核电厂常规岛后备监控技术研究

李 力

（国核电力规划设计研究院有限公司，北京 100095）

摘要：对核电厂数字化仪控系统进行失效模式和影响分析，提出核电厂数字化仪控系统的两种故障模式："DCS 人机接口全部丧失"和"DCS 控制层故障"。通过对机组稳定运行所需的监控信息进行分析，以及机组在发生参数异常后的安全停机需求进行分析，首次提出基于数显仪表、报警灯和操作开关一体化的后备监控理念，研发一种常规岛后备监控盘。常规岛后备监控盘上数显仪表和报警灯的数量和种类满足在"DCS 人机接口全部丧失"情况下机组在限定时间内稳定运行监视要求。常规岛后备监控盘上的操作开关数量和种类满足在"DCS 人机接口全部丧失"和"DCS 控制层故障"情况下机组安全停机要求。核电机组通过配备独立于 DCS 的常规岛后备监控盘，满足在全部失去电站计算机信息和控制系统时维持核电机组在一定时间内安全运行并能够将核电机组带入安全停堆停机状态，实现了核电机组仪控平台的多样性，防止在一套平台内部出现共因故障而丧失监控功能。

关键词：核电厂；常规岛；后备监控；分布式控制系统(DCS)；失效模式和影响分析(FMEA)；数显仪表；报警灯；操作开关

中图分类号：TH868 **文献标志码**：A **文章编号**：1671－1807(2023)09－0198－06

随着数字化仪控技术的发展，目前在运和在建的三代核电项目均采用了数字化仪控系统。与模拟控制技术相比，数字化技术具有明显的技术先进性和优势，也有利于改善核电厂的安全状态及稳定运行水平。采用数字化仪控系统已经成为核电发展的必然趋势。

核电厂主控制室设计也随着数字化技术的发展而逐步从常规主控制室走向全数字化主控制室。核电机组在采用数字化仪控系统后，考虑全部失去电站计算机信息和控制系统的可能性，需在主控制室内设置后备监控手段。后备盘是考虑在主要监控台以计算机为主的监控方式不可用时，维持核电站在一定时间内安全运行并能够将电站带入安全停堆停机状态的以硬接线为主的设备。后备盘与主要监控台采用两套完全不同的平台（一套为硬件，一套为软件），从而实现了平台的多样性，防止在一套平台内部出现共因故障而丧失监控功能[1-2]。

针对常规岛的后备监控技术，国内的研究较少。本文依托国和一号示范工程，从数字化仪控系统的失效模式和影响分析、后备监控方案、设计基准事件分析等方面对核电厂常规岛的后备监控技术进行研究，以满足在全部失去电站计算机信息和控制系统时维持核电机组在一定时间内安全运行并能够将核电机组带入安全停堆停机状态[3-4]。

1 核电厂仪控系统架构

1.1 仪控系统架构

核电厂仪控系统主要由 4 个层次构成：运行监控层、网络通信层、控制层、现场设备层，如图 1 所示。

运行监控层主要是为电厂运行人员提供一系列工作场所，操纵员可以从其中获取人机接口(HSI)资源。用来监视和控制电厂的 HSI 资源包括大屏幕信息系统、操纵员站、专用安全盘、DAS 盘、常规岛后备监控盘。

网络通信层主要功能是对控制层、操纵员站、服务器等之间的通信数据进行传输与处理。网络通信层的主要设备包括交换机、服务器、网关等。

控制层主要功能是对电厂的工艺系统、电气系统、仪表系统进行控制。控制层的主要设备包括控制机柜、逻辑机柜、遮断机柜、仪表监测机柜等。

现场设备层主要功能是对控制层发出命令的执行，以及向控制层反馈仪表信号和设备状态。现场设备层的主要设备包括仪表、阀门、泵、电气机柜、打包设备等。

收稿日期：2022-10-05

基金项目：国家科技重大专项(2014ZX06002007)。

作者简介：李力(1982—)，男，河南新乡人，国核电力规划设计研究院有限公司，设计总工程师，高级工程师，硕士，研究方向为核电厂仪表与控制系统设计。

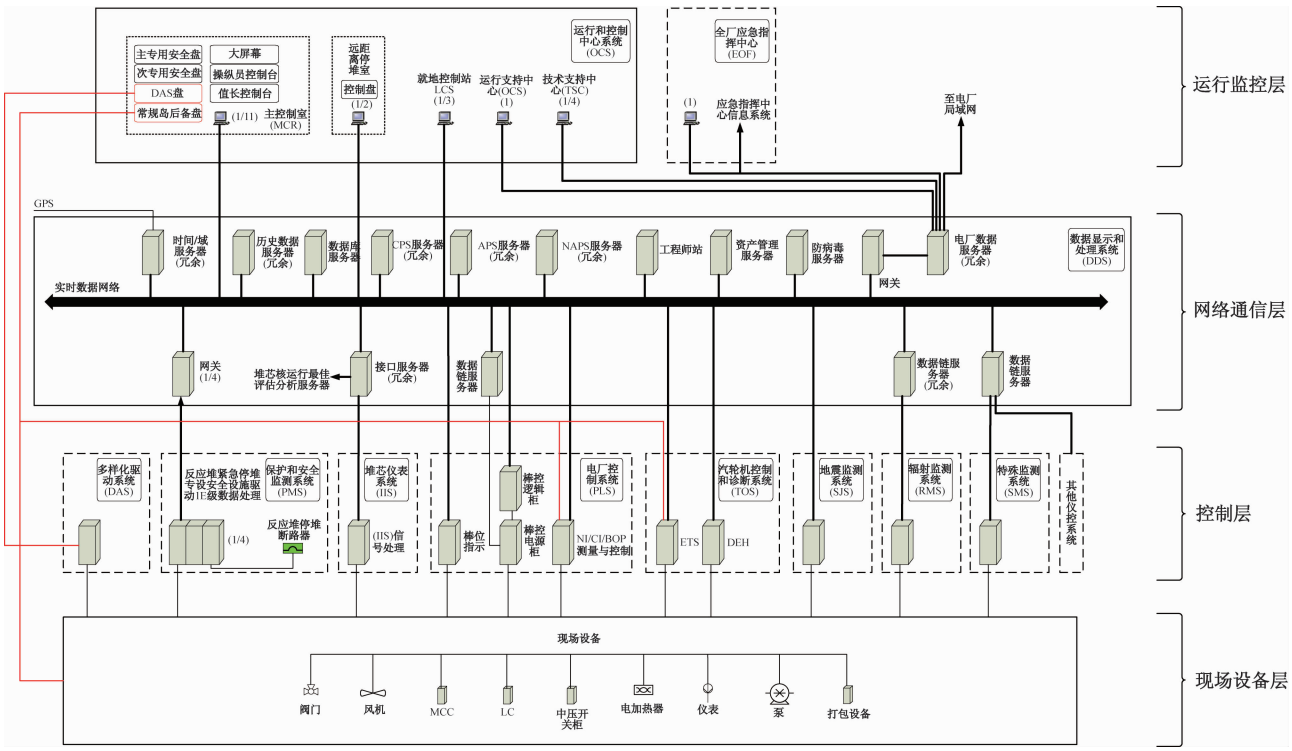


图 1　仪控系统总体架构

1.2　数字化仪控系统的 FMEA

失效模式和影响分析(failure mode and effects analysis,FMEA)是用于发现问题的一种系统化技术,它是一种“自底向上”的方法,它由系统内所有部件的一个详细的列表开始,一次一个部件地分析整个系统。需要时系统也可以分层次地划分为一些子系统和模块,层次结构中的每一个组均可以进行 FMEA[5-8]。

通过对 DCS(分布式控制系统)中各个部件进行 FMEA 分析,归纳出两种 DCS 失效的最终影响“DCS 人机接口全部丧失”和“DCS 控制层故障”,如图 2 所示。

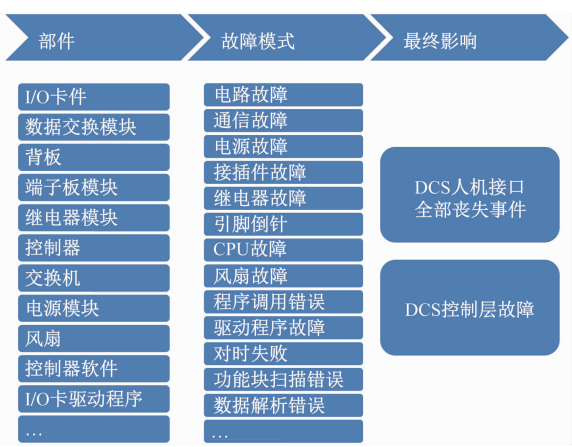


图 2　DCS 系统的 FMEA

DCS 人机接口全部丧失主要指主控制室所有操纵员站上的计算机出现“黑屏”“死机”“数据中断”等现象。发生 DCS 人机接口全部丧失事件后,操纵员将不能在计算机上获取电厂运行状态,也不能在计算机上对电厂设备进行操作。造成计算机“黑屏”“死机”“数据中断”等现象的原因主要有计算机电源故障、DCS 网络故障、系统负荷率过高造成网络通信堵塞等[9]。

DCS 控制层故障主要指控制层的控制器、I/O 等出现故障,导致控制系统不能执行机组正常控制功能和保护功能。发生 DCS 控制层故障后,操纵员将不能在计算机上获取电厂运行状态,也不能在计算机上对电厂设备进行操作,同时控制系统也不能执行机组正常控制功能和保护功能。

2　常规岛后备监控盘设计方案

2.1　DCS 故障后机组安全运行与停机需求

核电厂稳态运行时,当 DCS 上层网络、人机接口、DCS 控制系统发生故障,鉴于电厂安全功能有足够保障和提高机组经济效益,不必考虑立即手动停堆停机,允许电厂继续运行一段时间,以便对网络、人机接口和控制系统的故障进行修复。为此需要在主控制室内设置常规岛后备监控盘,后备监视和报警信号的数量和种类满足在 DCS 上层网络和人机接口故障情况下机组在限定时间内的稳态运

行监视要求。后备操作设备的数量和种类满足在 DCS 控制系统故障情况下机组安全停机要求。一旦在限定时间内发生瞬态事件，例如后备监视信号出现异常或报警信号产生，将利用后备操作开关实现安全停机。如果在限定时间内未完成网络、人机接口和控制系统的故障修复，也将利用后备操作开关实现安全停机。

在 MCR 内为常规岛设置独立于 DCS 的后备盘，在后备盘上布置有数显仪表、报警灯、操作开关。

数显仪表的数量和种类应满足在 DCS 上层网络和人机接口故障情况下机组在限定时间内的稳态运行监视要求。在该限定时间内允许电厂继续运行，进行故障修复，如果在该限定时间内未完成修复，将执行安全停机操作。后备操作设备的数量和种类按照满足在 DCS 控制系统故障情况下机组停机的要求进行设置。

2.2　数显仪表

2.2.1　数显仪表信号传输形式

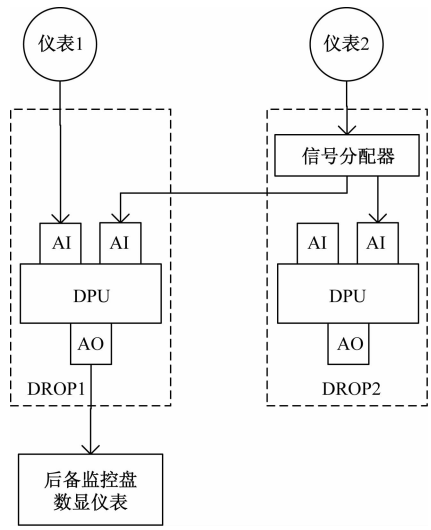
常规岛后备监控盘上的数显仪表信号可取自以下两个地方：就地仪表、控制系统 AO 卡件。鉴于目前 DCS 硬件的可靠性越来越高，数显仪表信号推荐采用取自控制系统 AO 卡件的方式。

信号传输方式应满足以下原则：

1）网络通信层故障不应导致常规岛后备监控盘上的数显仪表信号显示失效。

2）构成常规岛后备监控盘上的数显仪表信号的各原始信号应在一个 DROP 站，如果某一原始信号与常规岛后备监控盘上的数显仪表信号不在一个 DROP 站下，则该原始信号需要通过信号分配器分出一路硬接线信号送至常规岛后备监控盘上的数显仪表信号所在的 DROP 站，具体方式如图 3 所示。

3）控制系统 AO 卡件至常规岛后备监控盘上的数显仪表信号应采用硬接线传输。



DROP 为控制器站；DPU 为控制器；AI 为模拟量输入卡件；AO 为模拟量输出卡件

图 3　数显仪表原始信号分配图

2.2.2　数显仪表清单与组合逻辑

根据对 DCS 故障后机组安全运行与停机需求的分析，需要在常规岛后备监控盘上显示的数显仪表信息如图 4 所示。

每个数显仪表由 3 个冗余仪表在同一控制器内经过三取中算法后输出模拟量信号至常规岛后备监控盘，如图 5 所示。

2.3　报警灯

2.3.1　报警灯信号传输形式

一般地，报警灯表示机组出现某种异常情况，通常由多个触发条件组成，因此报警灯信号是一个综合信号，需要在 DCS 中进行逻辑判断后通过 DO 卡件继电器输出至常规岛后备监控盘。如果某个报警灯是由单一信号构成，也可取自就地仪表或设备。

构成常规岛后备监控盘上的报警灯信号的各

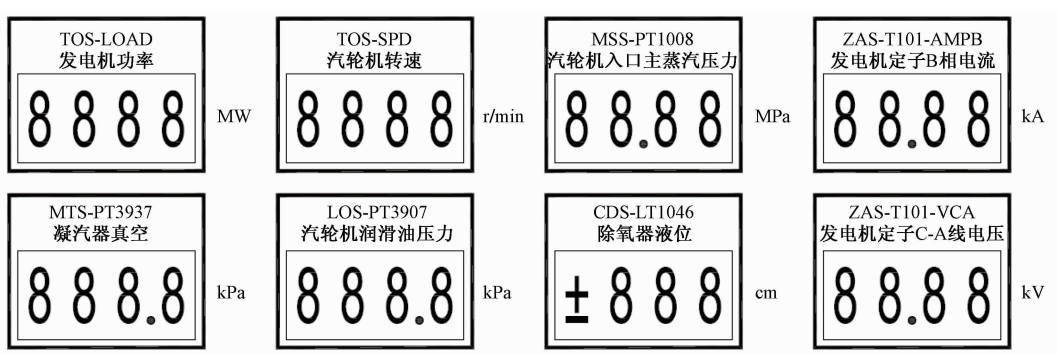


图 4　数显仪表布置

原始信号应在一个 DROP 站,如果某一原始信号与常规岛后备监控盘上的报警灯信号不在一个 DROP 站下,则该原始信号需要通过信号分配器分出一路硬接线信号送至常规岛后备监控盘上的报警灯信号所在的 DROP 站,或通过 DO/AO 硬接线输出至常规岛后备监控盘上的报警灯信号所在的 DROP 站,具体方式如图 6 所示。

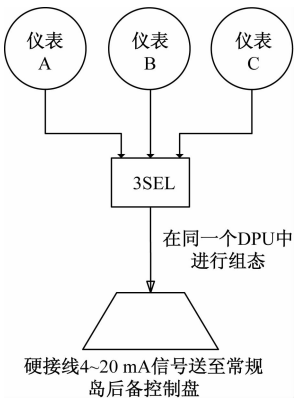
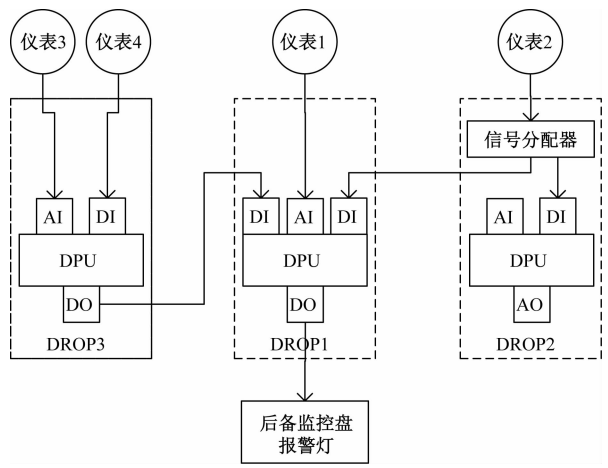


图 5　数显仪表组合逻辑

2.3.2　报警灯清单与组合逻辑含义

根据对 DCS 故障后机组安全运行与停机需求的分析,需要在常规岛后备监控盘上显示的报警灯信息如图 7 所示。



DROP 为控制器站;DPU 为控制器;AI 为模拟量输入卡件;AO 为模拟量输出卡件;DI 为开关量输入卡件;DO 为开关量输出卡件

图 6　报警灯原始信号分配图

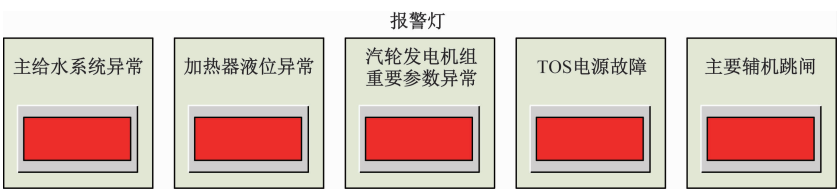


图 7　报警灯布置

主给水系统异常报警灯主要用于警告操纵员主给水系统可能发生主给水供水不足、主给水断水、主给水供水能力与反应堆需求不匹配等异常工况[10]。

加热器液位异常报警灯主要用于警告操纵员高加、低加、除氧器发生液位过高情况,可能会发生汽轮机进水。

汽轮发电机组重要参数异常报警灯主要用于警告操纵员汽轮发电机本体的监测参数发生异常,可能会导致汽轮发电机本体发生损坏。

TOS 电源故障报警灯主要用于警告操纵员发生 DEH、ETS、TSI 系统电源故障情况,可能会导致汽轮机控制系统发生失效。

主要辅机跳闸报警灯主要用于警告操纵员发生主要辅机跳闸情况,可能会导致二回路断水、机组失去热阱、失去设备冷却水源等。

2.4　操作开关

2.4.1　操作开关的设计原则

常规岛后备监控盘上的操作开关的主要目的在于当 DCS 发生故障时,操纵员仍具备对机组执行安全停机的操作手段。常规岛后备监控盘上的操作开关需要直接作用于 0 层的设备,独立于 1 层的控制系统和 2 层的数据网络,用于执行安全停机和设备保护等功能。

常规岛后备监控盘上的操作开关的设计应满足以下原则:

1)网络通信层故障和 DCS 控制系统故障不应导致常规岛后备监控盘上操作开关的执行动作功能丧失。

2)常规岛后备监控盘上操作开关至就地设备的动作信号应采用硬接线传输。

3)就地设备至常规岛后备监控盘上操作开关的状态反馈信号应采用硬接线传输[11-12]。

2.4.2　操作开关与指示灯布置

根据对 DCS 故障后机组安全运行与停机需求的分析,需要在常规岛后备监控盘上布置的操作开关信息如图 8 所示。

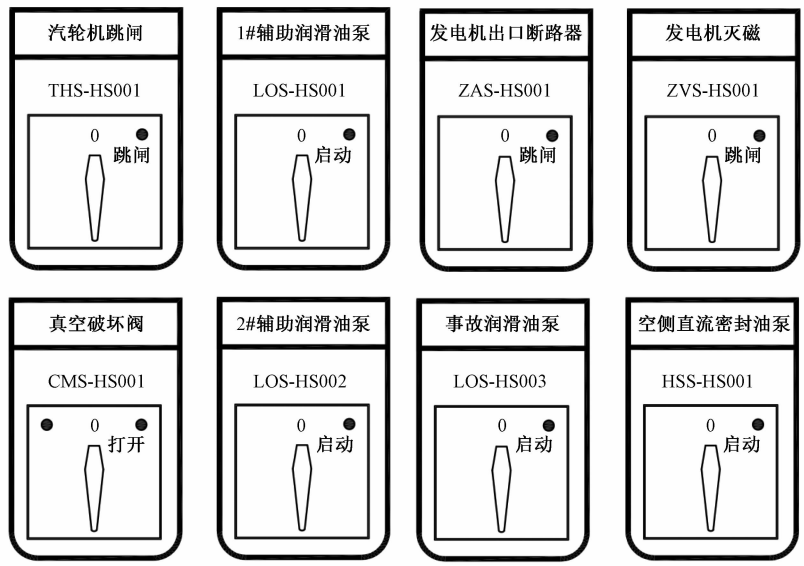


图 8　操作开关布置

3　设计基准事件与规程支持

3.1　DCS 人机接口全部丧失

DCS 人机接口全部丧失主要指主控制室所有操纵员站上的计算机出现“黑屏”“死机”“数据中断”等现象。发生 DCS 人机接口全部丧失事件后，操纵员将不能在计算机上获取电厂运行状态，也不能在计算机上对电厂设备进行操作。造成计算机“黑屏”“死机”“数据中断”等现象的原因主要有计算机电源故障、DCS 网络故障、系统负荷率过高造成网络通信堵塞等[13]。

若出现以下任一征兆，则进入常规岛后备监控操作规程，如图 9 所示。

1）主控制室内所有操纵员站显示器和大屏幕系统出现“黑屏”，此时表明主控制室内的计算机发生电源故障。

2）主控制室内所有操纵员站显示器和大屏幕系统出现“死机”，此时表明主控制室内的计算机发生病毒入侵或计算机故障。

3）主控制室内所有操纵员站显示器和大屏幕系统上的数据显示“超时”或“坏数据”，此时表明 DCS 网络故障。

3.2　DCS 控制层故障

DCS 控制层故障主要指控制层的控制器、I/O 等出现故障，导致控制系统不能执行机组正常控制功能和保护功能。发生 DCS 控制层故障后，操纵员将不能在计算机上获取电厂运行状态，也不能在计算机上对电厂设备进行操作，同时控制系统也不能执行机组正常控制功能和保护功能[14-15]。

若出现以下任一征兆，则进入常规岛后备监控操作规程，如图 10 所示。

1）控制层不能执行逻辑功能。例如存在汽轮机跳机信号，但汽轮机未跳机。

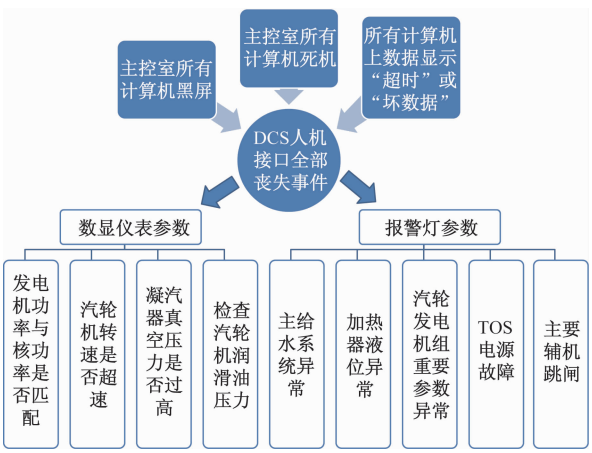


图 9　DCS 人机接口全部丧失事件与操作规程

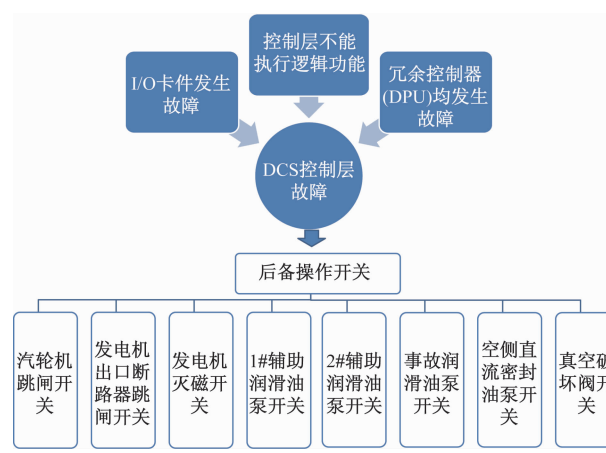


图 10　DCS 控制层故障事件与操作规程

2)冗余控制器(DPU)均发生故障。

3)I/O 卡件发生故障。

4　结论

通过对核电厂数字化仪控系统进行失效模式和影响分析,提出了核电厂数字化仪控系统的两种故障模式:“DCS 人机接口全部丧失”和“DCS 控制层故障”。通过对机组稳定运行所需的监控信息进行分析,以及机组在发生参数异常后的安全停机需求进行分析,提出了常规岛后备监控盘的设计方案。常规岛后备监控盘上的数显仪表和报警灯的数量和种类满足在 DCS 人机接口全部丧失情况下机组在限定时间内的稳定运行监视要求。常规岛后备监控盘上的操作开关数量和种类满足在“DCS 人机接口全部丧失”和“DCS 控制层故障”情况下机组安全停机要求。

参考文献

[1] 李敏,陈文浩,孔伟力,等. 核电厂主控室后备盘测试方法研究[J]. 核电子学与探测技术,2018,38(2):245-249.

[2] BOLDUC L P. X-33 redundancy management system[J]. Aerospace and Electronic Systems Magazine (IEEE), 2001,16(5):23-28.

[3] 李力,肖长歌. 基于马尔科夫模型的核电厂汽轮机保护系统可靠性研究[J]. 热力发电,2020,49(1):63-69.

[4] 刘文丰,寻新,刘红旭. 火电机组主保护硬回路典型设计及可靠性浅析[J]. 热力发电,2013,42(10):16-20.

[5] 系统可靠性分析技术 失效模式和影响分析(FMEA)程序:GB/T 7826—2012[S]. 北京:中国标准出版社,2012.

[6] WILLIAM M. 控制系统的安全评估与可靠性[M]. 北京:中国电力出版社,2008:143-217.

[7] 谢里阳,林文强. 冗余系统共因失效的载荷-性能分析与概率估算[J]. 核科学与工程,2003,23(4):289-295.

[8] 核电厂安全重要仪表和控制系统应对共因故障的要求:NB/T20068—2012[S]. 北京:中国电力出版社,2012.

[9] 火力发电厂热工自动化系统可靠性评估技术导则:DL/T 261—2012[S]. 北京:中国电力出版社,2012.

[10] 林伟波. CPR1000 核电厂主给水泵备用泵启泵逻辑优化[J]. 科学技术与工程,2012,12(28):7399-7401.

[11] 周丽,杨培成,崔 猛,等. 大型火电机组汽轮机保护控制系统的改进[J]. 热力发电,2010,39(8):88-92.

[12] 廖兴宝,高宏喜. 引进型 1 000 MW 等级核电汽轮机的设计特点[J]. 热力透平,2008,37(1):12-15.

[13] CHEN G Y, HUANG X Z, TANG X W. Analysis of phased-mission system reliability and importance with imperfect coverage[J]. Journal of Electronic Science and Technology of China, 2005,3(2):182-186.

[14] 李雨桐,喻潇白,刘官荣,等. 基于 FMEA 分析的核电厂安全级 DCS 系统仪控故障报警的分类及分级[J]. 仪器仪表用户,2018,25(11):30-35.

[15] 周海翔. 田湾核电厂数字化反应堆保护系统故障模式与后果分析[J]. 原子能科学技术,2007,41(6):702-706.

Research on Conventional Island Backup Control Technology in Nuclear Power Plant

LI Li

(State Nuclear Electric Power Planning Design & Research Institute Co. Ltd, Beijing 100095, China)

Abstract: The failure mode and effects analysis of the digital I&C system of nuclear power plant are carried out, and puts forward two failure modes of the digital I&C system of nuclear power plant: “all DCS man-machine interfaces are lost” and “DCS control layer failure”. By analyzing the monitoring information required for the stable operation of the plant and the safe shutdown demand of the plant after abnormal parameters, the backup control concept based on the integration of digital display instrument, alarm lamp and operation switch is proposed for the first time, and a conventional island backup control panel is developed. The number and type of digital display instruments and alarm lights on the conventional island backup control panel meet the monitoring requirements for the stable operation of the plant within a limited time under the condition that “all DCS man-machine interfaces are lost”. The number and type of operation switches on the conventional island backup control panel meet the requirements for safe shutdown of the plant in the case of “all DCS man-machine interfaces are lost” and “DCS control layer failure”. The nuclear power plant is equipped with a conventional island backup control panel independent of DCS to maintain the safe operation of the nuclear power plant within a certain time when all the computer information and control system of the power plant are lost, and can bring the nuclear power plant into a safe shutdown state, so as to realize the diversity of the instrument and control platform of the nuclear power plant and prevent the loss of monitoring function due to common cause failure in a set of platform.

Keywords: nuclear power plant; conventional island; backup control; distributed control system (DCS); failure mode and effects analysis (FMEA); digital display instrument; alarm lamp; operating switch