第 39 卷 第 3 期 核 动 力 工 程 Vol.39. No.3
2 0 1 8 年 6 月 Nuclear Power Engineering Jun. 2018

文章编号：0258-0926(2018)03-0095-05; doi:10.13832/j.jnpe.2018.03.0095

数字化安全级 DCS 紧急停堆系统共因失效分析

马 权，罗 琦，宋小明，刘艳阳

中国核动力研究设计院核反应堆系统设计技术重点实验室，成都，610213

摘要：以 2oo3 架构数字化安全级分布式控制系统（DCS）紧急停堆系统为研究对象，采用 Markov 方法对其建立可靠性模型，分别计算并对比了考虑共因失效和不考虑共因失效 2 种情况下紧急停堆系统的拒动概率，同时对系统拒动概率相对于共因失效因子变化的敏感性进行了重点分析。结果表明，拒动概率随着共因失效因子的增加而变大，因此，在系统设计中需采取有效措施对冗余系统的共因失效进行控制，降低共因失效因子，从而提高紧急停堆系统的可靠性。

关键词：数字化安全级分布式控制系统（DCS）；紧急停堆系统；2oo3 架构；共因失效

中图分类号：TL362 文献标志码：A

Common Cause Failure of Digital Safety Level DCS Emergency Shutdown System

Ma Quan, Luo Qi, Song Xiaoming, Liu Yanyang

Science and Technology on Reactor System Design Technology Laboratory, Nuclear Power Institute of China, Chengdu, 610213, China

Abstract: This paper takes the digital safety level DCS emergency shutdown system which used 2-out-of-3 architecture as the research object, and establishes the reliability model of the system by the method of Markov. The average probability of failure on demand, as so called the PFD_{avg}, under two cases of common cause failure and non common cause failure consideration are calculated and compared. In addition, it turns out that the PFDavg changes to be bigger with the increasing of the factor of common cause failure. Thus, in order to decrease the factor of common cause failure, it is necessary to control the common cause failure by some effective measures when designing the system to improve the reliability of RTS.

Key words: Digital safety level distributed control system (DCS), Emergency shutdown system, 2-out-of-3 structure (2oo3), Common cause failure

0 引 言

实际工程应用中，往往通过设计多通道并行冗余提高系统设备可靠性。然而，由于共因失效的存在，并行冗余设备的可靠性会大幅降低。因此，冗余系统共因失效分析是实际工程中特别是核设备工程中亟待解决的问题之一[1]。

数字化安全级分布式控制系统（DCS）相当于核反应堆装置的神经中枢，能够在危险情况下实现安全停堆以及事故后的监测，对核反应堆装置的安全稳定运行起着至关重要的作用。紧急停堆系统作为数字化安全级 DCS 的重要组成部分，其可靠性问题一直受到广泛重视，基本都设计为多通道冗余系统以增加其可靠性，然而，由于共因失效的机理使得紧急停堆系统的可靠性大大降低。对其进行共因失效分析显得尤为重要。

本文主要针对 2oo3 架构数字化安全级 DCS 紧急停堆系统进行建模，分析数字化安全级 DCS 紧急停堆系统拒动概率随着共因失效因子变化的趋势，并提出有效控制系统共因失效影响的措施及方法。

1 2oo3 架构数字化安全级 DCS 紧急停堆系统

数字化安全级 DCS 紧急停堆系统功能框图

收稿日期：2017-09-10；修回日期：2018-04-25

作者简介：马 权（1981—），男，高级工程师，硕士，现从事安全级 DCS 研发和供货工作

如图 1 所示，包括 3 个保护组，每个保护组由信号预处理系统（PIPS）和保护处理系统（RPC）以串联的方式构成。PIPS 对现场传感器或仪表信号进行采集和信号预处理，转换成标准工业信号发送给 RPC 进行逻辑运算和信号处理。系统逻辑表决器对 RPC 处理后的信号进行 2oo3 逻辑表决，最终输出紧急停堆信号。

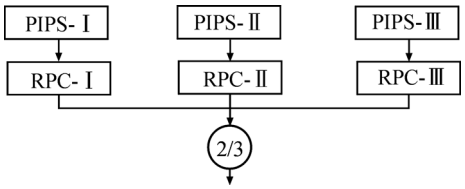

图 1 2oo3 架构数字化安全级 DCS 紧急停堆系统功能框图

Fig.1 Block Diagram of Digital Safety Level DCS Emergency Shutdown System with 2oo3 Structure

2 失效和共因失效机理

失效为设备失去完成规定功能的能力[2]，共因失效（共同原因失效）是指由相同原因造成多个相同部件、组件、单元或系统发生失效。各通道失效和共因失效的关系如图 2 所示。

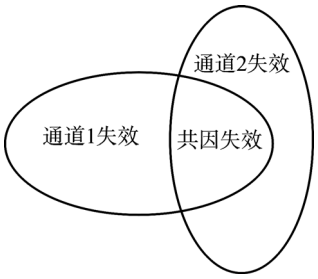

图 2 各通道失效和共因失效的关系

Fig. 2 Relationship of Common Cause Failures to Failures of Individual Channels

传统的可靠性分析方法仅仅考虑功能模块的总失效率 λ，随着对反应堆保护系统可靠性与安全性的重视程度的不断增加，同时也随着功能安全理念的引入，对于失效率进行了更深层次的细化。本文将功能模块的失效率 λ 细分为如下 8 个部分[3]：

$$\begin{aligned}\lambda &= \lambda_{\mathrm{S}} + \lambda_{\mathrm{D}} = (\lambda_{\mathrm{SD}} + \lambda_{\mathrm{SU}}) + (\lambda_{\mathrm{DD}} + \lambda_{\mathrm{DU}}) \\ &= (\lambda_{\mathrm{SC}} + \lambda_{\mathrm{SN}}) + (\lambda_{\mathrm{DC}} + \lambda_{\mathrm{DN}}) \\ &= (\lambda_{\mathrm{SDN}} + \lambda_{\mathrm{SDC}} + \lambda_{\mathrm{SUN}} + \lambda_{\mathrm{SUC}}) + \\ &\quad (\lambda_{\mathrm{DDN}} + \lambda_{\mathrm{DDC}} + \lambda_{\mathrm{DUN}} + \lambda_{\mathrm{DUC}}) \end{aligned} \tag{1}$$

式中，下标：S 表示安全失效；D 表示危险失效；SD 表示安全可检测失效；SU 表示安全不可检测失效；DD 表示危险可检测失效；DU 表示危险不可检测失效；SC 表示安全共因失效；SN 表示安全非共因失效；DC 表示危险共因失效；DN 表示危险非共因失效；SDN 表示安全可检测非共因失效；SDC 表示安全可检测共因失效；SUN 表示安全不可检测非共因失效；SUC 表示安全不可检测共因失效；DDN 表示危险可检测非共因失效；DDC 表示危险可检测共因失效；DUN 表示危险不可检测非共因失效；DUC 表示危险不可检测共因失效。

3 2oo3 架构数字化安全级 DCS 紧急停堆系统可靠性分析

3.1 Markov 模型的建立

通过对数字化安全级 DCS 紧急停堆系统进行分析，建立 Markov 模型如图 3 所示。

对数字化安全级 DCS 紧急停堆系统的状态转移图进行整理，得到相应的转移矩阵 $\boldsymbol{P}$ 如下（Σ 为所在行的其余列的失效率数值之和）：

$$\boldsymbol{P}=\begin{bmatrix}
1-\Sigma & 3\lambda_{\mathrm{SDN}} & 3\lambda_{\mathrm{SUN}} & 3\lambda_{\mathrm{DDN}} & 3\lambda_{\mathrm{DUN}} & 0 & 0 & 0 & 0 & \lambda_{\mathrm{SC}} & \lambda_{\mathrm{DDC}} & \lambda_{\mathrm{DUC}} \\
\mu_0 & 1-\Sigma & 0 & 0 & 0 & 2\lambda_{\mathrm{DDN}} & 2\lambda_{\mathrm{DUN}} & 0 & 0 & 2\lambda_{\mathrm{SN}}+\lambda_{SC} & \lambda_{\mathrm{DDC}} & \lambda_{\mathrm{DUC}} \\
0 & 0 & 1-\Sigma & 0 & 0 & 0 & 0 & 2\lambda_{\mathrm{DDN}} & 2\lambda_{\mathrm{DUN}} & 2\lambda_{\mathrm{SN}}+\lambda_{SC} & \lambda_{\mathrm{DDC}} & \lambda_{DUC} \\
\mu_0 & 0 & 0 & 1-\Sigma & 0 & 2\lambda_{\mathrm{SDN}} & 0 & 2\lambda_{\mathrm{SUN}} & 0 & \lambda_{\mathrm{SC}} & 2\lambda_{\mathrm{DN}}+\lambda_{\mathrm{DC}} & 0 \\
0 & 0 & 0 & 0 & 1-\Sigma & 0 & 2\lambda_{\mathrm{SDN}} & 0 & 2\lambda_{\mathrm{SUN}} & \lambda_{\mathrm{SC}} & 2\lambda_{\mathrm{DDN}}+\lambda_{\mathrm{DDC}} & 2\lambda_{\mathrm{DUN}}+\lambda_{\mathrm{DUC}} \\
\mu_0 & 0 & 0 & 0 & 0 & 1-\Sigma & 0 & 0 & 0 & \lambda_{\mathrm{S}} & \lambda_{\mathrm{D}} & 0 \\
\mu_0 & 0 & 0 & 0 & 0 & 0 & 1-\Sigma & 0 & 0 & \lambda_{\mathrm{S}} & \lambda_{\mathrm{DD}} & \lambda_{\mathrm{DU}} \\
\mu_0 & 0 & 0 & 0 & 0 & 0 & 0 & 1-\Sigma & 0 & \lambda_{\mathrm{S}} & \lambda_{\mathrm{D}} & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1-\Sigma & \lambda_{\mathrm{S}} & \lambda_{\mathrm{DD}} & \lambda_{\mathrm{DU}} \\
\mu_{\mathrm{SD}} & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1-\Sigma & 0 & 0 \\
\mu_0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1-\Sigma & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{bmatrix} \tag{2}$$

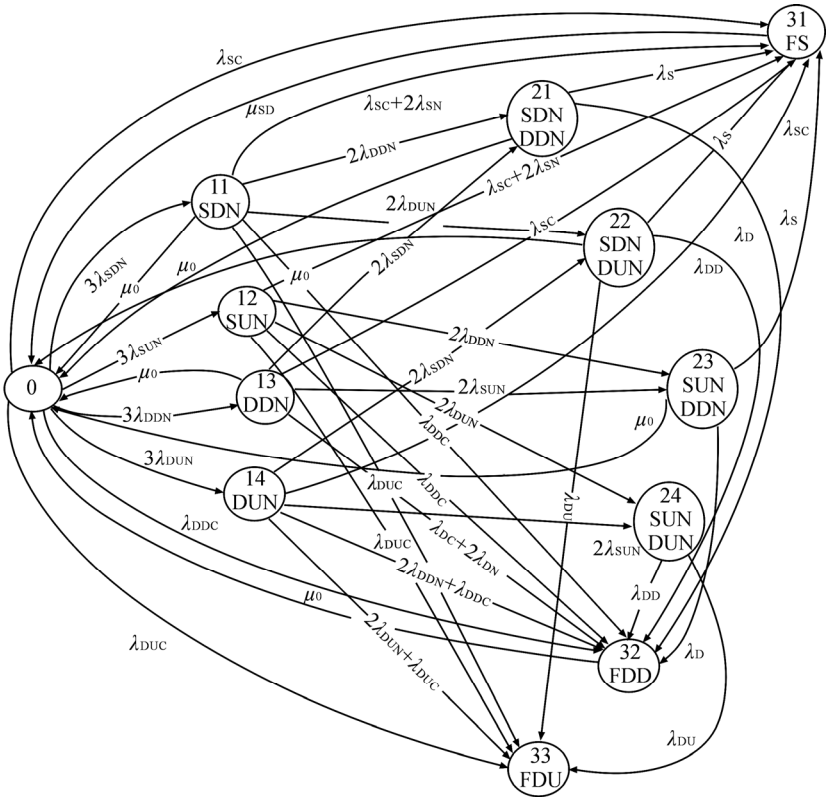

图 3　2oo3 架构数字化安全级 DCS 紧急停堆系统的状态转移图

Fig. 3　Markov Model of Digital Safety Level DCS Emergency Shutdown System with 2oo3 Structure

μ_0—维修率；μ_{SD}—系统误停堆后的重启率；FS—发生安全失效即误动作；FDD—发生危险可检测失效即可检测拒动失效；FDU—发生危险不可检测失效即不可检测拒动失效

表 1　模块可靠性参数值

Table 1　Reliability Data of Module

序号	模块	总失效率 /10^{-9}h^{-1}	安全失效率 /10^{-9}h^{-1}	安全失效诊断覆盖率	危险失效率 /10^{-9}h^{-1}	危险失效诊断覆盖率	无影响失效率 /10^{-9}h^{-1}
1	主控模块	2176.06	974.35	0.9860	294.20	0.9865	934.51
2	扩展模块	1637.54	723.45	0.9666	197.24	0.9758	716.85
3	模拟量输入模块	3081.81	1867.19	0.9781	382.87	0.9707	831.75
4	开关量输出模块	3653.47	1698.68	0.9876	208.60	0.9851	1746.19

3.2　2oo3 架构数字化安全级 DCS 紧急停堆系统拒动概率

通过求解 Markov 模型来计算系统拒动概率，具体的求解过程如下：

首先，将 2oo3 架构数字化安全级 DCS 紧急停堆系统的初始矩阵定义为 S_0：

$$S_0=\begin{bmatrix}1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0\end{bmatrix} \tag{3}$$

初始矩阵 S_0 表示系统在 0 时刻处于状态 0 的概率为 100%。通过式（4）可以计算系统从状态 0 开始，经过时间 n 的状态矩阵：

$$S_n=S_0\times P^n=\begin{bmatrix}S_{n0} & S_{n11} & S_{n12} & S_{n13} & \cdots & S_{n31} & S_{n32} & S_{n33}\end{bmatrix} \tag{4}$$

式中，P^n 表示状态矩阵 P 的 n 次幂。

如式（5）所示，再将式（4）状态矩阵中的 S_{n32} 和 S_{n33} 相加，可以得到系统在第 n 小时的危险失效概率 $P_{FD,n}$：

$$P_{FD,n}=S_{n32}+S_{n33} \tag{5}$$

系统工作 n 小时的平均危险失效概率，即拒动概率 $P_{FD,avg}$ 的计算原理如下：

$$P_{FD,avg}=\frac{1}{n}\int_0^n P_{FD,n}\mathrm{d}t \tag{6}$$

本文参考相关项目，得出数字化安全级 DCS 紧急停堆系统的计算基础数据如表 1 所示。

失效率的获得是依据各个模块的元器件，参照 SN 29500 标准采用应力分析法获得。以集成电路为例进行说明，在 SN 29500 标准中，集成电路主要分为模拟集成电路和数字集成电路，该标准将集成电路分成了以下 4 类进行失效率预计计算：

（1）具有一定范围工作电压的模拟集成电路，包括运算放大器、电压比较器和电压监控器等元器件。

（2）除（1）类外，在固定工作电压下运行的其余的模拟集成电路，如电压基准。

（3）基于互补金属氧化物半导体（CMOS） B 系列的数字集成电路。

（4）除（3）类以外的所有数字集成电路。

以（1）类集成电路为例，依据标准 SN 29500 中（1）类集成电路失效率预计计算的描述，该类集成电路的失效率计算公式为：

$$\lambda = \lambda_{\mathrm{ref}} \cdot \pi_{\mathrm{U}} \cdot \pi_{\mathrm{T}} \cdot \pi_{\mathrm{D}} \cdot \pi_{\mathrm{W}} \cdot \pi_{\mathrm{F}} \qquad (7)$$

式中，λ_{ref} 为参考条件下的元器件失效率；π_{U} 为电压系数，用以计算电压降额对元器件失效率的影响；π_{T} 为温度系数，用以计算温度降额对元器件失效率的影响；π_{D} 为漂移敏感系数，用以计算模拟电路或含有模拟电路的混合电路因漂移敏感导致失效率增加的值；π_{W} 为应力剖面系数，与元器件在设备运行期间是否受应力持续作用有关；π_{F} 为早期失效期系数，与元器件工作运行时间有关。

参考元器件数据手册和标准 SN 29500 中集成电路相关描述，结合核安全级 DCS 紧急停堆系统实际运行情况，对其失效率各个应力系数进行预计，得到失效率参数。

通过评估，2oo3 架构数字化安全级 DCS 紧急停堆系统的可检测共因失效因子 β_{D}=0.75%，不可检测共因失效因子 β=1.5%。假设定期试验周期为 3 个月，并将相关基础数据代入计算，即可得到考虑共因失效的系统拒动概率为：$P_{\mathrm{FD,avg}}=1.76\times10^{-6}$；不考虑共因失效时，系统拒动概率为：$P_{\mathrm{FD,avg}}=5.32\times10^{-8}$。

假设数字化安全级 DCS 紧急停堆系统的工作时间为 1 个定期试验周期，在各项参数不变的条件下，数字化安全级 DCS 紧急停堆系统考虑和不考虑共因失效时，$P_{\mathrm{FD,avg}}$ 随工作时间呈线性递增关系，曲线分别如图 4 和图 5 所示。

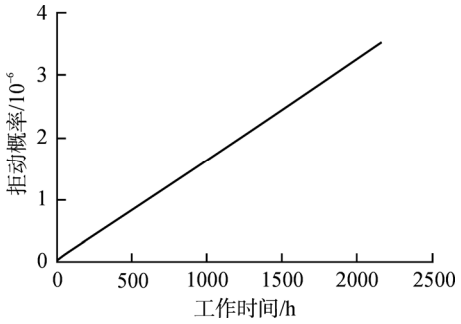

图 4 系统 $P_{\mathrm{FD,avg}}$ 随工作时间变化的曲线（考虑共因失效）

Fig. 4 Curve of $P_{\mathrm{FD,avg}}$ Changes with Work Time (Common Cause Failure)

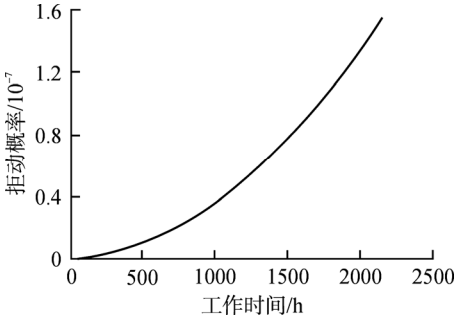

图 5 系统 $P_{\mathrm{FD,avg}}$ 随工作时间变化的曲线（不考虑共因失效）

Fig. 5 Curve of $P_{\mathrm{FD,avg}}$ Changes with Work Time (without Common Cause Failure)

4 拒动概率对共因失效因子的敏感性分析

本文在分析 2oo3 架构数字化安全级 DCS 紧急停堆系统拒动概率对共因失效因子的敏感性时，假设系统的其他参数不变，分析不同共因失效参数对系统 $P_{\mathrm{FD,avg}}$ 的影响，得到数字化安全级 DCS 紧急停堆系统的 $P_{\mathrm{FD,avg}}$ 随着共因失效因子的变化曲线（图 6）。从图 6 中可知，数字化安全级 DCS 紧急停堆系统 $P_{\mathrm{FD,avg}}$ 随着共因失效因子增大而变大。

5 结束语

本文使用 Markov 方法，首先对 2oo3 架构数字化安全级 DCS 紧急停堆系统建立可靠性模型，代入相关的基础数据，计算得到了考虑共因失效

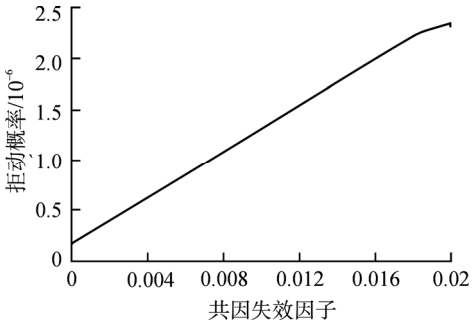

图 6　系统 $P_{FD,avg}$ 随共因失效因子变化曲线

Fig. 6　Curve of $P_{FD,avg}$ Changes with Factor of Common Cause Failure

与否 2 种情况下系统拒动概率随着定期试验周期的变化曲线。通过比较发现：在定期试验周期 3 个月时，系统拒动概率在不考虑共因失效的情况下比考虑共因失效时大约低 2 个数量级。此外，通过改变系统共因失效因子的大小，分析共因失效因子对系统拒动概率的影响，结果表明，拒动概率随着共因失效因子的增加而变大。可见，降低共因失效因子可有效提高 2oo3 架构数字化安全级 DCS 紧急停堆系统的可靠性。

为控制冗余系统的共因失效，给出如下建议措施：

（1）对系统的冗余部分（相同部件或通道）采用多样化设计，从而增加冗余部件或通道的差异性，以降低共因失效发生的概率。

（2）将冗余单元、部件隔离，让冗余部分保持相对的独立性，如：对冗余单元、部件进行物理隔离和电气隔离，防止故障蔓延。

（3）强化设计，可针对系统不同的应用环境和功能，采用专门的技术设计方案，即使用可靠性更高的元器件，系统使用元器件失效率越低，系统共因失效的失效率也相对低。

参考文献：

[1] 方云根，曾小青，王刚. 轨道交通列控系统共因失效分析[J]. 上海交通大学学报，2015, 49(7): 1052-1057.

[2] 中华人民共和国国家质量监督检验检疫总局，中国国家标准化管理委员会. 电气/电子/可编程电子安全相关系统的功能安全 第六部分: GB-T20438 [S]. 北京：中国标准出版社，2006:41-42.

[3] 张庆，马权，许标，等. 基于马尔可夫法的安全级 DCS 功能安全分析[J]. 仪器仪表用户，2016, 23(10): 77-81.

（责任编辑：马　蓉）