

DOI: 10.19666/j.rlfd.202605109

Hypervisor 架构下火电虚拟 DCS 控制器 异机冗余同步机制

宋美艳, 张勇, 刘畅, 翟亮晶, 项涛
(西安热工研究院有限公司, 陕西 西安 710054)

[摘要] 【目的】为解决火电厂虚拟 DCS 控制器在 Hypervisor 架构下跨物理服务器的异机冗余容错问题, 提出一种基于 SR-IOV 虚拟链路的 VM 级异机冗余同步机制。【方法】设计 VM 级异机配对冗余架构, VM 通过 SR-IOV 虚拟出至少 2 路 VF 冗余通信接口; 提出心跳+数据同步双任务冗余管理协议——心跳任务以 15 ms 周期通过 A/B 双路 VF 互发轻量化报文实现毫秒级故障检测, 数据同步任务由主机主动发起、备机被动接收, IO 数据经专用线程全量同步, FBD 中间变量跟随逻辑运算任务周期 (50~1 000 ms) 进行宏观全量、微观分级的同步策略, 减少主备 VM 运算偏差。【结果】在飞腾 S5000C 和嵌入式 Hypervisor 平台上搭建原型系统, 以 600 MW 超超临界火电机组实际控制逻辑为负载进行实验验证。在 4 种故障注入场景下主备切换时间均约 60 ms; IO 同步延迟约 85 μ s (2 KB), FBD 中间变量同步延迟 76~185 μ s, 均远小于控制周期; 切换过程控制输出连续平滑, SCADA 趋势无可见跳变。【结论】所提机制可为虚拟 DCS 控制器提供可靠冗余容错能力, 对推动国产化自主可控虚拟 DCS 技术的工程应用具有参考价值。

[关键词] 虚拟 DCS; 异机冗余; SR-IOV; Hypervisor; 无扰切换; 火力发电; 自主可控

[引用本文格式] (本段作者勿动) 作者姓名. 中文标题[J]. 热力发电, 年, 卷(期): 起始页码-终止页码. 作者姓名. 英文标题[J]. Thermal Power Generation, 年, 卷(期): 起始页码-终止页码.

Cross-machine redundancy synchronization mechanism of thermal power virtual DCS controllers under Hypervisor architecture

Song Meiyang, Zhang Yong, Liu Chang, Zhai Liangjing, Xiang Tao
(Xi'an Thermal Power Research Institute Co., Ltd., Xi'an 710054, China)

Abstract: [Objective] To address the cross-machine redundant fault-tolerance problem of virtual DCS controllers in thermal power plants under Hypervisor architecture, a VM-level cross-machine redundancy synchronization mechanism based on SR-IOV virtual links is proposed. In virtualized environments, controllers running as virtual machines on general-purpose servers must synchronize their control states across physical machines and Hypervisor layers, facing the challenges of virtualized I/O performance degradation, real-time master-slave role negotiation and fault detection, and bumpless control output transfer during switchover. [Methods] A VM-level paired cross-machine redundancy architecture is designed, in which each VM is equipped with at least two VF redundant communication interfaces through SR-IOV passthrough technology. The VFs are bound to different physical ports of the 10 GbE network controller to achieve full-path physical redundancy from the VF level through the physical port level to the entire server level. A dual-task redundancy management protocol combining heartbeat and data synchronization is proposed. The heartbeat task runs as an independent thread and exchanges lightweight 64-byte messages via dual A/B VFs at a 15 ms period to achieve millisecond-level fault detection and master-slave role

收稿日期: 2026-05-29 修回日期: 2026-07-04 接受日期: 2026-07-09 网络首发日期: XXXX-XX-XX

基金项目: 国家科技重大专项(2025ZD1701001); 西安热工研究院有限公司研发基金项目(TV-26-TYK13)

Supported by: National Science and Technology Major Project(2025ZD1701001); Research and Development Fund of Xi'an Thermal Power Research Institute Co., Ltd (TV-26-TYK13)

第一作者简介: 宋美艳 (1979), 女, 高级工程师, 主要研究方向为发电控制系统开发、控制策略研究与应用, songmeiyan@tpri.com.cn.

通信作者简介: 张勇 (1988), 男, 硕士, 工程师, 主要研究方向为工业控制系统软件研发, zhangyong@tpri.com.cn.

management. The consecutive loss threshold of N equals 4 is selected to tolerate one to two transient packet losses commonly observed on industrial Ethernet while maintaining fast detection speed. The data synchronization task is initiated by the primary VM and passively received by the standby VM through a dedicated server thread. IO data are fully synchronized through a dedicated thread, while FBD intermediate variables follow their respective logic execution task cycles ranging from 50 ms to 1 000 ms using a macro-level comprehensive yet micro-level tiered synchronization strategy—all intermediate variables are covered in their respective task cycles at the macro level, while the transmission is distributed across different time slots at the micro level to avoid instantaneous network congestion, thereby reducing master-standby computation deviation. [Results] A prototype system was built on the Phytium S5000C ARM processor and an embedded Type-1 Hypervisor platform, and experimentally verified using the actual control logic of a 600 MW ultra-supercritical thermal power unit as the workload. Under four fault injection scenarios—primary VM forced power-off (simulating server power supply failure), simultaneous disconnection of both A/B redundant link ports (simulating optical fiber interruption), vDCS runtime process abnormal exit, and Host single network disconnection—the master-standby switchover time is approximately 60 ms. The IO data end-to-end synchronization latency is approximately 85 μ s for 2 KB of data transmitted in a 15 ms cycle. The FBD intermediate variable synchronization latency ranges from 76 μ s to 185 μ s, corresponding to data volumes from 0.2 KB to 18.6 KB, all substantially below their respective control task cycles of 5 ms to 1 000 ms. During the switchover process, the control output remains continuous and smooth, with no visible glitches on SCADA trend curves. A sinusoidal test signal generated by an FBD function block was monitored through the SCADA trend display, and no amplitude or phase discontinuity was observed at the switchover moment, providing intuitive visual verification of bumpless transfer. The FBD master-standby computation deviation is controlled within a single task cycle. [Conclusions] The proposed mechanism can provide reliable fault-tolerant capability for virtual DCS controllers, offering engineering reference value for promoting the reliability and engineering application of domestically-produced autonomous controllable virtual DCS technology.

Key words: virtual DCS; cross-machine redundancy; SR-IOV; Hypervisor; bumpless transfer; thermal power generation; autonomous and controllable

新型电力系统建设对火电机组控制灵活性、运行可靠性和智能化水平提出了更高要求。传统分散控制系统(DCS)采用软硬件绑定架构,存在扩展性差、升级成本高、难以与新技术深度融合等问题。柴天佑等^[1]提出了软件定义智能控制系统的未来发展方向,王亦卿等^[2]对虚拟控制器做了全面综述,国际上相关研究^[3]系统梳理了虚拟化在工业控制系统中的技术架构与应用前景。虚拟控制器借助软硬件解耦和资源虚拟化手段,推动工业控制系统向开放化、弹性化演进。赵琰^[4]研究了软件定义工业控制器的架构与任务调度方法,Kampa等^[5]研究了云基础设施上虚拟PLC的硬实时高可用性方案,借助RDMA完成了状态同步。2024年,中煤新集板集电厂基于VMware ESXi和RTLinux成功投运国际首台套虚拟DCS控制系统,验证了虚拟化控制技术在发电领域的工程可行性^[6]。

然而,冗余是虚拟DCS从“能用”走向“可靠”的关键瓶颈。传统物理DCS通过主备硬件模块实现冗余,虚拟控制器需以虚拟机(VM)形态运行于服务器且支持异机冗余部署。

本文所述“异机冗余”特指:运行于不同物理服务器上的2个虚拟机(VM_{Ai}/VM_{Bi})构成主备冗余对,通过以太网链路实现控制状态的跨物理

机实时同步与故障切换。该模式区别于同一物理机内VM间冗余(共享宿主机故障域)和共享VM模型(单一VM跨双物理机运行),核心特征在于主备VM各自独立运行、故障域严格隔离。该方案面临三重挑战:IO虚拟化引入的性能损失;冗余协议在故障检测速度与网络开销间的平衡;主备切换时控制输出连续性的保障(无扰切换)。

在冗余容错方面,唐孝舟等^[7]研究了水电厂双重虚拟化监控的独立冗余架构,切换时间 ≤ 3 s,但节点故障后需手动恢复。在IO虚拟化方面,董凯凯等^[8]验证了SR-IOV技术可提供接近物理网卡的通信性能。吕跃鹏等^[9]在航天领域研究了虚拟化平台软件冗余技术。王雅哲等^[10]指出嵌入式虚拟化隔离是构建工业控制器内生安全架构的关键路径。IECON 2025上提出的工业边缘虚拟化双模冗余调度机制^[11]为多冗余架构的性能比较带来了参考。

上述研究存在以下不足:一是现有VM冗余方案多是共享VM模型或应用层冗余,缺乏Hypervisor层VM级异机配对冗余设计;二是SR-IOV还没有被引入到工业控制冗余通信场景中,冗余主备切换的时间多在秒级,不能满足工业现场切换时间要求;三是现有方案多针对通用工业控制场景,未考虑火电控制的多周期任务调度、FBD中间

状态强依赖、大惯性过程无扰切换等需求,缺少面向火电机组的系统性冗余方案。

针对上述问题,本文提出了一种基于 Hypervisor 的虚拟 DCS 控制器异机冗余同步机制,核心亮点工作体现在以下 3 个方面:一是提出了基于 SR-IOV 虚拟链路的 VM 级异机配对冗余架构,每个 VM 通过 VF 直通获得接近物理网卡的通信性能;二是设计了心跳+数据同步双任务冗余管理协议,以独立线程分离角色管理与状态同步;三是构建了基于本地链路自检的状态监测机制,确保系统在网络故障下收敛到唯一主机状态。

1 系统架构设计

1.1 总体架构

系统采用 4 层架构(图 1),4 层协同实现从物理链路到应用状态的全栈冗余管理。

1) 物理硬件层:由 2 台飞腾 S5000C 服务器(64 核,64 GB 内存)和 Intel 82599ES 双端口万兆网卡组成,分别连接 2 台工业以太网交换机,消除交换机单点故障。

2) Hypervisor 层:采用 Type-1 Hypervisor,静态分配 CPU 核心、内存和 IO 资源,以中断直通和 CPU Pinning 保障 VM 的实时性。

3) VM 层:每台服务器部署 N 个 VM,各运行与物理控制器同源的 RTOS。(

4) 冗余管理层:部署在每个 VM 的用户空间中,是跨 VM 冗余同步的核心执行载体。该层包含 2 个并行工作线程:心跳线程负责主备角色识别、运行状态同步和故障检测,通过 A/B 双路 SR-IOV VF(Virtual Function)以高频周期(默认 15 ms)与配对 VM 互发心跳报文;数据同步服务线程在备机端监听主机发送的同步数据报文,接收 IO 数据和 FBD 中间变量并更新本地状态镜像,回复同步确认。

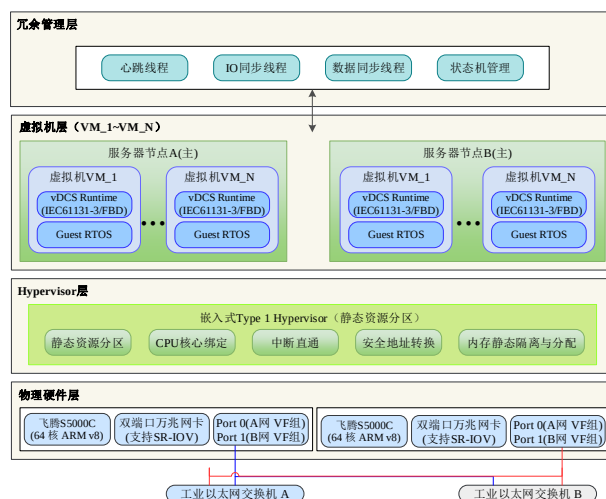


图 1 虚拟 DCS 控制器异机冗余系统 4 层总体架构
Fig.1 Four-layer overall architecture of the virtual DCS controller cross-machine redundancy system

1.2 VM 部署拓扑与冗余配对策略

本文采用 VM 级异机配对模型:服务器 A 的 VM_{Ai} 与服务器 B 的 VM_{Bi} 构成第 i 个冗余对。主机承担实际控制运算和对外通信,备机运行于热备模式,接收同步数据并维持状态镜像。同一冗余对的主备 VM 严格部署于不同物理机,确保单机故障不会导致冗余对同时失效。VM 独立分配 CPU 核心、内存区域和网络接口,无共享资源,防止单 VM 异常的扩散。异机部署拓扑如图 2 所示。

异机配对模型中主备 VM 各自独立运行,角色切换不涉及 VM 迁移或重启;冗余对之间互不干扰;VM 间通过 Hypervisor 硬件隔离,安全性优于共享 VM 模型的软件隔离。

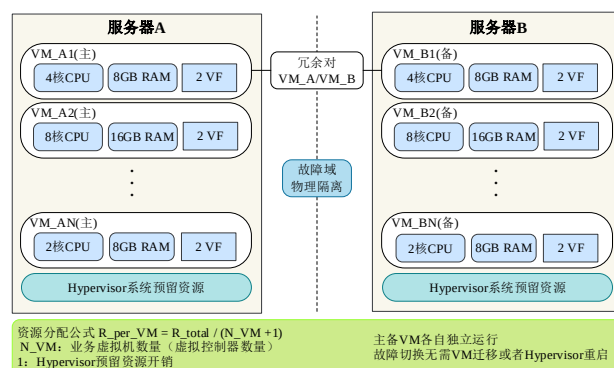


图 2 VM 异机冗余部署拓扑与资源分配示意
Fig.2 Schematic diagram of VM cross-machine redundancy deployment topology and resource allocation

1.3 基于 SR-IOV 的冗余通信链路设计

每个 VM 通过 SR-IOV 直通冗余同步 A/B 网

口。刘际会等^[12]研究了万兆以太网控制器上的 SR-IOV 技术设计方法。SOC-E 推出的 RELY-VPCIe 网卡^[13]将 HSR/PRP 零延时冗余协议和 PTP 精密时钟同步集成到 SR-IOV 虚拟化框架中,验证了 SR-IOV 与工业冗余协议融合的可行性。SR-IOV 直通性能基准研究^[14]表明 VF 直通模式可达到接近物理网卡的网络吞吐量和延迟水平。

82599ES 单端口支持创建最多 64 个 VF, 每个 VF 具有独立 MAC 地址、DMA 队列和 MSI-X 中断。VM 可直接与网卡进行 DMA 交互而无需 Hypervisor 介入。A/B 网 VF 分别绑定到 82599ES 不同物理端口, 物理端口各自连接独立交换机, 实现全链路物理冗余。SR-IOV 直通模式的选择基于以下工程考量: 为保障实时确定性, 不采用 virtio 等半虚拟化后端驱动, VF 直通是 VM 获取高性能网络访问的唯一可行路径。蒋坚强^[15]研究了 Xen Hypervisor 平台上 ARM 异构多核的 IO 全虚拟化, 梁克会等^[16]探索了 SR-IOV 在 Docker 容器网络中的应用, 为 SR-IOV 在不同虚拟化层次的部署带来了参考。冗余通信网口配置如图 3 所示。

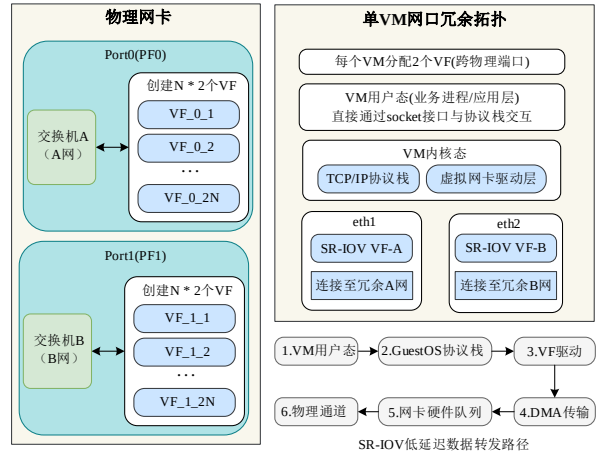


图3 基于SR-IOV的VM冗余通信网口配置
Fig.3 SR-IOV-based VM redundant communication network port configuration

1.4 链路级容错设计

链路容错分为 VF 级、端口级、整机级 3 级, 恢复时间逐级递增, 满足工业控制系统对分层故障管理的差异化要求。链路质量监测持续采集各 VF 错误帧率和队列深度, 劣化时触发预防性切换。三级链路容错的故障检测、切换恢复时间如表 1 所示。

表 1 三级链路容错机制
Tab.1 Three-level link fault tolerance mechanism

容错等级	故障范围	故障检测方式	切换/恢复方式	恢复时间
VF 级	单个 VF 驱动异常/PCIe 链路错误	链路状态监测+错误帧率超阈值	心跳机制切换至同 VM 另一 VF	≤ 单心跳周期(≤ 15 ms)
物理端口级	单物理端口故障/单交换机故障	该端口下所有 VF 批量失效检测	心跳机制切换至另一端口 VF 集; 单端口故障不影响另一端口	≤ 单心跳周期(≤ 15 ms)
整机级	服务器电源双路失效/主板/CPU 故障	备机心跳超时判定(连续 4 次)	备机升主管全部控制功能	≤ 60 ms

2 双任务冗余同步机制

2.1 总体设计

冗余同步机制设计为 2 类并行任务: 心跳任务和数据同步任务。心跳任务周期短但要求低延迟, 报文长度为数十字节; 数据同步任务传输实时控制数据(数百至数千字节), 周期与控制任务绑定, 对冗余链路负载消耗较大。双任务分离使每类负载可在各自优化空间内独立设计, 避免单一通信通道的竞争冲突。

Lee 等人^[17]在核电厂 PLC 虚拟化三模冗余研究中提出的虚拟模块冗余(VMR)思想, 与本文 VM 级软件冗余的理念一致。本文冗余同步机制针对每一组冗余 VM 对维护一个状态机, 如图 4 所示, 包含

4 个运行阶段: INIT——VM 启动后执行初始状态同步和角色协商; STEADY——主备角色确定, 心跳和同步正常运行; DEGRADED——单链路故障, 另一路正常链路维持运行(需告警); FAILOVER——主 VM 故障, 备 VM 升主并接管控制权, 备 VM 故障, 主 VM 保持并告警。

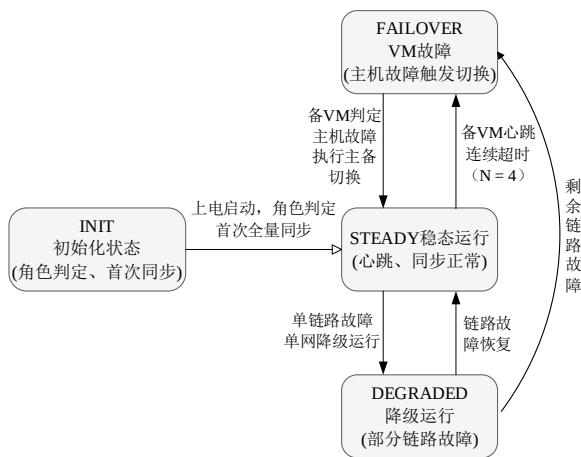


图4 冗余同步协议联合状态机

Fig.4 Joint state machine of redundant synchronization protocol

2.2 心跳任务设计

心跳任务以独立线程运行，备 VM 以周期 T_{hb} （默认 15 ms）通过 A/B 双网口同时向主 VM 发送心跳报文（报文逻辑如图 5 所示）。备机周期性发送心跳查询，主 VM 回复 ACK 并携带自身故障状态，备 VM 接收到 ACK 后比对双方状态，若备 VM 连续 3 次优于主 VM 状态，则备 VM 主动升主并向主 VM 发送切从报文令其降级；备 VM 若连续 4 次未收到主 VM 的 ACK 报文，判定主 VM 故障并触发切换流程。心跳周期与超时上限的选择基于以下权衡： T_{hb} 过短（如 5 ms）将显著增加网络带宽和 CPU 中断开销，过长（如 50 ms）则故障检测时间线性增长。15 ms 小于火电机组 100 ms 主流调节控制周期，可及时完成故障快速识别、主备切换。 $N=4$ 的选择则是为了容忍 A/B 双网同时发生 1~2 次偶发性丢包，在误判概率和检测速度之间取得平衡。

此外，备 VM 升主后通过 A、B 两路 VF 同时发送强制降备报文，只要主 VM 侧至少有一路 VF 仍正常即可接收到该报文并执行降级。

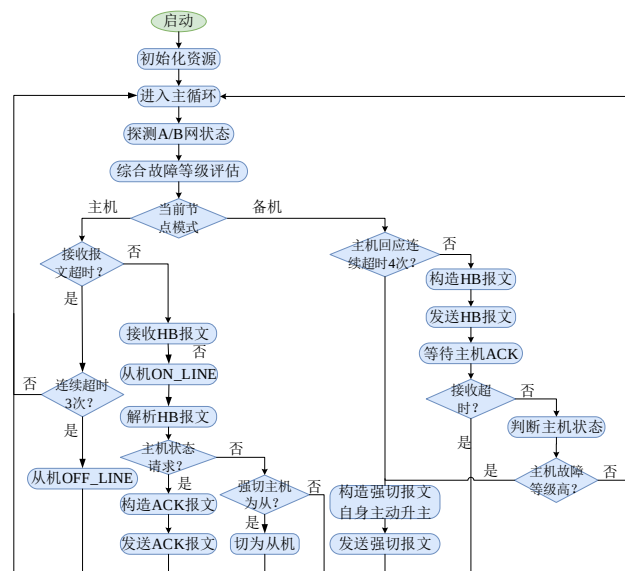


图5 双机冗余心跳流程

Fig.5 Dual-machine redundant heartbeat process

2.3 数据同步设计

数据同步由通过主机主动发起，备机被动接收并更新本地数据镜像，同步方向始终为“主机→备机”，确保数据源的唯一性。

2.3.1 同步数据范围

同步数据范围覆盖 VM 的 2 类运行数据：第 1 类为显式 IO 数据，包括数字/模拟 IO 变量和遥控遥调指令，是控制器与外部设备交互的直接映射数据；第 2 类为隐式中间变量，即 FBD 算法块运算产生的内部状态，如 PID 功能块的积分累加值、微分历史值和手自动切换状态，定时器/计数器的当前值与完成标志等。主备数据同步架构设计如图 6 所示。

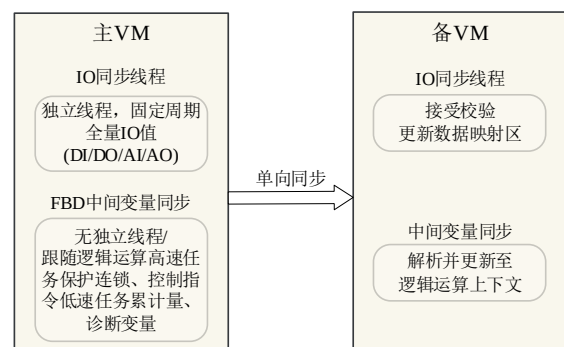


图6 数据同步双通道架构

Fig.6 Dual-channel architecture of data synchronization

数据同步采用乒乓同步策略：同步任务维护发送累计次数，发送前获取 A/B 网健康状态，若双网正常，奇数周期使用 A 网发送、偶数周期使用 B 网发送，每网口利用率为 50%，分散链路负载。若本

发送周期对应的单网故障时,立即切换至另一网口发送,仅 A/B 两网均失败才判定该周期同步失败。单网口故障条件下另一网口承担全部负载。

2.3.2 IO 数据同步

IO 数据由独立 IO 同步线程以固定周期执行。IO 同步线程的周期设置为快周期 (20 ms), 确保输入输出在最短时间内同步至备机。IO 同步线程从主机的 IO 映射区读取全部 IO 变量值,封装为同步报文发送。备机收到后更新本地 IO 映射表。IO 数据同步量取决于控制器 IO 点规模,本文实验负载的全量 IO 数据约 2 KB,在万兆以太网上的传输时间为微秒量级。

2.3.3 中间变量分级同步

FBD 中间变量同步不建立独立线程,而是跟随算法块所在的逻辑运算任务,每个运算周期内主 VM 完成该任务所有 FBD 算法块运算后,将对应的全部中间变量发送至备 VM。此设计将同步与运算紧密耦合,避免独立线程调度开销与数据缓冲竞争,同时确保同步数据的时效性及主备运算结果对齐。FBD 中间变量采用全量同步,宏观上看,所有中间变量在各自归属的任务周期内均完成同步,整体上全量覆盖,微观上看,同步跟随逻辑运算任务分批进行,将 IO 数据与各级 FBD 中间变量分散在不同时隙传输,避免了变量集中传输造成的网络瞬时拥塞,将每时隙的带宽占用控制在合理范围内。

逻辑运算任务的周期覆盖 50~1 000 ms 范围——实时控制任务 (50~200 ms) 包含一般模拟量控制和顺序控制步序逻辑,状态诊断任务 (500~1 000 ms) 包含累计量统计和诊断逻辑。以本文实验负载为例,100 ms 阀门控制逻辑的中间变量约 2.3 KB,200 ms 站间通信及负荷指令逻辑的中间变量约 18 KB,1 000 ms 的诊断及告警逻辑的中间变量约 0.2 KB。分级同步将全量 IO 数据与各周期中间变量分散在不同时隙传输,典型同步时序如图 7 所示。

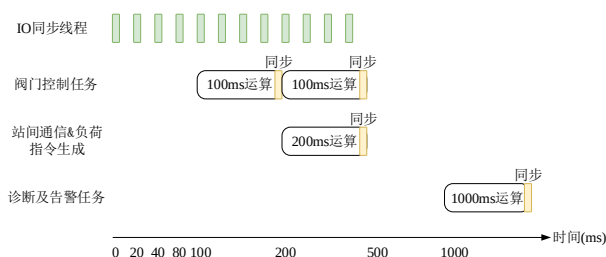


图 7 数据分级同步调度时序示意

Fig.7 Schematic diagram of data tiered synchronization scheduling timing

2.3.4 主备运算偏差控制

FBD 中间变量同步的核心目标是控制主备 VM 运算偏差在单个逻辑运算任务周期以内。在主备 VM 加载完全相同的控制逻辑配置和初始状态的前提下,若每个运算周期结束时备 VM 均能收到主 VM 本周期中间变量,则备 VM 在下一个周期的运算起点与主 VM 保持一致,主备运算偏差不超过一个任务周期内输入变量变化所导致的计算差异。以典型火电过程为例:主汽温调节时间常数约为 60~180 s,锅炉主汽压力调节时间常数约 90~160 s,给水流量时间常数约为 10~30 s,调节回路典型任务周期 T 一般为 100~200 ms,即使过程变量发生满幅阶跃扰动,单周期变化量一般不超过 0.1%,因此主备 VM 切换对正常调节的影响在工程可接受的范围内。

3 实验验证与分析

3.1 实验平台与负载

实验平台硬件:2 台飞腾 S5000C 处理器服务器 (16 核,64 GB 内存),各配 Intel 82599ES 双端口万兆网卡,分别连接 2 台工业以太网交换机。服务器部署 Type-1 Hypervisor,VM 中 OS 采用与物理控制器同源的嵌入式 RTOS。每台服务器部署 4 个虚拟控制器 VM,每 VM 分配 4 个 CPU 核心、8 GB 内存,通过 SR-IOV 直通 2 个 VF (A/B 网)。

实验负载采用某 1 000 MW 超超临界火电机组实际 DCS 协调控制逻辑:包括负荷指令形成、锅炉主控、汽轮机主控、燃料主控、水煤比控制、高低旁控制等复杂回路。变量总数 1 482 点、POU 页数 152 页、功能块 2 866 个、中间变量数 2 653。逻辑运算任务周期配置:100 ms (阀门控制)、200 ms (站间通信及协调控制)、1 000 ms (诊断及告警逻辑)。所有参数均为该机组实际工程配置。

3.2 冗余切换性能测试

实验通过故障注入法,选取火电 DCS 代表性的 4 类核心故障场景评估切换性能,每组 20 次取统计值,故障切换时间结果如表 2 所示。

由表 2 可以看出:主备切换时间为从故障发生到备 VM 完成升主的完整时间,各场景均值分布在 59.981~60.003 ms,标准差小于 0.01 ms,与心跳超时理论值 ($T_{hb} \times N$, $15 \text{ ms} \times 4 = 60 \text{ ms}$) 一致。所有场景切换过程中控制输出连续无跳变,仅偶发一个周期的输出保持,满足火电机组无扰切换要求。

本文方案备 VM 始终处于热备用状态, 切换仅涉及角色变更和控制权转移, 无需 VM 迁移或环境

重建, 切换速度具备量级优势, 切换总时间优于文献[7]的 ≤ 3 s 结果。

表 2 故障注入场景切换性能测试结果
Tab.2 Test Results of Switching Performance in Fault Injection Scenarios

故障场景	切换时间均值/ms	切换时间范围/ms	输出扰动
场景 A: 主 VM 服务器电源失效	59.998	59.995~60.002	无跳变, 画面偶发一个周期的输出保持
场景 B: 主 VM 服务器 A/B 网链路同时断开	59.981	59.976~59.992	无跳变, 画面偶发一个周期的输出保持
场景 C: 主 VM 服务器 DPU 进程异常退出	59.987	59.979~60.003	无跳变, 画面偶发一个周期的输出保持
场景 D: 主 VM 服务器单网链路断开	NA	NA	无切换, 输出无扰动

3.3 FBD 主备运算偏差验证

为验证 2.3.4 节的偏差控制目标, 设计如下对比实验: 在主备 VM 上同时部署正弦波发生器, 将其输出关联到 SCADA 趋势曲线中进行连续监视。正弦波是连续、周期性的标准信号, 任一周期内的微小不连续或相位跳变都能在趋势曲线中被清晰观察到。若主备切换后 SCADA 曲线保持平滑无跳变, 则可同时验证 2 个关键性能: 一是主备 VM 的 FBD 运算偏差被有效控制在一个任务周期以内; 二是控制输出的无扰切换性能。

除正弦波发生器外, 还部署了计数器块, 以固定周期驱动自增计数, 计数器当前值是典型的离散累积型状态, 任何一次同步丢失都会导致备机计数值落后于主机。

实验按以下步骤执行:

- 1) 主备 VM 以相同初始配置同时上电, 完成首次全量同步后进入稳态;
- 2) 稳态运行 5 分钟, 确认正弦波输出连续平滑、计数器值与主 VM 一致;
- 3) 手动命令触发主备切换;
- 4) 切换完成后继续观测 2 分钟, 确认新主 VM 输出稳定。

运算偏差测试结果如表 3 所示。可见, 在全部多组(不同周期、10 次)切换实验中, 均未观测到正弦波输出的可见跳变、毛刺或相位突变; 10 次切换中计数器输出值均完全一致(偏差=0), 验证了 FBD 离散量的同步精确性。实验验证了主备切换控制输出的无扰性。

表 3 FBD 主备运算偏差测试结果
Tab.3 Test results of FBD master-standby operation deviation

FBD 类型	任务周期	切换后偏差 (10 次均值)	<1 周期 偏差
正弦波发生器	50 ms/100 ms/500 ms	<0.05%振幅	满足
计数器	50 ms/100 ms/500 ms	0 (完全一致)	满足

3.4 冗余同步通信性能与系统开销

在 SR-IOV 直通链路条件下测试冗余同步通信性能。IO 数据(约 2 KB)的同步延迟(从主机发送到备机接收确认)中位数约 85 μ s, 远小于任务周期 20 ms 的实时约束。FBD 中间变量同步的延迟因各级任务中间变量数目不同而呈差异化分布: 100 ms 周期任务延迟中位数约 90 μ s, 200 ms 周期任务约 185 μ s, 1 000 ms 周期任务约 76 μ s。断开 A 网物理链路后, 同步任务自动切换至 B 网, 同步连续性不受影响, 测点波形未发生扰动, 验证了 A/B 网乒乓策略的单网故障切换有效性(图 8)。

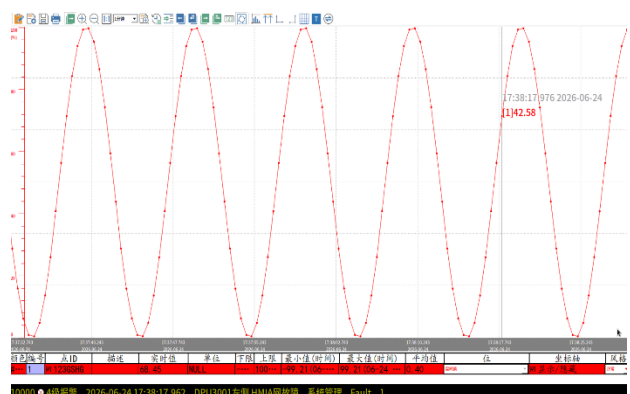


图 8 单网故障无扰切换效果示意
Fig.8 Schematic diagram of undisturbed switching effect in case of single network failure

当 4 对 VM 同时运行时, SR-IOV 网卡单端口有效吞吐量为 9.40 Gbit/s, 每端口创建 8 个 VF (对应 4 个 VM $\times$ 2 路 VF), 8 个 VF 同时满载发送场景下的可用带宽为 9.40/8 $\approx$ 1.18 Gbit/s。本文瞬时带宽需求峰值出现在 200 ms 周期任务的 18.6 KB 同步突发(瞬时带宽约 0.74 Gbit/s), 低于单 VF 最坏情况可用带宽, SR-IOV 带宽不构成瓶颈。各 VM 通过 CPU 绑定专用物理核心, VM 间无 CPU 调度竞争。

连续 72 小时稳态运行测试表明, IO 数据同步成功率 100%, 未发生同步超时或状态不一致。从网

络负荷角度分析, IO 同步线程以 20 ms 周期发送约 2 KB 数据, 约占万兆带宽的 0.08%; FBD 中间变量同步的瞬时带宽占用峰值在周期任务执行结束时出现, 但各周期任务的同步时隙交错分布, 网络负荷平稳、无明显突发拥塞。

4 结论

本文针对火电虚拟 DCS 控制器在 Hypervisor 架构下的异机冗余容错问题给出并验证了一套完整的冗余同步机制。主要结论如下:

1) 基于 SR-IOV 虚拟直通链路的 VM 级异机配对冗余架构能够为虚拟控制器提供高性能、确定性的冗余通信基础。SR-IOV 链路在万兆以太网条件下的通信性能满足 IO 数据(μs 级)和 FBD 中间变量(百 μs 级)同步的实时性需求。A/B 双网物理冗余结合三级链路容错, 能有效应对从单网口到整机的多粒度故障。

2) 心跳+数据同步双任务冗余管理协议通过功能分离和主机主动同步模式, 实现了快速故障检测(约 60 ms)与控制状态分级同步的高效并行。IO 数据由专用线程周期性同步, FBD 中间变量跟随逻辑运算任务周期同步——该策略在降低冗余网络负荷的同时, 将主备运算偏差控制在单个任务周期内, 从而实现了控制输出的无缝切换。

3) 在 Hypervisor 平台上的原型实验表明: 主备切换时间优于已有文献, 控制输出切换过程连续平滑; FBD 中间变量分级同步可控制主备运算偏差满足工程要求。该方案为火电厂虚拟 DCS 的冗余容错设计提供了可供参考的经验, 对于虚拟 DCS 的可靠性提升具有积极意义。

本文研究还存在一些局限: 当前仅在单 VM 异机冗余模型下完成验证, 未评估多对 VM 同时执行主备切换或同步大块数据时 SR-IOV VF 间的带宽竞争和 Hypervisor 调度延迟对性能的影响; 另一方面, 同步传输基于 UDP 协议, 尚未引入 TSN 时间敏感网络的确定性调度。后续工作将围绕 TSN 确定性冗余同步和更大规模工程验证展开。

【参考文献】

- [1] 柴天佑, 郑锐, 贾瑶, 等. 软件定义智能控制系统未来发展展望[J]. 东北大学学报(自然科学版), 2025, 46(7): 1.
Chai T Y, Zheng R, Jia Y, et al. Development and prospects for software-defined intelligent control systems[J]. Journal of Northeastern University (Natural Science), 2025, 46(7): 1.
- [2] 王亦卿, 夏长清, 金曦, 等. 面向信息物理生产系统的虚拟控制器研究综述[J]. 信息与控制, 2025, 54(2): 184.

- Wang Y Q, Xia C Q, Jin X, et al. Review of virtual controller research for cyber-physical production systems[J]. Information and Control, 2025, 54(2): 184.
- [3] Müller J, Giani M, Deubert D, et al. Virtualization in industrial production—a survey focusing on virtual and virtualized industrial controls[C]//2024 IEEE 29th International Conference on Emerging Technologies and Factory Automation (ETFA). Padova: IEEE, 2024: 1.
- [4] 赵琰. 软件定义工业控制器关键技术研究[与实现[D]. 广州: 广州大学, 2022: 18.
Zhao Y. Research and implementation of key technologies for software-defined industrial controllers[D]. Guangzhou: Guangzhou University, 2022: 18.
- [5] Kampa T, El-Ankah A, Grossmann D. High availability for virtualized programmable logic controllers with hard real-time requirements on cloud infrastructures[C]//2023 IEEE 21st International Conference on Industrial Informatics (INDIN). Lemgo: IEEE, 2023: 1.
- [6] 吴辰璇, 朱珂, 费盼峰, 等. 中煤新集利辛板集电厂虚拟 DCS 控制系统应用示范项目[J]. 自动化博览, 2025, 42(2): 81.
Wu C X, Zhu K, Fei P F, et al. Application demonstration project of virtual DCS control system in Banji power plant of China coal Xinji Lixin[J]. Automation Panorama, 2025, 42(2): 81.
- [7] 唐孝舟, 王言国, 张军华, 等. 基于双重虚拟化的水电厂计算机监控系统设计与实现[J]. 水电与新能源, 2025, 39(4): 13.
Tang X Z, Wang Y G, Zhang J H, et al. Design and implementation of computer monitoring system for hydropower plants based on dual virtualization[J]. Hydropower and New Energy, 2025, 39(4): 13.
- [8] 董凯凯, 袁合钊, 李达. SR-IOV 虚拟化技术在高并发环境中的应用[J]. 现代信息科技, 2025, 9(9): 102.
Dong K K, Yuan H Z, Li D. Application of SR-IOV virtualization technology in a high-concurrency environment[J]. Modern Information Technology, 2025, 9(9): 102.
- [9] 吕跃鹏, 刘俊阳, 杨喆. 基于虚拟化的火箭测发控软件冗余技术[J]. 航天控制, 2020, 38(3): 61.
Lü Y P, Liu J Y, Yang Z. Redundancy technology of rocket test and launch control software based on virtualization[J]. Aerospace Control, 2020, 38(3): 61.
- [10] 王雅哲, 任磊, 冯登国, 等. 面向感算控智一体化融合的工业互联网新型 PLC 安全增强: 趋势与展望[J]. 计算机学报, 2025, 48(3): 738.
Wang Y Z, Ren L, Feng D G, et al. Security enhancements for new-generation PLC of the industrial internet integrating sensing, computing, control and intelligence: trends and perspectives[J]. Chinese Journal of Computers, 2025, 48(3): 738.
- [11] Zhang X K, Gao S, Yu B T, et al. A high-performance fault-tolerant scheduling mechanism for virtualized industrial edge applications[C]//IECON 2025—51st Annual Conference of the IEEE Industrial Electronics Society. Madrid: IEEE, 2025: 1.
- [12] 刘际会. 基于万兆以太网控制器的 SR-IOV 技术研究与设计[D]. 上海: 中国电子科技集团有限公司研究生院, 2025: 59.
Liu J H. Research and design of SR-IOV technology based on a 10-gigabit Ethernet controller[D]. Shanghai: Graduate School of China Electronics Technology Group Corporation, 2025: 59.
- [13] SOC-E. Experience the premiere of RELY-VPCIe: SOC-E's breakthrough in virtualized industrial networking[EB/OL]. (2025-11-05). <https://soc->

- e.com/premiere-of-rely-vpcie.
- [14] Tran M N, Kim Y. Network performance benchmarking for containerized infrastructure in NFV environment[C]//2022 IEEE 8th International Conference on Network Softwarization (NetSoft). Milan: IEEE, 2022: 115.
- [15] 蒋坚强. 基于 Hypervisor 的 IO 设备虚拟化技术研究[D]. 哈尔滨: 哈尔滨工业大学, 2023: 21.
Jiang J Q. Research on IO device virtualization technology based on Hypervisor[D]. Harbin: Harbin Institute of Technology, 2023: 21.
- [16] 梁克会, 董龙, 洪华. 基于 SR-IOV 的 Docker 网络架构研究[J]. 智能计算机与应用, 2023, 13(1): 178.
- Liang K H, Dong L, Hong H. Docker container network architecture research based on SR-IOV[J]. Intelligent Computer and Applications, 2023, 13(1): 178.
- [17] Lee K I, Hwang S J, Yoon D H. Virtual modular redundancy of processor module in the PLC[C/OL]//Transactions of the Korean Nuclear Society Autumn Meeting, Gyeongju, Korea, 2016-10-27. Paper No.16A-512.
https://www.kns.org/files/pre_paper/36/16A-512_이광일.pdf.

(责任编辑 李园)