doi: 10.3969/j.issn.1672-6073.2023.02.025

# 基于 ARINC659 总线的互联互通 ZC 安全通信计算机平台的设计

魏东冬，郑长宗，许　镇
（中国铁道科学研究院，北京 100081）

**摘　要：**为了更好地满足城市轨道交通互联互通对信号领域安全通信的要求，将具有数据吞吐量大、传输时间确定、故障隔离严格、容错性好等特点的 ARINC659 总线用于城市轨道交通信号控制系统领域。提出了一种基于 ARINC659 总线技术的二乘二取二安全通信计算机平台的方案，用以实现 ZC 平台的对外通信功能和安全通信协议运算功能。设计其软硬件结构、用户软件和总线间线程的通信序列，并对数据的冗余处理和安全协议运算等关键功能进行研究，以满足系统高安全性、高可靠性和高实时性通信的需求。

**关键词：**轨道交通；ARINC659；区域控制器；互联互通；安全通信计算机平台；二乘二取二
**中图分类号：**U231　　**文献标志码：**A　　**文章编号：**1672-6073(2023)02-0198-06

# Design of Interconnection ZC Safety Communications Computer Platform Based on the ARINC659 Bus

**WEI Dongdong, ZHENG Changzong, XU Zhen**
(China Academy of Railway Sciences, Beijing 100081)

**Abstract:** To better meet the demands of urban rail transit interconnection on safety communications in the signal field, the ARINC659 bus is used in urban rail transit signal control systems. The advantages of the bus technology include large data throughput, definite transmission time, strict fault isolation, and high fault tolerance. In this study, a scheme of a double 2-vote-2 safety communication computer platform based on the ARINC659 bus technology is proposed to realize the external communication and safety communication protocol operation functions of the ZC platform. By appropriately designing the software and hardware structures, communication sequence of user software and threads between buses, as well as the research of key functions, including data redundancy processing and safety protocol operation, the system can meet the requirements of high safety, reliability, and real-time communication.

**Keywords:** rail transit; ARINC659; zone controller; interconnection; safety communications computer platform; double 2-vote-2

## 1　研究背景

随着城市轨道交通互联互通的发展，资源共享程度越来越高，系统的安全性、实时性也面临着更加严峻的挑战。同时，在区域控制器(zone controller，ZC)这种安全苛求系统中，实现安全、可靠、有效、通用的数据传输是关键之一。按照 EN50159 标准对安全相关控制系统采用分层模式的方案，将安全功能模块和

收稿日期：2022-03-21　修回日期：2022-09-20
第一作者：魏东冬，男，硕士，助理研究员，从事铁路通信信号方面的研究，weidongdong1111@foxmail.com
基金项目：中国铁道科学研究院集团有限公司科研专项(J2021G006)
引用格式：魏东冬，郑长宗，许镇. 基于 ARINC659 总线的互联互通 ZC 安全通信计算机平台的设计[J]. 都市快轨交通，2023，36(2)：198–203.
WEI Dongdong, ZHENG Changzong, XU Zhen. Design of interconnection ZC safety communications computer platform based on the ARINC659 bus[J]. Urban rapid rail transit, 2023, 36(2): 198–203.

通信功能模块独立出来，交由专门的安全苛求通信设备以达到分担逻辑运算压力、提升整体系统的性能、优化软件结构和便于研发人员的开发和维护的目的。

ARINC659 总线源于由 Honeywell 公司率先提出并负责制定的 SAFEBus 总线，其于 1993 年被美国航空电子工程师协会(AEEC)所采纳[1-2]，作为航空业标准发布，并首先应用于波音 777 客机中安全性等级要求为 A 级(系统失效率小于 10-9 次/飞行小时)的航空电子设备中。ARINC659 总线是一种半双工串行数据通信总线，在基于时间触发架构的基础上，通过四余度容错配置实现冗余线性多点拓扑结构[3]，其通信速率为 60 Mbps，具有无主运行模式、各节点完全平等以及鲁棒的分时分区等特性。将其用于城市轨道交通领域，作为安全苛求通信系统的通信总线，可满足系统高安全性、高可靠性、高实时性通信的需求[4-5]。

## 2 系统结构设计

### 2.1 系统的定义与边界

在区域控制器中，系统的通信接口功能以及安全通信协议运算功能由安全通信计算机子系统来实现，如图 1 所示。

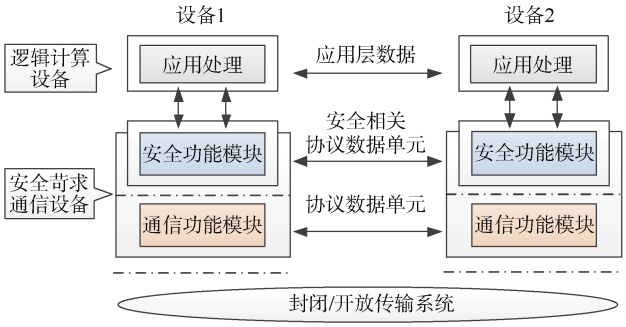


图 1 采用安全通信计算机平台的安全通信系统的总体结构

Figure 1 The structure of the safety communications system using the safety communications computer platform

系统功能如下：

1) 提供二乘二取二的安全通信平台；

2) 实现区域控制器对外部其他信号系统的通信接口功能，通信的物理层采用以太网接口，传输层支持 TCP 和 UDP 协议；

3) 完成区域控制器与其他信号系统之间传输数据的安全协议运算和处理功能，安全层支持 RSSP-I 协议和 RSSP-II 协议；

4) 对于其他信号系统数据发送的上行数据，对其进行安全通信协议校验后发送给上层逻辑安全计算机；对于逻辑安全计算机要发送给外部其他信号系统的下行数据，在经过安全通信协议封装后将其发送到目标设备；

5) 将整个系统的周期状态、报警日志等维护信息发送给维护终端。

### 2.2 背板总线结构设计

ARINC659 总线是半双工、四余度容错配置的串行数据总线，分为 A、B 两对总线，每对总线含有 x 和 y 两套总线[6-7]，共有 Ax、Ay、Bx、By 四余度总线进行信息传输，每套总线含有一个独立的时钟线(Ck)和两条数据线(D0、D1)[8]，同时传输数据或发送同步脉冲，因此完全的总线包含 12 条信号线，形成(AxAy)，(BxBy)，(AxBy)，(BxAy)4 个总线比较对，保证了两者比较的独立性，如图 2 所示。

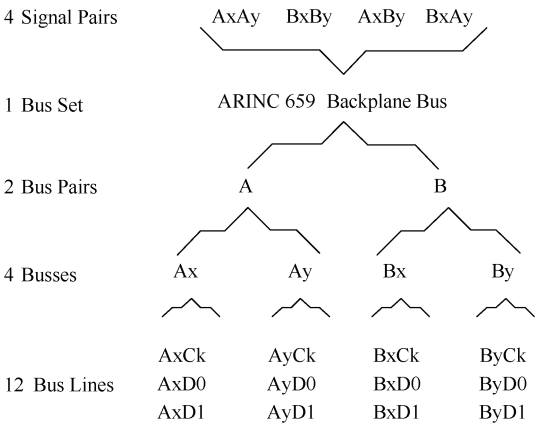


图 2 ARINC659 总线余度配置关系

Figure 2 Redundancy configuration relationship of the ARINC659 Bus

为了最大限度地降低单点故障对整个总线传输的影响，特别是为了防止总线接口单元(BIU)的异常导致总线上其他节点的工作异常，从而将故障扩展到整个总线，一个总线节点的 BIU 控制模块都包含了两个完全独立的 BIU 控制器(BIUx 和 BIUy)。BIUx 和 BIUy 各自拥有独立的晶振、电源等外围辅助电路，两个 BIU 在完成自身工作的同时，还会监控对方的工作状态，若发现对方 BIU 工作异常，则会立即切断对方对总线的输出使能[6]。因此两个 BIU 通过互相监控的二取二工作模式，严格地封锁了背板和背板上各个总线节点的故障边界，保证了背板上的单节点故障不会继续蔓延。较之传统二乘二取二平台内存比较的方式可能发生内存跳变等失效，ARINC659 总线对故障边界的封锁以及出现多总线同一时刻传输相同错误的极小的概率等优势，能够很好地提高比较判决部分的可靠性。

### 2.3 可靠性结构设计

1) 为实现系统结构的可靠性，系统设计采用双机热备结构，其中：

USC 由双系组成。每一系的组成为 1 个 659 总线母板及安装在母板上的板卡。板卡包括：1 个安全计算单元(safety compute unit，SCU)板及其后插板(SCU-EX，无源)，2 个多路总线接口板(multi bus interface，MBI)及其后插板(MBI-EX，无源)，1 个电源板(PS)。

SCU 是安全功能板卡，是双 CPU 板，CPU-X 与 CPU-Y 提供同步运算功能，SCU 板上的两个 BIU 与 659 总线提供输入输出比较功能，二者协同完成二取二的表决系统功能。系统的安全层及其之上的应用层功能都由 SCU 实现。

MBI 是非安全功能板卡，是单 CPU 板，板卡提供 ETH 接口功能。系统 ETH 接口的传输层与物理层由 MBI 实现，MBI 的功能故障不产生安全风险，安全防护功能由 SCU 提供。

SCU-EX 是 SCU 板后插板，为无源板卡，提供通过跳线区分 USC 的 A/B 系的功能。

MBI-EX 是 MBI 板后插板，为无源板卡，为 MBI 板的 ETH 接口功能提供 RJ45 接口。

2) 安全通信计算机的 A 系和 DCS-1 网相连，B 系和 DCS-2 网相连。

3) 为实现两系的工作状态同步，两系间设计有传输状态数据等同步数据的通道。

4) 双系之间相互独立工作，故障系的器件更换应不影响另一系的正常使用。

5) 系统整体硬件结构如图 3 所示。

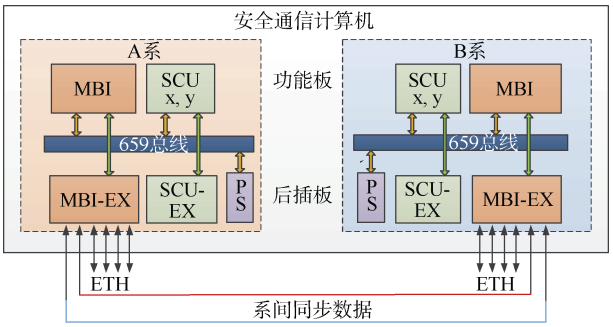


图 3 系统硬件结构

Figure 3 Hardware structure of the system

### 2.4 安全性结构设计

为实现系统安全性，系统单系采用二取二的同步运算表决结构。设计采用基于 ARINC659 总线的双 CPU 结构 SCU 板实现同步运算功能，采用 659 总线与 BIU 单元实现总线比较表决功能。其中，BIU 单元由 BIU 控制器、总线收发器、晶振和带电可擦可编程只读存储器(electrically erasable programmable read only memory，EEPROM)组成，每个 BIU 控制两路总线发送，每个 BIU 接收 4 路总线数据，每个 BIU 控制对方的发送使能，每个 BIU 有独立的晶振和 EEPROM。

SCU 板的 CPU-X 支路与 CPU-Y 支路各自进行周期性的独立运算，在运算的输入输出等关键步骤进行时序同步。BIU 单元协同 659 总线对 SCU 两个支路同步输出的数据按窗口长度进行逐位比较，以保证结果的一致性与正确性。对于比较结果一致的数据，可以正常输出；对于比较不一致的数据则导向安全侧，即无法通过 659 总线对外发送。系统单系设备的二取二结构示意图如图 4 所示。

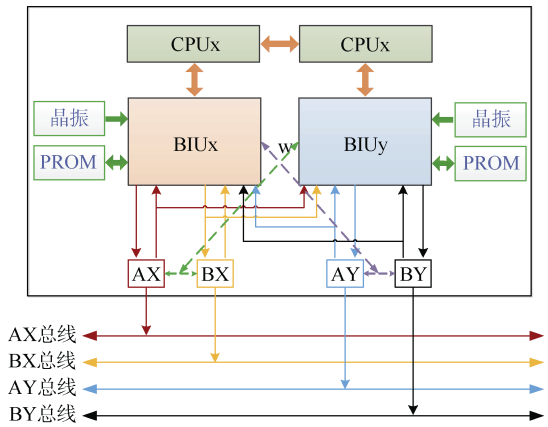


图 4 二取二结构

Figure 4 Structure of 2-vote-2

## 3 软件功能设计

### 3.1 软件层次划分

安全通信计算机的软件基于实时操作系统的多线程运行方式，将其自下而上划分为如图 5 所示的 3 个层次：用户层、传输层和总线层。

1) 用户层(user layer，UsL)。在该层中，SCU 板作为主板卡，主要负责应用数据逻辑处理功能和安全通信协议运算功能，为安全相关功能，安全完整性等级为 SIL4 级；MBI 板作为从板卡，主要负责数据的交叉处理和通信接口功能，为非安全相关功能，安全完整性为 SIL0 级。

2) 传输层(transport layer，TsL)。该层提供用户层

与 659 总线之间传输数据的分片组片功能、传输接口的适配管理功能以及应用层之间的异步通信处理功能；

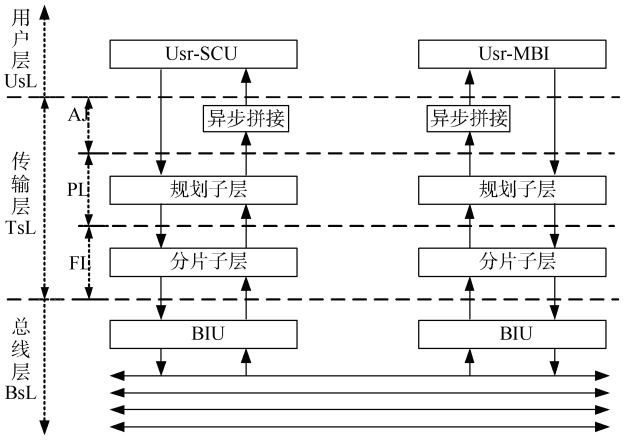


图 5　软件层次划分

Figure 5　Software hierarchy

传输层由分片子层、规划子层和异步拼接 3 部分组成。①分片子层(fragment sub layer，FL)。因总线传输数据大小有限，分片子层把用户层发送到 659 总线的数据进行分片组片操作，同时对传输数据进行相应的防护和校验。②规划子层(plan sub layer，PL)。该层用于查询传输数据所对应的目标板卡地址。用户层收发送信息时，只需提供接口编号，规划子层就能查找到对应的目标板卡地址，进行数据收发。③异步拼接(asynchronous joint，AJ)。因不同板卡之间的运行周期设计有差异，SCU 板设计采用 100 ms 周期，MBI 设计采用无周期循环，需处理板卡间不同的发送/接收周期的异步问题。该层可把多次发送一次接收的数据依据接口信息组合起来，在用户取数据时一次提交给用户层。

用户层发送数据时，调用传输层中的规划子层功能，适配发送数据的接口和目标板卡地址，然后通过传输层中分片子层对传输数据进行分片操作，并将分片数据发送到 ARINC659 总线接口单元 BIU 上并传输到目标板卡；对于接收方，分片子层从 BIU 中取得数据后将分片信息接收到队列中，由单独的线程组片，组片完毕后交由规划子层找到应用程序目标接口并存储起来，最后通过异步拼接功能将多次收到并存储的发送方数据一次性发送给应用层。

3) 总线层(bus layer，BsL)。该层实现单系内板卡间的数据在 659 总线上周期性传输的功能和数据的二取二比较功能，由 659 总线驱动和 BIU 单元的软件协同实现。

## 3.2　线程间的通信序列

如上所述，为实现不同层次之间的协作，设计了多任务(即线程)模式。用户任务(后面以周期 100 ms 为例进行描述)、组片任务(周期 20 ms)、收发任务(周期 10 ms)。其中，用户任务用于实现用户层的逻辑功能。用户发送数据时，调用了传输层的规划子层功能、分片子层功能，将发送数据分成片，存入对应的发送队列中；用户接收数据时，从组片任务提取组好的分片数据。收发任务用于实现发送分片信息到总线上，以及从总线接收分片信息。任务之间的通信序列如图 6 所示。

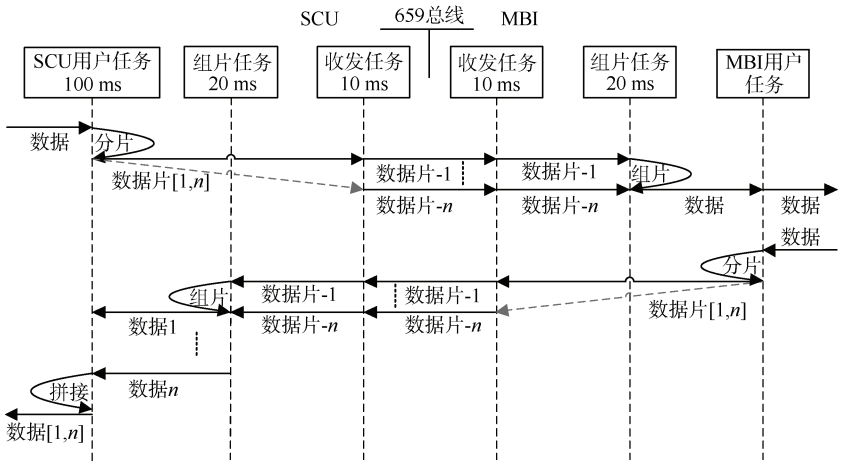


图 6　任务间的通信序列

Figure 6　Communications sequences between tasks

### 3.3 数据冗余处理功能

ZC 平台内部连接方式如图 7 所示。自上而下，上层逻辑安全计算机实现对应用数据的逻辑处理，下层安全通信计算机则负责完成对输入输出数据的安全协议运算功能，以及对外部设备的通信接口功能。正常工作时，安全通信计算机跟随上层逻辑安全计算机的状态，一系作为主系，对外输出运算结果，另一系作为备系，不对外输出运算结果，仅透明传输主系数据；主系自身软硬件故障时转为离线并停止对外输出，由备系升为主系对外输出。

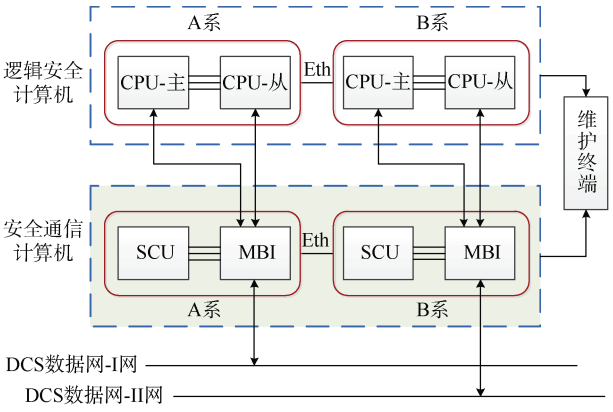


图 7 互联互通 ZC 平台内部结构

Figure 7 Internal structure of the interoperability zone controller

DCS 系统仅提供 I 网和 II 网两路数据分别同安全通信计算机的 A 系和 B 系相连，为了在 ZC 平台内部实现双网数据的安全冗余、避免不必要的倒机，以及降低系统布线的复杂性和逻辑安全计算机软件处理的难度，设计数据的安全冗余在安全通信计算机内部通过软件逻辑来实现。

对于上行数据，安全通信计算机的双系在收到对应的 DCS 数据网的数据后，将数据透明传输给另一系，使得任一系均可收到 DCS 双网冗余数据。对于下行数据，主控系将要发送给其他信号系统的发送数据复制一份给另一系，另一系透明传输主控系数据，保证对外输出的一致性。数据流如图 8 所示。

通过上述处理方式，当安全通信计算机的任一系与该系连接的 DCS 网连接中断时，仍可通过另一系的交叉接收和发送保持与 DSC 另一网的连接，不会因主系与 DCS 网通信中断而倒机，能够有效减少倒机的次数，提高整个系统的可靠性。

### 3.4 安全通信功能

对于适用于互联互通的安全通信计算机而言，为了

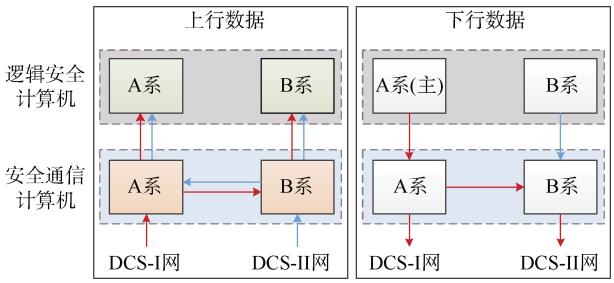


图 8 ZC 数据流

Figure 8 Data flow of ZC

应对复杂的通信环境，设计使用 RSSP-I 和 RSSP-II 两种安全协议来抵御传输过程中可能存在的各种干扰和威胁，其中，对使用 UDP 通信协议的数据采用 RSSP-I 安全协议进行防护，对使用 TCP 通信协议的数据采用 RSSP-II 安全协议进行防护。

RSSP-I 安全协议定义了 3 种报文，分别是用以正常通信的实时安全数据(RSD 报文)，用以时序校正的时序校正请求(SSE 报文)和时序校正答复(SSR 报文)[9-10]。安全通信计算机在收到数据包后，先校验报文头中的源地址、报文尾部的 CRC 值以及报文长度，然后判断报文类型。若是 RSD 报文，则继续校验序列号和安全校验码；若是 SSE 报文，则回复 SSR 报文；若是 SSR 报文，且是本方发起的时序校正请求，则校验 SSR 时间有效性和序列号，通过则进行时序校正并等待接收 RSD 报文，未通过则继续发出 SSE 报文。若本方未发起请求，则丢弃报文。

RSSP-II 安全协议，安全通信计算机设定消息鉴定安全层(MASL)对数据进行消息验证码(MAC)加密防护，安全应用中间子层(SAI)对数据进行重复、删除、重排序和延时防护，设定适配及冗余管理层(ALE)，实现消息鉴定安全层和通信层之间的适配和冗余处理[11-12]。安全通信计算机在接收到数据包后，先校验 MASL 帧头和 MAC 值的正确性，再检查 SAI 帧头中的消息类型，若为时钟偏移更新消息则进行相应更新，若为应用消息，则交由 SAI 层进行时间有效性校验和序列号校验，对于校验通过的数据，交由应用层处理，校验未通过的数据则依据错误处理规则进行处理。

## 4 结语

本文为满足城市轨道交通互联互通更高安全性、更高可靠性和更高实时性的要求，将 ARINC659 总线用于城市轨道交通领域，设计了一种基于 ARINC659

总线的适用于互联互通的区域控制器安全通信计算机，主要介绍了其系统结构和软件功能的设计、在 ZC 平台内实现数据冗余的方式，以及关键的安全协议运算功能。该安全通信计算机已通过必维质量技术服务(上海)有限公司的 SIL4 级安全认证，证书编号 X95P2200401。

## 参考文献


[1] 李育，安刚，李欣. ARINC659 总线多余度容错系统同步技术[J]. 航空科学技术, 2016, 27(12): 28-33.
LI Yu, AN Gang, LI Xin. ARINC659 bus redundancy fault-tolerant system sync technology[J]. Aeronautical science & technology, 2016, 27(12): 28-33.

[2] 郭亮，李玲，田泽，等. ARINC 659 总线接口芯片的 FPGA 原型验证[J]. 计算机技术与发展, 2009, 19(12): 240-242.
GUO Liang, LI Ling, TIAN Ze, et al. FPGA prototype verification of ARINC 659 bus interface chip[J]. Computer technology and development, 2009, 19(12): 240-242.

[3] 张喜民，魏婷. ARINC 659 背板数据总线应用研究[J]. 航空计算技术, 2011, 41(5): 105-109.
ZHANG Ximin, WEI Ting. Application of ARINC 659 backplane data bus[J]. Aeronautical computing technique, 2011, 41(5): 105-109.

[4] 许宏杰，田泽，郭亮，等. ARINC659 芯片设计与实现关键技术研究[J]. 计算机技术与发展, 2014, 24(3): 26-30.
XU Hongjie, TIAN Ze, GUO Liang, et al. Key technology research of ARINC659 chip design and implementation[J]. Computer technology and development, 2014, 24(3): 26-30.

[5] 胡志云. 基于 ARINC659 总线通信系统的研究与设计[D]. 西安：西安工程大学, 2016.
HU Zhiyun. The research and design of communication system based on ARINC659 bus[D]. Xi'an: Xi'an Polytechnic University, 2016.

[6] 苏罗辉，牛萌，刘坤. 时间触发系统体系结构研究[J]. 计算机工程与设计, 2014, 35(6): 1956-1961.
SU Luohui, NIU Meng, LIU Kun. Study on time-triggered system architecture[J]. Computer engineering and design, 2014, 35(6): 1956-1961.

[7] 王宇飞，邹小东，张明. 基于 FPGA 的 ARINC659 总线同步机制的研究与实现[J]. 电子测量技术, 2016, 39(1): 110-113.
WANG Yufei, ZOU Xiaodong, ZHANG Ming. Research and implementation of the synchronization mechanism of ARINC659 BUS based on FPGA[J]. Electronic measurement technology, 2016, 39(1): 110-113.

[8] 张锐，吴成富，段晓军. ARINC659 总线在飞控余度管理技术中的应用[J]. 航空计算技术, 2013, 43(2): 128-130.
ZHANG Rui, WU Chengfu, DUAN Xiaojun. Application of ARINC659 bus in flight control redundancy management[J]. Aeronautical computing technique, 2013, 43(2): 128-130.

[9] 刘鹏，徐德龙，逄增文. 客运专线计算机联锁系统安全环网的应用[J]. 铁道通信信号, 2015, 51(1): 60-63.
LIU Peng, Xu Denglong, PANG Zengwen. Application for computer interlocking safety ring net[J]. Railway signalling & communication, 2015, 51(1): 60-63.

[10] 张健. RSSP-Ⅰ安全协议在电子接口模块中的应用研究[J]. 铁道通信信号, 2019, 55(1): 44-47.
ZHANG Jian. Study of applying RSSP-Ⅰ safety protocol in electronic interface module[J]. Railway signalling & communication, 2019, 55(1): 44-47.

[11] 张淼，耿宏亮. 铁路信号安全通信协议中消息验证码算法的安全性分析和改进[J]. 铁路通信信号工程技术, 2014, 11(6): 4-7.
ZHANG Miao, GENG Hongliang. Security analysis and improvement of MAC algorithm in railway signal safety communication protocol[J]. Railway signalling & communication engineering, 2014, 11(6): 4-7.

[12] 李夏洋. 基于 RSSP-Ⅱ的城市轨道交通 ATS 与 VOBC 间安全通信研究[J]. 铁路计算机应用, 2017, 26(3): 53-57.
LI Xiayang. Communication between ATS and VOBC based on RSSP-Ⅱ for urban rail transit[J]. Railway computer application, 2017, 26(3): 53-57.


（编辑：王艳菊）