doi: 10.7690/bgzdh.2014.11.013

基于故障树分析的网络系统可靠性研究

殷明勇，孔思淇，刘爱民，廖晓菊
（中国工程物理研究院计算机应用研究所，四川 绵阳 621900）

摘要：针对企业对业务连续性的需求，以及现有网络系统可靠性评价方式的缺陷，提出基于故障树分析的可靠性评估建模方法。对通用故障树的分析、构造方法进行简述，采用熵来反映网络系统的健康状况，并进行可靠性测试及模型迭代优化。结果表明：该方法同年度统计指标符合度较好，能真实地反映系统运维现状同运维目标的差距，辅助运维人员进行改良。

关键词：故障树；可靠性；业务连续性；网络系统；熵
中图分类号：TP393.02　　**文献标志码**：A

Reliability Research of Network System Based on Fault Tree Analysis

Yin Mingyong, Kong Siqi, Liu Aimin, Liao Xiaoju
(*Institute of Computer Application*, *China Academy of Engineering Physics*, *Mianyang* 621900)

Abstract: For the purpose of business continuity to company, as well as existing defects of network system reliability evaluation approach, propose a method of reliability assessment model which based on fault tree analysis. Briefly described the analysis and the structure method of general fault tree, used entropy to reflect the health of network system, and progressed reliability tested and model iteratively optimized. Result shows the method is close to operation statistical data, can reflect gap between system operation status and operation target, and this method can be used to help operation staff improving system.

Keywords: fault tree; reliability; business continuity; network system; entropy

0　引言

目前，规模较大的企业通常有独立的网络系统，包含基础网络、基础服务、应用服务等多类设备或服务。企业的业务连续性在很大程度上取决于其网络系统的可靠性[1]，但目前对网络系统可靠性的研究以基于网络拓扑的理论计算为主，如何把网络可靠性理论同实际运维保障工作结合起来进行可靠性估计，从而指导企业 IT 服务水平规划、管理是一个急需解决的问题[2]。所以，对网络系统可靠性的建模和分析逐步成为研究的重点。笔者针对网络系统可靠性的统计规律及理论特征，从故障树的角度对其可靠性进行建模和分析。

1　故障树分析方法

故障树分析(fault tree analysis)由贝尔实验室提出，是安全系统工程中最重要的分析方法，是故障事件在一定条件下的逻辑推理方法，最先用于民兵式导弹发射控制系统的可靠性分析。故障树主要用来表示灾害事故的各种因素间的因果关系，通过对系统风险进行分析，确定系统故障原因的各种组合方式及其发生概率，进而计算系统故障概率，并据此采取提高系统可靠性的措施。

2　故障树构造方法

故障树的构造分为以下几个步骤：

1) 完善系统拓扑：利用软件自动扫描出系统拓扑，补充未包含的关键元素，形成完整的系统拓扑图，直观展现影响业务系统可靠性元素和相互关系；

2) 故障信息采集和整理：对故障进行归类整理，按照各故障出现的原因，故障源组件进行整理，形成系统运行故障表，为故障树的构造提供输入；

3) 系统故障树构造：故障树构造重点针对所需的应用场景，对该可能发生的故障进行原因分析，建立故障树。

3　可靠性评估建模

系统可靠性分析是正确进行系统可靠性设计的前提，故障树分析法能够按要素分析系统的薄弱环节，指导运行和维修，实现系统设计的最优化。

可靠性一般用 MTTF(mean time to failure)表示，产品的 datasheet 中会提供该产品的 MTTF 标称值，但在实际中发现，该标称值同实际符合程度很低，如某厂商路由器的 MTTF 标称为十几年，实际却在 1 年内多次发生故障。另外，传统对产品故障率的分布假定-Weibull 分布[3]，即浴盆曲线，认为产品在早期和晚期的故障率较高，在中间期会处于一个相对稳定的状态，从数据统计看来，这个假定的置信度也较低，产品故障率分布并未出现明显平稳期。对于故障出现次数的泊松分布假设，数据表

收稿日期：2014-06-17；修回日期：2014-07-20
基金项目：中国工程物理研究院科学技术发展基金(2011B0403072)
作者简介：殷明勇(1983—)，男，陕西人，硕士，工程师，从事网络与信息安全、无线通信等领域研究。

明符合度也较低。

通过对系统的深入理解，笔者提出从故障控制角度进行分析。一个故障从发生到修复所经历的时间包括故障发现和报告、故障修复 2 个阶段。故障发现和报告决定于监控测量水平、管理成熟度；故障修复取决于技术能力和管理成熟度。可靠性的量化同实际拓扑的串、并联、冗余结构是相关的，但在计算时采用的不是传统的单个节点故障概率，而是故障时间的累积分析。

从故障控制的角度，产品的故障概率分析采用统计概率+行业口碑+环境因素+维保水平+使用年限相结合的方法。统计该类产品过去的故障率 P，再根据后面几个因素进行修正。对于没有出现过故障的产品，可采用其标称值为故障概率(可理解为一个无穷大值，出现首次故障后进行赋值)，如某产品每年故障次数平均为 1 次，每次故障时间 2 h，则故障率为 0.23%。统计数据有限，需要引入其他指标进行平滑。行业口碑即大量用户对各厂商产品可靠性的评价，是个定性指标，定义分为 3 级。以网络交换设备为例，某厂商设备为 1 级，在业界和实际使用中均具有较好口碑，部分厂商设备为 2 级，其他为 3 级，用 R 表示；环境因素采用跟机房标准相对应的数据，即信息系统机房 C 级、B 级、A 级，用 E 表示；维保水平按照是否购买专业服务、服务规格，分为 A、B、C 三级，用 M 表示。使用年限用 Y 表示，按规律分布如下：

第 1 年为 2，第 2 年为 1，第 3～6 年为 0.5，第 7 年以后为 1，每年增加 0.5。

则先验概率计算方法为：Prel=$P \cdot Y/(M \cdot R \cdot E)$ 100%。

对于每个故障，可通过客观评估了解其最坏情况，再通过管理可靠度模型求解评价故障时间，故障时间由故障最长发现时间(MDT)和故障最长修复时间(MRT)，某故障最长发现时间由最坏发现时间(WRT)与管理成熟度 ldm 有关，故障最坏修复时间(WRT)与管理成熟度和技术及备品备件能力 lrm 相关。管理成熟度遵照 CMMI 管理成熟度体系进行评价，5 个成熟度级别对应 0.1、0.3、0.5、0.7、0.9，该值可在实际管理过程中进一步制定评分细则进行修正，因此有：

$$\mathrm{MDT}=\mathrm{WDT} \cdot (1-\mathrm{ldm}) \tag{1}$$

$$\mathrm{MRT}=\mathrm{WRT} \cdot (1-\mathrm{lrm}) \tag{2}$$

假设系统由 n 个独立子系统组成，则系统损失时间熵 C_t 为：

$$C_\mathrm{t}=\sum_{i=1}^{i=n}(1-P_\mathrm{rel})(\mathrm{MRT}+\mathrm{MDT}) \tag{3}$$

定义 S_t 为 SLA 中规定的最大不可用时间，T 为可用时间指标要求，则可用率的偏移程度为

$$P_\mathrm{con}=(T-(C_\mathrm{t}-S_\mathrm{t}))/T \tag{4}$$

同理，如果 SLA 中定义的最大故障次数为 m，则可靠性指标的偏移程度为：

$$S_\mathrm{con}=\frac{m-P_\mathrm{R}T}{m} \tag{5}$$

通过可靠性指标可体现出当前运维状况，可通过反向分析了解关键影响。由于采用了熵来反映健康状况，熵平滑了因组件先验概率估算产生的误差。

4　可靠性测试及模型迭代优化

可靠性测试同应急演练类似，根据系统的故障树分解，模拟各个环节的错误，收集故障发现及报告时间、故障修复时间，进而可评估团队的运维水平；另一方面，完善各系统的故障信息收集工作，按照故障树分解体系进行故障信息存储，并更新可靠性先验概率和系统的可靠性值。

基于该模型进行了内部网运行可靠性指标的预测和分配，并组织了应急演练，获得了可靠性指标基础数据。2 年的实验结果表明，该模型指标预测同实际运维指标的一致性较好。

设备每次发生故障后，先验概率会得到更新；每次故障的发现和修复时间会影响到平均故障发现和修复时间，也会得到更新；随着设备使用年限的改变，在计算中也会得到反映，通过持续的模型迭代优化，系统会更能反映真实的可靠性水平。

5　结论

笔者在故障树分析和构造方法的基础上，提出基于故障树分析的系统可靠性建模方式，采用熵的形式反映系统健康状况，平滑先验概率的误差，为运维服务团队提供支持，真实地反映系统运维现状同运维目标的差距。实践结果表明，笔者提出的同运维保障工作相结合的可靠性评价方法同年度统计指标符合度较好。

参考文献：

[1] 李洪敏, 李宇明, 葛杨. 虚拟化数据中心的安全设计[J]. 兵工自动化, 2012, 31(8): 49-51.

[2] 孔思淇, 潘泽友, 王开云. NDN 安全机制初探[J]. 兵工自动化, 2013, 32(2): 40-44.

[3] 叶慈南. 完全样本情形下威布尔分布参数的估计[J]. 应用概率统计, 2003, 19(3): 257-266.