

通用轨旁安全计算机平台设计

严文煜 迟宝全

(上海富欣智能交通控制有限公司,201203,上海//第一作者,工程师)

摘 要 介绍了已通过第三方 SIL4 安全等级认证的通用轨旁安全计算机平台的系统架构、安全设计原则,并对其安全性进行了分析。该平台采用 2 乘 2 取 2 安全架构,模块化、通用性、易扩展的硬件,以及跨平台、统一性的软件进行设计。该安全平台已成功应用于基于通信的列车控制系统、列车自主运行系统、有轨电车信号系统等多个工程项目。实践证明,该安全平台完全符合轨道交通产品安全性、可靠性、可维护性、可用性这 4 个关键要素的技术要求。

关键词 地铁; 轨旁安全计算机平台; 2 乘 2 取 2; 安全设计

中图分类号 U231.6
DOI:10.16037/j.1007-869x.2020.10.044

Design of General Trackside Safety Computer Platform for Rail Transit

YAN Wenyu, CHI Baoquan

Abstract The system structure and safety design principle of the general trackside computer safety platform are introduced, which has passed the third-party SIL4 level safety certification. The platform adopts double two out of two safety architecture, and uses modular, universal and scalable hardware, as well as cross platform and unified software for the design. As a result, the safety platform is successfully applied to many projects, such as CBTC (communication based train control), TACS (train autonomous circumambulate system), tram signal system and so on. The practice has proved that the safety platform fully meets the technical requirements of four key elements of rail transit products: safety, reliability, maintainability and applicability.

Key words metro; trackside safety computer platform; double two out of two; safety design

Author's address Shanghai Fuxin Intelligent Transportation Solutions Co., Ltd., 201203, Shanghai, China

近年来,城市轨道交通信号系统在 CBTC(基于通信的列车控制)的基础上迎来了新的发展。一方面,“融合”是总的趋势,比如 TACS(列车自主运行系统)融合了车载控制器、联锁及区域控制器,全电

子执行单元融合了离散 I/O(输入/输出)单元与继电器接口。从这个角度来看,轨旁信号设备变得更简洁了。另一方面,信号制式呈现多样化,比如有轨电车、跨坐式单轨、悬挂式单轨及自动旅客捷运系统等多种信号制式。这一“少”一“多”的变化,以及还要兼容既有的轨旁信号设备,就对设计一个通用的轨旁安全计算机平台提出了更高的要求。

本文所介绍的通用轨旁安全计算机平台,是在满足安全性和可靠性的前提下,主要考虑兼容 CBTC、TACS、多制式信号系统及全电子目标控制器等列控系统,由上海富欣智能交通控制有限公司自主研发的通用轨旁安全计算机平台。

1 通用轨旁安全计算机平台的系统架构

1.1 系统架构

通用轨旁安全计算机平台系统架构如图 1 所示,主要包含如下 5 个功能单元:

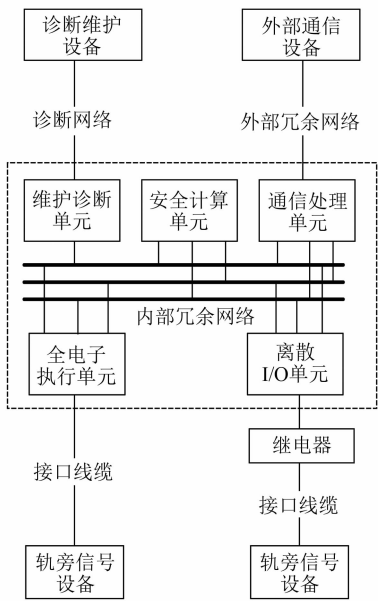


图 1 通用轨旁安全计算机平台系统架构

1) 安全计算单元。安全等级 SIL4,采用 2 乘 2 取 2 冗余安全架构,负责安全逻辑运算及内部通信

等功能。

2) 通信管理单元。安全等级为 SIL4,采用 2 乘 2 取 2 冗余安全架构,实现安全平台的安全协议组包、解析、内部和外部安全通信等功能。

3) 全电子执行单元。安全等级为 SIL4,采用 2 乘 2 取 2 冗余安全架构,由各种全电子执行模块组成,接收来自安全计算单元的控制命令,驱动信号机、转辙机、轨道电路等室外轨旁信号设备并采集信息。

4) 离散 I/O 单元。安全等级为 SIL4,采用 2 乘 2 取 2 冗余安全架构,为第三代计算机联锁的输入输出单元,通过驱动与采集继电器实现对轨旁信号设备的控制与监督。本单元与全电子执行单元并不一起使用,但从安全计算单元的视角来看,两者均为网络拓扑中的一个节点,除了应用逻辑方面的差异,在平台层是一致的。

5) 维护诊断单元。安全等级为 SIL0,实现安全平台的诊断维护与故障日志记录等功能。

1.2 硬件架构特点

1) 所有 SIL4 安全单元均采用 2 乘 2 取 2 的冗余安全架构,硬件设计完全兼容 EN 50129、EN 50124、EN 50121-4 及 EN 50125-3 等铁路标准。

2) 模块化。安全计算单元、安全通信单元、电子执行单元中的通信模块、离散 I/O 单元的通信模块等均复用相同的高性能处理器核心模块,且根据安全等级的不同可裁剪或增加模块数量,配置灵活,降低了认证、开发及维护成本。

3) 易扩展性。基于以太网的通信架构,包括单元间通信以及外部通信,1 000 M/100 M/10 M 自适应,满足不同通信速率的需求,兼容性强易扩展。

4) 通用性。CBTC、TACS、多制式有轨信号系统均使用通用的硬件平台,只是根据不同的需求进行裁剪及配置。

1.3 软件架构特点

1) 跨平台性。通过适配层接口对操作系统进行了封装,屏蔽了不同操作系统(VxWorks、Linux 等嵌入式操作系统)的差异性,按统一的接口与平台软件交互,使安全平台软件易于跨平台移植。

2) 统一性。各安全单元采用完全相同的平台软件架构,每个安全单元均能实现如下通用功能(包括但不限于):初始化上电自检、输入输出管理、系内同步管理、安全表决管理、系间同步切换管理、安全通信管理、在线自检管理、故障管理、诊断维护

管理、周期调度与监控管理、时钟管理、用户接口管理。

3) 具有自主专利的在线自检技术。

4) 2 取 2 的双 CPU 采用任务级同步的方式来实现状态信息与运算的同步。

5) 基于冗余网络通信的可靠双系切换方式,摒弃了传统的继电器切换方式,使双系切换软件化,节省了机柜内有限的物理空间。

2 安全设计原则

2.1 多层次系统化安全设计原则

通用轨旁安全计算机平台可抽象为如图 2 所示的安全组件。



图 2 安全组件分层设计结构

安全平台本身所包含的组件,如硬件、固件、BSP、操作系统、协议栈(比如网络协议栈)、核心处理层软件以及应用软件等均必须通过安全认证。同时影响安全软件开发的 EN 50128 定义的 T2 类与 T3 类工具也要通过安全认证,如编译器。

2.2 独立性原则

独立性原则在设计中主要有物理独立性、环境独立性及软件功能独立性三种实现方式。

1) 物理独立性。在硬件设计上主要依靠电气隔离来实现,包括而但不限于以下功能模块之间按 EN 50124-1 的要求定义隔离电压:①安全功能模块与非安全功能模块之间;② 2 取 2 的不同通道之间;③不同的通信接口之间;④强电与板内电路之间;⑤机壳地与板内电路之间。

2) 环境独立性。即减小环境干扰因素对安全功能的影响,比如静电干扰、电磁辐射干扰、浪涌干扰、温度变化等外部因素将引起的功能的独立性降低。在硬件设计上可通过添加合理的端口 EMC(电磁兼容)防护电路、提高产品的电磁屏蔽、采用宽温器件等方式来提高环境独立性。

3) 软件功能独立性。主要指软件安全功能与

非安全功能的隔离。比如,安全功能模块不调用非安全功能模块的函数,非安全功能模块与安全功能模块通过消息队列来进行交互,等等。

2.3 故障-安全原则

该通用轨旁安全计算机平台包含了 EN 50129 所定义的组合故障安全、反应故障安全及固有故障安全等 3 种应对单点硬件随机故障的实现方式,从而使系统在故障时导向安全侧。

两个通道的 CPU 分别通过本地总线与安全输入板和安全输出板实现数据读写;两个 CPU 之间通过千兆以太网实现任务级同步、数据交互和安全表决,每个周期两个 CPU 也会分别执行在线自检,并根据安全表决和自检结果把动态生命信号发送给安全电源板;一旦发生表决失败或者自检故障,安全电源板会立即切断安全输出板的输出电源,从而实现故障导向安全。以上的操作包含了组合故障安全与反应故障安全,其中的安全电源板具有固有故障安全的属性。

2.4 实时故障检测原则

实时故障检测也称为在线自检,其目的是及时发现硬件随机失效。硬件在线自检主要分为两类:一类是电源、时钟、温度、输入输出状态等功能单一的在线自检,这部分自检较为简单,在这里不做详述;另一类是以 CPU 为核心的最小系统组成的复杂系统的在线自检,由于单个芯片往往包含千万级或亿级的门电路,所以大大增加了充分自检的复杂性。

以通用安全计算机平台常见的 PowerPC 主控板为例来说明 VxWorks 操作系统从上电启动到进入多任务运行过程所涉及的硬件模块。非 ROM (只读存储器)驻留型的 VxWorks 的启动主要包含以下 3 个阶段:

第 1 阶段,上电复位初始化。上电复位后,CPU 读取配置字并跳转到 Flash 中初始化函数的入口地址,开始初始化地址映射、内存控制器、局部总线控制器等系统运行所需的基本配置。此时,代码(该代码为汇编代码)在 Flash 中运行。接着初始化函数调用所需要的栈,为 C 语言程序的运行做准备。由于 Flash 访问的慢速,因而接下来需把 Flash 中的程序段与数据段复制到 DDR SDRAM 中运行,以匹配高速 CPU。此阶段 Cache 处于禁用状态,指令单元通过 CPU 前端总线及局部总线从 Flash 中读取指令后并译码,有些指令还需通过装载存储单元从

Flash 读取数据并装载到寄存器单元以供运算单元执行。指令执行完成后,由装载存储单元把结果回写入寄存器单元并释放该指令所占用的流水线资源。

第 2 阶段,操作系统预内核的初始化。操作系统镜像复制到 DDR SDRAM(双倍速率同步动态随机存储器)后,开始操作系统预内核的初始化,包括清 BSS(未初始化数据区)、初始化中断向量表、初始化目标板硬件、配置 Cache、配置操作系统内核、启动操作系统内核。

第 3 阶段,操作系统内核启动后,开始初始化内存池、初始化 I/O 系统、初始化 MMU(存储管理单元)、配置时钟系统、安装设备驱动等,最后进入多任务的应用程序,至此启动过程结束。其中,VxWorks 对 MMU 的使用较为特殊,由于 VxWorks 中虚拟地址与物理地址相同,所以 MMU 的主要功能是对页面的缓存控制与访问权限控制,而非虚拟地址与物理地址的转换。

CPU 最小系统主要涉及的硬件模块如图 3 所示。在线自检应周期性地对这些模块进行检测。

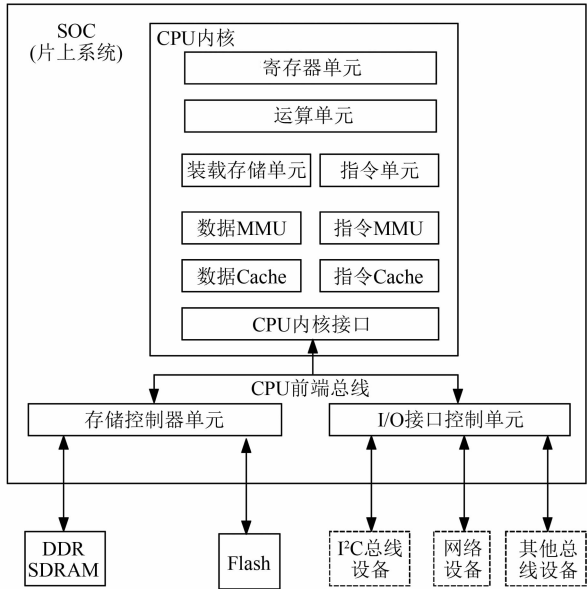


图 3 CPU 最小系统在线自检

另外,对与安全相关的通信单元,主要通过安全通信协议和组合故障安全来保证其通信安全,而不再对其硬件模块进行周期性自检。

2.5 冗余回检原则

冗余回检即对同一状态由双通道冗余回采并表决,减小因单通道回检失效而漏检,在安全平台中对继电器前后节点的回采、输入输出通道的回采

等均采用冗余回检的方式。

2.6 差异化设计原则

1) 硬件设计的差异化。比如输入采集双通道的硬件设计差异化。

2) 物理空间的差异化。比如双 CPU 的物理布局的差异化设计。

3) 处理时间的差异化。比如双通道分时处理同一输入。

4) 对同一信息编码的差异化。比如安全输入采集,双通道用不同的满足码距要求的 32 位编码表示同一个输入“1”。

5) 触发方式的差异化。比如通道 1 采用中断的方式来触发故障报警,而通道 2 采用差异化的信号量触发方式。

3 安全性分析

一个典型的通用轨旁安全计算机平台输出单元的安全架构如图 4 所示,通过对此安全架构分析来论证上述安全原则的理论依据。输出单元的每个通道的 CPU 从 RAM(随机存取存储器)中读取数据与指令,并通过同步接口进行输出表决,当 R1 CPU 与 R2 CPU 表决一致时,发出输出命令。其中, RAM、CPU、输出电路均有在线自检功能,自检失败会通过动态安全电源断开输出电源,所以该单元符合 1oo2D 安全模型。该安全模型需考虑共因失效、非共因失效、在线自检及同步表决对安全计算的影响。轨旁安全计算机平台属于连续操作模式,应使用 P_{FH} (每小时危险失效概率)来进行安全计算。

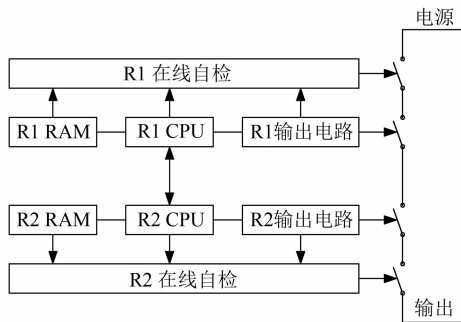


图 4 输出单元的安全架构

由于 P_{FH} 的计算只考虑危险失效的情况,综合考虑共因失效与在线自检的因素,可把危险失效分为以下 4 种:① DDC——被检测到的共因失效引起的危险失效;② DDN——被检测到的非共因失效引起的危险失效;③ DUC——未被检测到的共因失效

引起的危险失效;④ DUN——未被检测到的非共因失效引起的危险失效。

对符合 1oo2D 安全模型的单元只需考虑 DUC 与 DUN 两种情况。

1) 计算 RAM 的每小时危险失效概率 $P_{FH, RAM}$ 。 $P_{FH, RAM}$ 包含两部分值:一部分为共因失效未检测到的危险失效,另一部分为非共因失效未检测到的危险失效。考虑在 $[t, t+dt]$ 区间内,共因失效未检测到的危险失效概率为 $P_{FH, RAM, DUC}$,非共因失效未检测到的危险失效概率为 $P_{FH, RAM, DUN}$,则:

$$P_{FH, RAM} = P_{FH, RAM, DUC} + P_{FH, RAM, DUN} = \frac{1}{T} \int_0^T \beta_1 (1 - P_{DC, 1D}) \lambda_{1D} dt + \frac{1}{T} \int_0^T \int_0^T (1 - \beta_1)^2 (1 - P_{DC, 1D})^2 \lambda_{1D}^2 dt dt = \beta_1 (1 - P_{DC, 1D}) \lambda_{1D} + (1 - \beta_1)^2 (1 - P_{DC, 1D})^2 \lambda_{1D}^2 T \quad (1)$$

式中:

β_1 ——共同原因的未被检测到的失效分数值;

$P_{DC, 1D}$ ——RAM 危险失效诊断覆盖率, %;

λ_{1D} ——RAM 危险失效率, h^{-1} ;

T ——系统的生命周期, h。

2) 计算 CPU 的每小时危险失效概率 $P_{FH, CPU}$ 。CPU 的安全计算还要考虑同步安全表决的影响。

$$P_{FH, CPU} = \beta_2 (1 - P_{DC, 2D}) \lambda_{2D} + (1 - \beta_2)^2 (1 - P_{DC, 2D})^2 (1 - P_{DC, VOTE})^2 \lambda_{2D}^2 T \quad (2)$$

式中:

β_2 ——共同原因的未被检测到的失效分数值;

$P_{DC, 2D}$ ——CPU 危险失效诊断覆盖率, %;

$P_{DC, VOTE}$ ——R1 与 R2 CPU 表决的诊断覆盖率, %;

λ_{2D} ——CPU 危险失效率, h^{-1} 。

3) 计算输出电路的每小时危险失效概率 $P_{FH, OUT}$ 。

$$P_{FH, OUT} = \beta_3 (1 - P_{DC, 3D}) \lambda_{3D} + (1 - \beta_3)^2 (1 - P_{DC, 3D})^2 \lambda_{3D}^2 T \quad (3)$$

式中:

β_3 ——共同原因的未被检测到的失效分数值;

$P_{DC, 3D}$ ——输出电路危险失效诊断覆盖率, %;

λ_{3D} ——输出电路危险失效率, h^{-1} 。

则系统的每小时失效概率 $P_{FH, SYS}$ 为:

$$P_{FH, SYS} = P_{FH, RAM} + P_{FH, CPU} + P_{FH, OUT} \quad (4)$$

从式(1)~(4)可推出,要降低 P_{FH} 的值以满足 EN 50129 所定义的 SIL4 安全等级 T_{FFR} 小于 $10^{-8} h^{-1}$ 的要求,可通过以下几种方式来实现:

1) 减小 β 值(独立性原则、差异化设计原则)。在公式中既有 β 项也有 $(1-\beta)$ 项, β 项代表 DUC 项, $(1-\beta)$ 项代表 DUN 项。以式(1)中的 $P_{FH,RAM,DUN}$ 项为例,由于 $(1-P_{DC,ID})$ 与 λ_{ID} 均为平方项,且 λ_{ID} 为 10^{-6} 等级,而考虑安全数据在 RAM 中受到 16 位冗余编码保护,则 $(1-P_{DC,ID})$ 为 2^{-16} 等级,所以对于 DUN 项, β_i 越小, $(1-\beta_i)$ 的影响权重越小,该项主要影响因子为 $P_{DC,ID}$ 与 λ_{ID} 。

2) 减小 λ_D 值(独立性原则,固有故障安全)。

3) 增加 P_{DC} 值(组合故障安全原则,实时故障检测原则,冗余回检原则)。

4) 降低每个安全子系统的 P_{FH} 值(多层次系统化安全设计原则)。

4 不同安全架构的安全性比较

通用轨旁安全计算机平台主流的安全架构有 2 乘 2 取 2 与 3 取 2 两种,两者各有优劣。本文仅从 P_{FH} 值的角度来比较两种架构的安全性。

3 取 2 的工作原理是在 A、B、C 3 个通道表决中,只要有 2 个表决一致就可输出,即能容忍 1 个危险失效。所以 3 取 2 系统要产生危险失效输出需考虑以下两种情况:

1) 3 个通道中其中 2 个通道发生未被检测到的共因失效引起的危险失效,有 A 与 B、A 与 C、B 与 C 3 种组合。

2) 3 个通道中其中 2 个通道发生未被检测到的非共因失效引起的危险失效,有 A 与 B、A 与 C、B 与 C 3 种组合。

为了方便比较估算,采用封装了 β 、 P_{DC} 、 λ_D 的 λ_{DUC} 与 λ_{DUN} 来进行分析推导。

$$P_{FH,2oo3} = 3\lambda_{DUC} + 3\lambda_{DUN}^2 T \quad (5)$$

$$P_{FH,1oo2D} = \lambda_{DUC} + \lambda_{DUN}^2 T \quad (6)$$

式中:

λ_{DUC} ——2 个通道未被检测到的共因失效引起的危险失效率, h^{-1} ;

λ_{DUN} ——2 个通道未被检测到的非共因失效引起的危险失效率, h^{-1} 。

比较式(5)与式(6)可知,3 取 2 架构的 P_{FH} 值约为 2 取 2 架构的 3 倍,所以从安全性的角度来看,2 取 2 架构是更优的选择。

5 结语

本文对通用轨旁安全计算机平台的系统架构及软硬件设计思想进行了介绍。目前,该安全平台已获得了德国莱茵 TUV 的 SIL4 安全认证证书,并且已成功应用于上海浦东国际机场捷运线项目的联锁和区域控制子系统,苏州、武汉等城市有轨电车项目的道岔控制子系统,青岛 TACS 国家示范工程项目的目标控制子系统等项目。实践证明,该安全平台符合安全性、可靠性、可维护性、可用性这 4 个轨道交通产品关键要素的技术要求,并且兼容多种信号系统,具有通用性的属性。该通用轨旁安全计算机平台可推广应用到市域、城际铁路等项目中。

参考文献

- [1] The British Standards Institution. Railway applications-Communication, signalling and processing systems-Safety related electronic systems for signalling; EN 50129—2018 [S]. British: BSI, 2018: 76.
- [2] IEC. Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3; IEC 61508-6—2010 [S]. Geneva: IEC, 2010: 27.
- [3] 陈光武. 轨道交通安全计算机系统及安全控制机制关键技术研究[D]. 兰州: 兰州交通大学, 2014.
- [4] 姜坚华. 1oo2 模型分析及其在地铁列车自动防护系统中的应用[J]. 城市轨道交通研究, 2011(6): 25.

(收稿日期: 2020-06-02)

欢迎访问《城市轨道交通研究》网站

www.umat1998.com