第 34 卷 第 7 期 计 算 机 工 程 2008 年 4 月
Vol.34 No.7 Computer Engineering April 2008
·工程应用技术与实现· 文章编号：1000—3428(2008)07—0240—03 文献标识码：A 中图分类号：N945.15

直流配电盒的可靠性设计与分析

高从英，李 曦
(中国科学技术大学计算机技术系，合肥 230027)

摘 要：直流配电盒作为配电系统的核心，要求具有较高的可靠性。该文对基于 CAN/LIN 总线直流配电盒系统的容错设计和具体实现方案进行论述。通过运用马尔可夫随机过程理论和拉普拉斯变换工具，对直流配电盒的失效-修复这一随机过程进行可靠性分析，确定各个部件以及整个系统的可用度、可靠度和平均无故障工作时间。在可靠性分析的基础上，采用 Matlab/Simulink 对直流配电盒进行仿真，能够比较准确地反映暂态过程中直流配电盒系统的动态特性，直观地体现系统的性能。

关键词：马尔可夫模型；容错；可靠性；仿真；Matlab/Simulink 技术

Reliability Design and Analysis of DC Power Distribution Box

GAO Cong-ying, LI Xi
(Department of Computer Science and Technology, University of Science and Technology of China, Hefei 230027)

【Abstract】The DC power distribution box, as the key part of power distribution system, demands high reliability. This paper presents the fault-tolerant design and the implementation of the DC power distribution box based on CAN/LIN bus. It also analyzes the reliability of failure-repair stochastic processes. By using the Markovian process theory and the tool of the Laplace transform, some reliability indexes of the system are obtained, such as the availability, the reliability and the mean time between failures of components and the whole system. On the basis of the mathematical analysis, the model is simulated in Matlab/Simulink environment. The simulation results indicate that the power distribution system has good dynamic performance.

【Key words】Markov model; fault-tolerance; reliability; simulation; Matlab/Simulink

由于工业现场环境的复杂性，直流配电盒系统[1]必须具有很高的可靠性[2-4]。提高元器件本身的可靠性是提高系统整体可靠性的基础，要进一步提高可靠性，就必须采用容错技术。容错技术主要建立在“冗余”的设计上，即利用资源的冗余来提高系统的可靠性。

1 可靠性设计

将直流配电盒系统抽象为由CAN总线、微控制器(MCU)、片内FLASH串联而成[2-4]。为了保证直流配电盒系统高安全、高可靠运行，对系统的关键部件进行冗余设计。而系统中最为关键的部件是CAN总线通信系统和频繁地进行信息读取的片内FLASH。

1.1 双冗余 CAN 总线

在本系统中，现场总线担负着实时传输信息的任务，必须满足可靠性和实时性的要求。CAN总线本身是一种高实时性、高可靠性的现场总线[5]，具有高抗电磁干扰性、可靠的错误处理和检错机制，能够检测到消息帧的位错误、填充错误、CRC错误、格式错误和应答错误等。当节点出现严重故障时，能自动脱离总线，降低了故障节点对总线的影响。但是在CAN 总线的使用过程中不可避免地经受着各种自然或人为环境的考验，造成各种总线故障，如用于数据传输的双绞线的断线或短路、CAN总线驱动器故障、CAN 总线控制器故障等。一旦出现总线故障，实时数据就不能得到有效处理，严重时可能造成重大事故。因此，有必要对CAN总线进行可靠性设计，可以采用增加冗余的可靠性设计思想，对通信链路采取双冗余热备份结构[2-4]。具体实现时，系统使用2 套总线(CAN1, CAN2)，每一套包含独立的总线电缆、总线驱动器和总线控制器，2 套总线采用热备份方式运行：一个CAN控制器作为系统上电后默认的CAN(可称为主CAN)；另一个为系统的备用CAN(称之为从CAN)。系统正常工作时，主CAN总线(CAN1)投入运行。如检测到主CAN总线故障，则从CAN总线(CAN2)自动投入运行。这样在一套总线发生故障时，另一套总线自动继续工作，保证整个系统通信功能正常运行，大大提高了系统的可靠性，实现了CAN总线的全面冗余设计。双冗余CAN总线方案如图 1 所示。

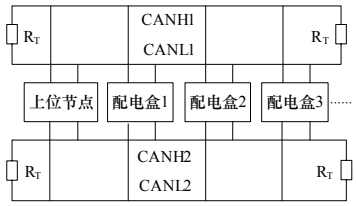

图 1 双冗余 CAN 总线

1.2 FLASH 三模冗余

直流配电盒把系统参数、配置信息存储在片内 FLASH。这些信息对系统的正常运行至关重要。期望这些信息可以永久完整地存储着。但是电源电压的不稳定、突发性断电以及配置信息更改频繁等原因会有损坏字节的可能，严重时可能造成重大事故。因此有必要对 FLASH 存储系统进行可靠性设计。

作者简介：高从英(1980－)，女，硕士研究生，主研方向：嵌入式系统设计；李 曦，副教授、高级工程师

收稿日期：2007-04-13 **E-mail：**cygao@mail.ustc.edu.cn

常用的纠错方案为三模冗余[2-4](Triple Modular Redundancy, TMR)，即将每个信息在 3 个互相无关的地址单元中存放，建立数据备份。当系统受干扰时可以通过三中取二表决程序恢复重要信息。三模冗余结构是一个高可靠、高安全性的冗余结构。

本系统中采用类似三模冗余的方法，即对需要记录的数据记录 3 次，分别是原始数据、备份数据、原始数据的 CRC。CRC 采用 16 位的 CRC-ITU。读出时先比较原始数据和备份数据，如相等则读取成功，否则对原始数据、备份数据分别进行 CRC 校验，返回校验通过的数据，并纠正错误的数据块。

2 可靠性分析

可靠性数学模型是可靠性从定性分析向定量分析转变的关键。由于构成配电盒系统的各部件的失效率和修复率都可看成常数，即随机变量的状态转移概率都保持为常数，因此可以把系统视为时间连续、状态离散的马尔可夫过程[6]。本文主要使用马尔可夫模型对系统的各部件进行可靠性分析。

2.1 双冗余 CAN 总线

系统的CAN总线通信网络相当于一个并联系统。CAN总线通信系统中包含 2 个完全相同的CAN总线，设每个CAN总线的失效率均为 λ_1，修复率均为 μ_1，由于在充分小的时间内，马尔可夫过程发生 2 次或 2 次以上状态转移的概率为 $o(\Delta t)$。双冗余CAN总线的状态转移[6]如图 2 所示。

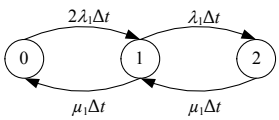

图 2 双冗余 CAN 总线系统的状态转移

此系统共有 3 个不同的状态。取系统的状态空间 $E=\{0,1,2\}$, $W=\{0,1\}$, $F=\{2\}$，含义如下：0，2 个单元工作正常；1，有 1 个单元失效；2，2 个单元均失效。根据系统状态转移图，得到转移率矩阵[6]：

$$\boldsymbol{A}=\begin{pmatrix}-2\lambda_1 & 2\lambda_1 & 0\\ \mu_1 & -\lambda_1-\mu_1 & \lambda_1\\ 0 & \mu_1 & -\mu_1\end{pmatrix} \tag{1}$$

可得到系统的马尔可夫状态方程[6]为

$$\begin{cases}(P_0'(t),P_1'(t),P_2'(t))=(P_0(t),P_1(t),P_2(t))\begin{pmatrix}-2\lambda_1 & 2\lambda_1 & 0\\ \mu_1 & -\lambda_1-\mu_1 & \lambda_1\\ 0 & \mu_1 & -\mu_1\end{pmatrix}\\ (P_0(0),P_1(0),P_2(0))=(1,0,0)\end{cases} \tag{2}$$

对式(2)两端作拉普拉斯变换，然后再进行拉普拉斯反变换，并且令方程 $s^2+(3\lambda_1+2\mu_1)s+(2\lambda_1^2+2\lambda_1\mu_1+\mu_1^2)=0$ 的 2 个根分别是 s_1, s_2。利用初始条件，可得：

$$\begin{cases}P_0(t)=\dfrac{\mu_1^2}{s1s2}+\dfrac{s_1^2+(\lambda_1+2\mu_1)s_1+\mu_1^2}{s1(s1-s2)}e^{s_1t}+\dfrac{s_2^2+(\lambda_1+2\mu_1)s_2+\mu_1^2}{s2(s2-s1)}e^{s_2t}\\ P_1(t)=\dfrac{2\lambda_1\mu_1}{s_1s_2}+\dfrac{2\lambda_1s_1+2\lambda_1\mu_1}{s_1(s_1-s_2)}e^{s_1t}+\dfrac{2\lambda_1s_2+2\lambda_1\mu_1}{s_2(s_2-s_1)}e^{s_2t}\\ P_2(t)=\dfrac{2\lambda_1^2}{s_1s_2}+\dfrac{2\lambda_2^2}{s_1(s_1-s_2)}e^{s_1t}+\dfrac{2\lambda_1^2}{s_2(s_2-s_1)}e^{s_2t}\end{cases} \tag{3}$$

因此系统的瞬时可用度是：

$$A(t)=1-P_2(t)=\frac{\mu_1^2+2\lambda_1\mu_1}{s_1s_2}-\frac{2\lambda_1^2(s_2e^{s_1t}-s_1e^{s_2t})}{s_1s_2(s_1-s_2)} \tag{4}$$

系统的稳态可用度是：

$$A=\lim_{t\to\infty}A(t)=\frac{\mu_1^2+2\lambda_1\mu_1}{s_1s_2}=\frac{\mu_1^2+2\lambda_1\mu_1}{2\lambda_1^2+2\lambda_1\mu_1+\mu_1^2} \tag{5}$$

为求系统的可靠度，只需令故障状态 2 为马尔可夫过程的吸收状态[6]，可以得到新的状态方程为

$$\begin{cases}(Q_0'(t),Q_1'(t))=(Q_0(t),Q_1(t))\begin{pmatrix}-2\lambda_1 & 2\lambda_1\\ \mu_1 & -\lambda_1-\mu_1\end{pmatrix}\\ (Q_0(t),Q_1(t))=(1,0)\end{cases} \tag{6}$$

对微分方程组(6)两端作拉普拉斯变换和拉普拉斯反变换，并利用初始条件，可得到系统的可靠度为

$$R(t)=Q_0(t)+Q_1(t)=\frac{1}{(s_1'-s_2')}(s_1'e^{s_2't}-s_2'e^{s_1't}) \tag{7}$$

其中，s_1', s_2' 是方程"$s^2+(3\lambda_1+\mu_1)s+2\lambda_1^2=0$"的 2 个负实根。因此，系统的平均故障间隔时间为

$$MTBF=\int_0^\infty R(t)\mathrm{d}t=\frac{3\lambda_1+\mu_1}{2\lambda_1^2}=\frac{3}{2\lambda_1}+\frac{\mu_1}{2\lambda_1^2} \tag{8}$$

其中，$\dfrac{3}{2\lambda_1}$ 代表 MTTF，是系统可靠性设计所提供的可靠性，即增加了冗余之后，双 CAN 系统的可靠度是单一 CAN 总线系统的 1.5 倍。而 $\dfrac{\mu_1}{2\lambda_1^2}$ 部分代表 MTTR，即由于采用了现场可维护策略使系统可靠性有所提高。

2.2 FLASH 三模冗余

系统的 FLASH 三模冗余系统也是现场可维修的。设该三模冗余(TMR)系统部件失效率均为 λ_2，修复率均为 μ_2，则 TMR 系统的状态转移如图 3 所示。

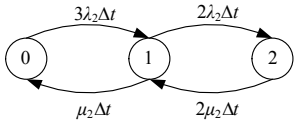

图 3 TMR 系统的状态转移

此系统共有 3 个不同的状态。取系统的状态空间 $E=\{0,1,2\}$, $W=\{0,1\}$, $F=\{2\}$。各状态空间的含义如下：0，2 个单元工作正常；1，有 1 个单元失效；2，2 个单元均失效。根据系统状态转移图，得到转移率矩阵：

$$\boldsymbol{A}=\begin{pmatrix}-3\lambda_2 & 3\lambda_2 & 0\\ \mu_2 & -2\lambda_2-\mu_2 & 2\lambda_2\\ 0 & 2\mu_2 & -2\mu_2\end{pmatrix} \tag{9}$$

可得到系统的马尔可夫状态方程为

$$\begin{cases}(P_0'(t),P_1'(t),P_2'(t))=(P_0(t),P_1(t),P_2(t))\begin{pmatrix}-3\lambda_2 & 3\lambda_2 & 0\\ \mu_2 & -2\lambda_2-\mu_2 & 2\lambda_2\\ 0 & 2\mu_2 & -2\mu_2\end{pmatrix}\\ (P_0(0),P_1(0),P_2(0))=(1,0,0)\end{cases} \tag{10}$$

对微分方程组(10)两端作拉普拉斯变换，然后再进行拉普拉斯反变换，并且令方程 $s^2+(5\lambda_2+3\mu_2)s+(6\lambda_2^2+6\lambda_2\mu_2+2\mu_2^2)=0$ 的 2 个根分别是 s_1, s_2。利用初始条件，可得：

$$\begin{cases}P_0(t)=\dfrac{2\mu_2^2}{s1s2}+\dfrac{s_1^2+(2\lambda_2+3\mu_2)s_1+2\mu_2^2}{s1(s1-s2)}e^{s_1t}+\dfrac{s_2^2+(2\lambda_2+3\mu_2)s_2+2\mu_2^2}{s2(s2-s1)}e^{s_2t}\\ P_1(t)=\dfrac{6\lambda_2\mu_2}{s_1s_2}+\dfrac{3\lambda_2(s_1+2\mu_2)}{s_1(s_1-s_2)}e^{s_1t}+\dfrac{3\lambda_2(s_2+2\mu_2)}{s_2(s_2-s_1)}e^{s_2t}\\ P_2(t)=\dfrac{6\lambda_2^2}{s_1s_2}+\dfrac{6\lambda_2^2}{s_1(s_1-s_2)}e^{s_1t}+\dfrac{6\lambda_2^2}{s_2(s_2-s_1)}e^{s_2t}\end{cases} \tag{11}$$

因此，系统的瞬时可用度是：

$$A(t)=1-P_2(t)=\frac{2\mu_2^2+6\lambda_2\mu_2}{s_1s_2}-\frac{6\lambda_2^2(s_2e^{s_1t}-s_1e^{s_2t})}{s_1s_2(s_1-s_2)} \tag{12}$$

稳态可用度是：

$$A=\lim_{t\to\infty}A(t)=\frac{2\mu_2^2+6\lambda_2\mu_2}{s_1s_2}=\frac{2\mu_2^2+6\lambda_2\mu_2}{6\lambda_2^2+6\lambda_2\mu_2+2\mu_2^2} \tag{13}$$

为求系统的可靠度，只需令故障状态 2 为马尔可夫过程

的吸收状态，可以得到新的状态方程为

$$\begin{cases}(Q_0'(t),Q_1'(t))=(Q_0(t),Q_1(t))\begin{pmatrix}-3\lambda_2 & 3\lambda_2\\ \mu_2 & -2\lambda_2-\mu_2\end{pmatrix}\\ (Q_0(t),Q_1(t))=(1,0)\end{cases} \tag{14}$$

对微分方程组(14)两端作拉普拉斯变换和拉普拉斯反变换，并利用初始条件，可得到系统的可靠度为

$$R(t)=Q_0(t)+Q_1(t)=\frac{1}{(S_1'-S_2')}(s_1'\mathrm{e}^{S_2't}-s_2'\mathrm{e}^{S_1't}) \tag{15}$$

其中，s_1', s_2' 是方程 $s^2+(5\lambda_2+\mu_2)s+6\lambda_2^2=0$ 的 2 个负实根。因此，系统的平均故障间隔时间为

$$MTBF=\int_0^\infty R(t)\mathrm{d}t=\frac{5\lambda_2+\mu_2}{6\lambda_2^2}=\frac{5}{6\lambda_2}+\frac{\mu_2}{6\lambda_2^2} \tag{16}$$

3 MATLAB 仿真

根据已经建立的数学模型，用Simulink[7]进行仿真。对于单个元件来说，设故障密度函数为 $f(t)$，主要通过以下几个可靠性指标衡量直流配电盒系统的可靠性：可靠度，$R(t)=1-\int_0^t f(x)\mathrm{d}x$；平均寿命，$MTTF=\int_0^\infty R(t)\mathrm{d}t$；失效率，$\lambda(t)=-\frac{\mathrm{d}}{\mathrm{d}t}\ln R(t)$。

CAN总线采用同轴电缆，其失效率一般是 200 FIT[8]，飞利浦半导体声称其LPC2100 系列MCU的失效率为 40 FIT，FLASH的失效率为 100 FIT。

可靠性设计前的系统可靠性仿真模型如图 4 所示，其参数设置：CAN1 模块的故障密度函数表达式为 2e-7×exp(-2e-7×u(1))；MCU 模块的故障密度函数表达式为 4e-8×exp(-4e-8×u(1))；FLASH 模块故障密度函数表达式为 1e-7×exp(-1e-7×u(1))。

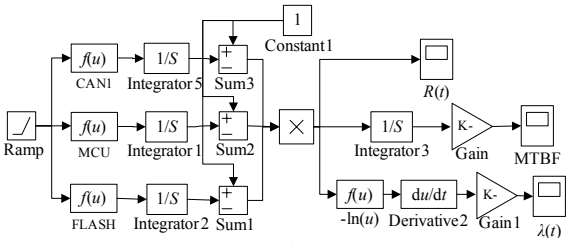

图 4　可靠性设计前的系统可靠性模型

可靠性设计后的可靠性仿真模型如图 5 所示。图 5 采用 Simulink 子系统封装功能，把双冗余 CAN 总线和 FLASH 三模冗余封装为独立的逻辑子系统，以便更加清晰。图 6 是双冗余 CAN 总线子系统的仿真模型。

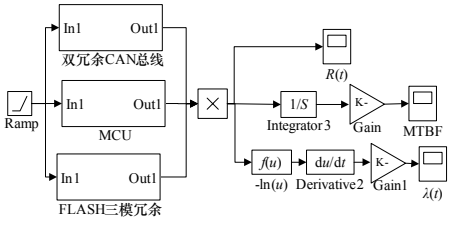

图 5　可靠性设计后的系统可靠性模型

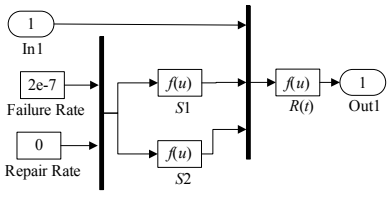

图 6　双冗余 CAN 总线子系统可靠性模型

根据已经建立的马尔可夫可靠度数学模型，其参数设置：

$s1$ 模块的表达式为

(-1×(3×u[1]+u[2])+sqrt(u[1]×u[1]+6×u[1]×u[2]+u[2]×u[2]))/2

$s2$ 模块的表达式为

(-1×(3×u[1]+u[2])−sqrt(u[1]×u[1]+6×u[1]×u[2]+u[2]×u[2]))/2

$R(t)$模块的表达式为

(u[2]×exp(u[3]×u[1])-u[3]×exp(u[2]×u[1]))/(u[2]-u[3])

MCU 模块的故障密度函数表达式不变。FLASH 模块的参数设置同双冗余 CAN 总线模块相似，在此不再赘述。

最后把仿真得到的可靠性设计前后的结果通过Matlab[7]编程生成在同一个图形里，各函数曲线分别为：可靠度 $R(t)$(如图 7)，失效率 $\lambda(t)$(如图 8)及系统平均寿命MTBF(如图 9)。

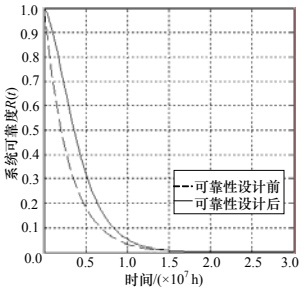

图 7　系统可靠度函数曲线

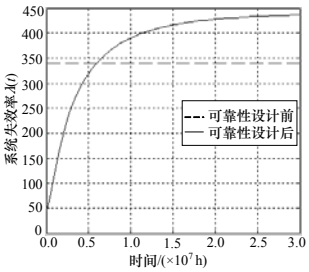

图 8　系统失效率函数曲线

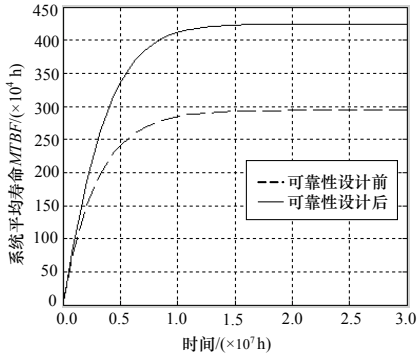

图 9　系统平均寿命函数曲线

图 7 显示系统可靠度随着时间增长而下降，但同一时刻，可靠性设计后的系统可靠度高于设计前的。图 8 显示可靠性设计后系统失效率在系统的前期随着时间增大，在系统的后期趋于一定值，并且前期的系统失效率比可靠性设计前低，而可靠性设计前由于系统各部分是串联的，并且失效率都服从指数分布，因此整个系统的失效率函数是一条直线。图 9 在时间趋于无穷大时对应的数值为系统平均寿命，可靠性设计前系统的平均寿命约为 300 万小时，经过可靠性设计后，提高到约 425 万小时。通过对 3 个图形比较分析可以得出，可靠性设计明显提高了直流配电盒的系统可靠性。

4 结束语

可靠性是产品质量的重要指标，本文给出了直流配电盒的可靠性设计方案，并运用马尔可夫随机过程理论对系统进行可靠性分析，建立了数学模型。马尔可夫随机过程能够较为真实地描述系统的实际工作情况。本文还使用 Matlab/Simulink 仿真技术，对数学模型给出仿真结果，可以直观地观察到可靠性设计带来的可靠性提升程度。对研究系统可靠性分析和仿真有很大的参考意义。

(下转第 256 页)