文章编号:1671-4598(2021)07-0218-05 DOI:10.16526/j.cnki.11—4762/tp.2021.07.043 中图分类号:TP273 文献标识码:A

双余度核电 DEH 设计与马尔科夫模型分析

牛其磊，张卫东
（上海交通大学 电子信息与电气工程学院，上海 200240）

摘要：可靠性在核电汽轮机数字电液控制系统（Digital electro—hydraulic control system，DEH）质量中至关重要；从提升系统可靠性的角度出发，分析了核电 DEH 的工作原理，设计了基于异构处理器的核电 DEH 系统，给出了 DEH 的系统架构、硬件构成及双余度设计方案；基于马尔科夫过程理论建立了双余度核电 DEH 的可靠度函数模型，结合可靠性框图及双余度系统状态转移图对核电 DEH 做了失效分类；引入失效率、维修率、共因失效因子与诊断覆盖率等参数，建立了状态转移方程，分析了系统在不同生命周期基于马尔科夫模型的可靠度；通过一个实例检验了双余度核电 DEH 的可靠性，为工程设计人员提供了指导与参考。

关键词：马尔科夫；双余度；数字电液控制系统；失效率；共因失效；可靠度；截尾寿命试验

Design and Markov Model Analysis of Dual Redundancy Nuclear Power DEH

NIU Qilei，ZHANG Weidong
（School of Electronic Information and Electrical Engineering，Shanghai Jiaotong University，Shanghai 200040，China）

Abstract：Reliability is very important in the quality of the digital electro—hydraulic control system（DEH）for nuclear power steam turbines. From the perspective of improving system reliability，the working principle of nuclear power DEH was analyzed. And a nuclear power DEH system based on heterogeneous processors was designed，and the system architecture，hardware composition and dual redundancy design scheme of DEH were given. Based on Markov process theory，the reliability function model of dual redundancy nuclear power DEH was established，and the failure classification of nuclear power DEH was combined with the reliability block diagram and dual redundancy system state transition diagram. The state transfer equation was established by introducing the parameters such as failure rate，maintenance rate，common cause failure factor and diagnosis coverage rate，and the reliability of the system based on Markov model in different life cycles was analyzed. The reliability of double redundancy nuclear DEH is tested by an example，which provides guidance and reference for engineering designers.

Keywords：Markov；double redundancy；DEH；failure rate；common cause failure；reliability；truncation life test

0 引言

可靠性的研究早在 20 世纪初期就已经开始了，伴随着数理统计理论的发展，相关研究在 20 世纪中后期逐渐形成体系，标准不断完善，在工业上的应用也逐渐普及。核电汽轮机控制系统的可靠性预测即是其中受关注较多的一个领域。作为核电厂核心的汽轮机控制系统以往更多的使用常规 DCS 控制系统，但随着机组容量不断扩大，工业需求日益复杂，使用专用的汽轮机数字电液控制系统就显得尤为重要了[1-2]。汽轮机数字电液控制系统（digital electro—hydraulic control system，DEH）不仅肩负着数据采集、处理，汽轮机状态监视等任务，更承担着汽轮机转速的控制与调节，同时也要与常规 DCS 系统之间保持稳定的通讯与信息传输。仅仅依靠提高系统各部件质量已无法满足日益严苛的可靠性要求[3]。因此，设计一套可靠的核电 DEH 系统并对其可靠性进行分析就显得十分重要且必要。本文设计了基于异构处理器的核电 DEH，并分析了双余度核电 DEH 基于马尔科夫（Markov）的可靠度模型，结合失效率、维修率、共因失效因子、诊断覆盖率等参数综合研究了可靠性变化趋势，最后使用实例检验了双余度核电 DEH 的可靠性，为核电 DEH 的可靠性分析提供了一种更加全面精准的预测方法。

1 双余度核电 DEH 控制原理与设计

1.1 核电 DEH 控制原理

核电发电的原理就是由原子核反应堆释放的核能通过

收稿日期:2020-12-06； **修回日期**:2020-12-31。
基金项目:北京市自然科学基金项目(4162025)。
作者简介:牛其磊(1994-)，男，河南周口人，硕士研究生，主要从事自动化仪控设备开发、工业过程控制及系统可靠性分析方向的研究。
张卫东(1967-)，男，黑龙江大庆人，博士生导师，教授，主要从事智能控制、模式识别等理论研究及海洋机器人、智能电网等方向的研究。
引用格式:牛其磊，张卫东.双余度核电 DEH 设计与马尔科夫模型分析[J].计算机测量与控制，2021，29(7)：218-222.

一套动力装置将核能转为蒸汽的动能，进而转变为电能。而汽轮机即是以水汽为介质，并把水汽的热量变换为动能的大型旋转设备。汽轮机牵引发电机的同时，将动能转为电能。在核电发电系统里，汽轮机是必要的组件，因此控制汽轮机安全可靠的运转就变得至关重要。

DEH 是一种根据电网负荷变化来调整汽轮机进汽量以达到稳定汽轮机转速，平衡电网负荷的控制装置[4]。DEH 主要包括磁阻/霍尔型转速测量仪表、IO 模块、控制模块、电动执行机构等。DEH 的原理框图如图 1 所示。

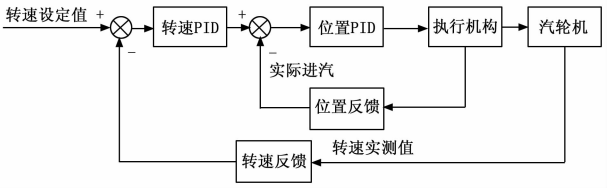

图 1　DEH 控制原理框图

转速仪表采集汽轮机转速值，经过 IO 模块调理为脉冲量信号，控制器将转速实测值与设定值比较后进行 PID 调节；汽轮机的转速输出调节作为位置调节回路的给定值，经过 IO 模块调理为电压信号，控制器通过将位置反馈值与设定值比较后进行 PID 运算产生最终驱动执行机构的模拟量输出信号，以满足稳定汽轮机转速的调节需求。

1.2　双余度核电 DEH 架构设计

如图 2 所示为某型双余度核电 DEH 设计方案，其使用快速处理控制器模块和混合型智能快速 IO 模块来完成对汽轮机的安全可靠调节。控制器可通过工业以太网连接上位机软件，进行监控数据的输入输出和组态策略的运算，并基于 IO 总线与快速 IO 模块互相交换数据，起到承上启下的作用。

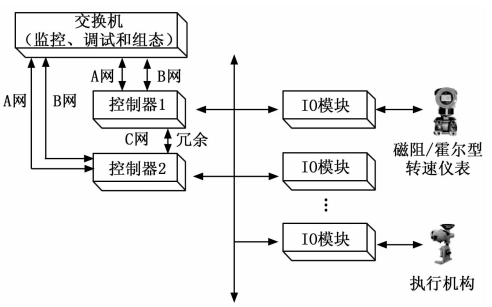

图 2　某型双余度核电 DEH 系统架构图

快速处理控制器模块采用三层 PCI 总线堆叠设计方案，第一层板卡通过总线接口和若干快速 IO 模块通讯，主要负责总线协议的处理和底层硬件接口的驱动；中间一层是嵌入式 x86 模块，主要通过 PCI 总线和另两块板卡交互数据，带 Linux 操作系统，负责组态逻辑运算、以太网通讯等功能；最上层是另一层总线接口板，主要负责与其他快速处理控制器模块之间的数据交互，并实现系统的扩展。控制器结构图如图 3 所示。

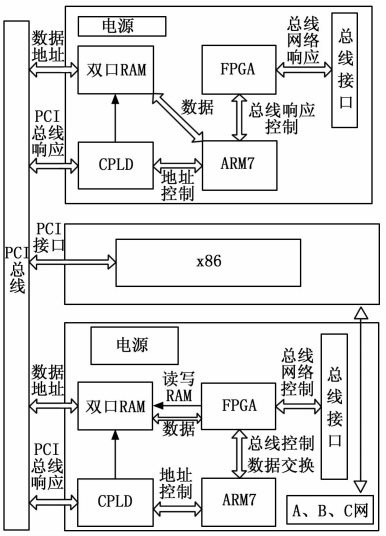

图 3　核电 DEH 控制器结构图

快速 IO 模块可实现转速采样、线性可变差动变压器位移传感器的 4～20 mA 电流采样、4～20 mA 电流输出、数字量输入输出等功能。快速 IO 模块结构图如图 4 所示。

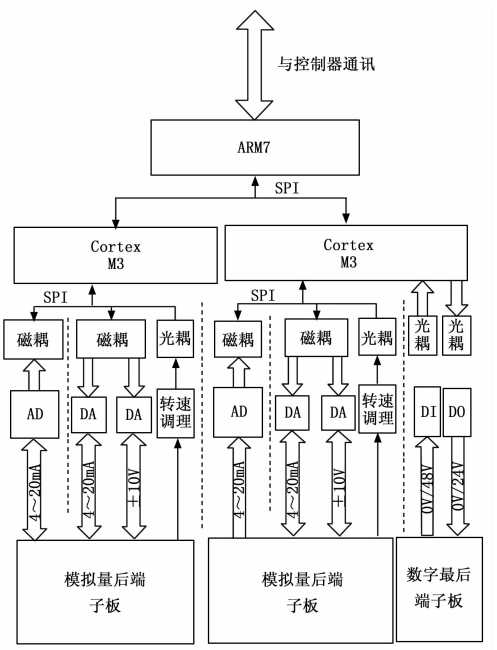

图 4　双余度核电 DEH 快速 IO 模块结构图

快速 IO 模块基于总线与控制器连接，模块上的 ARM7 负责并行总线通讯协议，2 块 Cortex M3 负责模拟量与数字量的输入输出，微控制器芯片与通道部分线路全部通过磁耦或者光耦隔离。

第一片 Cortex M3 负责处理 4 通道 4～20 mA 电流输入的模数转换和 4 路独立模拟量输出的数模转换。模拟量输出分别为 2 路 4～20 mA 电流（输出反馈）和 2 路±10 V 电压，±10 V 电压在后端子板上调理成±50 mA 电流信号。±50 mA 输出的电流信号通道带有输出反馈检测，以确保

输出回路工作正常。该 Cortex M3 同时还处理一路转速信号，转速信号通过后端子板调理成 3.3 V 方波，由微控制器计算频率。

第二片 Cortex M3 处理另外 4 路电流信号输入和 4 路模拟输出，以及全部的数字输入输出通道。模拟量输入输出与前一部分电路相同。12 路数字量输入通道经过后端子板处理内供电和外供电两种供电方式，将信号转换为 0 V/48 V电平信号，在快速 IO 模块上实现电平转换和采样，同时带有 10 ms 滤波，以避免现场干扰。8 路数字量输出通道由处理器发出指令，通过逻辑转换、输出驱动后，转换为 24 V电压，驱动后端子板上的继电器。

模拟端子板是该 DEH 中的一个子卡，主要作用是隔离现场和快速 IO 模块，保护快速 IO 模块不受损坏，以及根据现场需求配置快速 IO 模块输出并为快速 IO 模块提供必需的控制反馈，从而完成闭环控制。根据设计需求，后端子板含有 4 路电流输入通道，4 路模拟量输出通道（2 路 4～20 mA 和 2 路±50 mA）和 1 路转速通道，不同信号之间相互隔离，单独供电。同时后端子板提供 EMC 防护、热插拔冲击和其他保护。

数字量后端子板是阀门定位器的一个子卡，其在系统中的作用是根据控制器的数字输出指令产生继电器输出；接收现场开关信号，输出给控制器；另外提供 EMC 防护、热插拔冲击和其他保护。

整套双余度核电 DEH 的工作原理为：系统通过快速 IO 模块的转速通道接收来自汽轮机的转速值，通过控制器模块对频率做逻辑判断和运算，再由快速 IO 模块的模拟量输出通道来改变汽轮机的阀门开度的大小，同时通过快速 IO 模块的模拟量输入通道采样汽轮机的位移，实现闭环反馈，以实现稳定汽轮机速度的目标。快速处理控制器模块与快速 IO 模块等均采用冗余结构，互为冗余的两个模块一个处于正常工作状态，一个处于热备冗余状态，当处于工作状态的模块出现异常后将通过同步与状态检查机制及时检出，并自动切到处在热备冗余的模块，完成系统的无扰切换。

2 双余度核电 DEH 的 Markov 模型

2.1 求解 Markov 模型

如果某系统具有有限的状态个数，且其状态方程中的转移概率只和时移有关，和起点时刻无关，则可以用 Markov 模型的方法研究该系统状态变化规律。Markov 过程是看待系统变化的一种眼光，这是因为系统的变动往往可以看作是在若干个状态之间迁移[5]。Markov 模型可以实时地体现系统从运行到故障再到经过维修回到正常状态的一系列事件，既能反映系统设备之间的静态关系又能反映其动态关系，可靠性分析精度高。

图 5 为双余度核电 DEH 的 Markov 模型[6]，该模型包含 6 个状态，在图中分别用 6 个圆圈表示。分别是状态 0 为 OK（正常），状态 1 为 DDN（正常测出的危险失效），状态 2 为 DUN（正常未测出的危险失效），状态 3 为 FS（安全失效），状态 4 为 FDD（测出的危险失效），状态 5 为 FDU（未测出的危险失效）[7]。该结构的状态 0、1、2 都能够正常运行。当任意一个模块产生安全失效后，DEH 随即进入状态 3。在状态 1 和状态 2 时，DEH 由 1oo2 降级为 1oo1，这时对于 1oo1 的系统而言，如果产生安全失效，则进入状态 3；若发生危险失效，则系统进入状态 4 或状态 5。由于多通道的存在，共因失效的发生成为可能，当系统发生共因危险失效时，系统会从状态 0 转移到状态 4 或状态 5。此外，状态 1、3、4 都可以通过修复转移到状态 0。

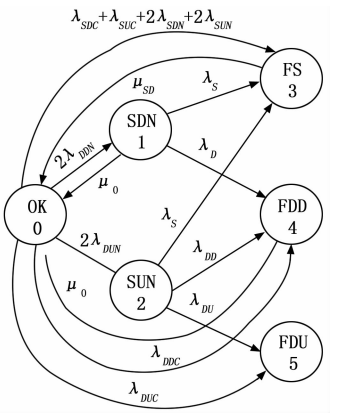

图 5 双余度核电 DEH 的 Markov 模型

其中，$\mu 0$ 为系统从检测到的危险失效转移到安全运行的几率；μSD 为维修率（h^{-1}）；λ 代表失效率，s 代表安全，D 代表危险，C 代表共因失效，N 代表正常，DD 代表可测的危险失效，U 代表不可检测；如参数 λsDc 表示检测出的共因安全失效率，其余参数可以此类推。各参数及相关衍生参数计算公式如表 1 所示。

表 1 可靠性参数含义表

参数/(h^{-1})	计算公式
λ^{SU}	$\lambda^{SU}=(1-Cs)\lambda^{S}$
λ^{SD}	$\lambda^{SD}=Cs\lambda^{S}$
λ^{SDC}	$\lambda^{SDC}=\beta\lambda^{SD}$
λ^{SUC}	$\lambda^{SUC}=\beta\lambda^{SU}$
λ^{SDN}	$\lambda^{SDN}=(1-\beta)\ \lambda^{SD}$
λ^{SUN}	$\lambda^{SUN}=(1-\beta)\ \lambda^{SU}$
λ^{DD}	$\lambda^{DD}=CD\lambda_D$
λ^{DU}	$\lambda^{DU}=(1-CD)\lambda_D$
λ^{DDC}	$\lambda^{DDC}=\beta\lambda^{DD}$
λ^{DUC}	$\lambda^{DUN}=\beta\lambda^{DU}$
λ^{DDN}	$\lambda^{DDN}=(1-\beta)\lambda^{DD}$
λ^{DUN}	$\lambda^{DUN}=(1-\beta)\lambda^{DU}$

其中，β 为共因失效因子；Cs 为安全覆盖因子；CD 为危险覆盖因子。

根据图 5 所示的 Markov 模型，双余度 DEH 系统状态转移矩阵如式（1）所示：

$$\boldsymbol{P}=\begin{bmatrix} 1-\sum & 2\lambda_{DDN} & 2\lambda_{DUN} & \lambda_{SC}+2\lambda_{SN} & \lambda_{DDC} & \lambda_{DUC} \\ \mu_0 & 1-\sum & 0 & \lambda_S & \lambda_D & 0 \\ 0 & 0 & 1-\sum & \lambda_S & \lambda_{DD} & \lambda_{DU} \\ \mu_{SD} & 0 & 0 & 1-\mu_{SD} & 0 & 0 \\ \mu_0 & 0 & 0 & 0 & 1-\mu_0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \tag{1}$$

式中，$\sum$ 表示该元素所在的行除此元素外其他元素的和。所有的模块在起始时刻均正常工作，则初始状态向量 $S_0=[1\quad 0\quad 0\quad 0\quad 0\quad 0]$。

2.2　基于 Markov 模型的可靠性

核电 DEH 的可靠性一般用 DEH 在指定的前提和指定的时刻，实现指定任务的几率表示[8]。如果 DEH 的寿命满足负指数分布特征，那么其可靠度如式（2）所示：

$$R(t)=e^{-\lambda t} \tag{2}$$

由上述分析可知，系统在时刻 t 处于状态 $n(n=0,1,2,3,4,5)$ 的概率为：

$$P_n(t)=\sum_{i=0}^{5}p_i^0 p_{in}(t) \tag{3}$$

其中：p_i^0 为系统在初始时刻处于状态 i 的概率，$p_{in}(t)$ 为系统在时刻 t 从 i 变成 n 状态的概率。

DEH 处于 0、1、2 均能够安全运行，所以 DEH 安全运行的概率为：

$$P_{ok}(t)=p_o(t)+p_1(t)+p_2(t) \tag{4}$$

DEH 可以细分为多个分系统，各个部分又由多个串、并联模块构成，所以基于 Markov 模型的可靠性为：

$$R_{\text{markov}}=1-\prod_{i=1}^{n}\left\{1-\prod_{j=1}^{m_i}p_{ok}^{ij}(t)R_{ij}(t)\right\}=$$
$$1-\prod_{i=1}^{n}\left\{1-\prod_{j=1}^{m_i}p_{ok}^{ij}(t)e^{-\lambda_{ij}t}\right\} \tag{5}$$

其中：R_{markov} 为基于 Markov 模型的可靠度，p_{ok}^{ij} 为分系统 i 的模块 j 在时刻 t 安全运行的概率；λ_{ij} 指分系统 i 的模块 j 的寿命满足参数为 λ_{ij} 的指数分布。

3　可靠性预测与试验分析

3.1　双余度核电 DEH 可靠性预测

由上述分析可知，某型双余度核电 DEH 共由 4 个部分组成，可进一步将每个部分划分为 3 个模块，如图 6 为其可靠性结构示意图。

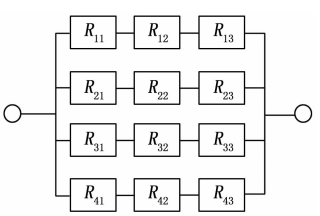

图 6　某型双余度核电 DEH 可靠性结构示意图

以该型 DEH 中分系统 1 为例，其余分系统可类比分析。依据国军标查询对应的失效率，获得分系统 1 各参数如表 2 所示。

表 2　双余度 DEH 分系统 1 可靠性参数值

参数	模块 1	模块 2	模块 3
$\lambda_S/(10^{-5}/\text{h})$	1.624	1.235	0.846
$\lambda_D/(10^{-5}/\text{h})$	6.896	5.394	7.256
Cs	0.990	0.990	0.995
CD	0.999	0.998	0.999
β	0.005	0.003	0.004
$\mu_0/(\text{h}^{-1})$	0.020	0.018	0.015
$\mu_{SD}/(\text{h}^{-1})$	0.025	0.015	0.013

设定 DEH 各模块在启动时为安全运行状态，根据表 2 中的数据，使用公式（4）求出该型 DEH 分系统 1 各个模块在时刻 t 为安全运行的几率，然后将结果代入（5）式，得出该型 DEH 分系统 1 的可靠性随时间变化的曲线[9]如图 7 所示。

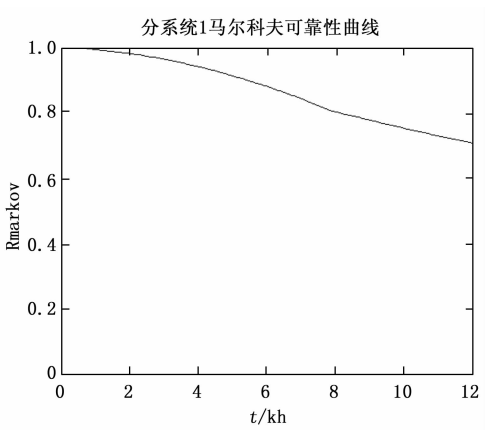

图 7　分系统 1 的 Markov 可靠度变化曲线

由图 7 可以看出，该型 DEH 的可靠度随着时间的增加而逐渐减小，且在其不同生命周期可靠度与时间并非线性化关系。在 DEH 安全运行的情况下，随着时间推移，DEH 的寿命超过当前时间的几率越来越小。

3.2　双余度核电 DEH 可靠性评估试验

在可靠性分析的基础上设计试验进一步评估 DEH 可靠性。考虑到核电的特殊性，为使实验结果尽可能接近 DEH 的真实寿命状况，对其进行无替换定时截尾寿命试验。抽取同一批生产的五套某型核电 DEH，在试验场地使用信号源、万用表等仪器模拟现场工况进行测试。截尾时间选取为 350 小时、700 小时、1 400 小时、2 100 小时、2 800 小时。

根据可靠性试验相关理论[10]，无替换定时截尾寿命试验如图 8 所示。

总试验时间为：

$$T_{r,n}=\sum_{i=1}^{r}t_{(i)}+(n-r)\tau \tag{6}$$

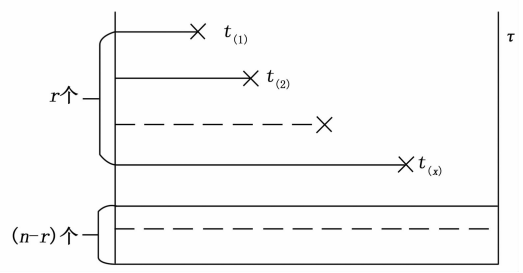

图 8 无替换定时截尾寿命试验

式中，n 为子样系统的个数，$t_{(i,i=0,1,2,\ldots)}$ 为寿命数据，τ 为截尾时间，r 为失效个数。

平均寿命为：

$$\hat{\theta} = \frac{T_{r,n}}{r} \tag{7}$$

预定任务时间 t_0 内的可靠度估计为：

$$\hat{R}(t_0) = e^{-t_0/\hat{\theta}} \tag{8}$$

根据试验得到的数据，绘制系统在每次试验总实验时间内的可靠度变化曲线如图 9 所示。

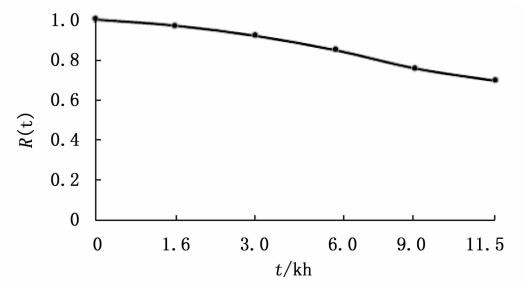

图 9 某型核电 DEH 可靠度评估曲线

从图 9 与图 7 的对比可以大致看出实际系统的可靠度变化趋势与基于 Markov 模型的预测基本一致。验证了基于 Markov 模型分析核电 DEH 可靠性的可行性。根据可靠性预测与评估试验结果，工程设计与实施人员在产品投入使用前进行老化试验，检出不合格模块，使产品进入稳定工作期，在其运行期间定期进行巡检，以此来提高核电 DEH 的可靠性，延长系统的寿命。

4 结束语

本文基于异构处理器设计双余度核电 DEH，通过隔离、防护、同步、冗余等措施保证了系统的安全可靠运行。核电汽轮机的 DEH 可靠性研究本身是一项复杂的工程，在研究其可靠性时借助于 Markov 过程模型，将 DEH 的工作状况进行划分，可以有效地评估 DEH 在不同工况之间的转移概率，进而可以针对系统的可靠性进行量化分析。从截尾寿命试验结果来看，基于 Markov 模型的可靠性分析更能反映系统的实际情况。相较于传统的可靠性框图和故障树分析方法，不仅综合考虑了失效率、维修率、诊断覆盖率等因素，而且可以大大简化计算，同时确定了 DEH 的多类可靠性参数，预测精度更高。对于提高核电 DEH 的工程应用水准以及确保核电安全运转都具有现实意义。

参考文献：

[1] 王 虎，李少华，赖福生，等. 基于马尔科夫过程的核电厂 DCS 可靠性分析方法 [J]. 黑龙江电力，2011，5 (2)：364－367.

[2] 何 程，秦 丽，于丽霞. 基于 Copula 的 MEMS 加速度计在振动环境下的可靠性评估 [J]. 仪表技术与传感器，2018，4 (46)：46－54.

[3] 刘克亚. 基于 1553B 总线三冗余飞行控制系统设计与可靠性研究 [J]. 计算机测量与控制，2018，26 (1)：119－123.

[4] 李 京，张永洋. 基于马尔科夫模型的船用柴油机电子调速器可靠性分析 [J]. 柴油机，2016，38 (6)：11－14.

[5] 陈 庚，蒋 敏，卢其龙. 基于马尔科夫过程的测控装备可靠性分析 [J]. 控制理论与应用，2018，37 (7)：8－12.

[6] 王华忠. 工业过程控制及安全技术 [M]. 北京：电子工业出版社，2020.

[7] 马 超，戴小氏，郭 勇. 四余度飞控计算机设计及基于马尔可夫模型的可靠性分析 [J]. 信息通信，2019 (10)：10－11.

[8] 尹 行，张文瀚，冯 力，等. 基于多元 Copula 函数的冗余系统可靠性模型研究 [J]. 测控技术，2020，39 (3)：39－45.

[9] 石良臣. MATLAB/Simulink 系统仿真超级学习手册 [M]. 北京：人民邮电出版社，2017.

[10] 胡湘洪，高 军，李 劲. 可靠性试验 [M]. 北京：电子工业出版社，2015.

(上接第 217 页)

[2] 李长星，王 波，胡振华. 基于 FPGA 和 ARM 的实时数据采集显示系统 [J]. 现代电子技术，2014，37 (3)：151－154.

[3] 杨 磊，刘美枝，高 海，等. 基于 FPGA 和 ARM 的高速数据采集系统设计 [J]. 山西大同大学学报，2017，33 (6)：32－36.

[4] 张朝元，邵高平，汪 洋. 基于 Zynq－7000 的嵌入式 Linux 移植 [J]. 电子科技，2018，31 (1)：9－11.

[5] 邢艳芳，朱金付，周晓梅. 基于 Zynq 多核运行设计 [J]. 计算机技术与发展，2018，28 (3)：60－62.

[6] 黄 禹，平佳伟. 基于 USB3.0 的小型化通用测试平台设计 [J]. 计算机测量与控制，2018，26 (7)：48－51.

[7] 罗 铿，平佳伟. 基于 ARM 的全自动数据采集系统的设计与实现 [J]. 计算机测量与控制，2016，24 (4)：159－162.

[8] 吴华侨. 基于 Zynq 平台的嵌入式操作系统实时性优化设计 [D]. 哈尔滨：哈尔滨理工大学，2018.

[9] 吕俊杰. 基于 ZYNQ 的数据中心接口单元设计 [D]. 合肥：中国科学技术大学，2018.

[10] 路明怀. Linux 服务器多网卡下的负载均衡研究与实现 [D]. 长沙：国防科学技术大学研究生院，2006.