机车电传动 2016 年第 4 期（2016–07–10）
ELECTRIC DRIVE FOR LOCOMOTIVES № 4，2016（July 10, 2016）
文章编号：1000–128X(2016)04–0066–03

可配置安全通信协议栈的设计

陈　昕，唐俊同
（株洲中车时代电气股份有限公司 通信信号事业部，湖南 株洲　412007）

摘　要：依据 IEC 62280:2014 标准并考虑车载 ATP 与 ZC、多普勒雷达、人机接口、BTM 之间的通信协议，设计了一种可用于城轨 CBTC 各子系统间通信的可配置协议栈。本协议栈提供了多种安全校验机制，在通信异常发生时，具有故障—安全的能力。

关键词：安全通信协议；协议栈；可配置；IEC 62280：2014 标准
中图分类号：U284　　**文献标识码：**A
doi：10.13890/j.issn.1000-128x.2016.04.102

Design of Configurable Safety Communication Protocol

CHEN Xin, TANG Juntong

(Signal & Communication Business Unit, Zhuzhou CRRC Times Electric Co., Ltd., Zhuzhou, Hunan 412007, China)

Abstract: According to the Standard IEC 62280:2014 for the communication among the subsystems of communication based train control (CBTC), and considering the protocols among on-board ATP, zone controller, Doppler, DMI and BTM, a configurable communication protocol was designed. This protocol provided various safety check measures, the fail-safe function of the protocol was verified when the link failure occurred.

Keywords: safety communication protocol; protocol; configurable ; Standard IEC 62280:2014

0　引言

基于通信的列车控制系统（CBTC）在城市轨道交通的建设热潮下得到了广泛的应用，成为城市轨道交通列车运行控制系统的发展趋势。

CBTC 中需要联锁、区域控制器、车载 ATP 各个子系统通过通信方式进行大量、频繁的数据交互，交互信息的真实性、完整性、时限性、次序性是 CBTC 系统安全运行的基石。

CBTC 系统中的 2 个子系统间通信的打包、发送、接收、解包的过程称为传输系统。IEC 62280:2014 标准比较 IEC 62280:2002（GB/T 24339.1 等同于 IEC 62280:2002）而言，该标准将封闭式传输系统和开放式传输系统统一作为传输系统进行描述。该标准提到，传输系统可能会遇到重复、删除、插入、重排序、损坏、延迟和伪装等安全威胁。安全通信协议要求对传输系统中的安全威胁进行防御，对于无线接入等原属于开放式传输系统的传输网络，需要在安全通信协议或 DCS 中进行加密处理，并辅以 MAC 或 IP 绑定等手段应对网络攻击。

为了防御标准中定义的威胁风险，要求接收方必须对接收到的信息的收发双方的身份信息、信息帧的正确性、信息帧的时效性和信息帧序列的正确性做出检查以保证数据包的真实性、完整性、时限性、次序性。在某些开放式网络环境下，为防止伪造数据包恶意入侵，在协议栈内还需要对数据包进行加密校验。

完成以上功能的软件模块通常称为安全通信协议。

国内城轨及铁路领域常用的安全通信协议为 RSSP-I（运基信号 [2010]267 号 . 铁路信号安全通信协议 -1）及 RSSP-II，RSSP-I 通过序列号、线性反馈移位时间戳、源标示 SID 和双重校验等手段保证封闭式传输系统中的信息传输安全，RSSP-II 则通过 TCP 协

收稿日期：2015–11–30

议通信机制、时间戳、消息验证码 MAC 和源目的标示符等保证传输系统中的信息安全。

1　安全通信协议栈设计

1.1　协议栈的需求

遵循 IEC 62280:2014 标准并考虑城轨信号系统自身需求，本协议栈应具有以下功能与特点：

①2 个子系统间的通信协议还需要考虑兼容串口、CAN 等传输介质的传输系统。在这类通信过程中，一个整包数据通常会被协议（如 CAN）或者由于线路原因分批到达传输系统的接收方，接收方需要将多个数据包拼合后再对其数据的真实性、完整性、次序性作出校验，某些传输过程还需要保证数据的时限性。

②在基于串口、CAN 等传输介质的传输系统中，通常都会尽可能减少传输的字节，往往都会使用校验和、单字节发送序列号等较简单的校验机制。

③协议栈应支持 RSSP-I、RSSP-II 安全通信协议。

④协议栈应适用于已有的 DMI、BTM、多普勒雷达等通信协议。

⑤协议栈应支持多条通信链路，且链路间数据、状态应相互隔离。

⑥协议栈提供给上层应用的接口函数不应与底层通信介质、通信协议格式关联。

⑦适用于开放式传输系统，支持 AES、3DES 等多种加密方式。

⑧协议栈应具有良好的可扩展性、可移植性。

1.2　协议栈构架

协议栈构架如图 1 所示。

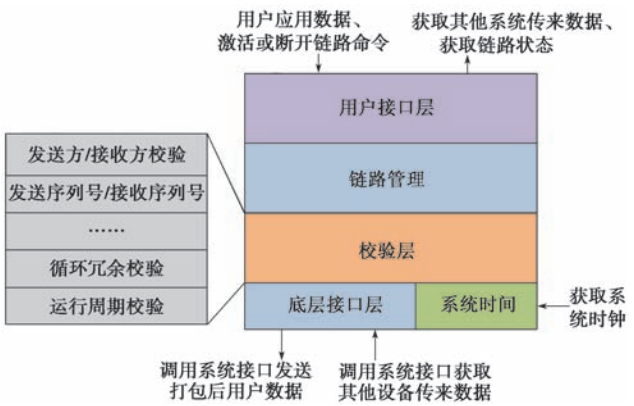

图 1　协议栈构架

协议栈通过修改底层接口层的接口函数，可移植到不同操作系统，操作不同底层接口即可实现通过不同的链路连接方式 (以太网、CAN、串口等) 进行通信。

校验层提供了各种校验机制，用于保证数据包的真实性、完整性、时限性、次序性。

设备启动时，链路管理层需要加载本设备的所有通信链路的参数配置、通信协议结构等。在运行时，链路管理层获取校验层校验的结果与用户接口层对通信链路的激活或关闭命令，控制协议栈内每条链路的链路状态变化。

用户接口层提供接口函数供上层应用调用，用以激活断开链路、获取链路状态、收发应用数据等。

1.3　协议栈配置

协议栈中通过对每条链路的配置包括 3 个部分：

①协议结构：声明某一条链路上采用的安全通信协议采用何种校验机制或者哪些校验机制的组合，有发送方 / 接收方检验、发送序列号 / 接收序列号、单序列号、CRC16、CRC32、CRC48、校验和、时间戳、周期戳、AES、RSSP–1、RSSP–2、固定的单字节包头、固定的双字节包头、透明传输等可选配置；

②协议参数，如：超时容忍值、序列号容忍值、收发双方类型及识别号等；

③如果协议栈结构为 RSSP–I 或者 RSSP–II，则需要进行 RSSP–I 的 ADDRESS、SID、SINIT、DATAVER 等参数或 RSSP–II 协议中 ETCSID、SAI 标示符、超时器阈值、密钥等参数进行配置。

1.4　协议栈主要内容

1）发送方 / 接收方

系统间通信将有一个系统作为发起方，另一个系统作为应答方。在不同的通信链路上，发起方和接收方由系统双发协定。当数据包中的发送方或接收方数据域与本条链路配置不符时，协议栈将该数据包丢弃。

2）发送序列号 / 接收序列号

发起方、应答方任意一方将要发送出一包数据时，会将内部发送计数值加 1，并将该值随数据包一起发出；当接收到合法数据包时，会将内部接收计数值加 1。当数据包超过该校验机制允许门限值后，该链路断开。

3）循环冗余校验

协议栈提供了 3 种循环冗余校验，它们分别是 CRC16、CRC32 与带签名的 CRC48。

CRC 将除了 FFFE、简易 AES 加密外的其他部分如：帧类型、日历时间、传输序列号、接受序列号、EC、应用数据长度、应用数据、签名一起作为 CRC 校验计算的输入值。

如果采用带签名的 CRC48，需要在配置文件中指定链路签名。在每次 CRC48 计算过程中，会将该链路对应的数字签名与将要发送的数据一起进行 CRC48 校验计算。当接收方接收到数据包后，需要将该链路对应的数字签名与接收到的数据内容一起做校验计算，以检测通信是否在合法实体间进行。

当数据包不满足任何一种循环冗余校验机制时，协议栈将丢弃该数据包。

4）运行周期校验

应用数据应该防护延迟威胁，运行周期校验的安全防御技术可用于保护消息的时效性。

运行周期校验机制是保证在 2 个固定周期运行设备间时效性的校验机制。如果设备无固定周期值，则