 年：-2；>4 年：-1；>2 年：0；>1 年：1；<1 年：2。
x_8	规格变更频率	基本没有：-2；少量：-1；偶尔：0；比较频繁：1；频繁：2。
x_9	消耗工作量的程度	实际消耗工作量/需要工作量

3 软件可靠性增长试验定量分析方法

软件可靠性增长试验是指在给定运行剖面下，做随机输入，对软件进行考核试验，使其暴露缺陷，进而分析缺陷，改正设计，并验证改进措施的有效性，以提高软件可靠性的实验方法。任何一个软件在开发过程中，其软件可靠性一般都在增长，但这种增长并不是可靠性增长试验。如白盒子测试可以使软件的可靠性得到增长，但却不是可靠性增长试验。在软件可靠性增长试验中，大量的增长试验模型成为对其进行定量分析的基本依据，通常有：Jelinski-Moranda 模型 (J-M) 模型、NHPP 模型、S-shaped 模型、Duane 模型以及由何国伟修改的 Schneidewind 模

型等。由于软件功能各式各样,软件的开发各有不同,因此在众多模型中,尚没有一种通用的模型。对于防空武器系统,在实际运用中,一般认为比较有效的模型是 J-M 模型或何国伟修改的 Schneidewind 模型。

J-M 模型是一种应用较早的软件可靠性增长试验模型,该模型的假设为:

1) 软件于 $t_1, t_2, \dots, t_n$ 时刻出现失效,出现失效后立即排除缺陷,因此在每发现一次失效后,软件的残余缺陷数就减少 1;

2) 每一个缺陷数对软件失效率的贡献相等,均为 λ_0 。

根据假设,可知在 (t_{i-1}, t_i) 时间范围内,软件失效率为常数 λ_i :

$$\lambda_i = \lambda_0 (N - i + 1)$$

其中, N ——软件开始测试时的缺陷总数。

设 $\delta_1, \delta_2, \dots, \delta_n$ ($\delta_i = t_i - t_{i-1}$) 表示相继出现的失效之间的时间区间样本。根据假设,可知在每两个失效之间,软件的寿命服从指数分布,该软件的概率密度函数为:

$$f_i(\delta_i) = \lambda_i e^{-\lambda_i \delta_i} = \lambda_0 (N - i + 1) e^{-\lambda_0 (N - i + 1) \delta_i}$$

采用极大似然法对 N 和 λ_0 进行点估计,其似然函数为:

$$L(N, \lambda_0) = \prod_{i=1}^n \lambda_0 (N - i + 1) e^{-\lambda_0 (N - i + 1) \delta_i}$$

将上两式分别对 N 和 λ_0 进行求导,并令其结果为 0, 得:

$$\begin{cases} \sum_{i=1}^n \frac{1}{N-i+1} - \sum_{i=1}^n \lambda_0 \delta_i = 0 \\ \frac{n}{\lambda_0} - \sum_{i=1}^n (N-i+1) \delta_i = 0 \end{cases}$$

由此方程组可解出 N 的似然估计量 $\hat{N}$ 满足:

$$\sum_{i=1}^n \frac{1}{\hat{N} - i + 1} = \frac{n}{\hat{N} - (\sum_{i=1}^n \delta_i)^{-1} \cdot \sum_{i=1}^n (i-1) \delta_i}$$

解出 λ_0 的似然估计量 $\hat{\lambda}_0$, 从而可以推出软件在 (t_{i-1}, t_i) 时间范围内的可靠度为:

$$R(t) = e^{-\hat{\lambda}_0 (\hat{N} - i + 1) \cdot (t_i - t_{i-1})}$$

在 J-M 模型中,其基本假设为“每一个缺陷对软件失效率的贡献相等”,这一点与现实是不符的。但由于在随机测试过程中,失效率高的缺陷一般先暴露,且相继暴露的缺陷在一定时间内差别不会太大,故在小型软件开发中,由于时间相对不长,且失效率不太多的情况下,该模型是完全适用的。然而,对于规模大、开发复杂的软件来讲,该模型就不能胜任了。在这一点上,何国伟修改的 Schneidewind 模型显现出了优势,原来的 Schneidewind 模型认为:当软件的故障率 $\lambda(t)$ 大时,缺陷易于暴露,因此 $d\lambda(t)/dt$ 应负得更多一些。基于此,该模型假设在不太长的时间区间内, $d\lambda(t)/dt = -\beta\lambda(t)$, 其解为 $\lambda(t) = \alpha e^{-\beta t}$ 。该模型把时间区间从 $t=0$ 起分为等长时间间隔,第 i 个区间的 $\lambda_i = \alpha e^{-\beta(i-1)\Delta t}$ ($i=1, 2, \dots, k$), 利用在第 i 个区间内发现并纠正的故障统计数,依据最大似然法求出模型参数估计 α 和 β , 于是在最后一个区间内即第 k 个区间的故障率 $\lambda_k = \alpha e^{-\beta(k-1)\Delta t}$ 。由于 Schneidewind 模型只利用到了每个时间区间内的错误发现并纠正的总统计数,而未利用到每一错误发现并纠正的具体时刻,因此原始统计数据的信息并未利用充分;而何国伟修改的 Schneidewind 模型在这一点上就充分利用每一错误发现并纠正的具体时刻信息,给出了一种新的软件可靠性增长模型。

该模型假设第 i 个错误被发现并纠正的时刻为 t_i ($i=1, 2, \dots, k$), 则类似 J-M 模型的推导方法,得到 α 和 β 的最大似然估计满足如下非线性方程组:

$$\begin{cases} \frac{k}{a} - \sum_{i=0}^{k-1} e^{-\beta t_i} (t_{i+1} - t_i) = 0 \\ -\sum_{i=0}^{k-1} t_i + a \sum_{i=0}^{k-1} t_i e^{-\beta t_i} (t_{i+1} - t_i) = 0 \end{cases} \quad (2)$$

于是在 t_k 时刻的故障率估计值为:

$$\lambda(t_k) = \alpha e^{-\beta t_k}$$

上述模型在具体运用中,需要对参数 α 和 β 进行数值确定。但由于方程组 (2) 的非线性很强,用诸如简单迭代法、牛顿迭代法等进行数值求解将遇到初值如何选取的问题;而用区间迭代法等具有全局收敛的方法进行数值求解,往往在

求解的速度和效率上将付出很大的代价,故一般性数值求解并非易事;并且对于方程组的解, β 小于 0 是无意义的。在这一点上,宋晓秋教授在其文章中 [2] 给出了有效的算法,运用其给出的算法,对参数 α 和 β 可以很高效地进行确定。

4 小结

作为近些年才发展起来的软件可靠性分配技术,在方法上还存在着一定的不足。本文的讨论仅仅考虑到了结构和开发过程等因素的制约,而对于费用因素没有单独考虑。在实际防空武器系统软件可靠性定量分配中,本文讨论的可靠性分配模型在具体运用上是较为成熟的;但从文中可以看出,该模型的使用必须是基于大量的统计数

字下进行的,在这一点上,该模型的运用受到了一定的限制。

软件可靠性增长试验相对于软件可靠性分配技术显然是成熟多了,可以运用的模型也相对较多。本文探讨的两种模型是众多模型中比较有代表性的模型,在具体运用中也比较有效。对于何国伟修改的 Schneidewind 模型,参考文献 [2] 以美国海军舰队计算机程序设计中心 (U.S.Navy Fleet Computer Programming Center) 的海军战术数据系统 NTDS (Naval Tactical Data System) 开发过程中的错误统计数据,以及装甲兵工程学院的某软件测试例子对其进行了检验,结果显示该模型的适用度是非常好的。

参考文献

- [1] 何国伟 主编. 软件可靠性 [M]. 国防工业出版社, 1998.
- [2] 宋晓秋. 软件可靠性修改的 Schneidewind 增长模型的特性分析[J]. 宇航学报, 1998 年, Vol.19, No.1. (2003-02-14 日收)

美国海军研究未来的战斧导弹战斗部

据《飞航导弹简讯》2003 年 9 月 26 日报导

继最近完成了两次动能贯穿战斗部演示飞行试验后,美国海军正为雷锡恩公司的战术战斧对陆攻击巡航导弹研究几种战斗部方案。192 枚战术战斧导弹的低速率初始生产正在进行中,首批导弹装备 450kg 爆炸/破片战斗部,定于 2004 年中期服役。美国海军计划首批采购 1350 枚导弹,但预计采购数量将增至 2000 多枚,以补充伊拉克战争后的库存,并能够研制替换战斗部。

据有关人士称,美国海军正在考虑战术战斧导弹下一步将如何发展,贯穿型是一种选择方案。正在考虑的其它战斗部方案有复合贯穿弹和爆炸/破片战斗部以及不同的弹药,如 BLU-97 复合效应集束炸弹和 BLU-108 传感器引爆武器。前两次贯穿试验的资金是作为先进概念技术演示项目而提供的,使用的是改进的 Block IV 导弹。到目前为止,这项计划已进行了两次研制试验和两次舰射作战试验,还计划进行两次作战试验,2003 年 7 月首次进行了潜艇垂直发射试验。作战评估将在 2003 年底进行,将包括 4 次发射试验,全速率生产的决定将在 2004 年作出。为美英海军规划的鱼雷管发射型的首次试验计划将在 2004 年底进行。