文章编号: 1001- 2486(2009) 02- 0099- 04

水下监测系统的生存性定义与模型*

周 睿, 乔纯捷, 王跃科
(国防科技大学 机电工程与自动化学院, 湖南 长沙 410073)

摘 要: 当水下监测系统遇到外部攻击、发生故障和事故时, 生存性为系统仍保证基本服务提供了保障。为准确衡量此类系统的生存性, 提出了它的生存性定义、计算方法和系统模型。生存性定义为在指定工作环境下, 受事件影响的系统服务仍能达到用户要求的能力, 表示为系统服务性能的数学期望。根据这种定义和计算方法能更准确地判别系统设计是否满足生存性标准。在基于多状态系统的生存性模型中, 服务性能是各子系统状态的函数, 与系统的结构函数有关。子系统状态的概率分布由系统的可靠性和安全性决定。最后通过实例说明了生存性模型的有效性。

关键词: 海洋监测; 生存性; 服务性能; 可靠性; 安全性
中图分类号: P715; TB114 文献标识码: A

Survivability Definition and Model for Underwater Monitoring System

ZHOU Rui, QIAO Chun-jie, WANG Yue-ke
(College of Mechatronics Engineering and Automation, National Univ. of Defense Technology, Changsha 410073, China)

Abstract: Survivability helps ensure that underwater monitoring systems provide essential services under conditions of attacks, failures, and accidents. To evaluate the survivability of such systems accurately, definition of survivability and its model is proposed in this paper. Survivability, the ability of a system to meet user's requirement of service when the system is affected by some events in a specified environment, and is computed by mathematical expectation of services performance. This method will have more precise result than others in judging whether system design achieves the criteria of survivability. To the survivability model based on multi-state system, service performance is the function of state of all subsystems, which is related to structure function of system. Probability distribution of subsystem's states is decided by reliability and security. In the end, an illustrative example is presented to prove the effective of the survivability model is presented in the end.

Key words: marine monitoring; survivability; service performance; reliability; security

本文研究的系统生存性问题主要针对海床基海洋环境监测系统平台(简称水下监测系统), 此类系统需要长期工作于海洋水下环境, 能够连续、实时地测量周围海域的多种环境参数, 包括海流剖面、温度等信息, 并具备一定抵御外部侵袭的能力。根据以往海洋监测设备的使用经验, 人为破坏、恶劣自然条件影响和内部故障是造成设备失效的主要原因。因此针对复杂多变的海洋环境, 需要对系统进行生存性研究, 以改善系统设计, 提高海床基海洋环境监测系统平台的使用效果。生存性最早的研究起始于海军舰船在遭受攻击后, 如何防止沉没以及如何挽救船员的生命。一战和二战时生存性研究逐步系统化, 并且转入航空领域, 此后扩展至多种武器装备。在重要的民用系统中也有应用, 例如通讯和电力供应系统[1-2]。目前网络信息系统成为生存性研究最为活跃的领域, 它主要解决网络入侵带来的问题[1-5]。

生存性强调了系统在遭受外部攻击、发生内部故障等情况时, 即使一些重要部件损坏, 仍然能够提供服务的特点[1-8]。它不仅在系统设计阶段根据用户需求提供生存性的设计建议, 而且在系统建成后可以对系统的生存状况进行评估和改进。因此, 很多重要系统在恶劣环境, 特别是战场环境工作时, 都

* 收稿日期: 2008- 06- 18
基金项目: 国家部委基金资助项目
作者简介: 周睿(1978—), 男, 博士生。

非常注重生存性的研究。

1 生存性定义

目前相关文献的研究表明,针对水下监测系统的研究往往集中在工程实现和可靠性研究上,并未从理论上研究此类系统的生存性问题。生存性与可靠性的区别、生存性的定义和计算,以及生存性模型一直是生存性研究的热点问题,但对生存性定义至今没有一个统一的标准[1]。系统具体应用特点不同是造成这种结果的主要原因之一。飞机生存性定义为:飞机在执行作战任务时,在不引起持久的削弱其完成指定任务能力的前提下,躲避和经受住人为敌对环境的能力[2]。在网络信息系统领域,Ellison 的生存性定义影响最大,被广泛引用。他的生存性定义为:系统在遭受攻击、发生故障或意外事故时,能够及时地完成其关键任务的能力[3-4]。Knight 对 Ellison 等的生存性定义进行分析后,认为这些定义还不够精确,缺乏判断标准,开发者无法根据这些定义准确判断某个设计是否满足用户需求,建议给出精确的适合应用研究的生存性标准,通过定量计算分析系统的生存性[2]。

为研究方便,现将外部攻击、发生内部故障和偶然事故等影响系统服务的事情均归类为事件。对于水下监测系统,在指定环境下提供满足用户要求的环境监测服务最重要,因此以事件影响下的服务能力来衡量生存性较为合理。并且系统的生存性与工作环境密切相关,不同环境下系统的生存性也会不同。综合现有的研究成果,生存性定义应当包含环境、用户、服务、事件、生存标准等要素,体现它们之间的关系。据此定义水下监测系统的生存性为:在指定工作环境下,受事件影响的系统服务仍能达到用户要求的能力。它包括服务性能、安全性和可靠性三个方面。安全性专指系统抵抗外部攻击的能力。因此,水下监测系统生存性可以说是一种广义的可靠性。下面介绍系统的生存性计算方法。

根据前面的生存性定义,在指定环境下系统的服务能力体现了生存性大小。首先分析系统服务数量与用户要求的关系。系统输出服务 S_E,在环境 E_N 中工作了时间 T,规定系统输出服务数量 $Q \geqslant Q_0$ 时(Q_0 为常数),系统在环境 E_N 中的生存性满足用户要求。已知系统服务性能为 g_k,且 $g_k \in [0, 1]$,最高服务性能为1。输出服务数量与服务性能和服务时间成正比,系统以服务性能 g_k 工作了时间 t_k 后,提供的服务数量为 $q_k = c \cdot g_k \cdot t_k$。$c$ 是服务性能和服务数量之间的比例系数,与系统具体特性有关。

系统在工作时间 T 内受安全性事件和可靠性事件的影响,可能会出现服务性能的变化,系统输出服务 S_E 的数量 Q 如式(1)所示。系统平均服务性能的计算如式(2)所示。重复这一过程 N 次,当 N 趋于无穷大时 t_k/T 就会接近服务性能 $G = g_k$ 的概率 p_k。由于 g_k 的数量和取值均有限,式(2)就转换为系统服务性能的数学期望,如(3)式所示。

$$Q = \sum_{k=0}^{K-1} q_k = c \sum_{k=0}^{K-1} g_k t_k \qquad \sum_{k=0}^{K-1} t_k = T \tag{1}$$

$$G = \sum_{k=0}^{K-1} g_k \frac{t_k}{T} \tag{2}$$

$$S = E(G) = \sum_{k=0}^{K-1} g_k p_k \tag{3}$$

即当系统服务性能的数学期望 $E(G) \geqslant G_0$(G_0 为常数)时,系统服务性能满足用户需求。这样系统在指定环境 E_N 中的生存性 S 量化为服务性能的数学期望,如式(3)所示。

传统的可靠性计算将服务性能 G 作为两个状态{0, 1},要求系统在规定条件下,$G = 1$ 的概率大于等于 P_0,即 $\Pr\{G = 1\} \geqslant P_0$。如图1所示,服务性能在AB线段上满足可靠性要求。如果将服务性能量化为多个等级(包含了服务降级使用),则根据文献[6-8]的生存性计算方法,当 $G \geqslant G_0$ 系统生存,生存性大小表示为 $\Pr\{G \geqslant G_0\}$,满足生存性要求的条件为 $Pr\{G \geqslant G_0\} \geqslant P_0$。服务性能的分布扩展至图1所示的单位矩形内,其中处于 $0 \leqslant G \leqslant G_0$, $0 \leqslant P \leqslant 1$ 矩形内的服务性能表示系统生存,当该区域服务性能的概率之和大于等于 P_0 时,系统性能满足生存性要求。这种计算方法不能准确表示系统提供服务数量的多少。

而以服务性能的数学期望计算生存性, 满足生存性要求的条件为 $E(G) \geqslant S_0$, 生存性标准 $S_0 = G_0 P_0$。该标准在图 1 中表示为通过(G_0, P_0) 点的双曲线 ECF, 服务性能的数学期望位于双曲线 ECF 上方时满足生存性要求。从满足文献[6– 8] 生存性标准的系统可得(4) 式。这意味着以服务性能的数学期望为生存性标准时, 如果 $S_0 \neq 0$, 文献[6 – 8] 的方法就有可能漏掉系统服务满足用户要求的设计。例如服务性能分布在 CFD 区域的系统就可能被认为没有达到文献[6– 8] 的生存性标准, 不满足用户要求。

$$\sum g_i p_i \geqslant G_0 \sum p_i \geqslant G_0 P_0 \quad g_i \geqslant G_0 \tag{4}$$

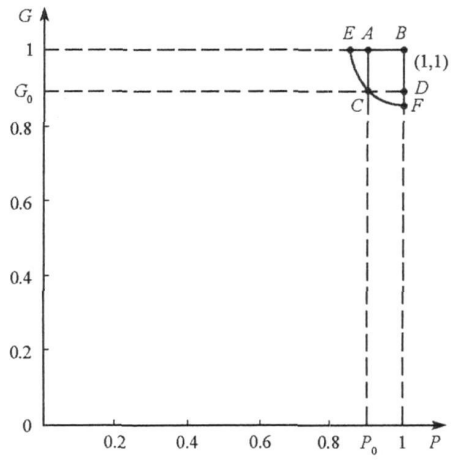

图 1　生存性标准

Fig. 1　Survivability criterion

2　生存性模型

从最简单的情况分析, 系统仅有两种状态{0, 1} , 提供一种基本服务, 性能等级为{0, 1} , 0 表示失效, 1 表示正常, 即系统正常状态时的服务性能正常。那么根据生存性的计算式, 只要知道服务性能正常时的概率就可以计算系统的生存性。服务性能正常概率由系统安全性和可靠性决定, 它们分别用安全概率和可靠度定量表示。如式(5) 所示, P_C 表示安全概率, P_R 表示可靠度, 由于 $G = 1$, 生存性在此处可理解为系统服务性能的生存概率。这是系统基本的生存性模型, 服务性能、可靠性和安全性是系统生存性模型的三要素。

$$S = \sum_{k=0}^{1} g_k p_k = P_C P_R G \tag{5}$$

模型进一步细化, 系统由 n 个子系统组成, 它们在系统结构和功能上相互独立。子系统的状态和系统结构决定了系统的服务性能。子系统状态和服务之间的关系可以利用系统的结构函数表示。系统结构函数表述如下: 系统由 n 个子系统组成。用 x_i 表示子系统 i 的状态, $x_i = 1$ 表示子系统 i 正常, $x_i = 0$ 为失效。记子系统的下标集为 $N = \{0, 1, \cdots, n-1\}$, 再记所有分量都只取 0, 1 值的向量 $\boldsymbol{x} = (x_0, \cdots, x_{n-1})$ 为子系统的状态向量。假定系统服务性能亦只有失效、正常两状态, 分别用 0, 1 表示, 再设系统服务性能完全由子系统的状态决定。对给定的状态向量 x, 用 $f(x)$ 表示系统的服务性能, 它是 $\{0,1\}^n \to \{0,1\}$ 上的一个函数, 称作系统的结构函数[9]。

这样利用结构函数$\{0,1\}^n \to \{0,1\}$表示水下监测系统中子系统状态和服务性能之间的关系。系统提供 3 项服务, 表示为 $S_E = \{s_{e0}, s_{e1}, s_{e2}\}$。整个系统结构如图 2 所示。“1”、“2”表示子系统标号。①、②表示保护层的标号, 保护层用来抵抗外部攻击。一旦被外部攻击摧毁, 就认为系统将会完全失效。(a) 图中系统工作在方式 1, 能够提供服务$\{s_{e0}, s_{e2}\}$, 整个系统处于保护层 1 的保护。方式 1 在工作周期 T 内的安全概率p_{c0}, 概率密度均匀分布。(b) 图表示系统工作在方式 2, 能够提供服务$\{s_{e0}, s_{e1}, s_{e2}\}$。系统受到保护层 1, 2 的保护。方式 2 在工作周期 T 内的安全概率$p_{c1}(p_{c0} < p_{c1})$, 概率密度均匀分布。子系统的可靠度分别为 p_{r0}, p_{r1}, 保护层 2 的可靠度为 p_{r2}。保护层 2 失效的情况下, 系统在工作方式 2 时的安全概率为 $p_{c2}(p_{c2} < p_{c1})$, 概率密度均匀分布。系统状态向量 $\boldsymbol{x} = \{x_0, x_1, x_2\}$, 分别表示子系统 1、2 和保护层 2 的状态, 由于子系统状态和服务均是{0, 1} , 因此采用布尔函数表示三种服务的服务性能, 如式(6) 所示。

$$\begin{cases} g_0 = f_0(x) = x_0 \\ g_1 = f_1(x) = x_0 \cdot x_1 \\ g_2 = f_2(x) = x_0 + x_0 \cdot x_1 \end{cases} \tag{6}$$

那么系统性能分布如表 1 所示。当服务性能为 0 时, 系统不具备生存性, 不考虑安全概率。t_1 表示在工作周期 T 内, 系统为提供服务在工作方式 1 所用的时间。t_2 表示在工作周期 T 内, 系统为提供服

务在工作方式2所用的时间,且 $T = t_1 + t_2$。系统三种服务性能的综合评定方法如式(7)所示,w_i 为各项服务性能的权重。根据式(3)计算系统的生存性,结果如式(8)所示。

表1 服务性能分布

Tab.1 Distribution of service performance

状态	服务性能	可靠度	安全概率
000	000	$(1-p_{r0})(1-p_{r1})(1-p_{r2})$	/
001	000	$(1-p_{r0})(1-p_{r1})p_{r2}$	/
010	000	$(1-p_{r0})p_{r1}(1-p_{r2})$	/
011	000	$(1-p_{r0})p_{r1}p_{r2}$	/
100	101	$p_{r0}(1-p_{r1})(1-p_{r2})$	p_{c0}
101	101	$p_{r0}(1-p_{r1})p_{r2}$	p_{c0}
110	111	$p_{r0}p_{r1}(1-p_{r2})$	$(t_1p_{c0}+t_2p_{c2})/T$
111	111	$p_{r0}p_{r1}p_{r2}$	$(t_1p_{c0}+t_2p_{c1})/T$

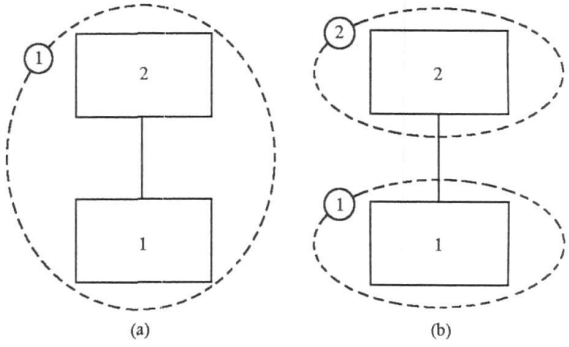

图2 (a)系统工作方式1,(b)系统工作方式2

Fig. 2 (a) Mode 1 of system working, (b) Mode 2 of system working

在表1中均按照系统具备的最大服务性能进行生存性计算,并未考虑生存策略的影响。例如系统在状态{1, 1, 0}时,采用不提供 s_{e_1} 的生存策略。结果虽然缺失了 s_{e_1},但提高了安全性,即提高了其它两种服务的生存概率。因此是否提供 s_{e1},需要根据两种生存策略下系统生存性的大小判断。随着外部环境的变化,采用的最优生存策略可能也会变化。

$$g_k = \sum_{i=0}^{2} w_i g_{ki}, \quad \sum_{i=0}^{2} w_i = 1 \tag{7}$$

$$\begin{aligned} S = E(G) &= \sum_{k=0}^{7} g_k p_k = \sum_{k=0}^{7} p_k \sum_{i=0}^{2} w_i g_{ki} \\ &= p_{r0}(1-p_{r1})p_{c0}(w_0+w_2) + p_{r0}p_{r1}(1-p_{r2})(t_1p_{c0}+t_2p_{c2})/T + p_{r0}p_{r1}p_{r2}(t_1p_{c0}+t_2p_{c1})/T \end{aligned} \tag{8}$$

3 结论

本文在现有生存性研究成果的基础上,结合水下监测系统的具体情况给出了生存性定义和模型。生存性定量表示为服务性能的数学期望,与用户对系统的要求基本一致。生存性与可靠性相比,研究范围更加广泛,服务性能、可靠性和安全性是本系统生存性研究的三要素。基于系统状态和结构函数的生存性模型,根据不同状态下的服务性能和概率分布计算系统生存性。模型包括子系统的可靠度和保护层的安全概率计算,并讨论了多种服务性能评估方法,对本系统的设计和评估提供了定量计算的依据。

今后还有一些问题需要进一步分析研究。例如文中给出的系统结构较为简单,子系统和服务性能的取值还可扩展至[0, 1]区间。生存策略还需要扩充到模型中。对于系统安全概率的计算还需要和具体工作环境结合,进一步分析它的计算方法。

参考文献:

[1] Westmark V R. A Definition for Information System Survivability[C]//Proceedings of the 37th Hawaii International Conference on System Sciences, Hawaii, 2004.

[2] Knight J C, Strunk E A, Sullivan K J. Toward a Rigorous Definition of Information System Survivability[C]//the DARPA Information Survivability Conference and Exposition, Washington DC, 2003.

[3] Ellision R J, Linger R C, et al. Survivable Network System Analysis: A Case Study[J]. IEEE Software, 1999, 7-8: 70-77.

[4] Ellision R J, Fisher D A, et al. Survivability: Protecting Your Critical Systems[J]. IEEE INTERNET COMPUTE, 1999, 11-12: 55-63.

[5] 黄遵国,卢锡城,胡华平. 可生存性技术及其实现框架研究[J]. 国防科技大学学报,2002,24(5): 29-32.

[6] Korczak E, Levitin G. Survivability of Series-parallel Systems with Multilevel Protection[J]. Reliability Engineering and System Safety, 2005, 90: 45-54.

[7] Korczak E, Levitin G. Survivability of Systems under Multiple Factor Impact[J]. Reliability Engineering and System Safety, 2007, 92: 269-274.

[8] Levitin G. Optimal Multilevel Protection in Series-parallel Systems[J]. Reliability Engineering and System Safety, 2003, 81: 93-102.

[9] 曹晋华,程侃. 可靠性数学引论[M]. 北京:高等教育出版社,2006.