文章编号：1001-0920(2009)12-1873-04

冗余系统的生存能力分析与评估

鲍 鸣，戴跃伟，孔建寿，邹 云
（南京理工大学 自动化学院，南京 210094）

摘 要：立足于任务这个高层次的用户需求，通过对系统持续执行任务能力的参数分析，给出了应用美国工业界武器系统效能委员会(WSEIAC)提出的效能评估方法来分析和评价系统生存能力的方法.在此基础上，针对应用广泛的 k/N 热备份冗余结构，给出了具体系统生存能力的分析和评估方法.仿真实验表明，该分析方法有助于分析冗余技术对生存能力的影响，以便系统设计者合理应用冗余技术，在有限的资源下尽可能增强系统的生存能力.

关键词：生存能力；分析与评估；冗余系统
中图分类号：TP303.08 **文献标识码**：A

Survivability analysis and evaluation for redundant system

BAO Ming, *DAI Yue-wei*, *KONG Jian-shou*, *ZOU Yun*
(School of Automation, Nanjing University of Science and Technology, Nanjing 210094, China. Correspondent: BAO Ming, E-mail: bm_2001@163.com)

Abstract: Based on the tasks, the high-level user requirement, and by analyzing the parameter of the continued ability to carry out its tasks, the method of the analysis and evaluation of system survivability based on weapon system effectiveness industry advisory committee (WSEIAC) is presented. Based on this method hot standby redundant structure (k-out-of-N system) can be analyzed and evaluated in detail. The simulation shows that the analysis method is useful for system designers to make reasonable use of redundancy technology, and can improve the system survivability with limited resources.

Key words: Survivability; Analysis and evaluation; Redundant system

1 引 言

生存能力研究是传统安全性研究基础之上更高一层的考虑，是综合了系统安全性、可靠性、容错性等领域研究成果的系统研究的新方向.生存能力是指系统在遭受攻击、故障和偶然事故时还能及时完成其任务的能力[1].这种能力意味着系统可以遭受入侵，可以部分受损，但只要系统仍然能够保证所执行的关键任务按时完成，虽然其安全策略是失败了，但其生存策略却是成功的.因此，生存能力是一个非常重要的系统性能参数，可以作为系统在遭受攻击、软硬件故障等意外事故后对其运行性能优劣进行评价和判定的指标.系统设计者可以依据系统的生存能力的评判给出该系统相应的改进建议，以便在有限的资源下尽可能提高系统的生存能力，使系统可以顺利完成用户需求的任务.

自 Barnes 等[2]于 1993 年提出可生存性的概念以来，围绕提高系统可生存性以及构建可生存系统的研究已取得了很大进展.目前，提高系统的可生存能力有两种主要技术：主动响应技术[3-5]和冗余技术[6-9].主动响应，即利用入侵检测技术发现系统中的恶意入侵或随机故障并迅速修复受损部件.其主要依赖于检测系统的检测能力.采用主动响应的方法来提高系统生存能力，实际上是在原有系统的基础上披上了一层保护安全的“外套”，并不具有本质上的生存能力.而基于冗余的方法则是对原有系统进行重新设计，使之具有本质上的容忍入侵能力.因此，分析和评估系统冗余对生存能力的影响，有助于系统设计者合理应用冗余技术，在有限的系统资源下尽可能增强系统的生存能力.

2 基于 WSEIAC 的系统生存能力评估方法

根据 Ellison[1] 对生存能力的定义，生存能力考虑的是在整个任务期间系统持续执行用户任务的问

收稿日期：2009-01-08；**修回日期**：2009-04-17.
基金项目：国家自然科学基金项目(60574082).
作者简介：鲍鸣(1982—)，男，江苏无锡人，博士生，从事信息系统生存能力相关技术的研究；戴跃伟(1962—)，男，江苏镇江人，教授，博士生导师，从事信息安全相关技术等研究.

题.常用的任务持续能力参数主要有任务可靠性、可信度和任务效能等.

任务可靠性是系统在规定任务的过程中,执行其要求任务的各种关键功能的能力概率度量.对于不可维修系统,任务可靠度可以用来表示系统的任务持续能力.

可信性表示在任务开始时系统可用性给定的情况下,在规定的任务剖面内的任一随机时刻,能够使用且能完成规定功能的能力.可信性的度量称为可信度(D),其表达式为

$$D = R_M + (1 - R_M)M_0. \tag{1}$$

其中:R_M 为任务可靠度,M_0 为任务期间的维修度.

可信度 D 表示的是任务开始时系统处于可用状态,且在任务结束时系统也为可用状态的概率.可以看出,当任务期间不允许维修时,$D = R_M$,即任务可靠度与可信度相同,可直接采用任务可靠度作为任务持续能力的评价参数.

任务效能是指给定任务目标达到程度的概率度量,用于描述系统完成给定任务的能力.任务效能是任务开始时系统可用性、任务持续期间的可信性和能力度量的综合度量,是对整个任务期间系统持续执行用户任务的综合性、全面性指标.因此,可以采用美国工业界武器系统效能委员会(WSEIAC)提出的系统效能评估方法来评估分析系统的生存能力,其表达式为

$$S = A \times D \times C. \tag{2}$$

其中:A,D,C 分别表示系统的可用度、可信度和能力度量.

可用度 A:是系统备用程度的度量.可用度向量 $A = [a_1, a_2, \cdots, a_m]$,其中 $a_i (i = 1, 2, \cdots, m)$ 表示开始执行任务时,系统处于状态 i 的概率.

可信度 D:是在已知开始执行任务时系统状态的条件下,系统在执行任务过程中的某一时刻或某个阶段由于出现事件而形成的系统状态的量度.可信赖度 $D = [d_{ij}]_{m \times m}$,其中 $d_{ij}(t) (i = 1, 2, \cdots, m)$ 表示已知系统在开始工作时处于状态 i,在工作到 t 时刻时转移到状态 j 的概率.

可信度实际上是系统环境影响系统生存能力的必然结果.系统环境越恶劣,即遭受的攻击、故障和偶然事故越剧烈,则系统从高性能状态转移到低性能状态的可能性越大,时间也越短.

能力度量 C:是在已知系统执行任务期间的系统状态条件下,系统完成规定任务的能力量度.能力度量很好地将系统性能状态和完成任务结合起来,体现了任务和能力这对密切联系的要素.

利用 WSEIAC 效能评估方法分析和评价系统生存能力,可以很好地将系统性能和用户任务需求紧密地结合起来,综合考虑任务可靠性、可信度和任务效能等指标,使评估结果更加符合系统的真实状况.

3 基于冗余的系统生存能力分析

在众多冗余结构中,由于 k/N 热备份冗余结构的高可靠性和普适性,该类冗余结构被越来越多地应用到现代高科技装备中,例如航天飞行器、飞机、舰船、导弹等.因此,分析 k/N 热备份冗余结构对生存能力的影响,有助于系统设计者根据分析结果给出系统相应的改进建议,使系统可以顺利完成用户需求的任务.

根据基于 WSEIAC 的系统生存能力评估方法,需要对 k/N 热备份冗余结构的系统可用度、可信度和能力度量进行量化分析.

3.1 可用度 A

设系统中有 N 个相同部件,系统部件 $i (1 \leqslant i \leqslant N)$ 的可用度 A_i 可以用系统保障期间的平均故障间隔时间 MTBF 和平均故障修复时间 MTTR 来描述,即

$$A_i = \frac{\text{MTBF}}{\text{MTBF} + \text{MTTR}},\ 1 \leqslant i \leqslant N. \tag{3}$$

则 k/N 热备份冗余结构系统的可用性 A_S 可表示为

$$A_S = \sum_{j=k}^{N} C_N^j A_i^j (1 - A_i)^{N-j}. \tag{4}$$

因此,系统开始执行任务时处于可用状态的概率为 A_S,系统可用度矩阵为 $A = [A_S, 1 - A_S]$.

3.2 可信度 D

可信性描述的是系统工作周期内外部事件对系统的影响.设系统部件遭受攻击、故障和偶然事故时,失效时间均服从参数为 λ 的指数分布且相互独立.当部件出现故障时,使用人员立即用备件替换下来(若没有备件,则系统停止工作,任务失败),换下来的故障件交给修理人员进行维修.现有 c 个修理工,每个修理工同时只能修理一个故障部件,修复时间均服从参数为 μ 的指数分布且相互独立.修好后作为备件可重新使用,初始备件数量为 $N - k$.

将处于在修或待修状态的故障件数量作为系统状态,状态空间为:

状态 0:处于在修或待修状态的故障件数量为 0;

状态 1:处于在修或待修状态的故障件数量为 1;

$\vdots$

状态 $N - k + 1$:处于在修或待修状态的故障件数量为 $N - k + 1$,也是任务失败状态.

1）当 $N-k \geqslant c$ 时，由于只有 c 个修理工，当故障件数量小于等于 $N-k$ 并且大于等于 c 时，同时只能有 c 个故障件处于在修状态，此时的修复率为 $c\mu$；当故障件数量小于 c 时，所有故障件都处于在修状态；当故障件大于 $N-k$ 时，则说明可正常工作的部件数小于系统所需的工作部件数 k，此时任务失败，在状态转移图中可以认为此时的修复率为 0. 因此，$N-k+1$ 为任务失败的状态，此时修复率为 0. 于是可以得到系统状态转移图，如图 1 所示.

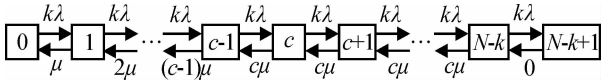

图 1　状态转移图

设 $f_{0,N-k+1}(t)$ 为系统从初始状态（失效部件数量等于 0）到任务失败状态（失效部件数量等于 $N-k+1$）时间（即首达时间）的概率密度函数，即

$$f_{0,N-k+1}(t)=\sum_{j=1}^{N-k+1}\frac{(k\lambda)^{N-k}}{\prod_{i=1,i\neq j}^{N-k+1}(x_i^{N-k+1}-x_j^{N-k+1})}\mathrm{e}^{-x_k^{(N-k+1)}t}. \tag{5}$$

其中：$x_i^{(N-k+1)}$，$x_j^{(N-k+1)}$ 为多项式 $M_{N-k+1}(x)$ 的零点；多项式 $M_{N-k+1}(x)$ 由下式的递推关系式确定：

$$\begin{aligned}&M_0(x)=1,\\&M_1(x)=x+k\lambda,\\&\vdots\\&M_{i+1}(x)=(x+k\lambda+i\mu)M_i(x)-\\&\qquad(k\lambda)(k_i)M_{i-1}(x).\end{aligned} \tag{6}$$

其中

$$k_i=\begin{cases}i\mu, & 1\leqslant i<c;\\ c\mu, & c\leqslant i\leqslant X.\end{cases}$$

因此，系统保持在可用状态的概率 P_A 就等于系统从初始状态（失效部件数量等于 0）到任务失败状态（失效部件数量等于 $N-k+1$）的时间大于系统要求的连续工作时间 T 的概率，故可得

$$P_A=1-P(t<T)=1-\int_0^T f_{0,N-k+1}(t)\mathrm{d}t=1-\int_0^T\sum_{j=1}^{N-k+1}\frac{(k\lambda)^{N-k}}{\sum_{i=1,i\neq j}^{N-k+1}(x_i^{(N-k+1)}-x_j^{(N-k+1)})}e^{-x_k^{(N-k+1)}t}\mathrm{d}t. \tag{7}$$

2）当 $N-k<c$ 时，系统正常工作过程不可能出现故障件数量大于 c 的情况，因此所有故障件都可以处于在修状态. 于是可以得到系统状态转移图，如图 2 所示.

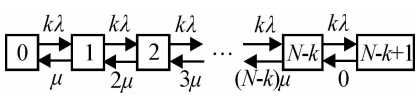

图 2　状态转移图

系统从初始状态（失效部件数量等于 0）到任务失败状态（失效部件数量等于 $N-k+1$）时间的概率密度函数 $f_{0,N-k+1}(t)$ 的计算公式为

$$f_{0,N-k+1}(t)=\sum_{j=1}^{N-k+1}\frac{(k\lambda)^{N-k}}{\prod_{i=1,i\neq j}^{N-k+1}(x_i^{(N-k+1)}-x_j^{(N-k+1)})}\mathrm{e}^{-x_k^{(N-k+1)}t}, \tag{8}$$

其中 $x_i^{(N-k+1)}$，$x_j^{(N-k+1)}$ 为多项式 $M_{N-k+1}(x)$ 的零点. 多项式 $M_{N-k+1}(x)$ 由下式递推确定：

$$\begin{aligned}&M_0(x)=1,\\&M_1(x)=x+N\lambda,\\&\vdots\\&M_{i+1}(x)=\\&(x+k\lambda+i\mu)M_i(x)-\\&(k\lambda)(i\mu)M_{i-1}(x).\end{aligned} \tag{9}$$

同理，根据式（7）可以得到系统保持在可用状态的概率 P_A. 再根据 P_A 的计算，可得到可信度矩阵

$$D=\begin{bmatrix}P_A & 1-P_A\\ 0 & 1\end{bmatrix}. \tag{10}$$

3.3　能力度量 C

系统能力度量 C 的计算是一项复杂的系统工程问题，涉及到系统的组成、性能和任务. 因此，应综合考虑影响系统生存能力的若干性能指标，采用品质效用函数的方法来获得系统的能力度量.

根据实际系统的性能、组成和任务，可以得到 m 个影响系统生存能力的性能指标 $Q=[q_1,q_2,\cdots,q_m]$. 这些性能指标对系统生存能力作用的重要程度并不完全相同，可用不同的指标权重来区分，设性能指标的权重为 $W=[w_1,w_2,\cdots,w_m]$. 借助模糊数学的方法，根据每个评估指标的特点，通过建立各项指标的隶属函数，可求得性能指标的隶属度 $\mu=[\mu_1,\mu_2,\cdots,\mu_m]$. 最后采用加权和法可以得到系统的能力度量

$$C=\sum_{i=1}^{m}w_i\times\mu_i.$$

4　实例分析

某 k/N 热备份冗余结构的系统需要有 4 个系统部件同时工作才能完成用户需求的任务，同时假设只要系统处于可用状态，系统便可完成用户任务，则处于可用状态时系统的能力度量为 1，处于不可用状态时系统的能力度量为 0. 表 1 给出了 3 组对照实验的系统参数，根据式（2）的计算可以得到各个时间段内系统的生存能力. 通过对系统生存能力的分析，有助于确定采用多少数量的冗余部件可以满足用户的实际需要.

表 1 对照实验参数表

实验	N	k	MTBF	MTTR	μ	λ	c
1	4	4					
2	6	4	200 h	50 h	0.2	0.1	2
3	7	4					

在实验 1 中，$N = 4$，即系统没采取任何冗余结构部件，只要系统部件一旦损坏，系统就处于无法工作的状态，因此其初始备用程度（可用性）相对较低，而且当受到攻击事件影响时，其生存能力变差的趋势也比较明显. 如图 3 所示，系统初始生存能力为 0.4，相对较低；工作 3 h 后，其生存能力接近于 0.1，即完成系统任务的概率已经很小，几乎不可能完成任务.

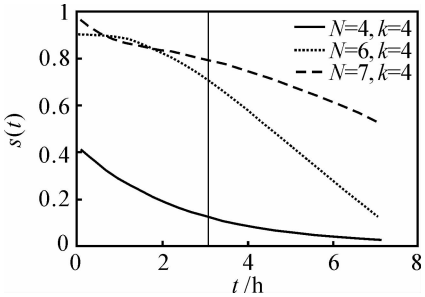

图 3 生存能力仿真曲线

在实验 2 中，$N = 6$，即系统采取了 2 个冗余部件的结构，因此其相对于实验 1 的系统初始备用程度要高一些；而且受到攻击事件的影响要相对小一些. 如图 3 所示，系统工作 3 h 内，其生存能力远远优于未采用冗余结构的系统，即完成系统任务的概率较大.

实验 3 中，$N = 7$，即系统采取了 3 个冗余部件的结构，因此其初始备用程度和受事件影响的变化程度均优于 2 个冗余部件结构的系统. 如图 3 所示，其初始生存能力优于采取 2 个冗余部件的结构，但优势不明显；系统工作 3 h 内，其生存能力随时间的变化趋势与只有 2 个冗余部件结构的系统差不多，稍微好些；但在 3 h 之后差别变大.

综上，如果用户只要求在 3 h 内的系统性能，则只需要采取 2 个冗余部件的结构即可；如果用户需要长时间的系统性能，则需要增加冗余部件的个数. 所以，基于 WSEIAC 的系统生存能力评估方法有助于系统设计者合理应用冗余技术，在有限的资源下尽可能增强系统生存能力.

5 结 论

生存能力研究是传统安全性研究基础之上更高一层的考虑，其考虑的是在整个任务期间系统作为一个整体持续执行用户任务的问题，而非其某些组件在恶劣环境下的生存能力. 本文通过对任务可靠性、可信度和任务效能等常用的任务持续能力参数的分析，提出了基于 WSEIAC 的系统生存能力评估方法，并针对应用广泛的 k/N 热备份冗余结构，给出了具体的生存能力的分析和评估方法. 仿真实验表明，该分析方法有助于分析冗余技术对生存能力的影响，有助于系统设计者合理应用冗余技术，在有限的资源下尽可能增强系统的生存能力.

参考文献（References）

[1] Ellison R, Fisher D, Linger R, et al. Survivable network systems: An emerging discipline [R]. Pittsburgh: Carnegie Mellon University, 1997.

[2] Hallway B A, Neumann P G. Survivable computer-communication systems: The problem working group recommendations[R]. Washington: US Army Research Laboratory, 1993.

[3] Fisher J, Linger R. Survivability: Protecting your critical systems[J]. Internet Computing, 1999, 3(6): 55-63.

[4] Knight J C, Sullivan K J, Matthew C. Survivability architectures: Issues and approaches [EB/OL]. http://www.cs. Virginia. edu/jck/publications/discex2000.

[5] 包秀国，蒋宗礼，张永. NTP 自主配置的自组织途径[J]. 计算机学报，2005，28(5)：759-766.
(Bao X G, Jiang Z L, Zhang Y. Self-organizing paradigm for NTP autonomous configuration [J]. Chinese J of Computers, 2005, 28(5): 759-766.)

[6] 赵国生，王慧强，王健. 一种基于自主配置的网络可生存性增强算法[J]. 武汉大学学报，2006，52(5)：582-586.
(Zhao G S, Wang H Q, Wang J. An improved algorithm for network survivability based on autonomous configuration[J]. J of Wuhan University, 2006, 52(5): 582-586.)

[7] Zhang Y G, Vin H, Alvisi L. Heterogeneous networking: A new survivability paradigm[C]. Proc of the 10th New Security Paradigms Workshop Cloudcroft. New Mexico, 2001: 3-39.

[8] 黄遵国，卢锡城，胡华平. 生存能力技术及其实现案例研究[J]. 通信学报，2004，25(7)：137-145.
(Huang Z G, Lu X C, Hu H P. The survivability technique and its implementation case study[J]. J of China Institute of Communications, 2004, 25(7): 137-145.)

[9] 蒋卫华，杜君，邹永彦. 可生存系统的分层冗余结构与实现[J]. 计算机工程与设计，2008，29(9)：2203-2206.
(Jiang W H, Du J, Zou Y Y. Survivable system based on heterogeneous redundancy[J]. Computer Engineering and Design, 2008, 29(9): 2203-2206.)