造成环境考量往往在规划核心框架大致确定后才开始介入，其作用多是对既定方案进行补充性的评估与局部的修正，没法从源头上躲开重大环境风险，也无法引导规划走向更好的可持续之路。需要扭转这一态势，一定要推动环境影响评价完成根本性的范式转型，由“末端评估”转变为“规划早期参与、全过程融合”的主动式流程。核心要点为，把环境及可持续性目标融入规划自身的核心，保障规划构思在最初阶段，生态底线、资源承载力、气候韧性等重要环境维度，构成定义规划愿景与约束条件的基石。

实现这种深度的融合，应在规划编制的全部流程里，在关键决策的各个节点均嵌入严格的环境分析环节。在规划目标设定的阶段，应当按照区域生态环境本底状况评估的结果，制定可量化、可监测的生态保护与低碳发展目标。方案生成及比选优化阶段，需运用空间分析以及情景模拟等工具，对不同规划布局方案引发的生态系统服务损益、碳排放轨迹、资源消耗强度与环境健康影响做预测和对比。每个环节里的决策，明确详尽的环境及可持续性分析结论必须作为输入依据，使环境优劣变为方案取舍的核心标准之一，绝非事后的点缀物。

这种深刻的流程重造，肯定需要对现有的规划编制技术规程以及管理流程实施系统性革新。制度上要明确规定规划文本得有从头到尾的环境逻辑线和专题分析章节，同时明确其提交与论证的时间顺序，必须让规划编制单位和环境评价机构全程协同工作。双方要在早期共同成立团队，实现工作大纲制定、基础数据共享、模型方法对接、结论会商等环节的无缝协作。必须重点加强规划决策者以及环境管理者相关能力的建设，经由培训提升其综合思维素质，让其切实明白并看重早期环境介入的战略意义，可在审查决策中精准辨认与采纳融合成果，依靠管理终端保障这一变革切实落地[4]。

4.3 发展基于大数据与智能技术的创新评价方法

多种数据资源融合给交通与环境研究打下前所未有的分析基础，手机信令数据可连续且大范围地呈现人口流动的时空特性，浮动车轨迹数据细致勾勒出道路网络的运行情况与拥堵模式，环境遥感数据可对大气污染物分布、地表温度及植被覆盖变化进行动态监测，多维空间要素被地理信息数据整合起来。这些数据的交叉验证与叠加剖析，可以打造出一个高度精细、可视化的线状图像，清晰呈现出交通流分布规律，也一同呈现出与之有关的环境本底情形，像交通走廊跟空气质量监测高值区的空间耦合情况，给深入理解城市系统里人、车、环境的互动打下了坚实的数据底子。

有强大的数据做后盾，人工智能与机器学习技术介入，大幅提高分析模型智能水平与预测能力。借助训练深度神经网络之类的模型，可以深入钻研交通流量、车速、车型构成与噪声排放、尾气污染物的复杂非线性关系，实现对交通环境影响的高精度动态模拟及预测。这种智能分析能力进一步为规划过程的生态保护环节赋能，系统能自动掌握生态敏感区域多源特征。

更进一步说，这种技术集成体系可实现对不同规划情景可持续性绩效的快速、多维度评价，构建起数字孪生或仿真平台，可动态模拟不同交通发展策略、基础设施配置或管理政策施行后，交通效率、能源消耗、排放水平、生态影响以及社会经济成本等方面的综合成效。这种仿真过程可实时对参数进行调整，即时将结果可视化呈现，用直观图表、热力图、动画等形式呈现长期演变趋势与空间差异，这把传统又耗时又费力的评估工作变成高效的数字化推演，极大提升工作效率，可向决策者提供更深入的因果洞察以及前瞻性预警，支持达成更科学、更具韧性的可持续交通与空间规划方案[5]。

5 结语

区域综合交通规划的环境影响评价同可持续性探究，兼顾发展与保护、平衡效率与公平的必然需要。未来实践要把这些理念、框架及策略制度化、工具化，使环境可持续性目标真实变为区域综合交通规划的硬性规定与内在逻辑，进而促进形成绿色、高效、包容、韧性的区域综合交通体系，为区域高质量、可持续发展筑牢坚实根基。

参考文献

[1] 袁康贵.区域综合交通规划环境影响评价指标体系分析[J].皮革制作与环保科技,2021,2(20):151-152.

[2] 王艳,王浙锋,王一宁.对目前城市轨道交通建设规划环评编制的思考——以宁波市为例[J].绿色环保建材,2020,(10):56-57.

[3] 朱高儒,刘杰,王兰,徐洪磊,杨柳.区域综合交通规划环境影响评价指标体系研究[J].公路,2020,65(03):279-284.

[4] 熊吉安,梅仁明.我国规划环评现状与问题及对策建议[J].中国工程咨询,2018,(03):56-59.

[5] 程时广,孟娟.战略环评在城市群生态综合交通规划中的应用分析[J].交通与运输(学术版),2017,(02):85-89.

Research on Multi-Safety-Level Intelligent iRIOM

Ning Zhou[1] Xisheng Xia[1] Hongjie Liu[2] Chunyu Zhang[1]

1. MetaBox Technology Co., Ltd., Beijing, 100070, China
2. Beijing Jiaotong University, Beijing, 100044, China

Abstract

This paper addresses the issues such as equipment redundancy, space occupation, and high cost caused by the separate deployment of train network control equipment and signal system acquisition units in the electronic and electrical systems of rail transit vehicles. It proposes an intelligent acquisition system iRIOM for vehicle TCMS and signal integration. This scheme is based on a unified hardware platform, integrates the SIL2 network control acquisition and the SIL4 signal safety acquisition capabilities, and focuses on the goals of "high real-time, strong isolation, certified security, and operability". It covers the hardware architecture, software architecture, task scheduling architecture, and security mechanism design. The aim of this paper is to achieve resource integration and cost optimization throughout the entire lifecycle without lowering the SIL4 safety standard. It provides an overall solution that can be implemented in engineering for the safe integration of vehicle TCMS and signal systems.

Keywords

iRIOM; Multi-safety levels; Safety isolation; Real-time performance; Redundancy and fault tolerance

城轨车辆 TCMS 系统与信号融合智能驱采系统研究

周宁[1] 夏夕盛[1] 刘宏杰[2] 张春雨[1]

1. 米塔盒子科技有限公司，中国·北京 100070
2.北京交通大学自动化与智能学院，中国·北京 100044

摘 要

本文针对轨道交通车载电子电气系统中列车网络控制设备与信号系统驱采单元分立部署导致的设备冗余、空间占用、成本高昂等问题，提出一种车辆TCMS与信号融合智能驱采系统iRIOM方案。该方案基于统一硬件平台，融合SIL2网络控制驱采与SIL4信号安全驱采能力，核心围绕“高实时、强隔离、可证安全、可运维”目标展开，涵盖硬件架构、软件架构、任务调度架构与安全机制设计。本文旨在不降低SIL4安全标准的前提下，通过架构融合实现资源整合与全生命周期成本优化，为车辆TCMS与信号系统的安全融合提供可工程化实施的整体解决方案。

关键词

iRIOM；多安全等级；安全隔离；实时性；冗余与容错

1 引言

1.1 研究背景

轨道交通车辆电子电气架构由多个控制与安全子系统构成，其中：

列车网络控制设备承担大量非安全或 SIL2 安全等级 I/O 驱动与采集任务，驱采单元安全等级往往为 SIL0~SIL2[1]。

车载信号系统直接影响行车安全，其 I/O 驱采与安全处理链路通常要求 SIL4，并且在主机架构上常采用 二乘二取二（2*2oo2）或等效冗余策略，以满足极低失效概率要求。

行业中普遍采用“网络控制驱采”和“信号安全驱采”分立配置的原因很直接：SIL4 的安全认证、隔离要求、实时性要求、故障响应策略与 SIL2 明显不同。分立部署能降低耦合风险，但带来了系统层面的代价：

1）插箱数量增加、线缆与连接器规模膨胀、重量与体积上升；

2）运维对象增多、备件体系复杂；

3）设备间接口增多，潜在故障点增加；

4）多系统之间的时序协调与一致性维护更困难。

1.2 问题与挑战

把 SIL2 网络驱采与 SIL4 信号驱采融合到同一设备，需要解决两个问题：

1）实时性与确定性：信号驱采与 ATP 主机之间通常使用内部实时总线 / 专用链路，周期短、抖动要求严苛；驱采

【基金项目】国家自然科学基金（项目编号：52372310, U2569210）；北京市自然基金（项目编号：L251056）。

【作者简介】周宁（1988—），男，中国河南焦作人，硕士，工程师，从事交通信息工程及控制研究。

是 ATP 子系统 2*2oo2 安全链路组成部分。融合后如何保证该链路的端到端时延、抖动与吞吐不受 SIL2 业务影响 [2]？

2）可靠性与安全性：SIL4 需要强隔离、强诊断、确定的故障响应、可审计的安全机制 [3]。融合后如何避免“低安全等级故障向高安全等级传播”？

1.3 创新点

本文的主要贡献可概括为：

1）多安全等级融合的 iRIOM 架构：提出在同一平台内实现 SIL4 安全域与 SIL2 控制域并存的硬件 / 软件分区方案，明确隔离边界、受控数据交换路径与故障遏制策略。

2）面向 ATP 的 SIL4 驱采实现要点：给出双通道独立处理、2 乘 2 取 2 一致性比对、故障触发安全状态的关键机制及其工程化落地方式。

2 需求分析与总体指标

2.1 功能需求

1）SIL4 信号驱采能力：支持 ATP 需要的安全输入采集与安全输出驱动；支持 2 乘 2 取 2 处理与一致性判决；支持与 ATP 的高实时性、确定性通信接口。

2）SIL2 网络驱采能力：支持车辆控制与网络 I/0；支持列车网络通信；支持在线诊断与常规维护。

3）融合需求：两套功能在同一平台并存，互不干扰；同一供电、维护接口，减少系统级复杂度。

2.2 非功能需求

1）实时性与确定性：SIL4 任务周期、抖动、端到端延迟需可预算、可验证；SIL2 负载变化不得影响 SIL4 关键路径（强隔离、强优先级）。

2）可靠性与可用性：支持电源冗余、关键处理冗余（；故障可检测、可定位、可恢复，必要时进入安全状态。

3）隔离与故障遏制 [4]：SIL2 故障不得传播到 SIL4；SIL4 故障以 fail-safe 方式处置。

2.3 SIL2 与 SIL4 驱采差异对比

SIL2 网络驱采与 SIL4 信号驱采从多个角度的差异对比如表 1 所示。

表 1 SIL2 与 SIL4 驱采差异对比表

类别	SIL2 驱采	SIL4 驱采
典型架构	主备	2 乘 2 取 2
实时性	软实时	硬实时
诊断覆盖	基础诊断	周期自检
隔离要求	中等	强隔离
故障处置	重启、降级	阻断输出、进入安全状态

3 总体架构设计

3.1 系统架构

满足多安全等级融合驱采要求的 iRIOM 系统架构图如图 1 所示，系统架构设计依据如下原则：

1）安全域优先：SIL4 关键路径必须有“资源优先权”和“隔离保障”。

2）隔离先于共享：能隔离的先隔离，必须共享的通过网关受控共享。

3）故障可控扩散：定义故障遏制区域（Fault Containment Region），让故障在域内闭环。

4）证据链设计：架构设计同时考虑后续安全认证、测试与审计需要。

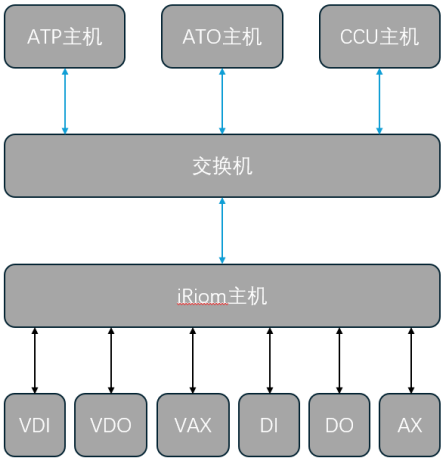

图 1 系统架构图

系统分为控制层、融合层、执行层。控制层包括 ATP 主机、ATO 主机、CCU 主机。融合层包括 iRIOM 主机以及交换机。执行层包括安全数字量采集板、安全数字量驱动板、安全模拟量混合驱动采集板、数字量采集板、数字量驱动板、模拟量混合驱动采集板。

3.2 系统接口

iRIOM 位于 控制层与执行层之间：

对上：与 ATP 主机进行高实时数据交互（安全输入 / 输出、状态）；与车辆网络 /TCMS/ 其他控制设备交换信息（非安全 / 低安全）。

对下：连接传感器、执行器、继电器、编码器等 I/O 现场侧。

4 硬件架构设计

多安全等级 iRIOM 的主控板将基于 2 乘 2 取 2 冗余架构设计，旨在提供极高的可靠性和功能安全。每个“2 取 2”系统 (即一个主控板) 内部将集成多核处理器，并通过硬件和软件层面的隔离，同时承载 SIL4 和 SIL2 级别的 I/0 驱采服务。

4.1 主控板硬件组成

每个主控板将包含以下主要硬件组件 [5][6][7][8]:

1）多核安全处理器 : 选择支持硬件虚拟化辅助功能的处理器，具备内存保护单元 (MPU) 和内存管理单元 (MMU)，以及可能支持缓存分区和内存带宽管理功能。处理器应具备高可靠性和容错能力，并符合相关功能安全标准。

2）安全 I/0 接口：包括数字输入 / 输出、模拟输入 / 输出等接口，用于连接 ATP、ATO、TCMS、牵引、制动等系统的传感器和执行器。这些接口应具备电气隔离、故障检测和故障安全输出等特性。

3）高速通信接口：如千兆以太网接口，用于与外部控制系统 (如车载 ATP 主机、ATO 控制器) 进行安全通信，并支持冗余通信。

4）安全存储：采用冗余存储或 ECC 内存，用于存储安全关键代码、配置数据和日志信息，确保数据完整性和可靠性。

5）电源管理单元：提供稳定的电源供应，并具备电源监控、欠压 / 过压保护、故障检测等功能。

6）硬件看门狗：独立的硬件看门狗电路，用于监控处理器和软件的运行状态，防止系统死锁或异常。

7）时钟同步单元：支持 PTP 等高精度时间同步协议，确保系统内部和外部设备的时间一致性。

在 2 乘 2 取 2 架构中，两个主控板 (每个主控板内部为 2 取 2 结构) 将并行工作，实现硬件层面的冗余。每个主控板内部的“2 取 2”结构通常由两个独立的 CPU 或处理通道组成，它们执行相同的逻辑并进行交叉比较。当两个主控板都正常工作时，它们会相互验证结果，只有当结果一致时才对外输出。当其中一个主控板发生故障时，另一个主控板可以继续提供服务，从而保证系统的持续运行和高可用性。

4.2 硬件隔离措施

iRIOM 采取以下隔离措施 [9]：

电源域隔离：SIL4 关键电源路径可单独滤波与监测；

背板与信号隔离：SIL4 关键链路不与 SIL2 共享非必要背板通道；

I/O 物理隔离：Vital I/O 与 Non-vital I/O 使用不同板卡或不同隔离区；

调试 / 维护口隔离：SIL4 调试口严控，避免被 SIL2 运维口侧向影响。

为解决“ATP 与驱采之间内部实时总线极高实时性”要求，融合 iRIOM 需提供：

专用 ATP Interface：SIL4 域到 ATP 的接口使用专用通道（点到点），避免与车辆网络共享；

确定性传输机制：硬件支持 DMA、优先级中断、固定周期触发；

资源不可抢占：SIL4 数据路径不受 SIL2 总线占用影响（仲裁优先级、独立链路或隔离带宽）。

4.3 网络隔离措施

本研究采用 交换机转发架构，通过专用 VLAN 对安全数据流进行逻辑隔离，并在交换机上配置优先级队列，保证毫秒级的确定性传输能力。网络规划遵循以下原则 [10]：

安全业务 VLAN 独立：iRIOM 安全以太网口与 ATP 安全以太网口加入专用 VLAN；

优先级队列保障：安全 VLAN 报文设置最高优先级，交换机按严格优先级或至少保证带宽进行转发；

非安全业务限流：对其他 VLAN 的报文进行限速或整形，避免抢占缓存与转发资源；

端到端黑通道 [11]：将交换机与以太网链路视为黑通道，安全由端系统实现的安全层保证。

5 软件架构设计

5.1 软件总体结构

iRIOM 按照以下结构进行分层设计，如图 2 所示：

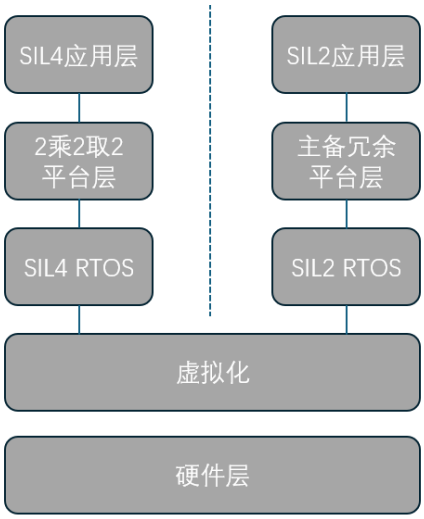

图 2 软件架构图

5.2 虚拟化层

虚拟化层作为软件架构的核心直接运行在多核安全处理器上 [12]，负责以下关键功能：

1）资源虚拟化与管理：将物理 CPU 核心、内存、1/0 设备等资源抽象为虚拟资源，并根据预设策略分配给不同的虚拟机。

2）严格的时间与空间隔离：确保不同虚拟机之间在 CPU 时间、内存空间和 /0 访问上的严格隔离，防止故障或恶意行为从一个虚拟机扩散到另一个虚拟机。

3）虚拟机调度：采用确定性调度算法 [8]，确保 SIL4 级虚拟机能够获得足够的 CPU 时间，并保证其任务的实时性。

4）中断管理：管理所有硬件中断，并将其安全、高效地路由到相应的虚拟机。

5）故障隔离与处理：监控虚拟机的运行状态，当检测到虚拟机内部故障时，能够将其隔离，防止影响其他虚拟机或整个系统。安全通信通道：提供受控的虚拟机间通信机制，如共享内存或消息队列，确保不同安全等级功能之间的数据交换安全可靠。

5.3 操作系统层

在虚拟化层之上，将运行不同类型的实时操作系统 (RTOS)，以满足不同安全等级应用的需求：

1）SIL4 RTOS: 专用于承载 SIL4 级应用 (如 ATPIO 驱采服务)。该 RTOS 必须是经过功能安全认证的，具备高确定性、高可靠性、小内存占用和严格的实时性。它将运行在虚拟化层分配的专用硬实时核心上，并独占分配的内存和 I/0 资源。

2）SIL2 RTOS: 用于承载 SIL2 级应用 (如 ATO、TCMS、牵引、制动 IO 驱采服务)。该 RTOS 可以是更通用的实时操作系统，如 Linux(经过实时补丁优化)、FreeRTOS 等。它将运行在虚拟化层分配的软实时核心上，并共享部分资源，但仍需确保其任务的实时性。通过虚拟化层的隔离，SIL2 RTOS 的故障不会影响 SIL4 RTOS 的运行。

5.4 软件隔离措施

除了虚拟化层提供的硬件隔离，软件层面还将通过以下机制增强隔离和安全性 :

1）内存保护 : 操作系统和应用程序将利用处理器的 MPU/MMU 功能，对各自的代码和数据段进行内存保护，防止越界访问。

2）任务调度隔离 :SIL4 RTOS 和 SIL2 RTOS 将分别管理各自的任务调度，虚拟化层确保不同 RTOS 之间 CPU 时间的隔离。

3）故障安全编程 [3]: 所有安全关键代码将遵循故障安全编程原则，包括防御性编程、错误检测与处理、余计算等。

4）安全通信协议栈 : 在应用程序和操作系统之间，以及虚拟机之间，将实现安全通信协议栈，确保数据传输的完整性、可靠性和时效性。

5）软件看门狗 : 在每个虚拟机内部，都将运行软件看门狗，监控应用程序和 RTOS 的运行状态，并在检测到异常时触发相应的故障处理机制。

6 安全机制设计

6.1 安全对比机制

为确保 iRIOM 不成为薄弱环节，iRIOM 安全域采用如下策略：

1）iRIOM 上行同一份安全输入帧同时送达 ATP 通道 A 与 ATP 通道 B（同 VLAN 高优先级）；

2）ATP 通道 A 与通道 B 分别生成安全输出指令帧（下行）；

3）iRIOM 同时接收两份下行输出指令并执行一致性检查：

指令内容一致

序号一致

周期计数一致

超时窗口一致

4）只有一致才更新 DO AO 输出；不一致或超时则进入安全状态并上报 ATP。

6.2 故障检测与恢复机制

故障检测与恢复流程如图 3 所示。

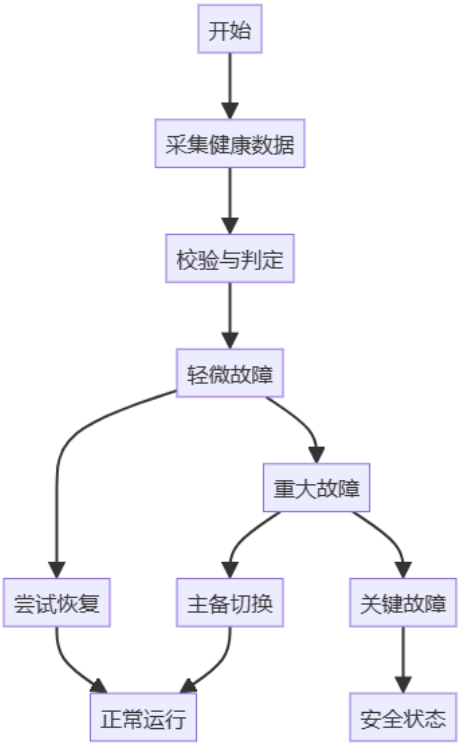

图 3 故障检测与恢复流程图

故障检测覆盖范围包括：

周期心跳与看门狗；

自检（上电 / 周期）；

输入范围与 CRC 校验；

任务执行超时监控；

双通道一致性监测。

故障恢复采用分层策略 [6]，措施如下：

轻微故障（Minor）：任务重启、模块复位、重新同步；

重大故障（Major）：主备切换、降级运行；

关键故障（Critical）：进入安全状态（阻断输出、通知 ATP）。

6.3 iRIOM 与 ATP 安全通信时序

iRIOM 与 ATP 通信时序如图 4 所示：

该时序强调：ATP 请求→双通道采样→比对→返回有效 / 故障。

7 验证与确认方案

7.1 实时性验证

建议采用“预算 + 实测闭环”：

静态预算：按关键路径拆解；

动态测量：用硬件时间戳、逻辑分析仪或内部 trace 记录周期与抖动；

压力测试[1]：将 SIL2 网络负载拉满，验证 SIL4 关键路径不劣化；

故障注入：模拟丢帧、延迟、CPU 过载，验证保护机制生效。

可以采用如表 2 的用例验证各种情况的实时性满足要求。

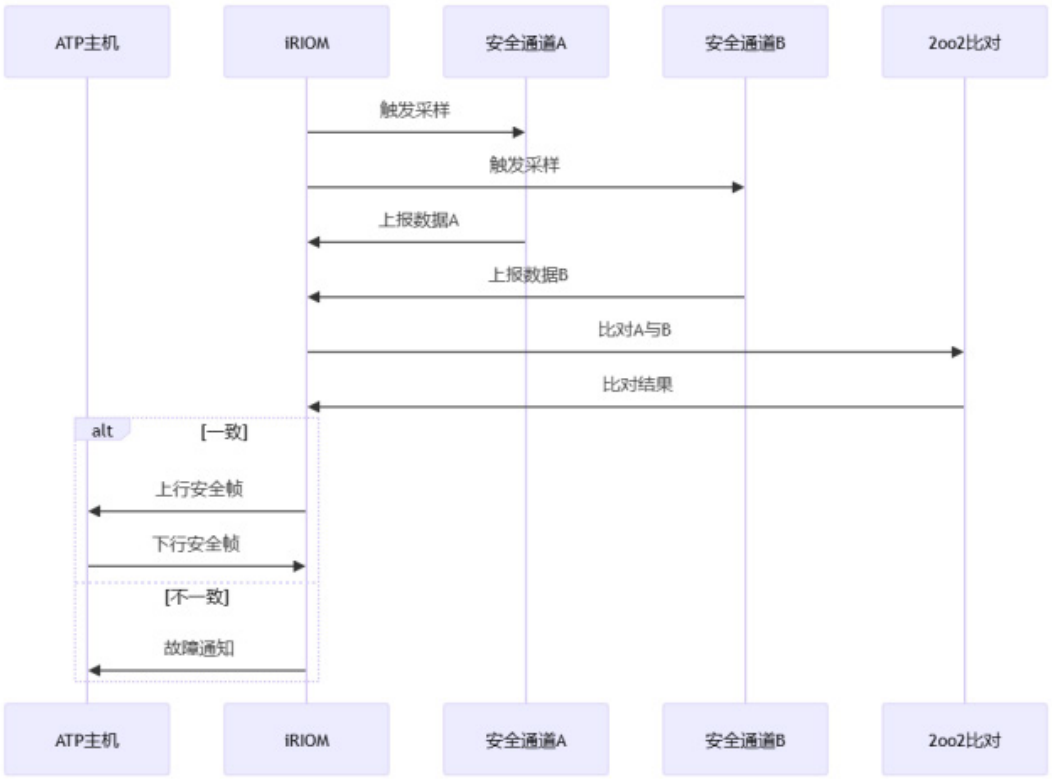

图 4 iRIOM 与 ATP 通信时序图

表 2 实时性验证表

测试用例	SIL4 周期抖动	iRIOM 到 ATP 延迟	ATP 到 iRIOM 延迟	判定
标称	记录	记录	记录	不超预算
非安全满载	记录	记录	记录	安全不退化
大帧阻塞	记录	记录	记录	阻塞不超上界
拥塞注入	记录	记录	记录	超时触发安全
丢包注入	记录	记录	记录	序号机制生效
乱序注入	记录	记录	记录	周期计数生效
延迟注入	记录	记录	记录	超时进入安全
切换测试	记录	记录	记录	切换满足门槛

7.2 容错与冗余验证

为了检验系统的容错能力[8]，建议从以下几方面进行验证：

电源切换测试（Power A/B 断电切换）；

主备处理切换测试（Failover latency）；

I/O 通道异常与 2oo2 不一致触发测试；

安全状态触发后的输出阻断与 ATP 通知验证[9]。

8 结语

本文针对轨道交通车载电子电气系统多安全等级 I/O 融合的工程挑战，提出了一种多安全等级智能 iRIOM 的总体设计方案。该方案旨在打破传统“网络控制驱采”与“信号安全驱采”分立部署的模式，在同一平台内融合 SIL2 网络控制驱采与 SIL4 信号安全驱采能力，从而显著降低设备数量、线缆规模、维护复杂度和生命周期成本。

参考文献

[1] 孙传亮. 青岛地铁一期工程拟采用的行车组织运营方式介绍[C]//降低地铁造价及工程建设管理等若干问题的研究论文集. 北京，2003：368-377.

[2] 魏涛,曹志刚,孙建.基于时间敏感网络的城市轨道交通列车多系统融合控制研究[J].城市轨道交通研究, 2025, 28(11): 1-5.

[3] 梁鸿煜,周小路,苏科.铁路控制和防护系统的工具安全性研究与