文章编号：0258-0926(2014)01-0122-03

核电厂仪控系统纵深防御和多样性设计

周继翔，朱 攀，肖 鹏

中国核动力研究设计院，成都，610041

摘要：针对事件发生时用于保护堆芯和限制放射性扩散的功能，核电厂设计有多层次的防御，仪控系统的设计支持这一理念，通过纵深防御和多样性设计，保证保护屏障和措施的完整性和有效性，抵御潜在的共因故障的影响，有利于限制核电厂事故的发展，减轻事故后果，保证反应堆及核电厂设备和人员的安全，防止放射性物质向周围环境的释放。

关键词：核电厂；仪控系统；纵深防御多样性；共因故障

中图分类号：TL362 文献标志码：A

0 引 言

经典的纵深防御设置是防止反应堆放射性释放的三道物理屏障：燃料包壳、一回路压力边界和安全壳。

反应堆仪表和控制系统在配置上有专门的纵深防御原则，防御层次分为：控制系统、反应堆停堆系统、专设安全设施驱动系统以及监测和显示系统[1]。

多样性是对纵深防御原则的补充，采用多样性设计有利于提高为某个层次提供防御而动作的可能性。多样性是核电厂仪表系统设计的一个原则，要求通过监测不同参数，使用不同的技术、不同的逻辑或算法、不同的驱动手段提供探测和响应重要事件的途径。不同层次的防御也可以考虑多样性。

1 仪控系统纵深防御设计

在核电厂仪控系统设计中，根据 NUREG/CR-6303 对 4 重防御层次的要求以及多样设计考虑，需要针对仪控系统所须完成任务开展多样性和纵深防御设计。

1.1 控制系统防御层

控制系统防御层设计为由非 1E 级的自动或手动设备组成，用于防止反应堆的运行偏向不安全的区间，适用于反应堆正常运行期间的操作，有关的指示和报警都包含在控制系统防御层。控制系统防御层的设备可作为 1E 级反应堆保护系统的后备，以抵御保护系统中极不可能发生的共因故障。控制系统防御层实现的功能在非安全级的电厂控制系统中实现。该系统的功能是将电厂维持在运行限值以内，以避免引起停堆或专设安全设施驱动。

1.2 紧急停堆系统防御层

紧急停堆防御层设计由 1E 级设备组成，用于反应堆出现不受控的偏移时快速减少反应性。它由保护参数监测仪表、相关的逻辑处理设备和驱动器组成，通过快速插入控制棒的方式实现其防御功能。紧急停堆防御层实现的自动停堆功能在安全级的反应堆保护系统和非安全级的多样化驱动系统中实现。

1.3 专设安全设施驱动系统（ESFAS）防御层

ESFAS 防御层设计由 1E 级设备组成，用于排出反应堆热量并维持防止放射性释放的 3 重物理屏障（燃料包壳、反应堆压力容器和安全壳）的完整性。该防御层监测有关的保护参数并在需要时完成以下功能：应急冷却、压力释放或卸压、隔离以及不同支持系统（如应急柴油机）或装置（阀门、电机、泵）的控制。ESFAS 防御层实现的自动专设驱动功能在安全级的反应堆保护系统和非安全级的多样化驱动系统中实现。对于西屋公司设计的 AP1000，由于是非能动的第三代核电厂，因此不需要应急柴油机、电动机或泵来执行

收稿日期： 2012-09-26；修回日期：2013-11-12

专设驱动功能。

1.4 监测与指示系统防御

相比上述 3 个防御层，监测与指示系统防御层是最缓慢但同时也是最灵活的防御层。与其他 3 层一样，操纵员需要依赖有关的探测器信息来执行任务，但是操纵员可以根据获取的信息和恰当的方法执行事先未指定的逻辑计算以应对不可预知的事件。监测与指示系统防御层包括那些名义上分配给其他 3 个防御层的 1E 级和非 1E 级的手动控制、监测及指示。由监测和指示防御层实现的手动停堆和手动专设驱动功能包含在安全级的反应堆保护系统和非安全级的多样化驱动系统中。

2 仪控系统多样性设计

多样性设计是防御共因故障的重要手段，然而多样性设计不能抛开独立性，甚至多样性设计更宜视作对独立性的补充以提高系统抵御不确定的共因故障的能力，不具有独立性的多样性设计将因为系统间的相互作用导致系统同时故障。

多样性设计主要考虑 6 个方面：人因多样性、设计多样性、软件多样性、功能多样性、信号多样性和设备多样性：

（1）设计多样性：设计多样性主要指设计时需要考虑采用不同的技术（如采用模拟技术和数字技术），或在某种技术中采用不同的设计方案（如采用交流电和直流电的仪表），或者采用不同的结构。

（2）设备多样性：设备多样性主要指设备是基于不同设计由不同或相同的厂家制造的，或采用相同设计但由不同的厂家制造的，或相同的设计但版本不同的设备。对于数字化设备多样性更体现于不同的 CPU 结构、不同的 CPU 芯片版本、不同的印刷电路板设计、不同的总线结构。

（3）功能多样性：功能多样性主要指设计时考虑采用不同的机理（如插入控制棒和硼稀释），或达到不同的目的（如正常的棒控运行和紧急停堆），或针对某个事故工况在发展过程中的不同响应。

（4）人因多样性：人因多样性主要指设计由不同的公司，或同一个公司但是不同的团队，或者不同的设计者，或者不同测试、安装人员完成。

（5）信号多样性：信号多样性主要指通过感应不同的物理效应测量参数变量（如压力和中子注量率），或通过感应相同的物理效应测量参数变量（如不同压力传感器测量时的压力和水位参数），或通过几组相似的冗余探测器测量参数变量（如分别用于驱动多样性保护设备的 2 组冗余的水位探测器）。在核电厂仪控系统设计中，应对一个事件设置多样性的保护参数，用于触发紧急停堆和驱动专设安全设施，这些信号使用不同类型的传感器。

（6）软件多样性：软件多样性主要指设计中采用不同的算法、逻辑和程序，或不同的操作系统、不同的计算机语言。

3 AP1000 堆型仪控系统（I&C）中 D3 设计考虑

AP1000 I&C 系统多样化结构采用了多层防御的方法，将系统分成 3 层，由安全级和非安全级的仪表系统构成。该系统由以下 3 个部分组成：①完成纵深防御任务的电厂控制系统；②保护和安全监测系统；③多样化驱动系统。各个部分的功能如下：

（1）电厂控制系统：电厂控制系统为非安全级系统，该系统提供从电厂冷停堆到满功率正常运行的必要控制，将电厂工况维持在运行限值范围内。电厂控制系统由非安全级的仪控设备组成，可自动和手动实现控制反应堆功率、稳压器压力和水位、给水流量以及执行与发电相关的其他电厂功能。通过主控室或远程停堆站可实现对非安全级部件的手动控制。

（2）保护和安全监测系统：保护和安全监测系统为安全级系统，该系统提供必要的安全功能，以监测电厂运行状态、停闭反应堆以及将电厂维持在安全停堆状态。保护和安全监测系统由安全级的仪控设备组成，可自动和手动实现紧急停堆功能、专设安全设施驱动。执行紧急停堆和专设安全设施驱动功能的仪控设备及有关的传感器和停堆断路器组合都是 4 重冗余的。通过主控室或远程停堆站可实现对安全级部件的手动控制。此外，保护和安全监测系统提供必要的设备用于监测核电厂事故监测仪表准则（RG1.97）要求的事故及事故后参数。

（3）多样化驱动系统：多样化驱动系统为非安全级系统，该系统提供紧急停堆和驱动选定的专设安全设施的功能，并向操纵员提供电厂信息。

多样化驱动系统直接接收专用传感器的信号，其处理单元使用了不同于保护和安全监测系统的硬件。

AP1000 设计的 4 个防御层由非安全级系统、安全级系统和非安全级的多样化系统构成，提供自动和手动驱动功能，用于支持 4 个防御层。I&C 系统的功能由基于处理器的子系统实现。图 1 显示非安全级、安全级以及多样化系统在每个防御层次中的作用。

对于那些用于将电厂维持在运行限值以内、触发紧急停堆以及驱动专设安全设施动作的手动控制，各系统都提供了支持这些手动控制的指示，即电厂控制系统的数据显示与处理系统将用于非安全级显示和报警的电厂数据，通过实时数据网提供给操纵员，保护和安全监测系统的 1E 级数据处理系统向操纵员提供安全级的显示，多样化驱动系统则向操纵员提供不同于保护与安全监测系统的非安全级的指示。

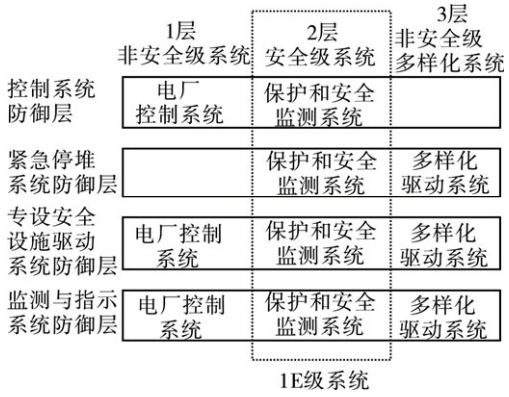

图 1 AP1000 仪表和控制防御层次

Fig. 1 AP1000 I&C Echelons of Defense

4 结束语

针对事件发生时用于保护堆芯和限制放射性扩散的功能，核电厂设计有多层次的防御，仪控系统的设计支持这一理念，通过纵深防御和多样性设计，保证保护屏障和措施的完整性和有效性，抵御潜在的共因故障的影响，有利于限制核电厂事故的发展，减轻事故后果，保证反应堆及核电厂设备和人员的安全，防止放射性物质向周围环境的释放。西屋公司仪控系统纵深防御和多样性设计在国内新堆型仪控系统设计中应加以借鉴。

参考文献：

[1] NUREG/CR-6303. Method for Performing Diversity and Defense-in-depth Analyses of Reactor Protection Systems[S]. 1994

Defense-in-Depth and Diversity Design of Instrumentation and Control System in Nuclear Power Plant

Zhou Jixiang, Zhu Pan, Xiao Peng

Nuclear Power Institute of China, Chengdu, 610041, China

Abstract: Nuclear power plant is designed with multiple level of defense for the function used to protect the core and limit the spread of radioactivity during an event. The design of instrumentation and control system supports this multiple level design philosophy. Defense-in-depth and diversity is considered in the design of instrumentation and control system to maintain the integrity and availability of protective barriers or means and defense potential common-cause failures. This can effectively limit the development of accident, mitigate accident consequence, prevent the spread of radioactive material to the environment and ensure safety of reactor and plant equipment and staff.

Key words: Nuclear power plant, Instrumentation and control system, Defense-in-depth and diversity, Common-cause failure

作者简介：

周继翔（1976—），男，高级工程师。1998 年毕业于西北工业大学电子与信息技术专业，获学士学位。现从事反应堆保护专业工作。

朱 攀（1981—），男，工程师。2007 年毕业于电子科技大学信号与信息处理专业，获硕士学位。现从事反应堆保护专业工作。

肖 鹏（1981—），男，工程师。2006 年毕业于电子科技大学测控技术与仪器专业，获硕士学位。现从事反应堆保护专业工作。

（责任编辑：刘胜吾）