

## 轨道交通云平台研究\*

冯浩楠<sup>1,2</sup> 潘明<sup>1,3</sup> 姜庆阳<sup>1,3</sup> 金安<sup>4</sup>

(1. 中国铁道科学研究院集团有限公司通信信号研究所, 100081, 北京; 2. 国家铁路智能运输系统工程技术研究中心, 100081, 北京; 3. 广州铁科智控有限公司, 510220, 广州; 4. 中国铁道科学研究院集团有限公司铁道科学研究发展中心, 100081, 北京)

**摘要** [目的] 为推动轨道交通控制系统的现代化进程, 并提升其安全性、可靠性和运营效率, 特设计了一种轨道交通云控制系统架构, 旨在将该系统的安全苛求功能与非安全功能有效集成并部署于云平台之上。[方法] 通过光纤方式连接对象控制器与云平台服务器, 实现远距离分布式控制。分析了轨道交通云控制系统的特点, 并从时间管理、空间管理、共享资源管理、运行模式管理、降级模式管理和安全监控等 6 个方面梳理了安全需求。[结果及结论] 云平台的虚拟化层须在空间隔离、时间隔离、故障隔离和管理、可预测性、安全性和机密性等方面进行设计; 云平台的调度机制包括时间触发调度和事件驱动两种机制, 二者对平台的时序约束产生不同的影响; 云平台的分层调度存在 4 种资源共享协议, 须根据不同的任务进行选择。

**关键词** 城市轨道交通; 云平台; 安全需求; 调度算法

**中图分类号** TP39; U231<sup>+</sup>. 92

**DOI**: 10.16037/j.1007-869x.2024.10.031

## Research on Rail Transit Cloud Platform

FENG Haonan<sup>1,2</sup>, PAN Ming<sup>1,3</sup>, JIANG Qingyang<sup>1,3</sup>, JIN An<sup>4</sup>

(1. Signal and Communication Research Institute of China Academy of Railway Sciences Group Co., Ltd., 100081, Beijing, China; 2. The Center of National Railway Intelligent Transportation System Engineering and Technology, 100081, Beijing, China; 3. Guangzhou Railway Sciences Intelligent Controls Co., Ltd., 510220, Guangzhou, China; 4. Railway Science and Technology Research and Development Center of China Academy of Railway Sciences Group Co., Ltd., 100081, Beijing, China)

**Abstract** [Objective] To advance the modernization of rail transit control systems and enhance their safety, reliability and operational efficiency, a cloud-based control system architecture for rail transit is designed. The aim is to effectively integrate and deploy both the safety-critical and non-safety-critical functions of rail transit system onto a cloud platform.

[Method] A cross-regional distributed control is realized by connecting target controllers to cloud platform servers via optical fiber. Characteristics of the rail transit cloud control system are analyzed, safety requirements of the system are outlined across six aspects: time management, space management, shared resource management, operation mode management, degradation mode management and safety monitoring. [Result & Conclusion] The virtualization layers of the cloud platform must be designed to ensure spatial isolation, temporal isolation, fault isolation, as well as management, predictability, security, and confidentiality. The platform scheduling mechanism includes both time-triggered and event-driven approaches, each impacting the platform temporal constraints differently. The hierarchical scheduling of the cloud platform involves four resource-sharing protocols, which must be selected based on different tasks.

**Key words** urban rail transit; cloud platform; safety requirement; scheduling algorithm

随着云平台技术的快速发展, 轨道交通系统中的非安全控制系统进行了云系统化的尝试, 如 ATS (列车自动监控系统)<sup>[1-2]</sup>、维修系统<sup>[3]</sup>和能源管理<sup>[4]</sup>等。2020 年, 德国西门子公司的 DS3 型云联锁系统通过 SIL4 (安全完整性等级) 认证并应用, 标志云技术在轨道交通安全控制领域应用研究的重大突破。

与现有的安全控制平台技术不同, 云平台凭借多核 CPU (中央处理器)、虚拟化等先进技术, 展现出强大的处理能力和灵活易扩展性等优势, 已成为轨道交通领域未来发展的重要趋势之一<sup>[5-6]</sup>。为了充分利用云平台的这些优势, 本文提出了一种轨道交通混合云控制系统的架构, 旨在将轨道交通系统的核心功能迁移到云端。在深入分析云平台架构的基础上, 本文对其安全需求和关键技术进行了全

\* 中国铁道科学研究院重点基金项目 (2021 YJ305)

面研究,以期为云平台的功能设计及实现提供科学的指导和规范。这一工作不仅有助于推动轨道交通控制系统的现代化进程,还为提高轨道交通系统的安全性、可靠性和运营效率奠定了坚实基础。

## 1 轨道交通云控制系统

### 1.1 系统架构

城市轨道交通的云控制系统架构包括聚合层、网络层和接口层,如图 1 所示。在聚合层,地面安全苛求系统,如 CBTC(基于通信的列车自动控制)系统中的 CI(联锁)系统、ZC(区域控制)系统的逻辑功能和安全等级低的 ATS(列车自动控制)、综合监控系统非安全功能统一汇聚在云平台中实现。接口层通过对象控制器实现对车载 ATP(列车自动防护)、轨旁设备的通信和操作以及维修功能。网络层保证对象之间的可靠通信。

城市云平台(以下简称“云平台”)详细架构如图 2 所示,每个应用程序在虚拟核中运行。管理程序作为云平台的重要管理部分,须根据应用程序的

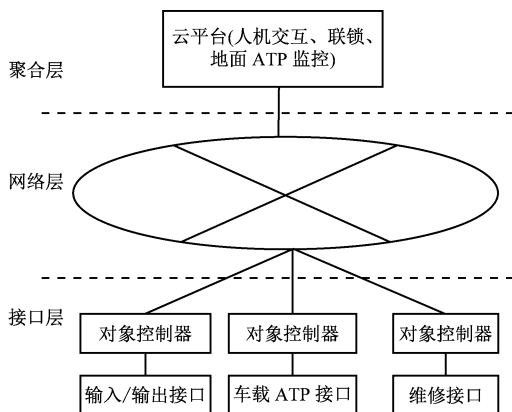


图 1 轨道交通云控制系统架构

Fig. 1 Architecture of rail transit cloud control system

要求进行调整和定制,且还需满足系统的实时性、电源效率、可靠性和安全性属性要求。当硬件是多核系统时,管理程序可以为分区提供比真实 CPU(中央处理单元)多的 vCPU(虚拟 CPU),以便开发可能需要多核解决方案的应用程序。

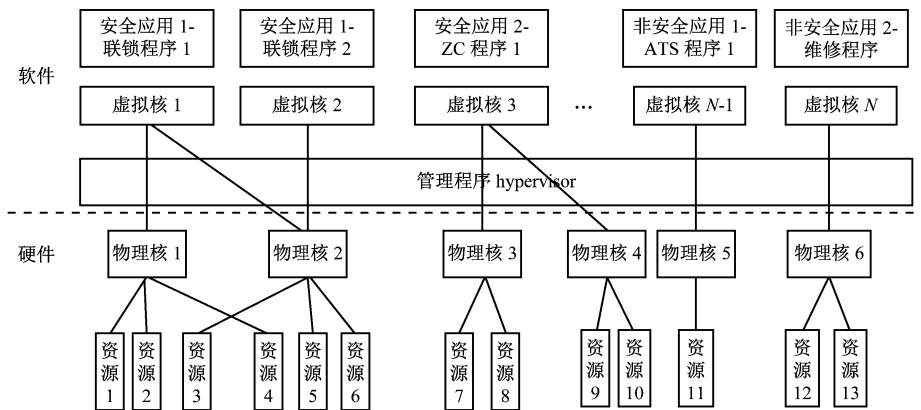


图 2 云平台详细架构

Fig. 2 Cloud platform detailed architecture

### 1.2 系统特点

云平台中的服务器在地理上实现了多点备份,确保了数据的安全性和系统的稳定性。OC(对象控制器)通过光纤与云平台的服务器相连,实现了远距离的分布式控制,增强了系统的灵活性和响应速度。与现有的轨道控制系统相比,原先分散在轨旁的各类安全及非安全应用程序被有效整合至云服务器或服务器集群中,实现了任务的集中处理与高效管理。其特点和优势具体体现在以下几个方面:

1) 通过备份服务器的容错机制,显著提高了系统的可用性。云服务器的应用层在遭遇负载均衡

不均、待机状态切换或服务器故障等情况时,能够迅速通过切换技术或动态调整内存、CPU 内核等资源,确保系统持续稳定地运行。

2) 服务器群之间的紧密交互,进一步增强了系统的可用性。云平台能够在多个服务器群之间同步控制逻辑,提供地理分布式的备份和备用功能,有效防止单点故障对整个系统的影响。

3) 利用最新的服务器硬件技术,不断提升系统性能,满足日益增长的业务需求。

4) 通过灵活添加服务器硬件资源,轻松实现系统的可扩展性,适应未来可能的发展变化。

- 5) 采用 COTS(商用现成品)服务器、常用操作系统以及非安全应用程序的标准软件库,不仅降低了硬件和软件的成本,还减少了对特定供应商的依赖,提高了系统的自主性和灵活性。
- 6) 借助虚拟化技术,系统能够独立于特定的硬件架构运行,增强了系统的兼容性和可移植性。
- 7) 通过在模拟器中运行现有的控制系统逻辑程序,简化了开发流程,缩短了产品上市时间,降低了开发成本。

2 安全需求

云平台中的各类安全苛求应用程序均运行在 VM(虚拟机)环境中,这些 VM 被严格封装以确保

安全性。VM 之间的错误隔离是关键,即一个 VM 中的错误不应触发其他 VM 中的任何故障,这可以通过对 VM 所需的资源进行精细分区来实现。此外,当多个 VM 在同一硬件上运行时,需要预测它们的运算时序行为,并采取措施排除多核处理器可能带来的干扰。同时,VM 必须能够安全可靠地与 OC 连接,以便有效地控制轨旁设备,如计轴器、信号机、道岔等。

针对上述轨道交通控制系统的安全需求和设计考虑,本文从时间管理、空间管理、共享资源管理、运行模式、降级模式以及安全监控等 6 个关键维度进行了全面的梳理和界定。具体内容总结如表 1 所示。

表 1 云平台的安全需求  
Tab.1 Safety requirements of cloud platform

安全需求	子需求	解释
时间管理	时间约束	在轨道交通控制系统中,存在“安全”和“非安全”的实时任务;安全任务优先级高,由系统功能、项目的风险评估以及相应安全标准确定
	任务到达间隔率	为了确保任务能够满足各自的时间门限,管理程序须控制任务的到达率、时间门限和阻塞时间
	计时故障传播预防	当实时任务发生故障或任务处理时间超时的情况时,故障不能影响平台其他分区中运行任务的时序属性;此外,云平台的安全监控须能检测此类故障发生
	时间管理软件的安全等级	时间管理软件安全等级须设计为最高安全等级
空间管理	逻辑隔离	平台中各应用任务都应在各自分配的内存空间运行,不得修改分配给其他任务的内存空间中的数据;须进行空间隔离以保护任务的数据、代码和堆栈
	硬件强制保护	为了确保多个独立分区的隔离,底层硬件应能够限制内存空间、处理时间和输入/输出的访问
	内存空间定义	内存分区的配置及其各自的大小应在离线时定义,不得在程序运行中修改
共享资源管理	分区内共享资源	资源共享协议应确保访问分区内共享资源所需时间是确定和可预测的;平台对分区内的任务进行调度性分析时,须确定访问分区内共享资源的阻塞时间上限
	分区间共享资源	资源共享协议应确保访问在分区之间共享的资源所需的时间是确定性和可预测的;平台对分区间的任务可调度性分析中,须确定访问分区间共享资源时的阻塞时间上限
	资源访问前的预计时限	任务在等待共享资源期间,任务的预留时间超时,任务将无法对共享资源进行访问直到任务的预留时间重新补充满足时限要求
运行模式管理	—	系统可在不同的操作模式之间切换,且不影响系统的安全性;轨道交通云控制系统须具备不同的操作模式,以满足对外部事件(例如传感器读取)和内部事件(例如硬件故障)的应急反应和处理。须始终确保系统的安全性在所有情况下都保持运行
降级模式管理	安全降级	为防止严重故障,系统须能暂停安全操作所需的非必要任务,在降级模式下运行
	任务暂停	遇到严重故障时,触发转换到降级操作模式,云平台须在运行时允许暂停任务
安全监控管理	故障分析	确保识别出须监控的所有潜在故障
	监控功能等级	平台硬件和软件监视功能等级应与被监视功能的最严重故障等级相适应
	监控和被监控功能之间的隔离	监控功能不应受被监控对象功能故障的影响,可通过将监控和被监控功能分配给不同的分区或者硬件实现
	定时故障检测	发生任务时序故障时,管理程序须能够检测故障并在应用程序生成故障报警事件

### 3 云平台关键技术

#### 3.1 虚拟化层

虚拟化是云平台的核心特征之一,它通过抽象底层硬件并提供 CPU 虚拟化的软件层来实现。管理程序(或称为 Hypervisor)能够控制多个相互隔离的虚拟机。虚拟化层作为所有虚拟机的公共基础,为了支持不同安全等级的应用程序,其设计必须遵循最高安全等级的标准。

##### 3.1.1 虚拟化层属性

虚拟化层的属性包括但不限于:

1) 空间隔离:管理程序必须能够对虚拟机进行空间隔离控制,确保每个虚拟机完全分配在唯一的地址空间(包括代码、数据和堆栈)。

2) 时间隔离:虚拟机的任务执行应独立于其他虚拟机,避免在执行过程中受到其他虚拟机任务的干扰。

3) 故障隔离与管理:当故障发生时,管理程序应能迅速检测并正确处理隔离故障区域,防止故障传播。云平台的故障模型应能覆盖并处理不同类型的错误。

4) 可预测性:管理程序应提供可预测的服务,包括分区执行中的操作及中断管理,以减少应用程序受底层软件(如客户操作系统或管理程序)和硬件的影响。

5) 安全性:必须采取措施防止虚拟机中的信息被未经授权的访问或修改。

6) 机密性:确保虚拟机之间不能相互访问对方的空间,也不能窥探系统的内部工作机制。

##### 3.1.2 分层调度

虚拟化层采用循环方式调度虚拟机,通过定义 MAF(主要活动框架)的时隙来确保每个虚拟机使用处理器的时间不超过预设的时间门限,从而避免对其他虚拟机造成不利影响。每个虚拟机都被分配在一个具有明确起始时间和持续时间的时隙中。若虚拟机内部存在并发任务,则需在虚拟机内部实现额外的调度算法进行控制。这种两级调度方案被称为分层调度。

##### 3.1.3 多核调度

虚拟化层支持多种调度策略,这些策略可以附加到任何处理器上。最常用的两种调度策略为:

1) 循环调度:以固定的、循环的方式调度虚拟机,确保每个虚拟机使用处理器的时间不超过预定

的时间门限。虚拟机的可用时隙在其配置文件中定义。

2) 优先级调度:根据虚拟机的优先级进行调度。优先级也在配置文件中定义。

##### 3.1.4 多模式调度

轨道交通云平台需处理多种类型任务,因此设计时采用了多种调度模式。在运行过程中,任务集可能会因任务参数的修改、任务的添加或移除等原因发生结构变化。虚拟机可请求从一个调度模式切换到另一个模式,一旦请求被接受,将在下一个 MAF 时间间隔结束后生效。

#### 3.2 调度机制

云平台采用时间触发和事件触发两种调度机制以满足对外通信的时间约束需求:

1) 时间触发调度:为服务资源请求分配不重叠的时隙,通过时域分离避免运行时间资源的争用。该策略的时序分析算法相对简单,可在调度配置工具中实现,以满足时序约束。

2) 事件驱动调度:通过优先级或仲裁机制预测并解决运行时间资源的争用问题。为满足时间约束需求,采用时序分析算法预测仲裁导致的时间延迟。

#### 3.3 资源共享协议

在云平台的分层调度中,为防止不同处理器上的任务在访问共享资源时出现无限阻塞现象,云平台采用了多种资源共享协议。目前主要有以下四种:

超限机制共享协议:允许处理器消耗额外预算时间以完成安全部分的任务,但可能违反时间隔离的安全属性。

SIRAP(子系统集成和资源分配)协议:在授予共享资源访问权限前进行预算检查,确保处理器有足够时间完成安全部分的任务。缺点是可能延长任务响应时间。

BROE(有界延迟资源开放环境)协议:当任务因预算不足无法访问临界区时,及时延长预算时间,以保持处理器响应时间和任务最大响应时间。

MC-IPC(混合临界进程间通信)协议:利用带宽继承概念,允许一台处理器代替另一台处理器处理任务的安全部分。该协议解决了安全任务预算时间不足的问题,但带来了新的挑战,如高迁移成本 and 方案复杂性。



## 4 结语

结合轨道交通控制的特点,本文对云平台的安全需求进行了梳理,并详细介绍了云平台的虚拟化层、调度机制、资源共享协议等关键技术。针对云平台在处理安全任务时可能遇到的预算时间耗尽问题,现有的资源共享协议仍有较大改进空间,是未来研究的重要方向之一。

## 参考文献

- [1] 王振东,齐威,苗义峰,等.基于云计算技术的铁路调度集中系统架构设计研究[J].铁道运输与经济,2020,42(1):38.  
WANG Zhengdong, QI Wei, MIAO Yifeng, et al. A study on the design of the architecture of railway CTC system based on cloud computing technology [J]. Railway Transport and Economy, 2020,42(1):38.
- [2] 赵宏涛,陈峰,许伟,等.基于云边协同的高速铁路智能行车调度系统研究[J].铁道运输与经济,2021,43(1):71.  
ZHAO Hongtao, CHEN Feng, XU Wei, et al. High-speed railway intelligent traffic control system based on cloud edge collaboration [J]. Railway Transport and Economy, 2021,43(1):71.
- [3] 李杰,徐启禄.基于云平台的城市轨道交通智能运维系统设计与应用[J].城市轨道交通研究,2021,24(8):213.

## (上接第182页)

- [4] 许成,王慧芳,王晓保.直流牵引供电系统短路计算模型分析[J].电力系统保护与控制,2013,41(22):84.  
XU Cheng, WANG Huifang, WANG Xiaobao. Analysis of short-circuit model for DC traction supply system[J]. Power System Protection and Control, 2013, 41(22): 84.
- [5] 张智杰.城市轨道交通DC1500V供电系统研究[D].兰州:兰州交通大学,2015.  
ZHANG Zhijie. Research on DC1500v power supply system of urban rail transit [D]. Lanzhou: Lanzhou Jiatong University, 2015.
- [6] 金雪丰,陈裕楠,童翔.直流牵引供电系统短路试验分析[J].都市快轨交通,2016,29(3):103.  
JIN Xuefeng, CHEN Yu'nan, TONG Xiang. Analysis on short circuit test of DC traction power supply system[J]. Urban Rapid Rail Transit, 2016, 29(3): 103.
- [7] 韩志杰.城轨直流牵引供电系统短路试验[J].都市快轨交通,2013,26(1):113.  
HAN Zhijie. Short-circuit test on DC traction power supply system of urban rail transit [J]. Urban Rapid Rail Transit, 2013, 26(1): 113.
- [8] 周邵钢,吴观华,李艳明,等.一种城市轨道交通接触网受

- 电检测装置及检测方法:CN 114 778973A[P]. 2022-07-22.  
ZHOU Shaogang, WU Guanhua, LI Yanming, et al. An urban rail transit contact network electrified detection device and detection method: CN 114 778973A [P]. 2022-07-22.
- [9] 郭泓宏.低压电器短路试验平台设计与运营[D].上海:东华大学,2022.  
GUO Minghong. Design and operation of short circuit test platform for low voltage electrical apparatus [D]. Shanghai: Donghua University, 2022.
- [10] 肖涛古.城轨直流供电系统模型及直流短路分析[D].广州:华南理工大学,2012.  
XIAO Taogu. DC power supply system model of subway and DC short circuit analysis [D]. Guangzhou: South China University of Technology, 2012.

· 收稿日期:2022-06-07 修回日期:2022-08-15 出版日期:2024-10-10  
Received:2022-06-07 Revised:2022-08-15 Published:2024-10-10  
· 第一作者:冯浩楠,副研究员,fln02212005@163.com  
通信作者:姜庆阳,副研究员,tklsjqy@163.com  
· ©《城市轨道交通研究》杂志社,开放获取 CC BY-NC-ND 协议  
© Urban Mass Transit Magazine Press. This is an open access article under the CC BY-NC-ND license