

文章编号：0258-0926(2015)06-0088-04；doi: 10.13832/j.jnpe.2015.06.0088

# HFETR 过程安全参数测量装置设计与应用

葛 源，武文超，李 普，陆 星，杨先军

中国核动力研究设计院，成都，610041

**摘要：**高通量工程试验堆（HFETR）过程安全参数测量装置采用三通道冗余结构设计，实现安全参数的监测和报警。装置具有进行参数定值试验简洁高效、便于维护的特点，投入 HFETR 运行后，性能良好可靠。其成功应用为我国研究堆安全级仪控系统数字化技术应用提供了实例。

**关键词：**HFETR；过程安全参数测量装置；核安全级；数字化仪控

**中图分类号：**TL38 **文献标志码：**A

## Design and Application of Measurement Device for HFETR Safety Process Parameters

Ge Yuan, Wu Wenchao, Li Pu, Lu Xing, Yang Xianjun

Nuclear Power Institute of China, Chengdu, 610041, China

**Abstract:** By using the redundant three-channel structure, the measurement device for HFETR safety process parameters was designed to implement the safety parameter monitoring and alarm. The device has advantage of parameter setting test method that is simple, efficient and convenient maintenance. It has performed well and reliably with its application in HFETR, which provides an example for the application of the safety class digital instrument and control system in the research reactor in China.

**Key words:** HFETR, Measurement device for safety process parameters, Nuclear safety class, Digital instrument and control

## 0 引言

高通量工程试验堆（HFETR）过程安全参数测量装置（简称装置）是反应堆仪控系统的重要组成部分。一方面，该装置作为保护系统的安全监测环节，实现 HFETR 安全参数的监测，监测结果用于安全逻辑装置触发停堆保护；另一方面，装置将处理完成的信号输出用于显示和报警，用于 HFETR 过程自动调节系统的调节控制。

## 1 设计要求

符合有关核安全法规标准和保护系统设计准则要求；具有安全监测与报警、向外部设备输出显示和控制信号；采用成熟的数字化技术，提高

可靠性和可用性；满足运行使用要求，便于操作和维护；满足现场的外部接口要求。

## 2 总体设计

### 2.1 组成和功能

如图 1 所示，装置在总体结构上由 3 个独立且功能相似的测量通道组成，各测量通道均由信号调理单元、输入输出（I/O）单元、通讯单元、主控单元、电源单元等部件组成。I/O 单元、通讯单元、主控单元实现数据的采集、输出、运算和管理。信号调理单元的作用是接收传感器信号、与 I/O 单元交换数据、对模拟量信号进行分配和通道隔离以及对外部系统设备的隔离，还具有为

收稿日期：2015-01-15；修回日期：2015-09-24

作者简介：葛 源（1983—），男，工程师，现主要从事反应堆仪表与控制系统维护、科研和设计工作

变送器配电的功能。各单元具有在线故障自诊断功能，且电源单元、主控单元、通讯单元均冗余配置。每个测量通道设置一个功能独立的机柜，实现了 3 个通道完全的物理隔离，满足独立性与隔离要求。此外，还设置一台维护计算机作为工程师站，用于调试、试验与维护操作。

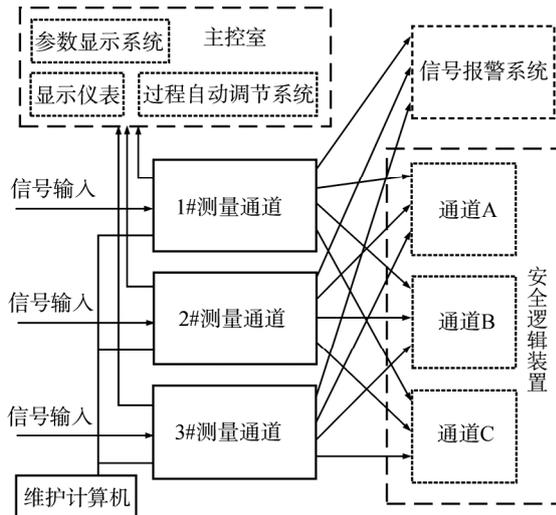


图 1 HFETR 过程安全参数测量装置结构图  
Fig. 1 Structure of Measurement Device for HFETR Safety Process Parameters

## 2.2 结构原理

装置的安全监测与报警功能按以下原理实现：每个测量通道分别将各自的参数报警信号送往信号报警系统和保护系统，3 个测量通道与安全逻辑装置形成了 3 通道冗余的结构。来自现场的 3 个独立过程安全参数测点信号，作为该保护参数的 3 个冗余测点，分别进入装置的 3 个测量通道（1#、2#、3#）进行运算，当某个测点参数实际数值超出警告或自降报警阈值时，测点所属的测量通道将相应报警信号送往信号报警系统，提醒运行人员；当冗余的 2 个或 3 个测点参数实际数值超出停堆保护报警阈值时，所属测量通道将相应报警信号同时送往安全逻辑装置的 A、B、C 三个逻辑通道；在满足 3 取 2 的情况下，安全逻辑装置触发停堆保护动作。

各测点信号进入信号调理单元后，由隔离放大器分出相应的标准模拟量信号，分别供给给主控室的显示仪表、参数显示系统和过程自动调节系统。为保证安全监测功能的完全性、完整性、独立性，将 I/O 单元和信号调理单元的信号通道设置为输入输出安全隔离和路路隔离<sup>[1]</sup>。这使得装

置向主控室仪表设备输出显示信号不会影响安全监测通道，简化系统硬件结构。

## 2.3 定值整定试验功能的实现

安全参数定值整定试验的目的是通过试验，检查过程安全参数的测量准确度、报警阈值，以及输出至安全逻辑装置的停堆保护报警信号的逻辑符合是否满足要求，以确保反应堆安全稳定运行。这是 HFETR 开堆前的一项重要工作，该功能由装置实现，操作方式如图 2 所示。

具体如下：通过分断试验端子，将仪表的真实信号与系统断开，测试人员通过精密信号发生器给出试验模拟信号，经端子上端内部接线上传给过程测量系统，根据信号发生器的显示记录定值试验值，也可以通过维护工具对系统的输出信号进行回读以记录试验定值。

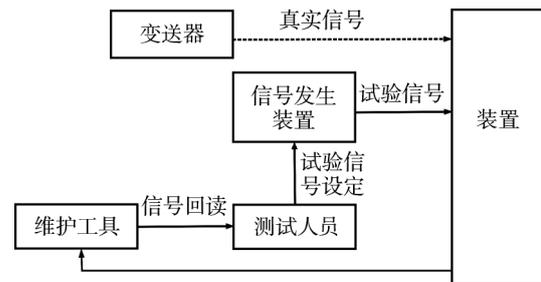


图 2 参数定值整定试验的方式  
Fig. 2 Way for Neoteric Parameters Alarming Experiment

采用这样的定值试验方式具有以下优点：避免频繁拆线、接线对设备的影响，操作简单，减少人因失误的风险；参数整定值可修改和调整，适合 HFETR 不同工况下的警告、保护定值误差超出运行要求时的校准；设置可调的报警回差，报警可在一定范围内保持，同时防止继电器输出状态不明确等问题。

## 2.4 供电设计

在外部供电电源设置方面，每个测量通道各使用一路独立的、经不间断电源（UPS）的可靠外电源供电，以满足独立性和电气隔离要求，减少共因故障。

单个测量通道供电分配见图 3。机柜内部低压电源单元的设计采用 4 电源冗余配置方案，每个 24 V 直流电源模块组成一个局部冗余组，从而形成 2 个互为冗余的冗余组，共同为设备供电。此外，部分模块（如主控单元和通讯单元）由互为冗余的 2 个 5 V 直流电源模块供电，这 2 个电

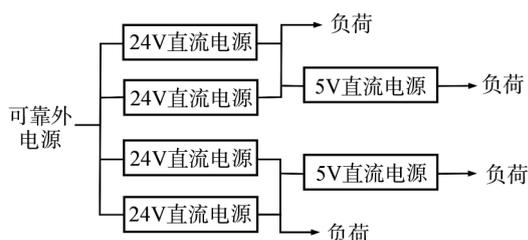


图3 单个测量通道供电分配框图

Fig. 3 Block Diagram for Power Allocation of a Single Measurement Channel

源模块的供电分别取自2个24V直流电源模块冗余组。每一路电源均处于降额使用状态, 负荷裕量在50%以上<sup>[2]</sup>, 当一路电源故障时, 另一路电源也可以在满负载情况下正常工作。

### 3 参数测量与处理的实现方法

装置采用国产核安全级分散控制系统(DCS)平台——FirmSys进行开发集成。装置根据参数测量要求, 利用该平台进行硬件、软件组态, 使设计满足要求。

#### 3.1 硬件实现

装置的主要部件调理单元、I/O单元、主控单元均采用模块化、机箱式设计, 使结构紧凑、便于维护<sup>[3]</sup>。FirmSys平台的每块模块均具有状态指示灯, 如出现故障, 可用于电源、通讯和超量程的初步诊断, 智能模块具备自诊断功能, 并显示故障代码便于检修维护。在此基础上, 装置中为主控的单元、I/O单元、电源单元、通讯单元等智能模块设计了一套综合故障报警指示系统, 预定的某一处发生故障, 将在柜体顶端点亮红色的综合故障指示灯, 以提醒运行人员。为了提高线路的抗干扰能力, 包括电缆在内的信号传输通道均设置了隔离和屏蔽措施, 设置了信号地、屏蔽地和保护地3种接地方式以保证可靠接地<sup>[4]</sup>。

根据接口信号类型和传输的不同特点, 参数的测量和处理方式如下:

##### (1) 单路直接测量、直接运算参数处理

该类参数由变送器直接测量得到, 包括: 压力、液位、温度、流量。测点信号依次经调理单元、I/O单元送至主控单元处理, 再由I/O单元输出报警信号至外部的安全逻辑装置和信号报警系统。去往主控室的数字显示器、参数显示系统和过程自动调节系统的信号, 由位于通道前端的调理单元分出后直接输出; 需要经过主控单元运算

后再送主控室显示的信号, 由I/O单元输出至信号调理单元进行隔离、转换后再输出, 如流量参数需要经过主控单元进行开方运算。采用此方案能减少系统硬件规模, 有利于提高输出信号的传输速度和可靠性, 同时保证在智能卡件不能正常工作时, 主控室仪表仍能继续正常监视堆的状态。

##### (2) 多路测量运算参数处理

对于温差、压差、热功率等需要多路参数进行运算的参数, 其运算过程则是在主控单元内部, 分别取相应的温度和压力信号进行运算, 再由I/O单元、调理单元输出至外部。

#### 3.2 软件

3.2.1 应用软件设计 应用软件设计的内容主要包括嵌入式应用软件设计和应用软件组态<sup>[5]</sup>, 通常包括SAMA图设计、应用软件I/O点表设计、应用软件整定值设计、应用软件组态、应用软件下装、软件操作界面设计, 大致流程如下:

(1) SAMA图设计: 根据技术要求, 设计功能算法和逻辑图算法, 以及参数测量控制的具体原理和方法, 绘制全部参数的SAMA图, 并按照SAMA图进行应用软件组态。功能算法主要包括: 信号输入检测、阈值比较、报警阈值(整定值)设置、定值试验、参数运算、输出处理等算法。

以热功率参数为例介绍, 热功率计算公式为:  $P=Q \cdot t/0.86$ 。SAMA图中, 主要有以下流程:

将流量变送器的压差信号进行开方运算, 得到一次水流量信号; 堆出口温度与入口温度进行减法运算, 得到堆出入口温差信号; 计算一次水流量和堆出入口温差的乘积; 根据公式计算出热功率, 作为阈值比较的输入变量, 该变量与报警阈值比较, 输出不同级别的3种报警信号: 警告、自降、保护(停堆)。

不同报警级别的报警阈值可根据运行要求设定, 该值为报警基准值和超出基准值的百分数的乘积, 并通过回差设置使报警在一定范围内保持。报警阈值分为3种: 警告报警, 110%; 自降功率报警, 115%; 保护报警, 120%。软件设置了试验信号输入变量和旁路测试变量。旁路测试变量和实测信号的输入变量之间可进行切换选择, 利用旁路测试功能可对报警信号输出状态进行旁路或强制设定。

(2) 应用软件I/O点表设计: 根据技术要求, 对SAMA图中所有的I/O变量进行定义和整理, 按照I/O变量所在的卡件位置及变量类型生成相

应的组态 I/O 清单配置文件。

(3) 应用软件整定值设计：根据 SAMA 图，列出所有参数清单，并根据设定值清单（包括基准值、报警值、保护值），对各个参数进行赋值，把所有参数变量及变量类型生成相应的参数清单配置文件。

(4) 应用软件组态：在工程师站组态软件中对测量通道及主控单元、I/O 模块等硬件进行组态配置。硬件配置完成后，向组态软件中导入设计好的 I/O 清单和设定值清单的配置文件，再根据 SAMA 图，对各个站分别进行相应参数的算法组态，组态完成后，进行编译并生成软件代码包。

(5) 应用软件下装：利用维护工具软件包将生成的下载文件下载到 1#、2#和 3#测量通道的主控单元中，并将回读通道中的参数和算法进行校验，以确保下载的正确性。

3.2.2 维护软件 维护软件（也称为工程师组态软件）的主要功能是根据测量参数的数目、通道的需求和规模创建工程，建立整个工程的操作站，并对站内设备进行组态（变量组态和算法组态），站与站之间的网络拓扑等操作，组态编译后生成系统嵌入式软件工程文件并执行下装。同时，维护软件为调试和维护人员提供所有参数的数值和数值有效性的实时监测、设备状态在线查看、测量参数回读、输入输出量的强制输出等功能。在授权的前提下，利用维护计算机可进行维护软件的操作，工程文件根据要求设置相应的权限，可以防止误操作影响正确的运行方式。

## 4 质量鉴定结果和应用情况

### 4.1 可靠性分析结果

根据装置结构和工作过程建立装置功能丧失的故障树，符合并-串联结构可靠性模型<sup>[6]</sup>。

通过分析装置的可用率和输出拒动的概率对装置可靠性的影响，验证设计的合理性。可靠性分析结果如下：装置的可用性非常好，达到 99.99984%；输出拒动的概率最低为  $7.914 \times 10^{-9}$ 。

### 4.2 硬件质量鉴定结果

按照相关法规和标准的要求，从抗震动、电磁兼容、稳定性等方面进行装置的整机鉴定。鉴定试验的结果符合要求：整柜样机抗震试验后，外观正常、结构完整、无变形、无裂痕，工作性

能和功能保持完好，为现场安装提供了指导意见；

电磁兼容试验项目和结果满足 IEC61000 有关要求；装置进行了带电运行 72 h 的稳定性考验，设备功能和性能保持完好。

### 4.3 软件验证和确认（V&V）结果

在应用软件开发的全过程，按美国电气和电子工程师协会（IEEE）的有关标准要求实施了下述 V&V 活动：概念 V&V、需求 V&V、设计 V&V、实现 V&V、测试 V&V、安装和检验 V&V。V&V 活动保证了项目开发每一阶段的输出文件满足输入基准文件的要求，同时保证了安全级应用软件的安全性和可靠性<sup>[7]</sup>。

## 5 结束语

(1) 装置具有良好的性能：可用率达到 99.99% 以上；响应时间小于 41 ms；模拟量信号输出精度达 0.02%；参数整定值误差小于 0.25%。

(2) 装置使用和维护简单，为 HFETR 过程安全参数的定值试验提出了可靠、高效的方法，属国内首次。

(3) 各设备自诊断功能和综合故障报警功能的设计，为维护人员提供检修依据和参考。

(4) 装置长期运行稳定，为 HFETR 的安全运行提供了重要保障，其成功应用为我国研究堆安全级仪控系统数字化技术应用提供了实例。

参考文献：

- [1] 毛从吉, 毋琦. 从安全评审角度看核电站数字化仪控设计[J]. 自动化仪表, 2012, 33(7): 39-42.
- [2] 孙洪涛. 核电站安全级数字化保护系统供电设计研究[J]. 工业控制计算机, 2011, 24(10): 20-22.
- [3] 卢坤祥. 整机系统可靠性设计理论与实用技术[M]. 天津: 科学技术出版社, 1987: 328-329.
- [4] 张健. 核电站中基于 DCS 的抗电磁干扰设计[J]. 中国核电, 2013, 6(3): 209-216.
- [5] 郑伟智. 核电站安全级 DCS 应用软件设计过程浅析[J]. 自动化仪表, 2014, 35(2): 53-57.
- [6] 宋保维. 系统可靠性设计与分析[M]. 西安: 西北工业大学出版社, 2008: 45-48.
- [7] 刘真, 江国进, 孙永滨. 核电安全级仪控系统软件 V&V 活动及其方法研究[J]. 核科学与工程, 2011, 31(2): 45-50.

（责任编辑：张祚豪）