第 30 卷第 9 期
2002 年 9 月

同 济 大 学 学 报
JOURNAL OF TONGJI UNIVERSITY

Vol. 30 No. 9
Sep. 2002

铁路车站计算机联锁软件的安全性评估策略

严 黎, 吴芳美

(同济大学沪西校区 安全软件测试评估研究所,上海 200331)

摘要: 安全控制系统的行为直接关系人身和大宗财产的安全,如何定量地反映系统中计算机软件的安全性品质是一个值得探讨的问题. 应从软件可靠性和安全性含义的讨论中,明确它们之间的区别. 在此基础上,提出一种能定量反映计算机联锁安全软件安全性的评估策略,最后论述了对某制式铁路车站计算机联锁安全软件进行分级测试后,利用 J - M 可靠性模型对其进行安全性定量分析的方法.

关键词: 安全软件; 可靠性; 安全性定量评估; 计算机联锁软件
中图分类号: U 283.2, U284.3 **文献标识码**: A **文章编号**: 0253 - 374X(2002)09 - 1116 - 05

Strategy of Safety Assessment for Computer Interlocking Software of Railway Station

YAN Li, WU Fang - mei

(Safety Related Software Test and Assessment Research Institute, Tongji University West Campus, Shanghai 200331, China)

Abstract: The behaviors of safety - critical control systems are often directly related to the safety of people life and some tall money. It is worth discussing how to reflect the safety quality of software embedded in computer systems. Then, difference between software reliability and safety is argued with the meanings of them defined. Based on the knowledge above, the strategy of safety quantitative assessment for computer interlocking software (CIS) of railway station is presented. Finally, based on testing for CIS of certain system, the method of safety quantitative analysis about it is given out in detail by making use of J - M reliability model.

Key words: safety - critical software; reliability; safety quantitative assessment; computer interlocking software

安全性苛求系统(safety - critical systems,以下简称安全系统)的安全控制和防护是计算机的一个非常重要的应用领域. 典型的安全系统有:铁路信号控制系统、飞机飞行控制系统和核电站安全保护系统等. 嵌入于安全性苛求系统中的软件常被称为安全性关键软件(safety - critical sofeware,以下简称安全软件),其根本特征就是以安全性为第一性能[1].

由于安全系统的失效可能带来灾难性的后果(人员伤亡和重大经济损失),因此安全软件的可靠性、安全性问题已引起人们极大的重视和关注. 现代计算机技术、通信技术、大规模集成器件技术的发展,为铁路安全控制和防护技术带来了革命性的变化. 对于铁路车站安全和防护控制系统(以下简称车站信号系统)而言,就是以计算机联锁控制系统(以下简称联锁系统)取代原有的继电联锁控制系统,这已经成为铁路车站信号控制系统技术发展的趋势,它顺应当代科学技术发展的潮流. 计算机联锁软件属于安全软件,它的

收稿日期: 2001 - 12 - 04
基金项目: 铁道部科技研究开发计划资助项目(2001X005;2000X018)
作者简介: 严 黎(1977 -),女,江苏苏州人,硕士生.

失效会造成人员伤亡和大宗财产的损失或生态环境的破坏,因此要求其具有很高的可靠性和安全性.

近几十年来发展起来并在军事、航空、航天领域里广泛采用的可靠性评估与测试技术为计算机联锁控制系统软件安全性测试评估打下了基础.本文作者依托铁路车站计算机联锁软件测试评估平台(以下简称测试平台),借助已有的软件可靠性、安全性评估工具,研究对计算机联锁安全软件具有针对性和实用性的安全性评估理论与实现方法.显然,对铁路安全控制软件安全性评估理论研究与方法的优化是软件检测工具开发的一项非常重要的工作,它的完成将大大提高测试质量,并对计算机参与控制的铁路信号设备或系统的设计、选型、鉴定、验收乃至维护等都具有重要的理论指导意义和实际使用价值.本文阐述的内容将是围绕着如何进行计算机联锁安全软件的安全性定量评估展开的.

1　安全软件的可靠性与安全性

安全软件作为一种涉及生命财产安危的软件,其质量的高要求毋庸质疑.澄清对其质量认识上的一些概念是必要的,软件的可靠性和安全性存在密不可分的联系.因而在软件可靠性与安全性设计中,有许多方法与基本要求是相同的,但两者的目标侧重点则有所不同.

首先从数学定义的角度对比两者定量测度之间的区别.可靠性的定量测度为可靠度,其定义为:设在时刻 t_0 系统正常运行,则系统在整个时间区间$[t_0, t]$内正常运行的条件概率称为系统在时刻 t 的可靠度,记为 $R(t)$[2].

安全性的定量测度为安全度,其定义为设在时刻 t_0 系统正常运行,则系统在时刻 t 的安全度 $S(t)$ 是指系统在整个时间区间$[t_0, t]$内正常运行的条件概率加上系统在时刻 t 处于失效安全状态的条件概率[2].

仅从数学定义的角度看,可靠度与安全度是不同的.安全度是两个条件概率之和,其中第一个条件概率就是可靠度.因此,一个可靠度高的系统,其安全度也必然高;反之,一个安全度高的系统,其可靠度未必一定高.

一个运行可靠的系统可以被认定为是一个安全系统,但在系统设计过程中,对于铁路信号这样一种效率和安全两方面均要顾及的系统来说,仅仅注重软件的可靠性还是不够的.铁路控制系统安全软件的安全性重要的特征是首先要遵循故障 - 安全原则,即系统在预定(功能)意图未能实现的情况下,要求系统维持在安全状态,或向安全状态转移的原则,即故障后自动导向安全的原则.严格地说,不具备故障 - 安全特性的软件便不能达到铁路控制安全软件的基本安全性需求.

事实上,软件本身存在着一个可靠性指标,即软件在给定输入后得到预期结果的能力.而对软件的安全性,则必须统观整个系统,注意软件在各种运行环境(包括特殊环境)中产生的响应[3].

2　计算机联锁软件安全性定量分析策略

2.1　联锁软件安全性完善度等级及其划分

根据软件测试结果对被测软件进行评估是一项十分重要的工作.由于软件测试很难做到完备,因此实现精确评估难度很大.为了解决这个问题,在联锁软件测试结果的评估过程中,提出了一个粗分级的测试评估策略,同时引进了安全软件完善度等级的概念.安全软件完善度等级的概念最早是由 IEC 61508 草案引入的,它主要应用于安全控制系统的安全性等级划分.软件的安全性完善度等级是表示软件所要求的安全性完善水平的一种定量指标,是将安全性完善度根据软件关键功能失效的频率和产生的危害严重程度划分成的等级[4,5].

联锁软件作为安全软件,在测试的基础上,为了进行分级定量评估,首先将联锁软件测试结果分为三大类别:

(1) 正确,即测试结果与需求规格说明或期望的属性相一致.

(2) 故障 - 安全,测试证明被测软件输出(结果)不正确,但与此同时能使系统维持在安全状态.

(3) 失效,软件产生了危险输出,使系统处于危险状态.

对于(2)、(3)类测试结果数据,按铁路安全性要求和失效后果的严重性及危险发生的频度,根据国内外相关标准,将软件的安全性完善等级划分为 4 级:

A 级 ——软件失效将造成人员伤亡和(或)大宗财产损失的严重后果,一般称之为灾难性的或致命性的后果;

B 级 ——软件失效将造成人员伤残和(或)一般财产损失,通常称之为关键性的或严重的后果;

C 级 ——软件失效将导致较小人身伤害或可治愈疾病或造成较小财产损失,一般称之为边缘性的事件或轻度后果事件;

D 级 ——软件失效仅导致轻微后果[6].

对于不同的软件安全性完善度等级,在进行设计时需要采取与其安全性完善度等级相应的技术措施.

2.2 联锁软件的安全性定量评估准则

为了避开传统安全性定量评估时既要考虑失效概率又要考虑危害程度的困难,针对同一级别危害程度的软件失效子集,建立相应级别的安全性概念[7]. 测试平台对铁路计算机联锁软件进行的测试属于黑箱测试,在对联锁软件基于测试的评估中建立可靠性、安全性分析模型所要考虑的主要因素有:相关的失效模式、失效检测的可用性及执行情况、各种可能的输入情况及分布、残留故障数等.

一个失效的危害严重度(hazard severity)指当该失效发生后,对软件安全性最不利影响的一种度量. 参照国内外标准可以得到失效危害严重度的一种典型定性度量,如表 1 所示[7].

表 1 分级的失效危害严重度

Tab. 1 Classified hazard serverity degree by failure

等 级	事 故 说 明
Ⅰ:灾难的	人员死亡或大宗财产损失或系统报废或使局面处于失控状态
Ⅱ:严重的	人员严重受伤、引起严重职业病或一定数额的财产损失或系统严重损坏
Ⅲ:轻度的	人员轻度受伤、轻度职业病或部分财产损失或系统轻度损坏
Ⅳ:轻微的	低于“Ⅲ”项危害严重性的损失

显然,这种失效危害严重度的等级划分并非一成不变. 随着软件应用领域的不同,可以通过吸收领域专家和实际经验进行适当调整和细化. 为了讨论的方便,本文假定软件失效全集是按表 1 进行危害严重度分级的.

设软件失效全集为 F,其中的灾难性失效子集为 $F_{\mathrm{Ⅰ}}$,严重性失效子集为 $F_{\mathrm{Ⅱ}}$,轻度的失效子集为 $F_{\mathrm{Ⅲ}}$,轻微的失效子集 $F_{\mathrm{Ⅳ}}$,那么 $F_{\mathrm{Ⅰ}}$, $F_{\mathrm{Ⅱ}}$, $F_{\mathrm{Ⅲ}}$和 $F_{\mathrm{Ⅳ}}$构成了 F 的划分. 根据失效危害严重度的概念,同一失效子集中所有失效的危害严重度级别相同.

分级的安全度是指软件运行时不出现该级别危害严重度的软件失效的概率. 根据表 1,软件失效可以分成四种危害严重度等级,软件失效集也划分成相应的四个子集,因此,分级的安全性实质上是一个由四个级别安全度参数组成的向量[7].

定义 1 在软件分级测试中,设 $t_{\mathrm{Ⅰ}}$, $t_{\mathrm{Ⅱ}}$, $t_{\mathrm{Ⅲ}}$和 $t_{\mathrm{Ⅳ}}$分别为各级经历的测试时间,则向量($t_{\mathrm{Ⅰ}}$, $t_{\mathrm{Ⅱ}}$, $t_{\mathrm{Ⅲ}}$, $t_{\mathrm{Ⅳ}}$)称为软件分级测试时间向量,记为 T.

设 x_{k1}, x_{k2}, …, x_{kn}表示第 k 等级相继出现的失效之间的时间区间样本,则第 k 等级的测试时间 $t_k = \sum_{j=0}^{n} x_{kj}$,式中 $k \in \{\mathrm{Ⅰ}, \mathrm{Ⅱ}, \mathrm{Ⅲ}, \mathrm{Ⅳ}\}$. 若 $n_{\mathrm{rc}k}$, $t_{\mathrm{m}k}$和 r_k 分别为联锁软件第 k 级可接受的最大残留故障数、最小平均失效时间和最大风险值,则计算机联锁软件分级安全性评估准则如定义 2.

定义 2 计算机联锁软件分级安全性评估准则:软件经过分级测试时间向量 T 后,各级必须满足下列三个标准:

(1) 残留故障数: $N_{\mathrm{R}k}(t_k) < n_{\mathrm{rc}k}$.

(2) 平均失效时间: $t_{\mathrm{MTTF}_k}(t_k) > t_{\mathrm{m}k}$.

(3) 风险 $R_{\mathrm{s}k}(t_k) \leq r_k$.

联锁软件的分级安全性评估准则可延伸到其它领域的安全软件的评估,根据具体应用领域情况选取其中几项作为评估准则.

定义 3　安全软件的分级风险准则:在分级测试的基础上,把安全软件各个失效后果严重度等级的风险减少到相应等级的一个可接受的水平.

需要指出的是,目前基于软件风险概念的定量分析有两种含义:①软件失效出现的概率(P_s);②软件失效出现的概率(P_s) ×失效危害度系数(H_s).

对于像铁路计算机联锁软件或航天飞机飞行控制器软件等安全软件来说,在进行风险分析时必须考虑失效可能导致的后果差别.若采用②的风险概念,在计算过程中对 H_s 的量化十分困难,人的主观因素起到了决定性的作用.因此,本文中对联锁软件的风险预测是建立在分级测试的基础上,采用风险概念①的表述,这样能避免对 H_s 量化的难点.失效分类后再加上风险准则,就寻求到一种定义 2 中标准(3)可操作途径.

2.3　利用 J - M 模型进行联锁软件的分级安全性定量分析

显然,由于同一失效子集中的失效具有相同的危害严重度,安全性定量评估时不必涉及危害严重度,因此,利用传统的可靠性模型及指标进行软件安全性的定量评估是可行的.

适用于单数据点的 J - M 模型要求被测软件的每一故障有相同的等级.但对于安全软件,各故障等级显然不同,人们更关注会产生后果严重的失效,因此无法由测试数据直接使用 J - M 模型进行参数估算.分级测试策略很好地解决了这一矛盾.

Jelinski 和 Moranda 在 1972 年给出了软件可靠性 J - M 模型.其基本思想是当前的故障率正比于残留故障数,在下一个故障被发现的时间段内故障率保持常数,每当一个故障被修改后(测试中重复出现的同一故障不累计),残留故障数就减去 1[3].

J - M 模型假设:设软件中初始故障总数为 N,单位时间故障发生率为 $<$.第 i 个缺陷发现的时刻为 t_i ($i = 1, 2, \cdots, n$),则在 $[t_{i-1}, t_i]$ 间的软件故障率为常数 $\lambda_i = <(N - i + 1)$,相继出现的失效之间的时间区间 $x_i = t_i - t_{i-1}, t_0, <$ 和 N 最大似然估计满足以下方程组[3]:

$$\begin{cases} < = \dfrac{n}{N\sum_{i=1}^{n} x_i - \sum_{i=1}^{n}(i-1)\,x_i} & (1) \\ \sum_{i=1}^{n}\dfrac{1}{(N-i+1)} = \dfrac{n\sum_{i=1}^{n} x_i}{N\sum_{i=1}^{n} x_i - \sum_{i=1}^{n}(i-1)\,x_i} & (2) \end{cases}$$

先由方程(2)解出 N 的估计值 $\hat{N}$,然后代入方程(1)中解出 $<$ 的估计值 $\hat{<}$.

方程(2)用牛顿法或简单迭代法求解都有一定困难.已有软件可靠性工作者对此方程进行了参数特性分析[8],利用已有的研究成果,在误差允许范围内,可求得适合的 $\hat{N}$ 值.

受铁道部委托,自 1998 年至今,安全软件测试评估研究室成功开发了联锁软件自动测试评估平台,此平台对十多个车站的多种计算机联锁系统进行了联锁软件的分级安全性测试,积累了足够多的测试数据和经验,为联锁软件的安全性评估打下了坚实的基础.

通过计算机联锁软件测试评估平台对某制式标准站的联锁软件进行测试,该软件在交付使用前,发现第 I 级失效数 2 个,第 II 级失效数 5 个,第 III 级失效数 12 个,第 IV 级失效数 7 个.下面以第 III 级的失效数及间隔时间(见表 2)为例,讨论联锁软件第 III 级的残留故障,其余各级的算法相同,不再重复叙述.

对于表中数据,很难直接从中找出内在的规律,利用 MATLAB 的图形功能可实现上述数据的可视化.图 1 为表 2 的数据曲线.在图 1 中横坐标为 i,纵坐标为时间轴,单位是 d.最后得出 $<= 0.021\,92$, $\hat{N} \approx 15$,亦即估计软件第 III 级共有 15 个故障,已发现 12 个故障,则此联锁软件的第 III 级残留故障:$N_{re} = \hat{N} - n = 3$.还可以推算出其它参数,此联锁软件第 III 级的可靠度为

$$R = \exp\{- <[\hat{N} - (i-1)\,x]\} = 0.930\,59$$

表 2 某制式联锁软件测试结果统计数据

Tab. 2 Statistic data of testing the computer interlocking software

序号 i	间隔时间 x_i/ d	累计时间 $\sum_{j=1}^{i} x_j$	J - M 最大似然法估计结果		
			$\hat{N}_i$	$\hat{\Phi}_i$	$\hat{t}_{\mathrm{MTTF}_i}$
1	4	4			
2	3	7	14.000	0.021 05	3.653 85
3	5	12	8.000	0.036 15	4.611 11
4	1	13	34.000	0.008 60	3.419 12
5	7	20	12.000	0.025 51	4.900 00
6	4	24	23.000	0.012 25	4.537 04
7	6	30	22.000	0.012 81	4.475 00
8	5	35	12.000	0.026 14	7.650 00
9	9	44	17.500	0.016 12	6.532 16
10	4	48	20.000	0.013 95	6.518 18
11	13	61	14.875	0.020 59	9.965 03
12	15	76	14.281	0.021 92	13.901 59

另外,利用J - M 模型进行安全性评估时,关键是估算软件初始故障总数 N 的值,其它参数都可由 N 推算得到. 由于测试中难免会参杂某些不确定因素,仅根据一轮测试数据估算出的残留故障数就决定某软件的安全性,这种方法不够完善. 在今后的评估工作中,还可采用回归测试结果数据. 使用这些数据的前提是:假设在排除前一轮测试发现的软件故障的过程中未引入新的故障. 估算出同一等级不同轮次的原始故障总数 N(或残留故障数 N_{re}),找出它的分布规律和发展趋势,得出回归测试后某一等级最终的残留故障数 N_{re},这时得出的 N_{re}比第一轮得出的将更切合实际的数值,从而提高了评估的可信性.

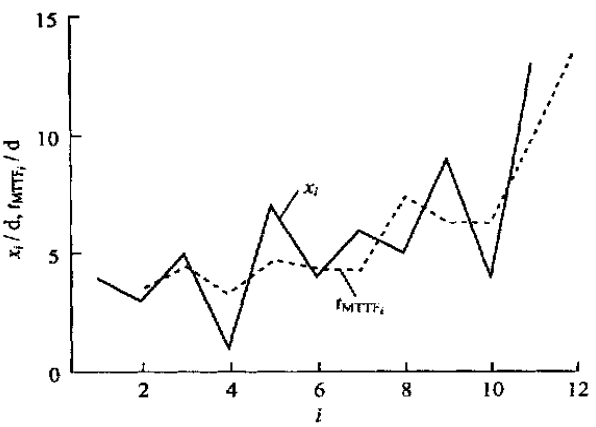

图 1 J - M 模型某组数据最大似然法结果

Fig. 1 Result with maxium likelihood method in J - M reliability model

3 结语

在软件的可靠性研究中已有软件残留故障的理论研究与实践成果,但在铁路控制的安全软件系统方面有关软件残留故障的较全面的理论研究与实践却很少. 对于计算机联锁软件系统的安全性度量估计及风险分析、预测的研究目前在国内尚属新的研究领域. 本文提出的计算机联锁安全软件安全性评估策略,通过分级测试避开了传统软件安全性定量评估的困难,并可充分利用软件可靠性的诸多成果,从而不仅提高了计算机联锁软件测试评估平台的测试质量,也给安全性分级定量评估提供了一种可行的方法,而且这种安全性评估策略在整个安全苛求系统领域具有广泛的应用价值.

参考文献:

[1] Goble W M. Control systems safety evaluation & reliability[M]. Second edition. [s.l.]:ISA,1998.

[2] 黄锡滋. 软件的可靠性与安全性[M]. 北京:科学出版社,1993.

[3] 郦 萌. 计算机软件的可靠性[M]. 北京:国防工业出版社,1998.

[4] STANDARD EN 50128 - 1994,Railway Applications:Software for Railway Control and Protection Systems[S].

[5] IEC 61508 - 1999,Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety - related Systems - Part 1:General Require2 ments and Part 3:Software Requirements[S].

[6] 吴芳美. 计算机联锁软件测试评估[J]. 铁路计算机应用,1999,1(1):26 - 133.

[7] 徐中伟,吴芳美. 基于测试的安全软件的安全性评估[J]. 计算机工程与科学,2001,23(5):94 - 96.

[8] 宋晓秋. 软件可靠性J - M 增长模型的特性分析[J]. 系统工程与电子技术,1997,19(9):44 - 46.