基于国产芯片的核级仪控系统主控板卡的设计与实现

马朝阳，王　勇，程　康
（上海中广核工程科技有限公司，上海 200241）

摘　要： 核电仪控系统关系国家的核电安全，采用国产芯片实现仪控系统至关重要，只有基于国产技术平台才能从内在保障核级仪控系统的安全。基于国产芯片实现仪控系统过程中，面临系统设计、器件选型，以及新的系统架构下如何满足产品的稳定性、可靠性、独立性和确定性等问题，给出了基于国产芯片、计算机技术平台的核级仪控系统主控板卡的设计与实现，并重点对独立性和确定性设计进行了说明。对主控板卡的性能指标进行了测量，结果表明使用国产芯片实现的控制系统满足关键指标要求，主控板卡的设计与实现对核电仪控系统国产化具有参考意义。

关键词： 核电；仪控系统；主控板卡；国产芯片
中图分类号： TP23　　**文献标识码：** A　　**DOI：** 10.19358/j.issn.2096-5133.2022.05.013
引用格式： 马朝阳，王勇，程康. 基于国产芯片的核级仪控系统主控板卡的设计与实现[J].信息技术与网络安全，2022，41(5)：82-86，91.

Design and implementation of main control unit for nuclear-level instrument control system based on domestic chips

Ma Zhaoyang，Wang Yong，Cheng Kang
(Shanghai CGN Engineering Technology Co.，Ltd.，Shanghai 200241，China)

Abstract： The nuclear power instrument and control(I&C) system is related to the country′s nuclear power safety. It is very important to use domestic chips to realize the I&C system. Only based on the domestic technology platform can guarantee the safety of the nuclear-level I&C system internally. In the process of implementing the instrument and control system based on domestic chips，we are faced with the problems of system design，device selection，and how to meet the stability，reliability，independence and certainty of products under the new system architecture. This paper presents the design and implementation of the control principle of the nuclear-level instrument and control system based on domestic chips and computer technology platform，and focuses on the independent and deterministic design. In this paper，the performance indicators of the main control unit are measured. The results show that the control system realized by using domestic chips meets the requirements of key indicators. The design and implementation of the main control unit has reference significance for the localization of nuclear power I&C systems.

Key words： nuclear power；instrument and control system；main control unit；domestic chips

0 引言

核级仪控系统是核电行业的核心关键部件之一，被称为核电站的“神经中枢”，对于保证核电站安全、可靠、稳定运行发挥着重要作用[1]。中国已经研制了自主知识产权的国产核级仪控系统，但是国产核级仪控系统核心芯片仍然使用了国外的芯片，而在当前国际背景下进口电子元器件存在的管控限制、安全隐患等问题愈发突出[2]。

近年来，国产芯片越来越多地应用到仪控系统中，通过不断验证、反馈、改进，芯片的性能也逐步提高。另一方面，国际环境中具有优势产业的国家利用其产业链的上游有利位置，不断对我国高科技企业进行技术打压，如限制本国企业向部分中国高科技企业出口芯片等。为了提高国产核级仪控系统的安全，掌握核心技术，以及解决核心技术被卡脖子问题，基于国产芯片技术实现核级仪控系统迫在眉睫。

由于主控板卡是核级仪控系统的核心部件，因此实现主控板卡的核心器件国产化替代是核级仪控系统国产化的重要研究方向。本文研究了基于国产芯片的核级仪控系统控制原理设计和实现。

1 基于国产芯片实现核级仪控系统主控板卡的技术分析

和睦系统(FirmSys)是我国首个自主知识产权的核安全级仪控系统平台产品，目前已经在阳江5、6号机组，红沿河5、6号机组，田湾5、6号机组，防城港3、4号机组等核电机组得到了应用[3]。主控板卡是核电仪控系统平台的核心板卡，目前该板卡的主要核心器件采用国外芯片，未来这些器件存在无法获取的风险，本文以和睦系统主控板卡为例分析基于国产芯片、技术平台实现的主控板卡设计方案。

和睦系统主控板卡主要元器件列表及功能如表1所示。

表1 主要元器件列表

序号	元器件名称	主要实现功能
1	CPU	板卡运算和控制功能的核心芯片
2	PHY	通信功能
3	可编程逻辑器件	逻辑译码和冗余逻辑、冗余同步的处理
4	SPI Flash	配置文件的存储
5	DDR内存	数据和代码的存储
6	电源	板卡供电

采用国产元器件进行核级系统设计，在原有系统基础上存在直接替代、基本替代、功能替代和降级替代几种方式[2]。研究表明，我国在通用元器件方面取得了一些成就，如阻容、电源等基础元器件已经实现大量国产化[4]，基本可以实现直接替代或基本替代，本文不将通用元器件作为方案研究的重点，而将研究的重点放在CPU、PHY、可编程逻辑器件等关键器件上，这些器件只能实现功能替代和降级替代，需要根据系统的功能重新开展设计工作。

基于国产CPU设计主控板卡，由于芯片架构发生变化，需要重新考虑核级设备的设计要求。核级主控板卡的设计要求来源于标准IEEE 7.4.3.2[5]、GB/T 13629[6]、GB/T 13286[7]、IEC 61508[8]、IEEE 603[9]和IEC 61513[10]等，主要包括独立性、确定性等[11-12]。在核安全级DCS产品设计中，应考虑不同的设备之间、内部的不同功能之间避免相互影响，按照独立性准则设计，采用电气隔离、通信隔离来满足独立性要求。主控板卡设计应保证产品的功能确定，这个确定包括行为确定、执行时间确定以及资源利用确定。独立性设计和确定性设计是核级主控板卡设计的重要方面，下面分别在硬件设计和嵌入式软件设计中进行重点说明。

2 主控板卡国产化设计及实现

2.1 总体方案

和睦系统示意图如图1所示，系统包括主控板卡、I/O通信单元、多点通信单元和点对点通信单元，由两套相同的控制器、公共采集单元和输出单元形成冗余系统。

仪控系统主控板卡是系统的核心单元，也是主控制站的核心。主控板卡功能划分为组态处理、算法处理、冗余管理、总线通信、维护功能、人机接口、自诊断部分，各部分实现的功能如下：

组态处理：接收、检查并配置应用组态信息。

算法处理：执行应用软件，运行逻辑算法。

运行调试：提供实时运行条件下维护，包括运行参数、运行变量、应用软件的调试和修改。

数据交互：实时运行情况下通过与通信单元之

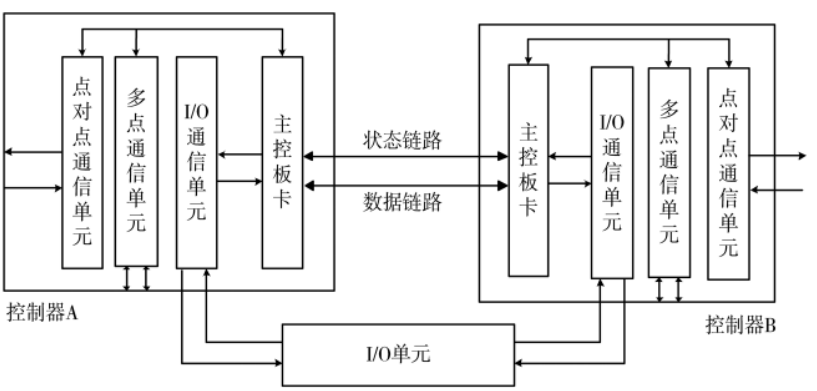

图1 和睦系统示意图

间的数据交互，接收和发送来自输入、输出、网络方面的数据，以及与工程师软件工具通信，实现调试、监视、试验方面的数据交互。

冗余功能：冗余配置下的冗余管理。

自诊断：为提供可靠性而对重要器件/功能的自诊断。

故障处理：根据设备运行的异常情况，采用措施保证故障安全并报告故障信息。

人机交互：提供人机接口，方便用户使用和维护本设备组态处理。

2.2 硬件设计

主控板卡硬件设计原理框图如图2所示。龙芯CPU和紫光FPGA之间采用PCIe总线接口，并通过FPGA扩展出Local Bus并行总线，主处理板卡经过Local Bus总线实现与机箱内通信板卡的数据交互；人机交互接口指示灯和点阵显示器、槽号、站号及在位状态信息连接到FPGA，CPU通过PCIe总线获取相关信息；冗余同步数据链路采用802.3以太网，网络芯片连接到FPGA，由FPGA实现对芯片的配置和控制；传输数据由龙芯CPU通过PCIe总线接收和发送；工程配置数据由集成在龙芯CPU的GMAC和外界以太网PHY完成数据交互。

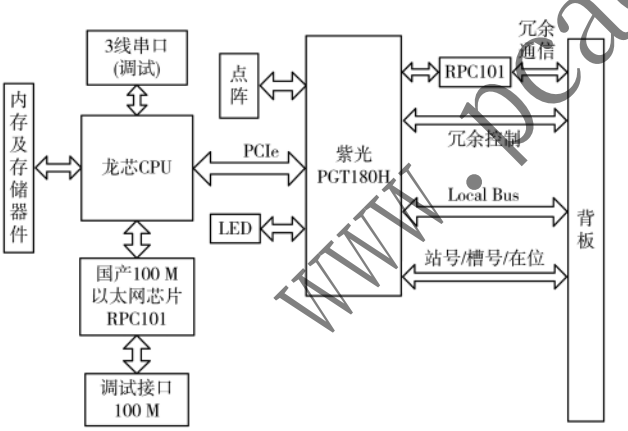

图2 硬件设计原理框图

电气独立性设计：两套相同的控制单元形成的冗余系统分为主机和从机，冗余系统独立供电，主从机之间的状态信号采用光电隔离，数据通信采用电气隔离，保证主从机系统隔离。电气隔离图如图3所示。

通信独立性设计：数据链路设计依据IEEE7-4.3.2《核电厂安全系统中数字计算机的适用准则》[5-6]要求进行通信独立性设计，主控板卡和通信板卡通过

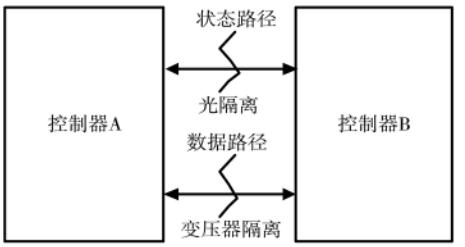

图3 电气隔离图

PCIe总线连接到FPGA并由FPGA适配双口RAM进行通信隔离，如图4所示，确保通信部分与控制处理部分之间的故障隔离，实现功能和故障检测的独立性。

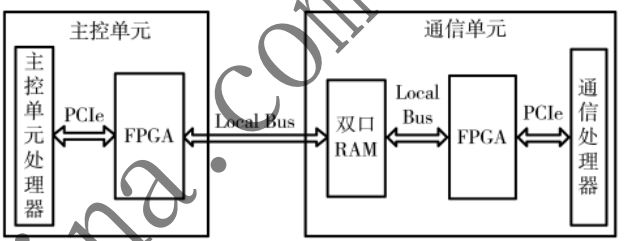

图4 通信隔离图

2.3 硬件选型

针对2.2节硬件设计，主控板卡采用以处理器为核心，可编程逻辑器件辅助控制的方式进行设计，主要器件选型如下：

(1)CPU选型

CPU采用龙芯中科公司的2K1000处理器。龙芯2K1000处理器是面向网络安全领域及移动智能终端领域的双核处理器芯片。龙芯2K1000处理器集成两个GS264处理器核，支持MIPS64指令集，集成1个64位DDR2/3-1333控制器，支持主要模块时钟动态控制；支持ACPI，设计主频800 MHz，典型功耗5 W，采用40 nm CMOS芯片制造工艺，芯片外围接口包括两路x4 PCIe2.0、64位DDR2/3及其他各种小接口等。

(2)FPGA选型

FPGA采用紫光PGT180H可编程逻辑器件，该器件为深圳市紫光同创电子有限公司推出的Titan系列高性能FPGA中的产品，它采用了完全自主产权的体系结构和主流的40 nm工艺。包含创新的可配置逻辑单元(CLM)、专用的18 Kb存储单元(DRM)、算术处理单元(APM)、高速串行接口模块(HSST)、多功能高性能I/O以及丰富的片上时钟资源等模块，

广泛适用于通信、视频、工业控制等多个应用领域。

(3)以太网芯片选型

以太网芯片采用中兴微电子 ZX5201，ZX5201 是新一代单口以太网 10BASE-T/100BASE-TX/1000-BASE-T 收发器，支持 RGMII 接口，支持 IEEE802.3，用户配置便捷。

2.4 可编程逻辑设计

FPGA 实现以下功能：(1)PCIe 到并行本地总线的数据转换，为 CPU 读取和配置通信板卡的数据通道；(2)看门狗的控制；(3)点阵以及 LED 的显示控制；(4)时钟电源的监测功能等；(5)冗余仲裁逻辑；(6)冗余同步数据通道的控制。可编程逻辑框图如图 5 所示。

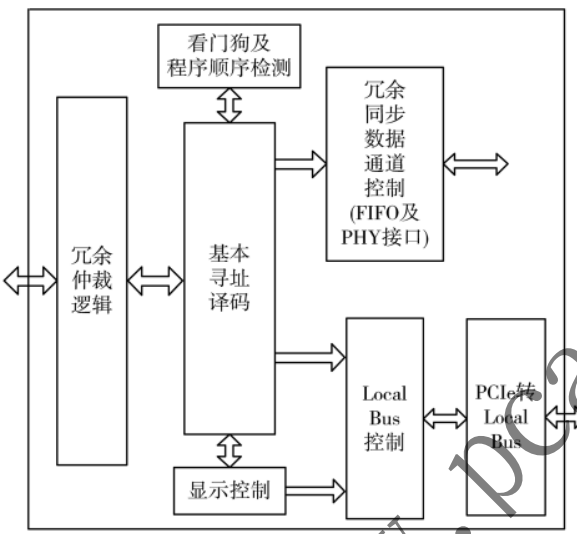

图 5 可编程逻辑功能框图

2.5 嵌入式软件设计与实现

在数字化安全级仪控系统中，嵌入式计算机系统是整个系统的“大脑”，而嵌入式软件则是“灵魂”。嵌入式软件架构为层次型架构，每层各司其职，每个模块完成特定功能，采用单入口单出口准则来降低接口的复杂性。当修改时，仅需要关注与其他模块的接口部分，以此降低错误蔓延的范围，并降低维护的复杂度。嵌入式软件层次架构如图 6 所示。

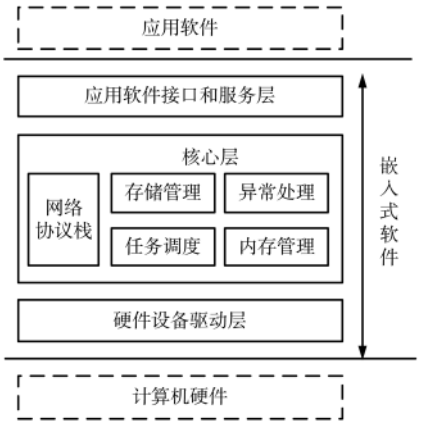

图 6 嵌入式软件层次架构图

为了满足系统不同运行状态的要求，主控板卡软件设计了三种工作模式：运行模式、测试模式、下装模式。主控板卡提供模式切换开关，方便操作人员手动操作。开关分为运行模式、测试模式、下装模式三个互斥的选项，不允许自行切换。运行模式与测试模式之间切换无需重启即可生效，但它们与下装模式之间的切换需重新上电才能生效。

为了保证系统能够正常启动，需要 Bootloader 软件引导硬件启动。系统功能软件包含 Bootloader 软件、下装模式软件和运行及测试模式软件。其中 Bootloader 软件完成基础硬件的初始化，并根据工作模式装载对应的平台软件；下装软件完成组态配置信息及工程应用软件的下装和存储；运行及测试模式软件完成硬件设备驱动层、核心层、应用软件接口和服务层功能，并调度工程应用软件。

依据核安全级软件的设计要求[13-15]，软件设计需满足确定性的要求，确定性是指软件在特定条件下行为是可预测的。为了提高软件的确定性，要保证运行时间可预测、内存使用可预测、控制流可预测，即时间确定性、空间确定性、行为确定性。

时间确定性是指能够在预定的时间内满足响应时间的要求，它是对系统实时性在更严格要求下的体现。

空间确定性是指存储空间的分配使用是可预测的。它能避免处理器异常访问内存空间，可以防止动态使用内存时产生的内存溢出、内存泄露、内存破坏，以及由此引发的一系列不可预知的错误。

行为确定性是指所有执行的任务能够按照期望的次序执行，保证结果可预测。

(1)时间确定性设计实现

采用定周期执行，数据采集、冗余同步、算法执行和数据输出顺序执行，同时配置独立时基看门狗电路和程序顺序监控设计，当运行周期超出规定值或程序执行顺序异常时，进入故障处理程序，从而确保软件时间的确定性。

(2)空间确定性设计实现

代码区和内存区使用不同的内存区域，内存区的输入和输出区采用分开的区域，这些内存区的分配在编译阶段即确定，保证空间的确定性；与工程应用相关的内存区域也在编译阶段确定并通过组态配置方式传递给平台软件，从而保证内存空间使用的确定性。嵌入式软件和工程相关的组态及软件存放在不同的 SPI Flash 芯片中，确保软件存储的确定性，避免误操作破坏嵌入式软件。

(3)行为确定性设计实现

禁止使用中断，采用无操作系统的单任务调度方式，避免中断或多任务任务切换带来的行为不确定性。通信采用无握手的异步通信方式，避免由于通信双方相互等待而造成的通信行为不确定性。

3 方案验证

3.1 性能测试

采用国产芯片的主控板卡部分关键性能参数与原主控板卡对比结果如表 2 所示。

表 2 性能测试结果

序号	测试项目	原主控板卡/μs	国产芯片主控板卡/μs
1	1 KB 内存 CRC 计算	156	62
2	1 KB 内存 4 字节拷贝	40	4
3	1 KB 双口 RAM 读	234	388
4	1 KB 双口 RAM 写	231	70

从测试结果可以看出，采用国产芯片的主控板卡性能远高于原主控板卡。其中测试项目 3 的性能低于原主控板卡，主要原因是硬件设计采用 PCIe 接口转双口 RAM 本地总线的方式造成额外的时间开销；测试项目 1、2、4 性能高于原主控板卡，主要是基于国产芯片的主控板卡 CPU 的性能较高。

3.2 响应时间测试

本文基于某核电站高温堆现场控制站进行方案验证。

选取源量程核功率高触发停堆逻辑进行紧急停堆响应时间测试。紧急停堆响应时间是仪控系统的一个重要系统指标，此指标关系着反应堆的系统安全，鉴于本文搭建的控制系统是以某核电站高温堆为原型，因此停堆响应时间要求也沿用此电站的系统指标，该核电站反应堆保护系统设备技术规格书中此指标为 300 ms。

测试环境示意图如图 7 所示。在源量程核功率输入通道注入跳变信号，满足触发停堆信号输出要求。使用示波器测试从源量程核功率高信号触发到停堆信号 DO 输出所用时间，测试 10 次，测试结果如表 3 所示。

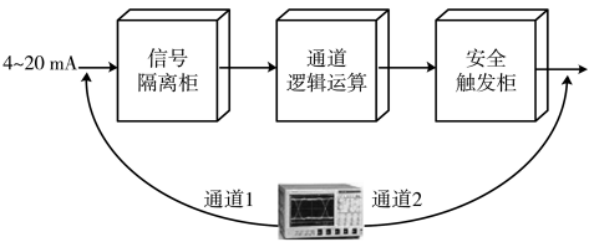

图 7 响应时间测试示意图

表 3 响应时间测试结果

目标值/ms	测试序号	测试值/ms
平均响应时间≤300	第 1 次	104
	第 2 次	128
	第 3 次	124
	第 4 次	116
	第 5 次	96
	第 6 次	112
	第 7 次	144
	第 8 次	136
	第 9 次	124
	第 10 次	152
	平均值	123.6

从测试结果可以看出响应时间<300 ms，满足系统要求。

4 结论

本文设计了一种基于国产芯片、计算机平台的核安全级控制系统方案，并完成了板卡的实现，系统的响应时间指标可以满足核安全级仪控系统的要求，可以替代原国外芯片的主控板卡，此方案对于基于国产芯片技术的核级仪控系统研制具有较高的参考价值。

参考文献

[1] 观察者网.核电站“神经中枢”实现中国造，不再受制于人[EB/OL].(2018-05-23).https://www.guancha.cn/industry-science/2018_05_23_457644.shtml.

[2] 王舜，刘明星，刘滨，等.核电厂 DCS 元器件国产化替代问题探讨[J].上海交通大学学报，2019,53(S1):24-28.

(下转第 91 页)

[5] 王建强,戴志敏,徐洪杰.核能综合利用研究现状与展望[J].中国科学院院刊,2019,34(4):460-468.
[6] 许莉,李锋,彭洪兵.中国海上风电发展与环境问题研究[J].中国人口·资源与环境,2015,25(5增):135-138.
[7] 王宇,朱沈超,陈芳斌,等.中国核电与可再生能源发电协调发展初探[J].可再生能源,2021,39(8):1069-1077.
[8] 张廷克,李闽榕,尹卫平.核能发展蓝皮书:中国核能发展报告2021[M].北京:社会科学文献出版社,2021.
[9] 郑钊颖,冯奕敏.广东海上风电产业发展路径与对策研究[J].南方能源建设,2020,7(4):18-25.
[10] 吴皓文,王军,龚迎莉,等.储能技术发展现状及应用前景分析[J].电力学报,2021,36(5):434-443.

(收稿日期:2022-03-01)

作者简介:

王秋洪(1963-),通信作者,男,在职研究生,高级经济师、高级工程师,主要研究方向:经济管理。E-mail:13808595918@139.com。

(上接第86页)

[3] 编辑部."和睦系统"——中国自主核级数字化仪控平台[J].中国核电,2017,10(3):305.
[4] 廖勇,袁圆.进口元器件自主可控的风险分析及对策建议[J].电子元件与材料,2020,39(6):14-18.
[5] IEEE standard criteria for digital computers in safety systems of nuclear power generating stations:IEEE 7-4.3.2-2010[S].2010.
[6] 核电厂安全系统中数字计算机的适用准则:GB/T 13629-2008[S].北京:人民出版社,2008.
[7] 核电厂安全级电气设备和电路独立性准则:GB/T 13286-2008[S].北京:中国标准出版社,2008.
[8] Functional safety of electrical electronic programmable electronic safety-related systems:IEC 61508-2010[S].2010.
[9] Criteria for safety systems for nuclear power generating stations:IEEE 603-2009[S].2009.
[10] Nuclear power plants-instrumentation and control important to safety-general requirements for systems:IEC 61513-2001[S].2001.
[11] 李明利,李刚,张杰.核安全级DCS通信网络残差率设计研究[J].自动化博览,2020,37(9):56-59.
[12] 郑伟智,李相建,朱毅明,等.核电站安全级数字化仪控系统设计标准分析研究[C]//第一届中国(国际)核电仪控技术大会论文集,2011:876-882.
[13] Nuclear power plants-instrumentation and control systems important to safety-software aspects for computer-based systems performing category a functions:IEC 60880-2006[S].2006.
[14] 核电厂安全重要仪表和控制系统执行A类功能的计算机软件:NB/T 20054-2011[S].2011.
[15] 核动力厂基于计算机的安全重要系统的软件:HAD 102/16-2004[S].2004.

(收稿日期:2022-01-11)

作者简介:

马朝阳(1978-),通信作者,男,硕士,高级工程师,主要研究方向:核电站安全级仪控平台。E-mail:mayangpony@126.com。

王勇(1975-),男,硕士,工程师,主要研究方向:核电站安全级仪控平台。

程康(1983-),男,硕士,高级工程师,主要研究方向:核电站安全级仪控平台。

版权声明

经作者授权，本论文版权和信息网络传播权归属于《信息技术与网络安全》杂志，凡未经本刊书面同意任何机构、组织和个人不得擅自复印、汇编、翻译和进行信息网络传播。未经本刊书面同意，禁止一切互联网论文资源平台非法上传、收录本论文。

截至目前，本论文已经授权被中国期刊全文数据库（CNKI）、万方数据知识服务平台、中文科技期刊数据库（维普网）、JST 日本科技技术振兴机构数据库等数据库全文收录。

对于违反上述禁止行为并违法使用本论文的机构、组织和个人，本刊将采取一切必要法律行动来维护正当权益。

特此声明！

《信息技术与网络安全》编辑部

中国电子信息产业集团有限公司第六研究所