

基于 Z 语言和贝叶斯网络的存储系统 可靠性评估方法

王颖颖, 庄毅, 孙逸帆

(南京航空航天大学大学 计算机科学与技术学院, 南京 211106)

摘要: 现有的存储系统可靠性评估方法难以动态地描述其可靠性特征, 也难以反映其与时间的关系; 针对此问题, 提出了一种结合 Z 语言、连续时间马尔科夫链以及贝叶斯网络的可靠性评估方法; 该方法将存储系统抽象为两级, 分为功能单元和存储系统整体两部分; 在针对功能单元进行可靠性评估时, 建立了一种基于 Z 语言的可靠性模型, 由于其关于时间的状态转移符合 Markov 链的性质, 因此引入连续时间马尔科夫链进行评估; 为了更清晰地表达存储系统与各个功能单元之间的多状态关系, 构建了功能单元失效率与存储系统整体失效率之间的贝叶斯网络; 基于贝叶斯网络计算出存储系统的整体可靠性, 并得到其可靠性关键模块; 最后, 通过实例分析与计算表明, 基于提出的可靠性评估方法能够准确描述存储系统的状态转移, 可以量化计算存储系统的可靠性, 得到其可靠度, 具有一定的实用价值。

关键词: 存储系统; 可靠性评估; Z 语言; 连续时间马尔科夫链; 贝叶斯网络

Reliability Evaluation Method of Storage System Based on Z Language and Bayesian Network

WANG Yingying, ZHUANG Yi, SUN Yifan

(School of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics,
Nanjing 211106, China)

Abstract: The existing reliability evaluation methods of storage systems are difficult to describe its reliability characteristics dynamically, and it is also difficult to reflect its relationship with time. Aiming at this problem, a reliability evaluation method combining Z language, continuous-time Markov chain and Bayesian network is proposed. This method abstracts the storage system into two levels, which are divided into two parts, functional unit and storage system as a whole. When evaluating the reliability of functional units, a reliability model based on Z language is established. Since its state transition with respect to time conforms to the properties of the Markov chain, a continuous-time Markov chain is introduced for the evaluation. In order to express more clearly the multi-state relationship between the storage system and each functional unit, the functional unit failure rate and the Bayesian network between the overall failure rates of the storage system are constructed. The overall reliability of the storage system is calculated based on the Bayesian network, and the key reliability modules are obtained. Finally, the example analysis and calculation show that the proposed reliability evaluation method can accurately describe the state transition of the storage system, quantify the reliability of the storage system, and obtain its reliability, which has certain practical value.

Keywords: storage system; reliability evaluation; Z language; continuous-time Markov chain; Bayesian network

0 引言

存储系统是计算机中外存与 CPU 进行数据交换过程中的必不可少的部分之一。其主要作用是暂时存放在程序运

行过程中由 CPU 产生的运算数据, 以及其他与硬盘等外部存储器交换而产生的数据。由于物理结构原因, 存储系统只能将数据保持很短的时间。为了保持数据, 存储系统使用电容存储, 所以必须隔一段时间刷新一次, 如果存储单

收稿日期: 2022-01-29; 修回日期: 2022-02-24。

基金项目: 国家自然科学基金(61572253); 江苏省软件新技术与产业化协同创新中心计划(CXZZ13_0171)。

作者简介: 王颖颖(1996-), 女, 河南商丘人, 硕士, 硕士研究生, 主要从事软件工程、可靠性方向的研究。

通讯作者: 庄毅(1956-), 女, 江苏南京人, 教授, 博士生导师, 主要从事分布计算、可靠性方向的研究。

引用格式: 王颖颖, 庄毅, 孙逸帆. 基于 Z 语言和贝叶斯网络的存储系统可靠性评估方法[J]. 计算机测量与控制, 2022, 30(4): 249-257.

元没有被刷新, 存储的信息就会丢失。关机也会导致丢失数据。

传统的可靠性评估技术主要是可靠性框图、故障树、事件树等。可靠性框图^[1]通过使用可用于分析系统故障概率的图形来表示系统及其组件, 每个图形根据它们对系统的影响进行链接, 从而实现对系统的可靠性分析。故障树分析方法^[2-3]是通过描述部件与部件之间、部件与系统之间的逻辑关系来进行可靠性分析的, 其逻辑关系主要是通过逻辑门来表达。事件树分析方法^[4]是将系统的失效与导致失效发生的各种原因之间的逻辑关系用一种树形图的方式表示, 通过对事件树的定性定量分析, 找出事故发生的主要原因。后来, Markov 理论^[4,6]、GSPN^[7-8]等方法被用来研究动态特征。

虽然传统方法已经取得了不少成果, 但是随着硬件结构的日益复杂, 传统方法也越来越难以描述可靠性的动态特征, 也难以反映可靠性与时间的相关性。

本文的主要贡献如下: 该方法将存储系统简化为两级, 分为功能单元和存储系统整体两部分: 1) 在针对功能单元进行可靠性评估时, 本文建立了一种基于 Z 语言的可靠性模型。该模型能够很好的描述存储系统功能单元的硬件结构及其组成对功能单元可靠性的影响; 2) 本文提出了一种基于 CTMC 的可靠性评估方法对功能单元的可靠性进行评估, 该方法充分考虑可靠性与时间的相关性, 能够更准确的评估和分析功能单元的可靠性; 3) 针对存储系统整体的可靠性评估, 本文通过建立功能单元失效率与存储系统整体失效率之间的贝叶斯网络, 依据 CTMC 计算得到各功能单元的失效率利用标准贝叶斯推理计算存储系统整体的可靠性; 4) 通过贝叶斯网络的双向推理特性得到存储系统整体的可靠度, 同时识别出薄弱的功能单元, 对存储系统的可靠性评估有一定的参考作用。

1 相关工作

可靠性描述的是系统可以持续提供正确服务数据的能力。因此, 可靠性一直是存储系统相关研究的重点关注领域之一。对于存储系统的可靠性研究, 国内外学者针对不同类型的存储系统的可靠性^[9-15]都做出了许多努力。文献^[16]在对分布式存储器进行可靠性分析时考虑顺序事件的时间相关性, 提出了一种基于多值决策图的方法来定量评估, 而且该方法适用于故障、盗窃或损坏的随机时间遵循任意分布的系统; Ma^[17]等人为了更好地发掘 NANA flash 存储系统中块的耐用性提高提出了一种基于过程变化感知的方法 Block Hammer, 该方法考虑了过程变化和块相似, 可以主动预测发生故障的块, 大大提升了 NANA flash 的可靠性; 黄敏^[18]为解决 MLC NAND flash 存储系统的错误率高的问题, 提出了两种非对称访问的方法; 为解决系统使用寿命较低的问题, 提出了一种非并行调度策略及混合并行访问策略; Wang^[19]等人针对基于分块散布的多副本系统的可靠性提出了一个可靠性的分析模型, 通过合并副本的

丢失概率来研究其可靠性水平。

此外, 也有很多研究工作是通过对建模的方式来研究存储系统的可靠性。D. Fitch^[20]等人提出了一个使用分层着色 Petri 网的形式化模型, 引入了新的机制来提高系统的可靠性; 李静^[21]等人基于蒙特卡洛仿真算法对主动容错副本存储系统的可靠性进行了分析, 采用韦布分布函数模拟系统中设备故障和故障修复的时间分布, 定量评价了各种事件对存储器可靠性的影响。文献^[22]将 SMART 属性值视为时间序列数据, 使用隐马尔可夫模型 (HMM, hidden Markov model) 和隐半马尔可夫模型 (HSMM, hidden semi-Markov model) 来预测磁盘的故障, 结果表明在 Hughes 数据集上获得了 0 误报率和 52% 的准确率; Tan^[23]等人则是提出了一种基于树扩张的朴素贝叶斯方法来提高硬盘的故障预测准确率, 结果表明当误报率为 30% 时, 其检测率可达到 80%, 而当误报率为 0% 时, 其检测率只有 20%~30%。

近年来, 随着机器学习技术的发展, 已有不少国内外学者将其引入存储系统可靠性分析中。文献^[24]针对存储系统中的扇区错误, 通过分类和回归树 (CART, regression tree)、随机森林、支持向量机、神经网络和逻辑回归技术进行分析, 结果表明随机森林可以准确预测硬盘驱动器中的扇区错误; 文献^[25]通过使用机器学习技术对分布式存储系统中的磁盘故障进行检测, 但该方法的不足之处在于对于不同型号磁盘的故障检测的正确率是不同的; 庞帅^[26]等人提出了一种联合贝叶斯网络模型来预测其剩余寿命, 该模型结合了人工神经网络、进化神经网络、支持向量机和决策树 4 个分类器的预测结果来共同完成; Xu^[27]等人基于硬盘 SMART 属性的时序性特征通过采用递归神经网络 (RNN, recurrent neural network) 来建立硬盘的故障预测模型, 使得故障预测的准确率有了很大的提高。

综上所述: 对可靠性的研究一直是国内外研究者的热点问题, 无论是基于模型的方法还是基于机器学习技术的方法都在可靠性的研究领域取得了不少研究成果。但目前的研究中仍然存在难以动态地描述系统的可靠性特征, 也难以反映其可靠性与时间的关系等问题, 针对此问题, 本文提出了一个基于 Z 语言和贝叶斯网络的可靠性模型, 其中 Z 语言可以对存储系统中的可靠性属性进行建模, 并具有强大的数据约束能力和可扩展能力; 贝叶斯网络可以清晰地描述系统的多状态关系, 使系统可靠性的评估计算更加简单。

2 存储系统结构分析

为了准确地对存储系统 (MS, memory system) 的可靠性进行建模, 本文将 MS 划分为不同的功能单元 (MFU, functional unit of memory), 包括存储模块、数据寄存器、地址寄存器和内存控制器共 4 个功能单元。其中, 存储模块 (SM, storage module) 是内存中负责存储数据的模块, 当存储模块发生翻转导致软错误的时候, 数据发生变化,

引发内存故障; 数据寄存器 (MER, memory data register) 是计算机控制单元中的寄存器, 寄存了将要写入到计算机主存储器的数据, 或由计算机主存储器读取后的数据。当数据寄存器发生翻转导致软错误时, 其中所转存的数据改变, 造成存储系统故障; 地址寄存器 (MAR, memory address register) 是用来保存当前 CPU 所访问的内存单元的地址。因此, 如果地址寄存器发生单位翻转时, 会使访问的内存地址发生改变, 引发数据错读, 造成存储系统故障; 内存控制器 (MC, memory controller) 主要是用来控制内存工作, 并控制内存与 CPU 之间进行数据交换。当内存控制器发生软错误时, 也会引发存储系统故障。

其次, 不同的功能单元也是由不同的组件构成, 以存储模块为例, 存储模块又可以分为存储体 (BA, bank)、地址译码器 (AD, address decoder)、行缓冲区 (RB, row buffer) 三个组件。存储体是由若干个存储单元组成, 当存储数据库中的存储单元发生翻转时, 所存数据发生改变, 造成存储模块故障。地址译码器又分为行译码器和列译码器, 行译码器负责输出行地址选择信号, 列译码器负责输出列地址选择信号; 当地址译码器输出信号错误时, 将访问错误的内存地址。行缓冲区主要负责将读出的行内容暂存, 等待列位址送到后输出正确的位元, 以及判断存储的内容是 0 还是 1。当行缓冲区里的存储单元发生翻转时, 也将造成存储模块故障。

因此, 从底层硬件和 MFU 出发对存储系统进行可靠性评估, 能够从本质上对存储系统进行可靠性建模与分析。

根据对 MS 体系结构的分析和抽象, 本文可以得到一个简单的 MS 抽象模型, 如图 1 所示。

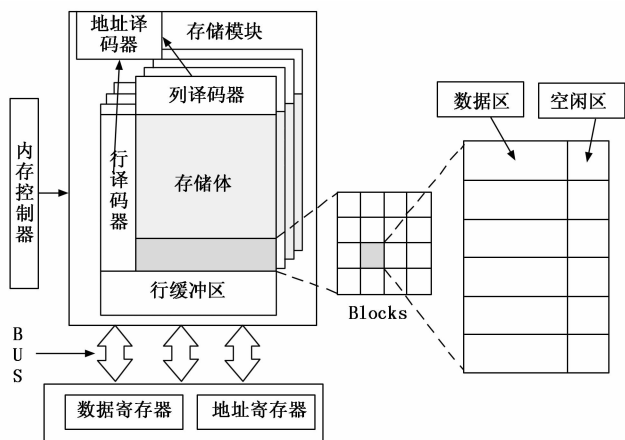


图 1 存储系统抽象结构图

针对该抽象结构, 本文给出了 MFU 以及 MS 的形式化定义如定义 1 和定义 2 所示。

定义 1: 以 MS 的存储单元 SU 为例, 其形式化定义可以用式 (1) 所示的一个三元组表示, 其中每个元素表示组成该 MFU 的一个组件。

$$SU = \{BA, AD, RB\} \quad (1)$$

其中: BA 表示组成 SU 的存储体, AD 表示组成 SU 中的地址译码器, RB 表示组成 SU 的行缓冲器。

定义 2: MS 可用如式 (2) 所示的三元组表示。其中, MFUs 表示构成 MS 的功能单元的集合, BUS 表示各个功能单元的连接总线。

$$MS = \{MFUs, BUS\} \quad (2)$$

从式 (2) 可以得到, 存储系统主要是由不同的功能单元 MFU 共同构成的, 而且也可以把总线看成是一个特殊的功能单元。所以, 针对存储系统可靠性的研究就可以从包含的功能单元出发, 而且研究其功能单元的可靠性能够从本质上对存储系统进行可靠性分析。

3 存储系统可靠性分析方法

3.1 存储系统可靠性建模与评估框架

本文设计的存储系统可靠性建模与评估框架设计如图 2 示。该框架主要分为 3 个阶段: 初始化阶段、MFU 可靠性评估阶段以及整体可靠性评估阶段。

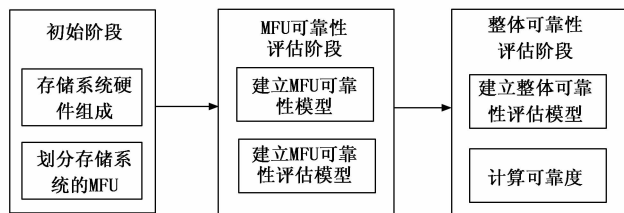


图 2 存储系统可靠性建模与评估框架

初始化阶段: 初始化阶段主要是在进行可靠性分析之前对存储系统的硬件组成进行分析, 并根据不同的功能把存储系统划分为不同的功能单元。

MFU 可靠性评估阶段: 该阶段是在划分的功能单元的基础上, 分别对划分的每个功能单元进行可靠性评估。提取不同功能单元中与可靠性相关的约束, 基于 Z 语言建立功能单元的可靠性模型。在可靠性模型的基础上, 基于相应的转换规则确定评估模型中的状态空间、转移概率等相关参数, 通过计算得到各功能单元的可靠度。

整体可靠性评估阶段: 该阶段是在得到各个功能单元的可靠度的基础上, 对存储系统整体进行可靠性评估。基于贝叶斯网络建立描述功能单元与系统整体失效率之间的可靠性模型。基于贝叶斯网络对系统进行可靠性计算, 并推理出系统的可靠性关键模块。

3.2 功能单元的可靠性评估

功能单元的可靠性评估过程主要分两步, 首先需要建立功能单元的可靠性模型, 其次根据相应的转换规则将建立的可靠性模型转换成相应的评估模型, 最后基于建立的评估模对功能单元的可靠性进行可靠性评估。

3.2.1 功能单元可靠性模型 Z-FURM

Z 语言是一种形式规格说明语言, 在精确描述系统状态与操作方面具有很大的优势^[26]。此外, Z 语言还具有支持可扩展、建模形式呈现模块化等优点。并且, 随着 Z 语言

的日益被重视,使得 Z 语言将拥有更加广泛的适用范围和更强、更规范、更简洁的描述能力。因此,这也是本文采用该语言作为建模语言的原因。

功能单元可靠性模型 (Z-FURM, functional unit reliability model based on Z language) 是通过使用 Z 语言将构成功能单元的元器件的可靠性元素与功能单元的可靠性相关联,将这两个层级融合到一起,使得功能单元的可靠性模型更清晰和简洁,能够更准确对可靠性进行描述。其中,单个功能单元的可靠性模型 Z-FURM 的定义如定义 3 所示。定义 3 详细描述了构成功能单元可靠性模型的要素。具体定义如下:

定义 3: Z-FURM 模型可以表示为一个如式 (3) 所示的三元组:

$$Z\text{-FURM} = (\text{FRate}, \text{States}, \text{STR}) \quad (3)$$

式 (3) 中, FRate (failure rate) 表示 MFU 的失效率, States 表示 MFU 的状态空间,包含系统中功能单元的所有可能状态; STR (state transfer relationship) 表示功能单元的所有状态之间存在的所有状态转移关系。本文将无法使用软件方法恢复的状态称之为失效状态 Failure State。失效状态可以通过系统重启等方式恢复。

1) 失效率 (FRate):

一个 MFU 通常也是由不同的模块构成,以存储单元 MEM 为例。根据定义 3 可知, SU 是由存储体 BA、地址译码器 AD 和行缓冲器 RB 组成。假设组成 SU 中的任意一个组件发生故障都会引起 SU 功能的失效,这些组件的失效率分别为 λ_{BA} 、 λ_{AD} 、 λ_{RB} ,则该功能单元的失效率 λ_{SU} 可表示为式 (4):

$$\lambda_{SU} = 1 - (1 - \lambda_{BA}) * (1 - \lambda_{AD}) * (1 - \lambda_{RB}) \quad (4)$$

Z 语言描述存储单元 MEM 的失效率如下:

<HFMName>FRate

BA_FRate: \mathbb{R}

AD_FRate: \mathbb{R}

RB_FRate: \mathbb{R}

SU_FRate: \mathbb{R}

$$SU_FRate = 1 - (1 - BA_FRate) * (1 - AD_FRate) * (1 - RB_FRate)$$

其中: BA_FRate、AD_FRate、RB_FRate 分别表示 λ_{BA} 、 λ_{AD} 、 λ_{RB} , SU_FRate 则表示功能单元 SU 的失效率,且 MS 中存在多个 MFU,所以可以通过在名称中加入 <MFU_Name>用以区别。

3) 状态空间 States:

在系统运行过程中,功能单元可能包含的状态有正常状态 (NS, normal state),故障状态 (ES, error state),失效状态 (FS, failure state),故障检测状态 (DS, detected state) 和恢复状态 (RS, recovery state) 等等。正常状态是指功能单元正常运行,通常被定义为开始时的状态。故障状态表示功能单元在某一时刻发生故障时所处的状态,是

一种瞬间状态;故障检测状态是在故障发生后由系统自主发起的一种对故障进行检测的状态,通常也是一种瞬间状态。由以上所提及的功能单元的状态可得功能单元的一种状态转移关系如图 3 (a) 所示。由于瞬间状态是一种转瞬即逝的短暂状态,因此在可靠性进行分析和评估时,通常不把这些瞬间状态考虑在内,因此将瞬间状态剔除后可得图 3 (b) 所示的关系图。在图中,圆圈即表示功能单元当前所处的状态,连接圆圈的弧线即表示两个状态之间的转移关系,发出箭头的圆圈表示转移关系中的源状态,箭头指向的一方表示转移关系中的目标状态;连接线上的参数表示状态转移概率,其图中各参数代表的含义如表 1 所示。

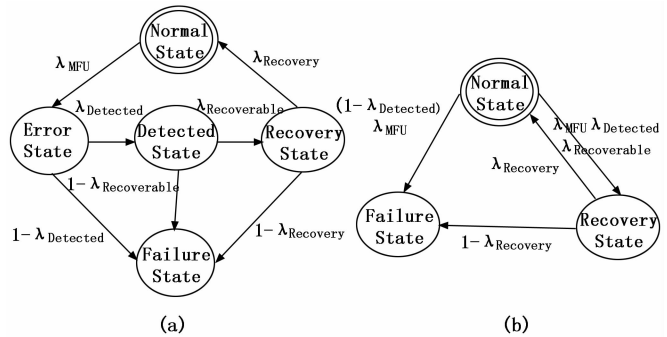


图 3 MFU 状态转移图

表 1 MFU 状态转移参数及其含义

状态转移参数	参数含义
λ_{MFU}	MFU 发生故障的概率,即失效率
$\lambda_{Detected}$	故障被检测到的概率
$1 - \lambda_{Detected}$	故障未被检测到的概率
$\lambda_{Recoverable}$	故障可以被修复的概率
$1 - \lambda_{Recoverable}$	故障不能被修复的概率
$\lambda_{Recovery}$	故障被成功修复的概率
$1 - \lambda_{Recovery}$	故障不能被成功修复的概率

通过上述的状态转移关系图即可得到每个功能单元的状态空间,因此可以采用以下方式对功能单元的状态空间进行定义:

<StateName>State

isInitial: \mathbb{N}

isArrive: \mathbb{N}

isInitial $\in \{0, 1\}$

isArrive $\in \{0, 1\}$

其中: isInitial 和 isArrive 分别表示是否是初始状态和是否是当前状态。

4) 状态转移关系 STR:

同样,通过图 3 构成的状态转移关系图也可以得到状态空间内所有状态彼此之间的转移关系。每一段状态转移

关系中都需要包含 3 个要素, 分别是源状态 (SS, source state)、目标状态 (TS, target state) 以及转移概率参数 (TR, transfer rates)。其中, SS 和 TS 必须是每个 MFU 状态空间中具有的, TR 则是对应于每个转移关系中存在的转移参数。具体 Z 语言模式定义如下:

<MFUName_STRName>STR

SS: State

TS: State

TR: R

Conditions: seq Predicate

3.2.2 功能单元可靠性评估模型 FU-REM

在功能单元的可靠性模型 Z-FURM 中, 根据其描述可知每个功能单元的可靠性都与时间相关联, 而且功能单元在不同时刻时所处的状态也都只与该时刻的前一时刻功能单元所处的状态相关, 与其它时刻的状态无关, 因此本文采用基于 CTMC 的方法建立功能单元的可靠性评估模型 (FU-REM, function unit reliability evaluate model based on CTMC)。本文建立的 FU-REM 可靠性评估模型定义如式 (6) 所示:

$$FU-REM = (S, S_m, T, t) \quad (6)$$

其中: S 表示评估模型的状态空间, 包含每个功能单元 MFU 中所有可能状态的集合; $S_m \in S$ 表示在进行可靠性评估时功能单元所处的初始状态; $T = [a_{ij}]$ 是状态转移概率矩阵, a_{ij} 表示一个功能单元 MFU 从状态 $s_i \in T$ 转移到状态 $s_j \in T$ 的概率; t 表示评估可靠性时的某一时刻。

当使用可靠性评估模型 FU-REM 对功能模块进行评估之前, 需要先把 Z-FURM 模型中的建模元素转换成 FU-REM 模型中的元素, 然后再进行相应的可靠性评估。在进行模型转换过程中, 因为需要将两个模型中的元素进行等价转换, 因此需要构建相应的映射规则。本文定义的两模型间的映射转换规则如表 2 所示。

表 2 Z-FURM 与 FU-REM 之间的元素映射规则

FU-REM 元素	元素含义	Z-FURM 建模要素
S	状态空间	Z-FURM 模型中定义的
S_m	初始状态	Z-FURM 模型中声明的状态
T	状态转移 概率矩阵	Z-FURM 模型中定义中声明的状态转移概率参数
t	时刻	Z-FURM 评估时的时刻

由于指数模型对功能单元失效率的真实曲线的拟合程度相较于其它模型更好, 因此本文采用指数模型描述功能单元失效率与时间之间的关系。其表达式如式 (7) 所示:

$$\lambda_{MFU}(t) = \exp(\lambda_{MFU} * t) \quad (7)$$

在式 (7) 中, $\lambda_{MFU}(t)$ 表示在 t 时刻功能单元的失效率, λ_{MFU} 表示当 $t = 0$ 时 MFU 的失效率。

根据 FU-REM 模型中的状态转移方程可得到如式 (8) 所示的关于 MFU 的状态概率方程:

$$P(t') = P(t) * T \quad (8)$$

式 (8) 中, $P(t) = (P_N(t), P_R(t), P_F(t))$ 表示 t 时刻时 MFU 的状态概率向量, $P_N(t)$ 表示 t 时刻时 MFU 的状态为正常时的概率, $P_R(t)$ 表示 t 时刻时 MFU 的状态为恢复时的概率, $P_F(t)$ 表示 t 时刻时 MFU 的状态为失效时的概率。同理, $P(t') = (P_N(t'), P_R(t'), P_F(t'))$ 表示 t' 时刻 MFU 的状态概率向量, t' 为 t 的下一时刻, T 表示状态转移概率矩阵, 是由图 2 (b) 得到的一个 3×3 的矩阵, 其具体表示形式如式 (9) 所示。其中, 行表示的是状态转移关系中的源状态, 列表示状态转移关系中的目标状态, 矩阵中的参数代表的是由源状态向目标状态转移的概率参数, 其含义如式 (9) 所示:

$$T = \begin{pmatrix} 1 - \lambda_{MFU}(t) & \lambda_{MFU}(t)\lambda_{Detected} & (1 - \lambda_{Detected})\lambda_{MFU}(t) \\ \lambda_{Recovery} & 1 - \lambda_{Recovery} & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad (9)$$

所以, 联立式 (7) ~ (9) 可得 MFU 的状态概率方程, 如式 (10) 所示:

$$\begin{cases} P_N(t') = P_N(t) * (1 - e^{\lambda_{MFU} * t}) + P_R(t) * \lambda_{Recovery} \\ P_R(t') = P_R(t) * e^{\lambda_{MFU} * t} * \lambda_{Detected} + P_R(t) * (1 - \lambda_{Recovery}) \\ P_F(t') = P_N(t) * (1 - \lambda_{Detected}) * e^{\lambda_{MFU} * t} + P_F(t) \end{cases} \quad (10)$$

通过对式 (10) 中方程的求解, 即可得到功能模块在 t 时刻时所处状态的概率分布。因此, 功能模块在 t 时刻时可靠度的计算方式如式 (11) 所示:

$$R_{MFU}(t) = 1 - P_F(t) \quad (11)$$

3.3 整体可靠性分析与评估模型

基于上述方法可以得到存储系统中每个功能单元的失效率以及可靠度, 但由于存储系统中功能单元较多, 其状态转移关系更加复杂, 在使用 CTMC 对其进行可靠性评估时计算量较大, 所以在对存储系统整体进行可靠性评估时, 本文建立从功能单元到存储系统整体的两层贝叶斯网络为系统整体的可靠性模型 (MSR-BN, memory system reliability model on Bayesian network), 以贝叶斯推理方式对存储系统的可靠性进行评估。

本节以两状态节点描述存储系统和功能单元的不同状态, 其两个状态分别为故障状态和正常状态, 用 1 和 0 表示, 且存储系统中各个功能单元之间相互独立。

3.3.1 MSR-BN 模型的构建

存储系统可靠性模型如式 (12) 所示:

$$MSR-BN = (G, P) \quad (12)$$

其中: $G = (I, E)$, I 表示构成 MSR-BN 模型中的节点, 即各功能模块的失效变量; E 表示有向边的集合; P 表示非根节点的条件概率表, 表示节点间的关联强度。所以, 构建 MSR-BN 的具体步骤如下:

1) 确定模型中的节点; 要构建 MSR-BN 模型首先应确定整个系统中可以设立的变量个数, 在上节中 MFU 的失效

率与其组件之间的关系已经根据 FU-REM 模型进行评估, 所以这里只考虑 MS 与 MFU 之间的可靠性关系, 不考虑 MS 与 MFU 组件状态的关系。因此, MSR-BN 中的节点即为存储系统整体 MS 和存储系统的 4 个功能单元, 存储单元 SU、数据寄存器 MER、地址寄存器 MAR 和内存控制器 MC。此外, 由第 3 节可知, 每个功能单元的失效率都可由 FU-REM 模型计算得到。

2) 确定模型中各节点的连接关系; 在确定完变量后, 需要分析变量之间的相互关系。本文假定一个功能单元失效就会引起存储系统整体发生失效。所以其 MSR-BN 中的叶子节点为存储系统失效, MSR-BN 中的根节点为 4 个功能单元失效, 然后根据各节点的依赖关系将各个节点用有向边进行连接, 从而就可以得到存储系统的 MSR-BN 模型。

3) 确定模型中节点的条件概率表; 在建立的 MSR-BN 模型中, 本文通过条件概率来描述变量之间的相互关系。通过分析模型中各个节点之间相互的逻辑关系, 为每个节点编写各自的条件概率表, 然后基于条件概率表来计算节点的条件概率。

由于各功能单元与存储系统为串联, 所以当功能单元中的任意一个发生失效时, 系统整体也会发生失效。因此, 可根据经验得到系统的条件概率表。

3.3.2 系统整体可靠性评估

系统整体可靠度是指系统处于正常运行状态的可能性大小, 是一个在 0 和 1 之间的概率值。当可靠度为 1 时, 说明系统处于完全失效状态; 当可靠度值为 0 时, 说明系统处于可靠状态或是正常状态。

基于贝叶斯网络的可靠性计算应首先要生成各节点的先验概率和条件概率, 其步骤如下:

1) 根据 MSR-BN 中的节点所对应的功能单元的失效率, 可以直接得到各根节点 (x_i) 的先验概率, 即各功能模块的失效率。计算公式如式 (13) 所示:

$$P(x_i = 1) = \lambda_i, i \in \{SU, MER, MAR, MC\} \quad (13)$$

其中: λ_i 即为第 3 节通过 FU-REM 模型计算得到的各功能单元的失效率;

2) 确定非根节点的条件概率。该模型只有两层, 所以非根节点即为叶子节点。因此, 非根节点的条件概率即存储系统的失效率。根据联合概率公式, 基于条件独立性原则, 存储系统的失效率的计算公式如式 (14) 所示:

$$P(MS = 1) = P(MS = 1 | x_{SU}, x_{MER}, x_{MAR}, x_{MC}) = 1 - \prod_{i \in \{SU, MER, MAR, MC\}} (1 - \lambda_i) \quad (14)$$

在式 (14) 中, $P(MS = 1)$ 即为存储系统失效率; λ_i 表示各功能单元的失效率, 即第 3 节求得的 $P_F(t)$ 。

3) 计算存储系统可靠度。针对 MSR-BN 模型, 可靠度的计算公式如式 (15) 所示:

$$R_{MS} = 1 - P(MS = 1) \quad (15)$$

由于各个 MFU 的失效率是依据 FU-REM 模型得到的,

因此 MS 的可靠度是一个随时间不停变化的值。

3.4 关键模块识别

关键模块是指存储系统中的可靠性关键模块。通过识别该模块能够分析出系统中的薄弱地方, 对提高系统的可靠性有着积极的作用。

本文在 MS 的故障条件下, 通过计算得到任意一个功能单元的后验故障概率, 然后计算底事件的重要度, 最后按照计算出的底事件的重要度进行排序, 从而识别出可靠性关键模块。本文主要从两个方面来衡量底事件的重要度。

3.4.1 概率重要度 I^{Pr}

概率重要度 I^{Pr} 是指当且仅当该功能单元处于失效状态时, 系统发生失效的概率。它反映的是当功能单元的状态发生改变时, 对系统状态变化的影响程度。

$$I^{Pr}(x_i) = P(MS = 1 | x_i = 1) - P(MS = 1 | x_i = 0) \quad i \in \{SU, MAR, MER, MC\} \quad (16)$$

3.4.2 关键重要度 I^C

关键重要度 I^C 是指功能单元发生失效的概率变化对系统发生失效的概率变化的影响, 是判断功能单元是否为可靠性关键模块的关键性指标。

$$I^C(x_i) = \frac{P(x_i = 1)[P(MS = 1 | x_i = 1) - P(MS = 1 | x_i = 0)]}{P(MS = 1)} =$$

$$\frac{P(x_i = 1)}{P(MS = 1)} I^{Pr}, i \in \{SU, MER, MAR, MC\} \quad (17)$$

式 (16) 和式 (17) 中, $x_i = 1$ 表示模块 i 处于失效状态, $x_i = 0$ 表示模块 i 处于正常状态, $MS = 1$ 表示存储系统处于失效状态。其中, 概率重要度和关键重要度均靠前的 MFU 被定义为可靠性关键模块。

4 模型应用实例

为了验证本文提出方法的有效性, 本文选取文献 [29] 中的实例进行分析和对比。

4.1 实例描述

某一型号的弹载固态存储器, 其主要组成有机械壳类和存储记录电路, 且此固态存储器可靠性研究重点在于存储记录电路。该弹载固态存储器的内部存储记录电路主要由模拟采编模块 1、模拟采编模块 2、数字采编模块、电源调节模块以及存储控制模块 5 个部分组成。从底层元器件出发对存储记录电路进行剖析, 电路各模块是由电阻与电容、连接导线、集成电路、接插件、印制板与焊点、半导体分立器件等组成。集成电路又包括模拟电路、模拟开关、A/D 变换器、数字电路、Flash 存储。半导体分立器件又包括二极管和光耦。存储记录电路如图 4 所示。

根据文献可以得到该固态存储器的存储电路不同的可靠性功能单元, 其可靠性如图 5 所示。

4.2 功能单元可靠性评估

本文以存储电路的电阻与电容 (RC, resistance and capacitance) 单元为例, 建立单个功能单元的可靠性评估模型。

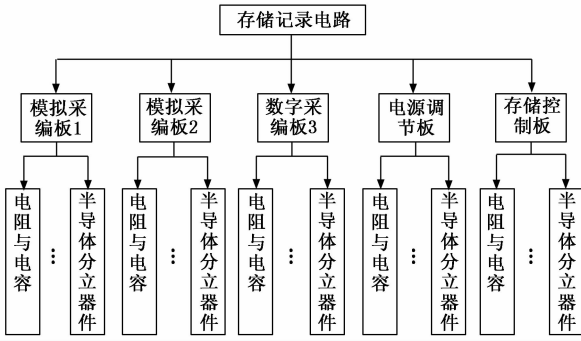


图 4 存储记录电路框图

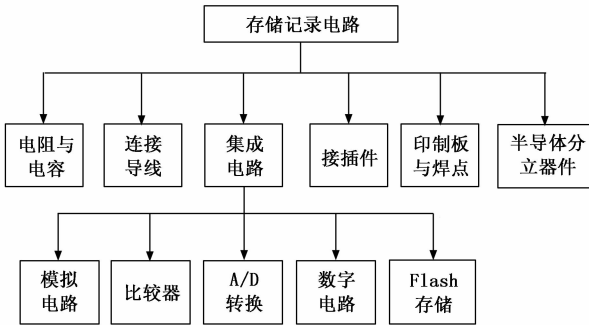


图 5 可靠性框图

1) 失效率 $FRate$:

根据文献可知, 与 RC 单元失效率相关的元器件的失效概率表 3 所示。

表 3 RC 单元中元器件失效率

元器件	失效率($\times 10^{-5}$)
电阻(Resistance)	9.22
电容(Capacitance)	4.24

所以, 由式 (4) 可知 RC 的失效率为:

$$\lambda_{RC} = 1 - (1 - \lambda_{Resistance}) * (1 - \lambda_{Capacitance}) = 1 - (1 - 9.22 \times 10^{-5}) * (1 - 4.24 \times 10^{-5}) = 1.35 \times 10^{-4}$$

RC 功能单元的失效率 RC_FRate 的 Z 模式可声明为:

RC_FRate

Resistance_FRate: \mathbb{R}

Capacitance_FRate: \mathbb{R}

MFU_FRate: \mathbb{R}

Resistance_FRate= 9.22×10^{-5}

Capacitance_FRate= 4.24×10^{-5}

MFU_FRate= 1.35×10^{-4}

2) 状态空间 States:

下面分别以 RC 功能单元的正常状态 NS 和失效状态 FS 为例, 演示状态空间的建模过程。

NSSState

isInitial: \mathbb{N}

isArrive: \mathbb{N}

isInitial=1

isArrive=1

FSSState

isInitial: \mathbb{N}

isArrive: \mathbb{N}

isInitial=0

isArrive=0

3) 状态转移关系 STR:

以 NS 状态和 FS 状态之间的转移关系为例进行演示说明。

RC_NStoFSSTR

SS: State

TS: State

TR: \mathbb{R}

SS=NSSState

TS=FSSState

TRate=RCFRate, MFU_FRate

图 2 中各项状态转移概率设置为表 4 中所列数据, 其中剩余的状态转移关系以同样的方式进行定义。

表 4 RC 单元各项状态转移参数设置

参数	数值
$\lambda_{Detected}$	0.998 67
$\lambda_{Recovery}$	0.97

根据 3.2 小节建立的 Z-FURM 模型, 结合表 2 所设计的 Z-FURM 与 FU-REM 的建模要素映射转换规则, 可以为 RC 功能单元建立评估模型 $FU-REM_{RC} = (S, S_m, T, t)$ 。其中, $S = \{NS, RS, FS\}$; $S_m = NS$; 转移矩阵:

$$T = \begin{bmatrix} 1 - e^{1.35 \times 10^{-4} * t} & 0.998\ 67 \times e^{1.35 \times 10^{-4} * t} \\ 0.97 & 0.03 \\ 0 & 0 \end{bmatrix}$$

将 $P_{F_RC}(0) = [1, 0, 0, 0]$ 与转移矩阵 T 代入式 (10) 可得 RC 功能单元处于失效状态的概率 $P_{F_RC}(t)$ 与时间 t 的函数关系为式 (18):

$$P_{F_RC}(t) = 0.001\ 33 \times \exp(1.35 \times 10^{-4} * t) \quad (18)$$

利用 Matlab 画出式 (18) 在时间范围为 $[0, 50\ 000]$ 之间的概率变化曲线, 如图 6 中实线所示。

从图 6 中可以看出, 当时间 t 接近 5×10^4 h 时 RC 模块的处于失效状态的概率接近 1, 这也与硬件的客观老化、淘这相符合。图 6 中的虚线则是 RC 单元的可靠性随时间变化的曲线。

4.3 系统可靠性评估及关键模块识别

4.3.1 系统可靠性评估

由分析可知, 该存储器电路的贝叶斯网络中共有 7 个变量, 分别是存储器电路失效、电阻电容失效、导线故障、集成电路失效、接插件故障、印制板和焊点失效以及分离

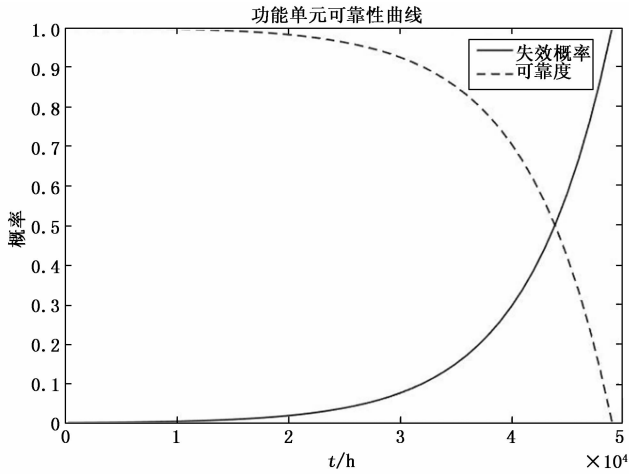


图 6 RC 单元处于失效状态时的概率曲线

器失效。

由文献 [27] 可知，该存储器电路为串联结构，其中一个功能单元失效都会引起存储器电路整体失效，所以可得其贝叶斯网络模型如图 7 所示。其根节点的先验概率即各功能单元的失效率可依据上述方法求得，表 5 中列出了当时间 $t=1\ 000\ \text{h}$ 时，存储器电路中所有 MFU 的失效率。

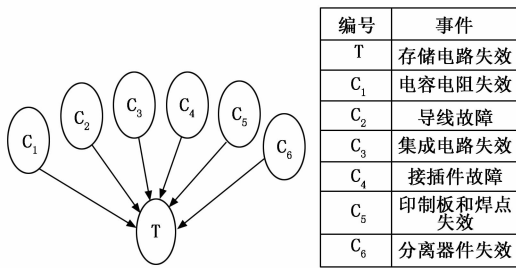


图 7 存储电路的 MSR-BN 模型

表 5 存储电路各 MFU 在 $t=1\ 000\ \text{h}$ 时的失效率

功能单元	失效率	功能单元	失效率
电阻电容	1.52×10^{-3}	接插件	1.34×10^{-3}
导线	1.33×10^{-3}	印制板和焊点	1.39×10^{-3}
集成电路	2.99×10^{-3}	分立器件	1.41×10^{-3}

所以，存储电路发生失效的概率为： $P(T = 1) = 0.99 \times 10^{-2}$ ；存储电路正常工作的概率即可靠度为： $R = 1 - (P(T = 1)) = 0.990\ 1$ 。

4.3.2 关键模块识别

由式 (16) 可得每个功能单元的概率重要度如表 6 所示。

由式 (17) 可得每个功能单元的关键重要度如表 7 所示。

为了更好地对结果进行分析，本文把每个模块的概率重要度和关键重要度画成折线图的形式来展示，如图 8

所示。

表 6 各个功能单元的概率重要度

节点	概率重要度 I^P
C ₁	1.000
C ₂	0.999
C ₃	0.999
C ₄	1.000
C ₅	0.999
C ₆	0.999

表 7 各个功能单元的关键重要度

节点	关键重要度 I^C
C ₁	1.529 2
C ₂	1.338
C ₃	3.008
C ₄	1.348 1
C ₅	1.387 1
C ₆	1.418 5

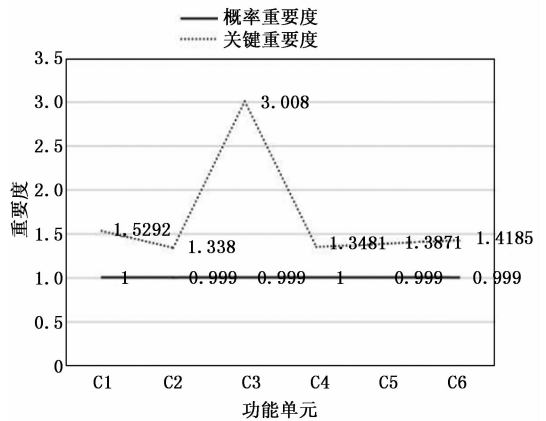


图 8 概率重要度和关键重要度折线图

从表 6、表 7 和图 8 可知，当系统失效时，计算的概率重要度和关键重要度中， C_3 、 C_1 、 C_6 对应的功能单元的重要度更加靠前。其中，节点 C_3 即集成电路失效排在第一，这说明集成电路失效对该存储器电路影响较大，而这也与实际情况相符，因此该存储电路中的可靠性关键模块为 C_3 。从文献 [27] 中，也可以得到集成电路为存储电路中的可靠性关键模块，以此说明了该方法的有效性和正确性。

通过实例分析与计算可知，存储系统基于本文建立的可靠性评估模型可量化计算其可靠性。同时，根据贝叶斯网络双向推理的优势，可以得到其可靠性关键模块。在使用期间，对关键模块进行维护与保养，可以有效地提高存储系统的可靠性。

5 结束语

针对传统的存储系统可靠性评估方法难以动态地描述

其可靠性特征, 也难以反映其与时间关系的问题, 本文提出了一种结合 Z 语言和贝叶斯网络的评估方法。该方法既具有 Z 语言的数据约束能力以及可扩展性, 又可以通过贝叶斯网络的双向推理特性得到系统的可靠度以及可靠性关键模块。最后通过一个实例, 验证了本文模型的正确性、评估方法和关键模块识别方法的有效性。

参考文献:

- [1] ZHOU G, GUO B, GAO X, et al. Research on the system reliability modeling based on Markov process and reliability block diagram [M]. Springer International Publishing, 2014: 375 - 407.
- [2] BIEBER P, CASTEL C, SEGUIN C. Combination of fault tree analysis and model checking for safety assessment of complex system [J]. Lecture Notes in Computer Science, 2002, 2485: 19 - 31.
- [3] 史定华, 王松瑞. 故障树分析技术方法和理论 [M]. 北京: 北京师范大学出版社, 1993.
- [4] 周建方, 唐椿炎, 许智勇. 事件树、故障树、决策树与贝叶斯网络 [J]. 河海大学学报 (自然科学版), 2009, 37 (3): 351 - 355.
- [5] CHARLES J. Practical Markov chain Monte Carlo [J]. Statistical Science, 1992, 7 (4): 473 - 483.
- [6] RANA A S, THOMAS M S, SENROY N, et al. Reliability evaluation of WAMS using Markov-based graph theory approach [J]. Iet Generation Transmission & Distribution, 2017, 11 (11): 2930 - 2937.
- [7] EISENTRAUT C, HERMANN S, KATOEN J, et al. A semantics for every GSPN [M]. Springer Berlin Heidelberg, 2013: 90 - 109.
- [8] 谷春英, 姚青山. 基于 GSPN 的计算机硬件系统可靠性分析 [J]. 微电子学与计算机, 2013, (6): 122 - 125.
- [9] GAO K, XIAO H, MI J, et al. Optimal abort policy of a distributed system of computers with Weibull failure time [C] // 2020 Global Reliability and Prognostics and Health Management (PHM-Shanghai), Shanghai, 2020: 1 - 5.
- [10] LI J, LI P, STONES R, et al. Reliability equations for cloud storage systems with proactive fault tolerance [J]. IEEE Transactions on Dependable and Secure Computing, 2020, 17 (4): 782 - 794.
- [11] NACHIAPPAN R, JAVADI B, CALHEIROS R, et al. Cloud storage reliability for big data applications: a state of the art survey [J]. Journal of Network & Computer Applications, 2017, 97 (1): 35 - 47.
- [12] CHATTARAJ D, SARMA M, SAMANTA D. Stochastic Petri net based modeling for analyzing dependability of big data storage system [C] // Proceedings of IEMIS, 2019: 473 - 484.
- [13] CHEN Y, HUI L, LI K, et al. An improved P2P file system scheme based on IPFS and Blockchain [C] // Boston: 2017 IEEE International Conference on Big Data (Big Data), IEEE, 2017: 2652 - 2657.
- [14] 郑健. 基于模糊处理的医疗信息数据存储系统的设计 [J]. 计算机测量与控制, 2017, 25 (7): 298 - 301.
- [15] 古忻艳. 网络计算机模型下海量大数据存储系统设计 [J]. 计算机测量与控制, 2017, 25 (6): 246 - 249.
- [16] JIA H, PENG R, DING Y, et al. Reliability analysis of distributed storage systems considering data loss and theft [J]. Journal of Risk and Reliability, 2020, 234 (2): 303 - 321.
- [17] MA R, WU F, LU Z, et al. Block hammer: improving flash reliability by exploiting process variation aware proactive failure prediction [J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2020, 39 (12): 4563 - 4574.
- [18] 黄敏. 提高 MLC NAND Flash 存储系统可靠性的方法研究 [D]. 哈尔滨: 哈尔滨工业大学, 2016.
- [19] WANG J, WU H F, WANG R J. A new reliability model in replication-based big data storage systems [J]. Journal of Parallel and Distributed Computing, 2017, 108: 14 - 27.
- [20] FITCH D, XU H. A raid-based secure and fault-tolerant model for cloud information storage [J]. International Journal of Software Engineering and Knowledge Engineering, 2013, 23 (5): 627 - 654.
- [21] 李静, 罗金飞, 李炳超. 主动容错副本存储系统的可靠性分析模型 [J]. 计算机应用, 2021, 41 (4): 1113 - 1121.
- [22] ZHAO Y, LIU X, GAN S, et al. Predicting disk failures with HMM-and HSMM-Based Approaches [J]. Springer, Berlin, Heidelberg, 2010, 6171: 390 - 404.
- [23] TAN Y, GU X. On predictability of system anomalies in real world [C] // Miami Beach, FL, USA: IEEE International Symposium on Modeling, ACM, 2010: 133 - 140.
- [24] MAHDISOLTANI F, STEFANOVIĆ I, SCHROEDER B. Improving storage system reliability with proactive error prediction [C] // USENIX Association, ACM, 2017: 391 - 402.
- [25] 刘榴, 李小勇. 分布式存储系统中磁盘故障检测机制 [J]. 信息技术, 2018 (5): 83 - 89.
- [26] SHUAI P, JIA Y, STONES R, et al. A combined Bayesian network method for predicting drive failure times from SMART attributes [C] // 2016 International Joint Conference on Neural Networks (IJCNN), IEEE, Vancouver, BC, Canada: 2016: 4850 - 4856.
- [27] XU C, GANG W, et al. Health status assessment and failure prediction for hard drives with recurrent neural networks [J]. IEEE Transactions on Computers, 2016, 65 (11): 3502 - 3508.
- [28] 李蜜. 基于 Z 语言的嵌入式系统可靠性建模与评估技术研究 [D]. 南京: 南京航空航天大学, 2019.
- [29] 胡时光, 尤文斌, 丁永红, 等. 基于故障树分析的弹载固态存储器可靠性研究 [J]. 火炮发射与控制学报, 2020, 41 (4): 87 - 92.