城轨列车实时以太网环型拓扑结构分析及应用

段旭良　吴桂林　李　翀　白春光　钱江林

中车株洲电力机车有限公司　湖南　株洲　412000

摘　要：本文深入探讨了城轨列车中实时以太网拓扑结构的实施与优化。通过对城轨列车实时以太网典型拓扑结构的实际应用进行分析，本研究揭示了在列车层面采用双环网结构，以及在车辆层面采用双归属连接的拓扑结构，不仅确保了列车网络控制系统的稳定性与可用性，而且符合多网融合的技术发展趋势。此外，本文还提出了多网融合方案和网络防护措施，为多网融合技术的研究与开发提供了宝贵的参考。

关键词：实时以太网；拓扑结构；多网融合；网络防护

引　言：

随着全自动驾驶、健康管理、智能列车和大数据等新兴技术在轨道交通领域的广泛应用，传统的网络拓扑结构，如MVB和CAN网络，已难以满足轨道交通行业对数据的高实时性和大容量的需求。实时以太网技术的发展，凭借其开放性及高带宽等优点，使其在现代城市轨道交通车辆中得到了广泛应用，以其高效、准确和可靠的特性，广泛应用于列车网络控制技术。[1]

城市轨道交通车辆的智能化是其发展的主要方向，而数据是智能的基础，列车实时以太网网络控制系统高带宽和高数据传输速率，使其能够集成列车的控制、诊断、监测、维护等信息数据，为智能先进的城市轨道车辆提供数据载体，从而完成信息大容量传输、智能诊断、故障精确定位、专家诊断等功能，因此被越来越多地应用到城市轨道列车领域[2]。

一、 ECN拓扑架构

根据GB/T 28029.12-2020轨道交通电子设备 列车通信网络(TCN) 第3-4部分：以太网编组网(ECN)标准，其典型拓扑结构有以下几种。

（1）线性拓扑，如图1所示。以太网交换机采用单线串联，终端设备采用单线与以太网交换机相连，此拓扑结构的优点是：布线施工便捷，电气原理图设计简单，布线距离短，故障易排查；缺点是：若出现单点故障，会影响整个网络的数据传输。（见图1）

（2）双归属线性拓扑结构（并行网络），如图2所示。每个终端设备ED通过两条物理链路与以太网交换机进行连接，该拓扑结构的优点是：各个交换机连接在2 条独立且互为冗余的物理通信链路上，若一个链路上出现单点或是交换机故障，则另一链路仍可传输数据，不会造成通信中断；缺点是：2条链路增加了交换机设备的数量，同时也增加了布线和连接器的数量。（见图2）

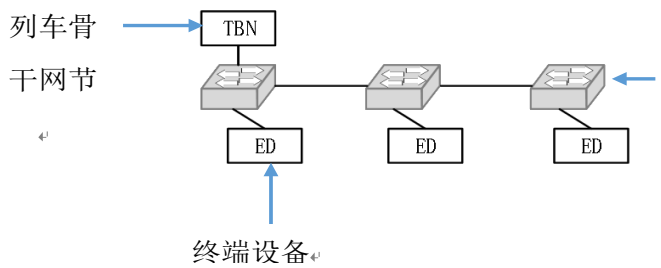

图1　线性拓扑图

（3）环型拓扑，如图3所示。在环型拓扑中，通过以太网线将以太网交换机连接成环，各个终端设备ED通过单链路与以太网交换机相连接，该拓扑结构的优点是：由于是环型结构，当单物理链路故障时，可自动切换传输路径，从而增强数据传输的可靠性。缺点是：若网络中有线路出现虚接的问题，则可能出现环网频繁组网的情况，导致数据丢失。（见图3）

二、网络拓扑结构的冗余分析

根据GB/T 28029.12-2020轨道交通电子设备 列车通信网络(TCN) 第3-4部分：以太网编组网(ECN)标准的定义，ECN的特定实现需要选择一种或是多种冗余方式以满足应用的要求，而冗余包括：网络级冗余和终端设备级冗余：

（一）网络级冗余包括:

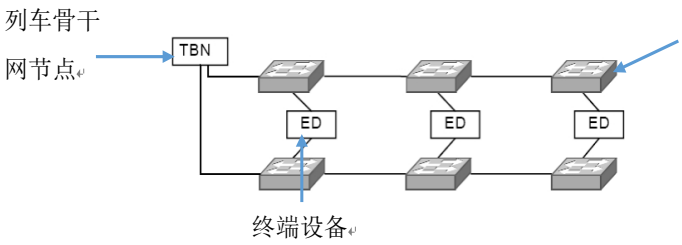

图2　双归属线性拓扑结构

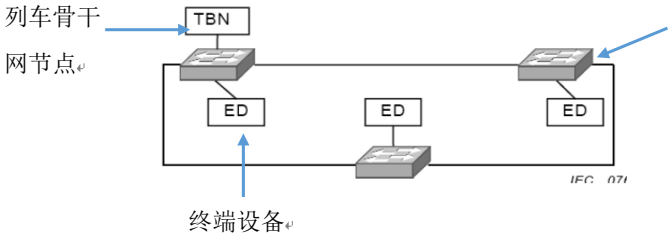

图3　环型拓扑

1、当ECN使用冗余机制时，完整网络中的单一网络部件失效后，不应影响网络其他设备的正常工作，以使得应用能够维持其功能；

2、当网络设备重启时，因网络重新配置导致的连接丢失持续时间应等于或小于恢复时间要求的值；

3、整个网络中任意时刻不能形成数据的转发环，以避免广播风暴的产生。

（二）设备级冗余：

具有互为冗余的两条链路的终端设备，称为“双归属”，双归属设备需使用独立的物理网络接口，且不能产生ECN上的环，如果冗余链路与多个编组交换机连接，则当一台编组交换机失效时，该双归属设备依然可以继续通信。

三、双环网+双归属的网络拓扑架构

在实际的项目实施中，列车网络控制系统作为整车数据的载体和通道，既要有一定的冗余性用于保证数据的稳定性和可靠性，又要考虑车辆实际的设备布置和线缆铺设的可行性，因此综合以上的几种拓扑结构，采用双环形+双归属的复合式拓扑结构，如图4所示：

（一）列车级控制总线采用ECN千兆双环网配置（简称A环和B环），其中A环只负责列车控制数据的传输，B环负责列车控制数据和维护数据的传输。

（二）车辆级控制总线采用点对点与以太网交换机连接，子系统设备A口和B口双归属冗余，分别接入A和B两个环网。（见图4）

此复合拓扑架构的特点有：

（1）冗余设计：包括列车级的双环网互为冗余，关键设备采用双归属的独立A/B网口接入环网中的交换机；

（2）实时通信设计：各系统间的通信采用TRDP协议，TRDP协议由位于TCP/UDP传输层之上的TRDP层执行，如图5所示。该层可选网络中任意两个终端设备之间关键过程数据和消息数据的安全端到端数据传送的安全层扩展[3]，并需符合IEC61375-2-3标准的SDTV2版本的要求。（见图5）

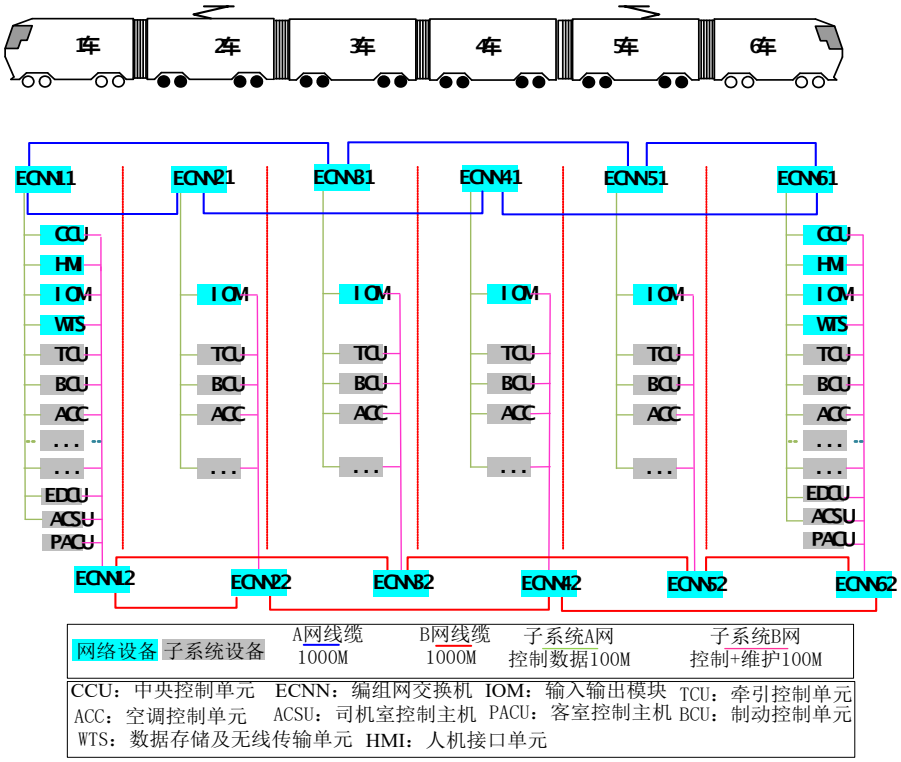

图4　双环双归属网络拓扑

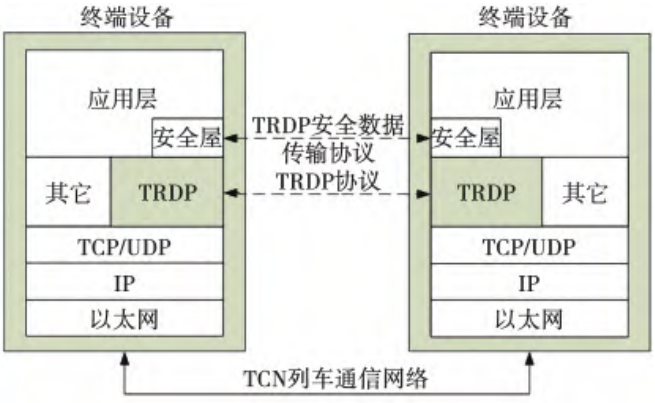

图5 TRDP协议栈

（3）网络融合技术：列车级采用物理隔离的双环网架构，保证了控制数据在A环和B环的独立传输，任一环网故障，均不影响列车的控制功能，同时B环融合了全车的维护功能和智能运维数据的传输功能，为了保证B环中的控制数据与维护数据与智能运维数据不相互影响，采用虚拟局域网（VLAN）划分技术，将B环网划分为两个VLAN，列车控制数据划分到VLAN1，维护数据与智能运维数据划分到VLAN2，从而实现列车控制数据和维护运维数据的隔离。

四、网络安全防护

根据国家等级保护制度标准2.0 中的标准GB/T 22239—2019《信息安全技术 网络安全等级保护基本要求》和IEC 62443 系列标准中的技术要求，列车通信网络安全防护可从区域边界、网络通信、设备安全3 个方面进行建设[4]。

（一）区域边界防护：

区域边界指的是内网和外网的边界，其中的内网指的是列车网络控制系统，外网指的是与列车网络控制系统相连接的无线传输系统，

在内外网传输的边界布置硬件防火墙，用于外部网络与车载网络的隔离防护，确保车载网络不受外界网干扰。车载防火墙可检测和防御针对车载通信协议的网络攻击，通过内置入侵防御特征库，使用特征匹配和异常分析的方法识别并阻断网络攻击行为（如各种DoS、DdoS 攻击行为）；

（二）网络通信防护：

网络通信防护分为列车网络控制系统内部通信安全和车地通信安全。对于列车网络控制系统内部通信的安全，针对关键控制系统，采用图5所示的安全协议。同时为了防止广播风暴的发生，通过限制交换机端口的入口速率和出口速率，实现交换机设备内最大广播流量的限制，防止过高的数据流量对终端设备造成的影响。对于车地通信安全，采用数据加密传输，数据接收进行进行合法性判断的方法，保证数据传输的安全性和完整性。

（三）设备安全防护：设备防护主要包括：

1、访问控制：根据列车网络通信的需求配置相应的白名单，实现对白名单内的设备通信的协议解析，同时支持私有协议的自定义解析；

2、会话限制：通过限制IP的最大并发会话连接数，避免由于单台设备的异常通信导致业务访问异常；

3、专用维护接口：通过在防火墙上设置专用的维护接口，避免无授权的外部设计接入；

4、维护PTU工具软件的注册与访问限制：根据需求设置PTU维护工具软件的白名单，白名单外的设备禁止接入。

五、结语

本文通过对ECN拓扑架构的分析，重点介绍了网络拓扑架构的冗余原理，并设计了双环网+双归属的网络拓扑架构，此种拓扑架构即解决了传统列车子系统相互独立，列车的电缆数量多、种类多、总线结构复杂等问题，也保证了列车网络控制系统的可靠性、可维护性，同时更好的支持了后续的多网融合和智能化业务的发展。本文件中提到的新型网络拓扑架构能支持更丰富的数据传输，为列车智能运维，智能驾驶等新功能提供了良好的数据平台，进一步促进列车制造及运营成本的降低、列车智能化水平的提升，更好地满足了城市轨道交通网络化运营的要求，并将助力我国城市轨道交通的发展。

参考文献：

[1]屈雪刚,吴君,钱兆勇.基于以太网的列车多网融合技术研究[J].铁道机车车辆,2023,43(5):50-54.

[2]丁超.城轨列车实时以太网拓扑结构分析及应用思考[J].现代城市轨道交通,2021.12,79-84.

[3] GB/T 28029.4-2020轨道交通电子设备 列车通信网络(TCN)第2-3部分：TCN通信规约.

[4]邹智荣，陈超群，陈勃，唐品.列车通信网络安全现状分析及应对方案研究[J].机车电传动,2023(1),78-85.

作者简介：

段旭良(1982—),男，汉族，河北遵化人，正高级职称，硕士学历，专业为控制理论与控制工程。