

变电站综合自动化系统的软件可靠性研究

刘洋¹, 罗毅¹, 易秀成², 涂光瑜¹, 陈维莉¹, 江伟¹

(1 华中科技大学电气与电子工程学院, 湖北 武汉 430074; 2 杭州易龙电气技术有限公司, 浙江 杭州 310000)

摘要: 提出在变电站综合自动化系统的软件开发中运用软件可靠性工程的理论, 以保证和提高软件系统的可靠性的观点。建立了基于改进的 JM 模型的变电站综合自动化系统软件可靠性模型, 改进模型在原有的 JM 模型基础上定义了故障消除概率, 从而克服了原模型对于排错过程估计过于乐观的不足。该模型可以根据软件测试中搜集的故障数据, 预测出软件系统可靠性增长的趋势, 从而得出软件可以达到的可靠性指标及达到该指标所需要的测试时间。算例说明了该模型的可行性与有效性。

关键词: 变电站综合自动化系统; 软件开发; 软件可靠性; JM 模型; 软件可靠性预测

中图分类号: TM76

文献标识码: A

文章编号: 1003-4897(2006)18-0031-04

0 引言

随着我国电力工业的发展, 对变电站的安全、经济运行的要求越来越高, 实现变电站综合自动化已经成为电力发展的趋势。当前, 计算机系统已被大量应用于变电站的运行与管理, 成为变电站综合自动化系统的核心, 其可靠性成为关系电网安全可靠运行的关键之一。尽管计算机系统的硬件复杂程度在逐渐增加, 但统计表明硬件可靠性随着硬件技术 (尤其是 VLSI) 的不断发展而得到很大提高。与此同时, 变电站综合自动化水平的提高极大地增加了软件开发的规模和复杂度, 软件故障逐渐成为实时系统发生灾难性事故的主要隐患。美加 8·14 大停电的调查报告证实 FE (First Energy) 的软件故障导致调度员对系统状态失去监视是事故的主要原因之一^[1]。因此在新形势下, 运用软件可靠性的理论来加强对变电站综合自动化系统 SAS (Substation Automation System) 的软件开发的管理, 成为减小这一安全隐患的有效途径。

软件可靠性的研究始于上世纪 70 年代, 现已在计算机、控制、航天、军事等领域得到较为广泛而深入的研究, 然而在电力系统中的研究尚处于起步阶段。文献 [2~4] 从不同的角度分析了软件可靠性研究在电力系统中的应用前景, 但是都只停留在定性的阶段, 没有阐明如何定量地对软件系统进行可靠性评估和预测。文献 [5] 认为应将软件作为构成电网调度自动化系统的设备之一, 并考核其可靠性水平, 文中介绍了软件可靠性模型和失效率的计算, 为进一步量化软件可靠性的评价和预测奠定了基础。软件测试是软件开发阶段的主要任务之一, 是

对设计和编码的质量的检测。大型的软件系统在运行之后一旦出错, 其损失将是巨大的, 因此在投运前必须进行大量测试和评估以确保软件的可靠。

本文针对软件开发阶段, 建立了基于改进的 JM 模型的变电站综合自动化系统软件可靠性模型, 预测出软件系统可靠性增长的曲线, 定量分析了软件可靠性的指标, 并通过算例证明了该模型在变电站综合自动化系统软件开发中的可行性与有效性。

1 软件可靠性

软件可靠性是软件质量的关键因素。1983 年美国 IEEE 计算机学会软件工程技术委员会将其定义为:

1) 在规定的条件下, 在规定的时间内, 软件不引起系统故障的概率。该概率是系统输入和系统使用的函数, 也是软件中存在的故障的函数。

2) 在规定的周期内, 在所述条件下程序执行要求的功能的能力。

其主要指标有: 软件中的初始故障数; 经测试排错后软件中的剩余故障数; 经预测得到的下一次故障的发生时间。

与硬件不同, 由于没有损耗, 软件不存在设备的浴盆曲线。绝大部分的软件可靠性模型属于软件可靠性增长模型 SRGM (Software Reliability Growth Model), 本文介绍的改进的 JM 模型也属于此范畴。SRGM 以软件运行和测试期间得到的故障数据为输入, 应用统计和随机过程的理论和方法, 对软件中剩余的缺陷数目进行评估, 并且预测软件在未来一段时间内可靠性增长情况。

2 变电站综合自动化系统的软件可靠性模型

2.1 SAS软件可靠性研究的必要性与可行性

较之常规的变电站自动化系统,变电站综合自动化系统的主要优越性体现在其借助通信,实现各个断路器间隔中的保护测控单元、变电站计算机系统、电网控制中心自动化系统之间的信息交换和信息共享,从而提高变电站运行的可靠性。可靠的通信一方面依赖于可靠的IED装置、计算机硬件、传输介质、接口设备、网络拓扑结构以及相关的抗干扰技术,另一方面依赖于实现各种功能的软件系统的可靠运行。衡量软件系统的质量需要相关的数学模型和指标,而软件可靠性模型恰好能满足这种需要,它能定性和定量地评价软件系统的可靠性,评价和预测可靠性走向,在软件产品的开发、运行和维护的各个阶段都能发挥其指导性作用。

本文具体针对软件开发阶段建立软件可靠性模型,为判断产品的质量达标与否提供理论依据。

2.2 JM模型介绍

JM模型(Jelinski and Moranda Model)是Z Jelinski和P. Moranda于1972年提出的,它把故障间隔时间看成一种随机过程,符合一定的分布,分布参数依赖于各间隔时间内程序中的残留故障数。模型基本假设如下:

1)软件中的初始故障个数为一个未知但固定的常数,用 N 表示。

2)故障一旦被查出即被完全排除,且不引入新的故障,于是每次排错之后, N 就减1。

3)任何时候的故障率都与软件中的故障剩余个数成正比,其单位故障率用 Φ 表示。

设 $t_1, t_2, \dots, t_n$ 表示相继出现的并被改正的故障之间的时间区间样本,则第 i 次故障发生的时间服从参数 $\Phi[N - (i - 1)]$ 的负指数分布,其故障密度函数可以表示为:

$$f(t_i) = \Phi[N - (i - 1)] \exp\{-\Phi[N - (i - 1)]t_i\} \quad (1)$$

该模型一直是学者研究的热点,如文献[6]研究了参数极大似然估计的存在性问题,并讨论了软件可靠性的置信限;文献[7]对JM模型做出了修改,假设不同的故障有不同的故障率并建立模型等。

2.3 一种适用于变电站综合自动化系统的软件可靠性模型

JM模型的数学表示简单,假设比较合乎直觉,

数据要求也较为简单。但是其假设2)不完善,因而缺乏广泛适用性。本文对假设2)做出修改,建立一个适用于变电站综合自动化系统的改进的JM可靠性模型。

2.3.1 故障消除概率的定义

在软件的开发和测试阶段,修改一处代码可能消除故障,也有可能引入新的故障。如果改正根故障可以消除很多故障,改正叶子故障只能消除一个故障;同样,引入一个根故障会引入多个故障,引入一个叶子故障会引入一个故障^[8]。于是,将故障的引入看作是负的消除数,那么软件故障消除数可当成随机变量,并假设它服从正态分布,则可以定义故障消除的概率密度:

$$p(x) = \frac{1}{\sqrt{2\pi}\theta} e^{-\frac{(x-\mu)^2}{2\theta^2}} \quad (-\alpha \leq x \leq \alpha) \quad (2)$$

其中: μ 为改正故障数的数学期望; δ 为改正故障数的方差。

当 $\mu > 0$ 时表示测试过程顺利,故障减少; $\mu < 0$ 时表示引入了新的故障,可靠性降低; $\mu = 0$ 表示改正无效,故障数不变。 μ, δ 的值可由测试记录数据用概率方法估算出。设 x_i 为每次改正的消除数。

$$\mu = \frac{1}{n} \sum_{i=1}^n x_i \quad \delta = \sqrt{\frac{1}{n} \sum_{i=1}^n (x_i - \mu)^2} \quad (3)$$

2.3.2 改进的JM模型

将假设2)改为:故障一旦查出即进行改正,每次改正后, $N - \mu$ 。根据假设,当第一个故障被排除以后,故障率就由 $N\Phi$ 变为 $(N - \mu)\Phi$,以此类推。代入式(1)就可得到改进的故障密度函数:

$$f(t_i) = \Phi[N - \mu_{i-1}(i-1)] \exp\{-\Phi[N - \mu_{i-1}(i-1)]t_i\} \quad (4)$$

获取一组观测值的似然函数可以表示成 $L = \prod f_i(t_i)$ 。两边取对数, $\ln L = \sum \ln f_i(t_i)$ 。于是JM模型可表示成为:

$$\ln L = \sum \ln\{\Phi[N - \mu_{i-1}(i-1)]\} - \sum_{i=1}^n \Phi[N - \mu_{i-1}(i-1)]t_i \quad (5)$$

令

$$\begin{cases} \frac{\partial \ln L}{\partial N} = 0 \\ \frac{\partial \ln L}{\partial \Phi} = 0 \end{cases}$$

整理得:

$$\left\{ \begin{aligned} \phi &= \frac{n}{N \sum_{i=1}^n \Delta t_i - \sum_{i=1}^n \mu_{i-1} (i-1) \cdot \Delta t} \\ \sum_{i=1}^n \left[\frac{1}{N - \mu_{i-1} (i-1)} \right] &= \frac{n \cdot \sum_{i=1}^n \Delta t_i}{N \cdot \sum_{i=1}^n \Delta t_i - \sum_{i=1}^n \mu_{i-1} (i-1) \cdot \Delta t_i} \end{aligned} \right. \quad (6)$$

其中: $\Delta t_i = t_i - t_{i-1}$, $t_0 = 0$ 。

从上式可以得出初始故障数 N 和单位故障率 ϕ 的最大似然估计值。

3 算例及分析

本文根据某变电站综合自动化系统软件的测试数据,利用基于改进的 JM 模型的软件可靠性模型预测出单位故障率,软件设计中存在的初始故障数及其查出时间。模型的仿真软件为 Matlab6.5,其算法流程如图 1 所示。其中,当前累积故障数表示到当前时间为止系统累积发生故障的次数;下一故障发生率为监测程序根据当前状况预测下一故障发生的概率;下一故障时间表示预测下一故障最有可能发生的时间;

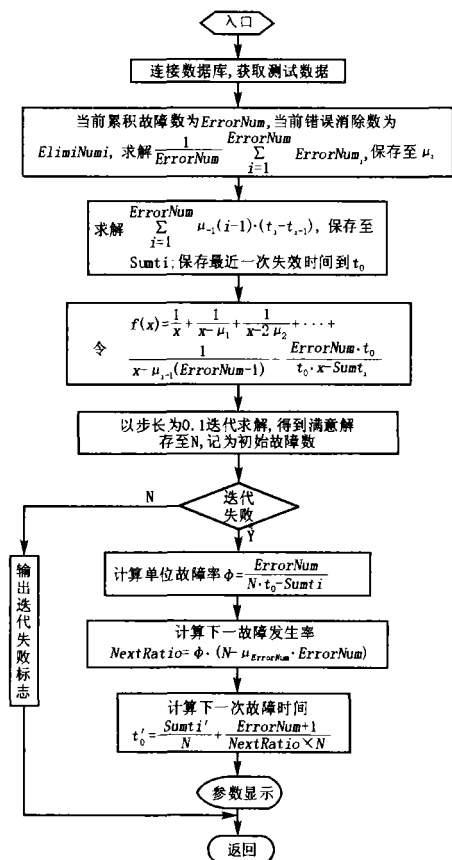


图 1 算法流程图

Fig 1 Flow chart of the algorithm

间;初始故障数为估计出的软件设计和编码中存在的原始故障个数。由于该模型的参数方程是非严格单调的,本文采用了步长为 0.1 的试探性数值求解法,以保证在较短时间内求得参数的满意解。

首先在系统测试过程中获得所需的数据,然后经过模型分析、计算,对某变电站综合自动化系统的测试结果,绘制出故障拟合及预测曲线图,见图 2。从图 2 中可以看出随着测试时间的增加,故障查出数量越来越多,曲线趋于饱和。测试终止后软件故障的更正工作很少,即认为软件的故障率将恒定不变。经过求解可以得到算例的初始故障数为 17,单位故障率为 0.009 4,最后一次故障查出时间为 360.510 6 天。

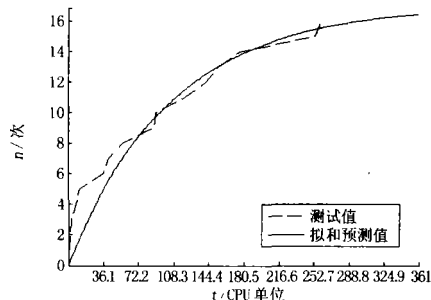


图 2 算例的故障拟合及预测曲线图

Fig 2 Curve of fault fitting and forecasting

通过对变电站综合自动化系统的软件可靠性的模型的研究,可以做以下工作:

a 对所开发的软件进行可靠性预测,并根据可靠性指标判断其是否能满足实际运行需要。实时系统的 CPU 为全天候工作,因此对于平均无故障时间 MTBF (Mean Time Between Failures) 的要求相对较高。根据变电站综合自动化系统的现场需求,应保证 MTBF 在 10 000 h 以上。算例得到单位故障率的极大似然估计为 0.009 4,表示当剩余故障数为 1 时,软件的故障率为 0.009 4。根据经典可靠性的理论可得 MTBF 为 106 383.0 天,共计 2 553.2 h,显然此时不满足现场需要,还需进一步纠错。当排除最后一个初始故障后,MTBF 将远大于 10 000 h,即表示测试 361 天后该软件满足现场运行的需求,可以投入市场。

b 可以利用该模型估算测试成本。其计算方法参考文献 [10]。在 t 时刻投放软件时期望的成本 - 收益函数为:

$$C(t) = \begin{cases} C_1 N \exp(-\phi t) + (C_4 - C_3 - B)(D - t) + (C_2 + C_5)t, & 0 \leq t \leq D \\ C_1 N \exp(-\phi t) + (C_2 + C_5)t + P(t), & t > D \end{cases}$$

其中: C_1 为投放每个错误的平均损失及修复成本, C_2 为执行每单位时间测试所花 CPU 时间的成本, C_3 表示软件已投放后人工所获收益, C_4 为每单位时间在应用中运行软件的成本, C_5 为测试期间每单位时间人工的成本。算例中估算出在测试阶段排除所有初始故障的成本为 103 950 元。

c 确定软件最佳投放时间,即将软件产品交付用户使用或投放市场的最佳时间。从实质上讲,测试终止时间和投放时间是一个问题,测试一旦终止,也就意味着产品可以投放市场了。结论 a 得到的是软件的可靠性指标, b 得到的是软件测试对软件开发总成本构成的影响。而最佳投放时间则是在综合考虑经济因素与可靠性指标的情况下确定的最优测试终止时间。其算法可以将 $MTBF \geq 10\ 000$ 作为成本-收益函数的一个约束条件,再求出 $\min\{C(t)\}$ 所对应的时间 t^* , 则 t^* 为最佳投放时间。由于在本算例中要满足可靠性指标就必须排除最后一个初始故障,所以软件最佳的投放时间为 361 天。

4 结语

针对目前电力系统对软件可靠性的研究相对薄弱的情况,本文对变电站综合自动化系统软件的开发测试阶段建立了软件可靠性模型并提出了相应的算法,提出的改进 JM 模型在原有 JM 模型的基础上引入了故障消除概率,从而克服了原模型对于排错过程估计过于乐观的不足。该算法能估计出软件初始故障数、单位故障率,并能预测出软件下一故障发生的概率及最可能出现的时间,为判断产品的质量达标与否提供理论依据。算例证实该软件可靠性模型的可行性和有效性。

参考文献:

- [1] 胡学浩. 美加联合电网大面积停电事故的反思与启示[J]. 电网技术, 2003, 27(9): 2-5
HU Xue-hao Rethinking and Enlightenment of Large Scope Blackout in Interconnected North America Power Grid[J]. Power System Technology, 2003, 27(9): 2-5
- [2] 徐立子. 变电站自动化系统的可靠性分析[J]. 电网技术, 2002, 26(8): 68-72.
XU Li-zi Reliability Analysis of Substation Automation System[J]. Power System Technology, 2002, 26(8): 68-72.
- [3] 所旭,张萍. 微机继电保护软件可靠性探讨[J]. 继电器, 2004, 32(12): 43-46
SUO Xu, ZHANG Ping Research on The Reliability of Digital Protective Relay Software [J]. Relay, 2004, 32(12): 43-46
- [4] 丁茂生,王钢,李晓华. 电网调度自动化系统可靠性研究(一)[A]. 电力系统及其自动化专业第二十一届学术对年会议论文集. 南宁: 2005. 19-25
DING Mao-sheng, WANG Gang, LI Xiao-hua Reliability of Digital Protective Relay Software [A]. Reliability Study on Energy Management System. Proceedings of 21th CUS-EPSS. Nanning: 2005. 19-25
- [5] 陈家鼎,张韧,吕波. JM 模型的统计推断[J]. 应用概率统计, 2001, 17: 403-409.
CHEN Jia-ding, ZHANG Ren, LÜ Bo Statistical Inference in JM Model[J]. Applied Probability and Statistics, 2001, 17: 403-409.
- [6] Ho Tsu-fens, Chan Wah-chun, Chung Chyan-gei A Quantum Modification to the Jelinski-Moranda Software Reliability Model[Z].
- [7] 方木云,屈玉贵,赵保华. 软件可靠性 JM 模型完全排错假设的修改[J]. 小型微型计算机系统, 2001, 22(2): 199-200
FANG Mu-yun, QU Yu-gui, ZHAO Bao-hua An Improvement on the Assumption of Thorough Faults-Removal in the JM Reliability Model [J]. MiniMicro System, 2001, 22(2): 199-200
- [8] 曾芳芳,孙建华,伍星,等. 监控系统的软件可靠性建模、度量与预测[J]. 计算机工程与应用, 2002
ZENG Fen-fang, SUN Jian-hua, WU Xing, et al Software Reliability Modeling, Measuring and Forecasting in Computer Supervisory System [J]. Computer Engineering and Application, 2002
- [9] 徐仁佐,等. 软件可靠性模型及应用[M]. 北京:清华大学出版社, 1994
XU Ren-zuo, et al Software Reliability Model and Application [M]. Beijing: Tsinghua University Press, 1994

收稿日期: 2006-04-03

作者简介:

刘洋(1982-),女,硕士研究生,研究方向为变电站综合自动化;E-mail: judith1130@tom.com

罗毅(1966-),男,副教授,从事 EMS 和 DMS 的研究;
易秀成(1965-),男,工程师,从事电力系统自动化技术的研究工作。

(下转第 51 页 continued on page 51)

收稿日期: 2006-02-10; 修回日期: 2006-06-14

现代电力电子技术及应用; E-mail: yb_wang@sdu.edu.cn

作者简介:

吕燕(1980-),女,硕士研究生,研究方向为现代电

王玉斌(1967-),男,副教授,博士生,主要研究方向为

电力电子技术及应用。

New precision detection method of harmonics and reactive current under asymmetrical three-phase voltages

WANG Yu-bin¹, LÜ Yan¹, LI Ying-jun²

(1. Shandong University, Jinan 250061, China; 2. Jinan University, Jinan 250022, China)

Abstract: Based on mathematical deduction and analysis, the problems are pointed out that concern the detection of harmonics and fundamental positive-sequence active & reactive current components with instantaneous reactive power theory under asymmetrical three-phase voltages. A new precision method to detect these current components is presented and analyzed by mathematical deduction in this paper. In this new method, an ideal fundamental symmetrical system, of which voltages are equal to the fundamental positive-sequence voltages of the original system, is constructed first, then harmonics and corresponding current components can be detected accurately. Simulation results show that the proposed method can accurately detect harmonics, active current and reactive current of fundamental when three-phase voltage is unbalanced and distorted.

Key words: instantaneous reactive power; harmonics; fundamental positive-sequence; reactive current; detection method

(上接第 17 页 continued from page 17)

Abstract: The configuration and setting of transformer protection is very important to ensure the safety of power equipment. This paper introduces the system connection and transformer protection configuration of 750 kV Guanting to Lanzhou Dong substation. The application principle on the configuration and setting of this 750 kV transformer protection is analysed and discussed in detail. The problem needing to regard is also discussed for others' reference. Since there are so much contradiction in the selectivity and sensitivity of transformer protection setting, the principle to ensure the safety of power equipment should be chiefly take into account in order to achieve a reasonable configuration and setting.

Key words: 750 kV; protection configuration; setting; transformer

(上接第 34 页 continued from page 34)

Studies on software reliability for substation automation system

LIU Yang¹, LUO Yi¹, YI Xiu-cheng², TU Guang-yu¹, CHEN Wei-li¹, Jiang Wei¹

(1. Huazhong University of Science and Technology, Wuhan 430074, China;

2. Hangzhou Yilong power Technology Corporation, Hangzhou 310000, China)

Abstract: The software fault is becoming one of the main reasons resulting in disasters in real-time system. To guarantee and improve the software reliability for substation automation system (SAS), it brings software reliability engineering to bear during the software development period. A software reliability model for substation automation system based on improved JM model is set up in this paper. Compared with the old JM model, it defines fault eliminating probability in the improved one, which makes the assumptions become more accordant with practice. It forecasts the reliability improving curve of the software system according to the fault data collected in the process of software test, and then concludes the reliable index that the software can achieve and the software test time to reach the reliable index. The computation results show the validity and efficiency of the method in the software development of substation automation system.

Key words: substation automation system; software development; software reliability; JM model; software reliability forecasting