doi：10.3969/j.issn.1672-6073.2017.04.011

基于互联互通的区域控制器安全通信计算机设计

魏东冬，卢佩玲，郑长宗，姜庆阳
（中国铁道科学研究院，北京 100081）

摘　要：为了实现列车在不同厂商提供设备的城市轨道交通线路或网络中安全运营、共线混跑以及资源共享，基于通信的列车控制系统互联互通已成为一个重要课题。根据正在起草的互联互通的行业技术规范，为满足不因通信中断而倒机的需求，提出一种实现区域控制中心与其他信号系统通信的专用二乘二取二安全通信计算机的方案，设计其软硬件系统结构、平台内部冗余的连接方式，对单系内的双CPU同步和数据安全比较、双系间的主备同步等关键算法进行研究，并针对安全通信协议中描述的风险设计相应的防御措施。

关键词：城市轨道交通；区域控制器；互联互通；安全通信计算机；二乘二取二；冗余；同步
中图分类号：U231.7　　**文献标志码**：A　　**文章编号**：1672-6073(2017)04-0055-05

Design of ZC Safety-related Communication Computer to Achieve Interoperability

WEI Dongdong，LU Peiling，ZHENG Changzong，JIANG Qingyang
（China Academy of Railway Sciences，Beijing 100081）

Abstract：Since the rail transits and the related facilities in cities are manufactured by different firms，the realization of safe operation and resource sharing for trains through interoperability of communications-based train control（CBTC）has become an important subject. Based on the technical specifications of interoperability which are currently being drafted，this paper proposes a scheme of a double 2-vote-2 safety-related communication computer which can achieve the communication between the zone controller（ZC）and other signal systems and will not switch when the communication is interrupted. The hardware and software system as well as the redundant connection inside the ZC platform are designed. The key algorithm to the double CPU synchronization and data safety comparison in the single system and the main-standby synchronization in the dual system are studied. The defense measures are also designed according to the risk described in the security communication protocol.

Keywords：urban rail transit；zone controller；interoperability；safety-related communication computer；double 2-vote-2；redundancy；synchronization

1　研究背景

现如今，轨道交通运营日渐网络化，多线路的并行建设正在逐渐取代单一线路建设，但是每条线路的建设状况和设计标准的不同，造成了各条线路单独运营、管理、维修的状况[1]。轨道交通的互联互通旨在实现装备不同厂家车载设备的车辆，可以在装配了不同地面供货商设备的线路或由不同运营商管理的线路上联通联运[2]，有利于不同车辆、设备的综合利用和相互兼容，便于既有线路的改造延长，促使可提供设备的供应商增加和整个系统的标准化，降低建设、培训和运营成本。因此，实现轨道交通的互联互通十分重要。

区域控制器（zone controller，ZC）是整个列车控制系统（communication-based train control，CBTC）的核心（见图1），其根据实时的列车位置、运行速度、行进方向、列车进路、道岔、列车自动监控系统（automatic train supervision，ATS）发送的线路临时限速以及其他障碍物等状态[3]，负责列车安全间隔、列车允许速度和进路联锁等逻辑运算，并将上述运算结果生成的移动授权通过数据通信系统（data communication system，DCS）及时发送给车载控制器（vehicle on-board controller，

收稿日期：2016-07-19　修回日期：2017-03-29
第一作者：魏东冬，男，硕士，研究实习员，从事铁路通信信号方面的研究，381238042@qq.com

VOBC),实现对区域内行进列车的控制。

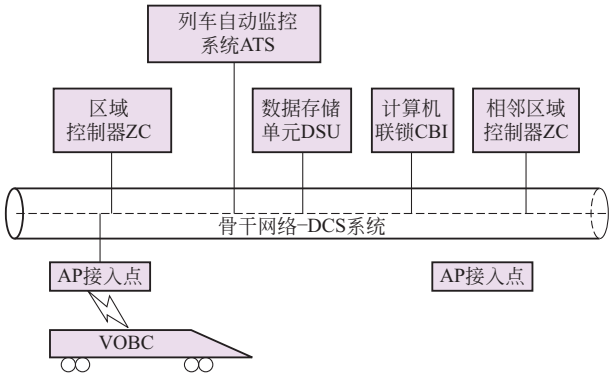

图1 CBTC系统基本结构
Fig. 1 The structure of CBTC

对于ZC而言,CBI为ZC提供道岔、信号机等联锁设备的状态,并处理ZC提供的命令信息;相邻ZC之间进行移动授权的请求和应答,从而保证相邻ZC对列车的控制权进行无缝交接;VOBC向ZC提供位置信息,ZC则为其提供移动授权;ATS主要完成临时限速功能[4]。ZC在CBTC系统中的信息交互如图2所示。

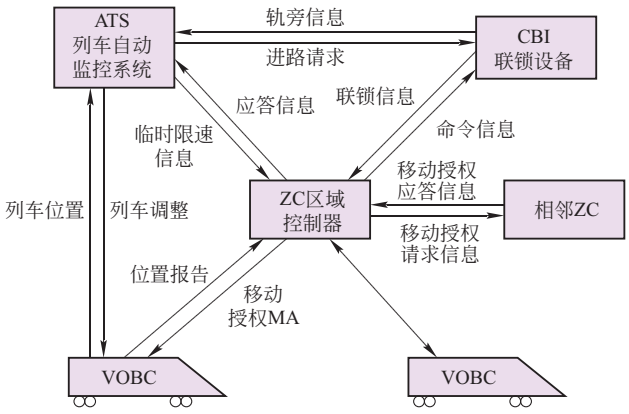

图2 ZC信息交互结构
Fig. 2 Information interaction diagram of ZC

在新的互联互通需求中,DCS网络提供2路数据(A网和B网各1路),ZC系统需要在平台内部实现数据的冗余处理,除此之外,ZC系统影响CBTC的运行效率以及行车安全,且其拥有较多的通信对象,对数据的安全级别要求高,需要严格进行实时性的复杂安全协议运算,在同一个安全苛求设备上实现的难度过大,且不利于设备主要功能逻辑的可靠性和安全性保障及安全验证。因此,为实现CBTC系统的互联互通及确保数据在通信中的安全性和实时性[5-6],以及实现双网数据的冗余处理,有必要研制能够满足通信需求和运算处理能力的、符合信号设备安全级别要求的专用安全通信计算机。

图3为取自《RSSP-II铁路信号安全通信协议》的两通信设备总体传输系统结构[7]。EN50159标准[8]要求需在安全相关设备中建立安全通信功能,应用程序通过安全功能模块提供的安全层的安全协议处理,检测并防护标准中所列出的威胁,从而实现安全传输的目的。

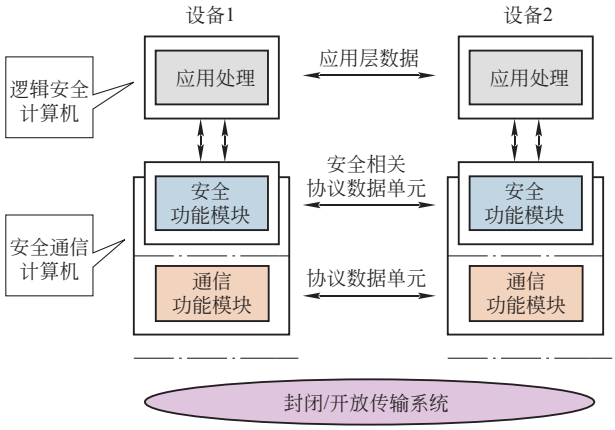

图3 采用安全通信计算机的安全通信系统的总体结构
Fig. 3 The system structure of safety communication system with safety-related communication computer

本文设计的ZC系统通信机将图3所示的安全功能模块和通信功能模块与应用处理模块分离开。其中,实现区域控制器主要功能的是逻辑安全计算机完成应用处理模块,而分离出来的安全功能模块和通信功能模块则由专用的安全通信计算机来实现。将通信功能由单独的计算机来实现,可以更充分地采用各种通信技术手段,更好地实现信号系统资源的共享与互联互通。

2 通信机的系统结构设计

2.1 通信机2oo2×2结构设计

目前,轨道交通设备多采用三取二(2oo3)或二乘二取二(2oo2×2)的冗余结构。前者结构简单,运行可靠,是兼顾了可靠性和安全性的混合冗余机构,稍偏重于可靠性和性价比;后者则结构相对复杂,更偏重于安全性和双子间的独立性、易维护性和可用性。在可靠性和安全性方面,2oo3和2oo2×2在指标特性上非常接近,但从冗余系统独立性的角度来看,具有良好安全性和可靠性的二乘二取二结构,能够在机柜、机笼、采集接点和驱动线圈等方面实现更加彻底的物理隔离,更加有利于实现安全性、可靠性所要求的独立性保障,更有利于系统的维修、维护以及软件更换等。综上考

虑,本文所设计的 ZC 安全通信计算机(ZCM)采用二乘二取二的结构。

为实现系统结构的安全性,设计系统的单系设备采用如图 4 所示的二取二结构。该结构由 2 个单板计算机(single board computer,SBC)组成,2 个 SBC 进行周期性的同步,在同步周期内进行互相独立的运算,对运算结果进行比较以保证一致性和正确性,对比较一致的结果进行输出,不一致时则按照故障处理措施进行处理,且实现 2 个 SBC 的统一管理调度,2 个 SBC 分别设计为主 SBC 和从 SBC。为实现 ZCM 单系的周期同步运算的输入、输出数据的交叉传输,2 个 SBC 之间设计有基于 VME 总线的数据传输通道。

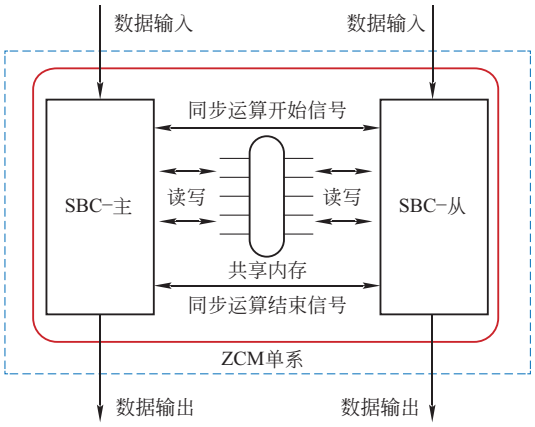

图 4　ZCM 单系结构

Fig. 4　Structure of ZCM single system

为实现系统结构的可靠性,设计系统为双机热备结构。该结构由 2 套设备组成,分别作为 A 系和 B 系。通信机的 A 系和安全网 A 相连,B 系和安全网 B 相连,两系设备的软硬件结构完全相同,同时工作。两系均设计有以太网口并通过以太网相连,作为数据传输的通道。

用于区域控制器的安全通信计算机采用此结构,既可保证区域控制器的整体结构安全、可靠的系统需求,也便于在满足该需求的同时实现 ZC 系统同其他信号系统之间的连接,更好地达到互联互通的要求。

2.2　通信机与逻辑部冗余连接

在 ZC 平台中,通信机主要完成对数据的安全协议运算和对其他信号系统的通信功能,数据的应用逻辑处理则由上层逻辑部来实现。DCS 系统仅提供两路数据,其中安全网 A 和安全网 B 各 1 路。为了在 ZC 平台内部实现双网数据安全冗余,减少倒机次数提高系统的可靠性,采用如图 5 所示的 ZC 平台内部冗余交叉连接方式。

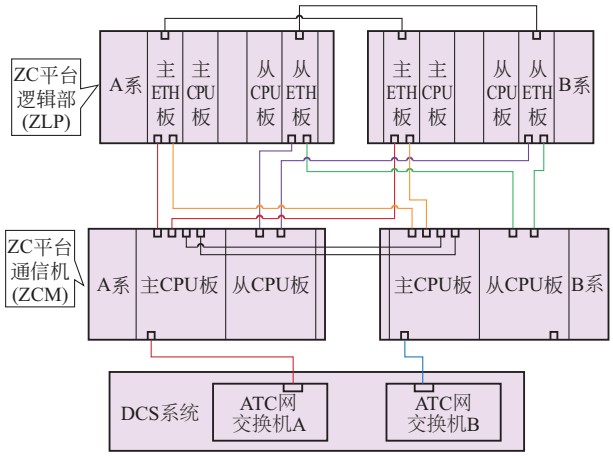

图 5　互联互通版 ZC 平台内部冗余结构

Fig. 5　Internal redundancy structure of interoperability zone controller

DCS 系统提供的 A 网和 B 网两路数据分别同通信机(ZCM)的 A 系和 B 系的主 CPU 相连,数据的安全冗余则在 ZC 平台内部通信机和逻辑部(ZLP)之间实现。通信机的 A 系主 CPU 分别与逻辑部的 A 系和 B 系的主 CPU 相连,从 CPU 则分别与逻辑部的 A 系和 B 系的从 CPU 相连;通信机 B 系的 CPU 与逻辑部的连接方式同于 A 系。当双网数据中的某一路连接中断时,逻辑部的双系仍可通过与 DCS 系统保持连接的通信机单系与其他信号系统进行数据交互,整个系统仍可正常运行;当通信机的某一系发生故障时,其对应的上层逻辑部单系仍可通过通信机的另一系与其他信号系统相连,从而不会因通信中断而导致逻辑部倒机。通过上述 ZC 平台内部交叉连接的方式,保证了 ZC 平台逻辑部对双网数据的冗余接收和发送,能够有效减少倒机的次数,提高了整个系统的可靠性。

3　通信机的软件功能设计

3.1　软件结构设计

通信机的软件采用基于实时操作系统的多线程运行方式设计,图 6 给出了通信机系统的软件层次结构设计,将其自下而上划分为 3 个部分:操作系统层、安全平台层和应用功能层。

操作系统层采用提供基于优先级的多任务、多线程管理的 VxWorks 实时操作系统。安全平台层主要包括 2oo2 同步和一致性比较、1oo2 双系同步和安全参数跟随。应用功能层则主要实现与逻辑部的数据传输(系内通信)、与外部通信对象的数据传输(外部通信)以

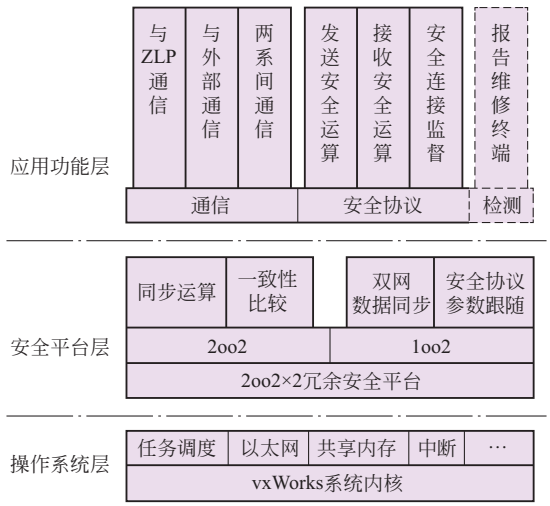

图6 通信机软件结构

Fig. 6 Software structure of ZCM

及两系间的同步和数据交互(系间通信)的通信功能,包括对接收数据的安全运算、对发送数据的安全运算以及安全链接状态监测的安全通信协议处理功能,实现对通信机软件的检测与自我诊断并实时向维修终端报告诊断信息的检测功能。其中,应用层的检测功能为非功能安全相关功能,故而在图6中用虚线表示。

3.2 同步功能设计

通信机系统功能中最关键的是必须在完备的故障检测的基础上,构建安全有效的同步功能和快速可靠的切换机制。由于2oo2结构的特点,需建立2种同步机制:为了保证安全性而进行数据周性期比较的单系内2oo2同步,以及为了实现双网数据冗余接收和发送确保可靠性的两系间1oo2同步。

3.2.1 系内同步和比较

目前,2oo2结构的主要同步方式有时钟级同步和任务级同步2种[9]。时钟级同步主要采用硬件完成2个CPU之间的同步和数据表决,对系统的比较结构、故障检测结构和整体的硬件框架都有较高的要求,实现难度大[10]。任务级同步方式中各子系可以基本完全独立甚至采用完全异构的硬件和软件系统,可有效降低共模干扰和共因故障影响的可能性;其比较表决机制也可不依赖于唯一的硬件载体进行,适用于松散耦合冗余结构的安全苛求系统。

ZC通信机采用任务级同步。同一系的2个CPU通过硬件信号实现主从握手的同步机制。当一子系CPU运行至其主、从同步点时,发出握手信号给对方CPU,并限时等待对方CPU回复的同步信号,只有在限时内收到对方回复的同步信号后,程序才继续向下运行。通过对整个通信及安全数据运算过程的分析,在每个任务周期内设计2次握手同步:任务周期开始同步,确保每个任务周期同一系的双CPU开始时间一致,防止双CPU因网络延迟等问题导致获取数据时间不同而收到不同的输入数据,从而发生严重的安全故障;周期运算处理同步,即在数据交叉运算等处理前进行同步,保证双CPU对数据处理输出的同步。系内的主从CPU周期性同步及比较的设计如图7所示。

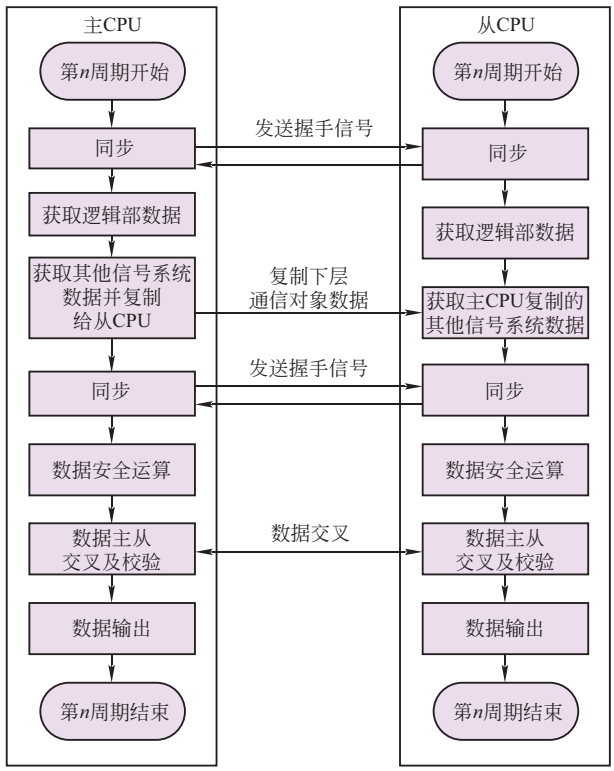

图7 系内主从周期性同步和比较

Fig. 7 Periodic synchronization and comparison in single system

每周期同步开始后,主从CPU均接收上层逻辑部交给的发送数据,而与其他信号系统的非安全信息传输的通信功能只由与DCS系统相连的主CPU来实现,保证对外通信数据的唯一性。主CPU在接收完其他信号系统的数据后,将其复制一份给从CPU,作为周期运算输入数据。两CPU对输入数据各自进行安全协议数据包的生成处理运算,然后再通过共享内存交叉数据,将自身的数据与对方的数据进行一致性比较。最后,要发送给上层逻辑部的数据由2个CPU通过冗余结构发送至逻辑部,要发送给其他信号系统的数据则由主CPU通过以太网对外发出。

3.2.2 系间同步

通信机主备之间的同步采用任务级的同步方式。为实现在主备切换时能够无缝运行，不中断与其他信号系统的通信连接，以及保证对外输出的双网冗余数据的一致性，系间同步的数据分为两类，一是需要实时更新的密钥、时间戳等安全参数信息和发送给其他信号系统的安全协议信息，二是要给其他信号系统发送的数据。

系间周期性同步示意见图 8。通信机双系在收到逻辑部要发送给其他信号系统的数据后，各自对数据进行安全协议运算并生成安全协议数据包，主系通过与 DCS 系统相连的主 CPU 将发送数据给其他信号系统，除此之外主系还通过两系间的以太网将 1 份数据发送至备系，备系将收到的数据与自身安全协议运算结果进行比较，结果一致则备系透明传输主系数据；若不一致，备系则采用“参数跟随”，即使用每周期由主系发送给备系的相关安全运算参数更新自身旧有的参数进行复算。

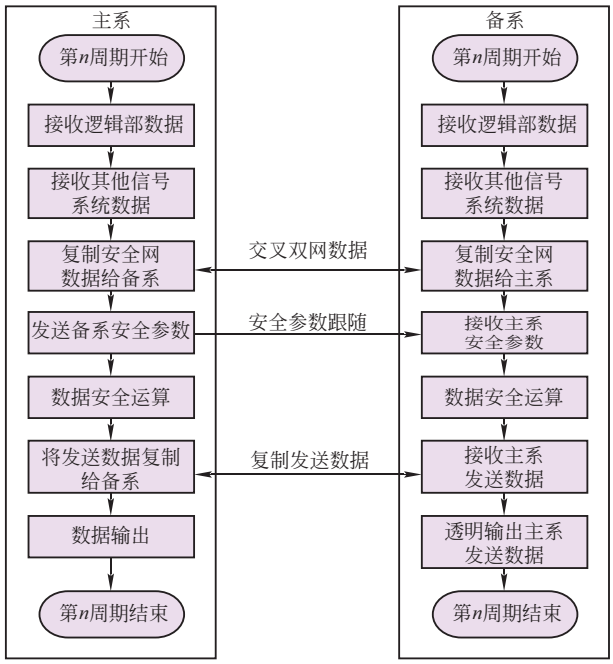

图 8 系间周期性同步

Fig. 8 Periodic synchronization in dual system

3.3 安全通信功能

对比孤立系统而言，安全苛求系统的通信要面对复杂环境，必须能够抵御通用传输系统中可能存在的各种干扰和威胁。通信机具备 RSSP-I 和 RSSP-II 两种安全协议的处理功能，按照模块化的设计思想，每种安全协议分别由独立的软件模块来实现，根据系统配置与指定通信通道进行适配。其中，通信机与 ATS、CBI 和相邻 ZC 的通信协议为 UDP，采用 RSSP-I 安全协议，与 VOBC 的通信协议为 TCP，采用 RSSP-II 安全协议。

通信机针对 RSSP-I 安全协议，随着系统软件内部周期增长的 32 位序列号保证报文的顺序性；使用与序列号同步增长的 32 位伪随机数时间戳保证报文的时间性；创建超时判断线程保证报文接收的时效性；使用 SID 源标识作为报文的身份安全码，保证真实性；使用反馈报文进行时序校正；采用双重校验，通过 2 个 32 位 CRC 校验和 2 个 32 位固定系统校验字来判断校验码的正确性，保证报文的真实性和完整性。对于 RSSP-II 安全协议，通信机设定安全应用中间子层（SAI），采用周期计数 EC 序列号防御和 TTS 时间戳防御，防止数据的重复、删除、重排序和延时；设定消息鉴定安全层（MASL），对接收到的数据进行加密、解密，保证数据的真实性和完整性，防止损坏、伪装、插入等威胁；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。

4 总结

本文为满足城市轨道交通发展互联互通的趋势，设计了一种专用的 ZC 平台安全通信计算机，主要介绍了其软硬件结构的设计，采用 ZC 平台内冗余连接的方式以及关键的同步功能。该通信机实现了 ZC 平台对其他信号系统通信的通信功能和进行安全通信协议运算的安全功能，通过在平台内部与逻辑部交叉连接，实现双网数据的冗余处理，减少倒机次数，提高整个系统的可靠性，更好地适应互联互通的新需求。

参考文献

[1] 武永军. 城市轨道交通信号系统互联互通解决方案[J]. 通讯世界，2014(10)：7-8，9.

[2] 王力. 京津冀区域轨道交通信号系统设计关键点及新技术应用研究[J]. 铁道标准设计，2015(12)：94-98.
WANG Li. Key Points in the design of regional rail transit signal system of Beijing-Tianjin-Hebei and application of new technologies[J]. Railway standard design, 2015(12): 94-98.

[3] 刘晓磊. 城市轨道交通区域控制器的研究[D]. 成都：西南交通大学，2011.
LIU Xiaolei. Study on zone controller for urban rail transit [D]. Chengdou: Southwest Jiaotong University, 2011.

（下转第 64 页）