doi:10.3969/j.issn.1673-9833.2013.03.013

核电站数字化仪控系统的安全预警

刘 华[1]，阳小华[2]，刘 杰[2]，刘朝晖[2]，吴取劲[2]

（1.南华大学 电气工程学院，湖南 衡阳 421001；2.南华大学 计算机科学与技术学院，湖南 衡阳 421001）

摘 要：核电站数字化仪控系统存在系统风险。基于安全性理论，风险形成是一个传导过程，针对仪控系统失效这一概率事件，提出一级预警和二级预警的概念。基于特征向量的安全预警，可以合理描述系统风险的各种情况，并提高对DCS仪控系统问题的预警时间裕量，增加核电站的安全及可靠性。

关键词：数字化仪控系统；安全；预警

中图分类号：TP27 **文献标志码**：A **文章编号**：1673-9833(2013)03-0061-04

Early Safety Warning on Digital Control System of Nuclear Power Station

Liu Hua[1]，Yang Xiaohua[2]，Liu Jie[2]，Liu Zhaohui[2]，Wu Qujing[2]

(1. School of Electrical Engineering, University of South China, Hengyang Hunan 421001, China；
2. School of Computer Science and Engineering, University of South China, Hengyang Hunan 421001, China)

Abstract: The digital instrument control system of nuclear power station exists risk. Based on the theory of safety, the risk forming is a conduction process. For the failure probability of instrument control system, puts forward the concept of the first and second level of early warning. The safety early warning is based on feature vector. It is reasonable to describe system risk situations. The warning time of DCS instrument control system is improved. The safety and reliability of nuclear power plant are increased.

Keywords: DCS I&C system; safety; safety warning

核电站数字化仪控系统是数字化技术在核电站的集中应用及体现[1]。安全、稳定、可靠是核电站的本质需求和要求，因此数字化仪控系统的安全、稳定、可靠运行是其在核电站应用的必然要求[2]。

目前，在核电领域，采用数字化仪表与控制系统是先进型反应堆的一个重要特征。数字化系统通过增加硬件可靠性和稳定性、减少人因失误、提高故障检测能力等方式大幅度提高核电站安全性。当前在运行核电站中正逐步采用数字系统来取代模拟仪控系统，而在建、筹建的核电项目中已经全面将数字技术整合到其设计中[3]。

1 系统安全性理论

处于运行状态的多输入多输出系统，是一个高度非线性、时变的系统。系统失效不是一个瞬态过程，一般经历从系统错误、系统缺陷、系统故障，最后到系统失效共4个阶段。

收稿日期：2013-04-10

基金项目：2011年湖南省高校科学研究重点基金资助项目（11A105），2011年湖南省自然科学基金资助项目（11JJ6047）

作者简介：刘 华（1979-），男，湖南衡阳人，南华大学讲师，工学硕士，主要研究方向为控制理论与核安全，
E-mail：lhsmile@163.com

通信作者：阳小华（1963-），男，湖南衡阳人，南华大学教授，博士生导师，主要从事核数据处理方面的研究，
E-mail：yangxiaohua@163.com

系统向外界传导释放数据和信息、能被外界感知的特性，称为系统可观测性。系统运行状态是多维向量，通过基于向量建立数学模型，系统能够从不稳定、不安全、风险态返回到安全、稳定态的特性[4]称为系统可控性。系统失效指系统不满足功能要求，偏离甚至失去对数据及控制的约束。

产生系统失效的原因多而复杂，但基于时间轴的角度，系统失效的产生不是突发性的，而是经过一段时间的积累，是系统故障或隐患的离散累加。处于运行状态的系统，只要满足系统可观测、可控性这2个特性，安全预警就可以实施。图1为系统风险的形成和传导的顺序图。

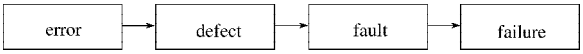

图1 系统风险的形成及传导

Fig. 1 Generating and conduction of system risk

系统失效必然导致系统风险。依照图1中error→defect→fault→failure顺序，可计算系统失效概率。

系统失效的概率计算：

P_1为系统错误引发系统缺陷的概率函数，对应P_1(error)= defect；

P_2为系统缺陷引发系统故障的概率函数，对应P_2(defect)= fault；

P_3为系统故障引发系统失效的概率函数，对应P_3(fault)= failure。

2 DCS仪控系统的安全预警

2.1 DCS I&C系统失效

核电站数字化仪控系统[5]，以下简称DCS I&C系统。由于采用DCS I&C系统后，核电站使用了大量微处理器（CPU）及对应的系统、I/O卡件等，经过逻辑设计将软件和硬件联系起来共同实现系统的预设功能。它可能会因设计中存在的不足或收到特殊的混合型输入的触发而导致失效。因此，虽然数字化仪控系统被普遍认为可以提高核电站的安全性和可靠性，但仍需要对数字化系统的安全运行进行有效监控。

DCS I&C系统在生命周期中的测试阶段，就已经清除很多错误，在核电站安装调试阶段又进一步经过软硬件联调、静态动态调试、带核运行调试和优化等，系统本身的安全、稳定、可靠性指标大幅提高，但不等于绝对安全。从概率的角度，始终存在一定的系统失效风险。例如版本升级带来问题、DCS系统通信协议的可靠性问题、系统模块间的不兼容、软件硬件接口的不稳定和实时约束问题[6]。

依据系统工程及可靠性理论，并非所有的故障都经历潜在故障再到功能故障的变化过程。核电站的系统故障也可分为潜在故障、显性故障及系统功能失效。众所周知，核电站的反应堆保护系统是核电站反应堆安全运行的重要保障。以此，核电站DCS I&C系统也需要一个保证其安全可靠运行的软件预警及监控系统。在核电站DCS I&C系统出现故障、失效等系列事件时，DCS I&C保护系统及时动作，防止问题进一步蔓延扩大，甚至提前预警，将隐患和潜在故障提早发现和清除。这就是DCS I&C系统的安全预警及报警。

2.2 DCS I&C系统安全预警特性

图2为系统预警特性参数说明。

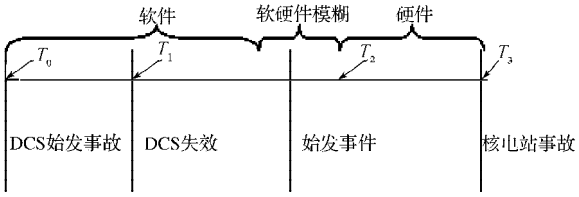

图2 系统预警特性

Fig. 2 Early warning characteristic of system

如图2所示，T_0为DCS系统始发事故的时间点；T_1为DCS系统失效产生的时间点；T_2为核电站始发事件的时间点；T_3为核电站事故的时间点。

$TT_0=T_1-T_0$，TT_0为DCS系统失效的一级预警；

$TT_1=T_2-T_1$，TT_1为DCS系统失效的二级预警；

$TT_2=T_3-T_2$，TT_2为始发事件造成核电站事故的时间延迟。

基于硬件、基于部件的失效是目前核电站安全分析的基本对象。将失效模式作用分析（failure mode and effects analysys, FMEA）与概率安全分析（probabilistic safety assessment, PSA）结合起来，被分析事物的时间区间从T_2到T_3。系统预警特性突出之处就在于把时间轴上的时间点从T_2再往左移动，提前到T_1甚至T_0。与此对应的，预警层次从硬件初始事故的报警提高到DCS系统失效二级预警甚至一级预警。

2.3 安全预警原理

安全预警的原理：核电站数字仪控系统对控制对象的实时监控，结合本身的自检验功能，与正常状态数据集合对比，找到不正常数据，得到符合预警的特征条件，认为系统处于偏离正常运行的状态或即将偏离，实现预警。

对控制对象的实时监控是利用硬件传感器、软件状态收集器，收集仪控系统的软件、硬件综合运行数据。仪控系统自检验是充分利用DCS控制功能

强大、监控对象及 IO 点数多的优点，在不干扰系统正常运行的情况下，不间断、自动检验系统的运行数据，发送校验指令，得到自检数据。把实时监控得到的仪控系统综合运行数据和系统自检得到的自检数据，与正常状态数据集合对比，就能发现仪控系统动态运行的不正常数据，进而得到特征条件，判断系统偏离正常运行。采用基于系统预警特征向量的数模模型可以抽象安全预警的特征条件。

2.4　安全预警方法

安全预警方法以核电站实际应用的数字化仪控系统为研究对象，提取出 DCS 仪控系统中能引发系统失效并可能进一步导致系统事故的关键要素，即表 1 的内容；采用系统仿真，将系统失效模型应用到基于系统故障的 DCS 操作搜索分析与预警监测中，针对 DCS 仪控系统达到提前预警的作用。

定义 1　系统预警运行特征向量 $\boldsymbol{X}$：能够抽象系统运行事件、状态的数据集合或数组

$$x_i=\begin{cases}1,\ \text{unsafe};\\ 0,\ \text{safe}。\end{cases}$$

其中，x_i 为特征向量 $\boldsymbol{X}$ 的元素，特征向量的元素取值为 1 或 0。系统风险传导及形成过程各阶段的特征向量反映各阶段、各时间段的系统安全性，系统的特征向量用来表示系统问题，特征向量中所有元素求和的结果作为系统风险的度量。特征元素为 1 对应的特征向量作为系统风险预警的判断依据。

如图 3，系统错误 error 对应特征向量 $\boldsymbol{E}_{1\times n}$，特征元素 $e_i,1\leqslant i\leqslant n$；系统缺陷 defect 对应特征向量 $\boldsymbol{D}_{1\times m}$，特征元素 $d_i,1\leqslant i\leqslant m$；系统故障 fault 对应特征向量 $\boldsymbol{F}_{1\times j}$，特征元素 $f_i,1\leqslant i\leqslant j$；系统失效 failure 对应特征向量 $\boldsymbol{R}_{1\times k}$，特征元素 $r_i,1\leqslant i\leqslant k$。

系统预警特征向量 $\boldsymbol{X}=\left[\boldsymbol{E}\mid\boldsymbol{D}\mid\boldsymbol{F}\mid\boldsymbol{R}\right]_{1\times(m+n+j+k)}$

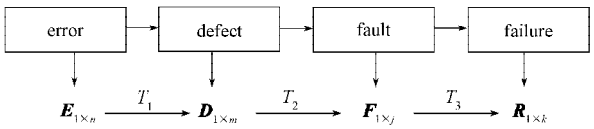

图3　系统风险各阶段的特征向量及提前预警时间

Fig. 3　Feuture vector of system risk and the early warning time

以下是系统风险衡量模型公式：

$$\begin{cases}\sum\limits_{i=1}^{}x_i=\text{sum}_x,\\ \sum\limits_{i=1}^{n}e_i=\text{sum}_e,\sum\limits_{i=1}^{m}d_i=\text{sum}_d,\\ \sum\limits_{i=1}^{j}f_t=\text{sum}_f,\sum\limits_{i=1}^{k}r_i=\text{sum}_r。\end{cases}$$

模型中 sum_x 等衡量特征向量中特征数据段的累加和。sum_x 值越大，风险越大；相应地，值越小，风险程度越小。现在依据特征向量中特征元素取值 0 和 1 的具体分布，作出如下假定：

1）理想情况是 $\boldsymbol{X}$ 所有元素均为 0，即最小风险态；

2）$\boldsymbol{X}$ 所有元素均为 1，即最大风险态；

3）$\text{sum}_e<\text{sum}_d<\text{sum}_f<\text{sum}_r$，发散的系统风险；

4）$\text{sum}_e>\text{sum}_d>\text{sum}_f>\text{sum}_r$，收敛的系统风险；

5）$\text{sum}_e+\text{sum}_d+\text{sum}_f=0$, AND $\text{sum}_r\geqslant 1$，前面 3 个阶段没有任何征兆，即不可预警的系统失效。这种情况可以理解成系统的瞬间失效。

6）$\text{sum}_e\times\text{sum}_d\times\text{sum}_f\geqslant 1$,AND $\text{sum}_r=0$，系统存在问题，但运行安全。

2.5　安全预警实例

依据前面的安全预警原理及方法，预警特征向量可以抽象为安全预警的特征条件，进而可以作为核电站仪控系统实际运行状态的预警判据。

下面将仪控系统安全预警的 3 种形式：基于物理参数阈值的预警、基于响应时间的预警、基于控制约束的预警，应用到具体的核电站仪控系统实例中进行说明。

1）基于物理参数阈值的预警。依据设定好的物理阈值，监控动态变化的核电站物理参数，包括生产变量、保护变量、停堆变量等。当监控参数超过正常阈值的范围，即符合报警条件，仪控系统实施预警。这类预警是核电站最基本的、最传统的监控方式。例如大亚湾核电站反应堆的安全阈值之一升降温速率≤ 56 ℃/h，还有堆芯出口温度 T 为 295 ℃、反应堆一回路压力 P 为 14.95 MPa 等。但这类预警的时间提前效应不好，当预警信号产生时，事故可能马上或已经发生，一般认为是事故后的报警方式。解决基于阈值预警效果不佳的方法是：记录核电站动态运行时的数据，并总结这些历史数据，依靠事件发生的时间序列，找到最早的初因事件，提高预警的时间裕量。

2）基于响应时间的预警。按照设计原则定义的基准时间、通过仪控系统时间戳得到自检时间参数，再与正常数据比对。当响应时间超过正常响应时间范围，即符合报警条件，仪控系统实施预警。例如秦山一期核电站反应堆保护系统的正常停堆响应时间约为 16 s，AP1000 反应堆停堆落棒系统的时间要求是不超过 0.5 s，反应堆喷淋注水的时间延迟参数为 40 s 等。DCS 系统的自检时间参数与上述这些存储在数据库中的正常数据集对比，可以很快判断 DCS 系统的运行状况，依据特征条件发出预警。

3）基于控制约束的预警。核电站 DCS 系统有复

杂的控制逻辑。控制约束是指不同的控制单元或控制指令间的相互关系。CTRL指仪控系统的控制单元或指令，ON指运行，OFF指不运行。有4类约束：

process 1 IF CTRL1 ON THEN CTRL2 ON；

process 2 IF CTRL1 ON THEN CTRL2 OFF；

process 3 IF CTRL1 OFF THEN CTRL2 ON；

process 4 IF CTRL1 OFF THEN CTRL2 OFF。

例如反应堆正常启动，保护系统及多样化驱动系统也相应启动，这符合process1的抽象；反应堆停堆信号产生，停堆指令生成，反应堆停堆继电器断电，控制棒下落，这符合process2的抽象；反应堆保护系统RPS停堆失效时，缓解系统才启动，这符合process3的抽象；反应堆正常停堆后，汽轮机也相应停机，这符合process4的抽象。这些process都是正常的运行动作及控制约束。这些符合安全的控制约束构成约束集合，一旦实际运行的控制动作指令等不符合控制约束集合，马上预警，将响应时间提前，起到预警作用。

利用预警特征向量可以合理描述并抽象基于响应时间、基于参数阈值、基于控制约束的预警这3类预警方法。特征向量的元素取值为1或0的算法判定：

对于x_i，默认初始值等于0。选择判决参数和判决规则如下：

rule 1 阈值处理（判决参数P>阈值W_1）or（判决参数P<阈值W_2）；IF rule 1 THEN x_i=1；

rule 2 响应时间处理（判决参数TP>T_1）or（判决参数TP<T_2）；IF rule 2 THEN x_i=1；

rule 3 控制约束处理，当仪控系统中实际运行子过程real process不符合对应的控制约束，形式化描述IF (real process)∉(process i) THEN x_i=1，i=1~4。

安全预警3种方法对应上面的3个判决规则。表1为核电站DCS系统始发事故表。

表1 核电站DCS系统始发事故表

Table 1 List of accidents for nuclear power plant DCS system

事故分类编号	分类描述	特征向量及元素映射	对应系统风险阶段
A1	版本升级	$\boldsymbol{D}$，d_i	系统缺陷defect
A2	数据溢出，数据格式不兼容	$\boldsymbol{E}$，e_i	系统错误error
A3	系统本身时序问题	$\boldsymbol{F}$，f_i	系统故障fault
A4	DCS系统通信协议可靠性	$\boldsymbol{R}$，r_i	系统失效failure
A5	软件模块间的不兼容	$\boldsymbol{E}$，e_i	系统错误error
A6	系统、硬件接口问题	$\boldsymbol{R}$，r_i	系统失效failure
A7	核电站DCS参数整定值	$\boldsymbol{R}$，r_i	系统失效failure
A8	核电站不同工况，DCS的软硬件复杂度不同	$\boldsymbol{D}$，d_i	系统缺陷defect

注意到，A1, A2, A5, A8处于时间轴较早的阶段，预警的时间提前量要大于A3, A4, A6, A7 4类DCS始发事故。这4类DCS问题都直接或间接与硬件关联。

3 结语

核电站DCS I&C系统是核电站控制的中枢神经。核电站DCS I&C系统存在风险，针对具体工况及失效模式归纳出的DCS I&C系统始发事故分类，利用预警特征向量可以合理描述并抽象基于物理参数阈值、基于响应时间、基于控制约束这3类预警形式，提前发现引发系统风险问题，提前预警，为核电站可靠性和安全性的增加做出贡献。

参考文献：

[1] 周海翔，徐玮瑛. 三代核电机组数字化仪控系统及其国产化分析[J]. 自动化仪表，2010，31(8)：61-66.
Zhou Haixiang，Xu Weiying. Third Generation Digital Instrument Control System of Nuclear Power Unit and Its Localization Analysis[J]. Automation Instrument，2010，31 (8)：61-66.

[2] 杨宗伟，黄铁明，冯光宇. 核电站仿真技术在反应堆控制系统调试中的应用[J]. 核动力工程，2009，30(6)：49-53.
Yang Zongwei，Huang Tieming，Feng Guangyu. The Application of Simulation Technology in Debugging for the Reactor Control System[J]. Nuclear Power Engineering，2009，30(6)：49-53.

[3] 郭晓明. 核电站数字化仪控系统可靠性分析方法研究[D]. 北京：清华大学，2011.
Guo Xiaoming. On Reliability Analysis Method of Nuclear Power Station Digital Instrument Control System[D]. Beijing：Tsinghua University，2011.

[4] Nancy Leveson. A New Accident Model for Engineering Safer Systems[J]. Safety Science，2004，42：237-238.

[5] 单锦辉，徐克俊，王 戟. 一种软件故障诊断过程框架[J]. 计算机学报，2011，34(2)：372-373.
Shan Jinhui，Xu Kejun，Wang Ji. A Framework of Software for Fault Diagnosis Process[J]. Journal of Computers，2011，34(2)：372-373.

[6] 陈延辉，胡立生，徐济鋆. 核电数字化保护系统软件的模块化设计[J]. 微型电脑应用，2009，25(8)：42-43.
Chen Yanhui，Hu Lisheng，Xu Jijun. Software Modular Design of Nuclear Power Digital Protection System[J]. Microcomputer Applications，2009，25(8)：42-43.

（责任编辑：申 剑）