

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2017年6月22日 (22.06.2017)



(10) 国际公布号
WO 2017/101031 A1

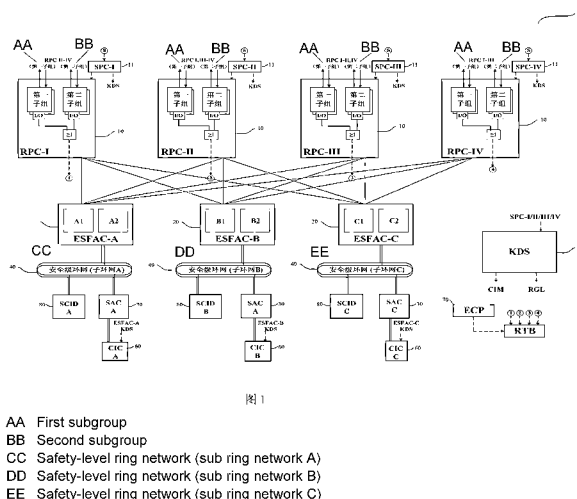
- (51) 国际专利分类号:
G21C 9/00 (2006.01) G21D 3/04 (2006.01)
- (21) 国际申请号: PCT/CN2015/097513
- (22) 国际申请日: 2015年12月15日 (15.12.2015)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (71) 申请人: 中广核工程有限公司 (CHINA NUCLEAR POWER ENGINEERING COMPANY LTD.) [CN/CN]; 中国广东省深圳市大鹏新区鹏飞路大亚湾核电基地工程公司办公大楼, Guangdong 518000 (CN)。 中国广核集团有限公司 (CHINA GUANGDONG NUCLEAR POWER HOLDING CORPORATION) [CN/CN]; 中国广东省深圳市福田区上步中路 1001 号深圳科技大厦 17-19 楼, Guangdong 518000 (CN)。
- (72) 发明人: 周叶翔 (ZHOU, Yexiang); 中国广东省深圳市大鹏新区鹏飞路大亚湾核电基地工程公司办公大楼, Guangdong 518000 (CN)。 任立永 (REN, Liyong); 中国广东省深圳市大鹏新区鹏飞路大亚湾核

电基地工程公司办公大楼, Guangdong 518000 (CN)。 田亚杰 (TIAN, Yajie); 中国广东省深圳市大鹏新区鹏飞路大亚湾核电基地工程公司办公大楼, Guangdong 518000 (CN)。 史赬 (SHI, Ji); 中国广东省深圳市大鹏新区鹏飞路大亚湾核电基地工程公司办公大楼, Guangdong 518000 (CN)。 汪伟 (WANG, Wei); 中国广东省深圳市大鹏新区鹏飞路大亚湾核电基地工程公司办公大楼, Guangdong 518000 (CN)。 梁玲 (LIANG, Ling); 中国广东省深圳市大鹏新区鹏飞路大亚湾核电基地工程公司办公大楼, Guangdong 518000 (CN)。 谭国成 (TAN, Guocheng); 中国广东省深圳市大鹏新区鹏飞路大亚湾核电基地工程公司办公大楼, Guangdong 518000 (CN)。 王巧燕 (WANG, Qiaoyan); 中国广东省深圳市大鹏新区鹏飞路大亚湾核电基地工程公司办公大楼, Guangdong 518000 (CN)。 杨震 (YANG, Zhen); 中国广东省深圳市大鹏新区鹏飞路大亚湾核电基地工程公司办公大楼, Guangdong 518000 (CN)。 彭华清 (PENG, Huaqing); 中国广东省深圳市大鹏新区鹏飞路大亚湾核电基地工程公司办公大楼, Guangdong 518000 (CN)。 陈卫华

[见续页]

(54) Title: NUCLEAR POWER PLANT REACTOR PROTECTION SYSTEM AND SAFETY CONTROL METHOD THEREIN

(54) 发明名称: 核电站反应堆保护系统及其中的安全控制方法



(57) Abstract: A nuclear power plant reactor protection system (100) and a safety control method therein. The protection system (100) comprises: an emergency shutdown system (10) divided into N protection channels, each protection channel obtaining protection parameters from a signal preprocessing system (11) to carry out threshold comparison; a special driving system (20) connected to the N protection channels, receiving a threshold comparison result, performing special driving logic processing according to the threshold comparison result, and outputting a first special driving instruction for driving an actuator that needs to be operated before a reactor reaches a controllable state and after a design reference accident of a nuclear power plant takes place; and an automatic safety system (30) connected to the special driving system (20) by means of a safety-level ring network (40), and generating a first device-level control instruction for controlling the actuator that needs to be operated when the reactor is converted from the controllable state to a safe shutdown state and after the design reference accident of the nuclear power plant takes place. The system and method can reduce the complexity of the maintenance and regular testing scheme for the protection system.

(57) 摘要:

[见续页]



(CHEN, Weihua); 中国广东省深圳市大鹏新区鹏飞路大亚湾核电基地工程公司办公大楼, Guangdong 518000 (CN)。黄伟军 (HUANG, Weijun); 中国广东省深圳市大鹏新区鹏飞路大亚湾核电基地工程公司办公大楼, Guangdong 518000 (CN)。江辉 (JIANG, Hui); 中国广东省深圳市大鹏新区鹏飞路大亚湾核电基地工程公司办公大楼, Guangdong 518000 (CN)。

(74) 代理人: 深圳市顺天达专利商标代理有限公司 (SHENZHEN STANDARD PATENT & TRADE-MARK AGENT LTD.); 中国广东省深圳市福田区深南大道 1056 号银座国际大厦 810-815 室, Guangdong 518040 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR,

IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

一种核电站反应堆保护系统 (100) 及其中的安全控制方法, 所述保护系统 (100) 具备: 分为 N 个保护通道的紧急停堆系统 (10), 每个保护通道从信号预处理系统 (11) 获取保护参数, 进行阈值比较; 与 N 个保护通道连接的专设驱动系统 (20), 接收阈值比较结果, 并根据阈值比较结果进行专设驱动逻辑处理, 输出第一专设驱动指令用于驱动核电厂设计基准事故发生后, 反应堆达到可控状态前需要操作的执行机构; 通过安全级环网 (40) 与专设驱动系统 (20) 连接的安全自动化系统 (30), 产生第一设备级控制指令, 用于对核电厂设计基准事故发生后, 反应堆从可控状态到安全停堆状态过程中需要操作的执行机构进行控制。所述系统和方法能够降低保护系统维护、定期试验的方案复杂程度。

核电站反应堆保护系统及其中的安全控制方法

技术领域

[0001] 本发明涉及核电站领域，尤其涉及一种核电站反应堆保护系统及其中的安全控制方法。

背景技术

[0002] 为了确保核电站反应堆安全运行，需设置保护系统。保护系统的结构设计与核电站的总体设计、安全分级、核级DCS（Digital Control System，数字化计算机控制系统）平台设计密切相关。

[0003] 在核电站发生设计基准事故的情况下，保护系统用于将反应堆带至安全停堆状态。其中，设计基准事故是指，核电站按确定的设计准则在设计中采取了针对性措施的事故工况。安全停堆状态是指反应堆以受控的方式停止的状态。此外，在安全停堆状态之前，反应堆先进入可控状态，这里的可控状态是指，反应堆的裂变链式反应处于可控状态。

[0004] 在保护系统中，从核电站发生设计基准事故后到反应堆达到可控状态的过程，以及反应堆从可控状态至安全停堆状态的过程，除实现反应堆自动紧急停堆功能外，一方面，需要根据保护参数进行对专设安全设施进行系统级的自动控制处理，另一方面，还需要对专设安全设施进行设备级的手动操作处理。其中，专设安全设施是指，核电厂在事故工况下投入使用并执行安全功能，以控制事故后果，使反应堆在事故后达到稳定的、可接受状态而专门设置的各种安全系统的总称。

[0005] 在实现上述现有保护系统的过程中，发明人发现现有技术中至少存在如下问题：现有的保护系统中，系统级专设驱动功能与设备级专设驱动功能被混杂在同一个子系统中实现，这样的子系统中，对于系统级专设驱动功能所使用的保护参数的控制处理等，以及对于设备级专设驱动功能所使用的用户输入指令的控制处理等，很多由同一设备实现，也即，实现两种功能的系统之间重合度较高，这导致保护系统维护、定期试验的方案较为复杂。

技术问题

[0006] 本发明提供一种核电站反应堆保护系统及核电站反应堆保护系统中的安全控制方法，能够降低保护系统维护、定期试验的方案复杂程度。

问题的解决方案

技术解决方案

[0007] 为达到上述目的，本发明的实施例采用如下技术方案：

[0008] 第一方面，提供一种核电站反应堆保护系统，具备：

[0009] 紧急停堆系统RTS，其分为N个保护通道，N为偶数且 $N \geq 2$ ，每个保护通道均对应连接一列信号预处理系统，其中，所述每个保护通道从对应的所述信号预处理系统获取保护参数，并根据所述保护参数进行阈值比较，得到阈值比较结果；

[0010] 专设驱动系统ESFAS，其与所述N个保护通道连接，用于接收每个保护通道的阈值比较结果，并根据所述阈值比较结果进行专设驱动逻辑处理，输出第一专设驱动指令，所述第一专设驱动指令用于驱动反应堆达到可控状态前的执行机构；

[0011] 安全自动化系统SAS，其通过安全级环网与所述专设驱动系统ESFAS连接，用于产生第一设备级控制指令，所述第一设备级控制指令用于对从反应堆达到可控状态到安全停堆状态的执行机构进行控制。

[0012] 结合第一方面，在第一方面的第一种可能的实现方式中，所述专设驱动系统ESFAS分为三个ESFAS序列，每个ESFAS序列均与所述N个保护通道通过点对点通讯连接。

[0013] 结合第一方面的第一种可能的实现方式，在第一方面的第二种可能的实现方式中，所述每个ESFAS序列均配置并行的、冗余的两个运算处理器。

[0014] 结合第一方面的第二种可能的实现方式，在第一方面的第三种可能的实现方式中，所述运算处理器用于对所述每个ESFAS序列接收的N个所述阈值比较结果进行符合逻辑处理，并且在所述N个保护通道中的部分保护通道失效时，按照符合逻辑退化原则进行处理。

[0015] 结合第一方面的第二种或第三种可能的实现方式，在第一方面的第四种可能的

实现方式中，还具备紧急控制盘ECP，其手动专设驱动按钮与所述专设驱动系统ESFAS通过硬接线连接，用于根据操作人员的操作指令输出第二专设驱动指令；

[0016] 所述运算处理器还用于对所述第一专设驱动指令与所述第二专设驱动指令进行或逻辑处理，输出第三专设驱动指令，所述第三专设驱动指令用于驱动反应堆达到可控状态前需要操作的执行机构。

[0017] 结合第一方面的第一种可能的实现方式，在第一方面的第五种可能的实现方式中，所述安全自动化系统SAS分为三个SAS序列，所述安全级环网分为三组安全级子环网，每个SAS序列通过一个所述安全级子环网与一个所述ESFAS序列一一对应连接。

[0018] 结合第一方面的第五种可能的实现方式，在第一方面的第六种可能的实现方式中，还具备安全级控制显示设备SCID，其分为三组，每组SCID通过一个所述安全级子环网与一个所述ESFAS序列及一个所述SAS序列一一对应连接；

[0019] 每组SCID根据操作人员的操作指令输出第二设备级控制指令，所述SAS序列接收所述第二设备级控制指令，并对所述第一设备级控制指令与所述第二设备级控制指令进行或逻辑处理，输出第三设备级控制指令，所述第三设备级控制指令用于对反应堆从可控状态到安全停堆状态需要操作的执行机构进行控制。

[0020] 结合第一方面，在第一方面的第七种可能的实现方式中，所述N个保护通道之间点对点连接，所述每个保护通道从另外N-1个保护通道获取所述阈值比较结果，

[0021] 所述每个保护通道均具备热备冗余处理器，所述热备冗余处理器根据来自所述N个保护通道的所述N个所述阈值比较结果得到第三局部停堆信号，

[0022] 所述每个保护通道均连接停堆断路器，所述停堆断路器从所述每个保护通道获取所述第三局部停堆信号，并执行所述第三局部停堆信号控制核电站停堆。

[0023] 结合第一方面的第七种可能的实现方式，在第一方面的第八种可能的实现方式中，

[0024] 所述每个保护通道均分为第一子组与第二子组，所分得的N个所述第一子组之间点对点连接，所分得的N个所述第二子组之间点对点连接；

- [0025] 每个第一子组均从另外N-1个第一子组获取所述阈值比较结果，每个第一子组均具备第一热备冗余处理器，所述第一热备冗余处理器用于对来自所述N个第一子组的N个所述阈值比较结果进行符合逻辑处理，并且在N个保护通道中的部分保护通道失效时，按照退化原则进行符合逻辑处理，输出第一局部停堆信号；
- [0026] 每个第二子组均从另外N-1个第二子组获取所述阈值比较结果，每个第二子组均具备第二热备冗余处理器，所述第二热备冗余处理器用于对来自所述N个第二子组的N个所述阈值比较结果进行符合逻辑处理，并且在N个保护通道中的部分保护通道失效时，按照退化原则进行符合逻辑处理，输出第二局部停堆信号；
- [0027] 所述紧急停堆系统RTS的每个保护通道还均具备RTS或逻辑处理电路，所述RTS或逻辑处理电路与所述第一子组及所述第二子组连接，用于对所述第一局部停堆信号与所述第二局部停堆信号进行或逻辑处理，输出所述第三局部停堆信号。
- [0028] 结合第一方面的第七种可能的实现方式，在第一方面的第九种可能的实现方式中，还具备紧急控制盘ECP，所述紧急控制盘的手动停堆控制按钮通过硬接线直接连接所述停堆断路器，并向所述停堆断路器输出第四局部停堆信号，所述停堆断路器获取并执行所述第四局部停堆信号控制核电站停堆。
- [0029] 结合第一方面，在第一方面的第十种可能的实现方式中，还具备多样化驱动系统KDS，其实现预期瞬态不停堆系统的系统ATWS的功能，用于在所述保护系统发生共模失效的情况下，从所述信号预处理系统或现场仪表或第三方监测系统获取保护参数，并根据所述保护参数输出停堆控制指令，
- [0030] 所述多样化驱动系统与棒控系统连接，所述棒控系统从所述多样化驱动系统接收所述停堆控制指令，并执行所述停堆控制指令控制核电站停堆。
- [0031] 结合第一方面的第十种可能的实现方式，在第一方面的第十一种可能的实现方式中，所述多样化驱动系统还用于根据所述保护参数输出第三专设驱动指令，所述第三专设驱动指令用于驱动反应堆达到可控状态前需要操作的执行机构。
- [0032] 结合第一方面的第十一种可能的实现方式，在第一方面的第十二种可能的实现方式中，还具备设备接口及优先级模块CIM，其与所述安全自动化系统SAS及所述多样化驱动系统连接，用于获取所述第一设备级控制指令及所述第三专设驱

动指令，还通过所述安全级环网及所述安全自动化系统SAS获取所述专设驱动系统ESFAS输出的所述第一专设驱动指令，并对获取到的多个指令进行优先级处理。

[0033] 结合第一方面的第十种可能的实现方式，在第一方面的第十三种可能的实现方式中，当所述紧急停堆系统RTS、所述专设驱动系统ESFAS正常时，所述多样化驱动系统的自动逻辑功能正常运行，手动操作指令闭锁。

[0034] 第二方面，提供一种核电站反应堆保护系统中的安全控制方法，包括如下步骤：

[0035] 阈值比较步骤，其中，紧急停堆系统RTS的多个保护通道均从对应的信号预处理系统获取保护参数，并对所述保护参数进行阈值比较，得到阈值比较结果；

[0036] 专设驱动步骤，其中，专设驱动系统ESFAS接收每个保护通道的阈值比较结果，并根据所述阈值比较结果进行专设驱动逻辑处理，输出第一专设驱动指令，所述第一专设驱动指令用于驱动反应堆达到可控状态前需要操作的执行机构；

[0037] 安全自动化步骤，其中，安全自动化系统SAS产生第一设备级控制指令，所述第一设备级控制指令用于对反应堆从可控状态到安全停堆状态需要操作的执行机构进行控制。

[0038] 结合第二方面，在第二方面的第一种可能的实现方式中，所述专设驱动系统ESFAS分为三个ESFAS序列，每个ESFAS序列均与多个保护通道通过点对点通讯连接；

[0039] 所述每个ESFAS序列均配置并行的、冗余的两个运算处理器；

[0040] 在所述专设驱动步骤中，所述运算处理器对所述每个ESFAS序列接收的多个所述阈值比较结果进行符合逻辑处理，并且在所述多个保护通道中的部分保护通道失效时，按照符合逻辑退化原则进行处理。

[0041] 结合第二方面的第一种可能的实现方式，在第二方面的第二种可能的实现方式中，所述核电站反应堆保护系统还具备紧急控制盘ECP，所述紧急控制盘ECP的手动专设驱动按钮与所述专设驱动系统ESFAS连接，根据操作人员的操作指令输出第二专设驱动指令；

[0042] 在所述专设驱动步骤中，所述运算处理器对所述第一专设驱动指令与所述第二

专设驱动指令进行或逻辑处理，输出第三专设驱动指令，所述第三专设驱动指令用于驱动反应堆达到可控状态前需要操作的执行机构。

[0043] 结合第二方面的第一种可能的实现方式，在第二方面的第三种可能的实现方式中，所述安全自动化系统SAS分为三个SAS序列，所述安全级环网分为三组安全级子环网，每个SAS序列通过一个所述安全级子环网与一个所述ESFAS序列一一对应连接；

[0044] 所述核电站反应堆保护系统还具备安全级控制显示设备SCID，其分为三组，每组通过一个所述安全级子环网与一个所述ESFAS序列及一个所述SAS序列一一对应连接，每组SCID根据操作人员的操作指令输出第二设备级控制指令；

[0045] 在所述安全自动化步骤中，所述SAS序列接收所述第二设备级控制指令，并对所述第一设备级控制指令与所述第二设备级控制指令进行或逻辑处理，输出第三设备级控制指令，所述第三设备级控制指令用于对反应堆从可控状态到安全停堆状态需要操作的执行机构进行控制。

发明的有益效果

有益效果

[0046] 在本发明提供的核电站反应堆保护系统及其安全控制方法中，对反应堆达到可控状态前与达到可控状态至安全停堆状态的保护功能进行区分处理，具体地，通过安全级环网，对用于实现重要的系统级自动控制功能的专设驱动系统，以及用于实现设备级安全辅助、支持功能的安全自动化系统分开实现，相对于现有技术中没有区分专设驱动系统与安全自动化系统而降两者的功能混杂在一个子系统中，本发明能够降低保护系统维护、定期试验的方案复杂程度。

对附图的简要说明

附图说明

[0047] 为了更清楚的说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0048] 图1为本发明提供的核电站反应堆保护系统的结构示意图；

[0049] 图2为本发明提供的核电站反应堆保护系统中的安全控制方法的流程图。

实施该发明的最佳实施例

本发明的最佳实施方式

[0050] 下面结合附图对本发明实施例的技术方案进行清楚、完整地描述，显然，所描述的实施例仅仅是本发明的一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动的前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0051] 实施例一

[0052] 以下，结合附图对本实施例提供的核电站反应堆保护系统进行说明。图1为本发明实施例一提供的核电站反应堆保护系统的结构示意图。

[0053] 如图1所示，核电站反应堆保护系统100主要具备紧急停堆系统（Reactor Trip System, RTS）10、专设驱动系统（Engineering Safety Features Actuation System, ESFAS）20、安全自动化系统（Safety Automation System, SAS）30及安全级环网SB（Safety System Bus）40。

[0054] 紧急停堆系统10具有如下功能：当反应堆运行中出现设计基准事故时，触发反应堆停堆，以实现对反应堆反应性的控制，一回路余热排出，反应堆放射性包容等保护功能。

[0055] 紧急停堆系统10分为冗余的N个保护通道，每个保护通道内具有相同的结构。其中，N为偶数且 $N \geq 2$ 。在本实施例中，以 $N=4$ 为例进行说明。4个保护通道分别为RTS IP、RTS IIP、RTS IIIP及RTS IVP。如后文所述，每个保护通道主要由停堆保护控制柜（Reactor Protection Cabinet, RPC）组成，如图1所示，4个保护通道分别对应RPC-I、RPC-II、RPC-III、RPC-IV。

[0056] 核电站反应堆保护系统100还包括N列信号预处理系统SPS（Signal Processing System）11。信号预处理系统11主要具备用于采集保护参数的传感器S及对传感器S采集的保护参数进行隔离、调理、分配等预处理的信号预处理柜（Signal Processing Cabinet, SPC）。保护参数是指核电站中与安全状态相关的各种参数，例如，稳压器的水位、稳压器的压力等。

[0057] 信号预处理系统11与保护通道一一对应。在本实施例中，对应于保护通道分为

4个，信号预处理系统11同样分为4列，对应的4个信号预处理柜为SPC-I、SPC-II、SPC-III、SPC-IV。每个保护通道均对应连接一列信号预处理系统11。例如，保护通道RTS IP连接信号预处理柜SPC-I对应的信号预处理系统，保护通道RTS IIP连接信号预处理柜SPC-II对应的信号预处理系统。

[0058] 每个保护通道（RTS IP、RTS IIP、RTS IIIP及RTS IVP）从对应的信号预处理系统11获取被预处理之后的保护参数。为了判断保护参数是否满足安全状态的要求，可设置相应的阈值。保护通道可将保护参数与阈值进行比较，得到阈值比较结果。举例而言，对于一回路中稳压器（未图示）的水位，设置一个阈值为安全水位，当稳压器的水位高于安全水位时，得到阈值比较结果“1”，用于表征稳压器的水位处于非安全状态；当稳压器的水位低于安全水位时，得到阈值比较结果“0”，用于表征稳压器的水位处于安全状态。如后文所述，阈值比较结果一方面供专设驱动系统20处理，另一方面供紧急停堆系统10处理。

[0059] 专设驱动系统20用于在核电站发生设计基准事故后将核电站带至可控状态，具体地，其可触发与设计基准事故相应的专设安全设施动作，例如安全注入、启动应急给水等。

[0060] 专设驱动系统20可分为冗余的多个序列，即ESFAS序列。每个ESFAS序列具有相同的结构，主要由专设驱动柜（Engineering Safety Features Actuation Cabinet, ESFAC）构成，ESFAC用于实现专设驱动系统20的功能，其中可配置并行的、冗余的两个运算处理器。在此，以3个ESFAS序列ESFAS A、ESFAS B、ESFAS C为例。如图1所示，3个ESFAS序列分别对应ESFAC-A、ESFAC-B、ESFAC-C。ESFAC-A配置有两个运算处理器A1、A2，ESFAC-B配置有两个运算处理器B1、B2，ESFAC-C配置有两个运算处理器C1、C2。

[0061] 专设驱动系统20与紧急停堆系统10的N个保护通道连接，更具体地，每个ESFAS序列均与N个保护通道通过点对点通讯连接。例如，ESFAC-A对应的ESFAS A与4个RPC-I、RPC-II、RPC-III、RPC-IV各自对应的RTS IP、RTS IIP、RTS IIIP、RTS IVP均连接。专设驱动系统20可接收每个保护通道各自得到的阈值比较结果，即N个阈值比较结果。在此，专设驱动系统20对N个阈值比较结果进行专设

驱动逻辑处理，输出第一专设驱动指令，第一专设驱动指令用于在可控状态前驱动与设计基准事故相应的专设安全设施（执行机构的一种），使得反应堆达到可控状态。因此，专设驱动逻辑处理是指，根据阈值比较结果确定需驱动的专设安全设施及其驱动方式。如后文所述，第一专设驱动指令将通过安全级环网40传输。

[0062] 区别于专设驱动系统20，安全自动化系统30用于将反应堆从可控状态带至安全停堆状态。而且，专设驱动系统20基于保护参数进行对专设安全设施进行系统级的驱动控制，而安全自动化系统30基于操作人员的手动输入操作对专设安全设施进行设备级的驱动控制。

[0063] 安全自动化系统30同样可分为多个序列，即SAS序列。每个SAS序列具有相同的结构，主要由安全自动化柜（Safety Automation Cabinet，SAC）构成，SAC用于实现安全自动化系统30的功能，每个SAS序列可配置热备冗余运算处理器（未图示）。如图1所示，以3个SAS序列SAS A、SAS B、SAS C为例。在此，安全自动化系统30根据操作人员输入的指令，输出第一设备级控制指令，第一设备级控制指令是针对单个设备的控制指令，用于对反应堆从可控状态到安全停堆状态需要操作的执行机构进行控制。

[0064] 安全级环网40是保护系统100中为连接专设驱动系统20及安全自动化系统30而设置的，用于将第一专设驱动指令与第一设备级控制指令输送至相应的执行机构。对应于专设驱动系统20与安全自动化系统30的冗余化设置，安全级环网40同样可以进行冗余化设置，即，安全级环网40分为多组。如图1所示，安全级环网40分为三组安全级子环网，分别为Train A、Train B、Train C。每组安全级子环网用于连接一个ESFAS序列及一个SAS序列，即，每个SAS序列通过一个安全级子环网与一个ESFAS序列一一对应连接。例如，SAS序列SAS A通过安全级子环网Train A与ESFAS序列ESFAS A连接，SAS序列SAS B通过安全级子环网Train B与ESFAS序列ESFAS B连接。

[0065] 由以上可知，在本实施例提供的核电站反应堆保护系统100中，对反应堆达到可控状态前与达到可控状态至安全停堆状态的保护功能进行区分处理，具体地，通过安全级环网40，对用于实现重要的系统级自动控制功能的专设驱动系统2

0, 以及用于实现设备级安全辅助、支持功能的安全自动化系统30分开实现, 相对于现有技术中没有区分专设驱动系统与安全自动化系统而降两者的功能混杂在同一个子系统中, 本发明能够降低保护系统维护、定期试验的方案复杂程度。

[0066] 实施例二

[0067] 本实施例在实施例一的基础上, 对现有技术中的核电站反应堆保护系统进行进一步改进。

[0068] 现有技术中, 针对二代压水堆核电站控制序列一般只分为A、B两列, 核级DCS平台相应地做A、B两列的结构设计。然而, 随着三代压水堆核电站的引入, 而三代压水堆核电站分为三个控制序列, 因此, 现有技术中的核电站反应堆保护系统的两列控制序列设计无法满足三代压水堆核电站的要求。

[0069] 为此, 本实施例提供的专设驱动系统20分为三个以上的ESFAS序列, 优选为三个ESFAS序列。如实施例一所述, 每个ESFAS序列均与N个保护通道连接。

[0070] 在本实施例中, 通过将专设驱动系统20设计为三个ESFAS序列, 能够满足核电站的工艺控制需求。而且, 三个控制序列相比两个控制序列能够进一步优化核电站控制功能的冗余性及独立性, 进而提高保护系统仪控实现的可靠性。

[0071] 如上所述, 每个ESFAS序列主要由ESFAC构成。ESFAC中的运算处理器除了用于实现专设驱动逻辑处理外, 还可用于对每个ESFAS序列接收的N个阈值比较结果进行符合逻辑处理。符合逻辑处理包括N取一符合逻辑、N取二符合逻辑等。以N=4为例, 每个ESFAS符合逻辑电路可对来自4个保护通道的4个阈值比较结果进行四取二符合逻辑处理。符合逻辑处理的输出结果供专设驱动逻辑电路进行专设驱动逻辑处理。

[0072] 并且, 当N个保护通道中的部分保护通道失效时, 按照符合逻辑退化原则进行处理。所谓符合逻辑退化原则是指, 当N个保护通道中的某个保护通道失效时, 符合逻辑处理退化为N-1取一符合逻辑、N-1取二符合逻辑等; 当N-1个保护通道中的某个保护通道失效时, 符合逻辑处理进一步退化为N-2取一符合逻辑、N-2取二符合逻辑等。举例而言, ESFAS符合逻辑电路初始时对来自4个保护通道的4个阈值比较结果进行四取二符合逻辑处理, 当某个保护通道失效时, 退化为

三取二符合逻辑处理，当又有一个保护通道失效时，进一步退化为二取一符合逻辑处理。

[0073] 另外，虽然在上述说明中初始时以N取二符合逻辑为例进行说明，但初始时也可进行N取一符合逻辑或N-1取二等。

[0074] 另外，在本实施例中，通过设置ESFAS符合逻辑电路，使得在保护通道部分失效的情况下也能够确保专设驱动系统20功能的正常实现。

[0075] 实施例三

[0076] 在上述实施例一或实施例二的基础上，本实施例用于对紧急停堆系统10进行进一步说明。

[0077] 紧急停堆系统10的N个保护通道之间点对点连接，每个保护通道从另外N-1个保护通道获取阈值比较结果。如图1所示，RPC-I从RPC-II~RPC-IV获取阈值比较结果。

[0078] 每个保护通道均具备热备冗余处理器（未图示），热备冗余处理器根据来自N个保护通道的N个阈值比较结果得到第三局部停堆信号。每个保护通道均连接停堆断路器，停堆断路器从每个保护通道获取第三局部停堆信号，并执行第三局部停堆信号控制核电站停堆。

[0079] 更具体地，紧急停堆系统10的每个保护通道均分为第一子组与第二子组，还包括与第一子组、第二子组连接的RTS或逻辑处理电路。每个子组内配热备冗余处理器（未图示），第一子组内的称为第一热备冗余处理器，第二子组内的称为第二热备冗余处理器。

[0080] 所分得的N个第一子组之间点对点连接，所分得的N个第二子组之间点对点连接。如图1所示，保护通道RTS IP的停堆保护控制柜RPC-I分为第一子组Sub1与第二子组Sub2。其他保护通道RTS IIP~RTS IVP同样分为第一子组Sub1与第二子组Sub2。4个第一子组Sub1之间两两连接，4个第二子组Sub2之间两两连接。

[0081] 根据两两连接的关系，每个第一子组均从另外N-1个第一子组获取阈值比较结果。第一热备冗余处理器用于对来自N个第一子组的N个阈值比较结果进行符合逻辑处理，即对该第一RTS符合逻辑电路所在的第一子组的1个阈值比较结果及另外N-1个第一子组的N-1个阈值比较结果进行符合逻辑处理。并且，在N个保护

通道中的部分保护通道失效时，按照符合逻辑退化原则进行处理，输出第一局部停堆信号。类似于第三局部停堆信号，第一局部停堆信号同样用于控制核电站停堆，但是，第一局部停堆信号属于中间信号。

[0082] 同样地，根据两两连接的关系，每个第二子组均从另外 $N-1$ 个第二子组获取阈值比较结果。第二热备冗余处理器用于对来自 N 个第二子组的 N 个阈值比较结果进行符合逻辑处理，并且在 N 个保护通道中的部分保护通道失效时，按照符合逻辑退化原则进行处理，输出第二局部停堆信号。第二局部停堆信号属于中间信号。

[0083] 需要说明的是，在本实施例中，根据多样化设计需求，第一子组Sub1及第二子组Sub2可分别处理不同类型的保护参数及其阈值比较结果，执行不同的保护功能。

[0084] 紧急停堆系统10的每个保护通道还均具备RTS或逻辑处理电路，在图1中用符号“ ≥ 1 ”表示。RTS或逻辑处理电路与第一子组Sub1及第二子组Sub2连接。根据与第一子组及第二子组的连接关系，RTS或逻辑处理电路对第一局部停堆信号与第二局部停堆信号进行或逻辑处理，输出第三局部停堆信号。

[0085] 如上所述，紧急停堆系统10用于当反应堆运行中出现设计基准事故时触发紧急停堆。在此，第三局部停堆信号可通过硬接线传输至停堆断路器RTB，从而触发紧急停堆。需要说明的是，与 N 个第三局部停堆信号相对应，停堆断路器RTB同样可设置为 N 对， N 对停堆断路器可通过硬接线实现 N 取二符合逻辑等，即至少两对停堆断路器打开才可实现紧急停堆。如有保护通道故障或失效，则停堆断路器硬接线符合逻辑依次退化为三取二、二取一。

[0086] 在本实施例中，通过第一子组Sub1及第二子组Sub2的设置，使得在保护通道部分失效的情况下也能够确保紧急停堆系统10功能的正常实现。

[0087] 在实施例二及三的一个更具体的实施方式中，核电站反应堆保护系统100还可设置紧急控制盘ECP（Emergency Control Panel）70。紧急控制盘70的手动专设驱动按钮与专设驱动系统20通过硬接线连接，用于根据操作人员的操作指令输出第二专设驱动指令。类似于第一专设驱动指令，第二专设驱动指令同样用于驱动反应堆达到可控状态前需要操作的执行机构。

- [0088] 专设驱动系统20可接收紧急控制盘70输出的第二专设驱动指令，其中的运算处理器还可用于对第一专设驱动指令与第二专设驱动指令进行或逻辑处理，输出第三专设驱动指令。类似地，第三专设驱动指令用于驱动反应堆达到可控状态前需要操作的执行机构。可以理解的是，在设置紧急控制盘70的情况下，在运算处理器的或逻辑处理的控制下，第一专设驱动指令与第二专设驱动指令转换为第三专设驱动指令，仅第三专设驱动指令输送至执行机构。
- [0089] 在该更具体的实施方式中，通过紧急控制盘70的设置，能够代替专设驱动系统20实现对专设安全设施的紧急驱动。通过运算处理器的或逻辑处理，能够协调专设驱动系统20与紧急控制盘70对专设安全设施的驱动。
- [0090] 除了代替专设驱动系统20实现对专设安全设施的紧急驱动外，紧急控制盘70还可直接手动实现紧急控制核电站停堆。在此，紧急控制盘70通过硬接线直接连接停堆断路器RTB，并向停堆断路器RTB输出第四局部停堆信号。停堆断路器RTB可获取并执行第四局部停堆信号控制核电站停堆。
- [0091] 与紧急控制盘70相对，核电站反应堆保护系统100还可设置可视化的安全级控制显示设备SCID（Safety Control and Information Device）80，其用于代替安全自动化系统30紧急驱动执行机构。在此，安全级控制显示设备80分为三组，每组通过一个安全级子环网与一个ESFAS序列及一个SAS序列一一对应连接。例如，组SCID A通过Train A与ESFAC-A及SAS A连接。并且，安全级控制显示设备80与安全自动化系统30连接，用于根据操作人员的操作指令输出第二设备级控制指令。
- [0092] 每组根据操作人员的操作指令输出第二设备级控制指令，对应的SAS序列接收该第二设备级控制指令，并对自身的第一设备级控制指令与该第二设备级控制指令进行或逻辑处理，输出第三设备级控制指令。类似地，第三设备级控制指令用于对反应堆从可控状态到安全停堆状态需要操作的执行机构进行控制。
- [0093] 通过安全级控制显示设备80的设置，同样能够实现对专设安全设施的紧急驱动。通过SAS或逻辑处理电路的设置，能够协调安全自动化系统30与安全级控制显示设备80对专设安全设施的驱动。
- [0094] 实施例四

- [0095] 在上述实施例一至实施例三中任一实施例的基础上，本实施例对现有技术中的核电站反应堆保护系统100进行进一步改进。
- [0096] 本实施例涉及预期瞬态不停堆系统(Anticipated Transient Without Trip System, ATWS)，ATWS对应通过多样化停堆控制及跳机，启动应急给水等功能缓解保护系统未能实现紧急停堆情况下的后果。
- [0097] 在本实施例中，还设置多样化驱动系统KDS (Diversity Actuation System) 50，其用于实现ATWS系统的功能。多样化驱动系统50可与每列信号预处理系统11连接，用于在紧急停堆系统10与专设驱动系统20发生共模失效的情况下，从信号预处理系统11获取保护参数，并根据所述保护参数输出停堆控制指令。
- [0098] 多样化驱动系统50还与棒控系统 (Full Length Rod Control System, RGL) 连接，棒控系统从多样化驱动系统50接收该停堆控制指令，并执行该停堆控制指令控制核电站停堆。因此，多样化驱动系统50能够在核电站反应堆保护系统100共模失效情况下，保证关键的保护功能实现。
- [0099] 并且，由于ATWT的功能被放在多样化驱动系统50中实现，因而不需要再单独设计一套ATWT实体机柜来实现该多样化功能，从而精简了核电站反应堆保护系统100。
- [0100] 在上述说明中，多样化驱动系统50与每列信号预处理系统11连接，从信号预处理系统11获取保护参数，但本发明不仅限于此，多样化驱动系统50可通过硬接线与第三方系统 (未图示) 连接，直接通过硬接线从第三方系统获取保护参数，或者，从现场仪表获取保护参数。
- [0101] 另外，多样化驱动系统50还可用于根据保护参数输出第三专设驱动指令，第三专设驱动指令同样用于驱动反应堆达到可控状态前需要操作的执行机构。第三专设驱动指令可传输至后述的接口及优先级模块CIM 60。
- [0102] 另外，当紧急停堆系统10、专设驱动系统20正常时，多样化驱动系统50的自动逻辑功能正常运行，但手动操作指令闭锁。
- [0103] 需要说明的是，多样化驱动系统50中实现的功能一般不属于核电站反应堆保护系统100中实现的保护功能，但是，在本发明中，鉴于核电站反应堆保护系统100与多样化驱动系统50的设置具有密切的关系，且ATWS系统功能在多样化驱动

系统50中实现，因此，可将多样化驱动系统50看作核电站反应堆保护系统100的一部分。

[0104] 另外，在现有技术中，没有对专设驱动系统20与安全自动化系统30进行区分设计，因此，第一专设驱动指令与第一设备级控制指令也没有被区分开来。然而，第一专设驱动指令相对于保护系统100而言更为重要，若不对两种指令进行优先级划分，将无法高效地实现保护系统100的功能。

[0105] 为此，核电站反应堆保护系统100还设置设备接口及优先级模块CIM 60。设备接口及优先级模块60与安全自动化系统30及多样化驱动系统50连接。设备接口及优先级模块60可分为三个序列，每个序列主要由设备接口及优先级柜CIC构成。如图1所示，CIM分为CIC A、CIC B、CIC

C这3个序列。并且，3个序列与3个SAS序列SAS A、SAS B、SAS C一一对应连接。设备接口及优先级模块60用于获取第一设备级控制指令及第三专设驱动指令。此外，设备接口及优先级模块60还获取专设驱动系统20。输出的第一专设驱动指令，其中第一专设驱动指令通过安全级环网40及安全自动化系统30。

[0106] 可以理解的是，虽然在上述说明中，第一设备级控制指令、第三专设驱动指令及第一专设驱动指令直接送至对应的执行机构，但是，在设置设备接口及优先级模块60的情况下，这些指令可先经过设置设备接口及优先级模块60的优先级处理之后再送至执行机构。也即，设备接口及优先级模块60可对接收到的多个指令进行优先级处理，确定优先级最高的指令，使得执行机构优先执行优先级最高的指令，因此，能够高效地实现保护系统的功能。

[0107] 另外，通过图1可以看出，本实施例提供的核电站反应堆保护系统100中不需要针对保护系统多样化设计要求另外设计一套冗余继电器硬逻辑，也即，不需要大规模的功能冗余继电器机柜。

[0108] 与此相对，在现有的核电站反应堆保护系统中，为了满足保护系统多样化设计要求，除采用数字化技术实现A、B两列监控功能外，另外设计一套继电器硬接线逻辑设计，实现数字化平台中重要的系统级控制功能的多样化冗余设计。

[0109] 本实施例提供的核电站反应堆保护系统100中由于采用了多样化驱动系统，因此，保护系统100不需针对重要保护功能增配一套继电器逻辑，大量减少了安全

级继电器机柜数量，精简了电缆数量，同时给电气厂房的布置降低了难度。另外，继电器逻辑的减少大大简化了电厂定期试验的要求，也降低了设备老化造成的故障风险。

[0110] 实施例五

[0111] 本实施例提供一种核电站反应堆保护系统中的安全控制方法，应用于对应于上述实施例一至实施例四所提供的任一核电站反应堆保护系统100中。如图2所示，所述方法包括如下步骤：

[0112] 阈值比较步骤S1，其由紧急停堆系统RTS执行，紧急停堆系统分为N个保护通道，N为偶数且 $N \geq 2$ ，每个保护通道均对应连接一列信号预处理系统，其中，每个保护通道从对应的信号预处理系统获取保护参数，并根据保护参数进行阈值比较，得到阈值比较结果；

[0113] 专设驱动步骤S2，其由专设驱动系统ESFAS执行，专设驱动系统与N个保护通道连接，用于接收每个保护通道的阈值比较结果，并根据阈值比较结果进行专设驱动逻辑处理，输出第一专设驱动指令，第一专设驱动指令用于驱动反应堆达到可控状态前需要操作的执行机构；

[0114] 安全自动化步骤S3，其由安全自动化系统SAS执行，安全自动化系统通过安全级环网与专设驱动系统连接，产生第一设备级控制指令，第一设备级控制指令用于对反应堆从可控状态到安全停堆状态需要操作的执行机构进行控制。

[0115] 关于各步骤的具体说明，可参照实施例一至实施例四的说明，在此不再赘述。根据本实施例提供的核电站反应堆保护系统中的安全控制方法，能够降低保护系统维护、定期试验的方案复杂程度。

[0116] 在实施例五的一个更具体实施例中，专设驱动系统分为三个ESFAS序列，每个ESFAS序列均与N个保护通道通过点对点通讯连接；

[0117] 每个ESFAS序列均配置并行的、冗余的两个运算处理器；

[0118] 在专设驱动步骤S2中，运算处理器对每个ESFAS序列接收的N个阈值比较结果进行符合逻辑处理，并且在N个保护通道中的部分保护通道失效时，按照符合逻辑退化原则进行处理。

[0119] 在实施例五的另一个更具体实施例中，核电站反应堆保护系统还具备紧急控制

盘ECP，紧急控制盘ECP的手动专设驱动按钮与专设驱动系统连接，根据操作人员的操作指令输出第二专设驱动指令；

[0120] 在专设驱动步骤S2中，运算处理器对第一专设驱动指令与第二专设驱动指令进行或逻辑处理，输出第三专设驱动指令，第三专设驱动指令用于驱动反应堆达到可控状态前需要操作的执行机构。

[0121] 在实施例五的又一个更具体实施例中，安全自动化系统分为三个SAS序列，安全级环网分为三组安全级子环网，每个SAS序列通过一个安全级子环网与一个ESFAS序列一一对应连接；

[0122] 核电站反应堆保护系统还具备安全级控制显示设备SCID，其分为三组，每组通过一个安全级子环网与一个ESFAS序列及一个SAS序列一一对应连接，每组SCID根据操作人员的操作指令输出第二设备级控制指令；

[0123] 在安全自动化步骤S3中，SAS序列接收第二设备级控制指令，并对第一设备级控制指令与第二设备级控制指令进行或逻辑处理，输出第三设备级控制指令，第三设备级控制指令用于对反应堆从可控状态到安全停堆状态需要操作的执行机构进行控制。

[0124] 在实施例五的又一个更具体实施例中，N个保护通道之间点对点连接，每个保护通道均具备热备冗余处理器，每个保护通道均连接停堆断路器，

[0125] 方法还包括停堆控制步骤S4，在停堆控制步骤S4中，每个保护通道从另外N-1个保护通道获取阈值比较结果，热备冗余处理器根据来自N个保护通道的N个阈值比较结果得到第三局部停堆信号，停堆断路器从每个保护通道获取第三局部停堆信号，并执行第三局部停堆信号控制核电站停堆。

[0126] 关于实施例五的各个更具体实施例中各步骤的具体说明，同样可参照实施例一至实施例四的说明，在此不再赘述。

[0127] 以上所述，仅为本发明的具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应以权利要求的保护范围为准。

权利要求书

- [权利要求 1] 一种核电站反应堆保护系统，其特征在于，具备：
- 紧急停堆系统RTS，其分为N个保护通道，N为偶数且 $N \geq 2$ ，每个保护通道均对应连接一列信号预处理系统，其中，所述每个保护通道从对应的所述信号预处理系统获取保护参数，并根据所述保护参数进行阈值比较，得到阈值比较结果；
- 专设驱动系统ESFAS，其与所述N个保护通道连接，用于接收每个保护通道的阈值比较结果，并根据所述阈值比较结果进行专设驱动逻辑处理，输出第一专设驱动指令，所述第一专设驱动指令用于驱动反应堆达到可控状态前的执行机构；
- 安全自动化系统SAS，其通过安全级环网与所述专设驱动系统ESFAS连接，用于产生第一设备级控制指令，所述第一设备级控制指令用于对从反应堆达到可控状态到安全停堆状态的执行机构进行控制。
- [权利要求 2] 根据权利要求1所述的保护系统，其特征在于，所述专设驱动系统ESFAS分为三个ESFAS序列，每个ESFAS序列均与所述N个保护通道通过点对点通讯连接。
- [权利要求 3] 根据权利要求2所述的保护系统，其特征在于，
- 所述每个ESFAS序列均配置并行的、冗余的两个运算处理器。
- [权利要求 4] 根据权利要求3所述的保护系统，其特征在于，
- 所述运算处理器用于对所述每个ESFAS序列接收的N个所述阈值比较结果进行符合逻辑处理，并且在所述N个保护通道中的部分保护通道失效时，按照符合逻辑退化原则进行处理。
- [权利要求 5] 根据权利要求3或4所述的保护系统，其特征在于，
- 还具备紧急控制盘ECP，其手动专设驱动按钮与所述专设驱动系统ESFAS通过硬接线连接，用于根据操作人员的操作指令输出第二专设驱动指令；
- 所述运算处理器还用于对所述第一专设驱动指令与所述第二专设驱动指令进行或逻辑处理，输出第三专设驱动指令，所述第三专设驱动指

令用于驱动反应堆达到可控状态前需要操作的执行机构。

[权利要求 6] 根据权利要求2所述的保护系统，其特征在于，
所述安全自动化系统SAS分为三个SAS序列，所述安全级环网分为三组安全级子环网，每个SAS序列通过一个所述安全级子环网与一个所述ESFAS序列一一对应连接。

[权利要求 7] 根据权利要求6所述的保护系统，其特征在于，
还具备安全级控制显示设备SCID，其分为三组，每组SCID通过一个所述安全级子环网与一个所述ESFAS序列及一个所述SAS序列一一对应连接；
每组SCID根据操作人员的操作指令输出第二设备级控制指令，所述SAS序列接收所述第二设备级控制指令，并对所述第一设备级控制指令与所述第二设备级控制指令进行或逻辑处理，输出第三设备级控制指令，所述第三设备级控制指令用于对反应堆从可控状态到安全停堆状态需要操作的执行机构进行控制。

[权利要求 8] 根据权利要求1所述的保护系统，其特征在于，
所述N个保护通道之间点对点连接，所述每个保护通道从另外N-1个保护通道获取所述阈值比较结果，
所述每个保护通道均具备热备冗余处理器，所述热备冗余处理器根据来自所述N个保护通道的所述N个所述阈值比较结果得到第三局部停堆信号，
所述每个保护通道均连接停堆断路器，所述停堆断路器从所述每个保护通道获取所述第三局部停堆信号，并执行所述第三局部停堆信号控制核电站停堆。

[权利要求 9] 根据权利要求8所述的保护系统，其特征在于，
所述每个保护通道均分为第一子组与第二子组，所分得的N个所述第一子组之间点对点连接，所分得的N个所述第二子组之间点对点连接；
每个第一子组均从另外N-1个第一子组获取所述阈值比较结果，每个

第一子组均具备第一热备冗余处理器，所述第一热备冗余处理器用于对来自所述N个第一子组的N个所述阈值比较结果进行符合逻辑处理，并且在N个保护通道中的部分保护通道失效时，按照退化原则进行符合逻辑处理，输出第一局部停堆信号；

每个第二子组均从另外N-1个第二子组获取所述阈值比较结果，每个第二子组均具备第二热备冗余处理器，所述第二热备冗余处理器用于对来自所述N个第二子组的N个所述阈值比较结果进行符合逻辑处理，并且在N个保护通道中的部分保护通道失效时，按照退化原则进行符合逻辑处理，输出第二局部停堆信号；

所述紧急停堆系统RTS的每个保护通道还均具备RTS或逻辑处理电路，所述RTS或逻辑处理电路与所述第一子组及所述第二子组连接，用于对所述第一局部停堆信号与所述第二局部停堆信号进行或逻辑处理，输出所述第三局部停堆信号。

[权利要求 10]

根据权利要求8所述的保护系统，其特征在于，
还具备紧急控制盘ECP，所述紧急控制盘的手动停堆控制按钮通过硬接线直接连接所述停堆断路器，并向所述停堆断路器输出第四局部停堆信号，所述停堆断路器获取并执行所述第四局部停堆信号控制核电站停堆。

[权利要求 11]

根据权利要求1所述的保护系统，其特征在于，
还具备多样化驱动系统KDS，其实现预期瞬态不停堆系统的系统ATWS的功能，用于在所述保护系统发生共模失效的情况下，从所述信号预处理系统或现场仪表或第三方监测系统获取保护参数，并根据所述保护参数输出停堆控制指令，
所述多样化驱动系统与棒控系统连接，所述棒控系统从所述多样化驱动系统接收所述停堆控制指令，并执行所述停堆控制指令控制核电站停堆。

[权利要求 12]

根据权利要求11所述的保护系统，其特征在于，
所述多样化驱动系统还用于根据所述保护参数输出第三专设驱动指令

，所述第三专设驱动指令用于驱动反应堆达到可控状态前需要操作的执行机构。

[权利要求 13] 根据权利要求12所述的保护系统，其特征在于，
还具备设备接口及优先级模块CIM，其与所述安全自动化系统SAS及所述多样化驱动系统连接，用于获取所述第一设备级控制指令及所述第三专设驱动指令，还通过所述安全级环网及所述安全自动化系统SAS获取所述专设驱动系统ESFAS输出的所述第一专设驱动指令，并对获取到的多个指令进行优先级处理。

[权利要求 14] 根据权利要求11所述的保护系统，其特征在于，
当所述紧急停堆系统RTS、所述专设驱动系统ESFAS正常时，所述多样化驱动系统的自动逻辑功能正常运行，手动操作指令闭锁。

[权利要求 15] 一种核电站反应堆保护系统中的安全控制方法，其特征在于，包括如下步骤：

阈值比较步骤，其中，紧急停堆系统RTS的多个保护通道均从对应的信号预处理系统获取保护参数，并对所述保护参数进行阈值比较，得到阈值比较结果；

专设驱动步骤，其中，专设驱动系统ESFAS接收每个保护通道的阈值比较结果，并根据所述阈值比较结果进行专设驱动逻辑处理，输出第一专设驱动指令，所述第一专设驱动指令用于驱动反应堆达到可控状态前需要操作的执行机构；

安全自动化步骤，其中，安全自动化系统SAS产生第一设备级控制指令，所述第一设备级控制指令用于对反应堆从可控状态到安全停堆状态需要操作的执行机构进行控制。

[权利要求 16] 根据权利要求15所述的方法，其特征在于，
所述专设驱动系统ESFAS分为三个ESFAS序列，每个ESFAS序列均与多个保护通道通过点对点通讯连接；
所述每个ESFAS序列均配置并行的、冗余的两个运算处理器；
在所述专设驱动步骤中，所述运算处理器对所述每个ESFAS序列接收

的多个所述阈值比较结果进行符合逻辑处理，并且在所述多个保护通道中的部分保护通道失效时，按照符合逻辑退化原则进行处理。

[权利要求 17]

根据权利要求16所述的方法，其特征在于，

所述核电站反应堆保护系统还具备紧急控制盘ECP，所述紧急控制盘ECP的手动专设驱动按钮与所述专设驱动系统ESFAS连接，根据操作人员的操作指令输出第二专设驱动指令；

在所述专设驱动步骤中，所述运算处理器对所述第一专设驱动指令与所述第二专设驱动指令进行或逻辑处理，输出第三专设驱动指令，所述第三专设驱动指令用于驱动反应堆达到可控状态前需要操作的执行机构。

[权利要求 18]

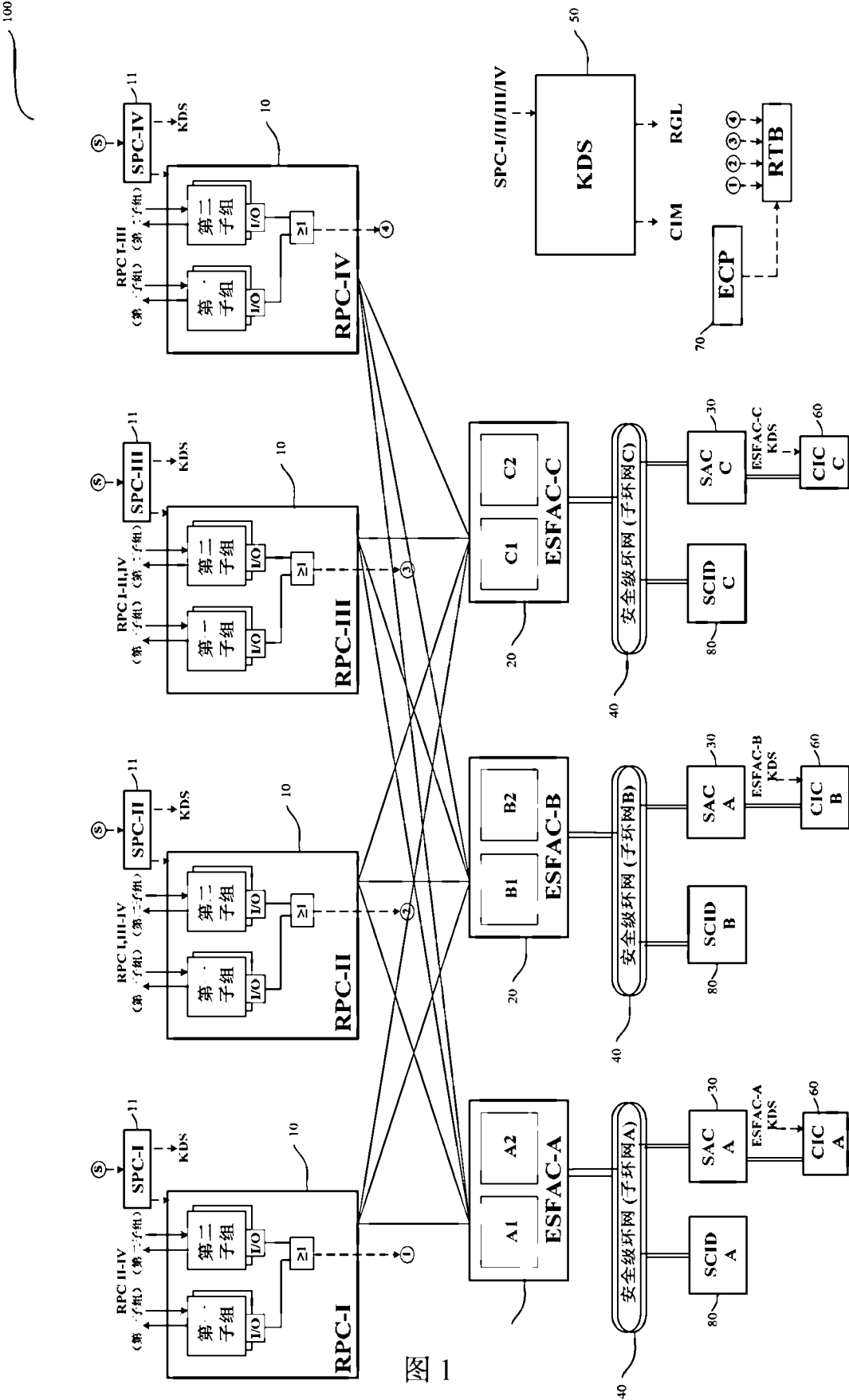
根据权利要求16所述的方法，其特征在于，

所述安全自动化系统SAS分为三个SAS序列，所述安全级环网分为三组安全级子环网，每个SAS序列通过一个所述安全级子环网与一个所述ESFAS序列一一对应连接；

所述核电站反应堆保护系统还具备安全级控制显示设备SCID，其分为三组，每组通过一个所述安全级子环网与一个所述ESFAS序列及一个所述SAS序列一一对应连接，每组SCID根据操作人员的操作指令输出第二设备级控制指令；

在所述安全自动化步骤中，所述SAS序列接收所述第二设备级控制指令，并对所述第一设备级控制指令与所述第二设备级控制指令进行或逻辑处理，输出第三设备级控制指令，所述第三设备级控制指令用于对反应堆从可控状态到安全停堆状态需要操作的执行机构进行控制。

说明书附图



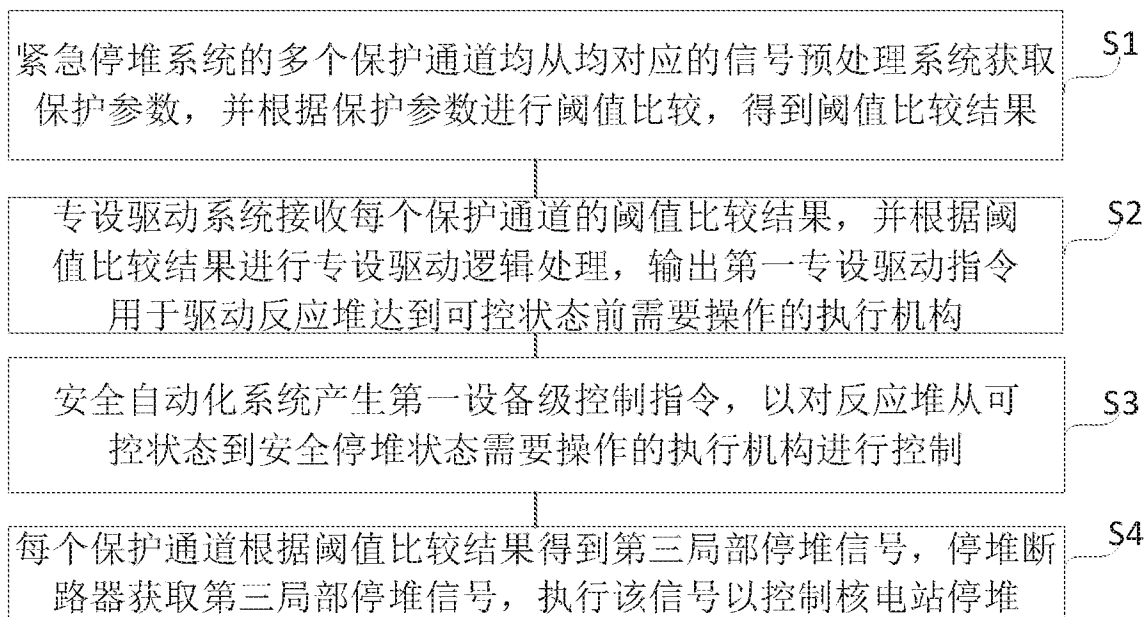


图 2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2015/097513

A. CLASSIFICATION OF SUBJECT MATTER

G21C 9/00 (2006.01) i; G21D 3/04 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G21C 9; G21D 3

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNKI; CNABS; CNTXT; VEN; EPODOC; WPI: nuclear, reactor, protect+, safety, reactor trip system, RTS, engineering safety features
actuation system, ESFAS, safety automation system, SAS, threshold, compar+, driv+, initiat+, actuat+, control+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2015/112304 A2 (NUSCALE POWER, LLC) 30 July 2015 (30.07.2015) the whole document	1-18
A	CN 102426863 A (CHINA GUANGDONG NUCLEAR POWER GROUP CO., LTD. et al.) 25 April 2012 (25.04.2012) the whole document	1-18
A	CN 102157208 B (CHINA GUANGDONG NUCLEAR POWER GROUP CO., LTD. et al.) 27 March 2013 (27.03.2013) the whole document	1-18
A	CN 101783192 B (CHINA GUANGDONG NUCLEAR POWER GROUP CO., LTD. et al.) 18 July 2012 (18.07.2012) the whole document	1-18
A	CN 101968974 B (CHINA GUANGDONG NUCLEAR POWER GROUP CO., LTD. et al.) 02 January 2013 (02.01.2013) the whole document	1-18

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“A” document defining the general state of the art which is not considered to be of particular relevance	“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“E” earlier application or patent but published on or after the international filing date	“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	“&” document member of the same patent family
“O” document referring to an oral disclosure, use, exhibition or other means	
“P” document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 16 August 2016	Date of mailing of the international search report 23 August 2016
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer WANG, Shuling Telephone No. (86-10) 62085648

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/CN2015/097513

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
WO 2015/112304 A2	30 July 2015	None	
CN 102426863 A	25 April 2012	CN 102426863 B	16 December 2015
CN 102157208 B	27 March 2013	CN 102157208 A	17 August 2011
CN 101783192 B	18 July 2012	CN 101783192 A	21 July 2010
CN 101968974 B	02 January 2013	CN 101968974 A	09 February 2011

A. 主题的分类 G21C 9/00(2006.01)i; G21D 3/04(2006.01)i 按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类		
B. 检索领域 检索的最低限度文献(标明分类系统和分类号) G21C 9, G21D 3 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用)) CNKI, CNABS, CNTXT, VEN, EPODOC, WPI, nuclear, reactor, protect+, safety, reactor trip system, RTS, engineering safety features actuation system, ESFAS, safety automation system, SAS, threshold, compar+, driv+, initiat+, actuat+, control+		
C. 相关文件		
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
A	WO 2015/112304 A2 (NUSCALE POWER, LLC) 2015年 7月 30日 (2015 - 07 - 30) 全文	1-18
A	CN 102426863 A (中广核工程有限公司等) 2012年 4月 25日 (2012 - 04 - 25) 全文	1-18
A	CN 102157208 B (中广核工程有限公司等) 2013年 3月 27日 (2013 - 03 - 27) 全文	1-18
A	CN 101783192 B (中广核工程有限公司等) 2012年 7月 18日 (2012 - 07 - 18) 全文	1-18
A	CN 101968974 B (中广核工程有限公司等) 2013年 1月 2日 (2013 - 01 - 02) 全文	1-18
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。		
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件(如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件		
国际检索实际完成的日期 2016年 8月 16日		国际检索报告邮寄日期 2016年 8月 23日
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451		授权官员 王树玲 电话号码 (86-10)62085649

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2015/097513

检索报告引用的专利文件			公布日 (年/月/日)	同族专利	公布日 (年/月/日)
WO	2015/112304	A2	2015年 7月 30日	无	
CN	102426863	A	2012年 4月 25日	CN	102426863 B 2015年 12月 16日
CN	102157208	B	2013年 3月 27日	CN	102157208 A 2011年 8月 17日
CN	101783192	B	2012年 7月 18日	CN	101783192 A 2010年 7月 21日
CN	101968974	B	2013年 1月 2日	CN	101968974 A 2011年 2月 9日