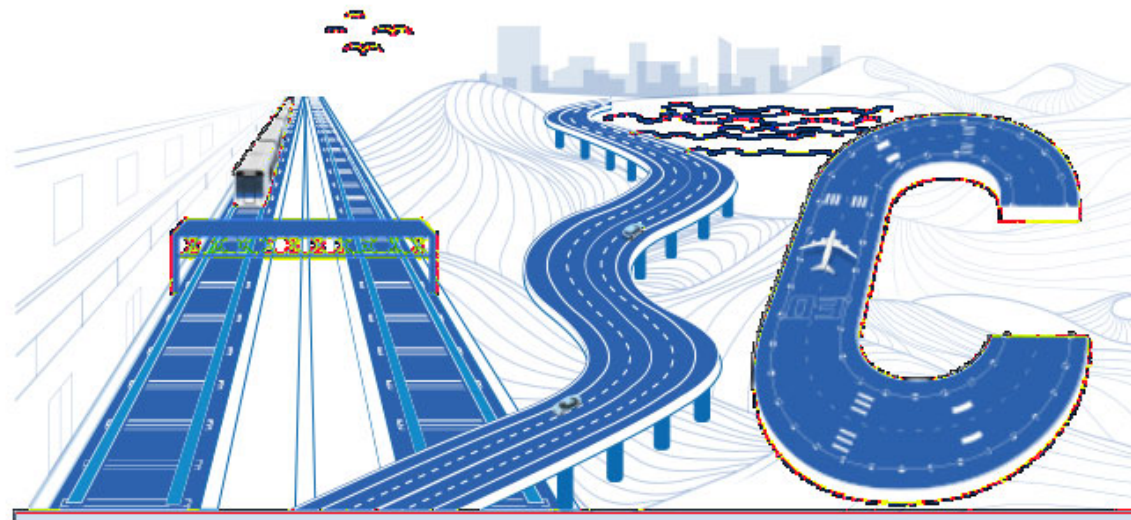


新华三交通行业

数字化转型白皮书



新华三集团

北京总部
北京市朝阳区广顺南大街8号院 利星行中心1号楼
邮编:100102

杭州总部
杭州市滨江区长河路466号
邮编:310052

www.h3c.com

Copyright © 2024新华三集团 保留一切权利
免责声明: 虽然新华三集团试图在本资料中提供准确的信息, 但不保证本资料的内容不会含有技术性错误或任何性质错误。
为此新华三集团对本资料中信息的准确性不承担任何责任。新华三集团保留在没有任何通知或提示的情况下对本资料的内容进行修改的权利。
CN-241030-20240123-BR-SD-V1.0

AI for ALL
精耕务实 为交通赋智慧

精耕务实，为交通赋智慧

文 / 辛龙超

交通是最早使用信息化技术的行业之一，但由于交通行业的专业性较强，对安全可靠性和移动性强等特点，在数字转型过程中相比于其他行业面临更多严峻的挑战和难题，例如安全和效率如何平衡、技术和场景如何融合、创新试点和规模复制之间如何转化等等。纵观交通行业信息化几十年发展史，经历了自动化、数字化、智慧化、绿色化四个阶段，每一个阶段的发展，都离不开政策的引领，需求的驱动以及创新技术的支撑。

政策引领、需求驱动、技术支撑，交通行业数字化转型全面加速

近年来随着交通强国战略等一系列国家政策的施行，2035年我国将基本建成交通强国，形成123出行交通圈及123快货物流圈。正如交通强国纲要中所提到的，近两年我们参与多个交通行业信息化项目建设，明显感受到了三个层面的变化：由速度规模向质量效益转变，交通基础设施建设增速减缓，从重视建设向建设运营并重转变；由独立交通向综合大交通转变，大型交通枢纽、城市综合交通、多式联运等交通一体化新形态涌现；由传统驱动向创新要素驱动转变，从运营交通到经营交通转型，从提供标准位移群体服务向精准消费个体服务演进。

在国家大政策的引领下，交通行业数字化转型也进入爆发期，无论是中国城市轨道交通协会发布的《中国城市轨道交通智能城轨发展纲要》，还是民航局发布的《中国民航四型机场建设行动纲要》，各省交通厅陆续发布的《智慧高速公路建设指南》，以及国铁集团发布的《铁路信息化总体规划》等行业政策，无一不在强调交通行业客户需求再发生重大变化，行业客户更加务实，不再满足于基本需求，不再盲目追求新技术、新产品，更多追求数字化技术与行业业务场景的深度融合。

与此同时，AIGC、云计算、大数据、5G、区块链等新技术也为智慧交通建设提供有效的支撑工具和手段。2019年全国高速公路取消省界收费站工程之所以能够快速建设完成，是因为ETC技术的成熟与普及；云计算技术和地铁业务深度融合，让城轨云建设成为地铁信息化建设的主流；多个城市地铁业主开始选择高性价比的5G公网作为车地无线通信网络制式，铁路5G-R专网建设也提上了日程；生成式AI技术在交通运营和运维场景逐步渗透，极大的提升了运营运维效率，真正实现了降本增效。

交通数字化转型需要技术和业务深度融合，创新业务价值

如上所述，智慧交通的建设绝不是新技术和新产品的堆砌，而是技术和业务的深度融合。数字化技术需要从建设阶段走入规划、运营、经营全流程，在重点场景选择合适的、高性价比的产品技术，实实在在解决问题，而不是最新的、最流行的技术，单纯的新技术的应用不是创新，对生产运营有帮助的场景才是创新。

当前交通行业的基础设施普遍缺乏数字化能力。例如，很多路侧、轨旁、场站及枢纽的终端还是“哑”的，尚未纳入交通运营管理。面对这个问题，也许大家首先想到的是5G技术去解决。诚然5G网络的低时延、广连接、大带宽特别适配交通移动性强、重资产、重安全等需求。我们也看到，无论是铁路、地铁、机场等行业都在积极布局5G行业的专属应用。但因为行业标准、产业生态、数据安全等一系列问题，5G在交通行业大规模成熟的应用仍需时日，所以我认为交通基础设施数字化的首选技术不能唯5G论。

在机场行业，物联网仍然是机场实现全域感知的重要技术手段。例如机场的无动力设备作业是航班地面保障的重要工作，然而无动力设备分布在机场机坪、停车场和库房等区域，数量多、使用分散、维护保养难，已成为整个行业近十年的管理难题。我们基于“云网一体化”的物联网数字基础设施，助力萧山机场打造了端到端无动力设备管理创新应用，采用“LoRa+卫星定位”技术方案，实现了室内、室外的连续性定位，有效提高了机场飞行区无动力设备的管理效率。

在城轨行业，市域（郊）铁路建设如火如荼，市域轨道普遍设计时速较高，如雄安新区至北京大兴国际机场快线（R1线），设计时速达到200km/h。市域（郊）铁路高速移动环境下，对车地无线通信网高速适应性提出了更高要求。新华三在业界率先完成了WLAN方案在260km/h高速移动环境测试，可达760Mbps传输带宽，完全满足市域铁路对于高速无线的需求。此外，Wi-Fi 6的技术也由生产领域延伸应用到运维、运营领域，为智能运维和智慧车站提供性价比极高的传输通道。技术的先进性不仅仅是指标的先进性，而是技术能否真正适合交通行业的应用场景。

另外一个层面，无论是地铁、铁路、空管、公路等行业，目前均在使用传输技术构筑骨干承载网络。诚然，传输技术在可靠性、业务隔离度、稳定性等各方面均具备得天独厚的优势。但随着智慧业务的发展，大量高清视频监控，车路协同以及智能传感器的引入，对交通骨干承载网的提出了新的业务诉求，如需要灵活地进行业务开通，给予业务更加精细化的带

宽保障。尤其是分布式云的出现，需要网络能够跟随算力实现精准的流量调度，能够可编程调度，而传输技术是无法满足这一点的。

新华三凭借对行业骨干网业务的理解推动IPRAN技术进一步演进，通过单台设备的统一交换架构，融合支持IPv6+和光层的能力，深度挖掘IPv6+的网络切片，业务感知和智能运维等能力的基础上，融合支持光层的大带宽、低延时、高可靠和硬隔离的能力，更好的服务智慧交通的业务发展，同时也可极大降低建设及运维成本。

通过参与众多交通行业云的实践，我们看到当前交通云的建设较以前发生了较大变化：云计算不再是标准的产品和工具，实现基础资源的云化，客户更希望云服务更加场景化、套件化，更加贴合实际业务的定制化需求。例如PaaS平台在向aPaaS演进，基于专属的PaaS平台进行云原生业务的开发。此外，云平台建设不仅是软硬产品的简单集成，更是一套复杂的系统方案，所以在云平台的建设上，客户不仅仅是在选择产品，更是在选择一家具备技术实力，能够长期稳定合作的行业伙伴。我们提出与交通行业客户深度合作，打造专属于客户的私有行业云。

截止目前，我们已经服务全国60余个城轨云建设，包括北京、南京、上海等一线城市超大规模城轨云项目。根据IDC发布的《中国城轨云基础设施市场分析》报告，新华三市场份额已连续三年排名第一。之所以取得这样的成绩，是因为我们将标准的云方案进行了深度的改造，以适配城轨云的特殊需求：针对CCTV业务进行组播数据优化，满足安全生产、内部管理、外部服务在三网隔离前提下实现统一云管，解决AFC系统在客流高峰期承载压力大的问题，满足信号系统上云的安全可靠性需求，兼顾未来新建或改造线路的接入扩容等等。这些改造和适配都需要大量的实践经验，需要对行业标准的深刻理解，用超强的方案定制开发能力去实现。

在车路协同场景中，智能网联车辆对于道路交通系统信息反馈的实时性、准确性、连续性的要求大幅提升，传统交通信息技术和系统无法满足这些新的要求。我们联合交通运输部公路院，搭建一套新的云边协同架构，通过引入高效、高可靠的边缘计算节点提升整个交通信息系统的协同服务能力。在智能交通技术交通运输行业重点实验室的支撑下，公路院与新华三集团组成了联合研究团队，研发了高可靠云边协同系统的架构原型，并在公路交通试验场开展了功能验证与应用示范，该云边协同架构能够实现当边缘设备出现故障及算力不足时，基于云平台调度功能实现边边、云边协同，大幅提升系统的可靠性及稳定性，通过云边之间的资源共享及协同控制，保障车路协同业务的连续性。

AI大模型已成为面向未来的战略性技术，数字时代的PC互联网、云计算大数据等技术带来了生产效率的提升，AI只是扮演了脑力辅助角色。而在智能时代，AI大模型将实现脑力生产效率的二次跃升，带来一场生产力和人机交互的革命。然而，通用AI大模型在交通行业落地面临着训练成本高、部署和运维复杂、行业数据安全风险高、行业专属能力差等一系列问题。为此，需要将AI通用大模型进行裁剪，使其能够轻量化低成本部署；同时公有大模型需要私域化部署，让行业专有数据不出域、可用不可见，帮助客户以私有数据训练定制化的人工智能，建设最“放心”的私域大模型；同时，也需要聚焦细分场景，打通垂直应用数据，形成精准、精确、精益的私域垂直特定能力，建设最懂行业的私域大模型，从AI in ALL到AI for ALL。

2023年6月，新华三在业界率先发布了百业灵犀私域大模型，致力于为百行百业客户建设行业专注、区域专属、数据专有、价值专享的私域大模型解决方案。在交通行业，我们与机场、公路、地铁多个客户的业务场景进行适配开发，发布了智能客服、安全事件分析、智能运维、运维管理、高速公路绿通违规解释、交通安全事件应急处置建议等多个场景化方案，极大提升了客户生产、运维领域的效率，降低了相关的成本。

合适和务实成为交通行业智能化建设的普遍理念



最后，我认为交通行业的数字化转型关键在于将技术与业务深度结合，实现创新和效率的双赢。然而，这并非简单地追求技术的领先地位，更不能被大而全的理念所迷惑。合适和务实已成为交通行业智能化建设的普遍理念。



注重合适性就是要在技术应用上要与行业的实际需求相契合。盲目地跟随科技潮流而投入昂贵的技术并不一定能够创造真正的价值。相反，交通企业应当审慎考虑自身的业务痛点，选择能够解决实际问题的技术方案。这需要深入了解交通生产、运营、运维的各个方面，从而找到真正适合的数字化解决方案。其次，追求务实，不仅仅关注技术的高级程度，更要关注技术的可操作性和实施的可行性。只有在技术创新与实际业务需求相结合的基础上，数字化转型才能够真正取得成果。

未来，新华三将持续以不断创新的技术实力，与客户、合作伙伴一道，精耕交通行业需求，推出更多务实、合适的行业解决方案，持续助力大交通行业数字化转型升级！

目录

CONTENTS

01 云城轨 智行远

第一章 探索城轨IPRAN骨干承载网新应用			
第一节 城轨骨干承载网技术演进趋势	02		
第二节 IPRAN技术挖掘城轨骨干传输网络新价值	03		
第二章 智慧城轨无线通信系统发展趋势			
第一节 背景介绍	07		
第二节 智慧城轨无线业务类型	07		
第三节 智慧城轨无线通信系统现状	08		
第四节 智慧城轨无线通信系统发展趋势	09		
第三章 城市轨道交通5G专网通信应用探讨			
第一节 背景介绍	12		
第二节 城市轨道交通5G专网通信场景及应用需求	13		
第三节 运营商垂直行业5G专网组网方案	13		
第四节 地铁5G专网发展现状	17		
第四章 Wi-Fi与IoT创新融合，构建城轨智能运维体系			
第一节 城轨智能运维需求	19		
第二节 Wi-Fi与IoT技术结合改变传统管理手段	19		
第三节 复用PIS系统轨旁AP实现轨行区的双网覆盖	20		
第四节 基于Wi-Fi+IoT的运维体系实现全流程自动化、智能化	21		
第五章 TSN在城轨行业的应用展望			
第一节 TSN技术简介	23		
第二节 TSN在城轨的应用	25		
第六章 扎实基础，创新延续：新华三如何定义下一代城轨云？			
第一节 IaaS底座，让创新与可靠合二为一	29		
第二节 推动“云数智”融合，以DaaS平台激活数据价值	31		
第三节 以业务逻辑为导向，加速云原生理念落地	31		
第四节 从安全、运维到运营，与城轨云变革相伴而行	33		
第七章 城轨云“和而不同”的发展之道			
第一节 主备同构，一云统管	34		
第二节 跨网异构，分散风险	36		
第三节 综合运营，全局统览	38		
第八章 构建城轨边缘数字底座解决方案			
第一节 城轨边缘数字底座的概念和特点	40		
第二节 城轨边缘数字底座的构建	41		
第三节 城轨边缘数字底座场景化应用探索与实践	47		
第九章 城市轨道交通云容灾技术分析			
第一节 容灾技术规范和标准	49		
第二节 容灾需求分析	51		
第三节 技术路线分析	53		
第十章 基于云平台的城轨信号系统建设探索与思考			
第一节 城市轨道交通信号系统智能化发展趋势	61		
第二节 新华三助力城轨信号系统安全云平台的探索与思考	62		
第三节 城轨信号系统安全云平台的优势	63		
第十一章 城轨云安全体系建设研究			
第一节 城轨行业的网络安全问题	65		
第二节 城轨云安全体系技术全景研究	66		
第三节 未来城轨安全技术研究	74		
第十二章 城市轨道交通云平台安全资源池最优方案探讨			
第一节 总体需求	75		
第二节 城轨云安全资源池最优方案探讨	78		
第十三章 城轨云平台商用密码应用安全性评估及建设			
第一节 背景介绍	87		
第二节 城轨云平台密码应用需求	89		
第三节 密码应用技术方案	90		
第四节 密码应用安全性评估	92		
第十四章 城轨数据中心液冷技术发展浅析			
第一节 液冷技术发展背景	94		
第二节 液冷技术介绍	96		
第三节 新华三液冷解决方案	99		

第十五章 四大集约化助力绿智城轨发展

第一节 业务集约化	102
第二节 数据集约化	103
第三节 平台集约化	104
第四节 组织集约化	105

02 云协路网 智行未来

第十六章 智慧高速如何“智慧”？

第一节 智慧高速概述	107
第二节 智慧高速发展历程	107
第三节 智慧高速建设模式	108
第四节 智慧高速整体建设思路	109

第十七章 基于SRv6的高速公路“自动驾驶”网络

第一节 传统网络不足以支撑车路协同全面建设	113
第二节 基于IPv6的解决方案	114
第三节 SRv6 Policy：让数据在高速公路网络中“自动驾驶”	115

第十八章 IPRAN2.0在高速公路路段接入网的应用探讨

第一节 从个性到共性，当前高速公路路段接入网技术路线应用分析	118
第二节 迈向智慧高速，路段接入网建设需求发生转变	118
第三节 基于“IPv6+”技术底座，IPRAN2.0推动高速公路路段接入网变革	120

第十九章 新华三IPRAN2.0让武汉绕城高速通信网“随需而变”

第一节 基于新华三IPRAN2.0，重构武汉绕城高速公路通信网	123
第二节 构筑坚实网络底座，推动智慧高速高质量发展	126

第二十章 依托站级云化智能底座推进收费站标准化

第一节 “新技术”+“老场景”，智慧收费站开辟新路径	128
第二节 站级云化智能底座是收费站标准化的核心	129
第三节 站级云化智能底座的价值	131

第二十一章 高速公路收费系统安全能力提升的思考

第一节 高速公路收费系统安全能力现状分析及建议	133
第二节 高速公路安全能力提升思路	135

第二十二章 关于高速行业如何用好AIGC的思考

第一节 AIGC的发展背景及私域建设的必要性	137
------------------------	-----

第二节 大模型私域落地需要关注什么	138
第三节 高速行业AIGC场景落地的思考	139
第四节 高速行业AIGC场景落地进度规划	143
第五节 新华三AIGC能力框架	144

第二十三章 零碳智慧服务区建设方案

第一节 零碳服务区建设背景	145
第二节 零碳服务区解决方案	145
第三节 零碳服务区建设优势	148

第二十四章 对公路基础设施全生命周期管理的思考

第一节 公路基础设施全生命周期管理的概念与方法	149
第二节 公路基础设施全生命周期管理的不同阶段	149
第三节 存在的问题及相关建议	150
第四节 公路基础设施全生命周期数字化管理解决方案	151
第五节 公路基础设施全生命周期管理的意义	153

第二十五章 数字化路网事件管理系统建设思路

第一节 标准规范建设体系	154
第二节 数字化路网事件管理系统总体架构	156
第三节 数字化路网事件管理业务流程	156
第四节 数字化路网事件管理系统功能设计	157
第五节 数字化路网事件管理的意义	159

03 云上机场 数智启航

第二十六章 机场上云、用云、云数融合思考与实践

第一节 对机场云的思考与理解	161
第二节 机场云建设解读	162
第三节 新华三机场云解决方案优势	165
第四节 某国际机场云平台实践	166

第二十七章 构筑机场集团“一朵云”，打造一云统管、资源共享、统一高效的数字底座

第一节 机场集团“一朵云”建设分析	168
第二节 新华三机场集团“一朵云”解决方案	169
第三节 广东机场集团“一朵云”案例实践	171

第二十八章 聚、治、融、享，高可信数据中台助力智慧机场建设

第一节 数据中台是机场突破数据瓶颈迈向智慧型机场的关键	172
第二节 聚焦“聚、治、融、享”，打造高可信数据中台体系	173

第二十九章 机场AIGC应用场景探讨	
第一节 AIGC正在成为数字科技的新变量	177
第二节 AIGC+机场：探索智慧机场发展的新方向	178
第三节 聚力同行，新华三以科技力量助力机场行业AIGC建设大放异彩	183

第三十章 “智慧墙”打造新一代机场飞行区周界安全防护系统	
第一节 传统周界安全防护技术流派对比及适用场景分析	184
第二节 新一代周界安全防护技术引领行业发展	185
第三节 新华三“智慧墙”新一代周界安全防护解决方案	186
第四节 机场智慧墙项目实践	188

第三十一章 机场物联网解决方案及案例实践	
第一节 传统机场物联网建设模式分析	189
第二节 新华三机场物联网解决方案	190
第三节 杭州萧山国际机场物联网案例实践	193

第三十二章 智能网络解决方案打造融合可信、畅通无阻的机场信息化“跑道”	
第一节 SDN：软件定义，融合统一	196
第二节 SRv6：极简部署，灵活编排	198
第三节 网络分片：带宽保障，一网多用	200

第三十三章 行业专属路由器助力智慧空管建设	
第一节 安全与创新之间需要平衡点	202
第二节 空管特性业务IP化分析	203
第三节 新华三空管特性专用路由器，助力空管业务IP化转型	206
第四节 空管智慧化业务新方向探讨——确定性网络技术	208

04 云端列车 智通四海

第三十四章 探索铁路下一代承载网发展趋势	
第一节 铁路5G承载网络技术分析	212
第二节 数据通信网与5G-R承载网络融合部署探索	218

第三十五章 铁路综合视频监控新标准实践分析	
第一节 现状分析	222
第二节 综合视频监控系统建设目标	223
第三节 综合视频监控管理节点关键技术应用	224

第三十六章 从“中国智慧”到“中国速度”，以云服务助力雅万高铁数智求变	
第一节 拥抱数字化，引领六大核心业务系统加速上云	235
第二节 链接未来，为智慧高铁升级进化构建扎实底座	236

第三十七章 京广高铁（武汉）综合视频一体化云平台	
第一节 铁路综合视频一体化云平台解决方案	237
第二节 方案价值	238

05 云港联动 智慧领航

第三十八章 新型数字化技术在智慧港口的应用浅析	
第一节 当前港口发展现状	240
第二节 智港口的建设目标及整体框架	241
第三节 新型数字化技术在港口的应用	242

第三十九章 浅谈双碳背景下智慧绿色港口建设之路	
第一节 双碳背景	248
第二节 如何降低港口碳排放	249
第三节 建设智慧绿色港口的关键技术和应用	251

第四十章 浅析人工智能在港口安全应急的应用	
第一节 当前港口应急遇到的痛点	255
第二节 人工智能助力打造港口智慧安全立体防护网	255
第三节 人工智能在港口安全应急场景中的应用价值	258

第四十一章 数智赋能航道 安全与效率齐升	
第一节 智慧航道概述	260
第二节 新华三智慧航道解决方案	262

06 行业探索

第四十二章 全新视角下的IPRAN	
第一节 IPRAN的前世今生	270
第二节 IPRAN技术演进	271
第三节 主流无线承载网技术对比	274

第四十三章 AIGC时代，核心算力基础GPU技术与应用场景解读	
第一节 GPU需求背景	277
第二节 GPU计算技术详解	277

第四十四章 AIGC在交通规划领域的应用探讨	
第一节 AIGC概述	284
第二节 交通规划领域的“老大难”问题	285
第三节 用AIGC预测城际出行交通方式	286

01

云城轨，智行远

第01章	探索城轨IPRAN骨干承载网新应用	02
第02章	智慧城轨无线通信系统发展趋势	07
第03章	城市轨道交通5G专网通信应用探讨	12
第04章	Wi-Fi与IoT创新融合，构建城轨智能运维体系	19
第05章	TSN在城轨行业的应用展望	23
第06章	扎实基础，创新延续：新华三如何定义下一代城轨云？	29
第07章	城轨云“和而不同”的发展之道	34
第08章	构建城轨边缘数字底座解决方案	39
第09章	城市轨道交通云容灾技术分析	49
第10章	基于云平台的城轨信号系统建设探索与思考	60
第11章	城轨云安全体系建设研究	65
第12章	城市轨道交通云平台安全资源池最优方案探讨	75
第13章	城轨云平台商用密码应用安全性评估及建设	87
第14章	城轨数据中心液冷技术发展浅析	94
第15章	四大集约化助力绿智城轨发展	102

探索城轨IPRAN骨干承载网新应用

文/刘杰

当前城轨行业通信系统骨干承载网建设主要以MS-OTN或PTN/SPN两大技术路线为主，但随着城轨业务系统的不断演进及业务数据模型的不断变化，传统传输技术体系在应用中也显现出一些弊端。

从业务维度审视，当前城轨行业的业务系统基本已经全部完成了IP化演进，当前城轨骨干承载网基本不再需要传统的E1接口和TDM数据的承载能力。传统的传输技术方案均保留了TDM业务的承载能力，从而导致设备成本较高。

从技术维度审视，传输技术封闭性较强，兼容异构能力低，业务编排与规划基本以手工方式为主，缺乏自动化编排和部署的能力。在后期运维阶段缺乏智能化的运维手段，对运维人员的专业技能要求较高。

从市场维度审视，由于技术的封闭性导致城轨行业传输市场完全被少数厂商垄断。由于传输系统无兼容异构能力，各家厂商设备均不支持异构组网，极易导致最终用户被设备厂商绑定，大大降低了最终用户的议价能力，投资成本往往居高不下。

一、城轨骨干承载网技术演进趋势

标 题：工业和信息化部等八部门关于推进IPv6技术演进和应用创新发展的实施意见
发文机关：国家发展和改革委员会；工业和信息化部；交通运输部；人民银行；国务院国有资产监督管理委员会；国家能源局；教育部；国家互联网信息办公室

发文字号：工信部联通〔2023〕45号

来 源：工业和信息化部网站

主题分类：工业、交通、信息产业（含电信）

公文种类：意见

成文日期：2023年04月20日

工业和信息化部等八部门关于推进IPv6技术演进和应用创新发展的实施意见

工信部联通〔2023〕45号

各省、自治区、直辖市通信管理局，各省、自治区、直辖市及新疆生产建设兵团工业和信息化主管部门，党委网信办、发展改革委、教育厅（教委、局）、交通运输部（委、局），铁路局，人民银行上海总部、各分行，有关中央企业、中央金融企业、工业和信息化部直属高校；

按照《中央网络安全和信息化委员会办公室 国家发展和改革委员会 工业和信息化部关于加快推进互联网协议第六版（IPv6）规模部署和应用工作的通知》（中网办发〔2021〕15号）要求，为加快推进IPv6技术演进和应用创新发展，赋能数字中国建设，现提出以下意见。

2023年4月工信部发布《工业和信息化部等八部门关于推进IPv6技术演进和应用创新发展的实施意见》。文件中明确指出“要求政务、金融、能源、交通、教育、制造等行业和领域，在IPv6规模部署基础上实现‘IPv6+’技术的广泛应用”。“IPv6+”即指在IPv6网络的基础上引入分段路由（SRv6）、网络切片、随流检测、应用感知网络（APN）和网络智能化等新型技术。交通行业作为IPv6+落地的重点行业，网络的智慧化转型需求迫切。

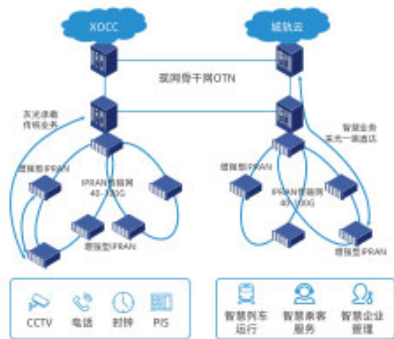
二、IPRAN技术挖掘城轨骨干传输网络新价值

城轨云已经成为当前智慧城轨建设标配，云化建设模式下的云网联动、云边协同催生了算力自动化调度的需求。业务系统已经全面拥抱IP化，需要一种更贴近IP化技术的承载方案。同时现阶段城轨骨干承载网建设也越来越看重技术的开放性、不同厂商间的设备异构兼容能力。具有更强开放性的技术方案可将引入更多的厂商共同构建良性的市场竞争环境，让客户有更多的选择和更强的议价能力。

基于上述需求，城轨IPRAN骨干网承载方案应运而生。IPRAN方案目前还未规模应用于城轨行业，但IPRAN技术本身已经非常成熟，被运营商行业应用多年，是标准的无线回传骨干网方案，其业务承载能力、网络可靠性、网络保护能力、自动化编排能力指标均可满足城轨业务的承载需求。

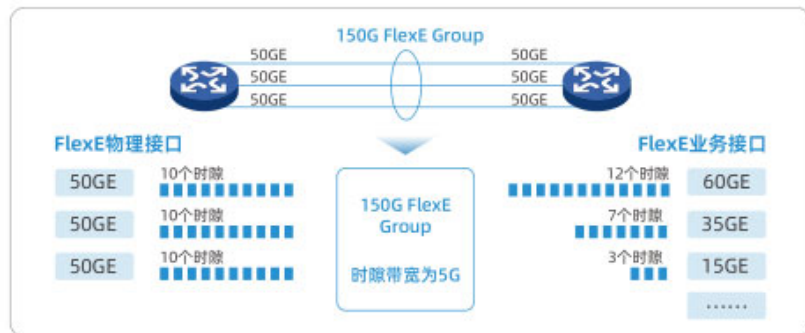
1. IP+光提供超宽业务承载能力

城轨IPRAN骨干网承载方案可支持灰光、彩光两种承载能力。对于城轨传统业务，数据流向为车站-车站、车站-控制中心，站间数据交互较多，更适宜用灰光承载。而随着城轨智慧化发展，越来越多的智慧业务未来都会引入到城轨行业，这些智慧类业务往往会围绕5G、AI、大模型等新技术构建。此类业务数据量较大，对骨干承载网的传输能力需求大幅提高。IPRAN方案的彩光承载能力通过DWDM密集波分复用技术，可在单根光纤中可同时传送多达80个100G波道，在不增加光纤资源的前提下近乎无限制的提升网络带宽。



2. FlexE技术实现业务物理隔离

城轨骨干承载网承载业务系统众多，各业务系统间均要求具备一定的隔离度，以避免不同业务数据抢占传输通道。城轨IPRAN承载网方案引入了FlexE技术，在以太网基础上通过时隙交叉技术和端口捆绑技术提供低成本、可动态配置的电信级接口。既保留了以太网技术的低成本、高可靠、灵活运维的优势，还具备了多粒度速率灵活可变、业务间硬隔离等特性。当前城轨行业主流骨干承载网带宽为100Gbps，通过FlexE技术可以实现骨干传输通道中切分出最小为10Mbps颗粒度的刚性传输通道，保障业务数据互相隔离，同时也满足了城轨场景小带宽业务的承载需求，提高整体带宽利用率。




3. SDN引入智能化的业务编排和运维能力

IPRAN方案基于以太网技术，支持引入SDN的能力实现业务、流量的自动化编排。基于SDN控制器可以支持更细粒度的运维能力，传统传输体系主要关注链路的质量，而基于以太网的IPRAN方案则在关注链路质量的同时还可以实时反应业务的传送情况，通过iFIT技术可跟随业务的报文对网络质量进行实时监测，可以反映出网络的真实丢包率和时延等性能参数。通过SDN的引入不但大大降低了业务规划的工作量，还从多维度为运维人员提供了更多的网络状态信息，更有利于保障网络的可靠性和稳定性。

4. 基于SRv6的完善保护机制保障网络可靠性

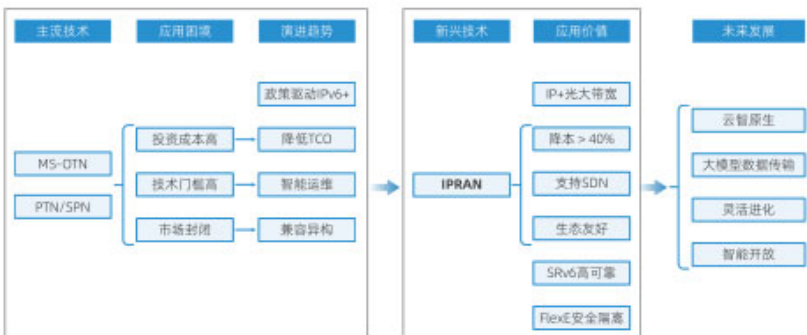
城轨行业对网络稳定性、可靠性要求极高，在骨干承载网建设时要求具备完善的网络保护机制，一旦出现网络的故障则要求在极短的时间内完成保护链路的倒切，避免出现业务的中断。传统的IP化网络在出现网络故障时均需要进行路由收敛计算，一旦涉及到计算过程则

收敛时间就会受链路节点数量影响，往往节点越多，则链路倒切时间越长。IPRAN方案底层基于SRv6技术，通过TI-LFA可支持任意拓扑的链路和节点保护，当某处链路或节点故障时，流量会快速切换到备份路径继续转发，从而最大程度上避免流量的丢失。TI-LFA会预先计算出备份路径，某处链路或节点发生故障时，通过SID列表显式指定备份路径，将流量快速切换到备份路径继续转发。完全不需要在链路故障时进行路由的计算，所以IPRAN方案的链路倒切时延并不受链路节点数数量影响。中国信通院测试报告中显示可在20ms内完成故障链路的倒切。

测试拓扑	
测试步骤	<ol style="list-style-type: none"> 1. 按照如上测试拓扑搭建测试环境，配置相应IP地址及IGP协议，实现路由互通 2. 创建VPN实例，配置SRv6 SID相关参数，配置IGP协议发布Locator 3. DUT1、DUT4作为L3VPN PE配置MP-IBGP邻居，与测试仪相连的端口绑定VPN，仪表A、B口模拟CE，接入VPN，配置链路COST使DUT1上不能形成到DUT4路由的PRR，R-LFA，使能GP TI-LFA 4. 查看MP-IBGP邻居状态，查看路由备份情况，测试仪A、B高发流量，有预期结果1 5. 模拟故障，观察流量，有预期结果2
预期结果	<ol style="list-style-type: none"> 1. 步骤4中，邻居状态已建立，有备份路由，流量无丢包 2. 步骤5中，切换后流量无丢包，记录收敛时间
测试结果	符合预期，通过 收敛时间：16.41ms

5. IPRAN方案相比传统传输方案投资规模降低40%

现有传输体系技术方案的技术封闭性较高，不具备兼容异构的能力，极容易形成用户与设备生产厂商的绑定关系，也因此导致了传输网络建设的成本居高不下。反观IPRAN方案，由于其基于以太网为底层技术，开放性非常强，市场竞争积极而和谐。良性的市场竞争也推动了解决方案，提供商不断优化方案，为客户提供更具性价比的解决方案。再加之IPRAN方案引入的SDN能力从业务规划和网络运维层面，全面提升了城轨骨干承载网的智能化水平，从运维层面也实现了降本增效。



承载网技术演进IPRAN成交通行业最佳选择

结语

未来的城市轨道交通一定是“云智原生”的，各个业务系统基于云生出智慧。城轨系统内的云、边、端纵向交互和业务系统间的横向交互纷繁复杂，业务的快速迭代，数据流量模型的不断变化，要求骨干承载网也能够灵活敏捷的满足业务承载需求。基于SRv6、FlexE等技术的IPRAN骨干承载网堪称专为业务快速变化的场景打造，同时基于iFIT等智能化的检测技术也可以提升运维的智能化水平，在成本方面得益于技术的开放性最大限度降低了客户的投资规模，更加智能、更加灵活、更加开放的IPRAN骨干承载方案应用将是轨道交通行业发展的必然趋势。



智慧城轨无线通信系统发展趋势

文/李婧

伴随着《中国城市轨道交通智慧城轨发展纲要》和《中国城市轨道交通绿色城轨发展行动方案》的发布，城市轨道交通行业各类智能化、绿色化的应用进入快速发展阶段，对于无线通信网络的需求越来越高。本文分析了智慧城轨无线业务需求、无线通信系统发展现状，旨在从不同角度探索智慧城轨无线通信发展趋势，助力智慧城轨高质量发展。

一、背景介绍

中国城市轨道交通协会在2020年3月印发《中国城市轨道交通智慧城轨发展纲要》，纲要明确提出了智慧城轨的定义：应用云计算、大数据、物联网、人工智能、5G、卫星通信、区块链等新兴信息技术，全面感知、深度互联和智能融合乘客、设施、设备、环境等实体信息，经自主进化，创新服务、运营、建设管理模式，构建安全、便捷、高效、绿色、经济的新一代中国式智慧型城市轨道交通。智慧城轨是利用新兴信息技术集成城轨交通各系统和集成各类服务的结晶，是城轨交通领域信息化建设进入新阶段的集中体现，因而信息化建设是智慧城轨建设的核心和基础。

无线通信是利用电磁波信号对可以在自由空间中传播的特性进行信息交换的一种通信方式。城市轨道交通的车地无线系统是支持业务系统运行中重要的通信系统，城市轨道交通行业各类智能化、绿色化的应用进入快速发展阶段，对于无线通信网络的需求越来越高。

二、智慧城轨无线业务类型

城轨车地无线承载的业务主要包含信号系统和PIS乘客信息系统、IMS视频监控等业务系统。信号系统是列车安全、精准运营的基础，与PIS、IMS等业务系统均为城市轨道交通重要的通信基础设施，其系统性能直接影响到运营的效率 and 乘客的体验。

城轨车地无线系统主要承载的业务类型如下：

列车运行控制业务

列车运行控制是列车的间隔控制，是以保障行车安全与效率为核心的系统。根据自动运行

的程度，可以分为四个不同的等级GOA1、GOA2、GOA3、GOA4。

列车紧急文本下发业务

列车紧急文本是指地面PIS服务器传送给车载PIS终端的紧急文本信息。

列车运行状态监测业务

列车运行状态监测业务是指列车运行状态实时监测系统，它主要是将传感器采集到的列车关键参数实时传送到地面监测中心，列车运行状态监测业务为周期性数据。

IMS视频监控业务

IMS视频监控是指将列车驾驶室、列车车厢的视频监控图像通过无线的方式实时传输到控制中心或地面监控站，进行集中监控。

PIS视频业务

PIS视频业务是指由地面将视频或图像信息通过组播传输到车厢内播放。

三、智慧城轨无线通信系统现状

截至目前，国内无线通信网络用到的技术包括WLAN、LTE-M、TETRA、物联网IoT、5G等。地铁车地无线通信系统目前所涉及的主要技术有如下几种：

WLAN

WLAN车地无线通信网络采用工作在开放频段，通过公共开放的非授权频段，实现轨道交通的无线覆盖。城市轨道交通无线网络作为有线网络的补充，提供列车与地面的通信。随着Wi-Fi 6技术和产品的成熟，从2020年开始新建线路主要以Wi-Fi 6为主。WLAN方案的组网包括轨旁和车载两部分，PIS系统中基于WLAN的无线通信，由车载AP经过车地通信网络与轨旁AP完成通信，车头车尾的2台车载AP进行冗余，实现主备通信。

TETRA

TETRA数字集群通信系统是欧洲通信标准协会为了满足欧洲各国的专业部门对移动通信的需要而设计、制订的统一标准的开放性系统。地铁无线通信采用800MHz频段的TETRA数字

集群系统为地铁运营的控制中心人员、车辆段人员，以及车站维护人员提供可靠的语音和数据交换，是重要的通信手段，保障列车的安全行车，提高地铁的整体运输效率以及改善地铁的服务质量，大幅提高地铁运营管理水平。

LTE

LTE是第四代无线移动通信技术，采用更大的载波带宽，并以OFDM与MIMO为基础，致力于降低传输时延、提高传输速率、提升系统带宽容量和增强网络覆盖范围。我国行业专网采用TDD制式，即TD-LTE。TD-LTE行业专网是相对于运营商建设的移动通信公众网络而言的，所谓LTE行业专网即各个行业用户根据自己的使用需求而建设的独立的、私有的TD-LTE制式的无线网络。

LTE-M标准是为了满足轨道交通行业综合承载业务需求，在3GPP、B-TrunC等标准基础上为轨道交通行业定制化的行业标准。LTE-M基于TD-LTE制式，在满足CBTC业务数据传输的同时，还支持列车运行状态、集群调度业务等信息的综合承载。

5G

5G技术具有大带宽、低时延、广连接的特性，可以为城市轨道交通提供所需的无线通信带宽，成为LTE-M系统的有效补充，助力绿色智慧城轨高质量发展。目前中国城市轨道交通协会组织编制的《城市轨道交通 5G公网》系列团体标准，提出基于运营商5G公网，利用网络切片技术，提供专属网络能力，承载轨道交通相关数据业务，覆盖轨道交通全场景，实现5G公网专用。

物联网IoT

现有物联网业务多样化，不同的物联网终端厂家采用不同的物联网协议信号进行数据的交互，实现数据实时采集、人员/设备定位、实时感知预警、资产实时定位等作用。常用的物联网采用2.4G RFID、BLE和UWB、ZigBee等物联网协议。目前的物联网也支持无线控制器管理，WLAN和物联网产品融合管理，统一设备管理平台，简化用户管理难度。

四、智慧城轨无线通信系统发展趋势

当下，城市轨道交通行业各类智能化、绿色化的应用进入快速发展阶段，对于无线通信网络的需求越来越高。车地无线支持高速移动、高可靠、低时延、跨线运营，互联互通。

1. LTE-M高可靠保证列车运行安全

根据轨道交通行业业务需求现状和无线通信技术发展趋势，与轨道交通生产安全相关的列车运行控制业务由LTE-M系统承载。目前在建城市轨道交通线路CBTC系统均已采用LTE-M技术，宽带集群采用LTE-M技术也已经成为发展趋势。城市轨道交通建设和运营正在从单线向互联互通发展，为满足日益增长的跨线和并线运营的要求，不同线路的信号系统需要通过互联互通实现对列车的调度控制。目前轨道交通领域内已有对于铁路信号系统互联互通实现和测试方法、城市轨道交通CBTC系统互联互通实现方法的研究。作为城市轨道交通CBTC系统的业务承载网络，LTE-M系统互联互通是实现CBTC业务互联互通的前提。

LTE-M互联互通包括数据业务的互联互通和宽带集群业务的互联互通，相比数据业务互联互通只在轨道交通列车跨线、共线或者延伸线场景中被需要，集群业务互联互通应用要广泛得多，在换乘站、控制中心等都需用到。LTE-M宽带集群互联互通标准是以B-TrunC2.0标准为基础进行深度行业定制，在本地组网的基础上，支持跨核心网的规模化组网，实现统一管理用户数据、支持本地网之间的互通，以及在不同本地网之间漫游等功能，从而为城市轨道交通特定业务提供支撑。

2. 城轨5G公网仍试验探索

智慧城轨无线业务的需求还有很多：涉及智慧乘客服务的PIS业务、智能列车运行的列车大数据业务、智能运维安全的视频监视业务和检修业务等。这些智慧城轨无线业务数据量大，传输数据速率高，因LTE-M系统带宽受限，需其他无线技术手段来解决。WLAN技术和5G技术是一种选择。但因5G技术在城轨行业上还处于试验和探索阶段，针对城轨行业5G公网专用的切片技术、商业合作模式、相关技术标准均还不完善。目前中国城市轨道交通协会组织编制《城市轨道交通5G公网》系列团体标准，提出5G公网承载的业务应包含：集群调度业务、列车运行状态监测业务、车载信号运维数据业务、车辆健康管理业务、列车紧急文本下发业务、PIS视频业务、数据采集类业务、轨行区综合巡检业务、车辆基地综合维修业务、信息管理业务、IMS视频监控业务等。

3. WLAN+IoT物联网融合，助力城轨智能运维

以智慧城轨为建设背景，城轨智慧无线可以提高运维效率、降本增效，为城轨行业的绿

智融合提供业务承载通道。智能运维体系中需要实现后端智慧业务平台与前端运维人员的实时通信，运维人员的智能终端设备需要无线接入服务。接入网及物联网的建设目标就是为了给各类智慧业务提供数据交互的通道，实现智能终端与业务后台之间的实时交互。对运维作业人员进行高精度定位，实时了解运维人员的位置信息。

与运维相关的智慧类业务会不断的向城轨行业拓展，无线网络建设的两个大方向：一个是实现各类终端的无线接入，一个是通过物联网或Wi-Fi网络实现高精度定位。接入网及物联网的建设目标是为了给各类智慧业务提供数据交互的通道，实现智能终端与业务后台之间的实时交互。WLAN+IoT物联网融合，可以充分利用Wi-Fi方案与IoT方案的融合能力，在站厅站台区域通过AP设备下挂物联网基站满足接入和定位需求，在轨行区则利用PIS系统建设的轨旁AP设备下挂物联网基站满足接入和定位需求。轨旁AP在提供MESH服务的同时还开启接入服务，在车辆运营结束后运维人员可在轨行区实现手持终端的Wi-Fi接入。

结语

城市轨道交通安全、高效的运营，需要一个庞大且功能完善的通信网络为之服务。智慧城轨无线通信系统在列车运行控制、维修指挥和客流疏导等工作中发挥着重要的作用。无线通信系统为城市轨道交通内部的固定工作人员和运营指挥人员提供了高效的数据及语音的通信。

城市轨道交通行业各类智慧化、绿色化的应用对于无线通信网络的需求越来越高。车地无线通信系统要求支持高速移动、高可靠、低时延、跨线运营，互联互通等特点。信号系统LTE-M将长期存在，除了因为地铁列车自身运行高安全可靠的要求，另外还要考虑CBTC本身的互联互通问题。LTE+5G公网是地铁车地无线长期存在的两种技术路线，LTE-M承载与列车运行直接相关的业务，5G作为补充LTE-M未来可能承载智能终端的视频大带宽业务。面对目前的智能运维，智慧乘客服务，WLAN+IoT物联网融合，接入网及物联网的融合，则可以给各类智慧业务提供数据交互的通道，实现智能终端与业务后台之间的实时交互。

城市轨道交通5G专网通信应用探讨

文/李婧

5G是第五代移动通信系统的简称，ITU为5G定义了eMBB增强型移动带宽、mMTC海量物联网通信和uRLLC超高可靠与低延时通信三大应用场景。5G的愿景与需求是满足未来爆炸性的移动数据流量增长、海量的设备连接、不断涌现的新业务和应用场景，满足垂直行业终端互联的多样化需求，实现人人、人物、物物通信的真正“万物互联”。

本文探讨了5G技术在城市轨道交通中的应用需求，针对业务与应用需求，分析了城轨5G发展背景、运营商5G专网建网模式、城轨交通5G专网通信应用存在的问题，旨在从不同角度推动探索5G在城轨行业的应用，助力智慧城轨建设和城轨行业高质量发展。

一、背景介绍

近年来，国家明确提出要加快“新基建”，发展以5G、人工智能、工业互联网为代表的新一代信息基础设施，通信基础设施中将5G置于首位；国家战略中的5G为城轨行业带来了新的发展机遇，城轨交通行业也在大力发展轨道交通与传统行业的深度融合，5G在城轨的探索和实践，旨在建设智能交通等融合基础设施。

中国城市轨道交通协会在2020年3月印发《中国城市轨道交通智慧城轨发展纲要》，纲要明确提出强力推进云计算、大数据、物联网、人工智能、5G等新兴信息技术和城轨交通业务深度融合，推动城轨交通数字技术应用，推进城轨信息化，发展智能系统，建设智慧城轨。

国家战略中的5G为城轨行业带来新的发展机遇。在新基建背景下，5G是城轨行业实现“十四五”规划中高质量发展的重要途径。《交通强国建设纲要》更是明确提出要瞄准新一代信息技术、智能制造等世界科技前沿技术，加强有可能引发交通产业变革的前瞻性、颠覆性技术研究。毫无疑问，5G是推动新一轮城轨通信产业变革的重要角色。

5G低延时、高带宽、广连接的特点将为城轨应用场景的不断丰富提供强有力的支撑，5G技术赋能城轨网络将是一个革命性的改变，然而如何把5G网络能力赋予城轨专网通信，5G如何助力智慧城轨建设运营，却依然是目前电信运营商、设备商及行业客户等共同探讨的话题。

二、城市轨道交通5G专网通信场景及应用需求

5G通信技术在城市轨道交通中的应用将有力推动城市轨道交通朝着更加自动化、智能化方向高速发展。相比于4G网络，5G在继续提升人与人之间通信服务质量的基础上，更侧重于满足物与物之间的通信服务需求，致力于实现“增强宽带、万物互联”，从而保障未来新型信息产业的发展。5G无线网络为了满足不同业务对带宽、时延、可靠性、连接数、吞吐量和移动速度等多样化需求，必须打破传统，设计一种新的、灵活的网络架构。5G从技术上使用新的编码方式、更宽的无线频谱、波束赋形、大规模天线阵列、超密集组网、新型多址，SDN/NFV、边缘计算、网络切片等全新技术。未来的地铁无线通信系统必须具备更多样化的性能保证以承载各种新兴业务，从而促进工业化和信息化的深度融合。5G的三大特性可以结合地铁典型业务场景进行深度融合，5G的特点就是最好的支撑架构，能够给轨道交通带来无限可能。

低时延

通过5G实现高速行驶下的列车信号控制系统通信，列车最高级别的全自动运行、车-车通信，使得整个列车控制的时间更短、列车行驶间隙更短，实现状态信息的高效传输，提升高速列车运行稳定性与安全性，大力提升运营效率。

海量连接

将轨道的设备传感器、各类智能传感器通过物联网整体接入联网，更实时地监控到全轨道状况，解决危险事件的发生，满足大规模通信设备连接需求。

大带宽

5G+云+AI，基于5G技术实时传输高清视频、虚拟现实等海量数据，实时监控车辆内部、车厢内部的紧急情况；通过AI实现智能识别，代替人工巡检，实现智能运维，提高运维效率，构建物与物、人与物、人与人相互沟通。

三、运营商垂直行业5G专网组网方案

由于工信部目前只向四大运营商颁发了5G频谱，所以国内各垂直行业使用5G专网时并不能像WLAN非授权频率一样自主采购设备建设，故垂直行业专网必须通过运营商建设并使用运营商的频率。5G赋能垂直行业是各大运营商在5G时代的重要战略之一。

各大运营商分别推出了针对垂直行业的5G专网模式，根据不同应用场景和用户需求，垂直行业专网包括三种组网方式。

5G专网部署模式	中国移动	中国电信	中国联通
<ul style="list-style-type: none"> 与公网完全共享 与公网部分共享 独立部署 	<ul style="list-style-type: none"> 优享模式 专享模式 尊享模式 	<ul style="list-style-type: none"> 致远模式 比邻模式 如翼模式 	<ul style="list-style-type: none"> 5G虚拟专网 5G混合专网 5G独立专网

图1 运营商专网部署模式对比

运营商5G面向垂直行业的三大建网模式分别是虚拟切片、虚拟切片+边缘计算和物理专网，探索各自的5G公有频谱的专网化的新道路。

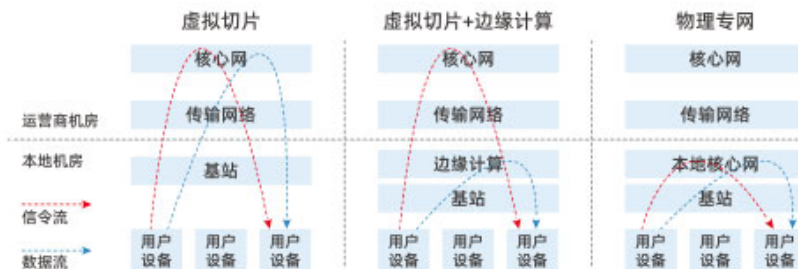


图2 运营商提供垂直行业三种可选组网方案

1. 虚拟切片

5G时代业务需求多样，对延迟、吞吐量、容量、可用性和安全隔离性有不同的要求。网络切片提供了一种解决方案，在相同的网络基础设施下，通过切片满足各业务的要求。5G的网络切片技术，则主要针对不同的业务应用，进行网络资源的切片化处理，在网络结构上也完全类似于一张独立的专网。

虚拟切片组网，对应中国移动的“优享”、中国电信的“致远”及中国联通的“虚拟专网”。将运营商5G大网通过网络切片方式划分出部分虚拟资源用于不同的垂直行业用户，各个切片用户和公众用户使用同一套物理资源，但在逻辑上是独立的，通过业务逻辑隔离，满足客户对特定网络速率、时延及可靠性的优先保障需求，支持按需灵活配置。

优势：成本低、业务开通速度快。

5G网络提供商可以为城轨行业及其他不同行业应用在共享的网络基础设施上，通过能力开放、智能调度、安全隔离等技术分别构建彼此隔离的5G网络切片，提供差异化的网络服务。

2. 虚拟切片+边缘计算

虚拟切片+边缘计算，对应中国移动的“专享”、中国电信的“比邻”及中国联通的“混合专网”。将运营商5G大网通过网络切片方式划分出部分虚拟资源用于不同的垂直行业用户，同时部署边缘计算设备将行业用户数据流本地卸载，只有信令流进入运营商大网，数据流本地处理。通过边缘计算技术，实现数据流量卸载、本地业务处理，满足数据不出场、超低时延等业务需求，为客户提供专属网络服务。

优势：数据流本地处理，安全性提高，端到端时延减小。

实现5G MEC取决于一个关键设备角色，即5G核心网的用户面网元UPF。5G核心网采用服务化网络架构和SDN/NFV技术实现网络重构，将控制面功能（包括AMF和SMF等）和用户面功能（UPF）分离。作为5G数据处理和转发的核心，UPF常被形象地比喻为5G用户数据流量接入行业客户网络的“桥梁”、运营商拓展5G ToB市场的“钥匙”。

城轨专网私有数据流通过私有切片传递到城轨私有UPF；公网数据流通过公网切片传递给电信运营商边缘云中的UPF。城轨内部控制数据、视频数据等保留在城轨行业内部，公众语音和互联网公共网络数据流则被传输至电信运营商的网络中。MEC边缘计算将数据缓存能力、流量转发能力与应用服务能力进行下沉，网络位置更接近用户，能够大幅降低业务时延，满足轨道交通应用场景中低时延业务需求，减少对传输网的带宽压力，降低传输成本，提升用户体验。同时，采用5G MEC可实现地铁业务数据不出本地，提高地铁数据安全性。

3. 物理专网

物理专网组网架构，对应中国移动的“尊享”、中国电信的“如翼”及中国联通的“独立专网”。运营商为垂直行业用户建设独立的本地轻量化核心网，针对行业终端的信令流和数据流都在本地处理，与运营商大网物理隔离。

通过对基站、频率、核心网等专建专享，为企业构建专用5G网络，提供高安全性、高隔离度的尊享定制化网络服务。

优势：数据安全性较高，时延低。这是城轨最理想的一种状态，对于生产型的数据、乘客数据是最优方式，时延也是最有保障的一种。

此种“物理专网”模式，新华三联合交控科技股份有限公司、北京移动，共同打造了“交控科技5G创新实验室”，进行了行业成功创新应用。中国移动向交控科技该行业客户提供了新华三的5G专网设备，在交控科技建设完整的5G网络，与5G公网完全隔离，专网专用，此种方式，控制面和数据面均在本地，对于城轨应用场景，对业务数据安全性及可靠性要求较高，5G独立专网是较为符合城轨应用场景的架构。

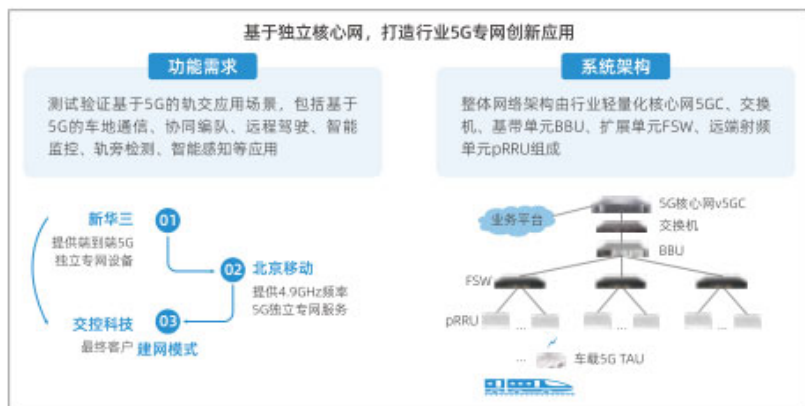


图3 交控科技5G创新实验室

新华三为该项目提供基于中国移动4.9GHz频段的5G专网整体解决方案，包括5G轻量化核心网v5GC、5G基带处理单元BBU、光口皮站扩展单元FSW、皮站射频拉远单元pRRU及相关配套软硬件产品，同时包含无线网络优化等服务，通过5G数字化室分实现交控科技大楼创新实验室区域内的无线信号覆盖，打造基于5G独立核心网的交通行业解决方案，验证实现5G轨道交通相关应用的创新解决方案，包括基于5G的车地通信、协同编队、远程驾驶、智能监控、轨旁检测、智能感知等应用，为推进5G网络在轨道交通领域的工程应用奠定基础。

四、城轨5G专网发展现状

1. 运营模式面临重构

原有的通讯承载方式已经形成了集成优势和成本优势，更换到5G，需要电信运营商、5G设备商和传统城轨系统制造商一起协作，协会通过引导和制定标准来推进。5G目前在轨道交通还处于起步阶段，5G产业可能会影响城轨原有的产业构造，一些系统可能会出局。新的一些潜在合作商，如一些互联网企业已经开始深度介入城轨领域发展，整个城轨格局和运用模式可能面临重构。

2. 城轨5G公网逐步推广

工信部目前只向四大运营商颁发了5G频谱，以地铁行业为代表的行业用户目前暂无5G行业专网频谱资源，只能依赖运营商的5G网络，即采用5G公网。目前中国城市轨道交通协会组织编制的《城市轨道交通5G公网》系列团体标准，提出基于运营商5G公网，利用网络切片技术，提供专属网络能力，承载城市轨道交通语音、数据等各类业务，覆盖城市轨道交通全场景，实现5G公网专用。多个城市也都在进行5G网络在城轨的应用探索建设。

3. 城轨上行业务带宽受限

城轨5G方案主要为公网专用，完全复用运营商的网络。城轨行业客户侧部署专用边缘计算节点进行数据分流。但这种方案业务承载能力受运营商5G大网业务模型影响较大，城轨受5G公网时隙配比策略影响承载能力有限，即上行带宽较低，与城轨行业客户的业务模型存在不匹配的问题。城轨行业客户的业务大部分均为上行业务，而公众用户大都是下行业务，导致5G公网方案上行能力有限，业务需要去适应5G网络的能力。

4. 产业链终端供给不足

5G在城轨的产业链终端还处在初级阶段，需要订制城轨行业的专用5G终端，切片、MEP等在轨道交通应用上也需一些时间，需要持续关注5G产业链的发展。目前国内轨道交通还没有5G专用频谱，要通过MEC边缘计算等跟运营商一起合作。如5G智慧维修传感器模块，因为需适应不同专业特点，差异化环境的产品还不够丰富。另外，5G模组目前价格较贵，针对智慧城轨需采用的大量5G终端模组，成本会较高。

结语

全球信息化变革以及通信技术的发展日新月异，从2020年5G在国内进入商用部署元年开始，5G网络建设成为新基建的热点，5G技术赋能城轨网络更是一个革命性的改变，5G技术在城轨交通中应用还有很长的路要走。5G技术不仅针对公众用户，而且要赋能各行各业，目前5G网络的建设主要由电信运营商来推动，但电信运营商对城轨行业并不完全了解，在推动行业专网应用上存在较大难度，因此，5G在城轨的应用不仅是技术问题，更是一个5G产业生态问题。

城轨5G公网专用对于城轨运营的安全和效率尤为重要，5G是面向垂直行业和运营商深度融合的网络，在安全性方面主要采用切片、边缘计算等技术来保证安全性和不同的服务等级要求，5G能否满足CBTC的要求还需进一步研究。另外，城轨5G公网和公众用户共享大网资源，在地铁乘客无线接入终端大幅增加时将对系统的承载能力及信息安全性带来极大压力。5G系统由于频率较高，无线信号的传输损耗也大幅增加，5G网络部署较为密集，无线系统的维护管理工作量将大幅增加。

作为地铁众多的无线通信技术之一，5G还需要进一步与城轨业务系统相融合，发挥其技术优势与特点。5G在城轨行业普及，需要业主、设计院、厂商、运营商等“产、学、研、用”强强联合，合理、高效地共同推进5G在城市轨道交通中的应用落地。



Wi-Fi与IoT创新融合 构建城轨智能运维体系

文/刘杰

随着我国城市轨道交通运营线网规模持续扩张，整个轨道交通行业对于保障运营安全、提高服务质量及降低运营成本需求愈发明显，同时对设施设备的可靠性、高可用性及安全性提出了更高要求。如此大体量的设备运维涉及到大量的人力投入及复杂的流程管理体系。而当前城轨行业运维管理体系仍然比较落后，仍存在大量以纸质工单、表格为载体的管理手段。管理流程也基本基于人工进行管理，缺乏自动化、流程化、信息化的管理手段。相对较为落后的管理手段也导致在管理流程中存在诸多安全隐患。

据中国城市轨道交通协会数据统计，每公里城轨投资约8亿元，根据行业经验，城市轨道交通运维支出占总投资的2%~3%。如何进一步提升运维工作的管理效率、降低运维成本成为城轨行业客户普遍关注的核心需求。新华三深刻理解用户需求，将Wi-Fi+IoT融合的无线网络技术与运维管理流程进行深度融合，实现了城轨运维管理的数字化变革。

一、城轨智能运维需求

城市轨道交通是复杂的系统，涉及车辆、信号、供电、通信、自动售检票等多个系统，包括众多子系统及产品部件，线网级的城轨系统设施设备的数量超过数十万台（套），零散分布于线网的延申区域，每天需要执行大量的运维任务，并且有大量的运维人员参与其中。传统的纸质任务工单管理模式效率低、问题回溯难。针对运维人员的管控精细度差，特别是在轨行区，运维人员基本属于“半失联”状态，针对运维工作进行中可能存在的风险无法做到及时感知。因此需要一套更加智能化的运维管理系统针对流程、工单、人员进行精细化管理，提高管理效率、降低管理难度、规避施工风险。

二、Wi-Fi与IoT技术结合改变传统管理手段

基于Wi-Fi与IoT网络的智能运维体系建设是基于两个维度，一个维度是建立人与智能业务系统的实时关联，第二个维度是实现运维人员的高精度定位，并结合智能运维平台与人员的位置信息进行运维管理。

建立人与系统的实时连接

通过宽带接入网实现运维人员的实时在线，将原有的纸质工单及流程体系全部进行数字化改造



实现人员的高精度定位

通过窄带物联网实时掌握运维人员的位置信息，基于位置信息实现运维人员的智慧化管理

智慧城轨运维管理体系建设两大维度

两大维度的应用需求主要通过Wi-Fi+IoT的宽带融合网络进行承载，其中Wi-Fi 6网络支撑海量终端接入的需求，充分发挥Wi-Fi 6网络的特性，在终端数量较多且频繁漫游的环境下提供更优异的接入体验。特别融合新华三自主研发的4i (iRadio、iStation、iEdge、iHeal) 技术在无线网络空口性能、漫游接入、应用保障、网络自动化等各个方面可以不断的深入优化网络，让无线网络更适应城轨行业的复杂环境。同时在宽带Wi-Fi 6接入网络之上融合窄带物联网技术，通过UWB方案实现运维人员的高精度定位，UWB技术以其较高的定位精度和低功耗特性著称，特别适合于城轨的站厅、站台、轨行区等地下空间部署。



宽带一体化融合网络架构

三、复用PIS系统轨旁AP实现轨行区的双网覆盖

轨行区是运维作业的集中区域，运维人员多，运维工作复杂，是需要进行高度精细化管理的区域。在轨行区域最优化的部署方式就是将IoT物联网网关与车地通信系统既有的轨旁无线AP设备进行融合部署，既满足了网络覆盖的需求，又提高了设备的使用效率，降低了投资成本。IoT物联网网关可支持灵活多样的部

轨旁AP与物联网
基站共址部署站厅站台采用
室内型物联网基站

署方案，满足轨行区较为苛刻的安装环境。在布线困难安装条件受限的情况下可考虑IoT物联网关与轨旁AP设备共站址的方案进行部署。每台轨旁AP下挂一台IoT物联网关，通过小型外置天线扩大UWB网络覆盖范围，在150米间隔部署的环境下仍可以实现5米的定位精度。

四、基于Wi-Fi+IoT的运维体系实现全流程自动化、智能化

如何将新技术与实际的业务应用需求结合是构建城轨智能运维体系的重点探索方向。新华三基于高精度的位置信息，为城轨行业客户开发了智能化的运维管理软件，贯穿了城轨运维工作的各个环节，同时实现了监督人员、管理人员、监管人员、作业人员等运维主体的有机整合。

1. 运维计划阶段

传统运维管理流程中在运维计划阶段往往存在大量的纸质台账、工单、记录，管理效率低下等问题。基于智能运维管理平台可以将原有的流程全部实现电子化，将原有的台账、工单等全部转化为电子流，不但大幅提高了运维管理的效率，还可以在计划阶段将每一项运维工作的人员配置信息、运维工作内容、运维作业区域进行精细化的编排。

在智能运维平台可以基于线路情况及每一项运维作业的工作内容，为每一项巡检任务绘制具体的作业区域，再将高精度定位终端与运维任务进行绑定，即可实现人员、区域、任务的精细化管理。同时需要针对每一项运维任务指定合理的告警规则，包括界内/界外告警、聚众告警、离群告警、徘徊告警、超员告警等。一旦出现与原运维计划不符的情况，管理人员可及时接收到告警信息。

2. 运维执行阶段

在运维执行阶段，作业人员首先在电子流程中完成运维任务的登记和确认。按照运维计划佩戴好定位终端，之后进入到计划好的作业区域进行运维作业，管理人员可以在智能运维平台实时监控作业人员的位置，通过智能运维平台与视频监控平台的对接，管理人员可以随时调取作业区域周围的视频终端实时调看作业区域的视频图像，在触发告警时也可以实现告警信息与视频监控的自动联动。对于一些重要的运维器材和仪器仪表也可以通过加装定位终端避免设备遗落在轨行区影响运营安全。

3. 运维评价阶段

当天运维工作结束后，可通过电子点名功能对所有定位终端的位置信息进行刷新，由于人员已经与定位终端进行了强制绑定，则可以通过定位终端的位置，确保人出清、车安全。运维平台会记录所有作业人员的行动轨迹，一旦发现运维遗留问题及安全性风险可对运维工作进行全流程的追溯，责任落实到人。

基于高精度位置信息的智慧运维管理流程



结语

网络化是智能城市轨道交通的基础条件和支撑平台，也是实现轨道交通资源共享和协同创新的重要途径。智能城市轨道交通将进一步利用云计算、物联网、移动互联网技术等，实现轨道交通系统的数据集成、信息互联、服务互通等功能。而融合的网络势必成为网络化建设的重要标准，Wi-Fi与IoT技术的融合是目前应用前景最广阔、生态链最完善、性价比最高的融合方案。特别是IoT能力，将赋予无线网更加广阔的应用空间，不但可实现高精度的定位功能，还可以利用声、光、热、电、力学、化学、生物、位置等传感器采集到各种需要的城市轨道交通信息。通过采集到的数据支撑智慧运维业务应用，实现轨道交通系统的自主学习、自适应调整、自我优化、自我诊断等功能，提高轨道交通的智能化程度和运营效果。

TSN在城轨行业的应用展望

文/童修品

TSN (Time Sensitive Networking, 时间敏感网络), 是IEEE 802.1工作组的时间敏感网络任务组制定的一组标准, 具有时间同步、延时保证, 以确保网络数据传输的时间确定性, 以及智能开放的运维管理架构, 可以保证多种业务流量的共网高质量传输, 兼具性能及成本优势。相较于传统网络的“尽力而为”传输, TSN可为网络中的业务传输提供确定性的时延, 被普遍认为是下一代网络的演进方向, 它将是未来汽车、轨道、工业4.0、电网、5G场景中的主要网络技术之一。城市轨道交通各业务系统传输的业务数据类型繁多, 对网络的要求差别较大。面对这种情况, 实际项目中或采用划分多个虚拟局域网, 或采用建设多张物理网络方式进行传输各类业务系统不同的数据。无论采用哪种方式, 对时延、安全性、可靠性以及建设成本都不能做到良好兼顾。利用TSN技术或许可以解决这一问题。

一、TSN技术简介

1. 发展历程



图1 TSN技术发展历程

2004年7月IEEE 802.3工作组提出为家庭以太网中的音视频业务提供精准时间同步、有界时延抖动和带宽保障等能力的技术研究, 之后该研究项目由IEEE 802.3迁移至IEEE 802.1, 并于2006年3月正式成立AVB任务组。

2012年, AVB更名为TSN, 标志着其应用方向不再局限于音视频业务, 而是面向对传输时延、丢包率等要求更严苛的工业控制等行业领域。

2015年, 互联网工程任务组 (IETF) 成立了确定性网络 (DetNet) 工作组, 致力于将TSN中开发的技术扩展到路由器, 这样在TSN中开发的技术就可以扩展到路由数据流。

2019年, 成立了汽车等更多的TSN行业应用工作组, 同时成为确定性网络的候选底层技术。

2. TSN主要功能特性

TSN技术不是一个协议标准, 而是由一族工作在MAC层的协议组成。在这些协议的支持下, 一方面TSN能够确保交换网络中的数据传输时延, 另一方面时间敏感数据流和非时间敏感数据流能够在同一网络中混合传输, 非关键负载的并行传输不会影响到关键负载的传输时延。按照其功能可以归纳为时钟同步、低时延、可靠性保证、资源预留4种。每一种功能特性都可应用在城轨通信网络。

网络特性	技术标准
时间同步	时间同步 (IEEE 802.1AS)
确定性低延迟	基于信用的整形器 (IEEE 802.1Qav3) 帧抢占 (IEEE 802.3br&802.1Qbu1) 流量调度 (IEEE 802.1Qbv1) 循环队列及转发 (IEEE 802.1Qch1) 异步整形 (IEEE P802.1Qcr) QoS保障 (IEEE 802.1DC)
高可靠性	帧复制 (IEEE 802.1CB) 路径控制 (IEEE 802.1Qca1) 流过滤 (IEEE 802.1Qci1) 时间同步可靠性 (IEEE P802.1 AS-Rev)
资源管理	流量预留协议 (IEEE 802.1Qat3) TSN配置 (IEEE 802.1Qcc2)

表1 TSN相关协议

时间同步: 为列车通信网络提供统一的时钟基准, 用于流量调度和提供时间服务, 为实现分布式功能同步提供支撑。实现时间同步的是IEEE 802.1AS协议, 它是TSN的核心协议, 也是实现其他协议功能的基础。而新华三在这一方面为用户提供“SyncE频率同步+PTP相位同步”的综合方案来实现高精度的时间同步, 精度可达到纳秒级别。

确定性低延迟：流量调度、循环队列及转发技术能够实现端到端的确定性传输，传输信息经过每个网络交换机的延时是在固定范围内的，保证控制信息传输延迟确定性。帧抢占技术可以保障紧急制动等安全控制数据的最高传输优先级和最低传输延迟。

高可靠性：帧复制实现交换机和终端站的冗余传输帧的识别与复制、重复帧识别和消除重复帧，能够实现无丢帧的线路冗余切换性能，支持环网线路冗余和并联线路冗余，为网络冗余提供统一的技术标准，解决目前各个厂家网络设备冗余协议不兼容的问题。相比传统的环网技术，节省了倒切的时间，进一步降低网络时延。

资源管理：TSN遵循SDN体系架构，配置从系统视角对TSN单元进行集中配置，按照网络承载的业务数据传输需求划分网络资源，进行网络性能计算分析。

TSN的研发重点是对网络数据链路层进行特性增强，为关键性的业务数据流提供确定的延时，进而保证流量的确定性。

二、TSN在城轨的应用

未来新一代的城轨运行系统整体采用“云-边-端”三层架构，实现车-车、车-地、车-云的控制协同和安全协同，实现任何车辆任何时间任何地点互联，将列车从单车智能过渡到列车/车队/车轨协同的多智能体智能。然而多智能体的协同需要城轨通信网络提供确定性的时延和可靠，才能真正提升新一代城轨运行系统的效率与安全性。城轨通信网络主要有车载网络和地面网络。目前城轨地面通信网络主要有信号系统独立建设的环网和其他多业务系统共用的通信传输网，本文主要讨论TSN是如何为信号系统地面网络和车载网络提供确定性的时延和高可靠性的。

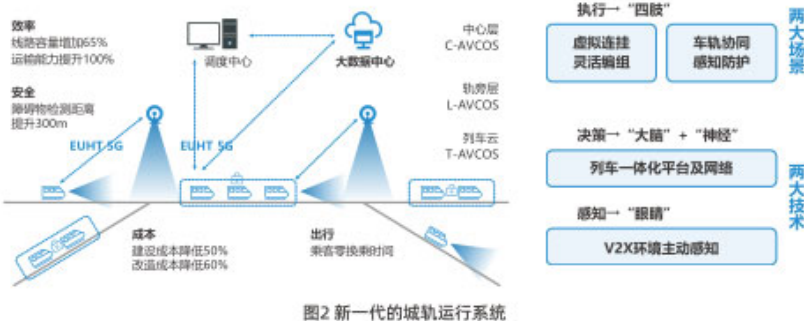


图2 新一代的城轨运行系统

1. TSN在信号系统地面网络的应用

信号系统地面网络的现状与需求

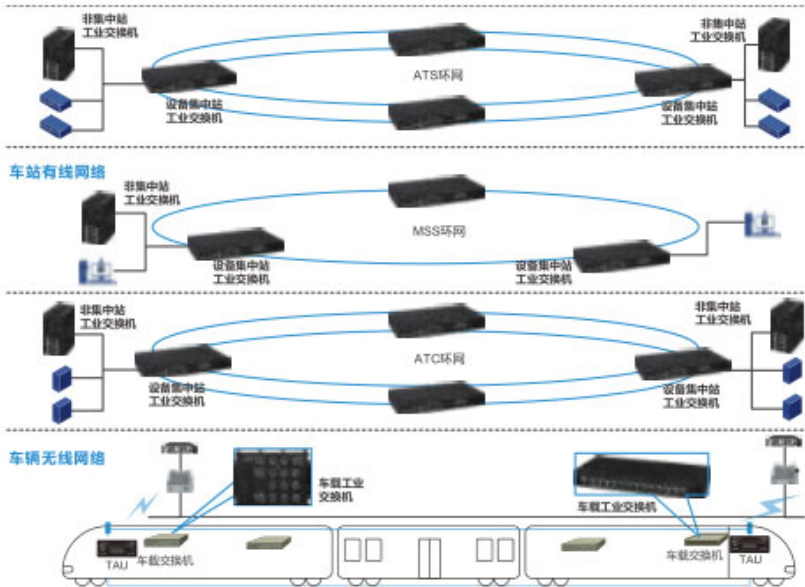


图3 城轨信号系统地面网络

目前城轨信号系统地面网络多采用五张独立的环网，或七环网，分为ATS双网、ATC双环网、无线双环网（五环网时与ATC网合并建设）和一张MSS环网。ATS、ATC等采用A/B双网冗余架构，其中A网单独用于信号系统控制数据的传输，B网用于控制数据的备份并传输语音、CCTV等其他业务。同时ATC环网或无线网业务需要支持1588V2时钟同步协议为信号各终端提供统一的时钟基准。信号系统之所以独立建设通信网络，且采用多张物理隔离的环网，就是因为传统以太网的“尽力而为”的传输模式无法保证业务低时延、高可靠、时钟同步的需求。多环网模式堆砌的可靠性、低时延也造成了网络建设成本较高，网络结构复杂。

同时，信号系统也在不断发展，未来车地通信可能采用5G技术来提供更低的时延，更大的带宽，需要车载和地面网络同步具有低时延、大带宽的特性才能充分发挥5G等新技术的优势，为未来新一代的城轨运行系统提供支撑。近年来，城轨信号系统厂家正在研究为信号系统各个终端设备建立实时数字孪生体，可以在后台实时掌握各终端的状态，及时发现因终端

设备问题带来的城轨运行安全隐患。以上的需求都需要城轨通信网络具有低时延、高可靠、大带宽、良好的兼容性等特性，如果采用传统以太网就略显能力不足。而遵循标准的以太网协议体系的TSN技术或许可以解决这些问题。

TSN在信号系统地面网络应用探讨

TSN网络中的流量调度、循环队列及转发技术能够实现端到端的确定性传输，传输信息经过每个网络交换机的延时是在固定范围内的，保证控制信息传输延迟确定性。帧抢占技术可以保障紧急制动等安全控制数据的最高传输优先级和最低传输延迟。基于IEEE 802.1Qbv或IEEE 802.1Qch标准的门控调度机制对特定标识的数据帧加以控制，结合IEEE 802.1Qci标准对入口数据进行筛选和过滤，是实现数据安全确定性传输底层的技术基础。TSN最关键的目的在于“同一”网络的数据传输，即周期性地控制通信数据与非周期的数据在同一个网络中传输。信号系统网络所承载业务中的CBTC信息、紧急文本信息、视频监控等业务的优先级和所需的带宽各不相同，因此可以使用TSN交换机构建有线网，给网络中各个业务规划固定的传输时隙。具体而言，基于时分多址的思想，在循环周期内根据各业务带宽划分指定时隙给对应的业务，时隙大小根据业务带宽而定，如此规划后，不仅各个业务的传输互不干扰且时延可控，同时可将各业务集中在同一物理网络上传输。七环网将可以减至2张TSN网，甚至1张，大大减少网络建设成本。

2. TSN在车载网络的应用

信号系统车载网络的现状与需求

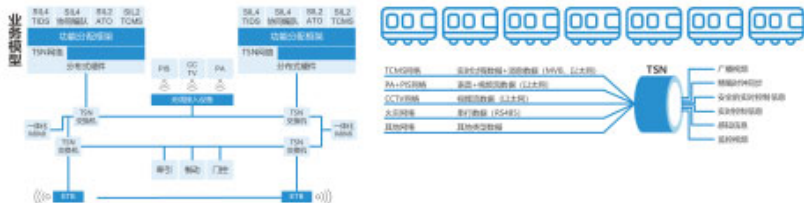


图4 新一代城轨运行系统下的列车车载网络

车载网络主要用来连接TCMS（列车控制与管理系统）、PIS（乘客信息系统）、TCU（牵引控制单元）和BCU（制动控制单元）等。因为各业务系统对网络时延带宽的需求不一，以及传统以太网数据传输的不确定性，无法保证传输PIS等大带宽的多媒体流数据时对

TCMS等列车控制数据的零影响，传统的车载网络是将信号系统的车载网络和PIS车载网络采用物理隔离的两套设备构建。这种模式布线成本高，网络架构复杂，占用有限的车上空间。

列车多网融合是指采用单一的网络来连接列车上所有的设备，是未来主流的列车网络形式。这就需要融合网络能解决车上各业务系统单元数据在同一网络中传输可以区别性地提供不同时延、不同带宽、不同优先级的问题。

TSN在车载网络的应用探讨

在车载网络中，确保流量中的帧在确定的、可预测的时间内送达是一个非常重要的技术指标要求。精确同步的时钟是TSN的基本元素，采用基于IEEE 802.1AS实现全网时间同步，并在此基础上进行数据流量调度。基于IEEE 802.1Qbv或IEEE 802.1Qch标准的门控调度机制对特定标识的数据帧加以控制，结合IEEE 802.1Qci标准对入口数据进行筛选和过滤，是实现数据安全确定性传输底层的技术基础。使用TSN交换机将TSN时间同步、帧抢占、帧复制技术应用到列车多网融合网络系统中，将安全等级高的数据和安全等级低的数据予以区分，可保证TCMS等控车数据传输的确定性，消除多媒体流数据在网络拥堵时对TCMS等控车数据传输造成的影响，进而实现列车网络真正的融合，简化车载网络架构。

结语

TSN具有实时性、可靠性、灵活性、可扩展性和开放标准等多个优势，使其能够满足不同行业和应用的实时、确定和可靠的数据传输需求。然而目前TSN准协议簇中部分协议依旧处于修订、更新和评审状态，尚未得到广泛应用。同时，要想真正发挥TSN的价值，需要整个网络系统中的各个节点均支持TSN相关协议，需要有支持TSN各项协议的终端器件。随着各方面技术的成熟及行业迫切应用需求的增加，相信未来TSN技术将会在轨道交通领域得到广泛的应用。

扎实基础，创新延续： 新华三如何定义下一代城轨云？

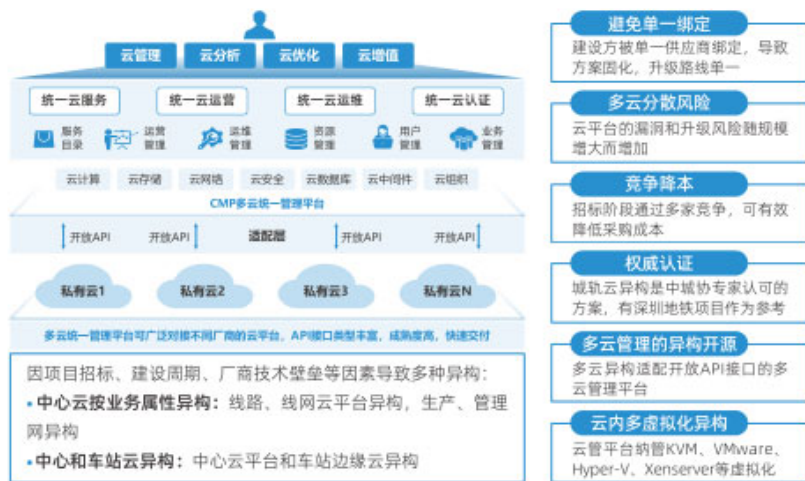
文/张一琛

城轨业务上云，既受数字经济深度融合趋势的外在推动，也是城轨提升效率、优化体验、服务升级的内生要求。过去多年，从虚拟化到云计算，城轨云在底层技术的演进下经过了几个不同的阶段。在摸索和试验的1.0阶段，城轨云缺少整体的规划和部署，难以实现高效的资源调度和灵活的业务匹配，“数据孤岛”仍旧是一个难以根除的问题。随着私有云、专有云等云架构的普及和应用，2.0阶段的城轨云在很大程度上解决了遗留的问题，让业务上云的模式日趋成熟，建设周期不断缩短，开始以“数据+业务”的双轮驱动，实现城轨效率、服务和体验的全面优化升级。

站在新的起点上，城轨云在业务敏捷创新和数据价值交付等方面，也需要新的技术来解决新的难题。作为数字化解决方案领导者，新华三集团依托在全国参与城轨云建设所积累的经验和技术，从城轨数据中心、安全、业务的顶层规划设计出发，以“全域统一管理”作为立足点，以专业服务团队提供全生命周期服务，通过综合运管平台、IaaS、PaaS、DaaS以及云安全、云运维、云运营等各个层面的融合创新，实现资源一体化管理，优化运行效率和应用体验，重塑下一代城轨云的规划理念和建设范本。

一、IaaS底座，让创新与可靠合二为一

一座城市的城轨要为千百万乘客提供出行服务，其多样化的需求必然会造就更复杂的业务架构，也让城轨云需要应对更多场景的转型挑战。一方面，城轨云不仅要承载普通车站、集中车站、智慧枢纽等不同分支机构云上业务，另一方面更要为办公管理、专业生产、创新测试等应用场景提供专业、高效的服务和资源。



城轨云的异构统管

为此，新华三在城轨云的设计和建设上，十分重视提升IaaS的可靠性，通过多云异构解决了技术绑定、风险集中等问题，复合式灾备架构在提升可用性的同时，避免数据和业务的“割裂”，保障业务的稳健运行。此外，在稳定可靠的基础上，新华三在可扩展性的提升上也采取了多项创新举措，计算、存储、网络的弹性调度和多线路接入，给未来的增长预留了扩展的空间，同时以性能提升数倍的核心交换机和专业定制开发支撑起大规模线网云SDN组播技术的应用，简化业务运行逻辑，提升城轨云承载业务的整体效率和性能。

为了避免重复建设带来的浪费，新华三在城轨云的设计上也尤为注重基础设施的充分复用。特别是在SDN软件定义网络的利用上，PaaS平台可以复用SDN实现跨数据中心的大规模组网，打破社区开源网络组件的规模局限性；南北向、东西向的云安全也可以复用SDN网络对流量进行安全编排，复用底层的虚拟化集群，在降本增效的基础上持续提升城轨云的灵活性和安全可靠性。此外，新华三将创新的能力延伸到车站边缘，以瘦终端VDI推动控制中心降本增效，以胖终端IDV、VOI满足车站智能转型的全方位需求，并且能够以“零信任”的理念重新定义城轨云的接入和管理标准，让城轨云桌面走向“胖瘦终端皆为美”的新阶段。

二、推动“云数智”融合，以DaaS平台激活数据价值

数字底座提供了高效调度的算力，但只有算力在算法的驱动下与数据充分融合，才能最大程度推动行业变革。新华三整合了多源数据，以沉淀多年的数据治理和开发能力打造出大数据平台，租户可以通过统一云门户自助申请、部署、配置和使用大数据资源，大数据应用的发布，云管理者也能高效灵活地对大数据资源进行调度，提升云数融合的深度，以全方位的数字化能力引领智慧车站、智能调度、智慧运营等应用的创新和部署。

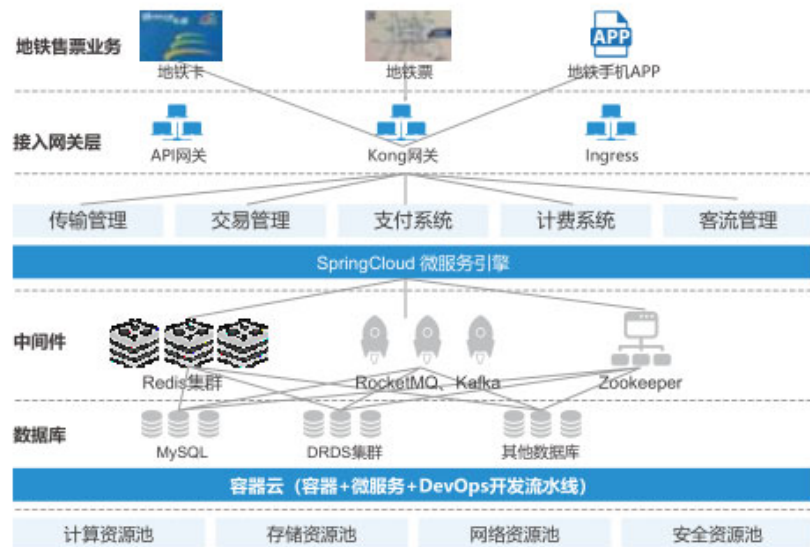


城轨大数据的云数深度融合

在数据接入、治理、挖掘等全生命周期的建设上，新华三从数据标准、数据模型、指标计算、数据服务等维度出发，全力推动城轨大数据治理服务的场景化、套件化，从完整的数据治理体系中提炼出随产品配套发布的安装包和技术文档，规范数据治理服务中的接口、标准、流程、服务等工作，不仅能够降低数据治理的成本，提升数据应用的效率，更把过去的经验化为后续建设的工具，以大规模复制的模式，让城轨大数据平台建设事半功倍。

三、以业务逻辑为导向，加速云原生理念落地

在PaaS平台的建设上，新华三坚持以业务逻辑为指导进行IT架构的规划布局，推动业务的微服务化改造，将新技术能否满足业务需求作为衡量PaaS平台性能和价值的标准。例如在北京地铁，新华三构建的PaaS平台就立足容器、微服务、DevOps等云原生技术构建高效灵活的容器云底座，引入Kafka中间件、DRDS分布式数据库等，以微服务架构应对潮汐流量的高并发、和业务敏捷开发的快速更新迭代场景，满足ITP等创新型业务的实际需求。



新华三在推动技术创新之外，更聚焦于提升城轨PaaS平台的建设和部署效率。一方面，新华三整合过往经验推出了全流程维护手册，覆盖建设前、中、后各个阶段，以整体性的设计避免了多厂商微服务“孤岛化”的复现，彻底打通技术和业务架构。另一方面，新华三也将“套件化”的理念延伸到了PaaS平台的建设上，将城轨云建设积累下的资源评估原则、组件选择方法、应用服务发布方式以及持续监测、治理的建设理念沉淀为城轨PaaS行业套件，全面提升业务系统的微服务改造、微服务架构部署、PaaS组件支撑等场景落地。



下一代城轨云平台发展趋势

在新华三看来，伴随着数字化的加速创新以及与业务的深度融合，“厚中台、薄前台”将是未来城轨云建设的潜在发展趋势。在统一的IaaS平台基础上，由DaaS平台逐步演化出的数据中台以及由PaaS平台演化出的业务中台，将为城轨云的建设和部署提供丰富的行业套件，通过与生态合作伙伴紧密配合，新华三将以“厚中台、薄前台”的理念重构未来城轨云，将业务服务、数据服务整合到云平台服务目录，打造城轨行业专属的云原生应用平台，进一步提升城轨云部署的效率，激活数据价值，赋能云原生应用的改造和创新。

四、从安全、运维到运营，与城轨云变革相伴而行

在安全层面，新华三以“融汇平台统保，贯通系统自保”为基本理念，通过为城轨云打造一体化的安全保障体系，实现云安全资源池的统一部署，规避安全建设“各自为政”导致的混乱无序。同时，新华三顺应云原生技术的部署需求，针对城轨云安全生产网、内部管理网、外部服务网提供数据安全、零信任、PaaS安全等全方位的场景化安全能力，在满足等保合规的基础上，向着局部安全进行精耕细作。

在运维层面，新华三积极推动城轨云从技术运维向业务运维转型的建设理念，以业务为视角，以CMDB为核心，以IT基础架构运维数据为基础，实现故障的快速定位和处理，进一步聚焦用户的真实体验，得出应用性能指数，在此基础上对应用进行自动发现、追踪和故障诊断，保障业务应用程序正常工作；在运维模式上，新华三也积极推动IT运维流程工单服务化，制定出一整套完整的IT运维流程，打破云运维和业务、设备运维之间的边界，实现不同运维逻辑的纵向贯通，确保每一项运维任务可跟踪、可管理，为城轨云提供及时、有效、全方位的服务保障。

在运营层面，新华三将业务运营的场景化定制服务作为推进创新的重要手段，依托统一、高效的数据治理和洞察能力，打造出智慧线网指挥中心、智慧车站、智慧防汛、智慧工地、智慧客服等一站式的场景化智慧城轨解决方案。例如智慧防汛，能通过对天气预报、雨情监测、城轨运行等数据的协同分析进行灾情推演，从而做到及时、精准的告警，保障乘客的人身安全和地铁的运行安全。

目前，新华三已经参与了北京、上海、广州、深圳、南京等47个城市的城轨数字化建设，落地60+城轨云实践。在“云智原生”战略的深化之年，新华三继续推动城轨云在“云数智”不同层面上的融合创新，以云平台、数据平台、业务平台以及配套服务体系的全面进化，满足智慧城轨业务应用的转型需求，与生态合作伙伴一道，推动智慧城轨向未来加速变革和前行。

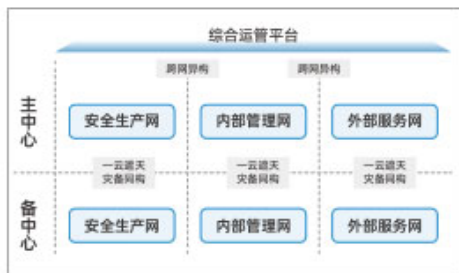
城轨云“和而不同”的发展之道

文/张一琛

经过近6年的反复实践验证，从2023年开始，全国各地城轨云的建设已经进入快速、大规模的发展阶段。过去是OA办公云、AFC清分票务云等一系列小规模试点建设，现在则是承载多线路业务和线网业务的线网级大云，体量和规模翻了将近十倍之多。线网大云一般会有一套主备双中心，三网架构，测试云一套，同时协同多线路的站段边缘云，共同打造一整套完整的城轨云体系。

量变引起质变，当项目规模超过一定体量的时候，就不得不重新思考既有的城轨云建设模式是否还能继续适用。线网云平台的主备中心的灾备关系需不需要考虑云平台厂商的异构？六张网络资源池要不要采用同一云平台架构？会不会出现所有鸡蛋都放在一个篮子里的风险？这么多张网络、不同地理位置的云资源池和管理平台怎么才能全局统筹监管？都是摆在全国地铁业主面前亟待解决的棘手难题。

新华三基于已参与的60余个城轨云项目，分析洞察到部分城轨云未来的建设趋势会呈现出“主备同构，跨网异构，全局统管”的大趋势。这种趋势不是任何一家业主、设计院、厂商能够主导的，是全国各地城轨云项目建设者的智慧集大成的体现。这种趋势既承接了过去专业云、单线路云的建设特点，又解决了线网大云存在的各种潜在风险。



主备同构，跨网异构，全局统管

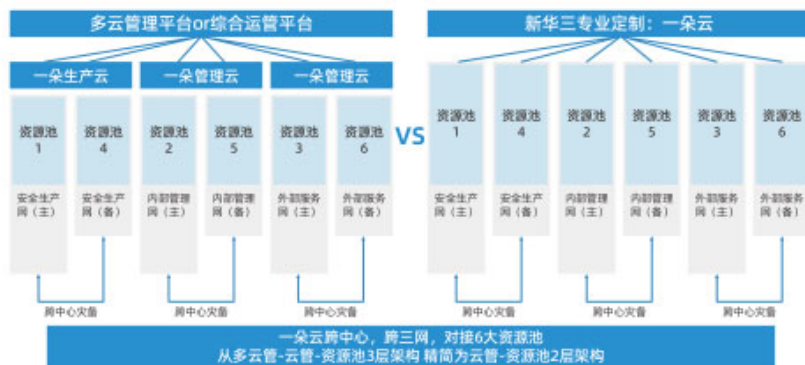
一、主备同构，一云统管

城轨云从来都不是单一数据中心的孤岛建设，为了充分发挥云平台高可用性的优势，灾备中心的建设成为最佳实践方案。在既有城轨业务系统自带的降级机制之上，叠加了云平台的灾备切换机制，使得主备双中心的城轨云在灾备等级上能够达到最高级6级，RTO和RPO均约等于0。

主备中心均部署安全生产网、内部管理网和外部服务网，跨中心的相同网络上的云平台和业务系统实现冗余灾备。过去在备中心多采用3-4级的数据级备份来保障数据的完整性，现在线网云的灾备水平逐步提高到5级实现业务系统的容灾，甚至是6级实现业务系统的双活。灾备等级的提高会涉及存储层的数据同步，计算虚拟化层的HA，数据层的数据库迁移，网络层的大二层快速切换，安全层的设备冗余，云管理层的心跳监测和应用层的无状态双活等多因素跨中心的联动。这就必然要求跨中心的相同网络云平台要由同构云厂商来承接建设，才能用最低的人力、时间成本实现最高的灾备水平。



主备中心技术栈同构才能满足应用级灾备要求



深度定制，一云统管，统筹全市多中心

同构云平台部署在主备中心的安全生产网、内部管理网或者外部服务网时，可以充分贯彻“一云统管”的技术策略。采用一朵云架构，一套SDN平台，对接主备双中心的相同网络的资源池，实现一朵云统一管理多地域Fabric的建设方案。该思路在《城市轨道交通云计算应用指南》中就重点提及，“一云双中心”高级别灾备模式是经过中国城市轨道交通专家们详细论证的先进理念。整个方案就只存在“云管理平台-业务资源池”两层架构，避免了“多云管理平台-云管理平台-业务资源池”的三层架构的出现。新华三城轨云经过深度开发定制，在北京等地已经落地该二层架构方案，完美契合城轨业务系统从“线网-线路-车站”向着“线网-车站”两层架构演进思路。

二、跨网异构，分散风险

2023年临近尾声，业界出现了几起大型云服务中断事件。据官方故障定位的道歉声明来看，可以发现上层基于云原生技术开发和发布的应用，其崩溃宕机多是由云平台故障导致。这一连串同构云平台事故给国内大型云平台建设项目敲响了警钟，单一品牌的同构云平台存在全局雪崩的风险，需考虑引入异构云平台进行风险分担。

如果着眼于城轨业务系统的属性区别，安全生产网主要面向信号系统、综合监控系统、自动售票系统等业务的运营和基础硬件设施的运维，内部管理网主要面向轨道交通集团员工的办公管理场景，外部服务网主要面向乘客民众对信息获取的需求。业务系统之间的差异会产生物理和逻辑上的隔离，这种隔离就导致我们常采用网闸和防火墙来应对，甚至采用不同厂商的云平台即异构云来实现隔离的深化建设。

2021年，深圳轨道交通网络运营控制中心（NOCC）二期项目中就因为线路业务系统和线网业务系统需要同时部署上云，且整体云资源投入达数亿，规模较大。经过深圳地铁业主、中城协等多方专家充分论证后，大家一致明确提出了“线路、线网采用异构资源池，可实现业务系统的应用级互备，以分散风险，防止单一资源池架构性故障，影响全部业务系统，造成业务瘫痪”。线路云和线网云分别由不同云平台厂家提供专业的技术支持服务，共同开放北向API接口，接受多云管理平台对异构云的资源的管理和运维。

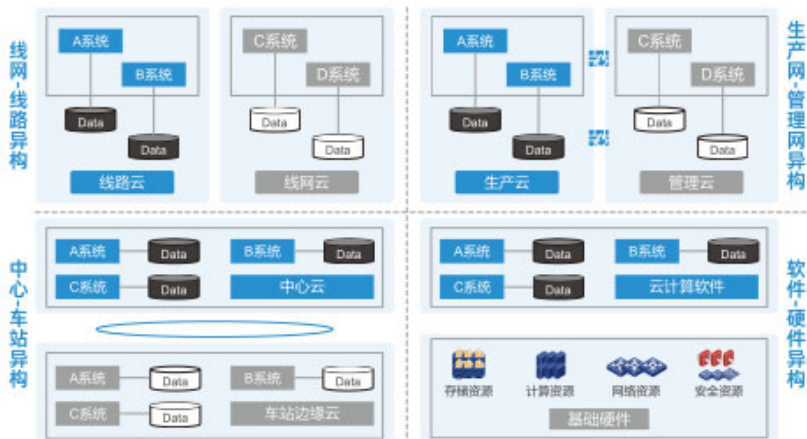
2022年，西安市地铁线网云平台工程项目中，因整体项目同样存在体量大，云平台将跨安全生产网、内部管理网和外部服务网的不同属性的业务系统资源过于集中的问题，西安地铁最终决定采用跨网之间的云平台异构方案。随着方案论证的深入，跨网异构的方案优势

愈发明显：

- ◆ 生产网和管理网的异构云平台能够将故障风险分摊，避免一个篮子中的鸡蛋全部碎掉。
- ◆ 异构云平台可避免被单一云厂商绑定，形成“鲶鱼效应”，激活不同云厂商的技术竞争，将技术路线和价格谈判的主动权牢牢掌握在业主手中。
- ◆ 通过综合运营平台纳管异构云能提升整体数据中心的兼容性，足够的兼容开放带来足够的稳定性，原理类似软件的开源思路。

2023年，济南城市轨道交通4号线一期工程中基于同样考量，采用了类似西安的跨网异构模式，在生产网和管理网之间通过不同厂商的云平台实现风险分摊，最上层通过定制化的云管平台同时接入多个分布在不同地域的资源池，或通过同一个云管平台对主备中心生产网、管理网的资源池进行统一管理。

如果纵向梳理历年各地建设的城轨云项目，会发现存在四种异构方案。第一种，根据线网和线路业务系统的属性差异，决定线网云和线路云之间异构建设。第二种，根据安全生产网和内部管理网或外部服务网之间的业务系统和面向对象的差异，决定在不同网络中建设不同异构云平台。第三种，城轨控制中心或线网指挥中心云平台和车站边缘云异构。第四种，云平台软件和底层基础设施硬件异构建设。前两种按照业务属性差异划分异构云，第三种按照部署地理位置差异划分异构云，最后一种按照设备的软硬形态差异实现方案的异构建设。



城轨云的四种异构方案

三、综合运营，全局统览

在主备同构，跨网异构的整体建设下，必然需要有一个“全局统览”的指挥官辅助用户对整个城轨云数据中心进行深度运维。经过在武汉、西安、太原、上海等地的城轨云项目建设印证后，综合运营平台能够兼容异构资源池，开放数据协议和接口API，实现对各城市建设的主备云中心、站段云节点、大数据平台、测试平台等多个云资源统一运维，满足兼容异构云平台的统一账号管理、统一业务管理规范、异构云资源的统一调度和管理要求，支持用户实现资源的创建申请、释放申请，以及云主机、负载均衡等服务管理内容，实现运维管理、安全管理、网络管理等统一查看。综合运营平台的搭建是异构多云管理平台的技术延伸，是基础设施软硬件运维的功能扩展，为全国线网云的主备同构，跨网异构的框架赋予统筹管理、高效协同、智能加持和便捷交互的能力，助力城轨云的快速高质量发展。



构建城轨边缘数字底座解决方案

文/吕飞

随着城市轨道交通的快速发展，全国各地铁集团正在大力建设城轨云平台，以实现从自动化向智能化的技术升级，城轨云在历史上经历过三个阶段：

第一阶段，验证可行性：将管理类业务系统及个别生产业务系统做上云改造。

第二阶段，强化可靠性：将生产业务进行上云改造，主要通过虚拟化、容器方式做承载，强化生产业务的云上稳定性。

第三阶段，发挥先进性：将安全生产、内部管理、外部服务全城业务进行云化适配与优化，应用IaaS、PaaS、DaaS全栈能力。以上主要目标集中于通过云平台、大数据平台赋能中心级业务升级、改造。

既有城轨云项目普遍采用重中心化建设的模式，而在边缘侧只设置了“两台云节点服务器、两台车站汇聚交换机和防火墙”，这就导致了城轨云方案无法满足车站改造、智慧车站升级、智慧枢纽建设等复杂场景的需求。

同时车站、车辆段系统依然大量采用传统模式，其建设和运维面临着一系列的挑战，我们可以看到在地铁建设、运营、运维各阶段，边缘侧存在着效率低、成本高、运维散、架构重以及创新差等一系列问题和挑战。这些问题不仅严重影响了车站系统的正常运行，还给城市轨道交通的正常运营管理带来了困扰。

在建设阶段，首先，建设成本高、建设效率低是当前车站系统面临的一个主要问题，由于传统采购模式的限制，各类基础资源和智能服务资源的单独采购和重复构建，大幅提高了建设成本；其次，各类业务系统施工建设、部署安装和业务上线的割裂建设，资源缺乏有效整合；同时，改造难是由架构陈旧给车站系统带来的困扰，车站、场段业务的ICT基础架构陈旧，设备数量、冗余机制和安全防护具有明确的数量要求，相互存在绑定关系，灵活性差，不方便改造。

在运营阶段，创新能力差是边缘侧亟待解决的问题，传统业务的ICT基础设施无法满足业务智能化升级和赋能的需求，无法提供例如物联网、云IaaS、云PaaS、大数据等智能服务的能力，缺乏统一的边缘智慧化服务能力的统一规划也加剧了边缘场景的割裂性。

在运维阶段，运维效率低、成本高是另一个边缘侧突出的问题，目前大多数业务系统的运维服务采用人员外包模式进行，各个专业单独运维，不同运维班组和网管室之间缺乏有效的协作和沟通，对于ICT知识的了解也仅限于基础水平，缺乏统一的管理机制和手段，面对复杂问题的相互推诿和重复排查，各自为政，运维及其分散，难以针对性解决。

综上所述，当前车站系统面临着成本高、效率低、运维散、架构重和创新差等一系列问题和挑战，解决这些问题需要采取系统的建设模式、管理措施的变革，城轨边缘数字底座平台建设可以帮助实现包括提高建设和运维效率、降低成本，统一运维和管理、更新架构、促进创新，最终实现车站系统的高效、安全、智能运营等目标。

一、城轨边缘数字底座的概念和特点

1. 城轨边缘数字底座概念

城轨边缘数字底座是基于云边缘计算服务概念构建的，云边缘计算服务是指在靠近设备或数据源头的网络边缘侧，融合计算、存储、网络、安全、控制等能力，就近提供边缘智能服务，简称边缘计算服务（EaaS）。

边缘数字底座是构建在城市轨道交通车站、枢纽、场段等边缘场景下的云计算平台，为车站、枢纽、场段边缘位置提供计算、网络、存储、安全等全栈能力的云计算服务，并联通中心城轨云和边缘终端，构成“云边端三体协同”的端到端的技术构架，通过把网络转发、存储、计算，智能化数据分析等工作放在边缘处理，降低响应时延，减轻云端压力、降低带宽成本，并能提供城轨线网级的调度、算力分发等云服务。

2. 城轨边缘数字底座与城轨云平台的关系

城轨边缘数字底座是城轨云的一个组成部分，纳入中心云平台统一管理，具备与中心城轨云平台全面协同的能力，可灵活设置于车站、车辆段等。

城轨边缘数字底座特点：

承上启下：边缘数字底座北向通过线路骨干网与中心云平台进行数据交互，南向通过站段局域网与边缘无线网络接入端侧设备进行数据交互。

支持降级：边缘数字底座与中心通信正常的情况下，具备与中心云平台全面协同的能力，在与中心通信异常的情况下，边缘数字底座可实现自身的管理功能。

架构灵活：云边缘可根据地铁实际建设情况、业务系统功能需求进行“模块化”灵活配置。

二、城轨边缘数字底座的构建

1. 城轨边缘数字底座系统架构

边缘数字底座的部署位置可灵活设置于车站、车辆段等，并与城轨中心云平台、云及边缘端侧设备构成完整的城市轨道交通信息化“云-边-端”三层架构，边缘数字底座的总体架构如图1所示：



图1 城轨边缘数字底座总体架构图

边缘数字底座通过采用超融合硬件设备作为资源承载主体，通过统一边缘局域网，实现资源共享，同时边缘物联节点、视频节点可容器化部署在其中，提供可与中心协同的物联、视频分析能力。边缘数字底座系统功能架构如图2所示：

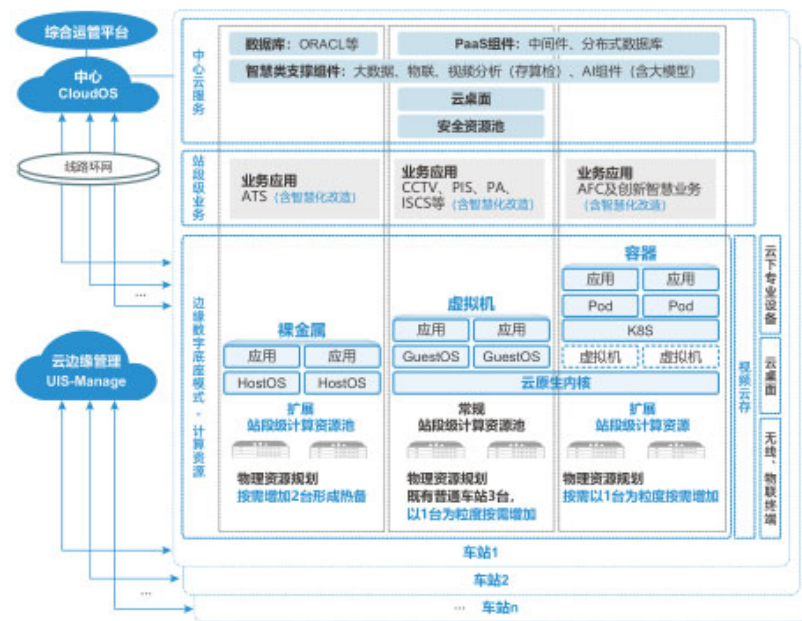


图2 边缘数字底座系统功能架构图

正常情况下，边缘数字底座通过骨干环网与中心云通信，具备与中心云平台全面协同的能力，在与中心通信异常的情况下，边缘数字底座也可实现自身的管理功能，支持业务系统降级模式；同时，云边缘可根据地铁实际建设情况、业务系统功能需求，将IaaS、PaaS、物联、视频分析等服务进行灵活的“模块化”配置。

2. 城轨边缘数字底座网络架构

边缘数字底座的网络架构与中心城轨云平台对应，同样划分为“安全生产网”、“内部管理网”及“外部服务网”的三网架构，不同的是，边缘场景由于业务及其对应资源部署情况与中心存在很大差异，边缘侧不再独立设置边界防护硬件设备。

横向维度，对于采用RJ45端口、TCP/IP网络协议作通信的生产业务专用设备及终端，通过云下接入交换机做汇聚后接入边缘数字底座核心交换机，对于物联网传感器类等采用物联、工控协议做通信的终端，则通过POE交换机做汇聚后接入边缘数字底座核心交换机。

纵向维度，边缘网络包含边缘网络设备及边缘接入终端，边缘终端和计算资源池通过边缘网络核心设备与中心云平台进行联通。

边缘网络架构如图3所示：

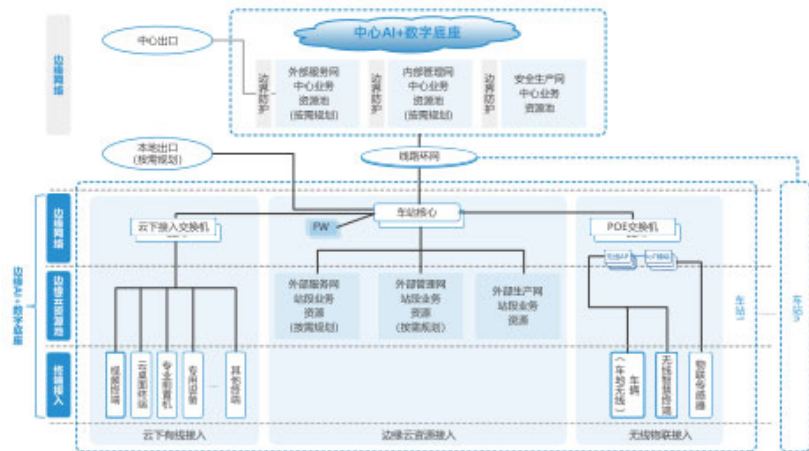


图3 边缘网络架构图

3. 城轨边缘数字底座系统构建

边缘数字底座平台可按需灵活配置云IaaS、轻量化云PaaS、大数据、AIGC、物联管理、视频分析等平台功能和服务。

常规情况下，通过3台超融合服务器提供业务系统所需的虚拟机资源及边缘数字底座IaaS服务，当资源不足时，可按需以1台超融合服务器为最小单位进行增加。同时，可以通过1台超融合服务器作为最小单元提供边缘场景下的轻量化云PaaS服务，包括容器集群管理、容器资源自动分发等。

对于调度类业务的操作工作站需求、边缘视频类业务的分布式存储需求，可以在边缘数字底座上扩展相关云桌面、视频云存储资源池，进行能力接入，与中心云平台进行能力协同。

在机房建设方面，边缘数字底座采用模块化机房的模式进行建设，即将机架式形式同时将“配电单元”、“空调”、“UPS”、平台管理、计算、存储、网络、安全节点进行融合部署，将机房中配电、制冷、监控、计算等集成到一体化机柜当中，提高机柜空间使用率、减少机房面积、降低能耗，减低机房整体PUE，同时通过动环监控系统实现机房运行的实时监控，承载所有ICT设备，最大限度实现边缘侧的绿色节能。

此外，当边缘业务系统的云下设备及端侧设备需要与云平台进行通信时，则通过边缘局域网络、边缘网络提供有线和无线不同接入方式，实现业务系统的云-边-端互联。

4. 城轨边缘数字底座成本分析

设备成本分析

通过边缘数字底座方式改造后需要资源为8台超融合服务器、2台汇聚交换机、2台防火墙、1台视频云存储及10台云桌面，传统模式边缘侧可云化业务系统资源与边缘数字底座建设模式可云化业务系统资源，如表1、2所示：

序号	类型	业务系统	服务器	交换机	防火墙	工作站	存储	备注
1	传统业务	ISCS	4	2	2	2	0	
2		AFC	1	2	0	2	0	
3		公专电话	0	2	0	0	0	
4		PIS	5	1	0	0	0	
5		CCTV	1	1	1	0	1	
6		信号系统	0	3	2	6	0	
7	智慧业务	智慧车站	4	2	2	0	0	客流监测、应急联动等
8		智能客服	2	2	2	0	0	
9		智能管控	2	2	2	0	0	
10		智能运维	4	2	2	0	0	
11		智慧枢纽	8	2	2	0	0	智慧商业、智慧物业等
合计			37	25	19	10	1	

表1 站段业务系统采用基础ICT设备建设模式下资源占用表

序号	类型	业务系统	超融合服务器	交换机	防火墙	云桌面	存储
1	传统业务	ISCS	8	2	2	10	1
2		AFC					
3		公专电话					
4		PIS					
5		CCTV					
6		信号系统					
7	智慧业务	智慧车站					
8		智能客服					
9		智能管控					
10		智能运维					
11		智慧枢纽					
合计			8	2	2	10	1

表2 站段业务系统采用边缘数字底座建设模式下资源占用表

分析对比得出，城轨边缘数字底座将原有92台ICT设备整合为33台ICT设备，设备数量综合降低75%，其中计算节点设备数量降低88%，网络设备数量降低92%，安全设备数量降低90%。

机柜数量成本分析

对于传统业务：每站减少ISCS机柜5个、通信机柜4个（PIS机柜2个、CCTV机柜2个）、AFC机柜1个、信号机柜2个（设备集中站2个、非集中站1个），减少共计12个机柜。

对于智慧业务：因功能配置、实现方式以及软件ISV的不同，每站按照智慧安检、智慧枢纽、智慧车站、智能管控、智能运维、安全防护集成的机柜最小总体规模核算，约减少8台机柜。

边缘数字底座考虑优化设备资源空间占用、降低整体能耗，建议进行“模块化机房”建设，将传统机柜优化为4个边缘数字底座机柜，整合了配电、制冷、监控、资源承载能力，同时预留智慧类业务机柜资源能力，可减少机柜总计数量约20台。

分析对比得出，机柜数量总体降低约80%。

机房面积成本分析

由于边缘数字底座将通用资源进行整合部署，同时优化设备资源空间占用，考虑车站综合

弱电机房包含边缘数字底座加传统业务系统工控设备机柜，单个车站机柜总面积可以从260m²（以杭州5号线为例，车站信号设备室100m²，综合监控设备室40m²，专用通信设备室60m²，公安通信设备室40m²，该线路边缘不含智慧业务资源占用）减少至120m²（其中传统业务系统专用设备机房占用面积进行整合为100m²，边缘数字底座资源占用20m²）。

机房面积总体降低约50%。

能耗成本分析

针对设备室ICT设备机柜总额定功率做估算50KW（5KW*10台），对边缘数字底座计算、存储、网络、安全设备机柜总额定功率做上限预估（包含智慧类业务）30KW（10KW*3台），全线共降低（20KW*20个站段*24小时*365天）约350万KW，全线每年约减少电费350万；同时估算供电系统总额定功率约50%（提供80KW）给ICT设备使用，边缘数字底座建设模式可降低50% ICT供电额定功率（提供40KW）。

ICT能耗降低约40%，全年站段电费降低350万。

5. 对于改造线路边缘建设场景的适配

当前各地铁集团都陆续迎来了改造、大修期，线路改造的主体是生产业务系统，采用“以专业为单位，分步骤招标、改造”的模式，相应的弊端逐渐显现：

- ◆架构陈旧：虽然硬件设备不断更新、性能不断升级，但没有改变业务系统架构陈旧的本质。
- ◆建设割裂：由于没有统一的数字化底座提供全栈能力支撑，业务即便存在新技术需求，也不得不独立建设一套包括云IaaS、PaaS、大数据、物联网在内的多个平台，反而加剧了边缘场景的割裂性。
- ◆实施繁琐：每个专业改造时，都需要部署、调试硬件环境，工作量巨大，同时故障点也大幅增加。
- ◆资源重复：每个业务建设有自己独立网络、安全、计算设备，独立升级改造，能力超标，资源重复，造成了建设成本和运营成本的浪费。

而边缘数字底座的灵活架构、强大功能、通用能力可以很好的解决这些问题，传统建设模式、城轨云建设模式下，边缘场景改造过程优化如图4所示：



图4 边缘场景改造过程优化图

三、城轨边缘数字底座场景化应用探索与实践

1. 轨旁智能运维场景的实践

基于城轨边缘数字底座能力与架构模块化灵活配置的构建思想，此方案已经在一些城市进行率先的尝试和探索，我借助于新华三集团及北京交通大学在各地铁路线路项目建设上的机会，参与了如下实践。

例如，在青岛地铁针对于轨旁、站厅、站台业务智能运维的场景，基于业务实际需求构建了以模块化数据中心、边缘数字底座节点、大数据节点、物联网节点为基础，覆盖云IaaS、大数据、物联网能力的边缘数字底座，并配置了手持台、手环等终端实现了物联网技术对轨旁运维人员的定位，这也是边缘数字底座方案在青岛地铁大规模应用，通过UWB定位实现的智能导航、电子围栏、Wi-Fi网络实现的智能终端接入功能，加之边缘数字底座节点上业务资源的快速部署、策略快速分发，大大提升了青岛地铁的运维效率，系统架构如图5所示：



图5 边缘数字底座场景下的智能运维架构图

2. 客流分析与客运调度场景的实践

此外，上海申通地铁针对于车站厅、站台的客流分析与客运调度场景，基于边缘数字底座的云计算、大数据、物联网的能力进行了实践应用。

首先将客流分析、调度场景拆解为站外、进站、站内、站台、换乘、乘车六大场景，以边缘大量感知终端视频数据为参照，做视频分析。

其次，通过边缘数字底座联通边缘终端设备，及控制中心的分析、调度应用系统。最后，实现线路人数统计、人群密度、排队长度、候车留乘等场景下的客流分析与乘客调度能力，场景分解如图6所示：



图6 客流分析与客运调度场景分解图

3. 车站智慧防汛的实践

由于目前极端天气、突发情况频繁出现，昆明地铁基于车站智慧防汛场景也做了课题实践，在边缘侧搭建边缘数字底座模型，并将车站站外、站内进行智慧防汛的场景进行联动，最终实现防汛监测、视频监控、应急响应等功能，智慧防汛系统实践效果如图7所示：



图7 智慧防汛系统图

城市轨道交通云容灾技术分析

文/史钰果

信息系统的连续性服务是城市轨道交通运营管理的生命线，对安全生产和故障应急而言至关重要。近年来，一二线城市均构建了较为完善的城轨云平台，广泛应用到生产和运营管理等各专业领域，部分二三线城市也积极推进云平台扩建和在建，特别是新建地铁城市，基于云平台架构建设基本成为标配。然而随着线路规模的快速扩展和运营业务的日益增加，城轨云平台信息系统连续性服务工作面临巨大挑战，为保证信息系统安全、稳定、可靠运行，一些城市在着手规划建设应用级容灾中心，以期在本地业务系统出现不可恢复的物理故障时，有容灾中心提供业务接管和应用服务。快速发展的云计算技术和相关业务服务，为容灾中心建设提供了新的方案选择。

通常情况下城轨云规划建设两个大型数据中心，两个数据中心的业务和数据系统为双活或主备架构。当灾难发生时，需实现从生产中心到容灾中心的切换，实现业务连续性的要求，且数据库恢复点目标（RPO）接近于0（亚秒级），恢复时间目标（RTO）为5~10分钟，容灾中心信息资源水平需要与生产中心水平相当。

一、容灾技术规范和标准

《信息安全技术信息系统灾难恢复规范》国家标准（GB/T20988-2007）是我国灾备份与恢复行业的第一个国家标准。该标准由国务院信息化工作办公室领导编制，并于2007年11月1日开始正式实施。该标准规定了信息系统灾难恢复应遵循的基本要求，适用于信息系统灾难恢复的规划、审批、实施和管理，并参照国际标准SHARE 78的7个层级定义，确定了符合中国国情的6个容灾能力等级，要求如下表所示：

国际标准SHARE78		《信息系统灾难恢复规范》GB/T20988-2007	
Tier-0	无异地备份数据	第1级	基本级，基本支持备份介质并场外存放
Tier-1	有备份数据，无异地备用系统，用交通工具运送备份数据		
Tier-2	有备份数据，有异地热备份站点，用交通工具运送备份数据	第2级	备份场地支持，网络和业务处理系统可在预定时间内调配到备份中心

国际标准SHARE78		《信息系统灾难恢复规范》GB/T20988-2007	
Tier-3	通过网络传输备份数据，提高灾难恢复速度	第3级	电子传输和部分设备支持。容灾中心配备部分业务处理和网络设备，具备部分通讯链路，关键数据定时传送
Tier-4	定时备份数据，网络自动传输，根据备份策略的不同，数据的丢失与恢复时间达到天或小时级	第4级	电子传输和完整设备支持。数据定时批量传送，网络/系统始终就绪，少量数据丢失
Tier-5	数据在两个站点之间相互镜像，由远程异步提交来同步，为关键应用使用双重在线存储，所以在灾难发生时，仅传输中的数据被丢失，恢复的时间被降低到了分钟级	第5级	实时数据传输及完整设备支持。采用远程复制技术，实现数据实时复制，数据丢失趋于0，网络具备自动或集中切换能力，业务处理系统就绪或运行中
Tier-6/7	数据零丢失，数据同时被写入到两个站点，在本地和远程的所有数据被更新的同时，利用了双重在线存储和完全的网络切换能力，不仅保证数据的完全一致性，而且存储和网络等环境具备了应用的自动切换能力。一旦发生灾难，备份站点不仅有全部的数据，而且应用可以自动接管，实现零数据丢失的备份	第6级	数据零丢失和远程集群支持。数据实时备份、零丢失，系统/应用远程集群，可自动切换，用户同时接入主备中心

容灾等级要求

根据《智慧城市轨道交通信息技术架构及网络安全规范》要求云平台总体架构应按照GB/T20988-2007标准，满足各业务系统等保安全的需求，能够支持智慧城市轨道交通信息技术架构达到4级以上的灾难恢复等级，具体RTO/RPO等级要求可参照下表所示：

等级	等级要求	RTO	RPO
第1级	基本级，基本支持备份介质并场外存放	2天以上	1天至7天
第2级	备份场地支持，网络和业务处理系统可在预定时间内调配到备份中心	24小时以后	1天至7天
第3级	电子传输和部分设备支持。容灾中心配备部分业务处理和网络设备，具备部分通讯链路，关键数据定时传送	12小时以上	数小时至1天
第4级	电子传输和完整设备支持。数据定时批量传送，网络/系统始终就绪，少量数据丢失	数小时至2天	数小时至1天
第5级	实时数据传输及完整设备支持。采用远程复制技术，实现数据实时复制，数据丢失趋于0，网络具备自动或集中切换能力，业务处理系统就绪或运行中	数分钟至2天	0至30分钟
第6级	数据零丢失和远程集群支持。数据实时备份、零丢失，系统/应用远程集群，可自动切换，用户同时接入主备中心	数分钟	0

GB/T20988-2007《信息系统灾难恢复规范》RTO/RPO与灾难恢复能力等级的关系

二、容灾需求分析

根据《智慧城市轨道交通信息技术架构及网络安全规范》要求云平台总体架构应按照 GB/T20988-2007 标准，满足各业务系统容灾需求。结合当前各城市轨道交通云平台及入云业务系统的现状及规划，通过云平台容灾系统的建设，需能够支持智慧城市轨道交通信息技术架构总体达到5级及以上的灾难恢复等级。

云容灾系统涉及三方面的容灾需求，包括云平台自身、线网级业务系统及线路级业务系统的容灾需求，下面逐个进行分析。

1. 云平台自身容灾需求

云平台作为重要基础设施，承载线网级、线路中心级业务系统，云平台自身应达到5级以上的灾难恢复等级。当主用中心云平台瘫痪时，容灾中心云平台应具备云平台管理能力，继续为线网级业务系统提供计算、网络、存储、安全等服务。整体而言，云平台整体 RTO 应为分钟级，RPO 应为分钟级。

云平台自身容灾对象包括云管系统、SDN 管理系统及云平台配套的网络接入及安全防护设备。

- ◆云管系统和 SDN 管理系统是云主机、云网络、云存储等云服务生命周期管理的重要工具。在主用中心故障时，备中心云管系统和 SDN 系统应支持云管理平台业务平滑切换至备中心。

- ◆网管系统用于对容灾中心云平台设备的网元级管理，包括数据中心存储、服务器、交换机等物理设备，需保证所有物理设备的集中监控，并对网络的配置、服务器的部署、存储的资源配置提供可视化界面，实现对数据中心物理设备的统一管理。

- ◆容灾系统切换后，备中心云平台应支持远程管理主用中心资源的能力，可在主用中心云平台管理面业务出现重大故障或重大升级时，临时接管云管理业务，不影响线网及线路业务系统的运行。

2. 线网级业务系统容灾需求

线网级系统指入云的线网控制中心级系统，线网级系统需在容灾中心具备对应计算、存储、网络及安全等方面服务能力和资源，在主用中心故障时，备中心能够有足够的资源承载线网级系统平滑切换。

具体要求包括：

- ◆采用应用级容灾模式，容灾中心具备实现主用中心出现重大问题，接管主用中心线网中心业务的能力。

- ◆主用中心、容灾中心具备后续扩展能力，支撑后续入云的线网中心级系统提供主备/双活容灾。

- ◆容灾中心部署与主用中心相同配置的计算、存储、网络及安全等资源池，在主用中心和容灾中心均部署容灾应用系统的数据库、中间件和应用软件。

- ◆容灾中心具备与主用中心数据处理系统一致的数据处理能力，可实现容灾切换。

- ◆主用中心和容灾中心存储系统实现数据同步，并保障数据一致性。

- ◆主用中心和容灾中心实现基础物理网络、虚拟网络、网络资源管理能力，提供充足的网络带宽，保证数据传输带宽大于业务峰值所需的带宽需求。

3. 线路级业务系统容灾需求

线路级业务系统相比于线网级业务系统的重要性略低，且故障时影响业务范围也较小，因此线路级业务系统容灾优先考虑数据级备份能力。云平台可以为线路级业务系统提供数据备份空间及工具，线路业务系统可通过备份工具设置不同的备份策略，将关键数据周期性备份至容灾中心云平台。

关于数据备份，具体要求至少包括：

- ◆备份系统宜采用基于备份软件的集中备份方式，可由备份管理服务器、备份介质服务器、备份存储系统、备份软件、备份网络等构成。

- ◆备份管理服务器、备份介质服务器宜采用物理服务器冗余部署方式；根据备份数据量可采用合设或分设模式；备份介质服务器可按服务器集群方式进行横向扩展。

- ◆根据异地数据备份的需求，在主用中心和容灾中心之间宜提供不小于10GE的专用数据备份链路；在不影响主备中心之间业务应用数据传输的条件下，可共享业务平面网络互联链路。

- ◆数据备份系统应能纳入云管理平台实现统一管理。

- ◆备份系统应能实现对操作系统、数据库、文件系统、虚拟机等的备份，应能针对不同的备份对象制定相应的数据备份及恢复策略。

- ◆备份系统应支持完全图形化的管理功能，实现对分布在不同地点的备份系统进行集中统一管理，具备备份策略管理功能，针对客户端可统一定义和修改备份计划策略、存储策略和恢复计划策略等。

4. 容灾总体目标

通过需求分析，城市轨道交通容灾中心的主要目标包括：

- ◆云平台管理业务自身应具备主备中心切换能力，并能够实现分Region管理。当主用中心出现问题时，云平台管理业务可平滑切换至容灾中心，RTO分钟级、RPO分钟级。

- ◆实现线网中心级系统的应用级容灾，当主用中心故障时，容灾中心可拉起业务云主机，接管线网中心级系统业务。

- ◆为线路业务系统提供数据备份服务能力。

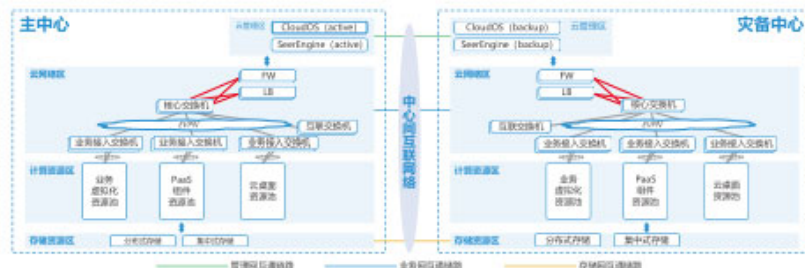
三、技术路线分析

容灾技术是系统高可用性技术的一个组成部分，容灾系统更加强调处理外界环境对系统的影响，特别是灾难性事件对整个IT节点的影响，提供节点级别的系统恢复功能。从其对系统的保护程度来分，可以将容灾系统分为：数据容灾和应用容灾，数据容灾就是指建立一个异地的数据系统，该系统是本地关键应用数据的一个定时或实时复制。应用容灾是在数据容灾的基础上，在异地建立一套完整的与本地生产系统相当的灾备应用系统（可以是互为灾备），在灾难情况下，远程系统迅速接管业务运行，数据容灾是抗御灾难的保障，而应用容灾则是容灾系统建设的目标。

1. 应用级容灾

1.1 技术路线

◆主备容灾



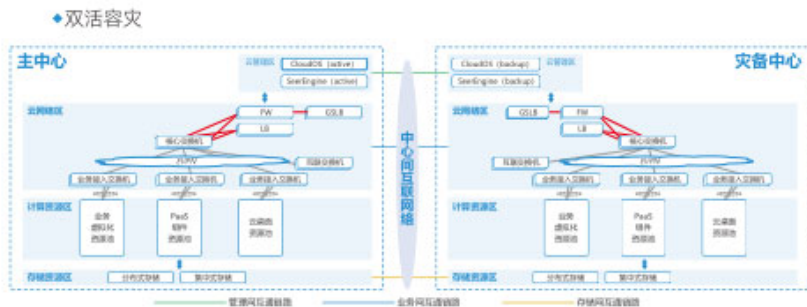
主备容灾即同一时间只有一个云数据中心提供在线服务，容灾中心处于空闲状态，负责在灾难发生后接管应用系统运行。在很多情况下往往将业务系统分为两部分，选择不同的数据中心分别作为这两部分业务的主中心，对这些业务而言，另一个数据中心即为其灾备中心，这种互为主备容灾的方式能够在考虑业务系统容灾需求的情况下充分利用灾备中心的资源。

主备容灾适用场景为同城两个数据中心由一套云管理平台统一管理，不同业务分别承载在两个数据中心内。生产状态下，业务在主数据内运行，提供业务访问；当主用数据中心发生故障后，业务异常，业务访问中断；通过容灾切换，将容灾业务在备中心恢复，重新提供业务访问。对于单一业务来说，在两个数据中心实现主备容灾。

主备容灾方案中容灾中心业务系统与主用中心业务系统的软件和操作系统环境相同，主用中心系统业务软件调整后，容灾中心系统应能自动进行同步保持一致；容灾中心可按主用中心相同配置或等比例减配计算和存储资源。云计算中心作为主生产中心，负责日常所有业务系统的运行，灾难发生时，整个数据中心进行切换，由容灾中心接管运行生产运营关键业务，保证各个业务系统的核心数据不丢失。

主备容灾技术方案主要包含以下技术要点：

- ◆两个数据中心各自部署一套标准的计算、存储、网络、安全资源池。
- ◆两个数据中心共用一套云管平台和SDN控制器平台。
- ◆两个数据中心通过波分设备物理互联。
- ◆两个中心的网络、存储复制链路分别需要互联。



双活容灾即两个数据中心都处于运行当中，运行相同的应用，能够提供跨中心业务负载均衡运行能力，充分利用资源，实现持续的应用可用性和灾难备份能力。

双活容灾适用场景为同城两个数据中心由一套云管理平台统一管理，在同城两个数据中心同时对外提供相同业务，实现业务双活。通过在数据中心出口位置部署GSLB，实现不同客户端对同一业务进行访问时的流量在两个数据中心进行负载均衡；当一个中心出现业务故障时，GSLB会将该中心原有的访问流量切换到另一数据中心，提供故障后的自动切换保护。

双活容灾技术方案主要包含以下技术要点：

- ◆两个数据中心各自部署一套标准的计算、存储、网络、安全资源池。
- ◆两个数据中心出口各部署两台GSLB全局负载均衡设备（4台组成集群）。
- ◆两个数据中心共用一套云管平台和SDN控制器平台。
- ◆两个数据中心通过波分设备物理互联。
- ◆两个中心的网络、存储复制链路及两个数据中心的ED设备分别需要互联。

1.2 技术对比

指标项	主备容灾	双活容灾
容灾能力等级	4-5级	5-6级
RTO	分钟级	分钟级
RPO	分钟级	0
容灾切换	一键手工切换	通过双活主机的状态探测触发自动切换，在主用节点故障时自动将业务切换到备用节点

指标项	主备容灾	双活容灾
资源占用	较少，计算、存储资源1:1预留 主备业务占用一个IP 仅主业务运行能耗	较多，计算、存储资源1:1预留 双活业务占用两个IP 双活业务运行能耗为双份
地域	可同城、可异地	同城
关键技术实现方式	基于镜像文件复制、存储LUN级复制、数据库日志复制	基于业务应用驱动业务数据层面同步、GSLB、DNS、SLB联动切换
成本投入	适中	较高
实现可落地性	技术成熟，可快速交付	技术复杂，案例较少
是否需要业务改造	不需要业务系统改造，容灾切换后IP不变，对业务无影响	需要业务系统改造，个别业务系统可能不支持双中心同时运行（IP不同），不同IP下运行需要支持主备角色切换
性能影响	单中心运行，无影响	要保证数据强一致性，对业务性能有影响

1.3 对比分析

通过以上各项对比，结合城市轨道交通云平台建设现状从以下几个维度展开分析：

- ◆实现可落地性方面，主备容灾技术成熟、落地案例多且可快速交付，而双活容灾技术复杂，落地案例较少。
- ◆建设难度及成本方面，主备容灾需要对两个数据中心存储层面做远程复制，网络链路延迟不高于50ms，整体建设难度较小、成本适中；而双活容灾对主用数据中心和容灾数据中心之间的网络链路要求高，存储层需要部署双活，网络链路延迟不高于10ms，且需要部署全局负载均衡、本地负载均衡、DNS服务器联动保证业务自动切换，整体建设难度大、成本高。
- ◆业务改造方面，主备容灾模式业务系统同时运行在单个数据中心，在容灾切换后业务访问IP地址不变，对业务无影响且不需要业务系统进行改造。而双活容灾模式下业务系统需要同时运行在两个数据中心，业务访问的IP地址不同可能导致部分业务系统不支持双中心同时运行，需要对业务系统改造，改造难度较大。
- ◆资源占用方面，主备容灾计算及存储资源按照1:1预留，主备业务只占用一个IP，通常情况下仅主用中心运行能耗，资源占用较少；而双活容灾虽然计算及存储资源也按照1:1预留，但双活业务需要占用两个IP，双活业务运行能耗也为两份，资源占用较多。

综上所述，结合城市轨道交通云平台线网级业务系统现状，针对应用级容灾需求建议选择主备容灾模式，同时保持对双活容灾技术的跟进，待双活容灾技术成熟后视业务需求将主备容灾模式升级为双活容灾模式。

2. 数据级备份

2.1 技术路线

◆数据定时备份

数据定时备份是一种定时数据保护机制，根据备份策略和计划，在指定时间发起备份任务，读取需保护的数据，并写入备份介质。应用类型不同，其支持的备份类型也各有差异。

常见的备份类型包括如下表所示：

备份类型	描述	特点
完全备份	将所有选定的数据源备份到指定目的地中	最常见的备份类型。备份完整数据，恢复方便。备份耗时久，且反复备份，占用存储空间较多。
增量备份	只备份自上一次备份（完全备份或增量备份）后新增或变化的数据	备份数据量小，备份速度快。相对而言，所需恢复时间比完全备份或差异备份所需时间长。
差异备份	执行差异备份时，仅备份自上次完全备份后新增或变化的数据	备份数据量小，备份速度比完全备份快。相对而言，恢复数据所耗费的时间比完全备份时间长。如果大量数据发生变化，差异备份所耗费的时间比增量备份时间长。
事务日志备份	备份数据库中的事务日志。事务日志是数据库中已发生的所有修改和执行每次修改的事务的一连串记录	使用事务日志备份，可将数据恢复到精确的故障点。

数据定时备份技术具有良好的操作系统兼容性，可支持目前正在使用的大多数所有操作系统，同时备份系统可支持主流数据库接口级备份功能，以满足用户在现在及未来的任何发展需要。

◆数据实时复制

数据实时复制技术主要是将业务系统中的数据实时复制到指定路径，与数据备份方式不同，数据实时复制技术通过在操作系统核心层中植入文件过滤驱动程序，来实时捕获所有文件访问操作。对于需要实时备份保护的文件，当数据实时复制管理模块经由文件过滤驱动拦截到其改写操作时，则预先将数据变化部分连同当前的系统时间戳一起自动备份到存储资源，从而实现主、备应用数据的实时一致性。

数据实时复制技术需要首次将磁盘底层完全镜像，后续的实时日志采用I/O录像模式记录变化数据块的方式；通过客户端的持续监控磁盘扇区数据块变化情况，然后对比磁盘位图信息确保一致性，结合定时增量备份数据在服务端进行逻辑上的融合，当需要提取改点数据时会自动形成一个全量数据点。

2.2 技术对比

指标项	数据定时备份	数据实时复制
RTO	与数据量有关，小时或天级	分钟或小时级
RPO	小时级	秒级或分钟级
数据获取方式	通过客户端软件调用应用API备份接口	通过客户端软件对磁盘扇区数据块持续的监控
数据一致性	极端情况下依然能够保障数据一致性	极端环境存在应用数据不一致的可能
架构支持方面	LAN、SAN都支持	LAN、SAN都支持
有无代理	无	有
云平台集成能力	有	无
备份方式	定时备份、全量备份、增量备份、差异备份	首次磁盘底层完全镜像，后续实时日志采用I/O录像模式记录变化数据块
存放方式	通常为数据库打包集格式或备份系统私有格式	通常基于磁盘I/O监控模式保留格式为磁盘底层原块格式
备份数据恢复	存在一定的恢复时间，恢复时间与数据量和带宽资源成正比	由于数据格式同原数据格式一致，恢复耗时短
业务连续性	需要一定的时间进行业务和数据恢复，无法保障业务连续性	具备一定的业务连续性
运维成本	低	高

2.3 对比分析

通过以上各项对比，结合城市轨道交通云平台建设现状从以下几个维度展开分析：

◆在数据一致性方面，数据定时备份技术是通过应用API备份接口获取的数据，极端情况下依然能够保障数据一致性；而数据实时复制技术由于备份客户端软件通过持续监控磁盘扇区数据块的变化，不考虑应用、不通过应用的备份接口获取数据，备份数据极端环境存在应用数据不一致的可能。

◆在代理方面，数据定时备份技术支持无代理备份，减少了资源消耗；而数据实时复制需要在目标主机安装客户端代理，通过对数据块持续的监控，连续捕获数据变化，将变化后的数据块进行同步保护，降低了物理设备的资源使用率。

◆在与云平台的集成方面，数据定时备份技术支持与容灾中心云管理平台的深度融合，在

云管理平台云服务目录的备份界面即可实现备份服务功能的下发操作，降低了运维成本；而数据实时复制不能与云管理平台深度融合，独立的管理服务界面以及业务操作流程提升了业务的复杂度，增加了运维成本。另外，根据线路级业务系统容灾需求，数据备份系统应能纳入云管理平台实现统一管理，数据实时复制技术无法满足此需求。

综上所述，结合城市轨道交通云平台线路级业务系统现状，推荐采用数据定时备份技术。后续随着容灾技术的不断发展及业务系统需求的变化，可继续开展针对线路级应用数据实时复制技术的研究和探索。

结语

城市轨道交通数据中心双活容灾解决方案对于集中式管理的数据中心，可更大程度保证业务的连续性，也可有效保障灾难发生后业务恢复的时效性。该技术架构需解决存储双活、网络层双活、数据库双活、计算层双活、应用层双活，容灾切换速度快，资源利用率高，应用服务可靠性高，理论上可做到RPO&RTO=0。但是，双活容灾中心投资高，实施难度大，运维复杂，对运营维护人员要求高，且无法规避逻辑灾难。对于生产中心设置于控制中心，灾备中心设置于车辆段的方案，生产与灾备中心同时接纳数据交互，技术难度很大，需要更改众多业务系统底层程序。当灾难发生时，两中心间的数据同步效率如达不到要求，将会造成业务数据的丢失。

城轨云容灾应充分利用云计算特性，结合各业务系统应用需求，统筹考虑各业务系统的业务强相关性和当地人力、物力的配备，按需选择实现底层存储双活、网络双活、数据库双活，甚至计算层双活和应用层双活，利用云计算的漂移特性、主备中心互连网络，可使调度、指挥等工作按照一个控制中心来实现。而对于使用者和管理者来讲，具体业务实现是由生产中心提供还是灾备中心提供是透明的。

基于云平台的城轨信号系统建设探索与思考

文/吕飞

作为城市轨道交通运行的“大脑”和“中枢神经”，城轨信号系统无疑是保障安全、可靠、高效运行的最重要、“最传统”的系统之一，说其传统是因为其系统可靠性会直接影响到整个城市轨道交通线网的运行与乘客生命及财产安全，建设方、总包商会对其持有更严谨、更严苛的态度，而具体到实现方式，往往是通过设置多重冗余机制与硬件设备，采用工控设备、异构芯片等从不同维度保证其安全性。

近几年云计算、大数据等新技术在城市轨道交通行业的实践和应用逐渐增多，同时，越来越多的地铁建设单位、信号系统总包商也期望通过数字化手段对城轨信号系统进行智能化升级，以精简其复杂的系统硬件架构、减少硬件投资、实现旧线“无感改造”、提高线路运维的效率和灵活性、实时全面的进行设备监控，最终实现动态时刻表，改变传统城市轨道交通运营方式、优化乘客出行体验，就此，一个“基于云平台的城轨信号系统”新趋势拉开序幕。所谓基于云平台的城轨信号系统，即利用云计算技术将原有架构基于工业服务器进行替代，将其演进成为基于云服务承载的、多核CPU安全平台的信号系统。

在建设投资方面，云信号系统可以精简复杂的系统硬件设备架构，减少硬件投资，实现更高的经济效益并有利于可持续发展。

在行车控制方面，云信号系统可以利用云计算、大数据等新技术做数据分析，智能化的进行列车运行控制，不仅可以提高行车效率和准点率，还能够更好地应对客流高峰期的运力需求，减少人员和物质资源的浪费，实现动态时刻表，解决仅通过固定时间间隔、人工操作带来的列车行驶效率低和资源浪费的问题。

在运行维护方面，云信号系统将所有的运营数据和实时状态进行管理和分析，运营管理人员能够快速根据系统状态作出相应的调整和决策，实现智能、高效的运维，同时对信号系统长期的数据进行分析，可以更科学、合理的制定维修计划，即实现状态修和预测修。

在乘客出行方面，由于精简硬件架构、高效运维可以有效降低系统故障率，减少乘客出

行方面的投诉，同时，传统模式下乘客往往需要面对列车延误、拥挤和不确定性等问题带来的威胁也有望解决。

一、城市轨道交通信号系统智能化发展趋势

1. 城轨信号系统发展历史和周期分析

城市轨道交通信号系统运行控制方式的发展，大致可以总结为三个阶段：

第一个阶段，从传统的基于点式控制方式的信号系统发展为基于通信的列车控制系统，即CBTC系统。

第二个阶段，由CBTC系统发展为全自动运行系统，即FAO系统。

第三个阶段，由FAO系统发展到列车自主运行控制系统，即TACS系统。

每个阶段的发展大概均需经历5-8年的过渡周期，当前城市轨道交通的信号系统虽然在控制方式、安全性、运行效率等方面较之前已经取得了大幅的升级迭代，但随着新技术、新需求的不断涌现，以及为应对例如北、上、广、深等超大规模城市乘客出行特点所带来的新挑战，一个利用云计算技术的，架构更精简、运维更高效、支持无感改造的“基于云平台的城轨信号系统”成为必然的发展选择。

2. “云信号系统”的出现背景及应用

根据可查阅的材料显示，早在2018年西门子与奥地利铁路集团就“基于通用设备的联锁系统”展开了现场测试，并于2020年在奥地利铁路实地投入运营。这是信号系统中SIL4安全等级功能首次基于虚拟化技术进行落地实践，该实践证明了通过虚拟化技术承载大多数信号系统功能组件可能性。

而该实践也得到地铁建设、运营单位、行业专家越来越多的关注，同时，由于信号系统安全功能组件被虚拟化承载的可行性已被验证，也有一些信号系统集成商提出进一步将信号系统功能组件全面云化，通过应用云服务将系统智能化升级，更大程度的实现城轨信号系统灵活调度、高效运维、全域监控、实时智能调整运行方式的目标。

二、新华三助力城轨信号系统安全云平台的探索与思考

新华三长期以来致力于城市轨道交通行业数字化建设，通过提供ICT基础设施能力，助力地铁集团实现数字化转型，助力业务实现智慧化升级、迭代。近年来，通过不断与合作伙伴针对云信号系统的可行性评估、工程化落地方案进行深入研究，逐步打破了由于安全性、实时性等严苛要求导致的信号系统鲜有实质性创新的局面。

新华三与合作伙伴经过研究推出基于云平台的城轨信号系统架构，即由基础设施、云操作系统、功能组件、业务系统资源、业务系统应用软件等五层架构组成，其中主要攻坚点集中在云操作系统层与业务系统安全相关功能组件层的融合、适配与调优，在不影响业务系统实时性的前提下，充分利用云服务及其强大算力实现信号系统灵活的功能调度、智能管理及运维。

业务应用	SIL0		SIL2		SIL4	
	运行维护管理、网络管理		ATO、ATS		联锁、ZC、ATP、安全计算	
业务资源	裸金属	虚拟机	容器	容器虚拟机		
功能组件	应用管理	时钟管理	时延管理	维护管理		
操作系统	虚拟化管理、分布式存储、SDN管理、安全管理					
基础设施	计算设备、存储设备、网络设备、安全设备					

基于云平台的城轨信号系统

那么，如何实现在云平台上构建一个满足SIL4等级要求的信号系统？需要重点在以下几个方面进行研究，即可靠性、实时性、安全性、同步机制、信息安全，以解决由于云平台的加入带来的潜在风险和隐患，简单阐述说明：

可靠性：云平台统筹规划，与集成商一同做系统设计，例如原有SIL4级别安全系统的影响多停留于本站，现在上升到云平台层，虽然影响范围变成了整个线路或线网，但可以通过云服务协同联动站间功能组件的方式增加系统可靠性，或者在云平台外挂安全计算单元，使系统多一层保障，增加保障系统功能安全方式，灵活设计、选择方案。

实时性：根据安全功能控制周期（即输入到控制逻辑再到输出执行整个时间）的要求，通过云平台在平台层提供快周期的任务执行机制，满足有实时性要求的业务需求。

安全性：由于业务承载方式从服务器升级为云平台，这意味着系统复杂度上升，需要将平台与业务软件失效带来的影响最小化。可以通过软、硬件异构、多重表决等多种方式来应对。例如，当一个业务进程表决不通过，有序退出再经过同步重新进入，云平台强大的计算能力，可以既满足多重表决的性能需求，也兼顾安全和可用性，避免简单地导向系统宕机的机制。

信息安全：功能安全设计并不能覆盖信息安全攻击带来的影响，由于云服务与业务系统功能调度的深度相关性，需从全生命周期考虑信息安全威胁以及防护机制，新华三结合云计算和工控系统信息安全的总体需求，打造了一套面向信号安全云系统的满足等保三级的网络安全体系。

目前，经过先后数轮测试，初步验证了云平台计算、存储、网络等服务在满足业务逻辑的前提下与业务系统协同调度的可行性。

三、城轨信号系统安全云平台的优势

基于云平台的城轨信号系统一旦完成验证和工程化实践，对城市轨道交通型号系统成本优化、行车控制、运行维护等多方面能力和效果都会带来飞越式的提升。

首先，其可以精简复杂的系统硬件设备架构，减少硬件投资，更高的经济效益并有利于可持续发展。

其次，充分利用云服务及其强大算力可以更灵活的做功能调度与智能管理。

再次，支持实时、全面的设备监控功能，实现更高效的维护服务。

最后，云信号系统采用精简、统一化的硬件架构设计，这可以让业务系统在升级或改造时仅关注于应用软件本身，最终实现“无感改造”。

展望

下一步，新华三将与合作伙伴在“单主机、虚拟机、容器失效影响分析”、“虚拟机间可预测性分析”、“多任务安全执行保障机制”、“非预期性行为监测与可控”等方面继续加大投入，持续测试与优化。

未来，城市轨道交通信号系统一定会从现有的传统建设、运行模式转向基于云平台的城轨信号系统的建设、运行模式，这种智能化升级，不仅可以精简复杂的系统硬件设备冗余设计，减少硬件投资，提高线路运维的效率和灵活性、更实时全面的进行设备监控，还便于后期的旧线“无感改造”，最终实现动态时刻表，改变城市轨道交通运营的方式、乘客出行体验，为城市绿色高效出行、智慧交通可持续发展提供新的支撑和动力。



城轨云安全体系建设研究

文/张一琛

一、城轨行业的网络安全问题

1. 城轨安全的整体框架仍需完善

在城市轨道交通跨入蓬勃发展的黄金机遇期，城轨云建设也已进入到大规模开发和应用阶段。然而城市轨道交通行业尚未形成统一的、成体系的信息网络安全建设思路，仍旧将等保测评要求作为面临传统安全威胁和新兴云平台安全威胁的唯一安全基线，业务和云平台难以剥离，安全建设缺乏统一规划，迫切需要完善的城轨安全整体框架来指导城市轨道交通信息系统网络安全的长期演进。

2. 等保测评难匹配城轨行业的安全特性需求

在国内全行业统一执行的《信息安全技术网络安全等级保护测评要求》不完全匹配城轨行业的防护场景，难以针对新兴的云平台、云上租户安全、容器安全、数据安全、各业务特征进行专属安全防护，需要额外参考诸如《智慧城市轨道交通信息技术架构及网络安全规范》、《数据安全法》等标准来完善城轨安全建设。

3. 城轨云的建设引入新的威胁风险面

云安全联盟CSA罗列出了最为常见、危害程度最大的7种威胁：滥用和恶意使用云计算、不安全的接口和API、心怀好意的内部人员、基础设施共享问题、数据丢失或泄露、账户被劫持，以及其他未知的风险。将上述风险类型归纳，主要包括5类城轨云安全风险。

3.1 城轨云访问授权的身份假冒

城轨云平台基于网络为各个业务应用提供云服务，即作为各业务系统访问的第一道防线。一旦攻击者获取到用户的身份验证信息，假冒合法用户，用户数据将完全暴露在其面前，其他安全措施都将失效，攻击者将可以窃取、修改用户数据，窃听用户活动，恶意消费等。因此，合适的身份认证机制对于确保身份识别信息的安全性至关重要。

3.2 城轨云资源共享的风险

城轨云中软硬件平台通过虚拟化为多个运营公司或者运维管理员担当的租户所共享，以此实现IT资源利用效率和灵活性的最大化，但是虚拟化技术也打破了物理安全边界，使得各租户间隔离更加脆弱，之间的恶意代码传播更加容易，常出现数据泄露到多租户的情况。

3.3 城轨云数据安全及隐私泄露

城轨云业务系统产生的生产管理数据在传输、处理、存储的各个环节都存在泄露和被篡改的风险。疏于防范的信号系统、AFC系统客户端可能被黑客控制或者运行木马程序，导致重要数据从终端泄露或者被篡改；综合监控系统和时钟、ATS、ACS等业务之间有接口，需要接收数据并监管各业务系统，进而导致数据被过度访问甚至篡改。

3.4 城轨云平台本身存在风险

城轨云平台以多种标准和协议为基础，包含虚拟机管理软件、操作系统、中间件及各类应用系统等大量软件，系统非常复杂，且地铁业务系统的保守性直接导致云平台多年不更新版本，因而很难避免漏洞的存在，防护不当的计算和存储会导致用户的私密数据被非授权用户非法访问。

3.5 城轨云与业务系统之间的风险接口

城轨云会按照三网架构内不同类型应用，将硬件和平台的API接口开放给应用软件和用户，由用户将其集成到上层应用，按需使用。不安全的API将使云计算应用面临极大风险，如通过API实施注入攻击，可能篡改或者破坏用户数据。

3.6 城轨云原生安全建设的忽视

城轨行业的ITP业务、能源管理、智能火灾报警等诸多新应用开始尝试采用容器微服务框架开发部署，云原生平台和云平台有着本质区别，但是云原生安全风险评估和防护机制仍缺乏统一标准，还处于探索之中。

二、城轨云安全体系技术全景研究

为了避免城轨行业在数字化网络化发展过程中出现信息安全和网络安全问题，保证当下城轨信息技术系统和未来智慧城轨系统的传统架构安全、云计算环境安全、工控安全、数据安全以及主要业务系统安全，结合诸如北京地铁、太原地铁积累的顶层规划设计经验，南京

城轨云安全落地交付经验，再结合城轨行业的建设特点，本文提出新华三自主创新的城轨安全体系技术全景图，如下：

国外理论参考模型 网络滑动标尺模型	基础安全建设	被动防御	主动防御	情报收集	进攻防御
国内的建设理论模型	政策驱动（当下阶段）	安全事件（已知威胁）驱动	未知威胁驱动	安全运营中心 SOC、漏洞安全体系运营与审计工作的自动化能力	安全及服务驱动
云上安全	IaaS 云安全	1. 等级测评：云平台统保，云租户安全 2. 密评测评	1. 态势感知和其他安全设备的联动 2. 零信任的SOP、微隔离		1. 风险评估：信息安全风险评估，新系统上线评估 2. 漏洞扫描：安全规划与漏洞扫描，数据安全治理保障 3. 工程实施：安全加固服务，安全产品维护服务 4. 攻防对抗：安全应急响应服务，安全攻防演练服务 5. 教育培训：攻防对抗培训，实验室共建服务
	PaaS 微服务安全	PaaS过等保，作为云平台的一部分，复用云平台统保，过等保2.0测评	PaaS平台全套设施的安全方案，含有容器、微服务、数据库、中间件的完整性防护		
	Daas 大数据安全	Daas过等保，大数据平台算作云平台的一部分，过等保2.0测评	大数据数据安全体系防护		
云下安全	传统网保	等级测评：一中心三重防护	态势感知和其他安全设备（含探针）的联动		
	工控安全	依据《信息安全技术 网络安全等级保护基本要求》《工业控制系统的信息安全扩展要求》、《工业控制系统信息安全防护指南》、《关键信息基础设施网络安全保护条例》过等保2.0的测评	工控安全运营平台发挥全局联动功能 重点工控安全监测与审计设备作为探针		
	数据库安全	等级中的数据安全防护：二级或三级测评中数据备份和有效性 《数据安全法》的安全防护需求	安全日志的历史数据的安全数据库安全防护体系		
新华三安全理念3.0	全网感知零信任		业务安全新中台	业务运营新服务	

1. 城轨安全建设理论模型

中城协提出纵深防御，安全可控的二十字方针：系统自保，平台统保，边界防护，等保达标，安全确保，其整体思路是结合城轨行业特性的等级保护建设的一种延伸，但仍处于被动防御阶段。

城轨行业在安全领域需求已逐步过渡到“主动安全”的范畴，倡导“主动发现，智能分析，提前预警，及时响应”的建设思路，与广为接受的国外网络滑动标尺模型不谋而合。网络滑动标尺模型将企业信息安全能力建设分为五个阶段：基础架构阶段，被动防御阶段，积极防御阶段，威胁情报阶段和进攻反制阶段。如果结合我国城轨安全建设的阶段特点，可以凝练为四个阶段：安全政策驱动阶段，安全事件驱动阶段，未知威胁驱动阶段和安全即服务驱动阶段。

安全政策驱动阶段：基于网络安全法律法规进行初步的安全防护建设。纵观全国，很明显各地地铁公司的安全建设几乎都是政策驱动，以过等级保护测评为目标。

安全事件驱动阶段：基于已知的外部威胁及安全事件进行的事前事中事后的安全防护建设。在满足等级保护建设之后，如果考虑继续完善城轨安全防护体系，那么就可以结合具体城轨行业常见的威胁风险有针对性的完善安全建设，从而进入到主动安全阶段。

未知威胁驱动阶段：基于潜在的威胁风险，进行的识别、阻止、缓解威胁攻击，发现控制有效性不足的安全防护建设。主动跟踪行业内前沿的安全技术发展，及时关注收集漏洞发布信息，并联合相关科研院所进行专业性研究和防护。

安全即服务驱动阶段：基于安全现状的梳理而进行的安全评估类、运营类、运维类、培训类和规划类服务的提供。

2. 城轨云安全建设

在过去几年的城轨安全实践中，参照“系统自保”的原则建设后，发现城轨安全出现一个棘手的问题-各系统厂商采用的安全建设手段不统一。为了避免全网中安全设备孤岛化，各设备难联动，每年都要重复造轮子等问题，因此考虑城轨云安全建设需要由安全厂商统一负责，参考传统业务安全建设模式，结合云上租户安全的规划，实现云上云下统一步调的安全体系。

在云平台的IaaS层面，遵照中城协提出的“平台统保，系统自保”的安全建设原则，结合全国已有案例实践，提出“融汇平台统保，贯通系统自保”的新建设理念。平台统保需要融汇既有和新建的软硬件安全资源，系统自保需要在原有各业务系统建设安全防护的过程中时刻强调租户防护的贯通。确保贯通云平台和业务系统租户的安全建设，贯通安全设备的联动，避免安全建设的一盘大棋被下成各自为政的安全孤岛。

2.1 融汇平台统保

新华三城轨云安全通过“云网安一体化”的建设思路，打造具备完善安全能力的云平台。将安全能力与云平台、SDN网络、虚拟化平台等深度融合，并在云平台上呈现唯一用户接口，灵活、高效地实现云安全的整体交付。以等级保护三级作为基线，将云平台视为地铁运行的一个业务系统，并进行外部基础架构的安全防护和内部虚拟化安全的策略部署。

◆城轨云平台的安全管理中心

城轨云平台本身的等保建设需要首先考虑整个安全体系的大脑，即安全管理中心。安全管理中心包括系统管理，审计管理，安全管理和集中管控。前三者的设定是基于三权分立思想提出，要求系统、审计、安全管理员各司其职，协同管理。

系统管理、审计管理、安全管理均要求对其管理员进行身份鉴别，限定操作方式，并对其操作行为进行审计，因此在安全管理中心常采用安全运维审计设备实现。常采用态势感知和日志审计设备对审计数据进行汇总和集中分析，对安全策略、恶意代码、补丁升级等事项进行集中管理，同时能对网络的各种安全事件识别、报警和分析。

◆ 城轨云平台的安全区域边界

安全区域边界内容细分包含边界防护、访问控制、入侵防御、恶意代码和垃圾邮件防范、安全审计以及可信验证等多个部分。可以采用下一代防火墙应对边界完整性检查，使得跨边界的访问和数据流经过边界设备的清洗后再通信。

◆ 城轨云平台的安全通信网络

安全通信网络从根本上对整体架构的安全性、冗余性和业务处理性能提出了针对性要求。比如网络设备应满足业务高峰时的带宽需求，这需要在方案设计阶段给出交换机网络设备具有合理的参数和策略。地铁生产业务系统中，因涉及民生安全，极少有VPN使用场景，所以城轨云的安全通信网络的建设更应该关注在网络设备的性能、区域划分、隔离、链路选择等策略的实现上。

◆ 城轨云平台的安全计算环境

安全计算环境必然离不开管理用户的登录和访问，其权限设置则需要依赖堡垒机，可见安全设备的作用并不局限在某一个位置上，而是在一个中心三重防御中多处反复体现。关键数据库审计功能要覆盖到每一个云租户，对异常的租户行为进行审计，虽然数据库审计放在了安全管理中心，但是也会在安全计算环境中发挥作用。以此类推，安全计算环境的安全审计依赖态势感知、日志审计等，入侵防范和恶意代码依赖防火墙或IPS。剩余的终端PC、工作站或服务器的安全和数据防护，需要在终端部署主机安全卫士、EDR等终端安全管理软件守护好最后一道防线，从而达到等保合规，满足网络安全法等政策要求。

2.2 贯通租户自保

新华三城轨云安全建设过程中提出安全即服务（security as a service）的理念，为云计算基础设施和云承载的IaaS、PaaS和SaaS提供南北向及东西向的安全防护能力。一体化方案从逻辑控制层的角度出发，屏蔽底层技术细节，将各类安全能力从单纯的产品配置转变为服务化配置，将繁琐的安全业务重新进行定义，从用户业务的角度出发，抽象为必要的实现逻辑。

安全防护主要分为三个层次，包含控制平面、数据平面和日志平面。

控制平面：主要通过网络控制器将网络和安全进行流量引导和策略下发，在云安全服务中心中为每一个租户也分配独立的安全资源，并打通安全资源与云计算资源的路径，实现安全资源与计算资源的衔接。

数据平面：通过专用硬件资源和NFV实现快速弹性的资源池化，通过专用硬件资源为所有租户提供高性能流量处理以及基于策略的快速转发；针对个性化的应用层安全能力，可以通过NFV的方式实现单租户个性化业务的快速部署，满足个性化需求。

日志平面：云安全资源池部署位置位于云计算存储资源池，能够处理95%以上的南北、东西向流量，可以全面抓取进出云租户的全部流量，所以在云平台内通过结合各大虚拟审计设备系统，可以分别对租户的外部威胁和流量进行完整的分析，为云租户分别呈现各自的整体安全态势。

新华三城轨云安全资源池在逻辑上可以细分为两大类：安全防护资源池和综合审计资源池。

◆ 城轨云租户的安全防护资源池

南北向安全防护

依据建设需求，利用硬件防火墙虚拟化实例技术通过区域边界划分和安全隔离，实现内部边界重塑，确保各业务系统重新树立安全边界。在平台边界进行多层防御，采用防火墙硬件设备实现云网络和其他区域的边界隔离，以帮助应对网络边界面临的外部攻击。

东西向安全防护

在云平台内部的计算环境中，虚拟机之间的虚拟交换组件使得安全计算域的划分、域内的结构安全、访问控制、边界完整性和通讯保密性等都变得较为复杂。针对虚拟机内部网络的数据隔离、过滤和基于VLAN的策略执行，都采用东西向的虚拟防火墙、云入侵防御等综合方案来实现云平台的安全。

利用防火墙的硬件虚拟化技术，构建防火墙基本策略，实现虚机与虚机之间的微隔离，实现跨VLAN的安全访问控制，实现东西向的安全访问控制，从而确保云租户、云服务方或第三方云资源的安全访问、使用和管理。

云平台内存在大量主机，其底层和业务应用系统的安全漏洞多是来自于最基础的TCP/IP协议漏洞，也可能是来自于操作系统、数据库或应用程序漏洞。构建入侵防御安全策略，对访问云平台的外部流量进行分析、检测、过滤，防护SQL注入，对攻击行为进行识别预警，从而发现网络攻击行为、识别网络攻击类型，并过滤网络攻击流量。

◆城轨云租户的综合审计资源池

租户级数据库审计

为云平台上每一个租户部署一套虚拟数据库审计，实现租户数据库的独立审计。虚拟数据库审计提供代理插件，以解决云环境数据库流量的精准审计。数据库审计系统通过全面记录对数据库服务器的连接情况，记录会话相关的各种信息和原始SQL语句。

租户级运维审计

为每一个租户部署一套虚拟堡垒机，实现租户级别的独立运维审计。通过引流方式将运维人员对各类IT资产的管理流量牵引至虚拟运维审计组件中，实现资产集中管理，单点登录，运维安全策略下发和运维安全审计。

租户级漏洞扫描

为每一个租户部署一套虚拟漏扫，实现租户级别的独立漏洞扫描工具，和云平台方案一致，通过漏洞扫描系统，实现各业务系统或主机脆弱性的统一管理。

租户级日志审计

为每一个租户部署一套虚拟日志审计，实现租户级别独立的综合日志审计能力，和云平台一致，对安全设备如防火墙、Web应用防火墙、数据库审计、网络行为审计等产生的安全日志进行收集，再结合操作系统日志、中间件日志等，综合对这些日志进行关联分析，从多个维度对目标的运行状态、主机情况进行分析，得出一段时间内目标系统及相关设备的安全运行状态。

通过城轨云安全服务中心的搭建，统管各项软硬件安全设备，构建安全资源池，同时复用云平台的SDN服务链引流串接安全资源池中的安全原子资源，将虚拟机、容器细颗粒度的安全资源划分到对应的业务系统上，从而实现安全厂商统一保障云平台以及业务系统一体化的建设模式。

3. 城轨云原生安全建设

新华三城轨云在建设中，涉及到了能源管理、信号智能运维和智能运营业务的容器微服务化的部署。其运行环境和云平台的虚拟机有着本质的区别，但是当前全行业缺乏相关安全规范要求，因此暂时划归到城轨云的一部分来复用城轨云的安全保障措施。该方法不具有持久性，因此借鉴互联网和金融行业的云原生安全案例，整理出针对城轨行业的云原生安全的初步建设思路。

3.1 城轨云原生平台的容器安全

城轨云原生平台的容器运行的全生命周期主要包括容器镜像、容器配置和容器运行三个阶段，保障这三个阶段容器的安全运行便是容器安全工作的重中之重。

容器镜像安全需要通过镜像数字签名技术防止镜像被篡改或损坏。在日常构建镜像时，接入白盒扫描，一旦核查出错就会直接中断CI构建，阻止后续代码的持续集成。

容器配置安全常采用Dockerfile核查技术判断容器文件是否具有漏洞以防被恶意利用，另外也会采用强制访问控制技术保障每个主体和客体之间都有一个安全标记。容器之间的隔离则借助Cgroups限制宿主机中不同的容器的资源使用量，借助namespace保证容器与容器，容器与宿主机的资源隔离。

容器运行时的安全则依赖于HIDS实时监控计算机内部的动态，以及黑白盒扫描来对应用功能的程序源代码进行查漏补缺。

3.2 城轨云原生平台的微服务安全

城轨云业务系统如互联网售票系统ITP的解耦部署会带来大量的微服务应用，跨多个微服务的调用会导致请求更难追踪，微服务之间共享上下文会要求信息传输中能够防泄漏防篡改。因此，在微服务的入口网关处需要提升身份认证和授权的安全性，需要能够类似传统防火墙对外部流量控制扫描以及能够在微服务访问链路中进行传输加密避免信息劫持。

3.3 城轨云原生平台的DevOps安全

DevOps安全需要关注内部研发团队的自研代码和外部第三方开源软件的安全，对于开发用到的代码所使用的依赖关系必须明确。如果底层依赖有风险，必须快速反向分析哪些软件会受到同样的威胁，常通过单元测试、静态扫描等基本手段进行代码安全合规性检查，扫描结果

一般包括bug、坏味道和漏洞等，方便在代码构建之前发现潜在的安全风险。

3.4 城轨云原生平台的中间件安全

在整个云原生环境中，中间件如MQ（Kafka、RocketMQ等）、Redis基本都是运行在云平台的虚拟机中，因此该组件的安全防护可以复用云安全服务中心的防护策略。

4. 城轨云下的传统架构的安全建设

全国城轨云的建设几乎都是针对新建线路开展的，老旧线路因为每天的运营的需求，无法短时间内进行业务迁移上云，更多的是将老旧线路的传统IT架构设施尝试接入到城轨云的网络之中，然而老旧线路并不能完全复用城轨云安全设施，只能继续参考以往模式-单线路单业务系统的二级或三级的等级保护测评的建设要求，其建设思路和城轨云平台统保思路一致。

5. 城轨云数据安全建设

城轨行业的数据存储在安全的终端环境中，也就是在云平台 and 租户都满足各自安全基线的前提下，继续保障数据安全，由此后续的数据安全建设便可以剥离云平台的干扰只考虑数据本身的安全性了。

目前国内已颁发《网络安全法》、《信息安全技术个人信息安全规范》等相关的法律和规范。为适应日趋严格的数据安全监管要求，并能灵活应对城轨业务的变化，在数据分类分级的基础上，遵循最小权限和动态授权原则，在数据全生命周期各个阶段建立数据可信接入、数据加密、数据脱敏、认证授权、数据操作审计等措施。整体流程可概括为满足数据安全政策驱动达标，保障日志等历史数据的安全以及备份的有效性，加强终端数据防泄漏，最后做到专项敏感数据防护。

从而实现如下目标：

- ◆数据可见：数据分布可见、数据流转可见、数据访问可见。
- ◆数据风险可控：风险驱动，减少数据安全风险暴露面，提升整体安全效能。
- ◆数据可管：贯彻IPDRR的理念（识别、保护、检测、响应、恢复），实现数据全生命周期可管。

三、未来城轨安全技术研究

城轨行业的网络安全建设方兴未艾，安全领域还有大量安全技术手段没有落实到项目实践和安全体系规划当中。

诸如基于城轨云安全服务中心建设云安全运营平台。2016年4月19日，习近平在网络安全和信息化工作座谈会上发表讲话强调：全天候全方位感知网络安全态势。知己知彼，才能百战不殆。没有意识到风险是最大的风险。随着时间的推移，安全大脑态势感知等设备的安全日志日积月累，越来越多，这时需要以态势感知作为日志的统一管理出口，将采集后的日志传输到安全服务厂商，经过安全服务商的安全中心建模，给本地用户提供云安全SaaS服务和云安全运维服务。让专业的人做专业的事，从而解放用户的安全管理压力。

考虑到城轨行业因其基础架构的复杂性，整个安全防护方案中缺少一个强统治力的安全智慧大脑。在城轨行业的安全建设中，将态势感知与统一运维管理平台合二为一，实现“安全+运维”的防护手段，将网络和安全融汇通，践行云网安融合的安全理念。同时态势感知可以适配云上云下不同场景，通过云安全服务中心集成态势感知，将网络安全和统一运维横向覆盖了云上云下全场景，进而做到了后台云网安一把抓，极大地释放了用户的管理压力。

另外还有身份认证加强版的零信任技术，安全颗粒度精细化的微分段技术以及量子密码技术等都可以在城轨云安全的土地上不断深耕，未来智慧城轨的安全建设需要摆脱传统设备的桎梏，大胆打开思路，尝试将新颖的安全防护技术纳入到安全体系建设中，注入新鲜血液，让城轨的安全建设体系不断升级迭代，与时俱进，才能真正推动城轨行业的安全能力达到领先水准。

城市轨道交通云平台安全资源池 最优方案探讨

文/沈明宇

—以某市轨道交通生产业务云平台为例

随着近年来我国城市化进程的不断加快，城市轨道交通建设如火如荼，为了实现地铁各业务系统统一部署、数据集中管理，《中国城市轨道交通智慧城轨发展纲要》将城轨云作为智慧城轨纲要的重点建设之一，极大加快了城轨上云的建设进度。

当前，全国各大城市所建设的城轨云，无论是专业云、线路云、抑或是线网云，工作重心均在业务系统入云，但业务系统所需的安全资源并未能由云平台提供，即“业务系统入云，业务安全未入云”。在这样的情况下，各业务系统的安全能力仍采用云下各自建设、各自管理的方式。这种割裂的、烟囱式的建设管理方式，存在重复建设、成本高、资源固化浪费等问题，而云平台安全资源池的出现就是为了解决上述问题。云平台除统一提供自身三级等保能力之外，也为各入云业务系统提供所需的云安全服务，从而提供计算、存储、网络、安全等全方位的云服务能力。

云安全资源池通过不断地汇聚云安全能力，构建一个统一管理、弹性扩容、按需分配、安全能力完善的云安全池化能力体系，可帮助用户实现云安全运营和云安全统一管理，快速应对云上租户安全问题，为用户提供一站式立体化的云安全综合解决方案，针对性解决用户业务上云后面临的难点与痛点。智慧城轨的基础是云计算，伴随着云计算的到来，城轨云安全资源池的建设成为智慧城轨必不可少的一环。

某市作为国内轨道交通建设线网规模最大、线路长度最长城市，具有代表性。本文以某市轨道交通生产业务云平台为例，探讨城市轨道交通云平台安全资源池建设的最佳方案。

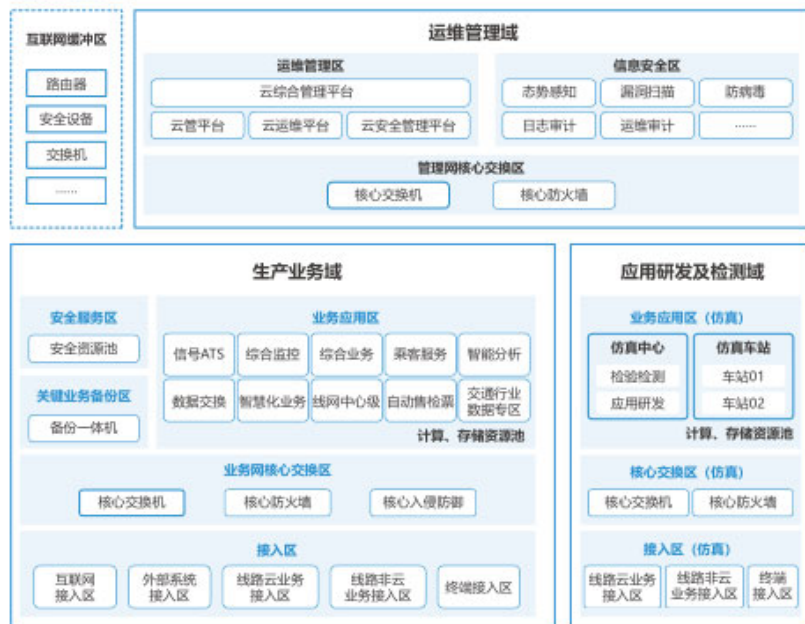
一、总体需求

1. 现状分析

1.1 生产业务云平台安全建设

某市轨道交通生产业务云平台数据中心架构如下图所示。在中心生产业务云平台部署

CloudOS云管平台进行统一运营管理。整体网络区域分为生产业务域、运维管理域、应用研发及检测域、互联网缓冲区。生产业务域是中心云平台的核心区域，各业务系统服务器运行在本区域；运维管理域包括云管平台、云运维平台和云安全管理平台，以及云平台自身的信息安全区。



云平台自身安全在防御能力、监测能力和检测能力三方面建设情况如下：

防御能力

- 部署核心防火墙、边界接入的线路云业务防火墙、线路非云业务防火墙、外部系统防火墙、业务和管理网边界防火墙、各车站节点车站防火墙做访问控制，保证区域间互访的安全性。核心接入防火墙按照每个租户划分虚拟防火墙实现租户间的安全边界防护能力。
- 在核心交换区部署IPS防御外部入侵攻击。
- 通过主机安全软件对云主机/服务器进行统一病毒查杀防护。

监测能力

◆信息安全区部署堡垒机对云平台运维人员的操作行为进行审计和监控，部署日志审计实现云平台设备一体化日志收集审计，数据库审计实现对数据库的操作进行审计。

◆资产管理：通过云管理平台对上云资产进行登记记录。

◆通过安全态势感知实现对云平台网络安全状态的一体化监视、展示。

检测能力

信息安全区部署漏洞扫描系统实现对云平台网络安全设备、服务器、数据库、Web应用等的漏洞风险发现。

1.2 业务系统安全建设

云平台目前根据业务系统划分为信号资源池、综合监控资源池、综合业务资源池和数据分析资源池4个资源池，再按不同线路划分不同VPC，云平台已通过等保三级测评。各线网中心级系统和线路级业务系统按照等级保护要求进行安全建设。根据《智慧城市轨道交通信息技术架构及网络安全规范第3部分：网络安全》要求，各系统应满足的网络安全保护等级如下：

业务系统	网络安全保护等级	业务系统类别	
TCC	三级	线网中心级业务系统	
ACC	三级	线网中心级业务系统	
信号 ATS	三级	线路级业务系统	
综合监控系统	三级	线路级业务系统	
多线路集约化电力监控系统（MSCADA）	三级	线路级业务系统	
多线路集约化环境与设备监控系统（MBAS）	三级	线路级业务系统	
多线路集约化火灾自动报警系统（MFAS）	三级	线路级业务系统	
通信系统	专用电话系统	二级	线路级业务系统
	综合无线通信系统	二级	线路级业务系统
	视频监控	二级	线路级业务系统
	公务电话系统	二级	线路级业务系统
	乘客信息系统	二级	线路级业务系统
	广播系统	二级	线路级业务系统
	时钟系统	二级	线路级业务系统
	线路传输系统	二级	线路级业务系统
	通信综合数据网络	二级	线路级业务系统

业务系统	网络安全保护等级	业务系统类别
自动售检票系统（AFC）	二级	线路级业务系统
乘客服务系统	二级	线路级业务系统

2. 安全需求

业务系统安全建设应符合国家网络安全等级保护要求，同时需结合轨道交通网络安全规范要求。为满足某市轨道交通业务安全管理需求，需要在轨道交通生产业务云平台当前建设的基础上，按照等级保护要求和信息系统密码要求建立完善的纵深安全防护体系，包括：

◆满足国家相关部门的安全标准和规范：符合《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）标准的相关要求。符合国家网络安全法的相关要求，其中相关日志、运行数据至少留存6个月。

◆构建安全资源池提供安全服务：配置能够满足业务系统安全需求所要求的各类安全软硬件和存储资源，并可针对不同的业务安全需求，提供不同类型的安全资源和服务。

◆形成全域纵深防御体系：针对可能遇到的各种安全威胁和风险，分别在边界防护、系统安全、身份认证、安全管理、安全监测等方面采取行之有效的技术和管理措施，形成功能完善的信息安全保障体系，并进行监督管理。

二、城轨云安全资源池最优方案探讨

1. 方案思路

1.1 生产业务云平台安全建设

云安全资源池为生产业务提供安全服务，整体建设思路如下：

- ◆根据轨道交通生产业务云平台架构，规划安全资源池部署方案。
- ◆根据合规要求及业务安全防护情况，梳理安全服务能力需求。
- ◆部署安全资源池，根据业务系统规模数量，规划安全资源池服务软件资源。
- ◆云平台提供的云安全服务与业务系统云下部分按照等保要求建设的安全边界防护设备协同保障业务系统整体安全。

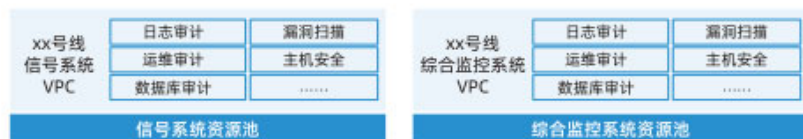
2. 总体架构

2.1 云安全资源池定位

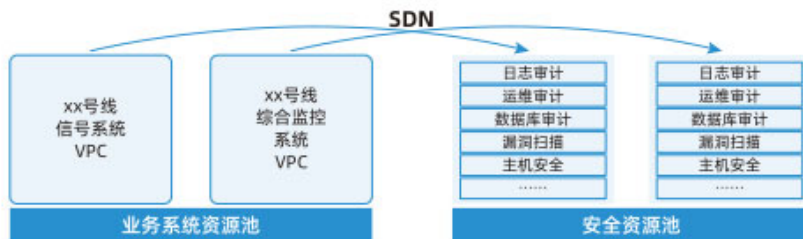
基于某市轨道交通生产业务安全防护需求，构建云安全资源池，将安全资源池化，为线路级/路网级业务系统提供安全服务。通过构建统一的安全资源池，业务系统按需申请云安全服务，云上安全业务快速部署，自动下发策略，避免传统安全设备采购、上线等冗长的周期。安全资源云端统一运维，提高解决问题的效率，降低故障响应时间。

2.2 技术方案比选

通常，云安全资源池有混合部署和独立部署两种技术方案。



方案一采用混合部署方式，即在业务系统资源池本地混合部署云安全资源池。将所需安全组件部署在本业务系统VPC内，为其提供安全防护。该方案安全组件需要占用对应业务系统VPC内的计算、存储和网络资源。

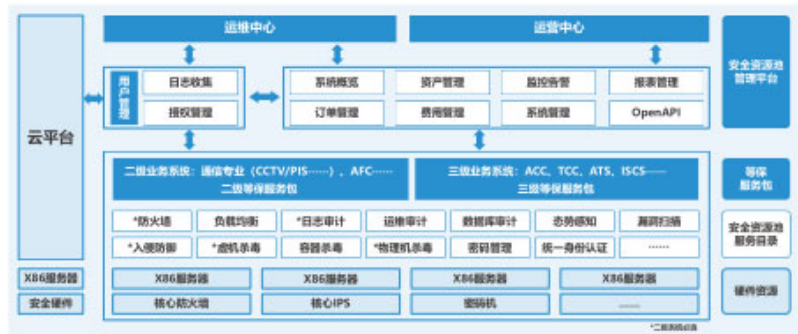


方案二采用独立部署方式，建设独立的安全资源池，部署业务系统安全VPC，利用SDN打通对应业务系统的VPC网络，为其提供安全防护。安全资源池的计算，存储，网络资源可独立分配。

通过对比以上两种方案可以发现，方案一，适用于超融合或云平台规模较小的场景，存在计算节点和安全节点故障相互影响，管理界面不清晰的问题。方案二适用于云平台规模较大的场景，其管理界面清晰，计算节点和安全资源池发生故障互不影响，便于故障定位，但搭建独立的安全资源池需要网络等基础设备的投资。

结合某市生产业务云平台的规模以及未来的发展规划，推荐使用独立部署方案。

2.3 安全资源池整体架构



构建独立云安全资源池，为业务系统提供云安全服务，各项云安全服务可按需扩展。在云平台管理区部署云安全管理平台，统一管理云平台安全资源池的各项云安全服务。安全资源池通过将底层硬件安全设备NFV功能虚拟化或采用安全软件加虚拟化服务器的形式部署，可以形成包含防火墙、负载均衡、日志审计、运维审计、数据库审计、态势感知、漏洞扫描、入侵防御、虚拟机杀毒、容器安全、物理机杀毒、统一身份认证、密码安全等在内的安全服务目录。并可以等保服务包的形式为二级业务系统和三级业务系统分别提供不同的安全服务组件组合，形成标准的安全服务建设内容。

通过安全资源池管理平台对用户、日志、授权、系统、资产、监控告警等进行管理，并与云管平台融合，形成统一的管理界面。同时还可将相关数据同步至运维中心或运营中心，辅助运营团队、运维团队生成相应的安全生产报告。

2.4 与既有云平台对接

云安全管理平台作为云平台的一个组件，部署于云平台上。通过登录云平台，完成云安全管理平台组件的部署，即启用相关功能。

云安全管理平台与既有云平台兼容，可实现业务系统/账户/资产信息同步；可实现对各类云安全服务的资源管理、策略管理、资源监控等，并在既有云平台上形成云安全服务目录；可调度既有SDN控制器，对安全服务进行引流、编排和配置下发。

3. 技术方案

3.1 云安全管理平台

云安全管理平台实现对各类软硬件安全资源的纳管，提供安全服务化、流量编排、策略管理、计量计费、态势呈现等诸多功能。



◆安全资源纳管

云安全管理平台可实现安全资源的全生命周期管理，包括热启动、安全防护策略的管理、安全服务的网络编排调度、安全服务的日常运营以及运维的统一化审计。

◆业务系统可持续运营

安全管理平台同时也是一个安全资源的运营平台，在分发安全资源同时，提供运营管理功能，管理员通过运营分析能够对安全服务运营情况了如指掌，从而达到一个平台统管各类安全资源的目的，有针对性地制定运营策略，达到精细化运营的目标。

◆可视化运营运维大屏

云安全管理平台的可视化大屏是针对城轨云安全综合运营情况所展示的数据大屏。包括整体云安全的评分、风险资产、风险业务系统Top5排名、运营过程中需要关注的告警信息等。



可视化大屏示例图

运营大屏主要展示以业务系统维度，统计各个业务系统的资源使用情况、工单情况、以及安全投入等综合数据情况。

运维大屏主要展示运维角度的综合数据，主要包含安全资源池的资源占用率、运维告警、运维工单跟踪等。

3.2 云安全资源池

安全资源池采用“虚拟化安全软件+安全硬件NFV”的方式进行部署，所有资源归属云安全管理平台纳管。可提供的云安全服务包括虚拟防火墙、虚拟运维审计、虚拟日志审计、虚拟数据库审计、虚拟漏洞扫描、虚拟态势感知、主机安全、统一身份认证、密码安全等。业务系统可以通过云平台申请相应的虚拟化安全产品部署在自己的VPC内。

◆部署通用x86/ARM服务器、专用硬件作为安全资源池载体，服务器数量根据业务需求量而定，可以按需平滑扩展。服务器通过安全资源区的Leaf交换机接入到业务网。

◆服务器上运行虚拟主机，每个主机承载一个安全业务，业务系统申请时，按照虚拟机方式交付。

◆流量通过SDN技术引流到VPC内部安全池相应的安全虚拟机上进行安全处理，然后转发到最终目的地，从而可以实现虚拟机迁移后相关安全策略可以自动跟随。

3.3 兼容性

云安全管理平台提供丰富的REST API接口与第三方系统对接，根据第三方系统的业务需求，提供相应的API接口的定制开发，保证与第三方应用系统的对接，实现一个安全与平台兼容的系统。

云安全管理平台通过开放北向API接口对接第三方平台，涉及租户管理或同步、主机管理或同步、网络同步、防火墙、负载均衡、漏洞扫描、堡垒机、数据审计、日志审计等服务，可以满足多数用户API对接需求，对于客户新的API需求可以快速响应，通过快速开发相应的API接口，及时与用户系统进行对接。

在接口开发前，需要针对具体的业务需求，经过分析预演，制定出合理接口实现方案，满足接口原则及规范。云安全管理平台可提供完整的API接口文档，下表为主要API接口类别以及相应功能说明。

API类别	说明
安全资源池管理	提供云安全资源池服务的列表查询、新增，云安全资源池服务的详情信息，包括型号、实例状态、分配状态、安全可用域等接口
防火墙管理	提供防火墙的创建、查询、编辑、删除，防火墙策略的创建、查询、编辑、删除，IPS/防病毒的创建、查询、编辑、删除等接口
运维审计管理	提供运维审计服务的创建、查询、编辑、删除，单点登录等
数据库审计管理	提供数据库审计服务的创建、查询、编辑、删除，单点登录等接口
日志审计管理	提供日志审计服务的创建、查询、编辑、删除，单点登录等
漏洞扫描管理	提供漏洞扫描服务的创建、查询、编辑、删除，漏洞扫描任务的创建、查询、编辑、删除，漏扫报告查询等接口
操作日志	查询所有操作日志
定制API接口	数量业务应用需求，提供API接口定制

4. 云安全服务模式

4.1 云安全服务组合包

按照等级保护要求，云安全资源池可提供定制化的安全组合包。如二级业务系统云安全服务组合包如下：

必选组合包：防火墙、入侵防御、防病毒、日志审计。

推荐组合包：数据库审计、运维审计、漏洞扫描、态势感知。

等保三级系统云安全服务组合包如下：

必选：防火墙、入侵防御、防病毒、日志审计、运维审计、数据库审计、漏洞扫描。

推荐：态势感知，密码安全等。

4.2 云安全服务提供方式

云安全服务提供方式主要分为托管模式和半托管模式两种。

在云安全建设阶段，无论是托管模式还是半托管模式，云平台需要负责防火墙，入侵防御等安全能力的建设。半托管模式云平台需要根据业务系统接入终端的地址，在云平台接入网络设备和防火墙上配置相应的放通策略，保证业务系统的安管终端可以接入云平台的网络。

在安全运营阶段，云平台需要对防火墙等云安全服务进行开通，同时还需要将防火墙，入侵防御等防护类安全服务分租户配置相应的安全策略，还需要按租户分配数据库、日志审计等审计类安全服务的账号和权限。

安全设备巡检，安全事件分析，系统漏洞扫描，安全加固建议，云审计，服务策略，配置优化等建设内容，托管模式由云平台负责，半托管模式由业务系统负责。

在安全维护阶段包括保护资产管理，漏洞修复和风险处置等方面的内容均由业务系统负责。

阶段	建设内容	托管模式	半托管模式	职责说明
安全建设	安全能力资源建设	云平台	云平台	负责防火墙、入侵防御、数据库审计、日志审计、运维审计、漏洞扫描、态势感知、主机防病毒等安全能力资源建设
	安管终端接入云平台网络	-	云平台	按业务系统接入终端地址，在云平台接入路径网络设备和防火墙上配置放通策略

阶段	建设内容	托管模式	半托管模式	职责说明
安全运营	云安全服务开通	云平台	云平台	防火墙、入侵防御、数据库审计、日志审计、运维审计、漏洞扫描、态势感知、主机防病毒等云安全服务开通
	云防护服务策略配置优化	云平台	云平台	防火墙、入侵防御按照租户配置安全策略并优化
	业务侧账号管理分配	云平台	云平台	按业务系统分配数据库审计、日志审计、运维审计、漏洞扫描、态势感知、主机防病毒资源和账号
	安全设备巡检	云平台	业务系统	定期巡检,查看安全设备运行日志、分析设备运行状况,及时处理设备告警信息
	安全事件监测分析	云平台	业务系统	定期对态势感知、日志审计、数据库审计、防病毒等安全事件监测分析
	系统漏洞扫描	云平台	业务系统	定期对系统进行漏洞扫描,将漏洞扫描结果反馈给业务系统负责人
	提出安全加固建议	云平台	业务系统	协助业务部门安全加固,提出事件处置和漏洞修复建议
	云审计服务策略配置优化	云平台	业务系统	数据库审计、日志审计、运维审计、漏洞扫描、态势感知、主机防病毒等服务策略配置/优化
安全维护	保护资产管理	业务系统	业务系统	同步需加入防护的资产给云平台,接入系统信息等沟通确认
	漏洞修复	业务系统	业务系统	对业务系统漏洞扫描发现的漏洞进行修复
	风险处置	业务系统	业务系统	对安全监测发现的业务系统风险进行处置

两种管理模式,主要区别在于全托管模式云平台需要建立安全运营中心,以满足不同阶段的职责要求,包括组织架构,业务流程,人员团队和工具平台等方面的内容,而半托管模式云平台仅需为业务系统提供接入安全资源池管理平台的网络,以满足业务系统对所用安全组件的监管需求即可。

结语

本文以某市生产业务云平台为例,对城市轨道交通云平台安全资源池最优方案进行探讨,形成宜采用独立云安全资源池建设方案的结论。

独立云安全资源池方案采用云网安一体化的网络架构,可与既有云平台形成一体化解决方案,云、SDN、安全管理平台相互嵌套调用,带来深度融合的优势。云安全资源池支持软件和硬件混合部署,防护类安全能力采用硬件NFV形式提供,稳定可靠性能高;审计类安全能力采用安全软件形式提供,虚拟化层基于既有云平台虚拟化环境开发,安全性能更好,并且部署扩展灵活,带来软硬互补的优势。除此之外,安全资源池账户与既有云平台账户体系全局打通,可以做到操作界面的统一。从而实现了城轨云安全防护的自动化,从逐数数据流到定义数据流,解决了传统模式下自动不够,手动来凑的问题。

城轨云安全资源池的建设不仅补齐计算、网络、存储、安全四大服务板块,使得云平台云服务多样性、全面性大大提升。而且安全服务云化,通过提供标准云安全服务,灵活快速配给满足业务系统安全需求,助力提升业务系统安全可靠的快速开通。同时,云平台面向线网业务系统和正线业务系统提供统一的安全运营中心、统一管理安全态势,实现安全事件闭环管理。除此之外,业务系统按需申请云安全服务,云平台统一建设,集约高效,节约机房空间,符合绿色城轨的发展方向。

城轨云平台商用密码应用安全性评估及建设

文/李婧

近年来，轨道交通信息化系统的集成化、智能化程度越来越高，业务运行过程对信息系统的依赖性日益增强，随之而来的网络安全面临更大的挑战。信息系统一旦停滞，车辆调度、故障报警、安全运维等各个环节都无法正常进行。轨道交通系统一旦出现网络安全事故将直接影响人民的正常生活，造成的损失不可估量。

密码技术作为网络安全的基石和核心技术，关系到我国轨道交通领域信息安全底座的建设与保障。在网络安全作为国家安全战略的形势下，轨道交通密码技术信息安全保障更具有重要价值和意义。密码在我国发展已经很多年了，2012年国家首次推出自主创新的密码标准，祖冲之序列密码算法，直到今天我国密码标准仍然在不断拓展完善。新修订的《商用密码管理条例》于2023年7月1日正式施行，全面落实《中华人民共和国密码法》要求。条例为推进新时代商用密码高质量发展、保障网络与信息安全、维护国家安全和社会公共利益、保护公民合法权益提供了有力法治保障。

本文探讨了商用密码技术在城轨云平台的应用需求，针对业务与应用需求，分析了商用密码应用建设背景、城轨商用密码应用建设技术方案，旨在促进城轨商用密码应用的安全性建设，进一步加强城轨业务系统安全防护。

一、背景介绍

随着网络信息的迅猛发展，用户身份认证盗用、黑客攻击、数据意外泄露等信息安全事件频发，越来越多的企事业单位开始关注信息系统的安全问题，尤其是一些关系国计民生的重点单位。加密技术作为加强信息系统安全的重要手段被广泛使用。国产商用密码技术为我国自主创新的加密技术，已成为我国信息加密的首选技术。

密码是国家重要战略资源，是保障网络与信息安全的核心技术和基础支撑，是解决网络与信息安全问题最有效、最可靠、最经济的手段。密码工作是党和国家的一项特殊重要工作，直接关系到国家政治安全、经济安全、国防安全和信息安全。商用密码技术作为国家自主创新的核

心技术，在维护国家安全、促进经济发展、保护人民群众利益中发挥着不可替代的重要作用。

《中华人民共和国网络安全法》第三章第三十一条中明确提出：“国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域等关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护”。

《中华人民共和国密码法》第二十七条中明确提出“法律、行政法规和国家有关规定要求使用商用密码进行保护的关键信息基础设施，其运营者应当使用商用密码进行保护，自行或者委托商用密码检测机构开展商用密码应用安全性评估”。

为贯彻落实《中华人民共和国密码法》、新修订的《商用密码管理条例》等规定，2023年9月26日，国家密码管理局公布《商用密码应用安全性评估管理办法》，统筹细化商用密码应用安全性评估（以下简称密评）对象范围、责任主体、工作原则、程序内容、实施规范等规定，依法规范密评工作，自2023年11月1日起施行。重要网络与信息系统建成运行后，其运营者应当自行或者委托商用密码检测机构每年至少开展一次商用密码应用安全性评估，确保商用密码保障系统正确有效运行。

1. 密码的定义与分类

密码是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。《中华人民共和国密码法》规定密码分为核心密码、普通密码和商用密码。商用密码用于保护不属于国家秘密的信息，公民、法人和其他组织可以依法使用。

2. 商用密码应用安全性评估

对采用商用密码技术、产品和服务集成建设的网络和信息系统密码应用的合规性、正确性、有效性进行评估。

合规性：信息系统使用的密码技术、产品和服务是否符合国密要求。

正确性：受保护对象是否明确，密码功能是否实现准确，密码产品参数是否配置正确。

有效性：检验或验证密码应用是否合规、正确，是否真正实现了受保护对象的安全防护需求。

大数据、云计算、物联网、人工智能等新兴技术的大规模兴起，有力地推动了城轨信息化产业的迅速发展。城轨信息化的健康发展离不开高效可靠的网络安全保障，高效可靠的网络安全保障要求采用高性能、高安全、高可靠的密码产品为信息系统提供网络安全保障服务，同时还要保证密码产品的自主创新。

二、城轨云平台密码应用需求

目前云计算、大数据、5G、物联网等主流技术已广泛应用于智慧城轨的建设，在新技术的应用中，也随时面临着身份假冒、重要信息内容篡改、敏感信息泄露等安全风险。结合城轨网络安全的要求，依据《GB/T 39786-2021信息安全技术 信息系统密码应用基本要求》，城轨云平台商用密码应用在各地城轨云建设中同步规划同步建设，使之符合网络安全等保三级的标准技术防护要求及信息系统密码应用三级要求，消除或降低安全风险及隐患。

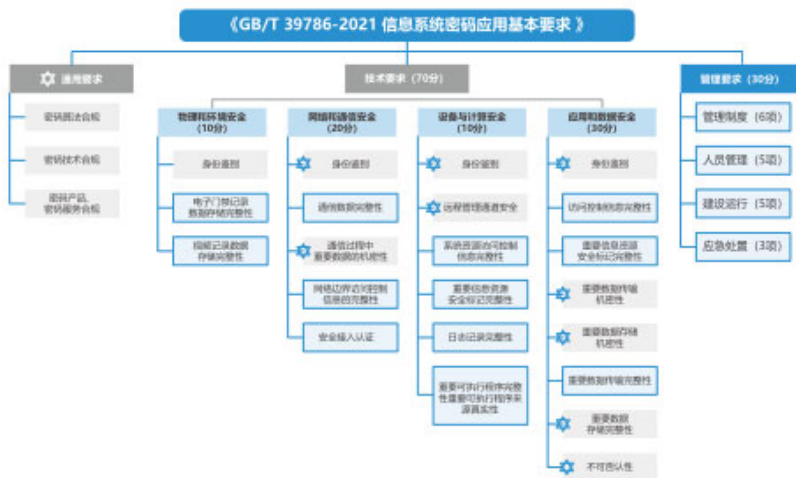


图1 信息系统密码应用基本要求

参照《GB/T 39786-2021信息安全技术 信息系统密码应用基本要求》中云平台三级系统指标要求，分别从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、安全管理等层面进行密码应用设计，为云平台安全稳定运行提供高效的密码支撑，满足云平台应用的安全需求。

三、密码应用技术方案

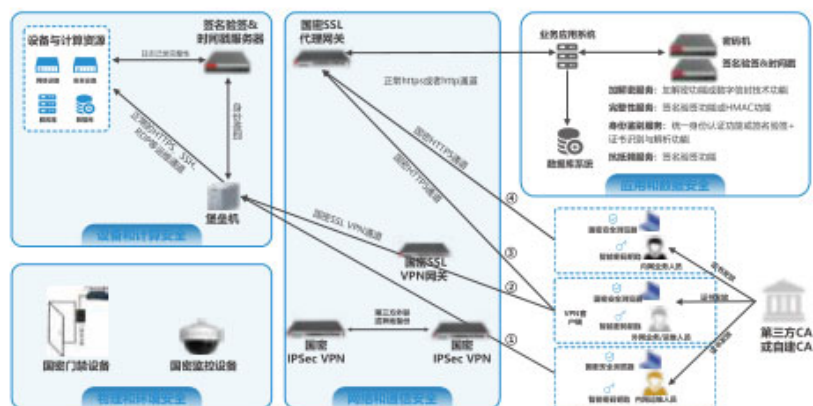


图2 密码应用安全合规流程图

1. 物理和环境安全

物理和环境安全方面主要考虑被测系统所在机房访问控制及记录数据的保护情况，涉及的测评对象主要为所在机房的电子门禁系统和视频监控系统。

城轨云平台所在机房部署需符合GMT 0036-2014《采用非接触卡的门禁系统密码应用技术指南》标准要求的电子门禁系统对进出机房人员进行身份鉴别，实现对电子门禁记录进行完整性保护；需要采用符合密码相关国家、行业标准要求的安全视频监控系统，对视频记录进行完整性保护，防止记录数据被非授权篡改导致数据不可信，提高记录数据的真实可靠性。

2. 网络和通信安全

网络和通信安全方面主要考虑在数据传输过程中的安全接入和控制，涉及的测评对象为信息系统与网络边界外建立的网络通信信道、访问业务应用系统的网络通信信道。

在运维管理网部署符合密码相关的国家和行业要求SSL VPN安全网关，平台管理员通过SSL VPN访问到平台内部实现对网络安全设备、服务器、数据库等远程管理，并基于密码技术实现平台管理员与SSL VPN服务端之间通信实体的身份真实性，防止与假冒实体进行通信；

并在通信过程中建立安全的传输通道，保护通信过程中重要数据的完整性和机密性，防止数据被非授权篡改，防止敏感数据泄露；部署符合密码相关的国家和行业标准要求SSL代理网关，实现云平台管理系统页面的SSL反向代理，远程访问云管理平台系统时采用HTTPS基于国产密码协议建立安全的传输通道，保护通信过程中重要数据的完整性和机密性，防止数据被非授权篡改，防止敏感数据泄露。

在不同系统间的边界接入区分别部署符合密码相关国家、行业标准要求的IPSec VPN，实现在通信前通信双方的身份鉴别，并建立安全的数据传输通道，保护通信过程中重要数据的完整性和机密性，防止数据被非授权篡改，防止敏感数据泄露。

基于密码技术保护云管理平台管理用户与平台之间的网络边界设备中的访问控制信息的完整性，防止被非授权篡改。

3. 设备和计算安全

设备和计算安全方面主要考虑设备的身份鉴别、远程管理通道安全及相关数据的安全防护，测评对象主要为通用服务器（如应用服务器、数据库服务器）、数据库管理系统、整机类和系统类的密码产品、堡垒机、各类虚拟设备等。

云平台运维人员的办公终端配发智能密码钥匙（含管理员合法可信身份证书），运维管理网部署签名验签与时间戳二合一服务器，并与堡垒机进行对接开发，实现堡垒机基于数字证书方式进行身份鉴别，防止假冒人员登录；基于密码技术保证各类运维人员在对平台设备进行运维管理时，使用安全的管理通道进行管理，保证管理数据在传输过程中的机密性和完整性，防止非法人员对平台设备和软件进行非授权的管理和操作。

通过部署符合密码相关的国家和行业标准要求签名验签与时间戳二合一服务器，基于密码技术保护服务器、数据库、网络安全设备等日志记录、系统资源访问控制信息的完整性，防止被非授权篡改；基于密码技术对需要安装的重要可执行程序的来源真实性和完整性进行验证，防止非可信程序的安装和部署。

4. 应用和数据安全

针对云管理平台的密码应用进行改造，向云管理平台管理员PC端配发智能密码钥匙（存

储符合国密要求的数字证书），服务端利用签名验签与时间戳二合一服务器，基于数字签名的方式对管理员进行身份鉴别，防止非授权人员登录。

在运维管理网部署符合密码相关国家、行业标准要求的签名验签与时间戳二合一服务器，对访问权限控制列表、配置文件等进行完整性保护，防止应用资源被非授权用户篡改。部署符合密码相关国家、行业标准要求的服务器密码机，在重要数据存储和读取的过程中进行加解密处理和完整性校验，保证数据存储的机密性和完整性，防止数据泄露给非授权的个人、进程，或被非授权的个人、进程进行非法篡改等。

5. 管理制度

密码应用正确有效的发挥作用依赖于密码技术和密码管理措施并举、双管齐下。基于GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》中关于密码管理安全方面的要求，建立各项与密码相关的管理制度，储备和任命密码相关管理人员，在平台建设和运行阶段，同步建设和落地执行密码应用相关制度要求，建立应急策略和安全事件上报流程，降低管理不到位的风险。

四、密码应用安全性评估

完成密码应用方案编制后，用户单位可以委托密评机构对方案进行评估，评估通过后，将系统密码应用改造方案向用户单位所属地密码管理部门备案，并同步对信息系统进行密码应用改造，选用通过检测认证合格的商用密码产品，合规、正确、有效的建设密码保障系统。

上线运行后，需要每年对系统进行一次密码应用安全性评估，并根据评估意见进行整改。当本系统在运行过程中发现重大密码应用安全隐患时，将停止系统运行，制定整改方案，按照整改方案对系统进行整改和密码应用安全性评估，评估通过后重新上线运行。

结语

随着国家合规标准的发布，给城轨行业用户提供了密码建设指导。从短期来看是以密码应用合规为主，来完善城轨自身的业务安全体系建设，长期来看，能够提升城轨行业整体安全体系架构的技术先进性，更好地应对未来可能存在的风险威胁。

目前城轨业务系统如信号系统、综合监控系统、自动售检票系统等的密钥均有采用国外密码算法，还未大范围应用国产商用密码标准算法，国密算法在城轨业务系统应用还需要进一步普及。针对目前的密评改造，城轨可根据业务属性及数据重要程度，对数据的传输、存储及人员操作行为进行分析，根据密码应用安全防护需求，明确以下密码应用改造方向。

明确重点，重点改造高风险点。针对身份鉴别、网络层通信数据机密性，设备层远程管理通道安全，应用和数据层的传输和存储机密性，通过数字签名技术防止人员关键操作行为的抵赖等这些高风险项目，进行重点改造。

聚焦难点，集中突破。针对业务系统定制化改造，调用密码机和签名验签服务器实现身份鉴别，实现传输及存储数据的机密性、完整性保护，重要信息的完整性保护；通过安全产品定制化改造，如日志审计、堡垒机定制化改造调用密码产品来实现日志记录完整性保护，身份鉴别，访问完整性保护。

力争得分点，稳住合规。针对物理和环境安全，部署合规的电子门禁系统、安全视频系统；针对通信和网络安全，部署国密SSL/IPSec VPN，保证通信传输机密性及完整性；建立密码安全管理体系并落地执行。这些不涉及对业务系统的改造，较为容易得分。

按照等级保护要求完成“一个中心，三重防护”安全防护体系建设的同时，为了进一步提升网络安全防护能力和水平，积极响应建设网络强国的号召，贯彻《密码法》关于密码应用的指导作用，落实国家密码管理局相关指示精神，促进密码网络及重要领域的应用，有效解决身份冒用、信息泄露、数据篡改、行为抵赖等安全问题。新华三提前全力布局密码产品，并借助自身产品研发及解决方案能力，完成了防火墙、国密代理网关、WAF、日志审计、运维审计、云管平台、大数据平台等与密码的全面融合。

新华三以自有商密产品为基础，充分整合密码应用需求，可以帮助城轨行业用户建立一套安全、合规、完整、有效的密码应用体系；底座云平台、网络资源、计算资源、存储资源已与密码产品完成对接，具备国密能力，提供多种密码安全服务，形成“云网安密”一体化的能力。

城轨数据中心液冷技术发展浅析

文/史钰果

当前，我国城市轨道交通仍处于快速发展阶段，截至2022年底，中国内地累计有55个城市投运城轨交通线路超过一万公里。积极引导低碳出行，加快城市轨道交通等大容量公共交通基础设施建设，成为了轨道交通的发展方向，其中绿色低碳是轨道交通发展的重大机遇。城市轨道交通系统非常复杂，各个生产业务系统综合应用了云计算、大数据、物联网、5G等多种信息技术以提高业务系统运行效率及稳定安全。

然而随着城轨线路的不断增多、各种信息化技术的不断运用，各地轨道交通总能耗不断上升，当前轨道交通总能耗94亿kWh，约占全国总耗电1.7%，未来预计年耗电量将达400亿度，占未来全国总耗电5%以上。根据对地铁的用电负荷统计分析，通风空调系统的能耗占总能耗的70%左右，这其中数据中心机房通风空调系统又占较大的比重，因此无论从绿色低碳的发展要求，还是从减轻城市运营成本的角度考量，地铁节能的必要性毋庸置疑，如何建成“低碳排、高效能、大运量”三个维度的绿色城轨，正成为行业发展的重中之重。当前城轨数据中心单位空间所产生的热量，伴随着芯片、服务器设备功耗的持续增长而不断提升，也使得单机柜功率密度越来越高，传统的风冷已无法满足数据中心散热的及时性要求，亟需探索液冷技术在城轨数据中心的落地应用。

一、液冷技术发展背景

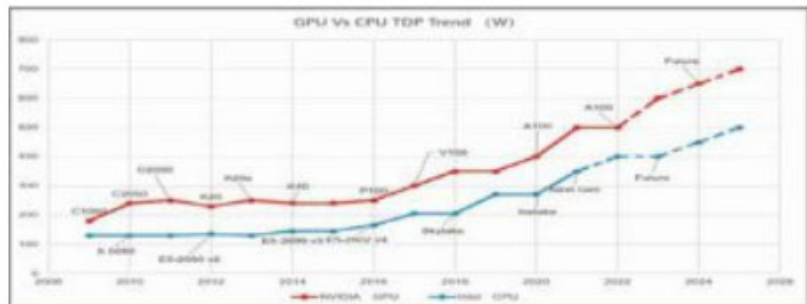
1. 政策背景

随着新基建、东数西算国家战略的持续赋能，新型数据中心建设迎来新机遇，成为我国数字经济高质量发展的关键基础设施。2020年9月习近平总书记在第75届联合国大会上提出了我国“二氧化碳排放力争于2030年前达到峰值，努力争取2060年前实现碳中和”的目标，在此背景下国家相继发布了《信息通信行业绿色低碳发展行动计划（2022-2025年）》、《工业能效提升行动计划》等系列文件，明确提出数据中心绿色可持续发展的行动计划，因此面向双碳，亟需顺应绿色节能、低碳可持续的发展趋势，探索新型绿色数据中心高质量发展路径，助力“3060”目标的实现。

中国城市轨道交通协会在2022年8月发布了《中国城市轨道交通绿色城轨发展行动方案》，方案提到以“绿色转型为主线，清洁能源为方向，节能降碳为重点，智慧赋能，创新驱动，开展六大绿色城轨行动，实现碳达峰碳中和，建设绿色城轨”为总体思路，在建设绿色城轨过程中实现碳达峰碳中和，在实现碳达峰碳中和过程中建设绿色城轨，统筹谋划设计“1-6-6-1-N”的绿色城轨发展的“一张蓝图”；重点实施“绿色规划先行行动、节能降碳增效行动、出行占比提升行动、绿色能源替代行动、绿色装备制造行动、全面绿色转型行动”的六大绿色城轨行动；制定实施“提高思想站位、创新体制机制、压实各方责任、引导试点示范、多策并举发力、建立标准评价体系”的六项保障措施；精心打造一批绿色城轨示范工程，引导企业编制实施“N个企业绿色城轨发展实施方案”，确保如期实现碳达峰碳中和目标，建成绿色城轨。

随着双碳战略的纵深推进，各地城市轨道交通近期密集发布系列绿色低碳政策，进一步明确了数据中心的能效要求，推动数据中心绿色、高质量、加速发展。

2. 技术趋势



随着AIGC等人工智能、大数据技术浪潮的来袭，服务器设备算力与功耗持续增长，数据中心单位空间所产生的热量也随之提升。如上图所示，服务器CPU的TDP（热设计功耗）已经接近500W，而GPU功耗更是达到700W，在提供强大算力的同时也对散热造成了极大困扰，散热能力不足则意味着设备一来无法达到正常的运行状态、发挥最佳性能，二来会对设备稳定性造成极大影响，此外为保证散热效果，往往会降低机柜内的设备部署密度，从而对机柜和机房的的空间造成极大浪费；换言之，一旦能有效解决目前高能耗设备的散热瓶颈，就能充分释放算力，提升机房效率。

液冷散热是利用液体介质的高换热系数、大比热容，通过液体对流、换热，将电子器件产生的热量带走，从而降低器件的温度，防止高温条件下的电子器件失效或快速老化，让电子设备发挥出最佳性能。与风冷相比，液冷的优势明显，冷却效率更高，同体积的传热介质，冷却剂传递热量的速度是空气的数倍，冷却液传热次数更少，容量衰减更小，可更有效降低CPU、GPU等关键组件的运行温度及性能损失，因此液冷技术凭借其支持高功耗芯片、实现高密度部署、节约电费、减少碳排放等优势，成为新型数据中心建设的重要选择。

3. 用户需求

当前各一二线城市轨道交通已完成城轨云平台的建设工作，其他城市也纷纷进行城轨云的建设，城轨云建设通常会采用设备集中的方式，以提高设备的利用率和生产效率，这对数据中心机房的散热能力提出了较高的要求；另外随着城轨智能化发展，越来越多的领域和业务场景都需要较高的计算和处理能力，城轨行业客户也在不断探索和应用GPU等异构计算技术，导致城轨数据中心整体能耗不断上升，越来越多的客户都在探索新的数据中心散热技术以发展绿色城轨建设。

二、液冷技术介绍

液冷是一种用液体来冷却电子设备的散热技术。液冷的工作原理是以液体作为冷媒，利用液体的高热容和高热传导性能，通过液体流动将IT设备的内部元器件产生的热量传递到设备外，使IT设备的发热器件得到冷却，以保证IT设备在安全温度范围内运行。根据冷却液与发热器件的接触方式不同，可以分为间接液冷和直接液冷。间接液冷是指服务器热源与冷却液之间没有直接接触的换热过程，以冷板式液冷技术为主。直接液冷是指将发热部件与冷却液直接接触的冷却方式，包括浸没式和喷淋式液冷技术。其中又可以根据冷却液是否会发生液态到气态的转变，将浸没式液冷分为单相浸没式液冷和双相浸没式液冷。当前，冷板式液冷和浸没式液冷为液冷的主要形式。

液冷系统通用架构包括室外侧和室内侧两部分：室外侧包含冷却塔、一次侧管网、一次侧冷却液；室内侧包含CDU、液冷机柜、ICT设备、二次侧管网和二次侧冷却液。室外侧为外部冷源，通常为室外的冷水机组、冷却塔或干冷器，热量转移主要通过水温的升降实现；室内侧包括供液环路和服务器内部流道，主要通过冷却液温度的升降实现热量转移；两个部分通过CDU中的板式换热器发生间壁式换热。

1. 冷板式液冷

冷板式液冷属于间接液冷，冷却液不与服务器芯片直接接触。冷板式液冷也被称作芯片级液冷，技术原理是通过在服务器组件（如CPU、GPU等高发热部件）上安装液冷板（通常为铜铝等导热金属构成的封闭腔体），服务器组件通过导热部件将热量传导到液冷板上，然后利用液冷板内部的液体循环将热量传递到远离服务器的散热单元；同时一般会增设风冷单元为低发热元件进行散热。

冷板式液冷系统主要由冷却塔、CDU、一次侧&二次侧液冷管路、冷却介质、液冷机柜组成；其中液冷机柜内包含液冷板、设备内液冷管路、流体连接器、分液器等。

2. 浸没式液冷

浸没式液冷属于直接液冷，将发热器件浸没在冷却液中进行热交换，依靠冷却液流动循环带走热量。

浸没式液冷系统室外侧包含冷却塔、一次侧管网、一次侧冷却液；室内侧包含CDU、浸没腔体、IT设备、二次侧管网和二次侧冷却液。使用过程中IT设备完全浸没在二次侧冷却液中，因此二次侧循环冷却液需要采用不导电液体，如矿物油、硅油、氟化液等。

浸没式液冷根据冷却液换热过程中是否发生相变，可以进一步分为单相浸没式液冷和双相浸没式液冷技术。

2.1 单相浸没式液冷

在单相浸没式液冷中，冷却液在热量传递过程中仅发生温度变化，而不存在相态转变。单相浸没式液冷的技术原理为：CDU循环泵驱动二次侧低温冷却液由浸没腔体底部进入，流经竖插在浸没腔体中的IT设备时带走发热器件热量；吸收热量升温后的二次侧冷却液由浸没腔体顶部出口流回CDU；通过CDU内部的板式换热器将吸收的热量传递给一次侧冷却液；吸热升温后的一次侧冷却液通过外部冷却装置（如冷却塔）将热量排放到大气环境中，完成整个冷却过程。

2.2 双相浸没式液冷

双相浸没式液冷的不同之处在于冷却液会发生相态转变。双相浸没式液冷的传热路径与

单相浸没液冷基本一致，主要差异在于二次侧冷却液仅在浸没腔体内部循环区域，浸没腔体内顶部为气态区、底部为液态区；IT设备完全浸没在低沸点的液态冷却液中，液态冷却液吸收设备热量后发生沸腾，汽化产生的高温气态冷却液因密度较小，会逐渐汇聚到浸没腔体顶部，与安装在顶部的冷凝器发生换热后冷凝为低温液态冷却液，随后在重力作用下回流至腔体底部，实现对IT设备的散热。

3. 喷淋式液冷

喷淋式液冷属于直接液冷，将冷却液精准喷洒于电子设备器件进行散热。冷却液借助特制的喷淋板精准喷洒至发热器件或与之相连接的固体导热材料上，并与其进行热交换，吸热后的冷却液换热后将通过回液管、回液箱等集液装置进行收集并通过循环泵输送至CDU进行下一次制冷循环。

喷淋式液冷系统主要由冷却塔、CDU、一次侧&二次侧液冷管路、冷却介质和喷淋式液冷机柜组成；其中喷淋式液冷机柜通常包含管路系统、布液系统、喷淋模块、回液系统等。

4. 不同液冷技术对比

	冷板式液冷	浸没式液冷		喷淋式液冷
		双相浸没式	单相浸没式	
原理	冷板贴近服务器芯片等高发热元件，利用冷板中冷却液带走热量；同时增设风冷单元带走低发热元件散热	服务器完全浸没在冷却液中，冷却液发生相变汽化并带走热量	服务器完全浸没在冷却液中，冷却液循环流动并带走热量	冷却液从服务器机箱顶部喷淋下来，通过对流换热为发热部件降温
节能性 (PUE)	1.2	1.04-1.07	1.09	1.1 左右
主要优势	兼容性：可兼容现有硬件架构，改造成本低，灵活适用于旧机房改造和新建机房 散热效果与节能性：冷却效果和节能性要远好于风冷 可靠性：液体与设备不直接接触，可靠性更高 维护性：系统易维护 噪声：风机转速大幅降低	散热效果与节能性：直接接触式的热交换，传热系数高，冷却效果与节能性更好 紧凑：支持高密机柜，同时，机柜间无需隔离距离，机房不需要架空地板、无需安装冷通道封闭设施等 可靠性：设备完全浸没在液体中，排除了温度灰尘等带来的可靠性问题 噪声：100%液体冷却，无需配置风扇	安装便捷，空间利用率高，设备静音，节省冷却液	

	冷板式液冷	浸没式液冷		喷淋式液冷
		双相浸没式	单向浸没式	
局限性	液体没有与电子器件直接接触，而是通过金属管壁进行热交换，与直接接触的浸没式液冷相比冷却与节能效果欠佳 IT设备、冷却液、管路、供配电等不统一，服务器多与机相深耦合 管路接头、密封件较多，漏液维护复杂	兼容性差：IT设备需要定制，光模块、硬盘等部件兼容性仍待验证 维护复杂：浸没式液冷设备维护时需要打开Tank上盖，并配备可移动机械吊臂或专业维护车实现设备的竖直插，维护复杂度高 承重要求高：因浸没式液冷系统Tank内充满冷却液，整机重量大幅增加，对机房有特殊承重要求 国产冷媒待验证：单相浸没式液冷方案所使用的国产冷媒仍待验证	节能效果差于浸没式液冷，且存在与浸没式液冷相同的局限性 问题	
应用范围	目前应用最为广泛	适用于对功率密度、节能性要求较高的大型数据中心，现阶段落地应用相对较少		不适合高密度服务器和超大规模数据中心，现阶段落地应用相对较少

通过冷板式液冷、浸没式液冷和喷淋式液冷三种技术的对比分析可以看到，目前冷板式液冷技术无论是从兼容性、可靠性、维护性以及落地成熟度来讲都是最适合城轨数据中心的，因此建议城轨数据中心优先采用冷板式液冷技术，并保持对浸没式液冷和喷淋式液冷技术的不断跟进，待技术成熟时再考虑这两种路线。

三、新华三液冷解决方案

为了进一步降低数据中心PUE，提升算力效能，新华三集团推出了数据中心全栈液冷解决方案，从节流入手，提升数据中心运用效率，降低PUE，其中的关键之一就是降低冷却ICT设备的高能耗，推动液冷技术在数据中心的应用和部署。

作为数字化解决方案领导者，新华三集团在液冷机房的设计上参与了多项行业标准规范编写，在板式液冷、浸没式液冷等方面进行了持续的投入和研发，推出涵盖多元异构算力服务器、交换机、核心路由器、液冷基础设施、运维管理的全栈式液冷解决方案，适用于云计算、HPC、智算中心、传统数据中心改造等多种高功率密度数据中心的场景。

1. 新华三数据中心全生命周期服务能力

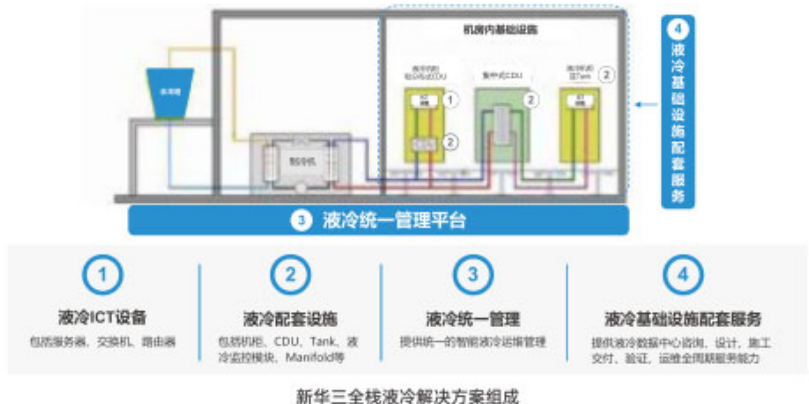
新华三数据中心业务，在数据中心行业内享有盛誉，是国内最顶尖的数据中心专业服务厂商。

商。服务涵盖数据中心咨询、设计、实施、验证、运维全生命周期，同时也提供项目管理、数字化转型BIM服务、ECC及数字展厅服务以及微模块数据中心解决方案等。过去的10年，新华三服务了近400个数据中心，建筑总面积超过300万平方米，也是业界唯一同时为BAT互联网巨头提供设计、管理及测试验证服务的厂商，也为四大国有银行、上交所、中债登、深交所等众多金融业主提供了专业的服务，其中就包括业内颇具样板效应的液冷数据中心。



2. 新华三全栈式液冷基础设施解决方案能力

针对数据中心液冷方案组成的ICT设备、散热设施、液冷统一管理和配套服务，提供完整的方案覆盖和交付能力



新华三全栈液冷解决方案包含完整的液冷数据中心设施及服务：

- ◆ 由液冷服务器、交换机、路由器等产品所组成的液冷ICT基础设施。
- ◆ 由液冷机柜或浸没式TANK、集中式或分布式CDU冷量分配单元、机柜监控模块、Manifold分集水器及快接头所组成的液冷配套设施；并同时支持冷板式、浸没式多制冷技术路线。
- ◆ 基于设备、机柜、机房级别的统一运维管理。
- ◆ 提供数据中心咨询、设计、施工交付、验证、运维全周期服务。

结语

据估算到2025年，中国数据中心液冷市场规模将达到359亿元左右，AI数据中心液冷市场规模将达到280亿元左右。城轨数据中心液冷虽然还处于起步阶段，但随着生成式人工智能横空出世，助推AI算力到达一个新的景气度。受ChatGPT为代表的生成式人工智能大模型等新业态带动，全新的AI应用场景有望在未来3-5年爆发，城市轨道交通也势必会受到影响，积极探索液冷技术在数据中心的落地将是每个大中型城市必须要关注的课题，新华三也将持续深耕全栈液冷解决方案，助力城轨客户数据中心全生命周期绿色降碳。



四大集约化助力绿智城轨发展

文/张一琛

随着《智慧城轨发展纲要》和《绿色城轨发展行动方案》的相继发布，智慧城轨建设为绿色城轨提供强大创新动力，绿色城轨建设为智慧城轨提供更大发展空间。城轨绿色和智慧是一体之两翼、驱动之双轮，必须统一谋划、统一部署、统一推进、统一实施。

中国的城市轨道交通无论是从建设速度还是整体规模的发展都是处于世界前列的水平，新华三始终坚持行驶在智慧城轨的主干道上。城轨行业的发展从过去的自动化，到现在的数字化，以及即将完全迈进的智慧化和绿色化，都在昭示着“绿智融合”之下的城轨建设有着极大的发挥空间。

经过近些年的建设和思考，我们发现：智慧城轨的发展开始向着“四大集约化”逐步迈进。

这四大集约化涵盖了：基于技术架构搭建的云化IT平台，基于数据架构搭建的数字化运营平台，基于业务架构搭建的能力数字化平台和基于组织架构组建的轻量应用队伍，最后以上内容全部服务于上层的业务运营和后台运维。

一、业务集约化

每次谈到智慧城轨，大家都会联想到城轨数字化转型，转型的核心是“重构”。城轨行业中重构的原因是什么？是业务系统的打通，是协同联动。那打通和协同联动的原因是什么？是城轨场景化的建设需求。因此可以得到一个严密的逻辑结论：数字化转型的前提是重构，重构的前提是业务系统打通，打通的前提是场景化的建设需求，而现在智慧城轨的落脚点必然聚焦到一个又一个待挖掘的智慧场景中。

面向场景化的建设，最先要解决的就是要打通城轨业务系统之间的烟囱壁垒。目前有两类方式：一是城轨业务系统的厂家，如ISCS系统开发商倾向采用ESB服务总线来打通各个业务系统之间的通信路由。另一种就是做基础云平台的厂家，如新华三则选择了“多业务微服务共享平台”的路线。

第一种方式本质上是SOA架构，由于场景化的全局业务通信压力都集中在服务总线，一旦总线故障那么全盘停机。而且场景化的各业务和数据分隔在不同的烟囱中，对于城轨业务的持续发展和沉淀没有任何帮助。第二种方式本质是采用微服务架构来搭建业务系统、数据可共享的平台，实现多业务互联互通，沉淀业务服务模块，推动快速开发更新迭代，避免重复造轮子，最终实现跨场景跨业务的开放共享。基于上述原因，SOA架构也已逐步被微服务架构取代。

这里将新华三在全国落地的几个采用业务微服务架构的城市案例罗列出来：北京AFC改造、太原ITP-ACC重构、南京能效管理系统和深圳能源管理系统的微服务部署。当前以上各城市仅仅向着“微服务资源沉淀，多业务系统联动共享”迈出了第一步。如果我们将各个城市名称隐藏掉，当成是一个城市的建设成果，就会发现一旦微服务化业务形成规模，必然就会出现“共享业务服务，共享数据服务”的特性。业务集约化的建设过程，就好像背后有一只隐形的推动着我们站在前人的肩膀上，复用既有业务服务资源，做厚共享平台，创新场景应用，实现快速的新业务新方案的创新。

二、数据集约化

城轨行业的数据集约化讲究“全连接”，从过去的数据仓库到现在的数据湖称呼，就能体现一二。业务层面要连接IoT各种业务系统的前端设备和物理模型，运维层面要连接各种ICT基础设施的指标度量。只要是地铁用户的资产，全都尝试用数字化呈现在数字大屏和数字空间。

当海量的城轨大数据源源不断涌来时，应对的最佳方案是“宜疏不宜堵”。数据集约化的最终目标不是封闭，而是开放，予取予求般地开放，开放是数据流通的最佳路径。正如新华三基于既有项目经验，打造出来的城轨行业通用套件，零编码一站式API开放平台，能够使得数据的提取、推送就像吃饭喝水一样简单。用户可以通过该平台完成数据的采集、存储、分析、应用等全流程管理，极大地降低了数据开发成本。

随着城轨大数据平台的不断融汇贯通，可以预见数据集约化的成果会是一个“养成系”产物。大量地铁行车数据、时刻数据、客流数据、巡检数据等，就是养料，训练规则则是特定智慧场景的算法模型。无规矩不成方圆，如果没有算法模型点石成金的辅助，就不能将数据价值真正变现为业务价值，就更谈不上用数据指导决策了。当下全球掀起了AIGC技术大潮，恰逢其时地成为带动智慧城轨跨越“算法沟壑”的大杀器。新华三坚持相信，未来“大模型”

竞争的制高点一定在“私域”数据，城轨大模型的制高点一定在场景创新和场景服务。为此，新华三将为垂直行业和专属地域的客户，提供端到端的全栈ICT能力，提供安全、订制、独享、生长的智能化服务，将充分发掘城轨大数据平台潜在的业务价值。

当城轨数据的价值要在双碳战略背景下展现出来时，新华三认为城轨要实现降碳节能目标有四个发力点：源、探、管、服。源，即绿色能源的采用，绿电消纳，自发自用；探，即观碳，算碳，摸清城轨行业碳排放的家底，碳足迹，对轨道交通进行碳排放核算，实现双碳数字化。管，即能源管理和优化，依托城轨行业的历史大数据来建设综合能耗管理系统，一体化节能减排。服，即碳服务，为用户提供碳数据的处理和咨询服务，落实双碳路径规划，为碳服务碳交易提供碳排放数据资产服务。通过对城轨行业的能源消耗、碳排放、生产、减排、配额等海量数据的汇聚管理和分析，赋能碳排放核算、碳资产盘点、碳配额预估，推动减排潜力挖掘，降低履约成本，制定交易方案，打通碳资产管理和交易中心，为碳中和的达成提供强大服务支撑。

三、平台集约化

随着城轨云建设的推进，各城市云平台建设格局已基本形成。在后续的城轨云基础设施建设中，逐步放缓，用户关注点也从建设转向运营和运维。未来，城轨用户将更加关注如何形成具有行业特色的统一云管理、服务和运维门户。综合运营平台是平台集约化的集大成者，妥妥的城轨云服务的百宝箱。如果说2017年是城轨云IaaS的起步点，那么2023年的综合运营平台的大规模推广就表明开始进入到IaaS的收尾阶段。综合运营平台具有统一云门户、统一云服务、统一云运营、统一云认证，统一云运维的五大功能，横向拉通云、数、网、安、运维等工作，兼容异构资源池，纳管各城市建设的主中心、备中心、站段云节点、大数据平台、测试平台。综合运营平台还能将物理机房环境信息纳入管理范围，实现对城轨数据中心的全量监管，为绿色数据中心建设打下坚实基础。

2022年2月，随着“东数西算”工程全面启动，该工程被业界认为是一项开启算力经济时代的世纪工程，这意味着持续优化数据中心能源使用效率、提高算力基础设施的有效利用率，让用户以更低的价格获得更大的算力，成为未来的数据中心的的方向。《绿色城轨发展行动方案》中也强调提出要推进城轨数据中心集约化、高密化，促进新建数据中心全部达到绿色数据中心要求。

为了降低城轨数据中心的PUE值，使之能够满足《新型数据中心发展三年行动计划》要求：“2023年底新建大型及以上数据中心PUE降低到1.3以下，严寒和寒冷地区力争降低到1.25以下”，最佳的方式就是液冷数据中心——给机房设备洗个冷水澡。如果以IT负载6000kw数据中心为例，沉浸式液冷方案比风冷方案的PUE值降低约0.62，全年碳排放减少4005吨，年运营电费节省2073万元。

微模块化机房则进一步扩展机房“乐高积木式”模块化的思想，比如配电模块化、制冷模块化、全预制数据中心模块化等，可以实现快速部署、弹性扩容、运维简单，极大缩短设备从进场、安装、调试到最终运行交付时间周期。同时配合液冷服务器、液冷交换机等液冷全套方案，能够实现更高的能效水平，和更低的PUE值。

为了给服务器降温，传统数据中心仍采用老实本分的堆料模式，但是大量精密空调机组的使用导致高耗能，高PUE，不符合当前社会“双碳”数据中心建设要求。因此，城轨数据中心的打造要从“人工硬冷”进化到“AI智冷”。“AI智冷”数据中心采用预制化、模块化建设，将AI技术应用于数据中心，通过大数据建立神经网络模型，深度自适应逻辑控制，建立能耗与IT负载、气候条件、设备运行数量等机器学习模型，准确推理和配置出数据中心最优控制逻辑，实时调节参数，让数据中心的PUE再降一个台阶。

四、组织集约化

当业务、数据、平台集约化之后，匹配的必然是组织集约化。为了将业务与IT深度融合，将云平台与上层业务深度整合，城轨用户必然需要一个多兵种多功能的团队才能掌控全局，这样的团队应该包括业务人员、IT人员、数据人员、产品人员等角色。

经常有城轨用户问到：云平台建设后，云平台的运维技术人员是统一安排在一个部门合适，还是分别部署在各个业务部门合适？当地铁场景化建设的需求不断铺展开来，云、数、微服务、物联等平台与业务系统再难解分时，全能型的组织就要求既懂业务又懂技术，只有这样才能盘活完整的“城轨云业务”系统，才能真正推动智慧城轨的快速迭代发展。

城轨行业的四大集约化建设路径将会长期伴随着“绿智融合”的推进和开展，从技术架构、数据架构、业务架构以及管理架构上全面深入改造升级，让智慧城轨找到合适的场景，找到合适的技术平台，从而走出真正的数字化转型之路。

02

云协路网，智行未来

第16章 智慧高速如何“智慧”？	107
第17章 基于SRv6的高速公路“自动驾驶”网络	113
第18章 IP-RAN2.0在高速公路路段接入网的应用探讨	118
第19章 新华三IP-RAN2.0让武汉绕城高速通信网“随需而变”	123
第20章 依托站级云化智能底座推进收费站标准化	128
第21章 高速公路收费系统安全能力提升的思考	133
第22章 关于高速行业如何用好AIGC的思考	137
第23章 零碳智慧服务区建设方案	145
第24章 对公路基础设施全生命周期管理的思考	149
第25章 数字化路网事件管理系统建设思路	154

智慧高速如何“智慧”？

文/王泽宁

一、智慧高速概述

高速公路本身是一个民生工程，体量非常大，高速公路建设面临诸多痛点，通行效率、收费效率及准确率、路网安全等都是建设高速公路所必须关注的问题。普通高速公路领域的在用系统大概有几十个业务系统。如果总试图升级这些系统去变革面向管理者的建、养、管、运、服的全业务链，就还谈不上智慧高速，只能算是高速信息化。

我们对于智慧高速的内涵理解如下：首先，智慧高速的核心本质是在“智慧”一词上，应该具备像人一样感知、思考、理解、分析、执行、反馈的能力；其次，智慧高速的核心任务是保障人、车、路、环境、信息等多个要素之间高度协同运行，使得智慧高速系统整体运行效益最高；再次，智慧高速的核心目标是提质增效，也就是让高速公路更加安全、高效、便捷、绿色；最后，智慧高速庞杂的硬件设备和软件平台，应当有一套完善的运维管理系统作为支撑，保障核心系统的不间断运行。

二、智慧高速发展历程

一般认为智慧高速将经历三个发展阶段：

智慧高速1.0（信息化）：本阶段以高速公路传统应用和基础设施的数字化改造为主，逐渐用信息系统代替人工操作，减少人为失误。丰富路网感知手段，智能获取路网及路面状态，形成多维路网监测体系，同时服务于应急指挥及信息服务，提升服务体验。在顶层设计方面，初步形成智慧高速建设共识，逐步明确行动计划。

智慧高速2.0（智能化）：本阶段致力于为高速公路的相关方提供差异化、智能化服务。通过多维感知体系，结合AI智能分析，精准掌控路网状态，实时、高效应急处置；结合ETC（或北斗）等技术手段，实现快速精准收费；优化服务区产业，打造服务区+旅游、服务区+枢纽等主题服务区，提供精准个性化的定制化服务；初步探索自动驾驶、车路协同等前沿方向，在建设模式、运营模式方面形成经验积累。

智慧高速3.0（自动化）：本阶段将基本形成智慧化、无人化的营运体系。自动驾驶实现全天候、全路段普及，大幅提升交通运输效率，实现“四零”目标，即：零拥堵、零死亡、零管制、零排放。

有别于智能制造的发展历程（信息化-自动化-智能化），智慧高速的发展历程有着高速公路行业独有的特点。2019年的“撤站”，深化了高速公路收费联网体系，重构了高速公路的收费逻辑，夯实了全网自由流收费的基础，配合收费稽查、在线计费系统等系统，基本实现了精准计费；2020年的全国高速公路视频云联网，构建了一套庞大的在线视频共享体系，通过AI在线分析，及时发现路网运行事件，为应急指挥、运营管控提供了强有力的数据支撑；自2017年以来，在北京、江苏、浙江、上海等地开展了大规模的车联网示范区和先导区的建设，自动驾驶的产业结构基本形成，商业运营模式也开始进入探索阶段，为自动驾驶的推广创造了基本的发展条件。

因此，我国目前正处在智慧高速发展2.0-3.0的阶段。但信息化、智能化、自动化三个阶段并不完全是依次演进的过程，而是呈现出融合发展、协同发展的态势。信息化是智能化、自动化的支撑，不同程度的信息化水平，支撑不同程度的智能化和自动化。

三、智慧高速建设模式

高速公路ITS系统的发展经历了很多年，近些年也涌现出了很多智慧高速的项目建设，然而到目前为止，对于“智慧高速”的专业名词解释，基本很难去定义。务实的讲，受限于一性投入的投资规模、项目建设时业界的技术水平等原因，并没有出现管理体制、运营模式等方面革命性的变化。通过调研现有的智慧高速试点项目，我们发现大部分项目是选取了某一个或某几个方向进行深入的探索，如精准养护、基础设施数字化等等。

然而，智慧高速的建设存在着非常明显的木桶效应，这与高速公路本身的服务属性有关，服务是全方位的。比如养护系统很先进，能够长期保证一个良好的路面运行情况，但是服务区的服务体验不良，应急处置不太及时，对于高速公路的使用者来说，仍旧不是一条“智慧高速”。因此，“智慧高速”不能仅仅作为一个项目去建设，而应是一整套的建设体系和顶层规划。

近年来智慧高速的发展呈现出由“全面智慧”向“经济实用”转变的趋势。行业认识到智慧类建设应当适度超前，由大而全的智慧公路向能够解决实际问题的小智慧场景转变。

反应在建设及改造需求上，则有以下几个主要的转变：

第一，传统系统升级的需求迫切。拿收费系统举例，从2020年5月后联网收费稳定运行，路网运行更通畅、人民出行更便捷、为促进物流降本增效、服务构建新发展格局奠定了坚实基础。然而对标全国高速公路“一张网运行、一体化服务”新形势的要求，现有收费系统在计费准确性、业务规范化程度、系统标准化程度等方面，还有很大的提升空间。放在监控系统里也是一样，距离“可控、可服务”的目标，还有一段路要走。

第二，更加追求发挥现有数据的价值，而不是新建大量的感知手段。全国目前2.7万个门架、20余万路视频感知终端，还有很多物联网传感器，高速公路的数据保有量至少是以10PB为单位计量的，这些数据如何进行标准化、如何保障数据共享及数据安全，是当前需要解决的迫切问题之一。

第三，服务方式从“有服务”向“好服务”转变。“好服务”的含义分为两个层面，一是向出行者提供更好的服务，如强化服务区的服务能力，通过普及率已经超过70%的ETC技术向车主提供更多的信息服务等；二是向路段公司提供更好的服务，充分发挥数据的主观能动性，为路段公司在路网运营、应急指挥等方面提供更好的决策支撑。

第四，适度的智慧，由大而全的智慧公路向能够解决实际问题的小智慧场景转变，更加关注新技术与旧场景的结合，解决生产过程中的实际问题。

四、智慧高速整体建设思路

为更好的应对未来发展形势，我们提出统筹规划、因地制宜、适度超前、经济实用的发展建设思路。

统筹规划：统筹布局做好建设方向、空间布局、建设时序规划，近期应关注成熟技术的规模化、网络化应用，远期应跟踪前沿科技布置试点研究，并做好对接和预留。

因地制宜：结合特定区域、特定阶段、特定需求来开展高速公路智慧化建设。要针对不同高速公路的痛点问题给出有针对性的解决方案，实现“一路一策”，甚至“一路多策”。

适度超前：智慧高速建设应基于现状，适度超前布局，在技术、数据架构上适度超前布局，为未来做好技术预留。

经济实用：优先考虑解决实际问题和发展需要，着眼于效益提升，优先建设标准化收费站、车道级管控、在线计费、自动化运维、智能化养护、主动安全防护等能带来核心价值的业务应用，再考虑其他扩展场景的智慧化建设。

基于此思路，构建智慧高速的整体架构，分为以下几个层级：



泛物联网感知层：物联网感知是智慧高速系统的神经末梢，如“撤站”新建的ETC门架（RSU、视频感知终端等）、视频云联网新建或改造的监控终端等，服务区也是高速感知系统中的重要数据源之一。此外，对于桥梁、隧道，甚至是易损坏、车流量大的普通路段，可能部署有压力传感器、形变传感器等。随着北斗3号组网成功，促进卫星定位、导航、授时服务功能的应用，技术创新，配合差分定位，在一些高精度位移测量的场景，如边坡监测、桥梁监测方面也已有小规模应用。物联网感知获取数据的准确性、全面性，将直接影响智慧高速系统可用性、实用性。

数字基础设施层：分为两个板块，ICT基础设施和智慧传输。ICT基础设施即计算、存储等硬件承载平台，它是所有信息系统的基础。智慧传输即有线传输+以5G为代表的无线通信技术，新华三率先在高速行业提出IPRAN2.0技术路线，借助设备层实现电层和光层的融合，在控制层、转发层、光层实现突破，通过“IPv6+光”的扁平化架构大幅简化网络，提升多层网络控制、算路、维护的统一，进一步提升通信网络的服务能力。

数据中台层：分为三部分，智慧高速云、智慧高速数字孪生、业务能力平台。

◆智慧高速云是数据中台的底层支撑，但过分强调云平台本身的技术路线、私有公有其实毫无意义，应当关注云带来的技术便利：如云平台能够兼容异构IT设备，考虑到高速公路分段建设的模式，异构兼容能够大大提升设备折旧率，有效保护投资；如GPU资源池化，视频云联网之后，大量的视频数据需要通过AI分析才能发挥其最大价值。

◆智慧高速数字孪生平台由静态孪生和动态孪生组成。静态孪生是指通过搭建高速公路核心业务数据中台，融合原来的资产管理相关的业务管理系统前台与其数据后台，形成全生命周期的全资产管理体系、标准与管理信息平台，建立公路资产“0”号台账，提供资产保值、增值的大数据支持，为企业的管理提供决策支持；动态孪生是指对公路建设、运营的过程进行建模仿真，从而提供除静态孪生（BIM等）外的动态信息（结构安全、路面状况、运行状况等）。利用全生命周期管理，基于BIM+GIS全生命周期管控系统，采用云计算、人工智能物联网（AIoT）、结构健康预测、数字认证等技术实现基础设施动态管理网络化。

◆业务能力平台为上层应用提供必要的数据库、中间件、算法引擎等Paas服务。

智慧应用层：在建、管、养、运、服、新六个方面展开。建设板块主要围绕项目建设流程、进度、归档、资产移交等方面，强调的是工程全流程监控及呈现；管理板块以路网运行监测、入口治超为主；养护板块包含养护流程监管、基础设施健康监测、可预测养护等；运营板块主要聚焦服务区运营，服务区作为除高速通行费第二大收入来源，是运营板块的重要组成部分；服务板块主要是指公众服务系统、紧急报障系统等；新业态板块以车路协同为主进行探索。主动安全体系，保证业务系统安全合规，统一运维体系，采用自动化运维手段，降低运维工作对人员、财力的开销。

◆智慧+建设：围绕建设工程项目管理的核心业务，融合项目管理各应用系统模块采集和生产的数据进行数据挖掘分析，实现多层次、多维度的项目数据可视化展现，让项目管理者、施工方能够及时掌握项目动态，为管理决策提供科学支持。

◆智慧+管理：以路网数字化、交通全要素感知为基础，实现路网事件全生命周期管理，通过AI视觉，实现交通事件的自动发现，在应急处置过程中，涉及到数据的跨部门共享，将由数据中台作为底层支撑；此外，构建一套统一的高速公路统一运维平台，实现巡检自动化、配置合规自动化、维护操作自动化、安装部署自动化、配置手机自动化等能力，提供移动APP端，与运维工单系统联动，实现移动巡检，加强高速公路机电系统管理水平。

◆智慧+养护：在线监测与维修一体化：在线监测，健康状态评估，建立在线监测与维修桥梁关系，实现在线监测与维修一体化。故障诊断与维修方法一体化：构建故障诊断模型，基于日志分析系统，生成维修对策，建立故障与维修方法的关系，实现故障诊断与维修方法一体化；运维评估一体化，运维工作成果由运营监测指标体系的回升作为评判依据。

◆智慧+运营：智慧服务区、智慧商业管理系统：采用分级管理模式，服务区内商超拥有自主经营权，同时向集团上报每日经营情况，集团可以根据全省及该区域的商品销售趋势，指导各服务区优化商品销售策略，达到增值创收的效果。同时可以结合ETC支付的方式，实现无现金支付，做到人、车、物三合一。智慧能耗管理系统：构建源-探-管-服的零碳服务区体系架构，通过智能水表、智能电表等终端，实时监控服务区能耗情况，做到无人低耗、无车低耗；部署智能照明系统，做到无人弱光、无车弱光，大大降低服务区的能耗开销。

◆智慧+服务：基于云统一服务门户，整合路网监测系统、应急指挥系统、交通事件查询系统等，提供准确、实时的交通信息查询服务。

◆智慧+新场景：私域大模型，探索AIGC与行业场景的融合，在智能客服、绿通查验、应急指挥等场景，充分发挥NLP、CV、跨模态大模型的能力，助力传统业务数字化变革。车路协同采用先进云边协同架构，保障算力基础设施的高可靠性，探索V2X通信全流程的安全防护体系。

结语

因此，建设统一平台、应用新技术、融合全数据成为智慧高速建设的关键。在这样的理解下，新华三为高速公路行业量身定制了智慧高速解决方案，助力用户构建“高速公路数字大脑”，通过建设一张实现业务灵活调度的融合承载网络、一套具备全栈能力的云与智能平台、一套集成资产管理的主动安全防护体系、一个深入业务应用的统一运维平台，构筑智慧高速建设的基石，同时广泛与合作伙伴深度融合创新，共享资源，共建智慧高速。

基于SRv6的高速公路“自动驾驶”网络

文/李洋龙

自动驾驶已成为行业近十年来热议话题，在自动驾驶技术实现路径上，国家大力支持车路协同方案，指出车路协同是未来智慧高速的重要发展方向。目前多地都建设了智能网联先行先试示范区，推动车端、路端、云端应用布局不断得到完善，产业链也愈加成熟。随着测试场景从封闭走向开放、从单一走向多元化，车路云之间的智能信息交换共享对高速公路通信网络也提出了新的需求。第一，能够为海量的智能终端提供足够多的IP地址，随时随地发起连接；第二，能够为不同场景业务灵活提供差异化的网络质量保障；第三，车路协同系统中，车端设备关注的是数据是否可信、可靠，信息量是否充足，必须统筹考虑终端安全、通信安全；第四，需要一种智能的网络管控机制，实现基于业务意图的算网融合，使数据在网络中实现“自动驾驶”，赋能车路协同到端边云协同的发展。

一、传统网络不足以支撑车路协同全面建设

在现有车路协同项目中，通信网络通常采用以太网建设方案，在这种传统网络的建设思维中，经常通过考量带宽、延迟、丢包率三个指标，来不断的对网络升级改造。而车路协同的需求指出，连接和计算才是整个系统的基石，传统网络不具弹性的结构，“尽力而为”的服务模型已无法再满足未来车路协同逐步走向规模化与市场化过程中对网络海量的、随时随地可能发起的数据连接的要求，而且其使用的IPv4协议在寻址方式、对应用的保障能力及数据安全上也存在着缺陷。

1. 寻址方式

首先IPv4的私有地址空间很难满足车路协同大规模建设对网络地址的庞大需求，同时，IPv4在设计之初并没有充分考虑到节点移动性带来的路由问题，可能导致车路协同场景下车辆等节点移动时上层应用无法与移动后的车辆通信，而MIPv4（移动IPv4）虽然可以解决这一问题，但其实现机制只支持少量节点移动，当大量车端在不同网络间切换时会导致网络资源迅速被耗尽，影响整网通信。

2. 质量保证

网络的质量直接影响服务质量，是任何应用技术发展过程中必须解决的问题。目前网络中通过QoS来实现质量保证，例如可使用资源预留协议或是采用差分服务技术。这些技术从一定程度上解决了敏感业务对丢包、时延、抖动的需求，但这些方法往往是基于网络侧指标的考量，并没有从应用侧的实际需求出发，而车路协同场景中的服务质量往往需要感知侧和上层应用紧密结合。

3. 安全性

在车路协同建设中，制造成本决定了很多终端感知设备都是基于简单的硬件，不具备处理复杂应用层加密算法的能力。因此，靠传统的应用层加密技术很难满足终端侧数据在网络传输过程中的数据加密需求，数据存在被篡改、替换、重放的风险，成为影响交通安全的潜在因素。

二、基于IPv6的解决方案

IPv6是v6版本的IP协议，拥有128比特的网络地址空间，这个空间约有340万亿亿亿亿个，可以满足未来全国超大规模的车路协同建设所需的海量IP地址，让更多的车辆和设备能够互相通信，同时，它解决了上述传统IPv4网络中的一系列问题。

1. IPv6对移动性的支持

IPv6在设计时充分考虑了对终端节点移动性的支持，解决了MIPv4（移动IPv4）模式下网络的三角路由问题。首先，IPv4为了支持移动性所做的路由优化，在移动IPv6中是个内建的协议基础部分。其次，IPv6邻居发现使用的是ND（Neighbor Discovery，邻居发现），而不是移动IPv4使用的ARP（地址解析协议），由于不需要考虑ARP中的数据链路层，因此它增强了协议的健壮性并且简化了基于移动IP的应用。另外移动IPv6采用的动态宿主代理发现机制，使其更加高效和可靠。因此如果想真正实现终端对移动性的支持，IPv6是必然的选择。

2. IPv6的服务质量

与IPv4相同的是，在IPv6的数据包结构中有8比特字段用来对报文的业务类别进行标识，

另外IPv6有20比特的流标签字段用来对属于同一业务流的包做标识。这样对于具有相同流标签的同一数据流，网络就可以进行做快速相同的处理。IPv6可以只在必要的时候才对数据包携带标签，即只有节点在发送重要数据时，动态的提高应用服务质量，从而做到对服务质量的精细化控制。

3. IPv6的安全性

IPv6将IPSec协议嵌入到了协议栈中，路侧和云端的通信可以启用IPSec加密数据信息，这样即使外部攻击者通过中间人方式对通进程进行了劫持获取了数据包，也无法进行解码获取通信节点内容。同时，IPv6地址的分段设计将用户信息与网络信息进行了分离，使用户在网络中很容易被定位，保证了可以对攻击行为进行实时监控，提升了整网监控能力。

4. IPv6的扩展性

IPv6的报头由一个基本报头和多个扩展报头构成，扩展报头理论上可以任意扩展，使其具备了IPv4无法比拟的可扩展性，通过修改和定义扩展报头，IPv6可以实现对多种应用的灵活支持，同时又为未来支持新的应用提供了可能。目前基于IPv6扩展报头设计的IPv6+中的一系列技术已广泛应用于智能广域网，包括SRv6、IFIT和以网络分析、自动调优等网络智能化为代表的技术创新。

三、SRv6 Policy：让数据在高速公路网络中“自动驾驶”

除了车路协同等新兴业务，高速公路通信网络还承载了包括收费、视频监控、图像、语音等多种传统业务，随着这些业务走向全面数字化和智慧化，其对网络的需求不再仅是作为底层的传输通道，而是要求网络连接数量可以无限扩展，同时尽量减少其他与业务相关的限制，实现任意发展业务，即在可以满足基本通信连接的需求下，网络能主动“适应”业务流量，做到网络随应用需求而变。

SRv6是当下最热门的Segment Routing和IPv6两种技术结合体，为了在IPv6网络中实现SRv6转发，引入了SRH（SRv6扩展头）。如图1所示，通过在数据包中插入Segment指令（SID）来表达网络功能，这种指令可以理解为用户意图（SLA、服务链），包含寻址和行为的信。一个数据包中可以插入一系列Segment指令组合形成SRv6路径，在网络源节点基于

这些指令就可实现整网转发路径的预先定义，从而达到中间节点无状态的智能选路目的。另外，SRH中的每个Segment可以灵活分段，每段长度也可以变化，Segment序列后的可选TLV字段（Type（类型），Length（长度），Value（值））支持封装一些非规则信息，通过这三层的编程空间，使SRv6具备了强大的编程能力，可以更好地满足不同业务对网络路径的质量需求。

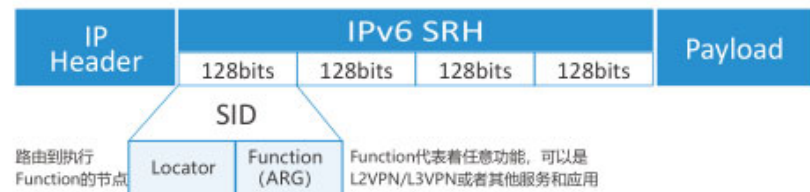


图1 SRv6数据包结构

在传统的高速公路网络运营中，通常为了保证收费等关键业务的网络质量，使其获得了过高的服务造成网络资源浪费，而未来的网络模型应当是由业务端发起，并由应用的具体需求来定义连接。因此，我们需要让网络能够实现从传统的静态策略到动态策略的智能感知和自主优化的进阶，实现业务数据在高速公路网络中“自动驾驶”，保障上层业务的极致体验。

在“自动驾驶”网络中，我们可以通过引入融合管、控、析一体的智能控制平台，统一整合全网资源、多维观测网络状态、智能分析运行数据，帮助网络管理者全方位理解业务意图，并将业务模型转换成网络模型，自动编排为Segment列表下发给网络设备，实现网络的自动、自愈、自优、自治（如图2所示）。例如当新建高速公路需要开通网络时，只需将设备安装到位连线加电，完成基本的Internet连通性配置后控制器会自动收集全网拓扑并推送最佳组网部署方案，减少施工周期和成本；当遇到节假日出行高峰时，控制平台可根据各场景应用的SLA等级，灵活定制调度策略，合理利用带宽资源优化链路质量，分级保障业务体验；当本地主机故障需要调度其它站点算力资源时，控制平台可通过建立跨广域的大二层连接，满足云主机的灵活迁移需求，实现应用与物理位置的解耦；当日常运维时，可通过流量预测及仿真，辅助运维进行网络优化设计，也可自动进行故障预测，评估链路或设备故障对网络的影响；当故障发生时，可在告警的基础上进一步根据内置的专家系统库，获取设备的状态及配置信息，得出故障的根本原因并联动进行故障恢复。基于此，由应用驱动的数据流可跨越传统网络边界，在动态调整的网络中实现“自动驾驶”。

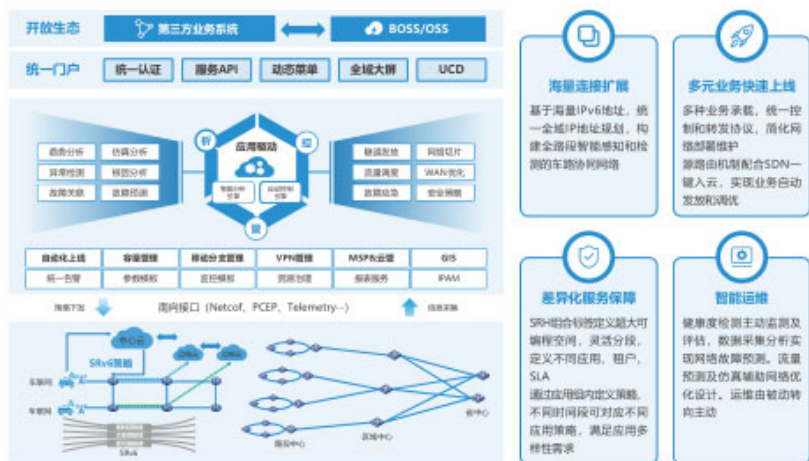


图2 自动驾驶网络架构

结语

随着SRv6技术和标准的不断成熟，SRv6跨域组大型网络、易于增量部署升级、快速业务开通的优势得到了充分体现。SRv6基于IPv6转发，完全兼容现有IPv6网络，其基于IP可达性可以让不同的网络域间更容易的连接，为未来基于人车路互联的智慧高速的发展带来更多增值可能。同时在大规模网络中，中间转发节点可以不支持SRv6，只需按照路由转发携带SRH的IPv6报文，因此在建设或改造周期很长的高速公路网络项目中可以分阶段进行更平滑的升级。另外，以SRv6、网络切片、随流检测、应用感知等在内的IPv6+技术体系，正在引领成为下一代网络的联接底座，更好的满足高速公路新生态的多样化需求。

随着高速公路智能化进程的发展，我们有理由相信，SRv6将会推动高速公路整网进入一个全新的All IPv6“自动驾驶”网络时代。

IPRAN2.0在高速公路路段接入网的应用探讨

文/李洋龙

按照《高速公路通信技术要求》，我国大部分省（自治区、直辖市）高速公路通信传输网由干线传输网和路段接入网构成，干线传输网设立在省级通信中心和通信（分）中心之间，路段接入网设立在通信（分）中心和收费站之间。由于干线传输网和路段接入网系统功能定位的不同，通常会采用不同的技术路线组建，共同为全路网的收费站、服务区、隧管所等站点的收费、图像、语音等各类业务数据和信息提供传输通道，是高速公路通讯体系中的重要组成部分。

一、从个性到共性，当前高速公路路段接入网技术路线应用分析

国内高速公路通信传输网采用的技术路线多种多样，其中干线传输网大都采用OTN系统组建或正在由SDH、PTN等向OTN系统演进，路段接入网中SDH、MSTP、PTN、OTN、以太网等多种新旧技术并存，路线比较开放。形成这种情况的原因在于干线传输网的主要作用是将各个路段的业务数据上传到省级通信中心，更加关注网络带宽和传输效率，因此OTN具备超大管道的特性非常适合干线传输网的大带宽需求。而高速公路运营相关的具体业务集中在收费站及路侧，路段接入网技术路线的选择需要更契合业务侧的接入需求，因此各省在路段接入网设计时，通常结合自身实际业务情况，从满足当前个性化需求出发，选择不同的技术路线支撑业务发展，后再根据业务演进带来的新需求更新路段接入网的规划建设，以太环网、PTN等技术就是在高速公路业务全面向IP化演进过程中逐步替代老旧的SDH、MSTP，得到大量应用。

总体来看，各省无论应用哪种技术，高速公路通信网建设模式主要采用以省级通信中心为核心的多级树形架构，解决收费站、通信（分）中心和省级通信中心之间的数据交互需求，有效支撑了高速公路不同发展阶段的信息化水平。同时也看到，在当前的树形架构下，路段接入网主要解决的是收费站到通信（分）中心节点间的数据传输，同级节点之间的信息交互是很难高效完成的。

二、迈向智慧高速，路段接入网建设需求发生转变

随着高速公路智能化发展，智慧高速的概念已扩展到“建管养运服”等高速公路建设的各

个阶段和业务领域，为持续推动智慧高速高质量发展，各省纷纷展开智慧高速公路建设指南的编制工作。通过研究各省建设指南可以发现，尽管在建设方向和技术路线的制定上仍存在差异，但行业对于智慧高速建设的基本原则正在趋向统一：不再只强调新技术、新产品“大而全”的概念堆砌，重点关注场景落地，让“智慧”产生价值，尤其是提升社会公众的体验感，使智慧高速建设理念回归到高速公路运营和服务的本质。

在以此为目标的前提下，车路协同、智慧养护、路网管控等极具代表性的应用正在开展建设，而和收费、视频监控等传统业务不同的是，这些智慧类应用的业务模型决定了数据从感知终端采集到上层应用分析再到提供信息服务的整个流程中，相应的通信连接是需要随着交通参与者的差异化需求灵活制定的，比如随时随地发起连接、就近横向转发、低时延保证等需求。例如车路协同场景下，感知数据在边缘计算平台完成融合计算后，需要将相应的结果数据分别传输给路侧RSU、其它相邻路段上的RSU、云端V2X业务运营平台，这就要求路段接入网具备应用意图感知，灵活调度的能力，为数据提供实时高效的交互服务，而现有的网络架构还不足以支撑数据多点流向，应用级意图识别的复杂需求。

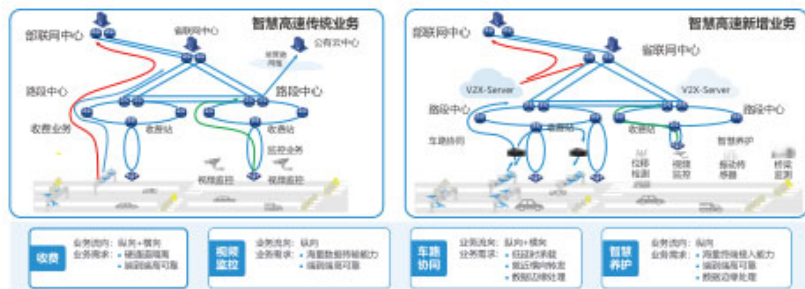


图1 智慧高速业务通信模型变化

从建设内容来看，物联感知、多元融合、协同控制等都依托于海量的物联终端设备，而IPv6已成为物联网的核心协议之一，尤其是国家将IPv6技术纳入到国家信息基础设施建设之中，其在高速公路行业的全面应用也只是时间问题，2023年4月，工业和信息化部、中央网信办、国家发展改革委、教育部、交通运输部、人民银行、国务院国资委、国家能源局等八部门联合印发《关于推进IPv6技术演进和应用创新发展的实施意见》，更是加速了这一进程。因此，在既有智慧高速体系框架下，如何应用分段路由（SRv6）、网络切片、随流检测、网络智能化等“IPv6+”技术来有效支撑交通基础设施数字化、智慧化转型，成为选择下一代通信传输网的硬性标准。

当前应用最为广泛的几类传输路线中，SDH和MSTP已逐渐被淘汰；OTN主要作为底层传输资源做合分波，不具备应用感知的能力；PTN和基于PTN发展而来的SPN，底层协议都是基于IPv4协议栈，对IPv6的支持并不友好；而IPRAN不仅可以同时支持以太、POS、SDH等业务接入，在充分融合了分段路由（SRv6）、网络切片、随流检测等一系列“IPv6+”技术之后，利用IPv6优秀的可扩展性发展成为IPRAN2.0，不仅支持现有IPv4业务，更为未来业务向IPv6演进提供了有力支撑。

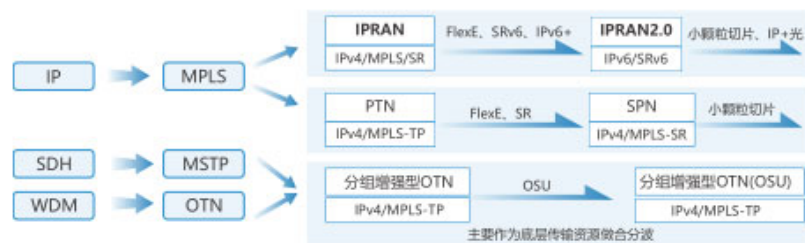


图2 主流传输路线能力对比

三、基于“IPv6+”技术底座，IPRAN2.0推动高速公路路段接入网络变革

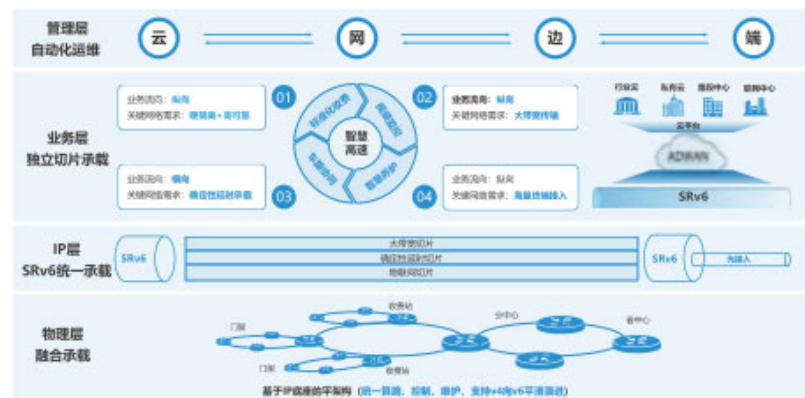


图3 高速公路IPRAN2.0路段接入网架构

随着未来智慧高速业务的持续发展，路段接入网的网络规模和架构必将更加庞大复杂，成为制约业务进一步演进的瓶颈，国内高速公路通信网大多采用IP底座+光底座的分层网络架构，IP层面和光层面的控制没有做到统一，存在算路效率低、电层映射效率低、光层控制面技

术落后等弊端。而IPRAN2.0依赖于和光传输完全不同的演进方向，在物理层、协议层和业务层都实现了突破，可以支持树形、交叉、环形、混合接入等任意的组网模型，非常适用高速公路复杂的通信连接需求，具备了重构高速公路通信传输网服务体系的能力。

1. 物理层融合承载

基于IP底座，IPRAN2.0实现和业务网的融合，这种扁平化架构大幅简化网络层级的同时，实现了网络控制、算路、维护的统一，进一步提升了整个通信网络的服务能力。在内蒙古、新疆等地域广阔的省份，收费站之间传输距离往往超过80km，IPRAN2.0还可通过在设备侧融合DWDM业务板卡实现远距离、大带宽传输等OTN网络才具备的特性，打破物理介质的界限，让业务可以充分享受到IPv6+的技术红利。

2. SRv6统一承载层协议栈

传统的光传输网络设备只有传送平面，没有智能化的控制平面，整张传输网的控制平面集中在传输网管平台，所有业务数据的转发通道都需要通过网管平台预先定义好，为业务提供面向连接的静态组网，这种机制很大程度上限制了整网的弹性和灵活性，无法为业务提供真正意义上的端到端调度。IPRAN2.0方案中路段接入网同时具备转发平面和分布式智能控制平面，并且以SRv6为主要协议，实现控制平面和数据平面的统一承载。SRv6的隧道基于SDN架构完成业务通道和物理网络的解耦，结合SD-WAN控制器的业务流量分析和自动化控制，使高速公路路段接入网实现任意节点间通信和路径智能调优的能力，打破应用和网络之间的鸿沟，极大提高了整个通信网的传输效率。

IPRAN2.0通过SRv6+EVPN技术可实现IPv4/v6双栈业务能力，在当前应用、终端不能完全适应IPv6单栈部署的情况下，采用EVPN VPWS over SRv6和EVPN L3VPN over SRv6方案，可以用来承载当前IPv4二层和三层业务接入，符合IPv6规模部署网络先行原则，优先将通信传输网络层面实现IPv6单栈网络环境，再逐步进行应用和终端侧的IPv6改造。

在可靠性方面，IPRAN2.0不仅可以提供和光传输一致的环网自愈保护机制来快速实现网络恢复，还基于多个层级的技术体系提升了业务的可靠性保障：

设备层：可提供单站点的双设备主备冗余保护，设备本身还具备板卡和部件级冗余，当单个设备完全故障时也对业务无影响。

链路层：通过链路聚合能力将多条物理链路捆绑为一条逻辑链路，当其中一条物理链路故障时，可快速剔除失效链路实现快速收敛，期间对业务无影响。当多条物理链路故障时，可基于TI-FLA/SRv6 Policy Hot-Standby技术实现快速收敛，收敛时间≤50ms。

3. 业务层差异化保障

收费业务是高速公路的核心业务，根据《高速公路通信技术要求》、《高速公路信息通信系统联网技术要求》(JT/T 918-2014)，为实现不同业务间硬隔离的要求，IPRAN2.0提供FlexE硬切片服务，实现收费业务、视频监控业务、综合信息化业务的网络通道物理隔离能力。FlexE是在Ethernet技术基础上，为满足高速传送、灵活带宽设置等需求，通过时隙交叉技术和端口捆绑技术实现的低成本、可动态配置的电信级接口技术，具备和传输设备相同的物理隔离能力，还可灵活切片和调整切片大小，支持新业务的快速上线和接口带宽的实时调整。

现实中每种业务对网络的质量要求往往不尽相同，在线计费需要高可靠、低时延的通道，视频监控需要大带宽、低时延的通道，自动驾驶需要确定性、低时延、任意就近转发的通道等等，IPRAN2.0可根据业务在时延、带宽、延迟、可靠性等多个方面的需求智能规划并构建端到端路径，实现全网差异化SLA保障，还支持更精细粒度的应用级识别和引流，从而实现更细致，更智能的业务品质保障。

云计算技术在智慧收费站、车路协同等场景的广泛应用，打破了物理设备和虚拟资源的边界，IPRAN2.0控制器支持和云控制器联动，将算力资源彻底“融入”通信网络，把云端的能力延伸到边缘侧，形成一个统一的服务体系，由统一的云控平台完成全网资源的动态分配和任务的智能调度，这意味着业务可以根据实际需求，灵活地选择将任务在云端或者边缘端进行处理，从而实现了应用和物理资源的解耦，实现更敏捷、更可靠的服务保障。

结语

智慧高速的建设是实现国家交通强国发展战略的核心内容之一，也是各类技术创新应用的前沿阵地，而技术路线的应用应当根据实际业务需求来制定，从SDH、MSTP到PTN和OTN，高速公路通信传输网的每一次技术革新都在推动着业务的快速发展。IPRAN2.0遵循成熟的技术标准，且仍在不断的更新迭代，无论从生态产业链成熟度还是从未来高速公路云网融合的角度来说，IPRAN2.0必将成为下一代高速公路通信传输网的最佳选择之一。

新华三IPRAN2.0让武汉绕城高速通信网“随需而变”

文/李洋龙

当数字世界里看不见的数据流与高速公路上看得见的车流相互叠加，会发生什么样的变化？有些人感受到的是畅通无阻、更加舒适的驾驶体验，有些人感受到的是路况信息实时获取，让路上等待的时间大大缩短。这些变化的背后，高速公路通信网络作为信息融合的纽带，是智慧高速深度转型的先决条件。

2023年5月，湖北省交通运输厅印发《湖北省“数字交通”三年行动方案（2023—2025年）》，将“推动智慧高速公路建设”作为主要任务之一，提出“推动高速公路感知网络与基础设施同步规划、同步建设人、车、路、云、边融合协同能力有效提升。在此背景下湖北联合交通投资开发有限公司（以下简称“湖北联交投”）基于所辖路段，开始研究可以适应智慧业务特点的高速公路通信网建设方案，旨在强化网络通信保障能力，提升高速公路通信网络的稳定性、可靠性和灵活性。其中武汉绕城高速公路作为武汉城市快速路网的组成部分，也是连接武汉市和周边城市的重要通道，而且绕城高速东北段的施岗通信分中心作为湖北省通信骨干传输网上的重要节点，承载多个分中心的业务上述互通需求，其通信网的传输质量影响着多个路段的业务转发，因此武汉绕城高速（东北段）通信网的转型升级意义更加凸显。

一、基于新华三IPRAN2.0，重构武汉绕城高速公路通信网

高速公路通信网具有接入业务类型多、覆盖范围广、安全和可靠性要求高、运维维护困难的特点，湖北联交投在进行高速公路通信网技术路线的比选时充分考虑了各方面因素，包括网络安全性、可靠性、灵活性、技术先进性、经济性、开放兼容性等多个方面。最终，湖北联交投选择与多年深耕智慧交通领域的新华三集团合作，通过引入IPRAN2.0+SDN的创新技术和解决方案来构建新一代高速公路通信网，这种以软件定义网络为核心的网络技术带来了全新网络架构设计理念，解决用户核心诉求的同时，使网络能够主动适应用户业务和流量变化，实现业务和底层网络解耦，满足高速公路感知网络普遍而广泛的灵活接入需求。

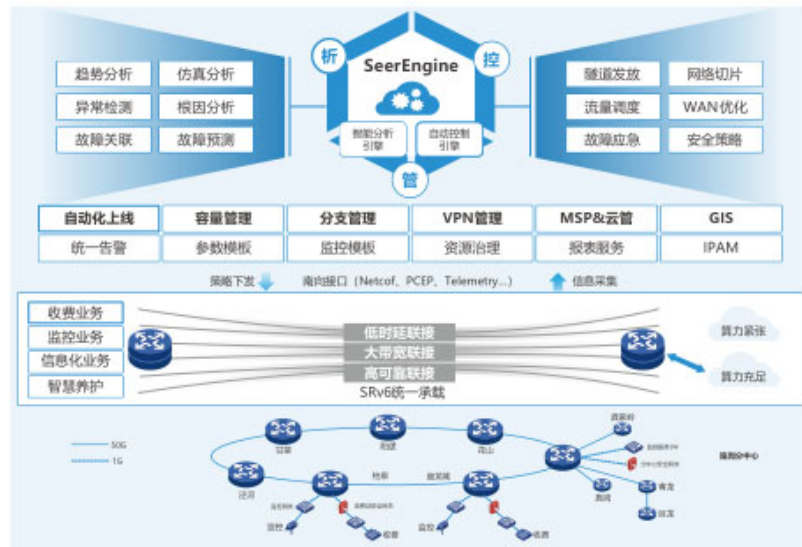


图1 武汉绕城高速通信网IPRAN2.0+SDN整体架构

1. 超大带宽网络切片，实现业务安全隔离

改造前武汉绕城高速SDH通信网带宽仅为622M，已无法有效承载视频监控的业务流量，通过采用H3C RA5300设备，湖北联交投将收费站到分中心间的通信网传输带宽升级为双环50GE互联，为保障业务之间的安全隔离，分别为收费系统、监控系统划分FlexE切片，在预留足够带宽资源的情况下，实现收费和监控系统之间的严格物理隔离，物理接口剩余带宽可为既有业务切片扩容，也可为未来新的业务接入提供带宽资源。

2. 全场景高可靠性，保障业务连续性

湖北绕城高速IPRAN2.0方案在设计时充分考虑了各种故障场景下的影响及业务恢复方案，并在项目中通过多重保护机制来实现整个承载网的可靠性：

设备层面：硬件设备所有组件都支持冗余备份。

设备协议层面：两台设备可以组成双机备份模式，对二、三层接入业务进行链路和节点保护。

链路层面：在网络设计时链路通过部署双链路环网，保证链路无单点故障，支持链路质量检测，链路质量劣化时触发倒换收敛。

协议层面：支持BFD协议做点到点、端到端的快速故障监测，支持BFD与多种协议联动，使得感知到故障后可以立刻通知其他协议快速收敛。

业务层面：通过BFD协议对链路、协议、隧道等进行故障监测，通过FRR、TI-FLA、SRv6 Policy Hot-Standby、主备PW等可靠性算法、业务保护机制。

正常情况下，业务数据流会在环网上的两条50G链路上负载分担转发，当其中一条链路故障时，业务会收敛到同一根连路上进行转发；当两条链路或链路上某个节点设备故障时，业务会切换至环网的另一个方向转发。

3. SRv6 VPN灵活承载，业务路径动态调优

传统SDH设备的特性决定了整套系统作为透明传输管道，仅可为业务建立静态连接，无法实现业务灵活调度的能力。通过建设IPRAN2.0方案，武汉绕城高速实现了各类业务的统一承载，基于SRv6 L2/L3 VPN不仅平滑接入现有业务，还可灵活改变业务原有流量模型，再结合iFIT随流检测技术实现通信网实时、全方位的网络运行状态监控，获取业务流量的实时SLA性能指标，再根据业务（或应用）的网络质量需求信息进行路径计算，为数据流提供了灵活的转发路径选择方法，让高速公路通信网具备业务路径动态调度能力的同时，对接入侧现有设备的功能和性能不产生任何约束性要求。

4. 构建网络控制中枢，实现“管、控、析”三维一体

在施岗分中心部署的SD-WAN控制器融合了网络管理、自动化控制、智能分析等组件，实现武汉绕城高速通信网端到端的网络和业务自动化、可视化、精细化管理。在首页界面可基于全局视角，通过统一整合全网资源、多维观测网络状态、智能分析运行数据，为运维管理部门提供深度网络可视（业务、网络、流量、路径可视化），智能运维，故障预测，简化了网络运维工作。在业务侧，随着越来越多的智慧类需求从云中心延伸到路侧边缘，SD-WAN控制器提供了自动化下发VPN业务、应用策略、QoS业务等，用户仅需在控制组件上指定业务部署逻辑，即可实现业务需求到网元配置的自动转化和下发，大大缩短了业务开通周期。



图2 武汉绕城高速通信网SD-WAN控制器

不难看出，无论是从底层设备还是到上层业务体验，IPRAN2.0为武汉绕城高速公路通信网带来了巨大的价值提升：

业务统一融合承载：一套设备实现收费站到施岗分中心的业务承载以及收费、监控视频等各类业务间的物理隔离。施岗分中心通过IPRAN2.0设备对接其它路段分中心节点，打破传统传输厂商间的技术壁垒，实现其它路段与省级节点之间的流量透传。

灵活演进的基础架构：武汉绕城高速通信网基于双链路50G环网，打造了超宽低延时业务通道，同时在单设备和整体网络架构升级方面具备灵活的可扩展性。

可靠的业务保障：通过设备级保护、链路级保护、架构级环网保护，IPRAN2.0为高速公路关键业务带来多重的可靠性保证。

精准投资：与传统的传输系统建设项目相比，IPRAN2.0方案以最小的投入实现了更大的回报。

二、构筑坚实网络底座，推动智慧高速高质量发展

当前智慧高速的建设内容大多关注“建、管、养、运、服”等场景的上层应用平台，而忽

略了底层网络基础设施的支撑，通过新华三IPRAN2.0解决方案，武汉绕城高速构建了一张面向未来的感知应用、灵活连接的通信网，为智慧高速各类上层应用提供了高质量的网络通信基础。

以承载车路协同业务为例，车辆碰撞预警、行人提示、盲区预警等路况信息，需要通过一定范围内的RSU实时共享给附近的车辆，当感知数据在边缘完成处理后，IPRAN2.0通信网可为车路协同业务数据交互提供多点到多点间的高可靠、低时延连接、流量就近横向转发的能力，

通过路径控制可以消除流量路径绕行行为，优化业务体验。另外车路协同业务对边缘计算的可靠性要求非常高，IPRAN2.0可以打通边缘资源池到中心云的网络边界实现云网联动，将中心云计算资源和边缘计算资源有机整合起来，当边缘计算故障无法提供服务时，可以动态的建立终端到中心云资源的连接，增强云端资源调用，保证车路协同业务的可靠性。

2021年12月，交通运输部在《数字交通“十四五”发展规划》发文中指出，要统筹利用行业和社会通信网络资源，推进行业IPv6规模部署和应用任务。2023年4月，在八部委联合印发的《关于推进IPv6技术演进和应用创新发展的实施意见》中提到分段路由（SRv6）、网络切片、随流检测、应用感知网络（APN）和网络智能化等成熟的“IPv6+”技术实现产品化落地。面对未来交通行业基础设施向IPv6演进的需求，IPRAN2.0在技术层面和对IPv6的支撑层面非常契合高速公路业务场景，它可以满足高速公路数字化、智慧化转型需求，支撑“IPv6+”技术在高速公路行业实现产品化落地。

武汉绕城高速公路通信网是国内首条采用IPRAN2.0技术方案组网的高速公路，时至今日，中国无数条高速公路正像武汉绕城高速公路一样，在数字化创新的加持下向着更高阶段的智能化加速演变，在这一过程的背后，新华三集团也将秉持着“精耕务实，为时代赋智慧”的理念，构建坚实有力的数智转型创新底座，通过前沿技术与高速公路场景的全方位融合，让更多出行者拥有高效、便捷的未来出行体验。

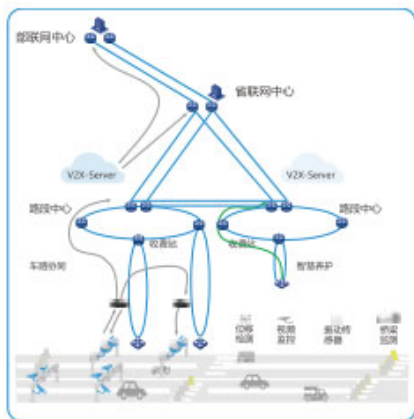


图3 IPRAN2.0支撑车路协同业务发展

依托站级云化智能底座推进收费站标准化

文/李洋龙

从1988年中国第一条高速公路沪嘉高速开通，截止2022年末全国高速公路里程已达17.73万公里。我国在35年时间里从零成长为全球高速公路里程最长的国家，在这个进程中收费系统也伴随着高速公路里程的发展迎来了多次飞跃，如2003年，开始实施高速公路电子收费；2008年，开始实行封闭式收费；2018年，开始提出取消省界收费站，并在2019年底实现了高速公路收费“一张网”。随着省界收费站的全面取消，使得跨省通行变得更加顺畅，但实体收费站的存在，尤其是一些交通流量大的主线收费站，即使在全网ETC使用率达到将近65%的情况下，依然会导致路段频繁拥堵，给出行带来不便，如果能像取消省界收费站一样取消高速公路出入口收费站，车辆可以自由进出收费高速公路，并可按照实际行驶路径自动完成里程计费 and 收费，无疑将使整个高速公路的运行更加通畅和便捷，因此自由流收费成为收费技术方案的下一个探索方向。但从客观实际出发，除核心技术路线选择有待确定外，还有车辆身份唯一性认证、车主信用体系构建、偷逃费涉及到的法律体系建设等等一系列问题需要解决，因此从多个角度看，全网自由流都会是一个循序渐进的过程，高速公路管理部门亟需寻求新的解决方案来提升收费站的通行服务能力。

一、“新技术”+“老场景”，智慧收费站开辟新路径

近两年，匝道预交易、智慧岗亭、特情自动化处理等新技术和新产品逐渐成熟，通过对相关技术和方案的验证，全国多地迈出了探索“准自由流”智慧收费站的第一步，整站应用基于以超融合云服务器为核心的体系构架，辅以ETC不停车收费、匝道自由流预交易门架、全车型车道机器人、智慧岗亭和特勤处理终端等智慧化设备率先打造出一批收费站数字化转型的“样板站”，实现了各类设备系统IP网络化，从之前的车道级“单机单控”升级为站级集成式“联网联控”，具备兼容性好、生态丰富和应用广泛等特点，有效保障了各类收费设备系统平稳运行，帮助收费站逐步向窄岛化、无岛化、无亭化、无人化演进，大大降低了车辆通行收费站的时间，推进了全网自由流的发展。

但是，通过深入调研可以发现已建成的智慧收费站中，各省之间、各区域之间普遍存在技术标准不统一，建设内容各异的情况。为支撑后续全网优化升级，推动高速公路“一张网运行、一体化服务”水平不断提升，交通运输部路网监测与应急处置中心在《高速公路联网收费

系统优化升级试点工作方案》中提出收费站标准化专项试点，旨在从用户服务规范化、运营管理精细化、站级设备系统标准化和网络安全保障等方面，全面提升收费站通行服务能力、业务规范性、计费精准性、精细化管理水平及系统稳定性。

二、站级云化智能底座是收费站标准化的核心

推进收费站标准化涉及到多个方面，例如车道设备设施、数据通信接口、网络安全、管理监测系统、收费系统等。分类来看，一方面因为全国各地地理环境、气候特征、社会活动的不同，决定了很难将外场设备设施做到细粒度的标准化；另一方面，收费系统作为收费站核心系统，全国1700多家高速公路业主单位使用的收费软件超过300种，且每种收费软件对运行资源和平台的要求各不相同，急需进行规范化和标准化，实现软件架构的统一。因此收费站标准化工作的重点应当在保留车道设备设施个性化需求的同时，着重规范收费系统建设标准，包括收费相关各类站级业务系统的标准、车道设备与站级业务系统间通信链路的冗余标准、车道设备与站级业务系统间数据通信接口的对接标准等。具体思路为仅将车道设备作为端侧智能感知单元，通过冗余链路和站级业务系统互联，各类业务系统充分融合云原生技术进行模块化设计，实现平台化、容器化部署，利于各系统的快速迭代和系统间的信息互通，打造“云-边-端”协同的站级云化智能底座，使收费站从管理侧到业务侧形成统一。“云”指的是基于“云”化能力构建的云管理平台，一般部署于省级中心或路段中心；“边”则将计算、存储、网络和应用软件等软硬件资源集成在一个超融合虚拟化环境中，主要部署在收费站；“端”是指体系化的车道智能设备感知系统，通过智能物联网关实现对车道外设的集中控制、监测和管理。



图1 站级云化智能底座整体架构

站级云化智能底座以收费站为单位重构业务体系，将基于车道收费模式升级为基于收费站收费模式，实现集约化建设、中心化管控、集中式收费。

1. 集约化建设

站级云化智能底座通过采用集数据计算、存储、网络等资源于一体的超融合技术架构搭建数字基础设施，实现基础设施集约化建设，构建了一平台管控多车道、多门架的体系架构，通过边缘收费终端+通信备份链路双保障机制确保收费系统的稳定运行。

计算资源集约化

传统收费站中的各个业务系统分散运行在各类设备上，例如收费数据服务器、收费视频服务器、传输服务器、费率服务器、PC主机、设备设施监测控制服务器等。站级云化智能底座依托超融合平台实现了收费站多个业务系统的统一承载，包括：站级收费服务系统、站级桌面管理系统、设备管理系统、运行监测及工况保障系统（含设备监测、业务监测）等。同时，云化智能底座支持裸金属、虚拟机、容器等多种计算形态，满足业务系统不同的资源部署需求。

网络安全资源集约化

收费是高速公路的关键业务，需要参照等保2.0三级等保要求建设，就目前来看，省联网中心的安全防护比较完善，收费站甚至是路段分中心级别的安全防护仍比较薄弱。站级云化智能底座支持以纯软件形态提供丰富的网络和安全功能，支持高效便捷的可视化部署，客户无须购买专用的网络安全硬件设备，便可用更低的预算满足网络和安全方面的需求。站级云化智能底座还可以与态势感知联动，将流量发送到态势感知做分析，实现实时告警，及时发现异常流量，将态势感知延伸至收费站及门架。

2. 中心化管控

随着收费站设备集约化和人员数量的降低，路段分中心作为高速公路的基层管理单位，无论从管理角度还是业务流程上都需要承担更重要的责任。通过在路段分中心部署云管理平台可纳管多个收费站超融合系统，统一以“云资源”形式进行管理，为高速公路业务提供“一站式”服务。云平台还可对纳管的收费站云资源进一步抽象，统一以“云服务”的形式提供，包括云主机、云硬盘、快照、镜像、虚拟网卡、密钥对、租户网络、安全组、报表等，为路段分中心提供一套集云资源、云服务、云运营、云运维为一体的云管理平台。

3. 集中式收费

传统收费车道级系统的控制核心是车道控制器，一般运行在基于x86架构的工控机上，工控机I/O端口实现对车道设备的控制驱动和数据采集等功能。通过建设站级云化智能底座，可以将原本分布在各个车道工控机上的收费系统统一部署在收费站超融合服务器上，实现了各个车道间数据的共享与协同，消除临道干扰的问题。站级云化智能底座的建设方案打破了传统单条收费车道离线式系统架构，实现了站级的集中式收费，较传统收费系统而言，主要在降本、提质、增效三方面实现了升级与变革。降本方面，通过收费业务上云、设备集约化、智能化降低建设和运营管理成本；提质方面，通过收费系统标准化、发票电子化，提高客户服务质量，提升通行体验；增效方面，通过在线计费、车型识别校验提升计费精准性。

三、站级云化智能底座的价值

相较于传统收费站机电建设模式，站级云化智能底座从多个方面带来了优化创新：

简易部署，缩短项目工期：通过云化智能底座统一承载多个应用系统，减少了设备设施的数量，有利于设备布线、调试；平台本身还支持主流应用、数据库的一键部署向导，通过向导式创建应用可快速完成多个系统的部署、调试，效率更高，效果更好。

简易扩容，保障通行效率：云化智能底座从资源按需扩展、业务按需调配、管理按需调度三个方面出发进行设计，支持多角色集群管理，实现在同一集群内同时支持包括融合型、计算型、存储型等不同类型节点，支持独立灵活扩容，满足收费站业务在运营过程中对资源的非线性扩容需求。在业务灵活性方面，平时车辆通行量较少时，收费站一般会关闭部分车道服务，云化智能底座支持秒级拉起车道计费系统，快速恢复车道服务，保障通行效率。

高可靠性，业务持续运营：云化智能底座采用高可用方式部署，可定时对集群内的主机和虚拟机状态进行监测，当主机发生故障的时候，受影响的虚拟机将在集群中的其它主机上自动重启，从而将停机时间和服务中断降到最低。除此之外还提供操作系统HA、应用HA等多种高可用方案，确保站级系统具有健壮性，在单点故障下有保障业务正常开展的应对措施。

简易运维，降低运维难度：借助云化智能底座丰富的资源支撑，针对收费站的高保障要求，云化智能底座提供智能运维平台，围绕设备监控、态势感知、远程回控等多个方面打造出一键运维可视化工具，实现对设施、应用、资源的全方位监测支持，为站场管理人员提供全面

的数字化管理新手段，同时也为智慧收费站未来站务“一岗多能”业务发展趋势提供必要的能力手段。

多维安全，等保安全合规：云化智能底座提供多维度安全防护体系，从管理层安全、内层安全、数据层安全、业务层安全、安全监控、安全审计和容灾备份等7个方面全方位保障业务安全。

便捷利旧，有效保护投资：云化智能底座基于同一套架构平台，未来在面临全网自由流的撤站需求时，可将收费站物理主机平滑上移到路段分中心或省中心进行复用，不用额外采购计算及存储资源，有效保护现有投资。

绿色节能，响应双碳战略：云化智能底座不仅通过设备集约化建设大幅降低了设备、制冷等用电成本，还支持智能电源管理功能，实时监测集群内主机的负载，当集群内的主机负载低于设定阈值时，将一台服务器上的虚拟机全部迁移到其他服务器中，并将该服务器自动关闭；当集群内负载达到指定阈值时，自动唤醒该主机，并通过动态资源调度功能实现负载均衡，进一步降低了能耗，推动智慧高速绿色低碳建设。

结语

随着收费站标准化专项试点项目的持续推进，在相关政策指导下，收费站建设标准将进一步得到规范，具体的场景和功能也会越来越明确，有望打通高速公路收费服务的“最后一公里”，为社会创造更为智能、便捷、安全的交通出行环境。站级云数字化底座作为收费业务和数据的最终载体，通过创新的建设和管理模式帮助收费方式实现了“准自由流”的跃迁，基于云原生构建的“云、边、端”一体化收费系统智能底座，将在真正推进“全网自由流”的那一刻再次释放价值。

高速公路收费系统安全能力提升的思考

文/王泽宁

一、高速公路收费系统安全能力现状分析及建议

自2020年5月恢复收费以来，高速公路联网收费系统初步建立起了较为完备的网络安全及数据安全体系。从《联网收费系统省域系统并网接入网络安全基本技术要求》到《联网收费系统网络分区域管理指南（试行）》，再到最近的《高速公路联网收费系统优化升级试点工作方案》中独立的试点项目-网络与数据安全提升专项试点的相关要求，行业内对于安全体系的技术要求越来越细致，体系规划也越来越系统。

然而，偶有发生的网络安全事件仍旧在时刻提醒着我们，当前的安全防护工作尚存在大量隐患，而安全风险一般都发生在防护最薄弱的地方；大量的标准规范、政策法规，需要和高速公路运营单位自身的管理体制、系统的实际运营风险结合进行针对性的优化，这也恰恰是当前缺失的主要工作之一。

抛开业务复杂性空谈安全会耽误实际生产业务，通过与多省业主单位的交流沟通，我们发现以下安全现状可能普遍存在。

1. 过于复杂的边侧安全防护需求

我们经常发现，网络数据安全防护意识、重视程度，呈现省联网中心-路段分中心-发行机构-收费站层层递减的情况，然而我认为主要原因并不是工作积极性的逐级降温，而是从省至站安全专业知识技能要求的“倒梯形”与从省至站实际安全运维能力的“倒三角形”的不匹配。

因此，一方面应当加强基层安全管理人员的培训，逐级根据实际情况，建立健全网络及数据安全管理制度并强化执行；另一方面则应当尽可能采用精简化、集成化、易操作、易运维的站级安全防护方案。



2. 需要完善的安全运维管理制度

当前安全运维工作，大多由外包技术服务公司负责，且由于部分系统随不同项目建设，各

系统维护单位众多，可能导致重要系统的运维工作分散到各运维机构，责任边界可能重叠或存在真空区域，缺乏统一的监控手段；运维工程师使用的终端，缺乏统一授权管控机制，却可以直接接入收费内网，存在安全隐患。

因此，一方面应当健全安全运维管理制度，明确各服务单位的职责范围，建立健全运维技术支持单位之间的协作机制；另一方面，通过技术手段加强运维终端管控，确保只有授信终端方能接入收费网络。

3. 有待提升的安全技术防护能力

按照《取消高速公路省界收费站总体技术方案》要求，省联网中心、ETC发行机构按照三级等保要求建设，路段分中心及收费站参照三级等保要求建设。但在多个方面仍然存在短板。其一是安全风险监测未覆盖全网，态势感知基本只覆盖到省中心及部分路段中心，未延伸至收费站及门架；其二是门架设施布设广泛，收费系统中存在大量的终端分散在外场，变相扩大了安全暴露面，而系统普遍缺乏基于资产的边界准入控制能力，无法阻断非授信终端入网，造成巨大的安全隐患；其三是部分单位存在一台终端双网卡分别接入专网和互联网、在专网注册的终端频繁接入互联网的情况，造成专网边界模糊；其四是终端杀毒及主机安全防护的缺失，主流的终端杀毒软件与部分收费站终端收费软件不兼容，大部分Linux主机未安装杀毒软件或主机防护系统，无法为主机提供杀毒、进程黑白名单管理、文件保护等保护措施；其五是部分边界防护设备存在参数配置不合理、部分功能未启用，特征库升级不及时等现象，造成现有安全资源的浪费。

技术层面的安全防护是重灾区，但却不可能一蹴而就，应当结合自身实际情况，按照由急至缓的原则，分阶段实施。如优先补足基于资产的准入控制能力，同时提升管理水平尽量杜绝非法违规外联，盘点安全资源利用情况，再逐步扩大态势感知覆盖范围，完善终端杀毒、主机安全等能力。

4. 暂时缺位的数据安全防护措施

数据是联网收费系统的重要资产，然而当前大部分运营管理单位不同程度存在未发布数据安全管理制度或相关管理制度不健全等问题。数据分级分类标准、数据安全保护工作流程、数据安全应急处置流程、数据共享监督及审查机制均不明确；同时，缺乏有效、配套的数据分类

分级、存储加密、数据安全审计、数据防泄漏、数据脱敏、传输加密等措施对重要数据、核心数据、敏感数据实行不同级别的安全防护。

因此，一方面应当出台数据安全相关规范，明确数据安全防护责任主体及边界；另一方面，建立数据安全管控平台，理清数据资产台账，完善数据加密、数据脱敏、数据库审计、数据水印、数据流量分析溯源等系统，优先以保有大量数据的省中心、发行方为主，但在路段分中心、收费站等层级，仍应当加强数据传输过程中的安全防护。

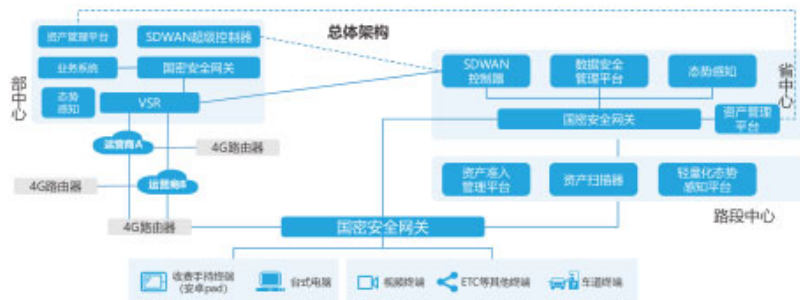
5. 尚待完善的国密加密应用要求

收费系统需要按照三级等保的要求进行测评，在《联网收费系统省域系统并网接入网络安全基本技术要求》中也有对国密加密有相关要求，但部分收费站部站通信链路、省站通信链路却没有采用国密加密的方式实现安全防护；除ETC专用设备外，未全面对数据传输、数据存储、身份鉴别、接入认证等方面采用密码技术进行保护。

二、高速公路安全能力提升思路

总的来说，行业当前面临的安全问题大致分为两类，其一是安全相关制度建设，包含了安全运维及安全运营两大板块，其二是安全系统架构。由于制度和体系的建设与运营主体的管理机制紧密相关，因此本文主要介绍第二类安全系统架构的规划思路。

当前系统架构存在诸多安全隐患，受限于一次性资金投入、安全技术不断迭代升级等原因，难以一劳永逸“一锤子”完成安全能力补全，因此采用“由急至缓”的原则，规划安全能力提升方案。



在收费站部署功能多合一的安全设备，对收费站欠缺的终端防护、态势感知等能力进行补齐提升；在路段中心新增对应的资产准入管理及态势感知平台，完成态势感知的分级部署及全网覆盖；在省中心及部中心，新增或升级原有平台，另外，通过SD-WAN平台，实现IPsec隧道的自动化部署。

1. 高度集成的站级安全，降低运维难度

为缓解收费站、门架层级的运营维护压力，规划采用功能高度集成的国密安全网关，在满足边界安全防护的同时，具备态势感知探针、终端资产准入控制、SD-WAN接入网关、国密加密的全部能力，ALL in ONE一体集成，大幅降低运维难度。

2. 网安融合的隧道加密，简化上线流程

IPsec隧道能够保障数据在专网及互联网链路传输过程中的安全性，也可与国密加密结合，但由于配置上线复杂，运营维护困难，实际使用率极低，因此考虑引入SD-WAN技术，完成IPsec隧道的自动化建立及维护。

3. 分级部署的准入控制，实现资产可控

建立省-路段两级的资产管理平台，对全网资产进行盘点，形成资产清单；对安全运维终端进行授权，形成运维授信清单，与国密安全网关配合，完成可信终端的入网管控。可考虑与数字证书结合，完成资产授信，实现“入网可知、资产可视、边界可控、仿冒可鉴、外联可管”。

4. 基于数据的全链防护，强化数据安全

建立数据安全管控平台，实现数据安全管控能力、数据安全风险监测能力、数据安全溯源能力，主动梳理、掌握敏感数据资产分布，跟踪敏感数据流转情况，控制敏感数据共享范围，以及数据加密、脱敏、容灾备份等机制，减少“非恶意”情况下出现数据泄露，数据丢失等情况。

关于高速行业如何用好AIGC的思考

文/王泽宁

一、AIGC的发展背景及私域模型建设的必要性

人工智能从1956年诞生之日起，先后经历了逻辑推理时期、专家系统时期，得益于算法和算力的革命性进步，从以视频AI为代表的专用智能阶段，逐步转变为以Chat GPT为代表的通用智能阶段，AI迎来了大模型的时代。2012年以来，随着深度学习的火热，分析式AI开始大规模使用，如最典型的推荐算法，大多执行分类、预测等任务，并不具备创造不存在于训练数据集中样本中内容的能力。大模型与传统AI（或小模型）最大的区别在于参数规模的量级。当前普遍认为，文本类模型的参数规模在10B（百亿）以上才能称为大模型，当模型规模超过某个临界点之后，能力会突然爆发，这也就是业界常说的模型“涌现”能力。

当前，大模型在文本、图像、视频、音频、生物制药、游戏等多模态、跨模态领域表现出色，也出现了诸如Chat GPT、文心系列、DeepFake、Stable Diffusion等明星产品。然而，当大模型的热潮涌向to B市场时，却总有龙门难越之感。那么，大模型在行业市场落地的阻碍究竟在哪里？

一是可落地性的限制。以GPT3为例，根据Nvidia测算，1024张A100 80G卡，3000亿字符，训练一次需要34天。即使抛开算力的资金投入，漫长的训练及微调周期，对行业应用来说也是无法接受的。这就势必需要在通识大模型基础上，进行量化、剪枝、知识蒸馏等操作，培养一个行业专用的私域模型。

二是大模型专业能力的限制。通识大模型在行业细分领域的认知能力非常有限，如通用模型尽管可以理解绿通等专业名词，但对于绿通查验需要参考的政策依据却并不清楚。其原因本质上是模型的训练数据集或向量知识库中缺乏这部分专业知识，这也就涉及到接下来说的第三点。

三是数据安全的限制。截至目前业内已出现多起引入Chat GPT后的数据泄露事件，甚至涉及到芯片设计。行业内的专有数据，根据《数据安全法》及行业内相关的数据安全防护要求，对于数据安全的防护等级要求只会更高。

二、大模型私域落地需要关注什么

私域大模型有其建设的必要性，但却不能直接把模型本身照搬到本地。大模型在行业私域场景化落地时，应当重点考虑以下几方面的内容：

行业场景对语言模型幻觉及实时性的容忍程度

你知道鲁智深三打白骨精嘛？

当然知道！鲁智深三打白骨精是中国古代小说《水浒传》中的一个著名故事情节。

故事讲述了鲁智深在自己喝醉酒后，被三个白骨精（金莲、银莲、玉莲）勾引欲害，但他识破了白骨精的诡计，最终一刀砍掉它们的头颅，平定了民间的祸乱。

三打白骨精这个情节描写了鲁智深忠勇干练的形象，是中国古代小说中的经典情节之一，流传至今，三打白骨精也因此被奉为中华文化中重要的正义之举，有着很高的文化价值和艺术价值。

图1 LLM的幻觉现象示例

模型幻觉是LLM普遍存在的现象，其通俗的表现形式为“一本正经的胡说八道”，比如图中LLM绘声绘色地杜撰“鲁智深三打白骨精”的故事等。在执行创意生成、文本撰写等工作时，幻觉有时能带来意外之喜；然而在to B的行业应用中，我们通常需要LLM进行拟人化的精准输出，如流程咨询、规章制度问答等场景。

庞大的模型参数赋予了模型认知能力，同时也意味着更长的训练及微调时间。当我们想通过模型获取实时信息时，由于微调需要一定的时间，获取的信息势必是滞后的，大模型的实时性和认知能力仿佛成为了一个悖论。

为了降低大模型的幻觉及实时性问题对行业应用的影响，针对结构化数据的知识图谱及针对非机构化数据的向量知识库，能够作为LLM的外挂“参考书”，开卷有益，LLM整合“参考书”中的标准答案，完成拟人化输出。

行业场景对模型输出合规性的管控程度

如不对私域大模型生成的内容进行管控，有可能造成信息泄露，影响企业的品牌形象，甚至可能导致法律纠纷。私域模型中将导入大量企业经营数据进行模型微调，如不对这些数据进行严格管控，势必造成数据泄露。

实际上，输出合规性的管控不只局限在LLM，对于图像生成而言，也存在生成违禁图片元素的可能。在私域大模型的落地过程中，一般要完成输入侧、模型侧、输出侧三个层面的信息过滤及规避，输入输出侧构建审核模型，对问题内容、答案内容进行审核；在模型侧，应当强化内部数据管理，避免违规数据、垃圾数据进入学习样本。

行业场景对CV及跨模态（图生文）误报率的容忍程度

当前通用CV模型的准确率有待提升，且在实际行业应用中也需要进行专项微调，如用在高速公路日常巡检场景，模型的注意力就应当放在路面是否平整、路面是否有病害、防撞栏是否变形等。而图像的维度远高于文本，导致CV及image caption（图像描述，跨模态模型的一种）模型的微调周期就比较长，再加上网络上的pix2words（图像对应文本）的优质样本很少，进一步增加了此类模型在行业中的落地难度。

因此在行业落地中，应当充分利用交通行业丰富的视频监控素材作为训练样本。可根据场景任务调整参数精度，如判断一般交通事件（如拥堵、缓行、排队长度等）可将参数设置为int8格式；判断路面病害，将参数设置为FP16格式，以此提升模型微调效率。此外，在落地部署时，可考虑将此类模型在工程二期上线，留出足够的时间裕量降低模型误报。

行业对解决特殊场景需求孵化定制化模型的需求程度

这里需要明确黑盒模型的概念。诸如神经网络、梯度增强模型或复杂的集成模型均属于黑盒模型（black-box model），这些模型的内部工作机制难以理解，也无法估计每个特征对模型预测结果的重要性，更不能理解不同特征之间的相互作用关系，但通常具有很高的准确性。这样的模型适用于大致知道输入输出的关联性，但无法准确按照专家系统的设计原则进行数学逻辑还原，在具备大量训练样本的情况下，可通过深度学习，完成场景化应用算法的开发上线。

在落地此类应用时，应当综合考虑需求的迫切性、投入规模大小、模型训练周期、模型孵化难度、训练样本规模、商用价值等因素，判断是否具备落地必要性。

三、高速行业AIGC场景落地的思考

1. AIGC+智能客服：改善体验，优化服务

当前高速公路客服系统一般分为话务端和微信端。就话务端而言，一般都存在菜单层级



过深的问题，导致用户单次访问耗时长、用户体验差，且人工坐席少，业务承载能力有限。就微信端而言，交互能力普遍偏弱，救援服务、费率查询等虽然有访问入口，但一般都指向话务端；路况服务、服务区信息等，又通常只能提供全局信息，有效信息指向性差，无法根据用户的实际情况给出有针对性的信息辅助。

因此可以考虑将LLM作为客服系统的核心，统一对接话务端及微信端，通过外挂向量知识库的方式，给模型赋予政策法规、实时路况、服务区实时状态等信息的回答能力。在微信端可直接返回文字；在话务端可通过语音识别等算法，实现LLM与出行者的直接对话。LLM对客服系统的赋能，能够带来的价值有：

降低话务等待时间，大模型自动识别客户需求，提供精准、快速的解决方案，降低话务平均等待时长，提升满意度。

降低人工成本，大模型自动处理大量客服问题，减轻人工客服压力，降低企业人工成本。

改善用户体验，大模型提供友好、自然的交互方式，帮助用户快速获取目标信息，及时匹配救援力量。

知识库积累学习，在日常处理客户问题的过程中不断积累知识，丰富内部知识库，实现知识传承，并实时更新。

2. AIGC+绿通违规解释：消灭疑问，提升效率



当前限制绿通查验效率的三个主要问题：一是查验人员的常识性、经验性知识很难通过培训实现知识共享；二是出现绿通违规时解释成本高，不仅降低通行效率，还容易导致现场纠纷甚至冲突；三是绿通参照的标准规范多，查验人员很难熟记全部规章制度的要求。

因此可考虑将《鲜活农产品品种目录》、《关于进一步提升鲜活农产品运输“绿色通道”政策服务水平的通知》（交办公路〔2022〕78号）等相关规定及有经验的查验人员形成的经验库以向量知识库的形式挂载到LLM，通过移动终端打通访问入口。查验人员在执行绿通查验任务时，可参考LLM给出的意见辅助判断非免检车辆是否符合绿通标准，如出现违规情况时，也可根据其生成的违规说明，高效准确的解释违规原因。

3. AIGC+高速应急处置：及时发现、及时响应、及时归档

高速公路交通事件应急处置存在事前发现、事中处置、事后归档三个阶段。当前，事前发现阶段，大多采用人工判别、应急报警等手段，事件发现不及时；部分路段通过视觉AI辅助判别，却也存在AI算法准确率低、误报率高的问题，反而提升了监控人员的工作量；传统视频AI只能实现预置的感知能力，对整体信息缺乏认知能力，导致出现特殊情况无法准确判断。事中处置阶段，应急事件种类繁多，应急处置流程复杂，一些经验尚浅的工作人员可能无法合理及时的采取应对措施；事后归档阶段，应急事件处置报告编写复杂，需要进行原因

分析，评估应急预案，分析事件原因，总结应急经验，提出改进建议等，大大增加了监控人员的工作量。



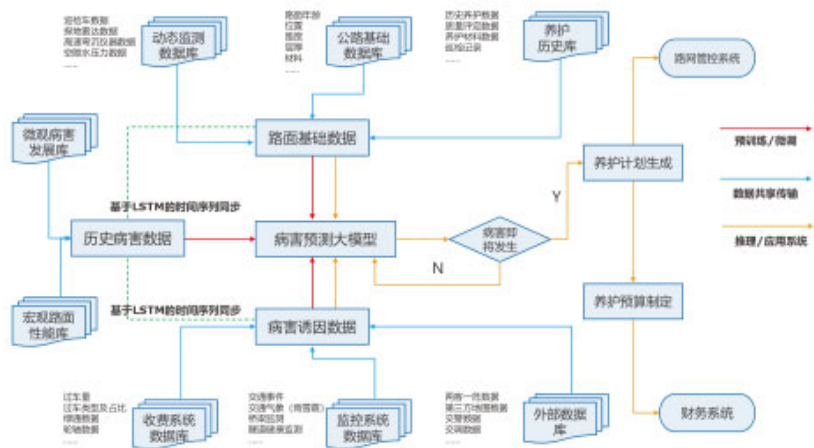
大模型与该场景的结合分为两个阶段。一是准备阶段，即低样本微调，以高速公路的路网监控数据、交通事件留档数据作为微调训练样本，对CV（computer vision计算机视觉）、IC（image caption图像描述）模型进行微调；将应急处置预案、历史事件处置报告等数据作为知识库外挂至LLM模型；根据事件处置报告的编写标准及要求，形成“交通事件应急处置助手”集成至AI助手中。

第二阶段为使用阶段，即模型推理。CV模型实时接入路网监控数据，将有包含交通事件的图像帧同步至IC模型，以提升IC模型的处理效率；IC模型分析关键帧中的事件信息，形成事件分析结论输出至LLM模型；LLM根据发生的事件信息，结合应急处置知识库，给出应急处置建议；监控人员及救援人员将处置过程以文本或语音形式反馈至LLM模型，模型按照事件报告的格式，自动完成事件处置报告生成；LLM分析事件处置建议与事件处置报告的差异，给出修改意见更新知识库，提升处置建议输出的可执行性。整个过程由模型使能平台完成调度。

4. AIGC+高速行业其他场景

在高速公路机电运维场景，存在多个管理域，且由于高速公路按路段建设的建设模式，同时存在很多运维平台，每天产生大量的告警信息且彼此之间有重叠，导致关键告警信息容易被掩盖，再加上排障需要大量的专业知识，故障定位时间较长；运维报表也很难根据用户需求定制。可考虑利用厂商提供的产品知识、运维指导书、产品联机帮助等文档，对LLM进行微调或知识库外挂，在发生故障时可有模型提供运维建议；同时，用户可利用大模型自动完成图形化报表生成。

在高速公路养护场景，当前存在病害发现不及时，病害修复时间长的问题，其主要原因是缺乏病害实时感知的手段，在发现病害后再启动养护计划又会涉及到养护预算制定、养护计划制定等流程导致时间拉长。因此可以考虑采用大模型的思路，利用高速公路运营过程中积累的大量历史数据作为训练样本，孵化预测型养护大模型，模型框架搭建思路如下图所示：



四、高速行业AIGC场景落地进度规划

高速行业AIGC场景落地大致分为三个阶段：

- 优先落地基本成熟场景，如智能客服、绿通查验、应急事件处置建议及事件归档等场景。此类场景以大语言模型为基础，上线时间短、可落地性强，也可推广至办公场景。最大限度发挥已经成熟的文本大模型能力，提前享受大模型红利，提升生产效率，降低企业运营成本，后期逐步扩大资源规模，初步具备微调所需的基本算力条件。
- 其次落地低样本微调场景，如交通事件发现、智能运维等场景。此类场景以CV、跨模态模型为基础，待CV、跨模态模型进行成熟商用阶段，基于行业已有数据完成模型微调，初步具备训练所需的基本算力条件，形成数据标注制度保障和人才储备。
- 最后落地联合孵化场景，如预测型养护场景等。此类模型以行业专用大模型为基础，将完全改变生产关系，模型、算法、数据逐渐从生产资料演进为生产工具。

五、新华三AIGC能力框架



整体框架分为基础设施层、模型层，使能层及行业应用层。在基础设施层，新华三提供完整的算力中心解决方案；在模型层，新华三具备百业灵犀大模型产品，现已支持NLP全部能力，2024年将发布CV及多模态能力，可辅助用户完成训练、微调、模型开发等工作；在使能层，提供模型使能平台，支持模型横向拓展、多模型任务低代码编排等服务；在行业应用层，提供AI助手，统一行业应用入口，简化客户与模型的交互流程。

零碳智慧服务区建设方案

文/王宇

一、零碳服务区建设背景

随着可持续发展的重要性日益凸显，全球各国正在致力于达成碳中和及可持续发展目标。作为公路交通运营中的主要碳排放源之一，高速服务区成为实现碳减排目标的关键阵地。2020年10月，交通部发文《2020年全国公路服务区工作要点》，指出加快推进智慧和绿色服务区建设，加强太阳能、风能等可再生能源及节能电器在服务区的推广应用，加快推进服务区充电和加气设施建设。2021年12月，国务院印发的《“十四五”现代综合交通运输体系发展规划》，要求选择条件成熟的公路服务区等区域，建设近零碳交通示范区。因此，对高速公路零碳服务区进行研究，有利于增强交通领域的实践研究，同时助力“双碳”目标实现。

高速服务区作为交通运营重要节点，昼夜不休，照明、空调等能耗巨大。随着新能源车渗透率提高，用电需求增加，碳减排压力加大，成为公路地理单元中的排碳大户。服务区内餐饮、商业、加油等设施需用电、用气、用水，如果不能采用清洁能源，将产生大量碳排放。因此，建设高速零碳服务区需要全面规划与设计，包括：最大利用可再生能源、推广电动汽车充电设施、利用绿色建筑技术、应用智能技术进行运营优化、实现资源回收再利用等。

按照零碳理念规划和建设高速服务区，不仅可以减少碳排放和能源消耗，也可以发挥示范效应，引领更多交通设施向可持续发展转型，为实现中国2060年碳中和目标作出贡献。这是一个系统工程，需要路桥、建筑、电力、交通等部门通力合作，以技术创新推动业务落地，造福社会。

二、零碳服务区解决方案

在零碳智慧园区的构建上，新华三集团依托“数字大脑”推出的“1+4”顶层设计理念，即一个零碳智慧操作系统和“源-探-管-服”四大模块。同时，新华三更能够做到全链条服务，在源头上推动清洁能源替代，在探测上完善碳排放监测机制，在管理上强化一体化能耗管理，在服务上做好能源利用，甚至更远期可提供碳咨询碳交易服务，全方位推动新一代“零碳智慧园区”的建设。



“1+4”模式，打造零碳服务区

“源”是从源头或者从可替代能源的角度来提升园区的能源使用效率，降低园区的碳排放。例如，我们可以采用风光互补路灯，这种路灯能够同时采用多种能源来发电，如光伏、风力等，实现多能互补。我们也可以安装光储充电车棚，利用服务区停车位空地，建设集光伏、遮雨棚、逆变器、车位、充电桩一体的模块化空间，以实现一站式服务。此外，我们还将建设建筑光伏一体化，有效利用建筑闲置屋顶建设分布式光伏发电。同时，我们还将利用光伏发电材料替代部分外立面瓷砖等材料，提供新型供电结构，实现节能环保的同时还能够提高建筑的美观性。我们在服务区的室外合适区域搭建储能设备，可以用以动态调节光伏与负荷之间的平衡，以充分利用可再生能源。这些措施可以满足服务区对能源的需求，同时实现零碳排放。

“探”主要解决园区当中的碳排放监测问题，包括园区有多少碳排放，分别来自哪里，也就是要知碳、算碳。建立实时高效的数据采集分析平台，通过新能源采集控制器完成终端对接和数据上报，实现对服务区碳排放的实时监测。新能源采集控制器能够准确测量和记录服务区的能源使用情况，包括电力、燃料等能源的使用量。这些数据将通过网络传输到数据采集和分析平台，进行统一管理和分析。其次，数据采集和分析平台将使用先进的算法和模型，对所收集到的能源使用数据进行分析和计算，以得出服务区的碳排放量。通过分析，我们可以了解园区的碳排放情况，包括哪些部分的活动是碳排放的主要来源，从而为制定减排策略和措施提供依据。通过实时监测和分析碳排放数据，我们可以及时发现并解决服务区中的排放问题。同时，这些数据还可以用于监测和评估碳排放减少措施的效果，以实现碳排放量的持续降低。除了对碳排放的监测和分析，我们还将借助先进的技术和系统，实现碳排放

量的精确计算和追踪。这样可以更好地了解碳排放的来源和分布情况，进一步指导我们对能源使用和排放的管理和调控，以实现园区的低碳化发展目标。总之，通过建立实时高效的数据采集和分析平台，我们可以实现对服务区碳排放的实时监测和精确分析，为制定减排策略和措施提供科学依据，同时也能够推动园区向低碳发展迈进。

“管”有两个层面：一是对园区清洁能源的管理、优化和调度；二是在园区的能耗管理方面做到节能减排，达到降低碳排放的目的。使用物联网技术，监测和控制整个服务区运营过程中照明配电、空调制冷、公共用水、垃圾桶溢出等服务，减少能源消耗。通过新能源管理平台可实现对闲置用电设备的开关控制，减少闲置期的待机能耗。通过零碳操作系统对服务区能源体系的信息收集，来智能化的为服务区管理人员建立一套能源指标监测管理体系，建立健全的管理手段再正向的反馈到服务区的用能设备上，优化设备的用能策略。借助数字化手段打造新能源电站的数字孪生体，构建从绿色发电到高效用电，集管理运营一体化的智慧能源系统。数字化技术赋能能源行业，通过细化场景应用、AI技术加持、海量数据挖掘，促进行业从野蛮扩张向精细化演进，为客户带来更高收益、极致安全、极简运维。利用物联网技术实现服务区水电能耗的智能管理：以H3C物联网平台为核心，LoRa和Zigbee物联网关为基石，各类应用场景传感器为触角，为服务区构建统一的物联网解决方案。

“服”：一是收集园区所有的能源数据、碳排放数据，做到园区碳排放的数据管理，为今后的碳服务碳交易提供支撑；二是提供园区碳排放咨询、碳排放交易服务、碳中和服务等。基于大数据和物联网技术，通过能源流、高速路网信息流、旅客流、天气信息等数据互动，实现能源的供需匹配、达到能源供应精准高效，节能减排。提供服务区动态数据对接能力，发布入服务区停车位、加油、充电桩、餐饮、住宿等信息，提升服务区整体能效及服务水平，提升旅客出行体验。根据电动车辆设备充电需求，采用国际先进的软开关技术，专业设计生产的锂动力电池充电机产品。带CAN通信接口，与电池管理系统BMS和充电后台监控系统实时通信，对锂动力电池的充电进行优化和可靠的保护。自动对进入服务区车辆的车牌、车型、车标等特征信息识别；对进出服务区车流量进行统计，辅助运营管理。自动检测停车场车位状态：空余/占用，实时检测停车场空闲车位数量，通过信息发布屏实时展示，提升司乘人员停车效率和体验。以高点全景相机为基础，其他视频系统通过虚拟标签方式接入，大幅提升指挥中心交互体验；通过视频感知终端高低联动，做到全局与细节兼顾，提高服务区安全管理和应急指挥工作效率。通过车辆结构化分析识别重点车辆（如两客一危），尤其是对违停的危化品车辆进行检测，并告警联动，使工作人员能够及时处理。

三、零碳服务区建设优势

通过清洁能源替代，实现服务区内产业的低碳化发展、能源绿色化转型和资源循环利用。我们提供综合能源服务和综合运营服务，旨在降低服务区的能源成本。对商超、餐饮、加油站、停车场、热水房、公共厕所、公共大厅等设施区进行独立的能耗统计，建立数据统计台账，使得能源消耗情况能够更加清晰地统计到特定区域甚至具体商户。通过利用视频AI等技术，实现服务区紧急事件的高效联动处置，实现跨业务部门协同，以保障服务区的生产与人员安全。同时，利用物联网技术实现对服务区的能源和储能设备进行实时监测和管理，并提供合理化建议以优化服务区的用能状况。通过大数据分析和监测服务区整体运行的关键指标，我们致力于调优服务区的智慧运营。通过零碳智慧服务区操作系统，我们能够实现系统间数据协同和业务联动，从而提升服务区的服务水平。此创新的业务模式不仅能带来新的利润增长点，还能提升园区的运营效率并降低运营成本。降低运营成本还能提高盈利能力并增加区内的税收。我们将全面且智慧化地监管服务区，实现对污染物排放的细粒度监管，从而有效解决服务区环境污染问题。

结语

在“双碳”目标的研究背景下，作为高碳排放的重要领域之一，零碳交通的高质量绿色发展显得尤其重要。实施“双碳”战略，既是我们国家的承诺，更是我们的担当与行动。新华三零碳智慧服务区解决方案通过“源”、“探”、“管”、“服”四大模块，为智慧服务区提供了多方面的支持。首先，通过“源”模块，我们可以为服务区提供清洁的绿色能源，例如太阳能等，以替代传统的高碳能源，减少碳排放。其次，通过“探”模块，我们可以实施全方位的排放检测，监测碳排放情况并配合处理策略，减少碳排放。再次，通过“管”模块，我们可以实现智能化的能耗管理，对能源的使用进行精细化的调控和管理，提高能源利用率，减少能源浪费和碳排放。最后，通过“服”模块，我们可以提供专业化的减排服务，包括提供减排方案、技术咨询和培训等，帮助服务区内的场景化业务应用实现低碳发展。新华三将积极推动全国高速公路零碳智慧服务区建设，助力实现“双碳”目标。

对公路基础设施全生命周期管理的思考

文/邵宁

随着交通运输行业的快速发展，公路是国家经济发展的重要组成部分。公路的建设和运营管理是一个复杂的过程，需要对其进行全生命周期管理，以确保公路长期运行平稳和可靠。全生命周期理念正是为了达到这一目的而应运而生的一种管理思路，它包括规划、设计、建造、运营、养护等阶段，将公路的生命周期从整体上进行管理。

一、公路基础设施全生命周期管理的概念与方法

1. 什么是公路基础设施全生命周期管理

公路基础设施全生命周期管理是从公路基础设施的规划、设计、建设、运营、养护整个运行周期的全生命周期管理，确保公路基础设施在整个运行过程中的高效、安全、可靠、环保、节能。进行全生命周期管理的意义在于一方面提高公路基础设施维护效率，降低运营成本，另一方面提升公路基础设施服务水平和安全系数，进而促进公路基础设施的可持续发展。

2. 如何进行基础设施全生命周期管理

公路基础设施全生命周期管理的关键在于对公路生命周期的每一个环节进行细致的管理与考虑，并且不止考虑当前环节的管理要素，更多的需要从整个生命周期的闭环角度考虑对于其他环节的影响。例如，规划和设计阶段需要考虑公路基础设施的使用功能、运维方案、技术水平、装备运输、环保节能等，运营维护阶段需要制定维修周期、升级计划、设备使用率、管理信息化等。

在整个生命周期的管理环节当中，由于涉及大量贯穿全周期的公路基础设施数据，同时又跨越多个管理环节和业务系统，宜采取信息化的方式，将基础设施数字化、管理流程信息化，继而在后续提供智慧化的决策分析功能。

二、公路基础设施全生命周期管理的不同阶段

1. 规划阶段

该阶段需要对公路的建设计划、项目可行性研究、交通流量预测、选址研究、环境影响

评价、设计标准、投资估算等进行综合分析和考虑。

2. 设计阶段

该阶段需要对公路的结构、设备、养护设施等进行整体设计。采用BIM技术以公路基础设施的各项信息数据作为模型的基础，进行公路基础设施模型的建立，基于BIM技术的公路全要素对象的全生命周期设计技术研究及其应用，是具有重大现实意义的。

3. 建造阶段

该阶段需要贯彻规划和设计要求，采用合适的工程技术，确保公路建设的顺利进行。运用BIM建模对整个建造过程进行量化监管，并对安全生产的过程进行实时监控。在施工过程中预留适当的空间和条件，为后期的养护工作奠定基础。

4. 运营阶段

该阶段需要对公路的正常运行进行有效安排和管理，确保人车安全顺畅、经济可持续。在运营阶段，为了保证公路的正常使用，须对路面、桥梁、设备和养护设施进行实时监测、定期监管、决策评估和运行维护，提高设施的可靠性和稳定性，延长全生命周期。

5. 养护阶段

在养护阶段中，需要对公路进行有效的养护工作，包括路面养护、桥梁养护、路基养护、设备养护等，以确保设施的正常运行和使用寿命的延长。

三、存在的问题及相关建议

基于数字化的方式构建公路基础设施全生命周期管理系统，目前主要存在两个方面的问题：一是数据不完善，由于公路基础设施的所有数据都存在不同的数据系统中，数据整合和统计存在一定困难；二是管理体系不完善，在公路基础设施的不同生命周期阶段与不同管理部门间，管理体系的闭环并不完整，体系化管理水平有待提高。

对于这些瓶颈，可以通过健全标准及保障措施，从而加强数据的收集与分析工作；同时也要重新梳理管理流程、对接相关部门，形成具有系统性、有效性和可持续性的全生命周期管理的体系。为了实现公路基础设施的科学、高效和可持续管理有以下措施建议：

- ◆建立一套标准化、科学化的公路基础设施全生命周期管理机制。
- ◆引进先进设备、技术和管理方法，提升公路基础设施的性能水平。
- ◆加强与前期规划、建设、设计、投资等有关的相关部门的沟通和协作工作，通过信息互通的方式，实现项目管理与数据沟通等。
- ◆推广数字化运维理念，通过BIM、GIS、北斗高精定位、人工智能、大数据、物联网和云计算等技术，实时监控和管理设施运行状态。

四、公路基础设施全生命周期数字化管理解决方案

公路全生命周期管理以“GIS+BIM”一张蓝图为基础，以公路基础设施“规划、设计、建设、运营、养护”全生命周期管理为出发点，建设公路基础设施管理与维护能力、故障应急响应能力、运维科学决策能力、养护科学决策能力几大核心能力，为公路交通的各类设施设备（公路、桥梁、隧道以及关键部位的传感设备）提供标准化业务流程支撑，实现对核心基础设施建设的科学化管理，对在役设施状态的持续性监测以及健康状态的评估等功能，全面提升公路基础设施全要素、全周期数字化水平。

1. 基础设施数字化

目标是将交通基础设施全要素、全周期进行数字化呈现，支撑工程全生命周期数字化应用。关键技术是采用BIM建模技术，将基础设施几何形体、过程特征信息以及行为特征信息进行数字化描述，依托于GIS地图进行搭载呈现。

BIM协同管理平台

BIM管理平台提供公路特征的参数化构件库，满足用户自定义构件库模板，提供完善的全专业构件库资源服务，支撑工程各专业参数化建模。为用户提供多终端、多专业、多用户的协同BIM建模方式，基于完善的参数化构件库资源及参数化构件库编辑器，通过OCR图纸识别工具快速提取二维设计信息，实现公路工程各专业BIM信息模型的快速建立。

BIM平台支撑能力

基于BIM协同管理平台的信息模型可以进行工程量计算，支撑工程量台账编制、计划进度、物资管理等相关应用；可以进行工程划分，形成符合工程质量检验评定标准的单位、分

部及分项工程划分清单，便于辅助进行分项设计及建造监管；可以进行进度实体分解结构划分，为进度过程管理提供结构物类型、工程设计数量、桩号及位置等实例属性信息。

2. 数字化基础设施管理应用

行业数字化监管

建立覆盖项目规划、设计、造价、投资、进度、质量安全监督、建设市场信用的监管体系，提供基础数据共享、省级路网及工程建设政务信息，为行业主管部门提供数字化服务。

企业级管理

按照“纵向贯通，横向融合”、“一数一源、一源多用”的原则，对工程规划、设计、建设、运营、养护各阶段的数据进行聚合、运算和分析，建立标准化的数字监管体系和跟踪指标体系，为各级领导和管理部门提供全面、科学的决策依据，提高监管效率和执行力。

◆项目管理

通过云计算、大数据、物联网、BIM、三维GIS、CA电子签名等技术的综合运用，建立业主单位、施工单位、监理单位等全员共享数字化管理模式，对安全、质量、进度、成本等核心业务进行全过程管理，同步生成竣（交）工信息模型及数字化竣工档案，提高项目管理效率，降低项目管理成本。

◆资产管理

基于二三维一张图，反映公路路产信息，实现公路资产的数字化和可视化。对路基、路面、桥涵、隧道、交安设施等资产开展在线采集工作，实现“一物一档”公路资产信息管理，形成资产清单。优化和盘活公路资产，提高公路资产管理效率和公路资产利用率。

◆养护管理

实现公路养护业务、养护资金、养护决策的全过程管理，规范公路养护管理业务，辅助管理者对养护信息的掌握、对养护作业的全程跟踪管理，提升公路养护业务的信息化管理水平，具体包括：

公路技术状况评定：支持公路资产评定和自动化评分，提供公路技术状况评定结果，支撑养护资源配置。

日常养护：日常巡查和维修保养事项的快速上报、推送和解决，提升作业人员的工作效率。

一张图：支持全方位查询养护设备、养护车辆、巡查情况等养护信息。

养护计划：养护计划制定、实施及完成情况的闭合管理，辅助管理者开展养护工作。

统计分析：实现对公路技术状况、养护信息和养护设备的多维度（年份、养护类型、工程类型等）可视化统计及展现。

◆ 监测管理

通过采用北斗地基增强及物联网技术，对边坡、隧道、桥梁结构状态进行监控与评估，及时预警基础设施的形变和位移。为公路基础设施在特殊气候、交通条件下或运营状况严重异常时触发预警信号，为基础设施维护维修与管理决策提供依据和指导。

五、公路基础设施全生命周期管理的意义

全生命周期管理可以对公路基础设施的状态进行有效的把控，有效地提高设施的运营效率，降低运营成本，减少维修养护费用。全生命周期管理能够在项目实施之前确定统一的标准与规范，充分地运用资源，降低后续管理难度。

全生命周期管理贯穿公路基础设施的规划、设计、建设、运营、养护等环节。优化公路基础设施的运营维护可以提升设施的安全系数，为交通运输提供更加便利和安全的服

数字化路网事件管理系统建设思路

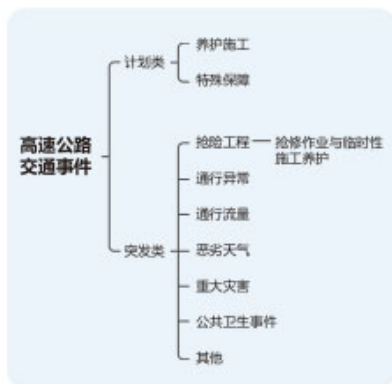
文/邵宁

在高速公路日常运营管理中，针对交通异常事件的检测和处置一直以来都是高速公路监控系统的难点和重点。现有交通事件管理较为粗放，存在权责划分不清、处置效率不高、服务信息不够等痛点，需要建立事件分级分类标准、事件标签标准、事件填报标准和事件处置规范等软科学研究成果，建设数字化路网事件管理系统，按照分级分类的思路实现事件的统筹派发、处置、跟踪与考核，明确各相关部门权责，提升事件处置效率。

一、标准规范建设体系

1. 事件分级分类

高速交通事件分级分类标准是建立数字化路网事件管理系统的关键，也是事件快速处置的基础。通过相关实践经验对高速交通事件分级分类标准研究，初步可以将事件分为计划类、突发类两大类：其中计划类事件包括养护施工、特殊保障等2个子类，并包含54个下级分类；突发类事件包括抢险工程、异常通行、通行流量、恶劣天气、重大灾害、公共卫生事件、其他等7个子类，并包含40个下级分类。



通过高速公路交通事件的时间维度、空间维度等方面，结合事件的特殊属性标签，对事件进行分级定义，针对不同级别的事件，将指定不同的责任人及处置流程。

2. 事件标签规范

对各类高速交通事件准确标注不仅仅是快速识别交通事件的基础，借助准确、丰富的标签系统，我们还可以对事件分级分类模型、派单模型等模型与算法进行持续迭代，进一步提升事件处置效率，因此规范化的高速交通事件标签体系显得尤为重要。

事件标签至少包含事件位置类标签、事件来源类标签、事件时间类标签、特殊车辆标签、事件影响类标签以及管制措施类标签六大类，具体分类如下：

事件位置类标签：发生地点、位置描述、重点地段。

事件来源类标签：设备检测、用户上报、业务人员巡查、其他部门。

事件时间类标签：发生时间、上报时间、续报时间、终报时间、实际结束时间、预计恢复时间、预计通行时间。

特殊车辆标签：危化品（运输货物类型）、客运车辆（荷载人数、实际载客人数）、货运车辆（运输货物类型）。

事件影响类标签：是否影响邻省道路、是否影响相邻路段、是否影响城市交通、影响范围及里程、整体阻断情况、是否占用车道、收费站影响、服务区影响。

管制措施类标签：单幅双向通行、单幅单向通行、单向部分车道封闭、带队通行、限速、限制车型通行、分流、限流、服务区容留。

3. 事件填报规范

高速公路事件来源众多，既有系统上报的事件，也有系统监测人员填报的事件，为确保事件处置的高效与准确，我们需对各个来源的交通事件填报要求进行规范。具体可分为接口上报和人工填报两种方式：

接口上报：接口上报的事件来源于系统对接，在制定事件填报规范时至少应考虑AI视觉监测系统、综合运行监测、业务管理系统等各个系统来源。

人工填报：针对人工填报的事件，考虑到高速公路交通事件多样化、现场复杂多变的特点，针对不同类型、不同级别的交通事件采用统一的填报页面是不合理的。事件填报管理重点是在分级分类定义的基础上，面向管理单位，提供可视化、定制化的填报内容管理，降低人工填报信息的复杂度，提升事件处置效率。

4. 事件处置规范

为规范事件处置流程，应重点分析路段级、区域路网级、省级等各类交通事件的特征特

点，结合各类事件处置过程中积攒的历史经验，形成高速公路事件处置规范，以管理单位业务诉求为出发点，指导运营过程中各类交通事件的精细化分级分类管理，明确处置责任人，规范处置流程、处置时限，为应急指挥调度方面提供依据，同时也为向全国进行交通事件精细化管理推广奠定基础。

二、数字化路网事件管理系统总体架构

纵向上，数字化路网事件管理系统向上将通过与TOCC的对接，实现跨行业转办（交警部门、气象部门以及国土部门等）事件以及上级部门交办事件的及时获取与处置结果的反馈，向下将通过与机电运维系统等多个路段级业务管理系统的对接，实现辖区路网事件的及时获取与处置结果反馈；横向上，数字化路网事件管理系统将实现与路网综合运行监测系统、高速客服系统的对接，同时预留与后期同期建设的省级智慧高速平台的接口。

数字化路网事件管理系统将通过数据中台或者业务系统与外场设备实现数据互通，设备包括但不限于视频监控设备、道路健康监测设备、流量检测器、毫米波雷达以及气象检测器等。

三、数字化路网事件管理业务流程

数字化路网事件管理系统一方面可实现全省交通事件的全量接入、智能识别分类、工单自动派发、事件协同处置、态势评估、仿真推演、自动督办、结果自动报送的闭环管理，另一方面还可以通过AI能力自我优化派单逻辑，从而最终实现派单自动化，提升派单效率，最后还可以打通事件与公众信息服务之间的壁垒，通过基于用户画像的精准出行信息服务系统为出行者提供更及时、更准确的出行服务信息。交通事件将按照如下流程进行处置：

- 数字化路网事件管理系统通过智慧高速平台获取全渠道交通事件信息，实现交通事件信息的汇聚。
- 数字化路网事件管理系统接收交通事件，并按照交通事件分级分类规范对交通事件进行智能识别、分类、分级，按照自进化模型分析结果对事件进行自动派单，当派单不合理时，工作人员可对派单进行修改，同时系统自动学习派单方式，并对派单模型进行优化。
- 系统自动实现工单流转，干系部门或人员可通过数字化路网事件管理系统对事件通过进行快速处置，在处置过程中，针对复杂事件，为提升事件处置效率与准确性，业务管理人员可

对事件态势进行分析评估，同时也可进行仿真推演。当超过工作规范日期或要求时，督办与效能监管人员对工单进行督办，督办可进行分级分类设置。

- ◆针对部分涉及通行或出行者利益的交通事件，干系人需按照基于用户画像的精准出行信息服务系统要求进行信息报送，出行信息服务系统可按照对象、服务方式进行有针对性的信息服务，提升用户获得感。

- ◆事件处置完成后，干系人可对工单进行办结，后续决策分析人员可从事件处置效率、满意度等多个维度对事件处置过程进行分析、复盘，从而不断优化事件处置流程。

- ◆路段、路网以及省厅各级领导可通过系统分级分类及时了解全省高速路网交通事件总体态势、处置进展，一方面及时洞察行业运行风险，另一方面通过对历史事件的分析为行业治理以及政策出台提供支撑。

四、数字化路网事件管理系统功能设计

对照数字化路网事件管理系统的定位、总体架构以及业务流程要求，该系统应面向日常工作人员（事件接报、派单人员、督办与效能监管人员）、决策分析人员、事件的干系方、路段路网省厅各级领导以及管理员提供事件接报、事件分级分类、工单派发、协同处置、信息服务、评估分析、全网事件一张图、系统管理等功能。

1. 事件接报

全高速路网交通事件的统一汇聚是统筹管理的基础，作为交通事件的汇聚入口，事件接报功能一方面需实现事件接入渠道的管理，另一方面还需实现事件填报、修改与删除。

2. 事件分级分类

事件分级分类管理将实现事件的精准识别，是精准派单的基础。对照定位，该模块一方面应严格按照“高速交通事件分级分类标准”要求实现事件分类以及分级的定义；另一方面该模块还需要通过分级分类模型实现事件的自动分类与分级，而为确保分类与分级的准确，此模块还需为派单人员提供分级分类管理功能；最后，为不断提升派单模型的准确性，此模块还需提供事件标签管理功能，从而为机器学习不断提供标注数据。

3. 工单派发

工单正确派发是高效处置的前提，从功能角度看，该模块首先应该能提供处置流程管理功能，包括对派单模型的管理、干系人的管理、时效管理、预警管理、通知渠道管理等；其次应该提供工单管理功能，该功能主要价值在于人工复核，确保工单的正确派发。

4. 协同处置

作为事件处置的核心关键模块，协同处置功能应能为一线人员提供工单处置功能。一线人员可依托该功能实现工单转办或工单信息（事件干系人、处置方式、持续时间、处置结果等）的填报，在事件处置过程中，为确保事件高效处理，该模块还需要为一线人员提供态势评估、历史案例借鉴、仿真推演等能力。

针对督办人员，该模块还需能提供工单督办能力。在派单期，系统可预设该此事件工单的预警时效、督办方式等内容，在工单协同处置期间，系统可自动按照预设信息进行督办，同时也可由督办人员发起其它督办。

5. 信息服务

作为数字化路网事件管理系统的对外接口，信息服务功能模块主要作用在于需要的时候，按照接口要求对外提供由于事件导致并且需告知公众的服务信息。其应包括信息服务模板管理以及信息服务管理两大功能，其中信息服务模板管理主要用于解决不同渠道、不同系统信息发布时的多样化要求，而信息服务管理功能主要用于对需对外提供的服务信息进行管理。

6. 评估分析

对评估分析的功能需求主要体现在四个方面，一是对单个事件处置全流程的评估分析，包括事件处置时效评估、处置流程评估、处置结果评估等；二是基于所有事件以及事件处置结果，对全局事件态势、满意度等方面的评估分析；三是对部分个性化需求的自定义评估分析；四是模拟演练需求。

7. 全网事件一张图

借助大屏展示系统，全网事件一张图功能可完整清晰的呈现当前所有的事件信息、事件发

展态势信息以及预警信息，从而为领导决策与指挥调度提供支撑，系统设计中应预留对接其它路段事件信息的接口，后续可建设成为全省路网的事件一张图。

8. 系统管理

实现用户管理，包括有角色管理与账户管理两大部分，各部分都包括新增、修改、删除等基本功能。

实现对外接口管理，对系统获取事件的对外接口进行管理，包括接口新增、修改以及删除。

五、数字化路网事件管理的意义

数字化路网事件管理系统可实现集团-路段两级事件精细化协同调度管理与应急指挥，该系统通过智慧高速平台全渠道获取交通事件信息，依托人工智能技术实现事件智能识别、分类、工单流转、协同处置与公众服务，实时跟进处置进展，并通过大数据分析实现全过程监管，最终实现事件处置闭环。高效支撑日常监测调度与重大突发事件处置，切实保障高速路网运行稳定畅通。



03

云上机场，数智启航

第26章 机场上云、用云、云数融合思考与实践	161
第27章 构筑机场集团“一朵云”，打造一云统管、资源共享、统一高效的数字底座	168
第28章 聚、治、融、享，高可信数据中台助力智慧机场建设	172
第29章 机场AIGC应用场景探讨	177
第30章 “智慧塔”打造新一代机场飞行区周界安全防护系统	184
第31章 机场物联网解决方案及案例实践	189
第32章 智能网络解决方案打造融合可信、畅通无阻的机场信息化“跑道”	196
第33章 行业专属路由器助力智慧空管建设	202

机场上云、用云、云数融合思考与实践

文/郝亚东

近三年以来，以云计算、大数据、AI、物联网等为代表的新一代信息技术正在拉开智慧民航建设的帷幕。2020年1月，民航局发布《四型机场建设行动纲要》，提出建设“平安、绿色、智慧、人文”机场，使得机场建设从过去的“量优式”发展转变为“质优式”发展，民航行业数字化转型大潮已至。

当前热门的新一代信息技术中，各大机场对云计算的“青睐”尤为突出，云计算已经成为赋能智慧机场建设不可或缺的智能技术底座。通过云计算技术能够大幅提升IT资源利用率，为机场业务提供安全可靠、灵活弹性的运行环境，实现应用和IT资源的统一的运营管理和自动化运维，提升管理和运维效率。云计算的集约化和共享化建设理念，为机场各业务场景的数据打造统一的数据存储底座，使数据在安全合规的前提下跨业务、跨主体、跨网络共享和交换不再困难。

一、对机场云的思考与理解

云计算为机场的生产、管理、服务、商业、能源、交通等各个领域的业务系统提供良好的支撑服务。那么一朵广泛适用于机场的云平台该具备哪些特性呢？新华三基于在云计算领域的深厚积累、全国二十余个机场云项目落地积累的丰富经验，总结机场云四大原则：以全量的应用承载为导向、以多维的安全合规为前提、以完备的容灾备份为保障、以良好的兼容开放为准则。

云计算对于机场的定位可以概括为机场的ICT能力中心，智慧化的基石，具体可拆解为资源承载中心、运营管理中心、运维保障中心、服务集成中心、业务赋能中心，助力机场实现资源集约化、管理统一化、运维简单化、服务标准化、业务灵活化。

1. 资源承载中心，打造云化基础设施

- ◆根据机场各类业务系统对IT资源的需求，按需提供不同规格和性能的服务目录。
- ◆满足机场业务的灾备需求，根据业务灾备等级提供对应的容灾及备份方案。
- ◆持续可扩展的服务目录满足当下及未来至少五年机场的业务发展所需。

2. 运营管理中心，聚焦良好建设效果

- ◆匹配机场组织架构，实现机场各部门、各级组织的统一管理。
- ◆计量计费能力，云平台资源使用情况精准管理和分析。

3. 运维保障中心，构造持续服务平台

- ◆通过云平台对数据中心机房整体硬件设备进行运维管理，简化运维工作量。
- ◆云平台对接机场统一运维中心，实现云内资源、应用的统一监控、自动化运维。

4. 服务集成中心，强化开放对接能力

- ◆云平台实现对大数据平台、人工智能平台融合共生，以云助数、以云赋智。
- ◆云平台对接机场第三方业务系统，如统一认证系统、4A系统等。

5. 业务赋能中心，激发应用创新活力

- ◆提供容器、数据库、中间件、微服务、DevOps等PaaS层服务。
- ◆支撑传统架构应用向云原生应用演进。

二、机场云建设解读



新华三云平台全栈能力构筑智慧机场基石

机场云建设是一个能力持续迭代、功能不断丰富过程，一般来说，机场在建云和用云时有两个行业现状需要充分考虑：第一机场行业属于强安全行业，对系统的稳定可靠更甚于技术先进；第二机场的业务系统大多数为直接购买的商用软件，非机场自研。基于此，机场对云平台的使用大致可以分为三个维度：基础用云、深度用云、云数融合。

基础用云：通过云平台提供基础必备的IaaS层服务，使机场业务系统能上云，云平台作为“资源整合中心”，为机场信息化建设提供底座支撑。

机场云最基础、最核心的使命是为机场全量的应用系统提供必备的计算、存储、网络、安全等IaaS层服务，要保障业务系统能够顺利上得了云。机场业务系统少则几十个，多则一两百个，在这如此繁杂众多业务系统中既有机场信息集成系统、安检信息管理系统、行李处理系统等关键业务系统，又有国界安全防护系统、飞行区管理系统、A-CDM系统等重要业务系统，还有呼叫中心系统、登机桥系统、暖通空调系统支撑服务类业务系统，以及OA系统、财务系统、物业管理系统等经营管理类业务系统。机场的这些业务系统对计算资源和存储资源需求不一，对安全防护要求并非一致，对容灾备份策略需求各异，并且还要保障每个业务系统在安全、稳定、可靠运行的同时在逻辑上具备相对独立的IT资源环境以保证业务系统之间不会互相侵扰，这些方面在机场云整体规划和建设时都需要着重考虑。

◆计算资源区按机场业务类型不同划分部署在不同的资源池，一般划分为生产运行类资源池、经营管理类资源池、测试类资源池、桌面云资源池等，各资源池归属于不同VPC，为机场各类业务系统在云上提供“专属空间”。

◆存储资源区规划分布式存储和集中式存储两种模式，对于数据存储性能、可靠性、IOPS要求高的应用场景（如核心运行类系统、数据库等）一般推荐用集中式存储；对于性能和IOPS要求一般且数据量大的应用场景（如视频监控、停车场管理系统、旅客服务系统、商业管理系统等）一般推荐用分布式存储。

◆机场云安全需要从云平台和云租户两个维度进行规划，机场云通过将提供给租户的安全服务能力与云平台的安全建设深度整合，建立统一的云安全资源池，按需为业务系统提供相应等级的安全防护能力。

◆一般情况下机场云纳管两个数据中心，分别为A域（ITC大楼）和B域（PCR机房），A域作为主生产数据中心，B域作为备生产数据中心。机场业务系统在做容灾规划时既要考虑生产

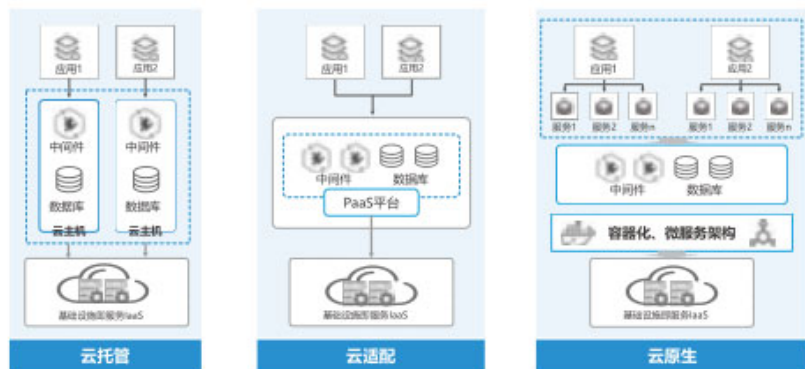
系统的高可靠需求，同时也要兼顾云平台和应用系统的建设成本和技术难度。机场核心业务系统在A域和B域做容灾部署，保障核心业务的高可用性。非核心业务系统做数据级备份，保障关键数据不丢失。

深度用云：构建PaaS服务能力，包括数据库、中间件和应用管理服务能力，构建初步的DevOps开发测试服务，使机场业务系统用好云。机场应用上云模型可以概括为以下三种，这三种模型面向不同场景和业务需求，会出现共生共存的局面，并且会长期存在。

◆云托管：机场业务应用承载的物理机替换成为云计算IaaS资源池里的虚拟机或者裸金属实例，不改变业务应用部署模式和架构。

◆云适配：机场业务应用的中间件&数据库转由PaaS平台上提供服务，通过云平台服务组件完成对业务的高并发、高实时的支撑。数据库和中间件按需申请，实现服务化交付、自动化配置部署、可视化管理和运维。

◆云原生：基于PaaS平台开发云原生应用，原有应用进行微服务和容器化改造，实现模块解耦，弹性伸缩，提高应用上线速度和版本迭代效率，加速业务重构与创新，有效支撑机场智慧化场景应用需求。



目前落地的机场云大多以基础用云为主，部分机场尝试深度用云，如通过云平台按需提供数据库、中间件等服务。基础用云主要提高IT资源利用率、简化数据中心管理和运维、便捷拉通跨应用数据，但并未改变应用的开发、测试、上线、部署等模式，应用难以敏捷开发和迭

代，随着机场智慧类应用的大量涌现和智慧化场景下对应用提出的更高要求，机场的部分应用必然会向云原生架构演进。机场应用系统做云原生改造建议优先从旅客服务类着手，此类为面向互联网的敏态类应用，有高并发、峰值访问、应用快速迭代的诉求，通过云原生改造可以带来如下价值。

◆应用快速迭代

能够快速响应机场业务需求变化，保持技术先进性，实现业务快速创新。

◆高效运维

提供自动化和智能化运维能力，提高运维效率，保障业务连续性、可靠性。

◆资源弹性供给

面对高并发业务场景提供敏捷性弹性资源，提升高并发场景下旅客访问体验。

云数融合：构建云数融合能力，在保证信息安全的基础上随时、随地为机场用户提供所需的数据。通过云平台与数据平台融合共建，云平台海量数据存储和集群化服务的能力助力数据平台实现云上众多的业务系统数据集成、数据治理、数据开发和数据共享等服务，将机场数据资产化。

数据平台是打破机场业务系统数据孤岛的一剂良方，以机场业务为核心驱动，聚焦“数聚、数治、数融、数享”四大能力，其中数聚是基础、数治是保障、数融是手段、数享是目的，通过数据平台四大能力赋能或再造机场智慧运行、智慧安全、智慧商业等各种业务场景，全面助力智慧机场建设。

三、新华三机场云解决方案优势

1. 安全可靠、可用性高

云平台具备完备的高可靠、高可用机制，包括云主机容灾备份、管理平台集群化跨AZ部署、保障业务系统上云后健壮性更强。

云网安一体化设计，云平台和租户的全方位安全防护能力，扫除一切业务系统上云后潜在的安全风险。

2. 轻量化、可定制

针对机场业务规模体量，提供轻量化、定制化方案，云平台管理节点轻量不笨重，节省投资，性价比高。

可根据机场业务需求，提供定制化服务能力，包括页面定制、流程定制、第三方平台对接定制等，打造机场专属私有云。

3. 兼容开放、解耦不绑定

云平台能够与服务器、存储、网络、安全等产品解耦，能够支持业内主流厂商产品，机场可按需选用，后续扩容也可灵活选择，不被厂商绑定，实现“自主创新”。

4. 实践广泛，服务完备

全国落地的机场云平台案例20余个，实践广泛，不仅懂云，也懂机场业务系统；具备长期服务机场行业的专业服务团队，可提供涵盖建云、迁云、用云端到端的服务支持。

四、某国际机场云平台实践

为满足旅客吞吐量快速增长的需求，某国际机场先后进行过多次大规模的改扩建，业务系统不仅数量庞大，而且结构日趋复杂，IT资源利用率低，管理和运维处于割裂状态，缺乏自动化的管理手段，快速反应能力有待提高，这些明显不符合该机场信息化发展需求，最终提出通过建设云平台为信息化发展构筑统一的数字化底座。

新华三提供了一套完整的私有云建设方案，协助机场打造专属的云平台顶层管理系统，这套系统能够向下集成基础设施即服务管理组件（IaaS），并且在后期能够与应用即服务管理组件（PaaS）、桌面云等进行集成，对外提供统一的云服务门户、云租户管理、云环境统一监控及运维、云配置管理、流程管理、统计分析等功能。云管理系统向上提供与机场ITSM、信息安全综合监测分析平台、机场统一身份认证等系统的对接接口，实现系统的整体集成。

机场云平台有效整合了计算、存储、网络等基础资源，实现资源协同，提高业务上线速度，提升运行效率。与此同时，云平台实现对原有虚拟化资源、网络资源的统一纳管，在保护首都机场原有IT资产前提下，有效提高资源集约化水平，降低管理难度。首都机场云平台主要建设内容概括如下：

◆统一管理：H3C CloudOS云平台同时纳管VMware资源池和CAS资源池，划分“生产、办公、测试”三个业务资源池，对资源用量、建设情况进行多指标监控分析，提供高效的统一运营管理工具。

◆业务上云：提供完整的P2V、V2V上云迁移服务，实现业务系统从物理机和VMware迁移至CAS虚拟化，CAS集群虚拟机规模超过500台，验证了新华三云平台大规模集群稳定服务能力。

◆定制化：提供定制化服务，实现统一身份认证、云主机界面改造、主机申请流程等相关功能与机场原有使用习惯匹配，与其他系统深度融合，充分发挥云平台价值。

结语

云计算作为破解机场传统信息化建设发展瓶颈的利器，能够有效支撑机场智慧化发展，构筑机场智慧化发展的基石。随着机场行业对云计算的使用由基础用云向深度用云和云数融合演进，机场将携云而行，实现智慧领航。

新华三作为数字化解决方案领导者，能够为机场客户提供从云平台咨询规划、建设实施、定制化开发、迁移上云等端到端的机场云建设和咨询服务，愿成为机场客户信息化建设、业务创新、数字化转型值得信赖的合作伙伴。

构筑机场集团“一朵云”打造一云统管、资源共享、统一高效的数字底座

文/郝亚东

云计算正在影响机场行业信息化建设进程，颠覆传统的信息化建设模式，铺就机场智慧化基石，为机场的生产、管理、服务、商业、能源、交通等各个领域的业务系统提供良好的支撑服务，是连接机场信息科技部门与业务部门的服务媒介，已广泛在机场行业落地应用。

云计算在机场行业的广泛应用使得机场集团面临着多云共存的局面，集团旗下的成员机场及分/子公司可能会用到多家厂商的云平台产品，这也为集团信息化的统一管理带来了一系列挑战。新华三为机场集团提供“一朵云”整体架构解决方案，通过对云平台的纳管和运营，确保集团和二级单位IT资源的高效利用和统一的服务标准，帮助集团有效规划和提升云服务能力，为成员单位提供更加稳定、高效的云服务支持，进一步增强集团层面对信息化的管控能力。

一、机场集团“一朵云”建设分析



由于前期缺乏集团层面的统一规划，机场集团面临着多云并存局面，导致IT资源无法统一管理、运维无法统一支撑、安全无法统一管控、标准无法统一规范，与机场集团数字化转型战略相悖。机场集团通过构建“一朵云”整体架构，能够有效解决上述问题，通过“一朵云”为

集团总部及二级单位提供一体化的管理运营平台，实现集团在信息化、数字化层面的集约化管理，助力机场集团提质增效，实现数字化转型。

实现机场集团“一朵云”整体架构的支撑在于多云管理平台的建设，常用做法是采用“成熟产品+定制开发”的形式打造机场集团统一云服务平台，通过成熟的多云管理平台产品实现对多云、多数据中心的统一管理，采用平台提供的功能实现资源的申请、运营运维管理；通过定制开发，满足机场集团个性化管理需要，提升用户使用体验，打造机场集团云专属品牌。

机场集团还可以通过“一朵云”量化云服务定价，为分/子公司或其他第三方单位提供有偿云服务。这种应用场景适合于分/子公司对信息化的建设需求不高，且自身的信息化管理运维团队能力薄弱，通过付费形式租用集团统一提供的云资源服务。从集团角度可以实现信息系统的统一部署和高效运维，从而解决分/子公司自身能力薄弱、信息化建设投入产出比低的情况。此种模式将集团的信息科技部门从技术提供者转变为服务提供者，从原来的“成本中心”演进为“盈利中心”，成为机场集团数字化转型的“智慧化运营中心”。

二、新华三机场集团“一朵云”解决方案

新华三凭借在云计算领域的深厚积累和对机场行业的深刻理解，为机场集团提供多云管理平台解决方案，能够管理机场集团存在的多种类型云资源（虚拟化、私有云、公有云），支持纳管主流的云厂商产品，包括VMware、Hyper-V、华为云、阿里云、腾讯云、OpenStack云平台等，可基于资源运行情况进行统计分析，为机场集团提供报表、报告以及自动化运维操作能力，助力机场集团实现集约化管理，在满足充分利用各家云厂商产品优势的同时，实现统一运营运维，形成物理分散、逻辑统一的“一朵云”架构。



新华三为机场集团提供的“一朵云”整体架构解决方案涵盖资源管理，运维管理，运营管理三大能力框架。通过这一整体解决方案，机场集团能够实现更高效的资源分配、精细化的运维管理以及灵活的运营服务，从而提升整体运营效率并降低成本。

资源管理：通过与集团旗下各家机场云平台资源进行对接，从集团层面实现对被纳管的机场云资源进行增删改查等管理工作，便于从集团维度实现更加快速的调度资源，能够对接主流的公有云、私有云和传统物理设备，进行统一的生命周期管理，从集团的多云管理平台中展现云资源分布区域情况、所属机房位置、云资源创建时间、以及业务分组等详细内容。

运营管理：将资源用量及成本进行可视化分析，变成可以运营的服务提供给租户，为管理员提供统一的运营平台。平台的各使用方可以通过工单委派、成本账单、消费明细、大屏展示等功能进行高效的互动。通过成本优化做到账单灵活自定义，做到费用管理、统计分析，资源成本预估。平台以数据可视化的方式，全面展现组织在公有云、私有云以及虚拟化环境等资源池中的各类资源年度总费用及各厂商费用总览，通过横向和纵向的深入成本分析，帮助机场集团了解实际使用情况，进行资源成本分析、并给出资源优化建议。

运维管理：通过对收集到的运维



信息（如告警信息、性能信息等）进行综合分析和呈现，为管理员提供统一的运维平台，通过监控数据与图表趋势清晰地了解资源的运行以及使用情况，并根据监控数据做出对应调整，让用户对资源的使用状况了如指掌。同时可根据监控数据设置告警，如果告警策略触发，平台将自动发送通知信息给告警联系人从而确保异常状态能及时解决。

三、广东机场集团“一朵云”案例实践

截至2023年，广东机场集团（包含分/子公司）存在华为HCS、H3C CloudOS和VMware等多家厂商的云产品，总数量达到了7个，这些云平台分布在集团数据中心和各个分/子公司的数据中心。广东机场集团根据业务发展需要，通过建设多云管理平台实现对集团存在的多套不同品牌的云平台进行集中管理，提升多个云平台纳管、资源管理、运维管理、运营管理能力，实现集团云计算资源的统一管理及资源调度，推动“机场一朵云”的落地建设。

新华三为广东机场集团提供了“一朵云”整体架构建设方案，旨在建立全集团的IT基础设施统一监控和运营平台。该方案涵盖了集团总部云平台、白机机场股份云平台、白云信科祥云平台、揭阳潮汕机场生产云平台、湛江机场生产云平台以及韶关机场云平台等，通过接口对接方式成功纳管集团现有的多家厂商的云平台，提供对云资源的计量计费、运营分析、审批流程管理等功能，实现云资源全生命周期管理。另外，整体架构具备良好的扩展性和演进能力，未来可以根据集团需要横向扩展纳管的云平台类型和数量。

结语

云计算在机场行业充分发挥价值需要遵循“三分靠建设，七分靠管理”原则，机场集团作为管理单位，通过构建“一朵云”整体架构实现面向多种云平台资源的混合管理与编排能力，面向应用与业务提供基于资源运行状况的分析、干预与自动化运行能力，帮助集团更加灵活的调度资源，在确保应用系统性能体验、业务可靠性、业务安全性的前提之下，实现最优成本的系统资源交付和运营模式。相信未来会有越来越多的机场集团通过构建“一朵云”整体架构，实现集团云资源的集约化管控，构建统一的云服务运营体系，支撑机场集团面向未来的数字化转型。

聚、治、融、享，高可信数据中台助力智慧机场建设

文/刘诚

伴随着信息技术水平的不断提升，机场作为综合生态体，也正在享受着技术革新带来的红利，从机场行业发展来看，其正在经历从Airport2.0的敏捷型迈向Airport3.0智慧型机场的过程中，智慧型应用持续不断涌现，数据呈现出爆发式增长，但随之而来的如数据孤岛严重、数据质量低、共享差等数据问题也日益凸显。如何让数据产生价值成为民航业信息化建设一大难题。

一、数据中台是机场突破数据瓶颈迈向智慧型机场的关键

2022年，民航局发布《智慧民航建设路线图》提出要围绕四型机场建设，提升机场协同运行效率，以智慧机场塑造民航业全新未来。政策加持下，民航业迈向“智慧机场3.0”步伐整体提速。随着智慧型应用不断涌现，各应用间联动性差所带来的一系列数据问题，给机场数字化转型造成挑战，其主要体现在：一是，信息孤岛严重，技术迭代更新、管理的渐次成熟造成机场烟囱式的IT建设，使机场内外部的航班生产、离港、旅客服务等系统各自为战，给多业态、跨领域数据共享造成困难；二是，数据接入标准混乱且质量差，缺乏统一的标准参考，加上数据质量参差不齐，导致大量数据资产没有产生真正的价值，一方面增加了数据开发和处理的难度，另一方面以错误数据做分析挖掘，其结果对指导管理决策意义甚微；三是，数据分析需求响应慢且成本高，机场管理者对运行场面态势掌控要求较高，尤其是突发事件如雷暴天气启动何种响应机制等，基于当前的数据分析模式无法快速响应即时诉求，且开发成本高，无法满足用户诉求；四是，缺乏强大的数据工具支撑，机场缺乏数据接入、数据融合、数据治理、数据加工和预测决策工具，影响了数据数据处理和高质量共享。



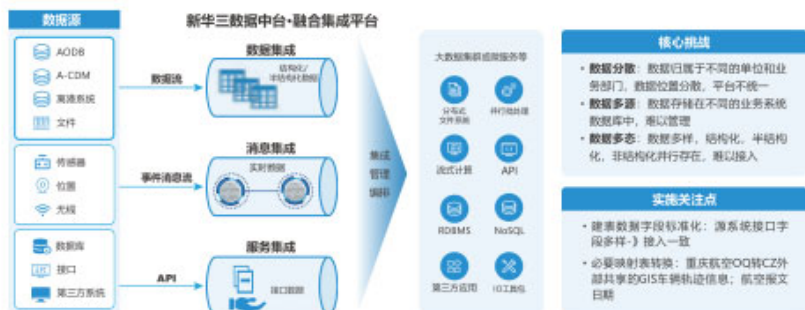
上述这些问题是机场迈向智慧型机场3.0期间数据赋能发展出现的瓶颈，如何解决这些问题，数据中台提供了一个较好的思路。作为大数据技术的融合体，数据中台可以实现统一的数据纳管，对数据标准、质量进行流程化管理，沉淀数据资产，全面对外快速响应赋能，实现服务业务全流程管理，是机场突破数据赋能瓶颈迈向智慧型机场重要支撑。

二、聚焦“聚、治、融、享”，打造高可信数据中台体系

基于对行业痛点的洞察和对技术的理解，新华三结合数据中台在各行业落地经验，推出了智慧机场数据中台整体解决方案。方案以业务为核心驱动，聚焦“数聚、数治、数融、数享”四大能力，采用一站式、轻量化、松耦合的数据中台工具，围绕数据“接、存、管、用”打造数据融合集成和运营平台，为机场提供稳定可靠的数据支撑底座，实现以数据中台为核心的业务数据化和数据资产化，系统化构建出高可信的数据中台体系，全面助力智慧机场建设。

1. 数聚：自动汇聚、统一纳管

由于机场大量的数据分散在不同业务系统和数据库中，而不同系统建设时间不同，技术应用跨度大，这就造成系统接口种类繁多、差异性较大。新华三在梳理数据源和业务基础上，通过融合集成平台为机场各类业务系统，提供服务、消息、数据集成，对业务应用屏蔽底层系统差异，提供统一服务支撑。平台支持海量多源异构数据接入，将机场自身生产数据（航班生产、旅客服务等）、行业数据（空管数据、航司数据、局方数据等）、外部数据（气象局、OTA等提供的数据）进行自动化汇聚，实现数据全面接入、融合与纳管，相当于将数据统一纳入数据池，为下一阶段的数据治理打下坚实基础。



数据：打破数据孤岛，实现数据全面接入

2. 数治：强化治理，标本兼治

数据治理是让数据具备高可信的前提。数据标准治理是数据治理的核心，数据标准不统一，也使得机场工作人员在不同业务系统中有时难以“找到”或“看懂”数据。机场系统建设繁杂，对于相同意思的字段如航班号，可能在不同系统里采用不同名称、定义及属性规范，这就造成数据标准不一，影响数据后续融合和加工。新华三依托数据中台灵活便捷的组件工具，参照《中国民航航班运行共享协议》等行业标准规范，依据定义标准建立规范的数据库，助力机场建设数据标准。

此外，关注业务侧的数据治理是“数治”能力实践的重点。基于对业务的理解，新华三提出业务侧数据治理的思路，即构建基于业务事实发生为基础的时空逻辑检核、辅以经验及第三方数据加以佐证判断检核。前者重点围绕业务流程时间和业务过程空间的正确性对数据进行检核。以航空器到港时间流程为例，正常情况：上轮挡时间 < 靠桥开始时间 < 开始下客时间，但在实际情况中，流程时间的采集可能受人为、系统接收延时、数据解析有误等情况影响，造成数据存在问题，因此通过时序检核暴露数据问题；后者则重点以第三方数据为参照验证机场数据的准确性。以飞机注册号等主数据为例，可以利用外部平台如民航局清算中心基础库平台、数字民航（民航吞吐量统计软件）等第三方公信平台主数据参数，验证机场主数据是否完整。

整体思路：构建基于业务事实发生为基础的时空逻辑检核，辅以经验及第三方数据加以佐证判断检核



数治：业务侧数据治理思路

3. 数融：响应细颗粒多维度的数据分析诉求

业务场景复杂、数据量庞大、数据结构繁杂使得数据开发难度陡然加大。为了解决这一问题，新华三针对标准数据进行指标关联，基于组件进行深层次挖掘，构建常规性查询统计、

吞吐量类、预决策类分析等通用主题库和业务专题库，打造细颗粒、多维度的业务专题分析，使运行类业务数据可细化到时间、航班性质、航线等信息，从而帮助数据开发人员多维度分析，实现数据一数一源等管理。



数融：打造细颗粒、多维度的业务专题分析

4. 数享：构建数据资产



数享：精细化数据共享，全面反哺业务创新

针对机场存在的数据资产管理混乱、无法提供对外接口的问题，新华三通过零编码API、简洁接入、安全管控的方式，就旅客、物流、安保、航班不同主题库形成多服务集成，类似于打造了一个数据资产“超市”，机场的其他部门或不同应用只要通过统一接口便可申请数据进行调用、处理和共享，为数据出售、数据资产增值和交换奠定基础。

除内部共享外，还能实现机场数据与业态公司、航空公司、民航局等外部单位精细化数据共享，从而全面反哺业务创新，赋能机场生产系统、分析应用及BI报表分析等，包括飞位占用预测、机场运行态势监测、人员聚集分析等，同时大屏、驾驶舱、PC/移动端等都能获得多元化、可视化呈现，如此一来，通过数据治理、数据融合后打造的机场数据资源管理中心，能为上层业务联动、业务创新提供数据支撑，实现数据对外高质量共享。

综上所述，该方案从梳理数据源入手，以集成平台汇聚各类业务数据，以运营平台来创建数据标准，提高数据质量实现数据治理，最后形成数据服务集市实现数据统一管理和精细化对外共享。四大能力中数聚是基础，主要解决机场内部信息“数据孤岛”问题，数治解决数据质量差问题，数融则是贯穿于所有过程，解决开发者多维开发的问题，数享是基于数融，破解机场外部信息“孤岛”。四大能力共同构成了新华三机场数据中台体系，助力机场实现以业务为驱动的精化管理，全面提升机场运行效率。



机场AIGC应用场景探讨

文/刘诚

在当前数字世界和物理世界加速融合的大背景下，AIGC人工智能生成内容正在悄然引导着一场深刻的变革，重塑甚至颠覆数字内容的生产方式和消费模式，将极大地丰富人们的数字生活，是未来全面迈向数字文明新时代不可或缺的支持力量。机场行业作为连接全球的桥梁，受益于AI技术的不断进化，正经历着一系列的变革。本文将简要阐述AIGC如何赋能机场行业，引领科技发展，驱动创新升级。

一、AIGC正在成为数字科技的新变量

随着人工智能和大数据技术的不断发展，AIGC正在改变数字科技领域的发展格局。AIGC是指利用人工智能技术生成内容的能力，它可以通过学习大量数据和知识，生成与人类创作相似甚至超越人类水平的文本、图像、音频、视频等内容。它是人工智能领域发展的新里程碑，能够加速内容生产，提高创作效率，降低创作成本，为人类提供更加便捷、高效、准确的内容生成服务。

AI加持，数字内容生产力大跃迁



AIGC正在成为数字科技的新变量

AIGC已经广泛应用于各个领域，包括文学创作、新闻报道、图片生成、视频制作、艺术创作、音乐创作等。AIGC的出现极大地改变了人们的生活和工作方式，为人类带来了便利和创新。AIGC作为一种全新的技术，正在成为推动数字科技发展的新变量，促进生产力大跃迁，赋能各行各业创新发展。

二、AIGC+机场，探索智慧机场发展的新方向

在数智时代，新技术以滚滚洪流之势不断塑造着各行各业的新格局与新未来。机场作为客流与货流的“交汇地”的大型生态综合体，也正在依托科技力量，着力实现发展方式从规模速度型向质量效率型转变，发展动力从要素投入驱动向创新驱动转变，在朝着服务自助化、运营社区化、功能多元化的方向发展。近些年，国内各机场纷纷围绕智慧发展，大力开展数字化、信息化工作。以科技赋能智慧机场建设实践不胜枚举，而AIGC作为科技新宠，凭借其智能生成内容的特性，也正在为机场行业带来新的变革。



AIGC赋能机场行业，助推细分场景智慧升级

机场业务场景与AIGC结合点众多，如在旅客服务方面，可以提供旅客问询、智能客服大模型服务；在运营管理方面，可以提供面向员工的百事通问、办公文档编写、管理流程助手等；在安全生成方面，可以提供安全运营管理、应急管理、机务维修等大模型。综合来看，AIGC可以助力机场管理实现效率提升，降本增效。以下将以智能客服、安全管理、系统运维三个应用探索方向为例，浅析AIGC如何赋能机场行业智慧发展。

1. 应用方向探索一：智能客服

随着经济的复苏，旅客对于出行的期望和需求正在不断变化，商务游、家庭游、银发族、背包客等旅客群体对机场的客户服务提出了新的挑战。而基于AIGC的智能客服应用，则提供了良好的解决方案。这也是AIGC发挥其大语言模型天然优势的最常见场景，也在其他行业有很好的落地经验。

智能客服或称AI客服，能够为客户提供即时响应的全天候咨询服务。智能客服的一个重要优点是其自我学习的能力。通过机器学习，可以从每次与用户的交互中学习和改进，使其服务质量不断提高。这种自我优化的能力使得智能客服能够提供个性化的客户体验，满足各种各样的用户需求。



应用场景 | 旅客问询-问询智能化，解锁出行新姿势

可以将AIGC部署在的航站楼服务终端设备或者旅客的App终端助手，以旅客自助问询形式，解决旅客问题，提高机场内的信息传递效率，提升乘客的出行体验。对于旅客来讲，一方面减少社恐症状的发作，旅客的安全隐私得到保护。另一方面基于自助化服务，旅客不会出现埋怨人工态度不佳的现象。此外，答复时效性更高，旅客可以随时查随时得到结果。对于机场来讲，大模型可以有效减少客服人力成本，同时在专业答复上，大模型比人工答复规则、制度信息更准确，在既定规则内更能快速给出最优答案。基于AIGC的旅客智能问询，可以为旅客提供以下服务：

- ◆ 7*24小时服务：理解乘客问题，并在规则规范下给出合理的咨询服务。
- ◆ 多语言支持：满足来自不同国家和地区的乘客需求。
- ◆ 个性化服务：给出机场休闲娱乐最佳方案，提供优惠营销，物品丢失招领。
- ◆ 实时更新信息展示：获取航班最新信息：登机口、步行时间、航班动态等。
- ◆ 无障碍服务：支持屏幕阅读器、语音合成，让视障人士方便获取信息。
- ◆ 安全与隐私保护：确保乘客的个人信息和隐私得到充分保护，防止数据泄露。

2. 应用方向探索二：安全管理

安全是民航业生命线。机场作为民航业正常运行的重要载体，其安全管理对于航班正常运行、旅客安全至关重要。机场传统安全管理，基本按照事前、事中、事后管理应对。在管理上也面临以下痛点：

- ◆ 事前管理靠预案，应急事件种类繁多，但应急培训及教育形式单一，预案及案例可读性有待提高。
- ◆ 事中以执行预案+信息协同为主，由于事件差异性较大，信息更新及态势判别较缓，再加上应急处置流程复杂，一些经验尚浅的工作人员可能无法合理及时的采取应对措施，导致处置缓慢。
- ◆ 事后靠人工总结分析，处置报告编写复杂，需要描述基本情况，分析事件原因，总结应急经验，提出改进建议，依靠人工难免出现无法全面准确反映安全事件的现象。



应用场景 | 安全管理-管理高效协同，效率显著提升

基于AIGC的机场安全管理则能够高效地协同处理安全事件，让应急管理协同高效，让日常安全管理事半功倍。以应急管理为例：

- ◆ 在事件发生时，基于人工智能算法，对机场内的监控视频终端、传感器和其他设备进行实时监测和分析，以识别潜在的紧急情况，如火灾、异常聚集等。当发现异常情况时，系统可以自动触发警报和通知，以便机场安全人员能够及时采取行动。

- 在事件判定过程中，AIGC可以利用预训练的知识和数据分析能力，为处理人员提供实时的决策支持。管理部门如运管委，可以通过AIGC辅助判断事件等级，是否启动预案，并获得关于应急处置策略、资源调配、人员安排等方面的建议，甚至未列入预案事件，AIGC可以自动生成可靠决策，帮助处理人员做出准确、全面的决策。

- 在预案下达分发环节，AIGC可以基于各部门职责，匹配预案并分发至职责部门，让各执行部门工作界限清晰，责任主体有效落实。

- 在预案执行过程中，AIGC可以作为协同工具，与处理人员进行实时的对话和沟通。通过与AIGC进行交互，处理人员可以共享信息、讨论问题，并协同制定应急处理方案。AIGC可以提供智能化的问答、推荐和反馈，促进团队之间的合作和协调，提高应急响应的效率和准确性，辅助一线员工了解进展，动态调整处置内容。

- 在事后总结时，AIGC可以自动分析和整合与事件处置相关的数据和信息，并生成详细的处置报告。它可以从多个数据源获取必要的信息，包括事件描述、相关人员、处理过程、采取的措施和结果等。通过自动化报告生成，AIGC可以大大减少处理人员手动整理和撰写报告的工作量，提高效率和准确性。

除应急管理协助外，AIGC在日常安全管理中也将成为不可或缺的助手。大模型可以基于历史数据、规章制度、管理条例、部门职责等辅助制定预案，更准确地评估风险、优化资源配置、制定应急计划。此外，AIGC可以用于自动化整理、管理和更新法律法规、作业手册、处置规则和各种预案等文档。通过对这些文档进行自然语言处理和语义分析，AIGC能够构建一个结构化的知识库，并根据需要提供相关信息。通过与AIGC进行交互，快速获得所需的法规、手册和预案内容，提高查找速度和准确性。

3. 应用方向探索三：运维管理

系统运维向来是机场信息部门工作的重点和难点。随着信息化进程的推进，机场信息部门需要确保整个组织运行支持的管理信息系统的稳定性和可用性。系统运维管理不仅涉及到IT设备的维护和管理，还涉及到各种业务系统的正常运行。这些系统包括航班运营、旅客服务、安全监控、资源管理等方面，每个方面都需要进行精细的运维管理。但随着业务系统的不断增加，系统运维也面临着以下诸多痛点：

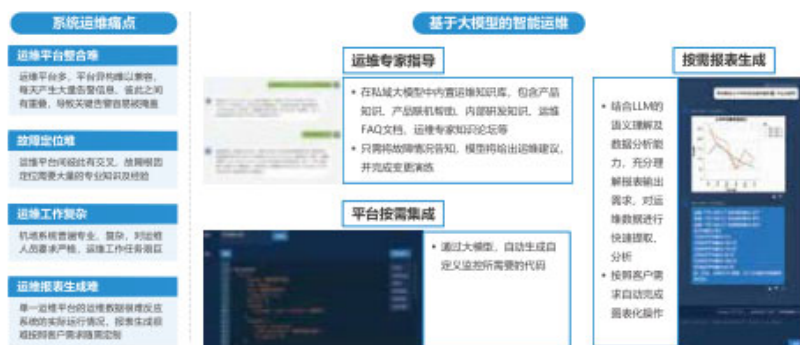
- 监控和告警不及时，传统的监控和告警方式往往无法及时发现系统异常情况，导致故障处理不及时，影响系统可用性和稳定性。

- 运维平台整合难，运维平台多，平台异构难以兼容，每天产生大量告警信息，彼此之间有重叠，导致关键告警容易被掩盖。

- 故障定位难，运维平台间彼此有交叉，故障根源定位需要大量的专业知识及经验。人工分析和诊断系统故障往往效率低下，而且容易出现误判和错误，影响故障处理的准确性和及时性。

- 运维工作复杂，机场系统普遍专业、复杂，对运维人员要求严格，运维工作任务艰巨。传统运维方式自动化程度较低，需要人工干预的环节较多，导致运维效率低下，成本较高。

- 运维报表生成难，单一运维平台的运维数据很难反应系统的实际运行情况，报表生成很难按照客户需求定制。



应用场景 | 智能运维-专家随行，报表随需，人人都是老师傅

而AIGC加持下的系统运维可以帮助企业提高IT运维的效率和效果，降低运维成本，提高系统的可用性和稳定性，形成运维专家随行，报表随需，让每个运维人员都是老师傅，从容应对运维事件。综合来看，AIGC可以为客户提供以下高效支持：

- 运维专家7*24小时指导，AIGC通过学习运维产品知识、产品联机帮助、内部研发知识、运维FAQ文档、运维专家知识论坛等，构建运维知识库，面向客户提供7*24小时专家指导，针对客户问题快速提出运维建议，客户只需将故障情况告知，模型将给出正确的运维建议，并完成变更演练。

◆平台按需集成，AIGC技术可以用于自动化监控系统的运行状态，及时发现异常情况，并生成告警信息，同时协助快速呈现平台预警展示，减轻人工监控的负担，提高运维效率。

◆智能分析和诊断，AIGC技术可以对系统日志、性能数据等进行智能分析，帮助运维人员快速诊断系统问题，并给出相应的解决方案。通过智能分析和诊断，可以降低运维成本，提高系统的可用性和稳定性。

◆自动化修复和恢复，AIGC技术可以根据预设的规则和策略，自动修复一些常见的系统故障，或者在发生故障时自动恢复系统的正常运行。通过自动化修复和恢复，可以提高系统的可用性和稳定性，降低人工干预的频率。

◆报表按需生成，AIGC技术可以结合LLM（大语言模型）的语义理解及数据分析能力，充分理解报表输出需求，对运维数据进行快速提取、分析，并按照客户需求自动完成图表化操作。

以上内容是AIGC技术赋能机场业务创新的众多场景之一。机场行业作为一个高度复杂和动态的领域，对于创新的需求和挑战永无止境。相信未来，随着科技的不断发展，AIGC在机场行业的应用将会越来越广泛，将为机场带来诸多优势和机遇，为旅客提供更优质的服务体验，为机场运营管理提质增效，同时也将推动机场行业的持续创新和发展。

三、聚力同行，新华三以科技力量助力机场行业AIGC建设大放异彩

创新引领助力智慧机场，新华三始终在路上。新华三作为国内较早投入AI领域的企业，有着长期的技术积累与实践经验。新华三贯彻AI in ALL战略，将AI融入到新华三全线软硬件产品组合，实现全栈全场景技术覆盖，同时将AI的能力融入端到端的解决方案中，从使能平台、数据平台、算力平台着手，全面满足用户的业务场景化需求，帮助机场客户快速构建行业专注、区域专属、数据专有、价值专享的行业私域大模型，以伙伴式服务，助力机场行业智能化升级。

“智慧墙”打造新一代机场飞行区周界安全防护系统

文/郝亚东

周界安全防护入侵探测系统是对重点区域周界进行探测、报警、确认的安全防护装备，它就像一道无形的防护墙，广泛应用于机场飞行区的外围防线，防范非法入侵，保卫机场周界安全。


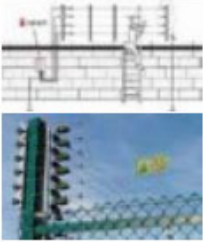
机场传统周界安全防护系统往往存在着漏报风险及误报率高等问题，存在严重的安全隐患，并且误报率居高不下，一天的误报次数成百上千，机场安保部门使用体验极其不佳。针对传统周界安全防护存在的弊端，新华三联合生态伙伴创新式构建了“智慧墙”入侵探测与视频智能复核深度融合的新一代周界安全防护系统，能够实现零漏报、低误报、报警智能判定、灵活运维等效果，助力机场实现现代化周界安全防护。

一、传统周界安全防护技术流派对比及适用场景分析

传统的周界安全防护多数采用振动传感类或射类防御技术，如振动光纤、振动电缆、红外对射、微波对射、张力围栏、电子围栏等，因入侵者触碰前端探测器或载体产生形变振动，或遮挡对射信号传输路线而产生报警。

通过对几种传统周界安全防护技术流派对比，可以看出其适用场景、功能特性各有千秋。

类型	装备图片	优点	缺点
振动光纤		可隐蔽安装，不受地形限制，可曲折、转角，适合于长距离部署	易受外界的影响，风雨天气及行人路过易产生震动导致误报；系统需有人值守；后期维护成本高
微波雷达对射		小巧美观，适用于开阔地面场所，不需要实体围界作为载体；不易受天气变化影响	地形适应能力差，不适用于不规则周界及高低起伏地面；易受雷达干扰；微波发射角度偏小，易被绕过防区突防；发射设备功率高、易老化

类型	装备图片	优点	缺点
张力围栏		实体阻隔，对入侵行为有一定的威慑与阻挡作用；接触报警，不受外界振动干扰	对冷热变化敏感，气温大幅变化时，前端钢丝因热胀冷缩发生形变，易引起误报；对工程施工与校正要求严格，造价较高
脉冲电子围栏		环境适应性强；实体阻隔，对入侵行为有一定的威慑与阻挡作用；可直接进行非致命电子打击有效击退非法入侵	误触电子围栏会产生脉冲电压，虽对人体无伤害，但会有触电般的痛麻感，不宜在人员复杂、孩童较多的敏感地区使用；可能产生电火花，不适用于易燃易爆环境；通过绝缘装备恶意入侵时易被突防

传统周界安全防护技术流派对比表

从对比表中可以看到，传统周界安全防护装备易受地形、地势、气象、植被等客观环境影响，发生漏报或无法有效过滤误报警等情况，还可能存在易被蓄意突防，无法发挥全面探测效果，此外还存在对施工条件要求较高，实施难度较大等问题。

二、新一代周界安全防护技术引领行业发展

针对市场新需求、新特点，周界安全防护技术需要突破传统定式，进一步提升工作效率，结合智能探测过滤能力与图像结构化自动识别算法的入侵探测系统，将是未来安全防护产业技术发展的重点方向。新一代周界安全防护应具备如下四大特性：

- **抗干扰性强，准备率高：**需要能够突破传统安全防护探测技术开关量报警局限，结合大数据智能分析技术，进行相关数据分析及算法模型计算，有效过滤各种环境干扰，整体提升系统抗干扰及误报过滤能力。

- **系统可靠性高：**需要能够解决传统探测技术易被跨越突防的致命漏洞，对入侵位置进行更加精准的定位。

- **实用性强：**需要能够互联互通，实现融合感知与协同探测，且便于安装管理，有效提升工作效率，减少资源消耗，节约设备维护运营期间的人力、时间、资金成本。

- **安全可控：**需要能够满足机场自主可靠、兼顾更高保密要求的新型技术方案。

三、新华三“智慧墙”新一代周界安全防护解决方案

针对机场传统周界安全防护存在的业务痛点，新华三联合生态伙伴创新式构建了智慧墙入侵探测与视频智能复核结合的新一代周界安全防护解决方案，能够实现零漏报、低误报、报警智能判定、灵活运维等效果，助力机场实现现代化周界安全防护的可靠性、安全性、实用性要求。（注：文中提及摄像机等监控设备非新华三技术有限公司提供）

“智慧墙”周界安全防护方案将智慧墙入侵探测与视频复核监控深度融合联动，构建了一种全新的周界安全防护技能，由智能探测线缆与视频监控设备组成。智能探测线缆内置大量微型自适应微波收发芯片，具备无线射频收发和有线信号传输功能，能够形成密度极高、相互交叠的分布式多发多收自适应透地微波阵列，结合空时信号处理技术与机器学习技术，在满足入侵探测要求的基础上，有效消除了自然环境干扰对系统的影响，具有更高的准确率和环境适用性。智能视频监控是通过应用AI视图分析技术，对入侵者进行智能检测识别，并产生报警，从而实现对周界防范。相比传统红外、电子围栏等周界防范技术实现了功能性防范技术向智能化防范技术的跨越，具备更加强大的防范扩展能力，更加便捷的系统部署能力，更加直观、形象化的应用体验。



“智慧墙”由前端探测、网络传输、AI分析与训练、监控平台、联动控制五部分组成，具备入侵报警、目标定位、身份识别、误报警智能过滤、自监控管理、高效联动等系统功能。基本弥补了传统周界安全防护技术的弱项，实现了以下六个方面功能提升：

◆提升报警准确率

“智慧墙”克服传统探测手段单一、误报率高、安全性差的缺点，采用主动探测模式，内嵌大量微型自适应微波收发芯片的智能探测线缆组成高密度排列、相互交叠、连续、均匀分布式多发多收自适应微波阵列，形成“无形的柱状墙”，对防御区域的立体空间进行全向探测。探测空间无死角、无盲区，不仅能防止非接触跨越突防，系统还能通过数据分析和多点扰动结果联合计算，对入侵位置进行精确定位，定位精度最高可以达到5米。

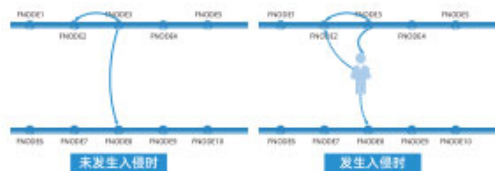


图2 无线传感技术示意图

◆引入AI算法智能过滤误报警

“智慧墙”集成了基于神经网络的AI算法，能够更加智能地对前端探测系统采集的信号强度、波形图像、传感数据等丰富信息进行联合分析、干扰判定，并将各种误报样本转化为标准模型，更新至数据库，如此持续识别、更新，循环往复，使系统具备不断自我学习和更新能力，有效降低干扰叠加，过滤风雨与小动物等的影响。

◆提升灵活运管水平

“智慧墙”向上可对接综合平台，与视频监控、出入口控制、人员管理等安全防护子系统高效联动；向下可联动视频感知终端、补光灯、警报器等终端设备，对围界进行全天候动态智能感知，不仅能够快速准确锁定入侵行为，还能有效降低虚警率和漏警率。此外，还具备防区灵活设置、身份识别管理等功能，可自动识别配带标识卡人员的授权信息，正常出入不触发报

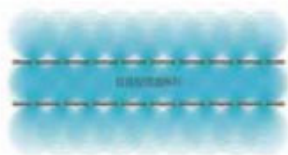


图1 自适应微波阵列示意图



图3 目标定位技术示意图

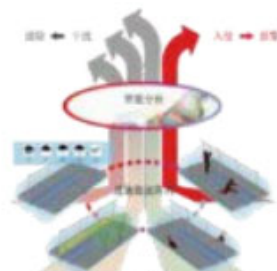


图4 智能过滤技术示意图

警，仅自动形成电子记录，实现全程数据可追溯。

◆安装更便捷

“智慧墙”具备地形跟随能力，面对复杂的户外环境，智能探测线缆能够克服弯曲、交叉、起伏、遮挡等地形变化，更好地适应各种复杂地形变化和建筑结构，且无需根据季节、天气变化对已安装设备进行调整。前端设备防护等级达到IP65以上，可适用于室外恶劣场景；线缆连接采用航空插头冷对接方式，无需专业工具即可完成。

◆维护更简单

“智慧墙”采用冗余设计，具备高抗风险容限，前端局部探测器的损坏可由其它探测器自动弥补漏洞，不影响系统正常工作。系统还具备自检功能，可实时监测运行状态，并支持远程诊断、快速恢复和更新升级。支持抗雷击特性，尤其在机场行业能够满足雨雪雷击等恶劣环境下的可靠性和可用性。

四、机场智慧墙项目实践

“智慧墙”目前已经成功应用于机场飞行区周界安全防护入侵探测场景，发挥及时、严密、立体、无缝的周界防护作用。

某国际机场原有周界报警系统使用振动光缆、张力铁丝和泄露电缆，误报、漏报率较高。“智慧墙”系统在此机场12公里的围界进行了布防，正式平稳运行多年，成功克服当地大风，雨雪的考验，验证了系统在恶劣环境下的可用性。

项目共计部署23.6km智能探测线缆，27台智慧墙分站，主体围界为钢板网，采用双线支出绑网安装，能够有效对非法入侵进行告警，降低误报率，保障机场飞行区域安全。

目前，新华三“智慧墙”系统已经在国内多个大型国际机场落地应用。未来，新华三将持续产品解决方案创新研发，全面服务国内机场安全防护系统，为机场周界安全保驾护航。



图5 机场应用实景

机场物联网解决方案及案例实践

文/郝亚东

智慧机场是建立安全高效、功能完善的机场体系的必经之路，是机场信息化水平的具体体现。《四型机场建设导则》提到智慧机场是生产要素全面物联、数据共享、协同高效、智能运行的机场，是利用全新的数字技术，使机场具备感知-分析-反馈能力，生产要素全面物联是智慧机场的基础和主要任务。物联网是建设智慧机场的重要技术支撑，能够有效带动和提升机场的信息化和智能化水平，进一步提高机场的管理能力和效率，提升旅客出行体验。

新华三致力于为机场提供一站式物联网解决方案，首创“云网融合”基础设施架构，依托“一平台、一网络”，实现机场所有物联终端设备统一网络接入、统一平台管理，为机场提供端到端的场景化解决方案，涵盖机场动力设备管理、井盖管理、垃圾桶管理、能耗管理、人员管理、智能卫生间、乘客导航服务、智能门锁、资产管理等。

一、传统机场物联网建设模式分析

国内众多机场都在积极探索物联网技术在机场的应用，尽管在一些中大型机场已经有落地，但仍存在一定的局限性，尚未实现广泛应用，这主要与传统的机场物联网建设思路有关。传统的物联网建设是机场各业务部门基于自身业务需求自己搭建“专用”的物联网系统，从机场来讲往往缺乏统一的物联网规划，此种建设模式存在如下弊端：

- ◆独立建设的物联网系统，是由各业务部门申请资金建设，无法做到统一管理，物联数据没有统一存储，形成数据孤岛，系统资源各自封闭，且后期各业务部门没有足够的技术支持能力，也无法对外提供数据服务。

- ◆随着智慧机场建设的持续深入，各物联网系统间涉及全场景联动需求，由于之前建设的物联系统相互独立，甚至可能涉及多厂商，各类厂商对外提供服务标准不一，使全场景联动需要多厂商对接、开发技术难度大、重复工作量大，往往投资大，而实际场景联动效果差，运维成本居高不下。

- ◆由于独立物联系统建设时，只需要聚焦单一应用场景，选用物联网协议可能涉及LoRa、

UWB、NB等，数据格式不一，上层的应用系统往往基于单一场景、单一数据格式进行定制化开发，各应用场景的定制化开发工作量无法复用造成浪费。

- ◆物联网在机场的场景价值未能充分挖掘发挥出来，甚至被贴上“投资收益低”的标签，多数物联网应用场景局限于只能“看”，无法实现管理联动，对机场的运营和管理提升有限。

二、新华三机场物联网解决方案

为消除传统的物联网建设模式存在的弊端，新华三业界首创“云网融合”架构的机场物联网整体解决方案，依托“一平台、一网络”，实现机场所有物联终端设备统一网络接入、统一平台管理。一平台是指：新华三绿洲物联网平台，能够满足机场全域物联网设备接入和数据采集，并提供标准数据开放给不同机场业务系统，绿洲物联网平台除具备通用标准功能模块外，还提供“网络管理子系统”，支持机场全域物联网的网络设备进行集中管理和智能运维；一网络是指：以Wi-Fi 6网络为基础，灵活拓展LoRa/蓝牙/UWB网络，满足各类终端和设施联网需求。新华三IoT物联网网关可灵活配置LoRa/ZigBee/RFID/蓝牙/UWB等多种物联网通信能力的插卡，灵活应对机场物联网网络差异化覆盖需求。

基于“云网融合”的机场物联网基础设施，新华三深入机场业务场景需求，提供包括无动力设备管理、井盖管理、垃圾桶管理、能耗管理、人员管理、智能卫生间、乘客导航服务、智能门锁、资产管理等物联网整体解决方案。



图1 机场物联网解决方案架构图

1. 一个平台：破解机场物联网数据孤岛

通过构建物联网平台，将机场所有物联终端设备进行统一管理，提供从广泛协议适配、终端快速对接到机场业务系统集成等全方面能力。

在协议适配方面，绿洲物联网平台支持低功耗广域（LoRa/NB-IoT）、短距无线（RFID/蓝牙/Zigbee）和MQTT等主流通信协议，并可适配第三方平台接口。

在终端对接方面，支持全图形化配置方式对接第三方终端，可适配终端消息封装格式，只需通过简单操作即可轻松接入第三方终端。

在系统对接方面，基于HES蜂巢边缘系统边缘侧软件可快速完成空调、能源管理等其他业务系统数据接入并实现业务联动。

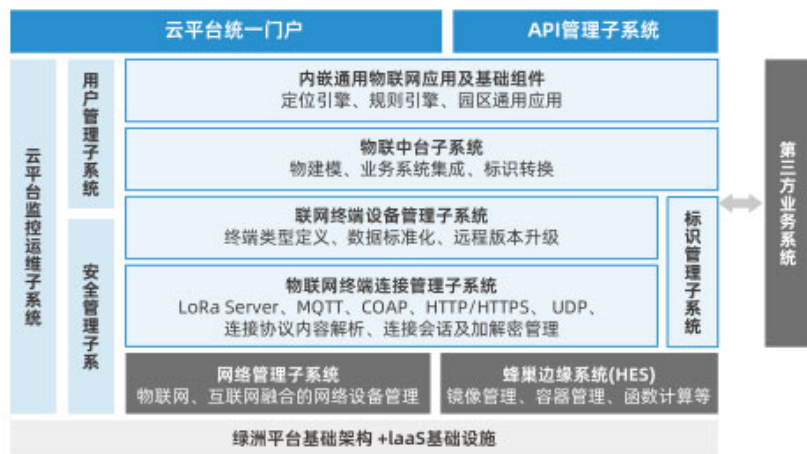


图2 绿洲物联网平台系统架构

绿洲物联网平台采用业界成熟的Kubernetes容器架构，业务模块容器化部署，根据业务需求灵活扩展资源，支撑机场应用迭代升级。除了具备标准的连接管理、设备管理、物联中台（物模型）和应用使能等标准功能模块外，还提供“网络管理子系统”，支持机场全域物联网的网络设备进行集中管理和智能运维。通过一个平台，可实现机场全域的物联终端、物联网和物联数据的统一管理，完全破解机场物联网系统的数据孤岛。

2. 一张网络：一体化网络提供泛在接入

机场网络逐步向智能化、融合化、统一化演进，新华三提出了“以Wi-Fi 6无线网络为基础，按需拓展物联网”的一体化网络建设思路。根据机场业务需求，基于Wi-Fi 6无线网络扩展LoRa/蓝牙/UWB等物联网通信能力，并通过Wi-Fi 6无线网络进行统一承载。



图3 基于Wi-Fi 6 AP拓展IoT网关示意图

一体化网络方案的核心是“八面玲珑”的T320系列IoT网关产品，内置物联网模块插槽，可根据机场业务需求灵活配置LoRa/ZigBee/RFID/蓝牙/UWB等多种物联网通信能力的插卡，即可实现对物联网网络覆盖，此外支持链式组网，通过总线方式实现级联，主网关通过标准网线连接从网关进行POE供电并做数据回传，节约物联网建设成本。

2. 典型应用：飞行区无动力设备管理破局大规模无动力设备管理困境

机场飞行区的无动力设备作业是航班地面保障重要工作，无动力设备管理工作是机场地面运行管理的主要工作内容之一。无动力设备包括了托盘、托卡、工作梯、牵引杆等，形状各异、功能各不相同，但都是保障航空器运行的重要设备，设备的状况和使用直接关系到机坪安全运行。然而无动力设备分布在机场机坪、停车场和库房等区域，具有数量多、使用分散、维护保养难等问题，管理不好易造成对航空器和地面保障车辆造成运行影响。

有部分机场采用传统的挂铭牌、喷印号码等方式对无动力设备建立统一台账，但由于无法联网，无法满足后台管理需求，很难采用智能化设备进行统一管理。也有机场探索采用RFID技术对无动力设备进行定位管理，但由于机坪、存放区、联络线等区域占地面积大、无法新增通信杆来部署RFID通讯设备（室外部署间距一般50米），因此实际落地性不强。无动力设备管理一直是困扰整个行业近十年的业务难题。

新华三基于“云网融合”架构物联网基础设施，为机场打造端到端无动力设备管理解决方案。在机坪的无动力设备加装GPS/北斗定位终端（电池供电，待机2年以上），基于在飞行区进行无线LoRa物联网覆盖，配合基于绿洲物联网平台的资产管理应用，实现对无动力设备使用过程中的位置进行周期性监定位管理。

◆室外精准定位：通过加装卫星定位终端，实现了无动力设备使用过程中的位置周期性监测定位管理。

◆低功耗广域覆盖：单台LoRa基站可覆盖1公里以上，基站与灯杆融合部署、无需新增杆体；定位终端一次充电可用2年，大大减少系统建设和维护成本。

◆创新管理应用：基于物联网平台打造的无动力设备管理应用，实现无动力设备借用管理、位置管理、定期盘点、电量监测、产权方变更等全流程管理。



图4 资产管理应用：机坪无动力设备管理

基于“云网融合”架构的无动力设备管理场景化方案，采用GPS/北斗定位技术，实时掌握无动力设备位置信息，提升了资源调度效率。通过构建全流程数字化体系，建立统一台账、实现领用管理，解决设备丢失、设备损坏无法追责问题，降低维护保养成本；通过主动识别机坪设备乱摆放违规行为等，避免出现影响机场运行的不安全事件，提高机坪安全性。

三、杭州萧山国际机场物联网案例实践

2021年，杭州萧山国际机场每天飞机起落超过650架次，平均每两分多钟就有一架航班起落。如此之高的起落频率，对机场的运营调度和管理能力带来了严峻考验，尤其是对飞行区无动力设备的管理一直是困扰萧山机场的一大难题。新华三基于“云网一体化”物联网数字化基础设施，助力萧山机场打造了端到端无动力设备管理创新应用，采用“LoRa+GPS/北斗定位”技术方案，有效提高了机场飞行区无动力设备的管理调度效率和安全管控，为萧山机场的智慧化管理打下坚实基础。



图5 萧山国际机场物联网建设架构图



图6 无动力设备安装定位终端示意图

在飞行区进行无线LoRa物联网覆盖，无动力设备加装GPS/北斗定位终端，实现对无动力设备使用过程中的位置进行周期性监测定位管理。无动力设备的定位精度在米级，可结合实际需求设置采集数据频率（默认30分钟上报一次），低功耗广域覆盖。采用LoRa低功耗广域覆盖技术，单台LoRa基站可覆盖1公里以上，基站与灯杆融合部署、无需新增杆体，定位终端一次充电可用2年，大大减少系统建设和维护成本。

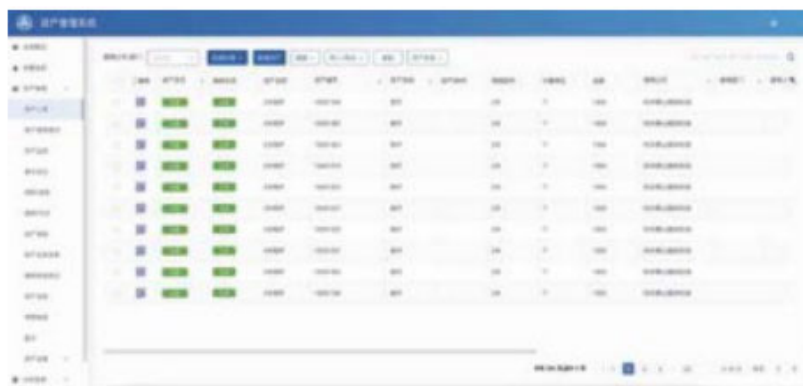


图7 无动力设备管理应用界面

基于物联网平台打造的无动力设备管理应用，萧山机场已经实现无动力设备借用管理、位置管理、定期盘点、电量监测、产权方变更等全流程管理，实现无动力设备可看、可管、可控，助力萧山机场践行智慧机场建设目标。

结语

新华三“云网融合”架构物联网基础设施，将会不断纳入新的机场业务及应用终端设备，全方位赋能新时代智慧机场建设。在数字经济大潮之下，新华三“云网融合”架构物联网基础设施，发挥自身“一平台、一网络”技术优势，围绕机场应用场景需求，联合生态共同打造场景化解决方案，助力智慧机场数字化转型，在民航产业高质量发展的大潮中破浪前行，创造无限可能。

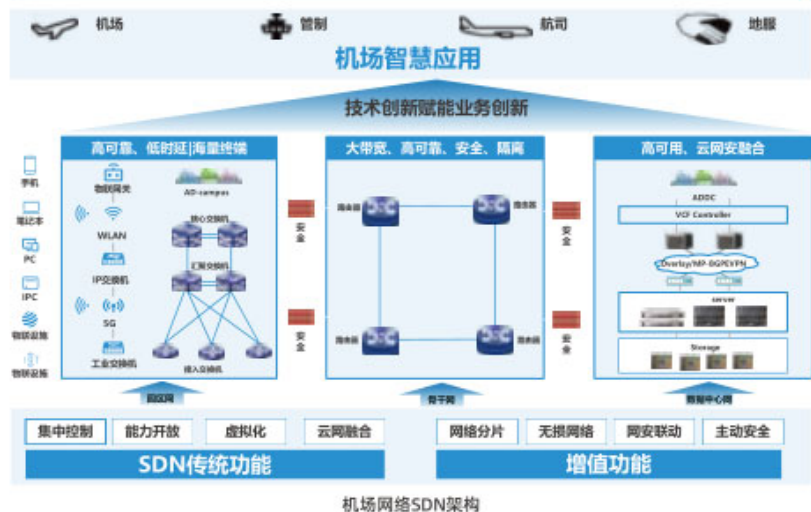
智能网络解决方案打造融合可信、畅通无阻的机场信息化“跑道”

文/闫泽瑞

近年来，民航局围绕智慧机场建设陆续出台相关政策文件，其中在2020年发布的《推进四型机场建设行动纲要（2020-2035年）》中重点提出：智慧机场是“四型机场”建设创新动力。而新技术的不断应用恰恰是智慧机场创新动力来源之一。通过综合运用大数据、云计算、人工智能、区块链等新技术，实现机场的生产要素全面物联、数据高度共享、跨领域高效协同。有了新技术助力智慧机场建设，才能更好的实现平安、绿色、人文机场的建设。

智慧机场是基于全要素、全流程、全场景的数字化、智能化、智慧化支撑的新模式与新形态，而网络作为全要素智慧连接的重要载体，承担着业务数据的高速交换职责。如何建设一个极简、超宽、智能、可信、融合的机场智能网络系统，则显得尤为重要。通过SDN、SRv6、Wi-Fi 6、网络切片等技术对机场用户网络进行赋能，使得机场网络具备业务全流程自动化，故障替换即插即用，网络管理员零干预，业务自动化部署，分钟级上线，多维可视等能力，为智慧机场的网络建设提供智慧承载平台。

一、SDN：软件定义，融合统一



机场网络不同于一般的企业网或者园区网络，一般的企业或者园区网络建设比较单一，建设过程中只需要考虑单独的园区网络或者数据中心网络即可。机场网络则不然，目前大型机场的网络系统整体上由数据中心网、核心骨干网、生产网、综合业务网、安全防护网、离港网、内/外联区和旅客无线接入网等网络组成。从网络组合中来看基本涵盖了数据中心网、骨干网以及园区网的全部网络类型。那么对于机场网络运维管理人员来说，经常面临因一个业务调整，从而分别对三张网进行网络策略调整，业务割接操作复杂，对网络运维人员的技术能力以及现网了解情况要求比较高。那么能不能有这么一套管控平台上能对数据中心网络、机场骨干网以及其他类型的园区网络业务进行统一的配置与管理运维，同时对端到端的VPN业务进行部署，从而构建一个统一的机场网络操作系统，避免运维人员陷入到机场网络系统间复杂的策略中呢？答案是肯定的，那就是SDN技术。

SDN软件定义网络：是一种新兴的控制与转发分离并直接可编程的网络架构。它的核心理念是，希望应用软件可以参与对网络的控制管理，满足上层业务需求，通过自动化业务部署简化网络运维。简单来说，就是把现在复杂的传统网络设备全部对上层应用不可见。上层管理层，只需要像配置软件程序一样，对网络进行简单的部署，就能够让网络实现所需要的功能。

根据网络类型的不同SDN技术同样拥有不同能力：

- 机场数据中心场景：在机场数据中心中部署AD-DC，因其网络能力开放化的特点，使得网络和数据中心计算、安全等资源更紧密协同。通过业务与物理位置解耦、多业务安全隔离、业务快速上线、业务灵活自定义、可视化运维等能力实现虚拟资源和网络安全策略快速迁移与同步，充分满足数据中心能力开放、虚拟资源的智能部署和迁移等需求。

- 机场骨干网场景：在骨干网场景中部署AD-WAN，逻辑控制集中的特点能进行多重资源协作；在SDN控制器中基于全局视角，通过统一整合全网资源、多维观测网络状态、智能分析运行数据，使整个网络实现多层次、全方位的可视化，并根据机场用户策略和应用需求进行集中控制、全局调度、及实时调优，实现应用驱动的骨干网服务。

- 机场园区网场景：在机场园区中通过AD-Campus控制器实现管控析融合，实现网络设备上线、策略部署、用户接入、智能保障功能的无缝集成，能够将传统网络的网络架构本身变得非常灵活，业务部署（应用/终端）可以做到与位置无关；另一方面可以彻底改变传统网络通道就绪，终端和人根据位置匹配通道的模式，将人和应用作为中心，所有网络的资源跟

随人和应用移动；同时能够有效提升系统的逻辑性、易用性，方便了网络运维人员对系统的使用，有效地提高了产品的易用性。

虽然SDN能力能够赋予网络更智慧的能力，但是不同网络仍需要部署不同的SDN控制器，在运维管理方面依旧需要管理人员登录不同的软件进行管理，还是无法解决管理困难的问题。针对此问题，新华三提出了AD-NET统一运维解决方案，AD-NET基于统一的数字底座将管理、控制和网络智能分析融为一体，聚焦园区、数据中心、广域骨干网场景化管控能力的落地，构建园区网随人动、数据中心网随云动、广域网随流动的智能网络。



通过AD-NET解决方案将机场园数WAN场景进行统一融合后，在整个机场网络中，可以将所有网络设备看做一个逻辑资源池，使整体网络看起来、管起来、用起来更加灵活，只需要在一套管控平台上，即可根据机场业务变化进行实际的网络资源调度，并控制整体资源，以此来响应各种业务变化带来的网络需求变更。使用同一套管控平台实现机场离港网、综合业务网、安全防护网等多种园区网络和数据中心网络、骨干网的设备自动化上线、业务配置以及运维管理。通过图形化的配置界面将机场多园区网络VPN、骨干网和数据中心网络对应的VPN拉通，实现机场不同逻辑网络之间的端到端隔离。在极大提升机场网络运维效率的同时，能够更好的协助机场运维管理人员专注于机场网络未来规划与建设，为机场建设一张软件定义、融合统一的智慧网络。

二、SRv6：极简部署，灵活编排

机场的骨干网作为整个机场各网络区域的数据交换的高速数据网络交换平台，在具备高

带宽、高可靠、易维护等基础能力以外，还需要对其上承载的多种业务数据进行控制，保证不同业务间的隔离以及安全可靠的通信。

过去机场在业务隔离控制方面主要采用MPLS技术，MPLS VPN是一种基于MPLS技术的IP-VPN，是在网络路由和交换设备上应用MPLS技术，简化核心路由器的路由选择方式，利用结合传统路由技术的标记交换实现的IP虚拟专用网络（IP VPN），可用来构造宽带的Intranet、Extranet，满足多种灵活的业务需求。但是MPLS技术也有一些缺点，比如：配置复杂，需要非常专业的人员进行维护，要求路径中每一台设备都支持MPLS协议并且在调整业务路径的时候需要逐台设备进行配置，工作量大、出错率高、维护成本高。

随着IPv6协议的推广以及SDN智能网络时代的到来，SRv6技术因其极简部署、自动化配置管理、路径可编排、流量灵活智能调度等特性成为了替代机场骨干网MPLS技术最好的选择。

Segment Routing（SR）是一种源路由技术。它为每个节点或链路分配Segment头节点，把这些Segment组合起来形成Segment序列（Segment路径），指引报文按照Segment序列进行转发，从而实现网络的编程能力。

Segment Routing有如下四个优点：

- ◆简化了控制协议。它只采用IGP，统一了控制协议，不再像MPLS那样在IGP的基础上还要LDP、RSVP-TE等协议，降低了运维的复杂度。

- ◆良好的扩展性。以前实现路径编程（流量工程，TE）时一般采用RSVP-TE，网络中的每个节点都要感知到每条路径的状态，协议的消耗很大，限制了TE隧道的规格，难以部署和维护。Segment Routing路径编程则是在头结点进行，海量的路径都是依赖于有限的表示链路和节点的Segment的组合，网络中间节点几乎不感知路径状态，具备很高的扩展性。

- ◆可编程性好。Segment Routing中的Segment非常类似于计算机的指令，通过对Segment的编排可以实现类似于计算机指令的功能。具备非常好的灵活性，可以非常灵活地建立满足不同需求的路径，释放网络的价值。

- ◆更可靠的保护。Segment Routing能提供100%网络覆盖的快速重路由（Fast ReRoute）保护，解决了IP网络长期面临的技术难题，能够在高可扩展性的前提下，又可以达到完全的可靠性保护。

SRv6（Segment Routing转发层通过IPv6进行封装）不仅继承了SR的优点，还具备标签空间数量无限、全网唯一、任意点可达的优点（IPv6地址特点）。进而可以实现只要地址可达，可以任意点接入，任意点之间互联。配合SDN控制器软件，可以做到极简部署、灵活编排，帮助机场用户实现更加智能可靠易管理的机场骨干网络。

举一个例子：机场网络中的综合业务网内部存在大量驻场单位的办公终端，这些驻场单位之间需要相互隔离，同时这些驻场单位的办公终端需要与其自身业务网络互通（比如南方航空办公终端需要访问离岗网以及自身业务）。基于这种需求，需要针对有业务隔离要求的驻场单位部署L3VPN。为了打通业务VPN，需要在骨干网使能MPLS能力，以便在骨干网上生成业务VPN需要的MPLS LSP。使能MPLS，包括开启MPLS能力和MPLS LDP能力。骨干网所有路由器上面向路由器连接的接口、Loopback0接口，都要使能MPLS，并且MPLS设备被部署到不同的网络域，例如骨干网、综合业务网和离岗网等，形成了独立的MPLS域，因此也带来了多个不同的网络边界。业务在端到端部署的过程中需要跨越多个MPLS域，这就带来了复杂的MPLS跨域问题，业务部署复杂度相对都较高，业务开通很慢。同时在L2VPN、L3VPN多种业务并存的情况下，设备中可能同时存在LDP、RSVP、IGP、BGP等协议，业务部署和管理复杂。

而采用SRv6技术，首先从兼容性方面，不需要全部的路由器均部署SRv6，只需要相关的业务接入设备升级支持SRv6，其他设备只需要支持普通的IPv6路由转发而不需要感知SRv6，部署简单，兼容性好。其次在跨域部署方面，SRv6跨域相对来说部署更加简单。SRv6的Native IPv6（原生IPv6）特质，使得它能够基于聚合路由工作。这样即使在机场的跨域场景中，只需要在边界节点引入有限的聚合路由表项即可。这降低了对网络设备能力的要求，提升了网络的可扩展性。并且在流量调度和可视化，SRv6技术可以更好的和SDN技术进行配合。作为一种源路由技术，可以通过SDN控制器，在头端节点即可指定整条转发路径，SRv6支持TE流量工程，对于需要调度的流量计算出显式路径，并下发Segment执行。通过与SDN控制器相结合，SRv6可以支持域内、跨域流量调度，并支持主备路径隔离等部署模式，真正实现业务部署自动化，流量路径可视化，大大节省了业务部署时间和运维工作量。

三、网络分片：带宽保障，一网多用

核心骨干网承载着离港网、地面运行网、综合业务网、安全防护网、生产网等生产业务数据及外连区、数据中心等业务流量，接入终端种类庞杂，不同的业务类型重要性不同，如何优先保证重要数据的优先传输，在过去机场用户都是通过QoS对业务数据划分不同的优先级队列来保

证带宽和传输稳定，但在实际使用过程中却又无法保证流量激增导致重要数据业务带宽被抢占的问题不会发生，那么网络分片技术就能解决您的问题。

网络分片技术其实早在运营商已经有所应用，将链路带宽划分为多条通道，不同通道之间的带宽相互独立、互不侵占，确保关键业务的带宽有所保障。FlexE技术就是其中的佼佼者，但是在类似机场这样的行业网中，FlexE技术却遇到了难题：

- ◆成本高：需要100G、50G接口才能支持，商务成本过高。
- ◆切片粒度大：标准的5G粒度切片，对于行业网来说，粒度太粗。
- ◆传输：需要传输链路支持，现网部署时，有比较大的不确定性。

针对这些技术困难，新华三推出了子接口切片技术，即通过硬件预留转发资源的方式实现，确保每个切片之间的带宽预留。其优点如下：

- ◆成本低：100G、50G、千兆、万兆均可以支持，机场网络主流端口。
- ◆切片粒度细：支持M级切片，切片个数可达4K个。
- ◆传输无限制：全部支持。
- ◆兼容性：异构厂商可以无缝对接。

通过网络分片技术，可以在一套机场核心骨干网中构建多个业务专网，针对不同业务做到带宽保障、一网多用，为机场客户提供更有保障的链接。



结语

随着SDN、SRv6、网络分片、无线物联网等技术的不断发展，新华三结合在机场网络建设的深度实践，不断深耕、助力机场打造一张“软件定义、统一融合、极简部署、一网多用、全域感知、人机协同”的智慧网络。未来，新华三将以不断创新的技术能力，持续助力机场智慧网络建设。

行业专属路由器助力智慧空管建设

文/闫泽瑞

空中交通管制（简称“空管”），是负责管理和指导航空交通的组织和系统。空管行业作为交通行业“十四五规划”中重要组成部分，在2021年发布的《“十四五”民航空管系统发展规划（2021-2025）》中重点提到：“到2025年，基本建成以‘四强空管’为内核的现代化空中交通管理系统，成为亚太一流的空中航行服务提供商；到2035年，全面建成现代化空中交通管理系统并运行有序，成为全球一流的空中航行服务提供商。”以“强安全、强效率、强智慧、强协同”为建设纲领，把握“两条发展线”：即守住安全底线，提升空管安全管理能力；突出智慧主线，立足我国空管发展实际需求，聚力战略性关键技术自主创新。推进现代化空管体系建设，提升我国空管的综合保障能力。

一、安全与创新之间需要平衡点

由于空管行业的特殊地位和作用，保障业务的安全性和可靠性始终是空管行业的首要工作，对安全隐患零容忍，坚守安全红线，是每一个空管行业从业者都应遵守的底线。因此，在创新性技术的应用上，空管行业一直保持着保守的态度。

空管核心业务主要包括甚高频话音、监视（雷达和ADS-B）、自动转报、管制移交电话等，目前除ADS-B数据以IP方式通信，其他业务大多通过光传输点对点通道（PCM）方式进行通信。基于光传输点对点通道通信好处是延时抖动稳定、话音通信质量清晰，并且运行多年，安全性，可靠性有保障。

管制业务终端设备有时需要同相关塔台、区域管制中心甚至全国管制中心实时互通，不同区域管制中心间也要实时动态互通，这就需要在电台、雷达等地面设备所在位置与不同管制中心之间分配不同光传输通道。这个过程实现起来非常不方便，且通信方式非常不灵活，效率较低；直接基于光传输通道方式的通信市场空间相对狭窄，且不符合主流通信技术发展方向，将来很有可能面临没有厂商支持的尴尬局面。

因此，在“十四五规划”中，明确的指出了应“加快推进基于网际互联协议的空管语音通信技术的试点和应用”，所以如何将空管专有业务IP化，IP化的业务如何保障安全性和可靠性成为了关键问题，行业需要在安全和创新之间找到平衡点。

二、空管特性业务IP化分析

1. 空管语音业务IP化可行性分析

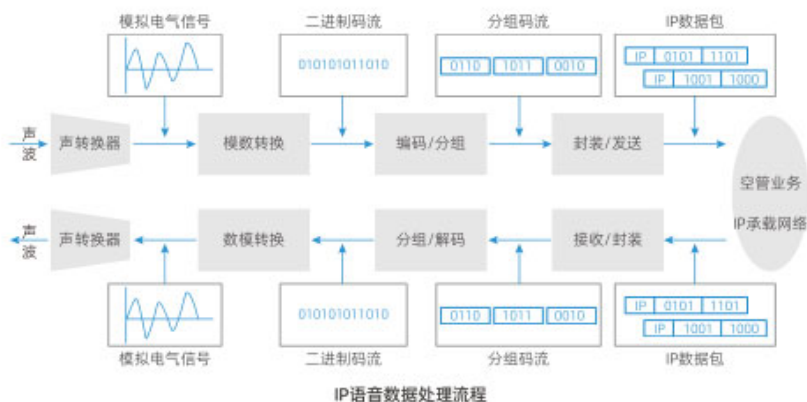
空管管制语音通信（电台、内话）对延时、抖动、可靠性要求极严格。

IP化语音通信需要将模拟语音采样、数字化、编码，然后在IP网上传输，到对端再解码复原。

IP语音延时通常高于TDM交换网络延时，延时包括3部分：编解码延时、设备延时、网络延时（由于空管语音透传业务通常不需要VoIP呼叫建立过程，为长通或摘机即通的专线状态，所以不必考虑呼叫建立过程中的时延，只需要考虑正常语音通信时延即可）。

◆IP语音通信编解码延时分析

IP语音数据处理流程如下图所示：



IP语音编解码延时同编解码类型、编码速率、帧长、Look-ahead相关，由表1可以看出，通常采用G.729、G.711、G.722编码的IP语音通信，编解码延时最大在60ms或75ms。

编解码类型	编码速率 (kbit/s)	帧长 (ms)	Look-ahead (ms)	编解码延时 (ms)	
				最小延时	最大延时
G.711	64	0.125	0	30ms	60ms
G.729	8	10	5	45ms	75ms
G.722	64/48	3	0	30ms	60ms

不同编解码类型延时对比

◆IP语音设备延时分析

随着技术发展，IP网络设备延时往往比较低，以一个128字节包在一台路由器FE端口延时为例，单设备端口延时在0.01883ms，即使语音数据包在IP网络上经过10跳也远小于1ms，所以设备延时很小。

包长	FE端口	GE端口
64Byte packets	0.0135ms	0.00935ms
128Byte packets	0.01883ms	0.00983ms
256Byte packets	0.02962ms	0.0103ms
512Byte packets	0.05133ms	0.01357ms
1024Byte packets	0.0948ms	0.02048ms

H3C SR66系列路由器端口转发延时

◆IP网络延时及抖动分析

IP网络在运行平稳时延时抖动恒定，其延时通常在30ms之内，这样，端到端IP语音单向延时最大为：

60ms/75ms设备编解码延时+30ms网络延时+1ms设备延时=91ms/106ms，根据ITU G.114建议，单向语音延时不超过150ms就可以接受。可见，91/106ms延时是可以满足管制员通信需求的。

一般来说，抖动主要是由网络拥塞或线路、设备不稳定引起。

对于网络拥塞，可以通过采用语音IP专网、IP延时固化补偿、缓冲区参数调整、高性能语音网关、DiffServ等技术来将抖动降到最低。另外，还可以通过RTP协议来实现IP网络优先转发语音数据包，从而减少语音抖动。语音接收方还可以通过去抖动处理技术来消除网络抖动对语音的影响。对于线路不稳定，可以采用端口抖动抑制来降低影响，对于设备不稳定，可以采用高可靠设备来解决。通过这些措施，IP网络抖动可以降到最低，接近TDM专线效果。

2. 雷达、转报、ADS-B IP化通信可行性分析

雷达数据通信同样关注点包括：

- ◆延时：指雷达数据在通信过程中网络时延。
- ◆抖动：指网络不稳定情况下延时的不确定性。

- ◆可靠性：要求网络不能中断或中断情况下有备份。
- ◆安全性：指数据在通信过程中不被篡改。

传统雷达终端接口类型和传输带宽要求如下表所示。雷达通信网络需要专网（雷达、转报、电台、ADS-B、内话等管制业务需要统一构建一个IP专网），避免非管制类业务对网络延时抖动造成影响。

接口类型	RS232、V24、V35
带宽占用	4.8K、9.6K、19.2K、64K
数据类型	HDLC格式或非帧格式
传输时延	<70ms
抖动要求	<30ms
安全性	专网专用，非承载在公共服务类网络

雷达通信对网络要求

传统雷达站都是以HDLC成帧方式或非成帧方式输出数据流，主要通信方式有光传输通道透传、ATM虚电路透传（已经逐步淘汰，不多赘述）和IP化透传三种。对于IP化透传，雷达数据通信延时包括三部分：解封包延时、设备延时、网络延时。

◆雷达IP化透传延时抖动分析

一般雷达业务在网络设备封装过程是把已经数字化的物理比特流直接封装到IP包里，不存在语音传输采样、按格式编码的开销，因此，解封包延时相对语音延时大大降低，可以在10ms范围之内。这样，一路雷达IP化透传延时为：

解封包延时10ms设备延时1ms+IP网络延时30ms，整体限制在41ms之内，符合雷达业务通信<70ms的需求。

近年来，雷达终端也逐步IP化，基于IP网络的通信逐渐进入应用阶段，采用成熟标准的IP网络对雷达数据进行透传是大势所趋。

同样，由于空管转报、ADS-B业务对延时、抖动、可靠性要求相对雷达宽松，安全性要求同雷达一样，所以转报、ADS-B业务实现IP化透传也没有问题。

三、新华三空管特性专用路由器，助力空管业务IP化转型

为了助力空管用户进行数字化转型，新华三专为空管用户开发了空管特性专用路由器并提供了空管TDM业务网络解决方案，新华三的空管专用路由器是针对空管行业需求定制的高性能设备，具备精准的流量控制和安全防护能力，其主要特性如下：

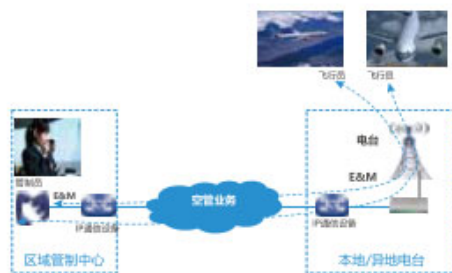
◆多网合一：新华三的MSR专用设备支持多种协议和接口类型（同/异步接口、E&M、语音、IP等），因此组建一套高可靠空管专用IP网络，就可以实现雷达、电报、转报、甚高频和管制移交电话等所有终端设备接入到IP网络。

◆专用技术：新华三为空管用户开发了空管特性功能，实现了E&M端到端延时（封装，网络传输，解封）可以控制在10ms之内！新华三路由器在64K通道可以传送4路语音！雷达IP化终端可以实现点对多点传送，满足空管所有业务场景。

◆应用广泛：新华三的空管接入方案于2005年就已经开始开发完成并投入使用，目前已经在国内各民航空管局广泛应用，产品成熟稳定。

1. 空管管制语音IP化通信实现方案

以空管管制员地空通话为例，管制员和航班飞行员之间要通过地面电台实现实时地空对话，发布管制指令。通常区域管制员往往面向多个省份进行高空飞行调度，因此电台设置在外省市，这就要实现异地地空对话，语音通信方式是通过广域IP承载网实现透传。



地空对话通信IP化透传方案

通过IP化透传，区域管制员可以集中调度几个省空域高空航班飞行，电台通过地面IP网络可以同任意区域管制中心或全国管制中心进行通信，不必额外调配传输通道，非常灵活方便。新华三的空管IP通信设备可以实现单向100ms延时，效果良好。

同样，采用G.722编码方式的内话VoIP通信技术也已经成熟，延时、抖动、可靠性可以满足需求。

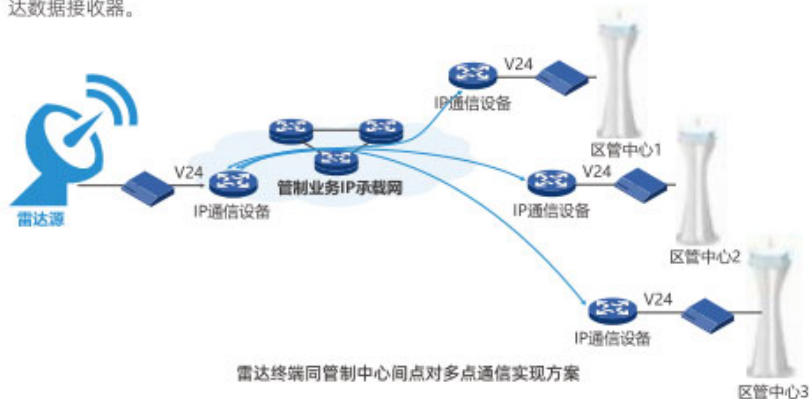
2. 雷达、转报、ADS-B IP化通信实现方案

◆雷达业务

雷达终端输出数据流格式通常是HDLC或非成帧格式，这些格式帧无法直接通过IP网络进行同步通信，需要IP网络能对这些数据进行透明打包传输，实现雷达数据点对点通信。



管制中心定时监测雷达数据，雷达终端把采集到的数据定时发送给管制中心雷达数据接收器，实现过程是：雷达终端通过同步串口把数据传送给IP通信设备，IP通信设备再通过广域网把雷达数据发送到管制中心IP通信设备，管制中心IP通信设备再把数据还原回雷达数据传给雷达数据接收器。



雷达终端同管制中心间点对多点通信实现方案

雷达数据多点之间通信实现方案如图4所示，这种方式主要用于雷达同相关机场塔台、区域管制中心间通信，IP化通信设备会将雷达数据同步广播到多个接收端的IP通信设备，对端的IP通信设备再通过同步口将数据传送给各个雷达接收设备。同样，管制中心还会同时接收多部雷达数据，实现针对同一架飞机多重监控。

点对多点透传方式实现了雷达数据充分共享，进而还可以实现空管部门同航空公司、机场等航班实时状态信息的及时横向互通。

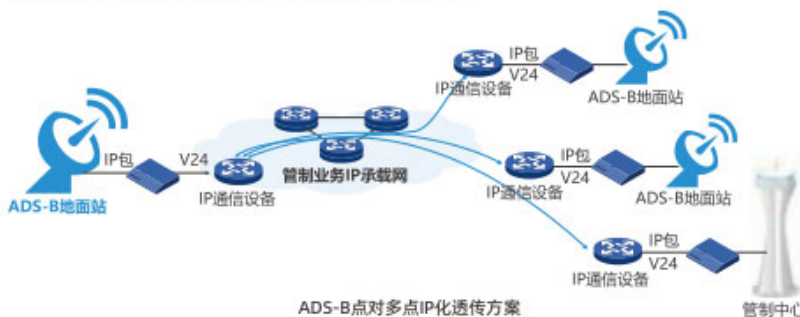
◆转报业务

当前在用的转报终端大多是非IP口，其基于IP网络透传实现方式同雷达业务类似。由于转报业务对延时、抖动相对雷达宽松，带宽占用也较小，因此，能够满足雷达业务透传的网络同样能够满足转报业务透传的需求。

对于IP口转报终端，可直接通过IP网络实现点对点、点对多点通信，对IP网络并无特殊要求，实现起来更加方便。

◆ADS-B业务

ADS-B实现航班状态实时监控，比雷达更加灵活、精细、高效，是未来发展趋势。ADS-B通信需求为实时点对多点通信，与雷达业务类似。同大多数雷达终端不同，ADS-B地面终端都是IP化接口，通过优化IP组播、广播技术实现点对多点，多点对多点实时高效通信。ADS-B设备终端通过IP接口与IP通信设备进行连接，IP通信设备将其广播报文同步转发到多个目的节点，实现多个站点间同步，多个站点同管制中心同步。



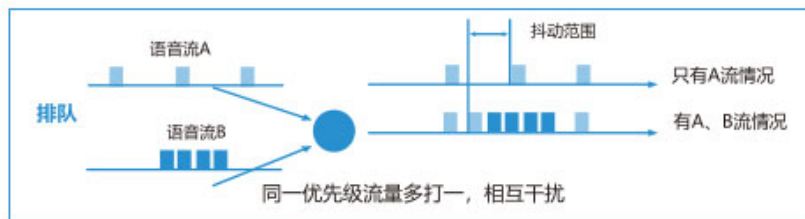
ADS-B点对多点IP化透传方案

四、空管智慧化业务新方向探讨——确定性网络技术

1. IP网络存在多种“不确定”因素

经过上文分析，我们能够确定空管特性业务进行IP化的传输是可行的，但是，我们熟知的IP网络其实有很多的特性与空管特性业务的需求并不完全适配。比如：

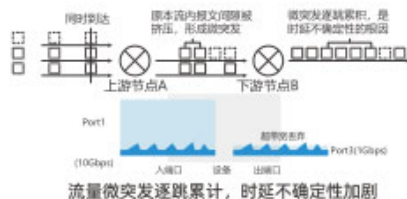
◆空管特性业务可靠性要求高，尤其甚高频业务对时延和丢包非常敏感，而IP网络是尽力而为的，即使在带宽保证的基础上也无法实现端到端确定性，相同优先级的业务流量互相也会造成干扰。



◆甚高频、雷达、转报等业务都需要在TDM网上进行传输，那么如何实现一网多用，在一张IP网络中虚拟出多张逻辑网络的基础上达到专网、专线的能力。



◆转报、甚高频等业务会涉及到跨区通信，跳数经过越多，时延和抖动在IP网络中会累加越多，而业务肯定希望端到端抖动是确定的，时延可以与跳数、距离相关。



2. 新技术给空管业务带来“确定性”

确定性网络的技术关键在于实现确定性时延、抖动、丢包率、带宽和可靠性等。确定性时延主要通过时钟同步、频率同步、调度整形、资源预留等机制实现；确定性抖动和丢包率通过优先级划分、抖动消减、缓冲吸收等机制实现；确定性带宽通过网络切片和边缘计算等技术实现；确定性可靠性通过多路复用、包复制与消除、冗余备份等技术实现。

空管特性业务的IP化是趋势，通过上述确定性网络技术能够帮助空管业务避免IP网络所带来的“天生的劣势”，保障空管特性业务的安全性和可靠性，提供确定的时延、抖动、丢包率等。同时，确定性网络技术是新一代网络通信体系发展方向，是先进技术的代表，提供确定性网络服务、构建重大网络基础设施，能够为空管行业占领信息技术发展的制高点提供新的机遇，也满足“十四五规划”中“守住安全底线，突出智慧主线”的战略要求。

3. 新华三提供确定性网络端到端解决方案

新华三是ICT的领导者，一直致力于ICT领域的开发与研究，在确定性网络方面做了很多探索和实践：

在局域网方面：有5G over TSN方案：它采用SDN方式，整合了RRU、BBU、核心网以及TSN交换机等诸多设备，实现5G专网内端到端的确定性传输。

广域网方面，有整套的端到端确定性解决方案：采用SDN方式，利用FlexE硬管道、SRv6可编程能力，再整合网络操作系统，实现跨地域的端到端确定性传输。

所以，新华三有能力和意愿，助力空管行业的确定性网络建设，共同提升空管行业的智慧和数字化能力。

结语

新兴技术正在为空管效率提升带来新动能，新华三空管特性专业路由帮助空管通信IP化，使得业务效率更高，更灵活，并且有利于实现区域管制一体化、全国管制一体化，有利于管制效率提升，还可以及时将航班异常信息传达给机场、航空公司，尽量减少航班晚点率及突发事件发生。目前，雷达、转报、电台IP化透传通信已经在中南、西南、西北、新疆、华北等地区管理局得到应用。同时5G、云计算、人工智能、大数据、确定性网络等一批新兴技术开始与行业深度融合，数字化、网络化、智能化、智慧化将成为空管未来发展的新基点。

未来，新华三将继续持续关注空管行业的技术发展趋势，以不断创新的技术能力提供高品质的产品和解决方案，为空管客户提供更加稳定、高效、安全的服务，助力智慧空管建设。

04

云端列车，智通四海

第34章 探索铁路下一代承载网发展趋势	212
第35章 铁路综合视频监控新标准实践分析	222
第36章 从“中国智慧”到“中国速度”，以云服务助力千万高铁数智求变	235
第37章 京广高铁（武汉）综合视频一体化云平台	237

探索铁路下一代承载网发展趋势

文/刘术伟

随着现代铁路运输的不断发展和智能化的崛起，下一代铁路通信承载网络迎来了巨大的挑战和机遇。通信承载网需要同时支持多种铁路通信业务，包括高速的5G数据传输、多媒体业务、实时监控、列车调度和乘客信息服务等。为了满足这些多样化的需求，下一代铁路通信承载网络需要充分利用一系列前沿技术。其中IPv6+技术为铁路通信承载网络带来了更大的地址空间和更强的网络安全性。这一技术升级将有助于支持更多的终端设备和连接，并提供更高水平的网络安全保护，以应对日益复杂的网络威胁。切片技术使铁路通信网络能够按需分割成多个虚拟网络，每个切片都可以为不同类型的通信业务提供定制化的服务。这种灵活性和可定制性使铁路能够更好地管理网络资源，确保各类通信业务都能获得高质量的服务。

一、铁路5G承载网络技术分析

1. 5G网络化架构分析

随着5G在中国的快速商用部署，面向5G的新一代承载网络成为运营商城域网的关键部分。5G核心网不仅提供了传统的基础通信能力，还增加了更多细分网元和网络切片等先进功能，支持多样化业务和服务，同时确保高安全性、可靠性和低网络时延。

承载网主要由城域网和骨干网组成。城域网包括接入、汇聚和核心三层，而骨干网分为省级和国家级。接入层从4G升级为5G，重构为CU（集中单元）、DU（分布单元）和AAU（有源天线单元）的新架构，有效满足不同场景的低时延和高可靠性需求。汇聚层则采用了如SPN切片分组网和IPRAN等不同的承载技术，分别依托其领先技术和成熟应用实现优化。

5G核心网的架构、技术和业务方面相较4G有显著提升，通过服务化架构（SBA）和云原生技术，增强了网络灵活性和融合能力。此外，它还支持多样化的业务场景，如移动VPN和远程医疗，为各行业提供定制化服务，开辟新的商业模式。

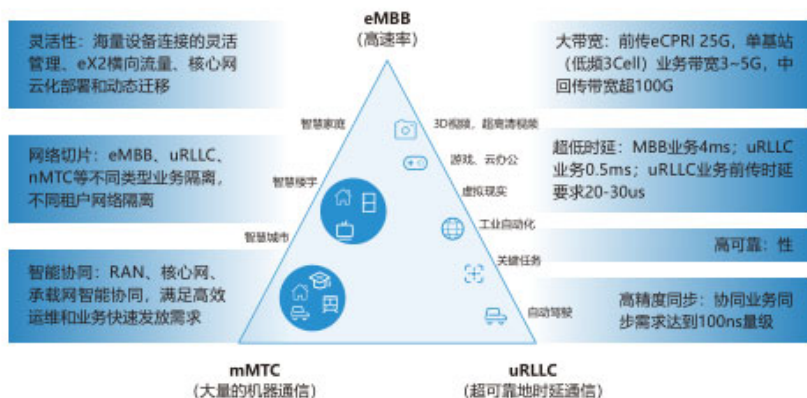
5G通过eMBB（增强型移动宽带）、URLLC（超可靠低时延通信）和mMTC（大规模机器类型通信）等应用场景，推动着新一代承载网向着超高速率、超大连接和超低时延的目标不断进化。

2. 5G承载网技术需求分析

5G承载网当前的技术需求主要来自七个方向:

大带宽

5G网络要支持高清视频、虚拟现实、云计算等大流量应用,这就对承载网提出了超大带宽的需求。根据ITU-R的标准,5G网络的峰值速率应达到20Gbit/s,流量密度应达到10Mbit/s每平方米。为了满足这些需求,5G承载网需要采用高效的物理技术和隧道技术,如WDM、PAM4、MPLS、SR-MPLS、SRv6等,提升网络的传输能力和灵活性。据粗略估算,5G承载网接入层需要具备10Gbit/s到站、50Gbit/s成环的带宽能力;汇聚层需要具备100/400Gbit/s的带宽能力;核心层需要具备400Gbit/s的带宽能力。



超低时延

5G网络要支持车联网、工业控制、远程医疗等低时延应用,这就对承载网提出了超低时延的需求。根据ITU-R的标准,5G网络的用户面时延应小于4ms,控制面时延应小于10ms;对于更严格的uRLLC场景,用户面时延应小于0.5ms,控制面时延应小于10ms,在承载网接入的前传上,更是需要达到20~30us的要求。为了满足这些需求,5G承载网需要采用低时延的传输技术和路由技术,如FlexE、OSPF、IS-IS、BGP等,优化网络的路径和转发。同时,5G承载网还需要调整网络的架构和功能,如无线接入网中CU和DU合设、核心网用户面下沉至无线接入网等,减少网络的层级和跳数。

高可靠

5G网络要支持工业制造、智慧城市、智能电网等高可靠应用,这就对承载网提出了高可靠性的需求。根据ITU-R的标准,部分uRLLC业务的可靠性应达到99.999%。为了满足这些需求,5G承载网需要采用高可靠性的同步技术和VPN技术,如同步以太、IEEE 1588v2、ITU-T G.8275.1、Atom GPS、L2VPN、L3VPN、EVPN等,保障网络的时钟精度和业务隔离。同时,5G承载网还需要采用高可靠性的物理设施和逻辑拓扑,如光纤化接入层、光缆直连机房、Spine-Leaf架构等,保障网络的连接质量和容错能力。

高精度同步

5G承载网对高精度时钟同步的需求:5G网络要支持高精度定位、车联网、智能制造等新应用,这就对承载网提出了高精度时钟同步的需求。根据ITU-R的标准,5G网络的时钟精度应达到10ns。为了满足这些需求,5G承载网需要采用高精度的同步技术和设备,如IEEE 1588v2、Atom GPS、同步以太等,保障网络的时钟准确性和稳定性。同时,5G承载网还需要采用高精度的同步传输和部署方案,如光纤直驱、无源WDM、有源WDM/OTN等,保障网络的同步传播和覆盖。此外,5G承载网还需要考虑同步网络的安全性和可靠性,如采用多源多路径的同步方案,避免单点故障和外部干扰。

灵活性

在灵活性方面,5G网络必须支持大规模设备接入、多元化业务承载,并适应不断变化的场景。这需要承载网具备快速接入、有效识别、智能调度、安全隔离等能力,以确保设备的可用性和业务质量。此外,5G还需支持各种应用场景和垂直行业需求,要求网络具有快速部署、灵活切换、智能保障的能力。同时,为适应高速移动、大规模并发和突发事件等变化场景,网络必须能快速感知环境、自适应调整和快速恢复。实现这些功能,承载网将采用诸如切片技术、SDN、AI、EVPN、SRv6、FlexE、Telemetry、IFIT、FRR等先进技术,以实现网络资源和服务的动态优化和故障诊断。

网络切片

5G网络要支持不同的业务场景和用户需求,如高可靠的邮件业务,低抖动的语音业务,接近零丢包的视频业务等,这就对承载网提出了网络切片的需求。网络切片是一种将物理网络虚拟化为多个逻辑网络的技术,每个逻辑网络可以根据业务特性和用户要求定制化网络资源和服务,实现端到端的业务隔离和保障。为了满足5G承载网对网络切片的需求,通常采用以下几种技术:

软件定义网络 (SDN)：这是一种将网络控制层和数据层分离的技术，可以实现网络资源的集中管理和动态调度，提高网络的灵活性和可编程性。同时SDN可以实现承载网在转发面的软切片，即在复杂的通信管道中部署不同的物理或者逻辑分割路径，以保障各切片业务的转发和调度。

灵活以太网 (FlexE)：这是一种基于以太网物理层的切片技术，可以实现对物理链路带宽的灵活分割和聚合，提高带宽利用率和传输效率。FlexE可以实现承载网数据面的硬切片，即在同一个物理链路上创建多个逻辑链路，为不同的业务提供不同的带宽、时延、抖动等服务质量。

智能协同

5G网络要支持多域、多层、多技术的网络协同，实现网络资源和服务的优化配置和动态调整，以适应不同业务场景和用户需求的变化。智能协同主要指以下几个方面：首先是跨域协同：5G承载网需要与无线接入网、核心网、数据中心等其他域进行有效的信息交互和业务协调，实现端到端的网络切片、网络编排、网络管理等功能，以保证业务的质量和连续性。其次是跨层协同：5G承载网需要在物理层、数据链路层、网络层等不同层次上进行灵活的资源分配和服务提供，实现不同业务类型和性能要求的网络切片，如LO波长切片、L1通道切片、L2/L3隧道切片等。为了实现跨层协同，5G承载网需要采用高效的技术和设备，如WDM、PAM4、MPLS、SR-MPLS、SRv6、EVPN等，实现不同层次之间的网络转换和连接。最后是跨技术协同：5G承载网需要在光传送技术、分组传送技术、IP传送技术等不同技术之间进行智能的选择和组合，实现不同场景和区域的网络部署和优化，如光纤直驱、无源WDM、有源WDM/OTN、SPN、M-OTN、IPRAN等。

3. 5G-R承载网络架构整体思路

我国铁路专用移动通信历经数十年发展，紧跟时代步伐，持续进行技术迭代、制式演进，从而满足日益丰富的铁路无线通信业务需求。从450MHz列车无线调度通信系统到铁路数字移动通信 (GSM-R) 系统的升级改造，实现了模拟制式向数字制式的跨越，GSM-R系统在我国的大规模运用，助力高速铁路发展。而GSM-R系统作为窄带制式，目前面临设备停产和无法满足宽带业务需求的问题，GSM-R系统向铁路新一代移动通信系统演进，实现窄带制式向宽带制式的升级，成为必然发展和迫切需求。

5G具有大带宽、大连接、低时延等优势，可实现人与物、物与物的泛在互联，是支撑经济社会数字化、网络化、智能化转型的关键新型基础设施。2020年初，中国国家铁路集团有限公司 (简称国铁集团) 经过业务需求分析和经济技术比选，结合我国加快5G网络等新型基础设施建设的决策部署，基本明确了5G专网的系统目标。由于铁路5G专用移动通信 (5G-R) 系统具有线路覆盖、站场覆盖和车内覆盖相结合的网络覆盖特征，以及部分应用业务对网络安全性和可靠性的较高要求，公网5G的技术和装备无法直接应用于铁路，铁路需根据应用业务特点，定制适用于铁路的5G-R系统架构和设备组成，形成完整、成熟、具备自主知识产权和铁路特色的5G-R技术体系及系列专用装备，保障5G-R系统的全生命周期可用、可控。

5G-R承载的业务类型包括列车控制和监测、高清监控、智能调度、互联网接入等。具体来说，以下是5G-R承载的业务类型：

列车控制和监测业务：列车控制和监测是铁路运输中最重要的业务之一，需要实时监测列车的位置和状态以确保列车的安全运行，5G-R技术可以提供高可靠性和低延时的通信服务。

高清监控业务：高清监控业务是针对铁路站点和乘客车厢内的视频监控，需要高速稳定的数据传输，以获取和处理高清视频数据。

智能调度业务：智能调度业务涉及铁路站点和路线的调度管理，需要实时获取各种数据信息，并对其进行分析和优化，以确保铁路运输的安全和高效性。

互联网接入业务：互联网接入业务是铁路乘客和工作人员接入互联网的业务，需要高速、稳定、安全的网络通信服务，以确保连接质量和数据传输能力。

根据上述要求按照区间、车站、路局、集团为边界进行层级规划，分别对应接入、汇聚、核心层。通过采用分层架构，方便以清晰业务的边界规划各类业务通信路径，按需疏导本层级的业务流量，减少核心层的流量需求。通过层层汇聚，减少高层级设备所需接口、光纤等资源。按照分层架构可以为每层级按需选用不同性能的产品，合理控制建设成本。也为5GC、下沉UPF等建设位置提供依据。



4. 5G-R承载网技术分析

目前5G承载网主要有IPRAN、SPN、分组增强型OTN等。

◆大带宽方面

IPRAN、SPN、分组增强型OTN均支持标准以太速率，如10G、50G、100G等。此外IPRAN和SPN还均支持使用FlexE捆绑技术将多个以太捆绑成一个大速率FlexE切片。IPRAN、分组增强型OTN还支持通过使用彩光技术配合光层系统来实现密级波分复用，来提高单条光纤中的传输带宽。目前可实现单条光纤传输96个波道。

◆低时延及可靠性方面

IPRAN和SPN均使用切片技术来实现业务隔离，同时保证不同切片的业务质量互不影响。不同切片组成不同的逻辑网络，确保低时延应用可以以最短路径访问到最优的边缘计算资源。

当前，IPRAN支持5G粒度的FlexE切片（支持在50G、100G以太网接口上进行切片）、10M粒度的小颗粒切片（支持在10G以太网接口或FlexE切片上进行切片）、1M粒度的SliceID切片（支持在任意速率以太网接口、FlexE切片、10M小颗粒切片上进行再次切片）；SPN支持5G粒度的FlexE切片、10M粒度的小颗粒切片，切片模型同IPRAN，不支持1M粒度的SliceID切片；分组增强型OTN支持1.25G粒度切片，OSU OTN支持最小2M粒度切片。

在可靠性方面IPRAN、SPN、分组增强型OTN均支持各类型故障收敛时间小于50ms要求。

◆灵活性方面

IPRAN支持异厂商组网，且有大量实施案例。SPN、分组增强型OTN不支持异厂商组网。

IPRAN支持第三方网管和控制器，在运营商有实施案例。SPN、分组增强型OTN不支持第三方控制器，无实施案例。

◆时间同步方面

IPRAN、SPN、分组增强型OTN均支持1588v2和SyncE。

◆智能应用方面

IPRAN支持基于APN6技术和智能运维技术识别应用、应用对网络的需求，按需将业务引入能符合应用需求的隧道、切片中。SPN、不支持APN6技术，无法识别应用，只能识别用

户，或者增加DPI硬件插卡或硬件设备来识别应用。SPN、分组增强型OTN只能基于接入接口、IP地址等区分用户、业务。

IPRAN可基于iFIT检测结果利用智能运维技术，及时对业务质量劣化事件进行干预，如发现应用的流量在网络中真实的质量劣化后将应用的业务流量调整至备份路径。SPN支持iFIT，可基于用户、业务检测质量，但不支持APN6，无法基于应用质量来调整流量转发路径。分组增强型OTN不支持iFIT，不支持基于业务质量自动调整业务路径。

◆在IPv6+方面

IPRAN全面支持IPv6+技术，如SRv6（IPv6分段路由）、APN6（应用感知网络）、SRv6 SFC（SRv6功能服务链）、SRv6 iFIT（基于SRv6的随流检测）、SliceID（基于IPv6源地址的网络切片技术）。

SPN基于IPv4内核使用MPLS-TP或MPLS-SR协议，目前仅支持承载IPv6业务，不支持IPv6+能力。

分组增强型基于IPv4内核使用MPLS-TP协议，目前仅支持承载IPv6业务，不支持IPv6+能力。

◆在设备生态方面

从产业生态分析，国内可实际支持SPN、OTN且有行业项目落地的厂商有华为、中兴、烽火三家。支持IPRAN且有行业项目落地的厂商有华为、新华三、中兴、烽火、诺基亚-贝尔、锐捷等。

二、数据通信网与5G-R承载网络融合部署探索

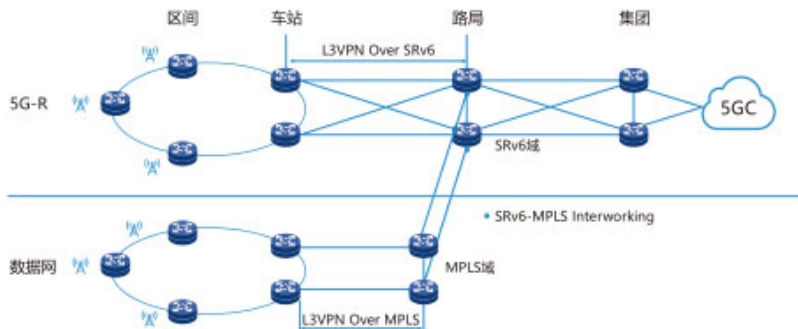
建设5G-R承载网后，原数据通信网仍将长期存在，考虑集约建设、保护投资等因素，可以考虑原数据通信网与5G-R承载网互通、逐步将原数据通信网并入5G-R承载网方案。

前期可以考虑在5G-R承载网网局与数据承载网做业务互通，5G-R承载网网局设备支持SRv6与MPLS Interworking，实现SRv6 SID与MPLS Label的交换，完成两网数据互通。

后期可考虑升级原数据通信网设备支持SRv6，平滑接入5G-R承载网。

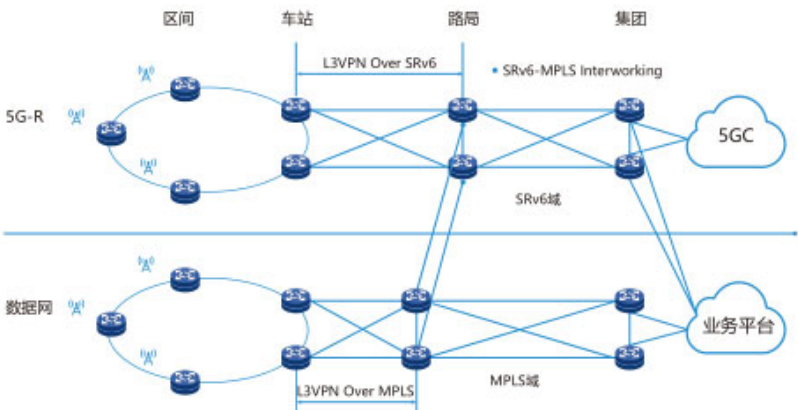
1. 互通方案

在边界设备采用SRv6-MPLS拼接技术，将数据网业务通过边界设备接入5G-R承载网，可在路局设备做SRv6-MPLS拼接。

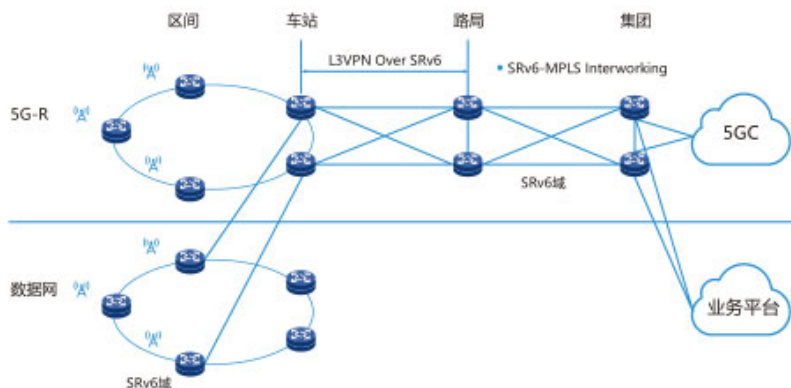


2. 数据网并入5G-R承载网

数据网设备初期不升级方案：数据网路局设备作为5G-R路局下站级设备接入，在路局做SRv6-MPLS拼接，数据网站级以上以5G-R为主用网络，数据网原汇聚、核心作为备份网络。集团业务平台同时接入5G-R核心层设备，同样以5G-R网络为主用网络，原数据网为备。



数据网接入设备升级支持SRv6后，可直接接入5G-R



综上所述，5G-R承载网和数据网业务可根据业务发展需求选择承载网络，按照发展趋势两张网络融合可减轻客户运维压力，减少建设投资。

结语

下一代铁路承载网的发展需要充分利用IPv6+及相关技术，以满足铁路系统日益增长的通信需求，并确保高效、可靠、安全的运行。以下是关于这一趋势的总结和未来发展的展望：

IPv6+及相关技术的应用

- ◆ IPv6部署：铁路系统需要大规模的IP地址分配，IPv6的大地址空间能够满足这一需求。通过采用IPv6，铁路系统可以支持更多的设备、传感器和通信终端，实现智能铁路的愿景。
- ◆ 物联网集成：铁路承载网需要与物联网设备集成，以监测和管理铁路基础设施、列车和乘客信息。IPv6+技术能够支持物联网设备的连接和数据传输，从而实现更智能的铁路运营和维护。
- ◆ 云计算与边缘计算：铁路系统需要处理大量数据，包括车辆监控、乘客信息和安全数据。云计算和边缘计算技术可以帮助铁路系统高效地处理和分析这些数据，以改进运营和安全性。

◆虚拟化与SDN技术: 虚拟化和SDN(软件定义网络)可以提高网络资源的利用率和灵活性,使铁路承载网更适应不断变化的通信需求。它们也可以支持网络切片,为不同的应用提供定制的网络服务。

◆网络安全强化: 铁路通信网络必须具备高度的网络安全性,以防范潜在的网络攻击和数据泄露。IPv6+技术中内置的安全特性和IPSec支持可以帮助确保通信的安全性。

◆高可靠性与冗余性: 铁路系统对通信的可靠性要求极高,因为它涉及乘客安全和运营。通过建立冗余路径、高可用性系统和灾难恢复机制,可以确保网络的稳定性。

◆自动化运维工具: 自动化运维工具可以加速问题诊断和故障修复,提高网络的可维护性和可用性。自动化还可以帮助减少运维成本和人为错误。

未来发展展望

未来,铁路承载网将继续演进,采用更先进的技术来应对不断增长的通信需求。随着铁路系统变得更加智能化和自动化,以下趋势可能会成为未来的发展方向:

◆5G和6G技术: 5G和6G技术将提供更高的带宽和更低的延迟,支持更多实时数据和应用,如自动驾驶列车和高清视频监控。

◆人工智能: AI技术可以用于数据分析、列车调度和预测性维护,提高了铁路运营的智能化和效率。

◆环境可持续性: 铁路系统将更加关注环境可持续性,采用绿色通信技术和能源节约措施。

◆增强现实和虚拟现实: AR和VR技术可以用于培训、乘客娱乐和列车维护,提升乘客体验和维修效率。

综上所述,铁路下一代承载网将继续利用IPv6+和相关技术来实现更高的智能化、高性能和安全性。未来的发展将积极响应新兴技术和可持续发展趋势,以满足铁路运营的不断演进需求。

铁路综合视频监控新标准实践分析

文/刘术伟

一、现状分析

铁路的安全运营离不开高效的视频监控系统,其中包括综合视频监控和专业视频监控两大部分。综合视频监控系统作为铁路安全的关键,广泛覆盖了包括工电基础设施在内的多个重要区域。它对客运车站、区间机房及其周边院落等进行全面监视,并延伸至通信、信号、牵引供电系统以及电力机房的内外部。此外,系统还重点监控车站的关键区域、公共铁路交叉点和隧道入口等,以保障铁路的畅通与安全。针对不同业务部门的需求,如调度、供电和公安等,系统提供了专门的用户终端,确保实时监控和高效通信。在专业视频监控方面,根据各业务部门的具体运营需求,铁路系统设置了多种独立的监控子系统。

铁路综合视频监控系统的结构,采用了三级存储和控制体系,涵盖车站、铁路局和总公司。这样的分层结构不仅提高了监控系统的灵活性和可扩展性,还确保了各单位能够根据自身需求进行有效的视频监控与管理,从而为整个高速铁路系统的安全运行提供了坚实的技术支撑。

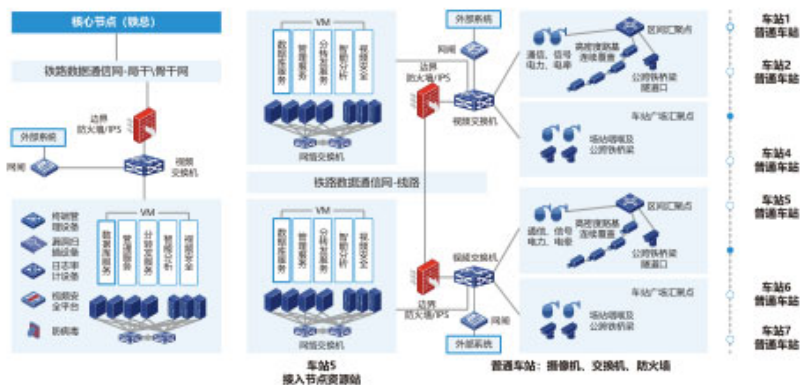
QCR 575(2022)规范中要求,铁路综合视频监控系统是应用音视频监控、通信、计算机网络、云计算、云存储等技术,构建的具有音视频数据采集、传输、交换、控制、存储、处理能力的监控系统。铁路综合视频监控系统由视频节点(包括视频核心节点、视频区域节点、视频接入节点)、前段设备(包括摄像机、NVR等设备)、网络设备和视频终端(包括管理终端、用户终端)组成。视频核心节点、区域节点、接入节点支持云计算、视频云存储技术,实现对计算资源、存储资源的统一利用与统一管理。



二、综合视频监控系统建设目标

铁路QCR 575 (2022) 标准对综合视频监控提出了创新的管理架构, 结合了一级管理与三级控制的模式, 这种结构与铁路运输管理系统紧密相连, 实现了对各管理层级的全面覆盖。这一系统的设计突出了扩容与延伸的灵活性, 同时加强了视频图像资源的高度共享性。与此相对的是, 专业视频监控系统, 尽管在基本功能和目标上与综合视频监控系统相似, 其主要聚焦于特定应用场景的监控需求。专业监控系统通常采用单层架构, 规模相对较小, 且其软硬件资源是独立设置的, 这限制了视频图像资源的共享可能性。

鉴于这些因素, 整合专业视频监控与综合视频监控系统, 构建一个统一的铁路综合视频监控云平台, 将为铁路图像资源的集中存储和管理提供一个有效的解决方案。通过这种整合, 不仅可以最大限度地利用软硬件资源和视频图像资源, 还能显著降低系统维护成本。这种一体化平台的建设, 将进一步增强铁路视频监控系统的效能, 确保铁路运输安全的同时, 提高资源利用效率和管理效能。整体架构如下图所示:



铁路视频监控系统的升级方案对网络带宽提出了新的高要求。随着沿线车站视频终端数量的显著增加, 我们面临着带宽需求与摄像机数量呈正比增长挑战。当前的Gigabit Ethernet (GE) 链路已不再足以满足视频数据的高传输需求。考虑到各车站和沿线视频终端的数量, 我们的数据链路需求至少为2000-3000Mbps。因此, 数据通信网络链路带宽只有从GE升级至10Gbps甚至更高, 才能确保视频监控系统的高效和稳定运行。以下内容暂不考虑网络带宽因素。

三、综合视频监控管理节点关键技术应用

在铁路综合视频监控系统中, 摄像机技术、编解码技术、视频存储技术、虚拟化技术、云计算技术等都是铁路综合视频关键技术, 本文仅对视频节点的云计算、云存储、安全防护等技术讨论。

1. 云计算技术

云计算是一种先进的技术模式, 它利用网络实现资源的可伸缩和弹性共享。这些资源, 包括服务器、操作系统、软件 and 应用程序, 都是通过一个物理和虚拟的资源池按需供应的。在这种模式下, 服务的提供和管理采取自助服务的方式进行, 突出了灵活性和用户控制的特点。在铁路综合视频中的云计算技术应用, 目前主要采用两种技术路径: 虚拟机 (Virtual Machine, VM) 和容器。虚拟机技术是一种操作系统级别的虚拟化, 它通过引入一个额外的虚拟化层来工作。这一层的作用是将运行在虚拟机中的操作系统指令转换为宿主机系统能够理解和执行的系统调用指令。通过这种方式, 虚拟机可以有效地与宿主机的操作系统进行异构操作, 从而实现高效的硬件利用。

与虚拟机不同, 容器是基于进程级别的虚拟化技术。容器技术完全依赖于操作系统内核的特性, 提供了一种与运行硬件无关的虚拟化方法。然而, 容器技术的一个局限在于它只能实现与宿主操作系统相同系统的虚拟化。

在铁路视频行业中, 虚拟机技术由于其成熟性和可靠性, 已经成为主流。尽管在磁盘空间占用、启动速度和资源利用率等方面, 虚拟机架构可能不如容器架构高效, 但它在视频行业的应用更为广泛。目前, 多数视频平台的主流厂商都倾向于采用虚拟机方案。

技术对比

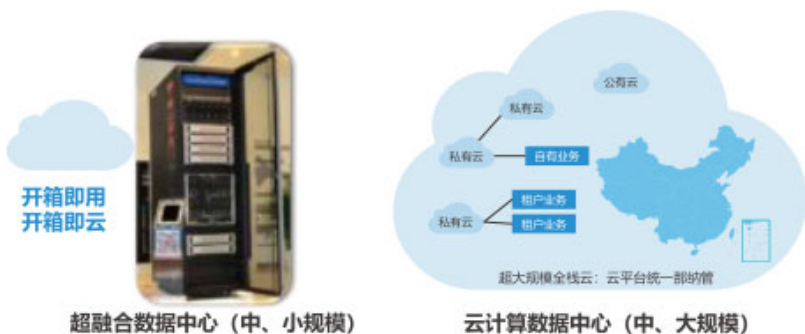
铁路综合视频监控云化建设过程中, 需要考虑哪种技术使用更适合, 在满足QCR 575 (2022) 规范的同时成本更优。虚拟化技术可以解决业务虚拟部署的需求, 但需要独立部署存储, 不能直接部署在物理服务器的硬盘之上, 否则会出现业务无法迁移的情况; 虚拟机+独立存储的方式管理相对较为割裂, 不利于后续运维管理。采用私有云或超融合集成度更高, 管理统一, 扩展性更强, 但私有云和超融合适合不同的业务场景。

私有云更适合中大规模的云计算建设, 同时所需要的基础资源相对较大, 出了至少三个管

理节点外, 还需要SDN控制器的配合, 且存储环境需要独立部署存储网络和存储设备, 成本和管理复杂度较高。

超融合技术 (Hyper-Converged Infrastructure, HCI) 作为一种集成较高的云计算技术, 更适合中小规模的数据中心建设, 铁路一体化视频建设在车站通信机房, 一般1-2个机柜部署视频业务, 超融合架构融合计算、存储和网络功能于单一系统。由一系列标准硬件单元组成, 这些硬件单元通过软件定义的方式进行管理和扩展。

综上所述, 超融合架构更适合车站云平台建设, 三台服务器节点即可为视频业务提供虚拟机、虚拟网络、分布式存储所需要资源, 保证业务安全的同时简化后续管理投入。



架构对比

超融合技术是近年来在IT领域迅速发展的一种技术, 它通过软件定义的方式将计算、存储、网络 and 虚拟化资源整合在一起。在铁路视频监控系统中, 超融合技术与传统方案相比, 展现了显著的优势。

- ◆性能: 超融合技术提供了更高的数据处理速度和更强的存储性能。与传统的物理硬件分离的方案相比, 超融合通过优化资源分配, 显著提高了数据处理的效率。
- ◆成本: 虽然超融合的初始投资可能高于传统方案, 但从长远来看, 由于其高效的资源利用和降低的维护成本, 总体拥有成本 (TCO) 更低。
- ◆可扩展性: 超融合平台的可扩展性远超传统方案。随着需求的增长, 铁路监控系统可以轻松添加更多资源, 而不需要对现有架构进行大规模的改动。

◆灵活性与简便性: 超融合平台的管理更加集中和简化, 使得系统的维护和升级更加高效, 减少了对专业技术人员的依赖。



超融合服务器选型和资源计算

按照铁路综合视频业务需求, 超融合节点物理服务器配置及超融合资源计算方式参考如下:

型号	常规服务器	其他服务器
形态	2U2节点机架	
处理器数量	2个	2个
处理器型号	4314 (2.4GHz/16核/24MB/135W)	7390 (2.7GHz/32核/64MB/225W)
内存	256GB	256GB
系统盘	480GB SATA SSD*2	480GB SATA SSD*4
缓存盘	960GB NVMe SSD*2	960GB NVMe SSD*2
数据盘	6TB SATA 7.2K 3.5in HDD*3	6TB SATA 7.2K 3.5in HDD*3
网卡	2端口10GE光接口网卡*4 (2块存储2块业务); 4端口RJ45千兆*1	
光模块	SFP+万兆模块 (850nm, 300m, LC) *4	
电源和散热	标配800W 1+1钛金冗余电源	

铁路综合视频监控系统一般包括数据库服务节点、管理服务节点、分转发服务节点、智能分析节点、网管&告警及事件存储节点、区域互连节点、图形诊断管理节点等。按照各类业务性能和数量需求来计算所需硬件服务器数量, 以下按照3600路视频规模参考业界常规视频服务资源消耗为例。(其中, 分转发服务器和视频节点数量相关, 每台分转发服务器预计可接入200路高清视频)

以上业务除视频分析诊断服务需要16核vCpu、32G内存和1000G存储外, 其他服务仅需要4核vCpu、16G内存和500G存储空间, 整体所需资源如下表:

单台虚拟机需求					虚拟机需求总数		
虚拟机名称	虚拟机数量	VCPU需求	内存需求	磁盘需求	VCPU数量	内存数量	硬盘容量
管理虚拟机	3	4	16	0.5	12	48	1.5
分转发虚拟机	18	4	16	0.5	72	288	9
网管、告警、事件存储虚拟机	1	4	16	0.5	4	16	0.5
区域互联虚拟机	1	4	16	0.5	4	16	0.5
图诊智能分析虚拟机	2	16	32	0.5	32	64	1
图诊管理虚拟机	1	4	16	1	4	16	1
备用虚拟机	2	4	16	0.5	8	32	1
总数	28				136	480	14.5

服务器资源计算如下:

CPU资源无超配比(分配给虚拟机或容器的CPU资源在理论上超过了物理CPU的实际容量)情况下, 总CPU资源(核心数)=物理CPU核心数×每核心的超线程数(如果启用)×颗数×(100%-29%虚拟化开销), 以上表常规服务器CPU型号计算, 单台服务器总CPU资源=16×2×2×71%≈45个vCpu, 三台服务器预计136个vCpu资源。如果CPU按照2倍超配比计算, 可用vCpu数量为268个, 铁路业务对可靠性要求较高, 建议资源计算不考虑超配比情况。如果参考表格中其他服务器, 由于单CPU核数为32核, 虽然比常规服务器降低约40%的性能, 但整体规格提高一倍, 所以也可满足136个vCpu的需求。

可用内存计算公式如下: 总内存=物理内存数量×(100%-20%虚拟化开销), 以上表常规服务器内存容量计算, 单台服务器可用虚拟化内存容量=256G×80%≈205G, 三台服务器可总内存容量为615G左右。如采用其他服务器, 也可实现600G左右的可用内存容量。

可用存储容量计算公式如下: 2副本可用容量=硬盘数量×硬盘容量×93%(可用比例)×(100%-15%开销)×50%(2副本50%/3副本30%), 以上表为例, 2副本可用容量=3×6×93%×85%×50%≈7.1TB可用容量, 三台服务器约为21TB整体可用容量。

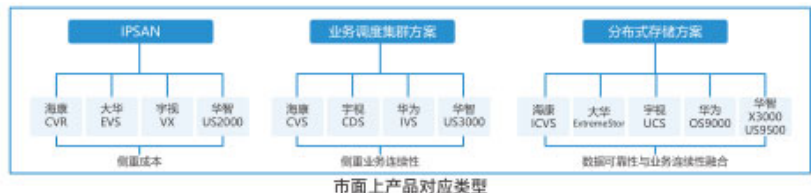
综上所述, 超融合采用常规服务器的情况下, 三台常规物理服务器或其他服务器均可满足3600视频节点所需的, 136个vCpu|480G内存|14.5T存储空间的要求, 为保证单节点故障

业务可顺利迁移, 实际项目中建议设备数量为N+1或N+2, 其中N为满足视频业务需求最低资源, 以保证业务高可用和应对突发业务增长。

2. 云存储技术

铁路视频云存储重点在于安全、高效地存储和管理大量的铁路视频数据。这种系统具备高度的安全性、大规模数据处理能力、实时数据传输和存储功能, 同时提供易于访问和共享的界面。它还包括重要的备份和灾难恢复功能, 并严格遵守行业合规性标准。云存储解决方案对于提高铁路运营的效率 and 安全性、优化资源管理和成本效益至关重要。视频类存储主要有单机磁盘阵列、IPSAN集群、分布式云存储等, 几类存储对比如下:

- ◆IPSAN(单机磁盘阵列): 经济, 性能低, 可靠性仅依靠单机RAID, 规模适应性弱(几台)。
- ◆业务调度集群(IPSAN集群): 业务层面实现集群管理, 支持单节点故障业务迁移接管, 规模适应性居中(几台~几十台)。
- ◆分布式云存储(纠删云存储): 数据层面拉通, 单机故障业务及数据均不受影响(几台~上百台)。



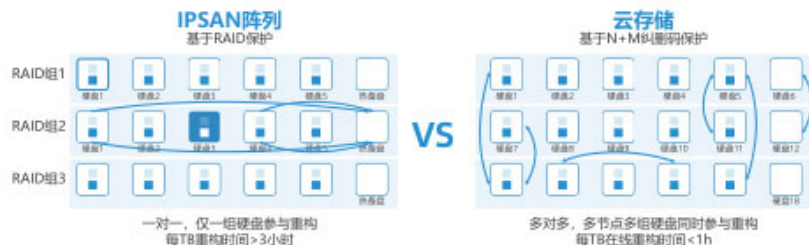
技术对比

IPSAN(IP存储区域网络)和云存储是两种不同的存储技术, 主要区别在于部署方式、可扩展性、成本和数据安全性。IPSAN是一种在内网中部署的存储解决方案, 提供高性能和低延迟, 适合单站部署和高速数据访问的应用, 如果多个车站共享的需求则无法满足。相比之下, 云存储是一种灵活的远程存储服务, 它允许用户根据需求随时扩展存储空间, 可部署在铁路任意车站, 其他车站只需要网络可达即可访问, IPSAN和云存储技术对比如下:

IPSAN与云存储技术发展趋势:

- ◆冗余策略: JBOD→RAID→纠删码/副本, 相比IPSAN云存储采用纠删码或副本方式可靠性更高。

- CPU架构: Grantley Platform→Purley Platform→C86, CPU架构支持目前主流的CPU平台。
- HDD单盘容量: 4T→6T→8T→10T→14T→18T-20T, 云存储当前单盘支持20T容量。
- 存储介质: HDD→SSD+HDD, 相比IPSAN云存储可采用SSD缓存+HDD模式, 性能更高。
- 数据重构速度: 10小时/TB→2TB/小时, 相比IPSAN云存储数据重构速度更快。



IP SAN存储特点:

- 竖着存: 摄像机和存储设备绑定, 不能跨主机分配资源
- 低可靠: 节点故障, 对应业务中断, 录像丢失无法恢复
- 低性能: 录像读写性能取决于单节点性能
- 扩展难: 扩容只能纵向增加扩展柜, 扩容受限

云存储特点:

- 横着存: 摄像机录像分散存储在节点, 可跨主机分配资源
- 高可靠: 单节点损坏业务不中断, 数据不丢失
- 读写快: 分布式存储和下载, 人多力量大
- 扩展易: 横向扩展, 系统性能和容量随节点增加线性扩展



可见, 从技术角度看, 云存储更适合铁路综合视频的发展特别是铁路一体化视频的建设要求。

架构对比

云存储和IP SAN存储在设计、性能和适用场景方面有所区别:

• 技术架构: 云存储依托于云计算技术, 提供了更为灵活和动态的数据存储解决方案。与传统的IP SAN相比, 它不依赖于物理存储设备的位置和配置, 而是通过虚拟化技术实现资源的最优化配置和使用。

• 数据管理: 云存储提供更加高效和智能的数据管理机制。它能够根据数据访问频率和重要性自动优化存储, 而IP SAN则需要更多的手动配置和管理。

• 扩展性与灵活性: 云存储在扩展性方面具有明显优势。随着铁路视频监控需求的增长, 云存储可以迅速增加存储容量, 而IP SAN的扩展则受限于物理硬件的限制。

• 成本效益: 虽然IP SAN在初始投资方面可能较低, 但云存储在运营成本、维护成本以及长期的可扩展性方面具有更大的优势。

• 安全性和可靠性: 云存储通过多重备份和分布式存储技术提高了数据的安全性和可靠性。相比之下, 传统的IP SAN由于依赖单一或有限的物理位置, 可能面临更高的数据丢失风险, 所以, 云存储更适合铁路综合视频监控系统建设。

同时云存储分为对称式云存储和非对称式云存储, 两种不同架构各有优劣, 但对称式云存储在设计上更简单、扩展性更强, 适用于处理大量均衡的工作负载; 而非对称式云存储则提供了更灵活的资源分配和任务专业化, 适用于更复杂或需求不均匀的应用场景。铁路综合视频监控系统由视频分发节点统一转储数据, 相对均衡, 所以, 对称式存储更适合铁路一体化视频的建设。



对称式云存储选型和资源计算

为了有效管理视频监控数据, 采取的是云存储策略, 即根据摄像机的分布情况, 在一条铁路线路中选取两个车站作为视频接入节点, 在这两个车站部署分布式云存储。这种布局策略的关键是根据接入的摄像机数量合理估算所需的云存储容量。

针对视频存储算法如下:

◆ 视频容量 = (码流大小 × 接入路数 × 3600s × 24h × 存储天数) / 8 / 1024 / 1024 = XXTB

考虑文件系统损耗/码流波动/满覆盖预留等上层业务的损耗, 预留5%空间

为保证节点故障后的业务接管, 预留5%空间

◆ 磁盘可用容量使用率: $1/1.024/1.024/1.024/1.024=91\%$

需求容量: $xx \times 1.05 \div 95\% \div 91\% \div 66\%$ (纠删码) = xxTB

◆ 计算硬盘数

有效硬盘数量 $D = \text{容量需求} \times \text{TB} \div \text{单个硬盘容量TB}$ (向上取整)

硬盘容量可选4T/6T/8T/10T/12T/14T/16T/18T

◆ 设备数量

主机数量 $N = D \div \text{单节点有效盘个数}$ (向上取整)

每台主机磁盘数 $P = D \div N$ (向上取整)

总硬盘数 $S = P \times N$

以3600路4M码流视频存储90天为例如下:

视频容量 = $4 \times 3600 \times 3600 \times 24 \times 90 / 8 / 1024 / 1024 = 13348\text{TB}$

需求容量 = $13348\text{TB} \times 1.05 \div 95\% \div 91\% \div 66\% = 24564\text{TB}$

有效硬盘数A (18T) = $24564\text{TB} \div 18\text{T} = 1365\text{块}$

有效硬盘数B (8T) = $24564\text{TB} \div 8\text{T} = 3071\text{块}$



主机数量A (60盘位18T主机,
数据存储58块) = $1365 \div 58 \approx 24\text{台}$



主机数量B (24盘位8T主机,
数据存储23块) = $3071 \div 23 \approx 134\text{台}$

经过计算, 3600路4M码流视频的云存储配置, 共需要15台A类云存储或85台B类云存储; 按照常规云存储配置, A类4U云存储共需要125U左右机柜资源 (3机柜), B类2U云存储共需要400U左右机柜资源 (10个机柜)。

总体来说存储容量的计算依据摄像机捕获的视频内容的重要性进行差异化管理, 基于1080P分辨率的视频流, 我们按照4Mbit/s (采用H.264编码) 的标准来估算所需的存储空间。在考虑到硬盘的冗余开销后, 实际可用空间约为硬盘标称值的67%。据此, 我们可以计算出单路摄像机在不同存储周期下所需的存储容量:

- ◆ 对于3天的视频存储, 所需的存储容量约为0.185TB
- ◆ 对于15天的视频存储, 所需的存储容量约为0.923TB
- ◆ 对于30天的视频存储, 所需的存储容量约为1.845TB
- ◆ 对于90天的视频存储, 所需的存储容量约为5.535TB

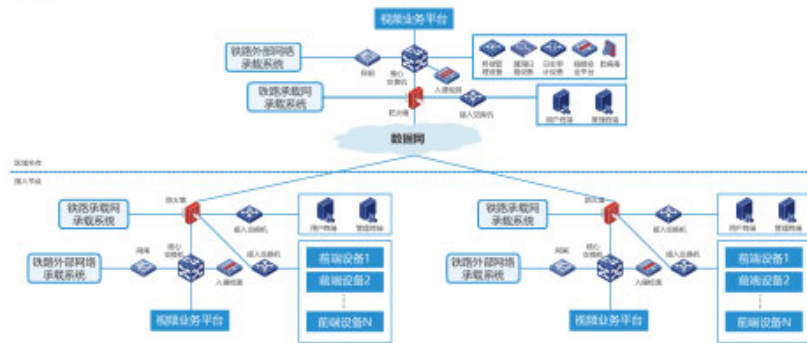
这种计算方法确保了存储容量的合理分配和高效管理, 满足不同级别视频内容的存储需求。

3. 安全技术

在构建符合国家网络安全法律法规、铁路行业标准及Q/CR 783.4要求的视频接入云节点时, 以下专业化的网络安全要求需得到严格遵守:

- ◆ 同步化安全策略: 确保网络安全措施在云节点的规划、建设和使用阶段实现同步化实施。
- ◆ 弹性虚拟化安全防护: 部署具有动态适应能力的虚拟化安全设备 (如虚拟防火墙、VPN、IPS、虚拟审计系统), 以适应业务环境的变化。
- ◆ 独立安全管理区域: 建立专门的安全管控区, 确保所有物理和虚拟资源的操作仅通过该区域, 并实施严格的操作审计和权限管理。
- ◆ 物理/虚拟边界防护: 在物理和虚拟边界处实施访问控制、入侵防御、恶意软件防护和安全审计技术。
- ◆ 综合安全应用服务区: 在物理/虚拟应用服务区域中集成身份验证、访问控制、安全审计、入侵防范、恶意代码防护、数据完整性与保密性、剩余信息保护等技术。

- ◆前端设备区安全措施: 确保物理/虚拟前端设备区具备身份验证、访问控制和安全审计功能。
- ◆终端设备区安全增强: 在物理/虚拟终端设备区实施身份验证、访问控制、安全审计以及数字水印技术。
- ◆统一安全管理与监控: 实现对视频接入云节点资源的统一安全管理, 包括对关键业务和应用资源的持续安全监测、集中展示、安全事件主动发现、分析、预警、溯源, 以及态势感知和及时的安全事件处理。
- ◆加密技术保护API: 对所有应用程序接口(API)进行加密处理, 确保资源访问接口的安全性。



这些高级安全措施的实施旨在加强视频接入云节点的整体安全防护, 确保其在符合相关法规和标准的基础上, 能够有效防范各类安全威胁, 保障数据的安全性和完整性。除此之外, 安全管理平台是视频安全管理的核心平台, 对安全资源管理、安全事件分析、安全风险评估等基础功能, 对视频终端类型、厂商、所属区域、风险视频终端状态及区域分布进行分析展示, 全方位解读视频终端安全态势。(注: 文中提及摄像机等监控设备非新华三技术有限公司提供)

结语

铁路视频节点的云化架构、先进的网络和信息安全技术, 显著提升了综合视频监控系统的智能化水平, 有效促进了系统建设的整体性能。铁路综合视频监控系统在现有基础上拓展了监控范围, 实现了各类专用视频系统的统一管理和资源共享, 优化了资源配置。在具有优质机房条件和维护环境的车站集中部署接入节点, 极大提高了运营和维护效率。云计算和云存储技术的应用, 显著增强了系统的容错能力, 提升了安全性、可扩展性和可维护性, 进而优化了铁路行业整体系统性能。



从“中国智慧”到“中国速度”， 以云服务助力雅万高铁数智求变

文/张仁琳

2023年10月17日，全长142.3公里，最高运营时速350公里的雅万高铁正式开通运营，成为中印尼共建“一带一路”合作的“金字招牌”。雅万高铁贯通印度尼西亚首都雅加达和旅游名城万隆的“大动脉”，将两座城市的交通时间从3小时缩短至40分钟，开通运营首月累计发送旅客38.3万人次。

作为印尼和东南亚的首条高速铁路，雅万高铁全线采用中国技术、中国方案、中国标准，被誉为中国高铁全系统、全要素、全产业链走出国门的“第一单”。是中国与印尼友好务实合作的代表作，并且对实现“一带一路”以及印尼经济发展都具有重要意义和价值。

正因如此，这条高铁自建设开始就背负着不一般的历史使命，所以在建设上也设定了前所未有的高标准。在尤为重要的数字化层面，中国国家铁路集团有限公司作为建设和运营主体，为其制定了一整套完善的“N+1”智能化建设目标，其中N是指智能票务、智能车站等应用系统，1则是指一个数据中心基础平台。为了更好地保障数字化平台的规划建设，国铁集团选择了紫光股份旗下新华三集团，联手打造出了融合前沿数字化创新的高铁云底座，为高铁运营、管理和服务提供强有力的支撑，提供了完整的云平台解决方案，除了云平台外，还提供了网络、安全、服务器、分布式存储等相关产品，在海外共建“智慧高铁”。

一、拥抱数字化，引领六大核心业务系统加速上云

为杜绝数据孤岛、标准不一，建造稳定可靠的雅万高铁数据中心基础平台，新华三集团以云化设计理念和深厚的铁路云平台建设经验，在安全生产网和外部服务网分别构建两朵云平台，安全生产云平台承载雅万高铁六大核心业务系统：动车组管理信息系统、风雨及异物侵限监测大数据分析系统、智能票务系统、智能车站系统、智能综合调度系统、高铁基础设施视频大数据应用系统，外部服务云平台承载互联网售票系统，实现资源的安全隔离。

通过两朵云，充分对分散在各系统中独立配置的硬件、网络、安全、系统软件等资源进行整合，实现系统资源的共享共用、统一运维和灵活调配。也方便了客户后续根据需要对系统进行必要的调整和扩充，可弹性扩充因增加新的应用所需的计算资源、存储资源和网络资源等。

如今，雅万高铁已经成为了一条真正在“云上”行驶的智慧高铁，从高铁运行环节智能化的调度指挥、风险因素的感知和识别，到旅客服务过程中简单便捷的数字购票手段、丰富多元的智能候车体验，数字化平台的构建让雅万高铁在运营管理、服务体验等各个环节都有了显著改进。

二、链接未来，为智慧高铁升级进化构建扎实底座

对于雅万高铁的乘客们而言，看得见的是智慧、便捷的出行体验，但看不见的是数据的“云上穿行”。在底层平台的构建上，新华三提供了全栈高铁云平台解决方案，包括网络、安全、服务器、存储等相关产品，充分发挥自身在算力、存储和智能联接等层面的全面实力，构建了一个功能强大、高效可靠的基础设施平台。

在资源管理层面，依托云平台对计算、存储、网络资源等基础设施进行统一管理，将资源封装以服务目录的方式展示给用户，同时可以将用户需求转换为配置指令，实现按需分配、灵活调用、降本增效。

在存储层面，利用新华三存储方案让雅万高铁能轻松应对运行过程中全生命周期的海量结构化、非结构化数据以及相关的外部数据，为未来智能应用的创新提供全方位的大数据支撑。

雅万高铁依托新华三云平台数字化底座突破了传统数据中心管理中存在的资源瓶颈、信息孤岛、标准不一、系统复杂、服务水平低下等问题，帮助客户实现了云化模式转型。让基础设施能够随需扩展，灵活调用。并且基于稳定可靠的IaaS服务能力，有效拉通数据中心基础设施资源；并为后续PaaS服务的演进提供了重要基础。帮助客户实现标准化提升、智慧化提升、效率能力的提升、以及成本效益的提升，为后续上层PaaS服务的部署和演进打好了扎实基础，不仅满足了当下的业务需求，更能支撑雅万高铁未来的长远发展。

新华三提供的产品方案及服务，有效保障雅万高铁信息系统安全高效运行，为“中国高铁”名片贡献力量。

随着雅万高铁正式投入运营，这条备受瞩目的世界性工程将在推动当地经济、造福一方居民上发挥更大的作用和价值。新华三集团也将秉承着“精耕务实，为时代赋智慧”的理念，让全面领先的数智创新走出国门，参与更多海外重大工程的规划建设，以“中国智慧”点亮中国基建的新名片。

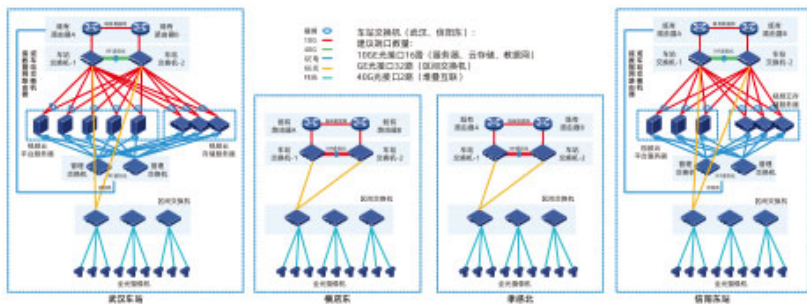
京广高铁（武汉）综合视频一体化云平台

文/王雪梅

京广高铁纵贯中国南北，跨越长江与黄河，沿途囊括高山、平原、丘陵等各类地貌，始于北京丰台站，途经石家庄、郑州、武汉、长沙等地，终到广州南站，全长2291公里，是世界上运营里程最长的高速铁路；京广高铁武汉铁路局管段设有武汉站、横店东站、孝感北站、信阳东站、明港东站、驻马店西站、漯河西站等7个车站。本次视频监控系统建设包括区域中心、视频云平台、视频采集点和终端设备组成，全线采用1080P全数字高清视频监控系统。

一、铁路综合视频一体化云平台解决方案

新华三采用云计算、云存储等技术的云架构设计，为铁路视频平台云化改造提供了强有力的支持。相较于传统综合视频监控系统设计方案，一体化综合视频监控系统将原有的7个视频节点减少至2个（武汉、信阳东站），实现了从传统的多节点系统到一体化系统的升级，能够实现虚拟化存储容量管理、在线维护和调整、数据保护等功能。该项目方案涉及云存储、交换机、服务器及超融合软硬件等产品，由视频核心节点、视频区域节点、视频接入节点、视频采集点、用户终端以及承载网络组成，在武汉站和信阳东站，分别采用超融合技术和分布式架构的云存储构建了视频云平台，能够提供更灵活、高性能的视频处理和存储能力，并实现全场景视频云边智能协同。这种改造还提高了业务时效性和数据覆盖范围，并确保了视频性能的稳定性，为其提供了高可靠性、高安全性和易扩展的技术方案。此外，新华三还为铁路视频平台提供了高可靠性的网络产品支持。在武汉站和信阳东站，新华三部署了高密度的万兆交换机，这些交换机提供了高带宽、高可靠性和低延迟的网络传输性能，保障了云平台 and 云存储的高速转发需求，为铁路视频平台的云化改造提供了可靠的网络基础。



二、方案价值

新华三为铁路视频平台进行了云化改造，使其能够更好地应对不断增长的视频处理和存储需求，让平台的运行更加高效和安全。改造后的平台可以实现统一的管理和监控，方便客户使用。同时，平台还可以根据需求进行灵活的部署和扩展，满足不同规模的需求，平台还采用了高可靠性和容灾备份技术，确保平台始终可用，并保护数据安全，为铁路视频平台保证了始终可用和数据安全的高质量监控保障服务。通过这些改造和支持，铁路视频平台能够提供更好的使用体验和价值，为客户提供更高质量的监控保障服务。



05

云港联动、智慧领航

第38章	新型数字化技术在智慧港口的应用浅析	240
第39章	浅谈双碳背景下智慧绿色港口建设之路	248
第40章	浅析人工智能在港口安全应急的应用	255
第41章	数智赋能航道 安全与效率齐升	260

新型数字化技术在智慧港口的应用浅析

文/葛云峰

港口作为集疏运节点，在综合运输体系中发挥着举足轻重的作用，其发展水平在很大程度上是一国物流发展水平的体现。随着高新技术的迅猛发展，云计算、物联网、大数据、人工智能等信息技术愈发成熟，为我国各大港口向智能化方向转型提供了重要的技术支持。智慧港口的建设是增强港口综合竞争力的重要手段，智慧港口已成为我国未来智能交通系统的主要发展方向。

一、当前港口发展现状

我国目前已经形成环渤海、长江三角洲、东南沿海、珠江三角洲和西南沿海5个港口群，煤炭、石油、铁矿石、集装箱、粮食、商品汽车、陆岛滚装和旅客运输等8个运输系统布局。水运承担了全国90%以上的外贸物资运输和大量的跨区域物资交流，在促进经济发展、支撑全面对外开放、保障经济安全等方面发挥了重要作用。虽然港口发展取得了长足的进度，但也面临着几个重大问题：

港城矛盾：随着城市边界逐步扩张，土地资源越来越稀缺，港口发展空间逐渐受到挤压。在沿海地区，越来越多的枢纽性港区处于城市包围中，港口与城市在发展空间、集疏运通道等方面的矛盾高发。“大港大城”型城市陆续实施“港退城进”，甚至出现“去港口化”倾向，“大港小城”型城市的港城冲突也趋加剧，即使部分新兴枢纽性港区在发展初期即面临港城矛盾。港城矛盾的高发，沿海港口核心资源被挤占的风险逐渐增大。

竞争压力：我国港口物流市场竞争日趋激烈。由于各个港口对接国际贸易的不断加强，国际货运企业也越来越多地进入中国市场参与竞争。同时，各地方港口之间也加强相互竞争。这些竞争对于一些港口来说，可能会失去部分货源，而对于整个港口物流市场来说，竞争则促进了其市场化和效率化运作。

物流体系升级：我国的物流体系日渐完善，快递、第三方物流等新一代物流企业崛起，当前，物流服务已经从简单的货运转变为更加注重时效性、可追踪性和服务质量等方面的综合化物流服务。因此，港口物流企业需要不断完善自身服务经营模式，提升服务水平，借助新技术提高物流效率，以适应不断升级的物流体系。

面临港口发展的各种困境与挑战，各港口企业在不断降低港口投资强度的同时，港口基础设施投资呈现智能化、信息化、综合化趋势。而智慧化转型，正成为港口企业应对行业不景气、自身供给能力过剩、提升核心竞争力等共同方向。

在2019年11月，交通运输部联合财政部、发改委等九个部门共同发布了《关于建设世界一流港口的指导意见》（以下简称《意见》），《意见》中指出绿色、安全、智慧、融合是未来港口的发展方向，并提到未来港口总体发展目标：“到2025年，世界一流港口建设取得重要进展，主要港口绿色、智慧、安全发展实现重大突破，地区性重要港口和一般港口专业化、规模化水平明显提升。到2035年，全国港口发展水平整体跃升，主要港口总体达到世界一流水平，若干个枢纽港口建成世界一流港口，引领全球港口绿色发展、智慧发展。”其中智慧港口是未来港口建设的核心。

二、智慧港口的建设目标及整体框架

业界普遍认为，智慧港口是以现代化基础设施及物流设备为基础，以云计算、大数据、物联网、移动互联网、人工智能等新一代信息技术与港口运输业务深度融合为核心，实现港口运输要素的全面感知，构建上下联动、纵横协管的智能物流服务体系，实现港口资源的整合和综合开发，促进资源共享，从而实现降低港口作业成本，提升港口服务水平，拓展港口经济腹地和提高港口企业效益的目标。



图1 智慧港口框架图

智慧港口应包含几个部分：

- ◆智能终端，实现港口信息的动态采集、实时通讯，建立港口智能感知和监控体系。
- ◆ICT基础设施，实现数据传输、数据交互、数据处理，构建智慧港口的底层基石。
- ◆智能数字平台，实现资源的整合与共享，数据的挖掘和分析，提供全域数据接入、一站式数据治理、智能化数据分析与统一数据服务的能力，承载各类港口智慧化应用。
- ◆智慧应用，以港口业务为落脚点，提供相应的智能子系统，为港口自动化、智能化化管理提供支撑。包括码头作业系统、智能闸口系统、智能安全防护系统、综合物流系统等。

三、新型数字化技术在港口的应用

1. 混合云在港口的应用

云计算从用户角度主要分为公有云、私有云以及混合云。港口用户可以根据自身不同的需求，来选择不同的云计算模式。

公有云是对公众开放的云服务，能支持数目庞大的请求，而且因为规模的优势，同时公有云的成本比较低。但是公有云也有很多不足之处。虽然公有云也有很好的安全方面的措施，但由于数据不在港口企业本地，企业难以控制云服务的稳定性和可靠性。与公有云不同，私有云主要是为港口内部提供云服务，不对公众开放，在企业的防火墙内工作，并且IT人员能对其数据安全性和服务质量进行有效控制。而私有云也有自己的不足之处，那就是前期投入大，还需要专业的云计算团队来持续运营，这导致了中小型港口难以搭建自己的私有云。



图2 混合云架构图

混合云结合了公有云和私有云的优势，是近年来云服务的主要模式和发展方向。一些大型港口既希望获得私有云的可定制优化、安全可控、稳定可靠，又想具备公有云灵活弹性、低运维成本，同时满足用户对于可靠和敏捷的需求。在这种情况下，港口企业可以把一些对外业务或辅助类业务部署在公有云上，如大量的文档存储，电子邮件处理，开发测试业务等。而把港口核心的业务处理留在私有云上，比如码头生产作业、智能闸口系统等等，通过混合云管理平台将私有云和公有云进行统一管理和运维。

港口混合云方案自动实现了大二层网络互通，让私有云和公有云混合部署，轻松实现跨云的网络自动配置。混合云方案可以提供统一服务目录，用户可以在获得一致的服务体验。同时提供了统一的管理服务平台实现云资源统一服务申请、运营、统一监控，业务跨云迁移和容灾，让用户使用和监控公有云资源更加方便，大幅降低了多云带来的运维工作量。

2. 人工智能在港口的应用

当前人工智能在港口的应用还处于初级阶段，主要集中在港口生产作业和安全管控方面。比如在闸口、岸桥、场桥等节点部署智能感知终端，在装卸船、堆放、理货、验残、提箱、出关等环节，对集装箱的全流程识别，包括集装箱箱号的识别，集装箱的验残，集装箱防吊起等等。人工智能视觉识别相较于传统的人工识别、OCR识别等方式，降低了投入成本，提升了识别准确率，大大提高了港口的生产效率。

在安全管控方面，我们可以通过将智能感知终端部署在闸口、周界、内部道路、重点区域、办公区、作业区等区域，实现不同场景的安全保护以及视频识别功能，来保障整个港口的安全。比如在闸口实现车牌识别和人员管控；通过在港口周界部署智能感知终端实现人员入侵防控，也可以解决港口内部道路交通阻塞、车辆超速问题；在重点区域监控贵重货物或危化物；在办公区实现人脸门禁，刷脸考勤、访客登记；在作业区可以通过智能感知终端识别出作业人员是否佩戴安全帽、反光衣等等。



图3 人工智能辅助港口运营生产

为了更加方面管理这些人工智能算法，我们可以使用开放算法仓库，让算法与平台解耦，规避厂商绑架，实战中可按需选择各场景中最优算法，多种算法调度策略，保障系统高效、灵活，有效辅助港口的运营生产。

3. 物联网在港口的应用

物联网技术也是建设智慧港口中一项重要新型数字化技术。通常对港口物联网概念抽象的定义是指充分借助物联网、传感网、云计算、决策分析优化等智慧技术手段进行透彻感知、广泛连接、深度计算港口供应链各核心的关键信息，实现港口供应链上的各种资源和各个参与方之间无缝连接与协调联动，从而对港口管理运作做出智慧响应，形成信息化、智能化、最优化的现代港口。具体而言，港口物联网综合使用无线传感器网络、RFID、移动通信及宽带通信等技术，对闸口管理、码头管理、堆场管理、车辆定位、人员管理、货品跟踪等方面进行综合运营管理。



图4 物联网应用于智慧港口

港口在物联网有着很多需求，主要有3个方向：

设施设备检测

港口基础设施覆盖整个港口，检测困难，无法快速发现问题。同时港口设备众多，关键设备或易损部件的健康度需要频繁检测。涉及危险品运输的码头对危险品泄露监测缺乏有效手段。通过物联网可以结合监测数据合理有效的实现设备远程控制和自动控制。同时可以通过各类传感器收集数据，分析并及时发现异常，对于关键设备或易损部件的健康度进行告警管理。还有港口环境监测，相应的模组可以收集上传空气温湿度、CO₂、有毒气体（NH₃、H₂S）、积水高度等参数，异常时预警，实现环境监测及危险品泄露监测。

能耗管理

港口不停息运行，且每日能耗巨大，缺乏对于能耗的精准管理。运营部门对于各种能耗（电、水、油、气）需分开管理，运维困难。通过物联网可以实时掌握水电情况，管控港口每日能耗情况。如果水电等能耗突增，可以及时发现，快速解决。其次是地下管道检测，通过物联网可以收集管道日常运行数据，巡检维护数据。可以对管道环境检测、设备监控、动力监控等各类监控和告警数据及时上传管理。此外，对于港口电源、电灯、路灯等设备，根据港口具体业务开启关闭能源设备，合理有效减少能耗开支。

人车物定位

随着物流业的迅猛发展，集装箱货运量上涨，往返于码头和后方堆场、运载集装箱的港区集卡车数量也不断增加。所以必须对港区内的工作人员、车辆、货物进行精准管理。对人车物的定位主要依靠RFID、GPS/北斗卫星等技术。人员定位标签包括智能手表、智能工卡、智能安全帽等，车辆集装箱定位主要依靠车载终端、或RFID标签等，针对港口集装箱车辆的实时位置、动态皆可随时获知，在管理平台上清晰展现。便于管理人员，及时掌握相关信息，确保安全运行。定位系统全面记录集装箱的历史活动轨迹，输入信息可查看其运输路线、在某区域停留时长等数据，便于监督管理，优化作业流程。

4. 5G在港口的应用



图5 港口5G网络架构

作为第五代移动通信技术，5G相较于4G在性能上有了很大的提升。具体来说就是eMBB大带宽，峰值速率达到10Gbps，平均吞吐率数百兆；mMTC海量连接，可以支持百万级的并发

连接；uRLLC低时延，空口时延低至1ms。这使得5G在未来商用领域有很大的应用前景。对于港口来说，提升货物转运效率是港口的核心业务诉求，货物的转运重点集中在集装箱堆场和桥吊作业区域，而具备大带宽、海量连接、低时延能力的5G技术，适用于港口集装箱全流程识别、垂直装卸远程控制、水平运输远程控制、视频监控与AI识别等应用场景。

港口5G专网的建设模式有三种，分别为虚拟切片、虚拟切片+边缘计算、物理切片。

- 虚拟切片：将运营商5G大网（包括5G无线网、传输网和核心网）通过网络切片方式划分出部分虚拟资源用于港口用户，各个切片港口用户和公众用户使用同一套物理资源，但在逻辑上是独立的。

- 虚拟切片+边缘计算：将运营商5G大网（包括传输网和核心网）通过网络切片方式划分出部分虚拟资源用于港口用户，港口业务数据无需传输到运营商核心网，在港口本地边缘进行计算。

- 运营商为港口用户建设独立的5G小基站和本地核心网，信令流和数据流都在本地处理，与运营商大网物理隔离。只存在远程网管维护通道。

港口5G专网具体选择哪一种模式，需和运营商一起根据业务需求以及建设成本等因素综合考量确定。从当前建设情况看，港口5G专网以虚拟切片和虚拟切片+边缘计算的模式居多。

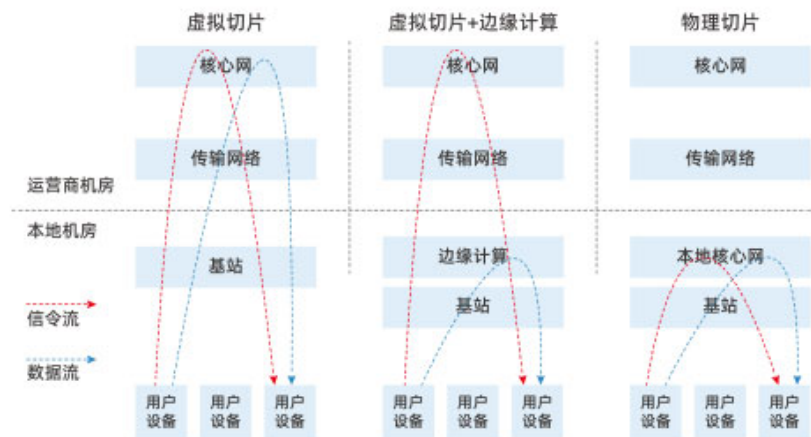


图6 港口5G建设模式

5. 区块链在港口的应用

港口运输提单电子化是未来货物提单发展的重要方向，目前基于EDI技术的电子提单模式可以有效的解决纸质提单的流转效率、流转成本和提单诈骗等问题，但存在电子化程度过低、责任分配不均及安全保障机制不够完善等问题。纸质提单容易被仿造、倒签，也可能由于被仿冒或者填写误差等原因产生诸多安全信任问题。区块链技术具有不可篡改、安全透明、智能合约和可验证性的特点，为解决电子提单在货物运输中的转让和占有问题提供新方向。



图7 传统提单流程

基于区块链的电子提单所涉及到的贸易信息是在区块链网络上使用电子密钥来发起、转让、更改、存储提单信息，避免提单被仿造、丢失、修改，只有交易方的私人密钥才能访问，是客户、码头、堆场、供应商、政府监管部门等物流参与方的交接凭证，可确保电子单据安全存储并且不可篡改。



图8 区块链在港口电子提单的应用

未来展望

尽管云计算、人工智能、物联网、5G、区块链等一系列新型数字化技术在港口行业中的应用还面临着诸多问题，但随着技术不断的发展完善，这些问题会得到解决。对新型数字化技术在港口行业中的应用的研究，将加快数字化技术在港口行业中的落地应用，实现港口泊位大型化、作业自动化、物流综合化、运营智能化，进一步提升港口生产效率、降低运营成本，打造高效安全、极致便捷、开放协同的智慧港口。

浅谈双碳背景下智慧绿色港口建设之路

文/葛云峰

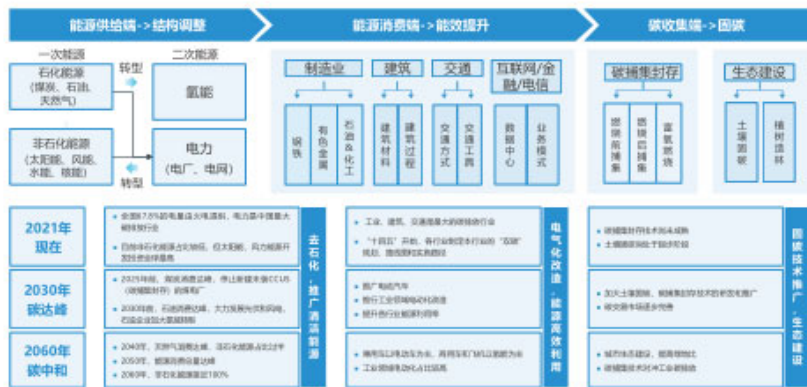
随着全球气候变化和环境污染问题的日益严重，各国政府和企业纷纷采取行动，推动可持续发展。中国政府提出了“双碳”目标，即碳达峰和碳中和，旨在减少碳排放，保护生态环境。在这一背景下，智慧绿色港口建设成为了行业发展的必然趋势。

一、双碳背景

早在2009年哥本哈根世界气候大会中，中国就承诺了到2020年的碳减排目标，并于2019年全部实现。在2020年我国提出二氧化碳排放力争于2030年达到峰值，2060年实现碳中和，也就是我们的“双碳战略”。中国积极承担了“碳中和”责任，将减排从承诺提升到国家战略层面，并正在采取实际行动和制定具体的时间表、路线图及顶层设计方案。

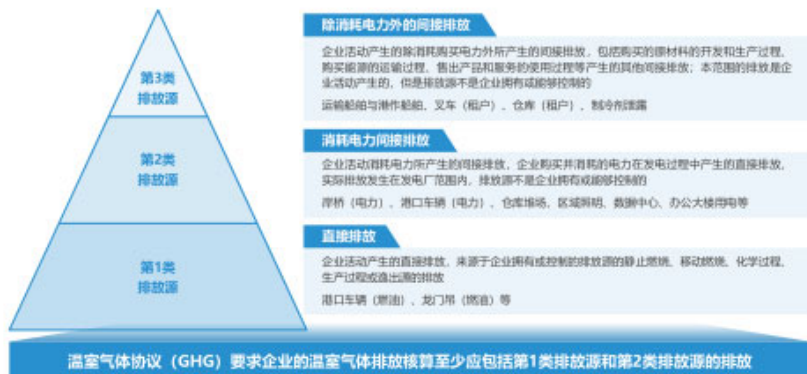
2009年12月	2015年11月	2020年9月	2021年3月	2021年5月
哥本哈根世界气候大会	巴黎气候峰会	第75届联合国大会	中央财经委员会第九次会议	“双碳”工作领导小组成立
提出到2020年单位GDP二氧化碳排放比2005年下降40%~45%，非石化能源占一次能源消费比重达到15%，森林蓄积量比2005年增加13亿立方米，该目标在2019年已全部实现	提出到2030年，中国单位GDP二氧化碳排放比2005年下降60%~65%，非石化能源占一次能源消费比重达到20%左右，森林蓄积量比2005年增加45亿立方米左右，风电、太阳能发电总装机容量将达到12亿千瓦以上	提出：“中国将采取更加有力的政策和措施，二氧化碳排放力争于2030年前达到峰值，努力争取2060年前实现碳中和”	习近平强调实现碳达峰、碳中和是一场广泛而深刻的经济社会系统性变革，要把碳达峰、碳中和纳入生态文明建设整体布局，拿出抓铁有痕的劲头，如期实现2030年前碳达峰，2060年前碳中和的目标	成立以国务院副总理韩正任组长，刘鹤、王勇、王毅、何立峰任副组长的领导小组负责制定碳达峰、碳中和的时间表、路线图等顶层设计
国际责任承诺，重点是减排（重点行业行动计划）			国家发展战略，重点是产业、结构、方式升级（全国行动计划）	

从中国碳达峰碳中和的路径全景图就可以看到，实现双碳目标，我们要在三个方面解决碳排放问题，一个是在能源供给端进行结构调整，我国目前大部分的电量都是由火电提供，占比高达67.8%。所以我们要逐渐去石化，推广清洁能源，如太阳能、风能、水能、核能等。到2030年石油消费达峰，2060年非石化能源接近100%。另一方面是在能源消费端进行能效提升。消费端制造业、建筑、交通等是耗能占比最高的几个行业。工业领域电气化改造，推广电动车、氢能车等，实现能源高效利用。三是在碳收集端，推广固碳技术，加大碳捕集封存技术的研发，加强生态建设，植树造林等。



二、如何降低港口碳排放

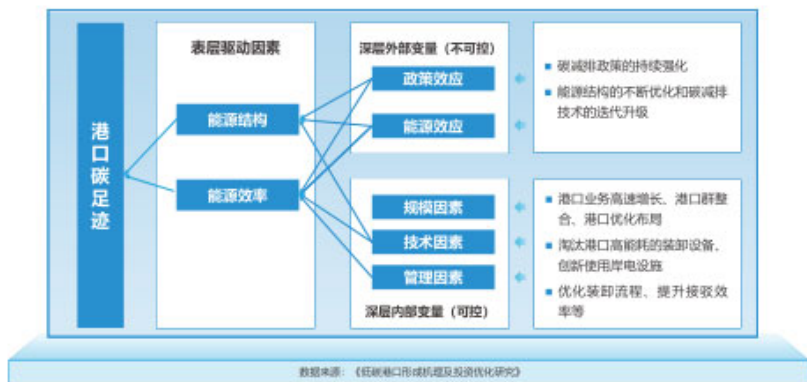
如何降低港口的碳排放，首先我们要知道港口碳排放源有哪些。根据温室气体协议GHG的定义，分为三类，第一类排放源是直接排放，来源于企业拥有或控制器的排放源静止燃烧、移动燃烧、化学过程、生产过程或逸出源的排放。比如港口的燃油车辆和燃油港机设备的排放。第二类是消耗电力的间接排放，企业购买并消耗的电力在发电过程中产生的直接排放，比如港口的耗电设备，如岸桥、电动车辆、区域照明、仓库堆场、数据中心等。第三类是企业活动产生除消耗电力外的间接排放。比如靠港船舶和到港集卡的碳排放，这类碳排放其实是非常大的，但不是港口企业能控制的。所以在很多核算港口碳足迹范围时，不会将这类核算进去，但是第一类和第二类至少是要包含的。



1. 影响港口碳足迹的因素

港口碳足迹的快速增长，是受很多因素影响的。在《低碳港口形成机理及投资优化研究》一文中，就提到了，港口碳足迹是受多重因素影响，涉及能源、技术以及政策等方面。总体分为表层驱动和深层驱动因素。

具体来说，表层驱动包括了两大因素，分别是能源结构和能源效率。深层驱动包括了政策效应、能源效应、规模因素、技术因素和管理因素。减少传统能源的直接燃烧是降低碳排放的方式之一，比如港机设备油改电，使用岸电技术，应用新能源等。但是我们前面提到，我国电力以煤生产为主的能源结构未发生根本变化，所以短期看，港口通过岸电技术改造降低碳排放的强度效果不佳，长远看，随着水电、风电、核能等清洁能源大幅增长导致能源结构不断优化，也必然致使高度依赖电力这种间接能源的港口碳排放强度持续下降。而现阶段来说，提高能源效率是抑制碳排放的更有效手段。



2. 建设智慧绿色港口的具体举措

具体来说，分为几种方式：

- 自动化码头的建设，通过优化港区码头布局和统筹生产调度，从而提高整体作业效率，降低集卡空驶率。
- RTG拖轮等老旧设备的改造，推进油改电，油改混合动力，采用能量回馈技术，提供能源利用效率。

- ◆推进现有码头和船舶岸电设施的改造，进一步加大岸电使用率。
- ◆提高清洁能源的占比，探索使用太阳能、潮汐能、风能等新能源的利用。
- ◆LNG集卡和LNG船舶的应用。现阶段LNG相对其他清洁能源的技术更成熟，加气站站建站灵活，车辆加气方便，比较适合港口使用。
- ◆建设绿色数据中心。除了在港口作业方面的耗能外，港口数据中心的能耗也是不可忽视的，所以建设港口绿色低碳数字中心也是必不可少的。通过集约化建设数据中心，可以有效避免IT重复投资，从而控制成本，降低能耗。另外数据中心内采用高效率的设备和可以降低数据中心的碳排放。
- ◆水电能耗智能管理。通过物联网技术，实现水电表的无线联网、智能监管、智能控制。
- ◆光伏储能应用。将光伏系统、储能系统、充电系统有机结合，并依托云计算、大数据实现电网的全面感知、数据融合和智能应用。

自动化码头建设 <ul style="list-style-type: none"> 优化港区布局和码头布局 统筹生产调度 提高货物装卸作业效率 降低卡车空驶率 	RTG、拖轮等改造 <ul style="list-style-type: none"> 推进RTG、岸桥等老旧设备“油改电”、“油改混合动力”技术改造工作，采用能量回馈技术，提高能源利用效率 	港口船舶岸电技术 <ul style="list-style-type: none"> 推进现有码头和船舶岸电设施改造，进一步加大船舶靠港使用岸电，推动岸电便利化使用 	提高清洁能源占比 <ul style="list-style-type: none"> 推进LED绿色照明等技术，探索港区的太阳能、潮汐能、风能等新能源的利用，提高自身清洁能源占比
LNG集卡应用 <ul style="list-style-type: none"> 推进集卡LNG能源替代 建设LNG加气站 逐步淘汰高污染车辆 	绿色数据中心 <ul style="list-style-type: none"> 采用云计算技术，集约式建设，避免重复建设 选用高性能的计算存储设备 采用液冷技术，降低能耗 	水电能耗智能管理 <ul style="list-style-type: none"> 采用物联网技术实现水电能耗智能管理 利用LoRa网关与前端水电表无线联网 能耗三级监测 	光伏储能应用 <ul style="list-style-type: none"> 光伏系统、储能系统、充电系统有机结合 运用云计算、大数据实现配电网全面感知、数据融合和智能应用

三、建设智慧绿色港口的关键技术和应用

建设绿色智慧港口的技术和应用有很多举措，本文聚焦在信息化领域。一方面通过信息化能力提升港口能源管控效率，另一方面降低信息化基础设施自身的能耗，实现绿色港口建设。

1. 液冷技术打造绿色数据中心

液冷技术是一种高效的冷却技术，能够有效地降低数据中心的能源消耗和碳排放。通过冷却液代替风冷，可以快速地吸收服务器产生的热量，并将其传递给外部冷却系统，从而实现更高的冷却效率。相比传统的风冷技术，液冷技术可以减少数据中心的能源消耗和碳排放，同时提高服务器的可靠性和稳定性。在绿色数据中心的建设中，液冷技术将成为未来的发展趋势。通过采用液冷技术，可以将数据中心的能源消耗降至最低，同时减少对环境的影响。此外，液冷技术还可以提高数据中心的计算性能和稳定性，为企业的数字化转型提供更好的支持。



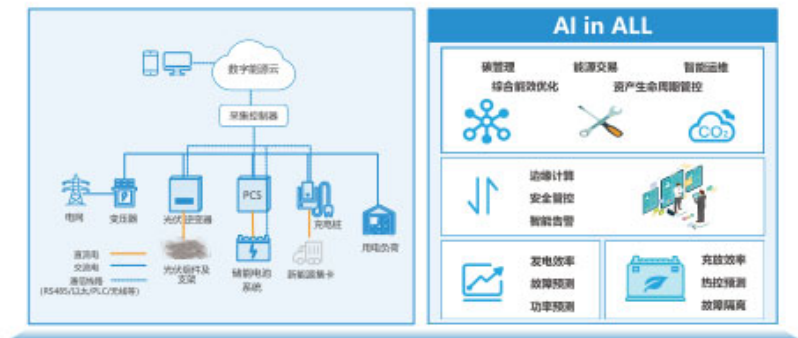
2. 基于物联网实现水电能耗智能管理

此外物联网技术可以实现港口水电能耗的智能管理。通过LoRa网关与前端水电表进行无线联网，再将水电数据回传给绿洲物联网平台，实现对水电表数据的远程采集，并对水电能耗进行三级监测，随时随地掌握港区用电用水情况，从而更快捷的实行节能操作。



3. 光储充一体化实现新能源智慧应用

在新能源应用方面，港口智慧光储充一体化，可以将光伏系统、储能系统、充电系统有机结合，实现信息流与能量流互动闭环。整体方案深度融合传统工业技术、物联网、云计算技术，全面配置智能配电设备，实现配电设备间的全面互联、互通和用电数据的精准采集。依托数字能源云对整个配电系统进行实时监控和运行质量的有效管理，实现配电网的全面感知、数据融合和智能应用。



4. “源碳管服”打造零碳智慧港区



依托“1+4”顶层设计理念，即一个零碳智慧操作系统和“源-探-管-服”四大模块，构建零碳智慧港区。在源头上推动清洁能源替代，在探测上完善碳排放监测机制，在管理上强化一体化能耗管理，在服务上做好碳咨询服务，全方位推动新一代“零碳智慧园区”的建设。

另外在港口企业搭建碳资产管理平台，在建立完善的碳排放数据监测报告、核查（MRV）制度的同时，为港口提供碳配额有效管理、碳交易深度参与、港口绿色形象塑造等服务，并以低成本履约方案、CCER项目管理、碳金融支撑等方式盘活港口碳资产，帮助港口在全国碳交易市场中获取减碳红利。同时可以在各级地方政府建立完善的碳资源管控平台，汇聚省市各行业各企业碳排放、碳资产、碳交易数据，实现数据可视化、可溯化、可控化，物联智能分析、及时预警，政府监督、核查。

未来展望

未来，智慧绿色港口将更加注重能源结构的优化和清洁能源的使用。我们将进一步推广太阳能、风能等可再生能源在港口和航道的建设和运营中的应用，减少对传统化石能源的依赖，降低碳排放，保护生态环境。同时，更加注重智能化技术的应用。通过引入先进的人工智能、物联网、大数据等技术，实现港口的智能调度、智能装卸、智能运输等环节的自动化和智能化，提高运营效率和服务质量，降低运营成本。

智慧绿色港口建设将在推动可持续发展和促进经济增长中发挥更加重要的作用。我们将继续深入探索智慧绿色港口建设的创新技术和方法，推动港口业的数字化转型和智能化升级，实现更加高效、环保、可持续的运营模式。



浅析人工智能在港口安全应急的应用

文/葛云峰

港口安全应急是保障港口安全的必要手段，是防范和应对港口恐怖袭击、交通事故、环境污染等突发事件的关键。随着国际贸易的不断发展和港口的日益繁忙，港口安全面临着越来越多的挑战，包括安全威胁、应急协调和信息共享等方面。建立高效健全的港口安全应急体系，不仅对于保障港口安全，保护人员和财产安全具有重要意义，也是维护港口形象和国家安全的必要手段。

随着机器学习、神经网络、AIGC大模型技术的逐渐成熟，人工智能也逐渐应用在了各行各业，比如自然语言、机器视觉、图像分析等等多个场景。人工智能技术的快速发展也为港口安全应急管理提供了新的解决方案。本文主要探讨了人工智能在港口安全应急场景中的应用，并对其效果进行了评估。在此基础上，文章还讨论了人工智能在港口安全应急管理中的未来发展趋势。

一、当前港口应急遇到的痛点

当前港口安全防护手段面临多种痛点，比如堆场集装箱堆箱较高，容易出现视频盲点，港区缺乏全局态势把控，目前以传统九宫格方式大屏监控居多，无法实现全景呈现。另外前端视频监控缺乏AI算法加持，无法动态智能监控港区异常状态。同时应急处置智慧联动少，预案执行落地慢等都是突出问题。

二、人工智能助力打造港口智慧安全立体防护网

在人工智能的加持下，可以在智能视频监控、港口智能预警、应急响应决策辅助、港口网络安全防护等方面，打造港口智慧安全立体防护网。

1. 港口智能视频监控场景

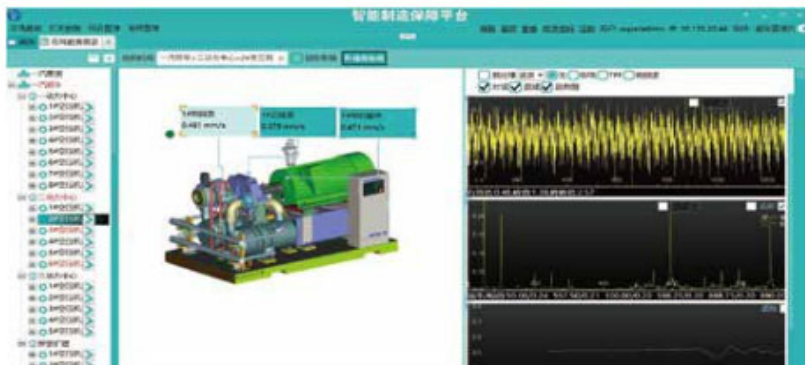
人工智能在港口监控领域的应用主要体现在图像识别和行为识别两个方面。通过计算机视觉和深度学习技术，智能监控系统可以实时监控港口水域、货物等，自动识别异常情况并触发报警。例如，系统可以通过对船舶行为的识别，自动检测到船舶碰撞、非法入侵等异常行为，并及时发出警报，从而有效预防事故的发生。

传统监控终端视角相对狭窄，难以掌控港区全局。如今可以通过在港区大楼顶、铁塔或高杆灯等高点布设全景相机，以更宽的视角俯视港区全貌。同时在闸口、查验所、码头前沿、堆场等关键地点布设枪机，搭配AI+AR、标签联动等技术，实现在高点全局画面中以画中画方式查看各类低点防控资源，高低两级协同，形成由高到低、由内到外的立体化防控体系。



2. 港口智能预警场景

在港口预警系统的构建中，通过大数据分析人工智能技术可以帮助对大量的数据进行快速、准确的分析。通过机器学习和数据挖掘等技术，可以对港口的海况、气象、货物、机械设备等信息进行深度分析，建立预测模型，对可能发生的安全风险进行预警。人工智能技术可以帮助进行预测性维护和故障检测。通过对设备运行数据的实时监测和分析，可以预测设备可能出现的故障和维修需求。例如，通过分析港机设备的运行数据，可以预测机械的维修需求和更换周期，从而提前进行维修和更换，避免设备故障对港口运营的影响。



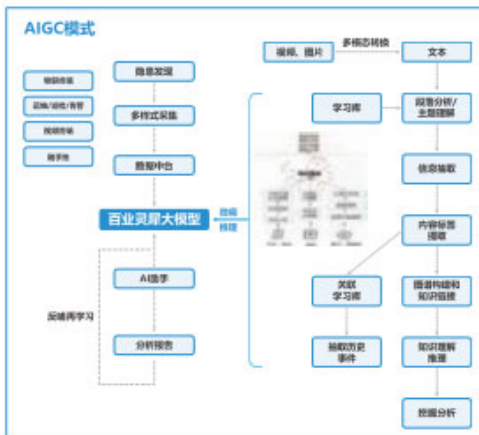
3. 应急响应决策辅助场景

在应急响应方面，人工智能的应用主要体现在两个方面。

一是通过应急指挥中心实现快速响应。在港口发生紧急情况时，应急指挥中心可以通过人工智能技术对实时数据进行快速分析和处理，生成最佳的应急响应方案。例如，在船舶碰撞事故发生后，应急指挥中心可以通过智能监控系统获取到船舶的位置、天气、海况等信息，再通过人工智能技术进行数据分析和预测，制定出最优的救援方案和紧急疏散方案。

二是通过自动化设备实现快速救援。人工智能可以通过对数据的分析和处理结果来控制自动化设备进行快速救援行动，例如控制无人机或机器人进行现场勘查或救援行动等从而提高应急处理的效率和准确性减少人员伤亡和财产损失等后果的发生。

在应急安全事项发生后，一般通过安全事件文本上报形式收集安全风险隐患或排查，虽已有系统支持，但主要围绕记录查阅功能展开，隐患深度分析缺乏工具，基本靠人工，如提取关键字，在手工分析等，效率低，潜在隐患也无法关联。而借助AIGC大模型的能力，实现安全事件的快速理解、归纳、分析、输出分析报告，辅助安全管理人员提升工作效率。



4. 港口网络安全防护场景

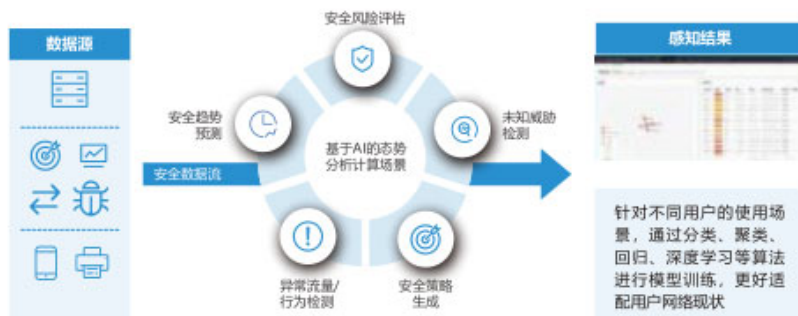
保障港口的网络安全、数据安全是打造港口安全立体防护网的重要一环，如果信息安全出现了问题，对于港口的影响是非常巨大的。比如2017年鹿特丹港遭到勒索软件攻击，导致马士基航运集团子公司APMT运营的两个集装箱码头瘫痪。所以借助人工智能技术更加快速、智能的做好港口网络安全防护是非常必要的。在网络安全防护场景中，人工智能可以在以下几个方面发挥作用：

入侵检测和防御：利用人工智能技术，可以实时监测和分析网络流量，识别异常行为，如未经授权的访问、数据泄露等，从而及时发现并阻止网络攻击。

恶意软件检测：通过分析网络流量和文件，人工智能可以识别并拦截恶意软件，如病毒、木马、蠕虫等，保护港口网络免受恶意软件的攻击。

漏洞扫描和修复：人工智能可以对港口网络进行全面的漏洞扫描，发现并报告潜在的安全风险，并提供修复建议，帮助港口及时修复漏洞，提高网络安全性。

安全审计和日志分析：利用人工智能技术，可以对港口网络进行全面的安全审计，分析网络活动、用户行为等日志信息，发现异常情况，提供对潜在威胁的早期预警。



风险评估和管理：通过大数据分析和模式识别技术，人工智能可以对港口网络进行全面的风险评估，识别潜在的安全隐患和风险，提供相应的管理建议和解决方案，降低网络风险。

三、人工智能在港口安全应急场景中的应用价值

在港口安全应急场景中，通过对人工智能的使用，可以给客户带来如下价值：

提高安全性和可靠性：通过人工智能的应用，港口可以建立智能化的监控系统，及时、精确地检测异常情况，例如危险品的泄漏或非法入侵等，从而提高港口的安全性和可靠性。同时，人工智能技术可以帮助管理人员进行实时监控和异常检测，及时采取措施，避免事故的发生。

优化运营效率：人工智能技术可以帮助港口实现智能化、自动化的装卸和物流过程，提高运营效率，减少人力成本。例如，通过人工智能技术，可以实现智能化自动化装卸的过程，增加装卸效率，减少人力成本。同时，人工智能技术还可以解决货物错发、滞留等问题，提高物流效率，降低仓储成本。

提升决策能力：人工智能技术可以帮助港口进行数据分析和预测，为决策者提供更加科学合理的决策依据。例如，通过大数据分析和模式识别技术，可以预测未来的天气、海况等信息，帮助决策者制定更加科学合理的运营策略。

增强应急响应能力：人工智能技术可以帮助港口建立应急响应系统，提高应急响应的效率和准确性。例如，在船舶碰撞事故发生后，人工智能可以通过实时监测和分析船舶的位置、天气、海况等信息，为应急指挥中心提供最优的救援方案和紧急疏散方案。这些方案可以提高应急处理的效率和准确性，减少人员伤亡和财产损失等后果的发生。

结语

人工智能在港口安全应急场景中的应用已经取得了显著的成效，提高了监控效率、降低了事故发生率、优化了应急响应、提高了工作效率及经济效益。随着技术的不断进步和应用范围的扩大，人工智能在港口安全应急管理中的应用前景广阔。未来，新华三进一步探索和实践，人工智能技术在港口安全应急管理中的更多应用场景和可能性。



数智赋能航道 安全与效率齐升

文/童修品

智慧航道是指利用智能传感器、物联网、自动控制、人工智能、云计算、大数据等技术，自动获取航道系统要素信息，通过融合处理与深度挖掘，动态发布航道有关信息，实现航道规划科学化、建养智能化、管理现代化，为航运企业运输决策、船舶航行安全、海事监管、政府水上应急等提供全方位、实时、精确、便捷的服务。智慧航道的发展对提升内河航运安全性及航行效率具有重要的促进意义。本文主要研究智慧航道各项智能化应用的支撑技术，选择合适的底层技术方能发挥智慧航道应用的价值，提高通航安全性和通航效率。

一、智慧航道概述

1. 智慧航道建设需求

- **市场需求增长：**随着我国经济的快速发展，交通水运优势突显，航运业的不断扩大，对传统航道通航安全和通航效率的要求也越来越高，急需通过数字化手段提升传统航道的通航能力。智慧航道为船舶船员提供了更加安全和便捷的航行环境，受到航运企业和货主的广泛关注。

- **国家立体交通发展需要：**交通运输部发布的《水运“十四五”发展规划》明确提出“十四五”期间新增国家高等级航道2500公里左右，加快智慧航道建设，加强航道基础设施信息采集能力建设，推动航道、航标、整治建筑物等全要素、全周期数字化。《关于推动交通运输领域新型基础设施建设的指导意见》要求建设高等级航道感知网络，推动通航建筑物数字化监管，实现三级以上重点航段通航建筑物运行状况实时监控。

2. 智慧航道发展历程

智慧航道行业的发展历程可以概括为以下几个阶段：

初期阶段：智慧航道行业的发展起步较晚，初期主要集中在一些发达国家和地区。在这个阶段，主要关注航道的监控和数据采集，通过传感器和监控设备收集航道的实时数据，并进行分析和处理。实现了对航道基础环境要素的实时感知，解决了船舶、监管单位对航道通航环境信息感知不全不及时的问题。

技术应用阶段：随着物联网、大数据和人工智能等技术的发展，智慧航道行业开始应用这些技术来提高航道的管理和监控。例如，通过物联网技术实现航道设备的互联互通，通过大数据分析提供航道的预测和决策支持，通过人工智能算法优化船舶的航行路径等。

综合应用阶段：智慧航道行业逐渐向综合应用方向发展，不再仅限于航道的管理和监控，而是将航道与其他相关领域进行融合。例如，将智慧航道与智慧港口、智慧物流等领域进行融合，实现整个物流链的智能化管理。

3. 我国智慧航道发展现状

目前，除长江航道、京杭运河部分航段，各省试点的部分航道完成初期阶段建设，在探索新兴技术应用外，全国大部分航道还停留在传统航道模式，缺乏基本的航道数据收集与监控能力，待进行智慧航道初期阶段建设。

有示范工程：“十四五”期，在数字航道基本建成的基础上，长江航道拟利用更先进的智能感知、大数据和信息技术赋能航道业务，进一步升级动态监测、养护管理、公共服务等基础体系，逐步建成动态感知更快、维护管理更准、服务供给更精的“智慧大脑”，积极探索“智慧航道”建设。将为我国内河智慧航道建设探索提供示范作用。

有指导规范：2022年1月份交通运输部水运局发布了《内河数字航道工程建设技术规范》，进一步完善了智慧航道建设标准顶层设计。

4. 当前存在的挑战

基础设施信息化不足

目前内河航道沿岸水上、水下、空中等维度感知手段不足、视频监控覆盖存在盲区、水流水位信息感知缺乏、导助航设施智能化程度不足，智能导助航技术缺乏，很多航道尚未建立电子航道图等智能应用。

数据资源利用差

基础设施、运营、服务、收费等信息散落在相关管理部门，部分信息未实现与港务、海事等其他涉水部门的数据共享、交换，且多以统计类信息为最终产出成果；无法很好整合，甚至无法整合，大量高价值信息仅被单一运用甚至被遗弃，极大地降低了各系统的使用效果。

平台支撑不足

传统航道，仅集成了航道部门管理的航道信息，而港务、海事等其他涉海部门也在建立各自的信息管理平台，也仅能支撑各自的基本业务系统运行，缺乏大范围协同监管、大区域监视监测和及时有效的数据平台、云控平台支撑能力。

统筹协调困难

水上突发事件环境复杂、破坏程度大，需要消防、海警、环保、搜救中心等多部门同事行动，应急救援指挥难度大、资源统筹协调困难。

基于以上问题，新华三结合自己在各行业数字化转型的经验和能力，提出了新华三智慧航道解决方案，为智慧航道应用选择合适的底层支撑技术。

二、新华三智慧航道解决方案



图1 智慧航道解决方案架构图

新华三智慧航道解决方案可归纳为“1+2+3+N”体系，“1”即一朵航道云：建立省级智慧航道云平台，承载区域内的各项智慧航道应用；“2”即感知、传输两张网：“实时监测、多维覆盖”的前端泛物联智能感知网络，综合承载、业务安全隔离骨干传输网；“3”即三平台：“统一发布、共享应用”的电子航道图支撑平台，“全域接入、分域分权”的数据服务平台，“真实模拟、智能运维”的航道数字孪生平台；“N”即N项智慧化应用：智能航标、水位遥测遥报、智慧船闸、桥梁防碰撞、智慧应急、智慧水上服务区、以及船岸协同助航服

务。下面将从感知传输网、航道云平台、数据平台方面探讨如何利用这些数字化技术支持智慧航道应用，如何提高航道安全性、效率性和可持续性。

1. 前端感知网

前端感知网指的是通过建设“一张网”连接航道外场诸多的感知终端（雷达、AIS、VHF、航标遥测遥控、视频感知终端、水位遥测遥报、北斗地基增强、船舶流量监测），作为航道大数据中心、电子巡航系统、船舶监管系统、航标遥测遥控系统、视频监控系统等应用系统的神经触手为各种智慧化应用提供源源不断的实时地航道环境数据、运行数据和管理数据。实现航道流域的实时监控、动态感知、监控预警、科学决策分析，提升航道的治理、管理和服务水平。前端感知网连接的设备种类繁多，有标准以太网设备，有无线终端，有工业传感器，需要有线（光纤、双绞线）、无线（4G/5G、LoRa、NB-IoT、WLAN）多种方式接入，对接入网关提出了很高的要求。新华三推出的航道岸测一体杆搭载的工业级物联网边缘AI网关可以提供丰富的接口类型和制式，可以让不同类型的终端设备接入，同时一体杆集成了雷达、感知终端等设备可支撑多种应用。例如：

交通流量监测：基于雷视融合技术，可对航道内货船、工作船进行统计监测。

船舶身份智能识别：船名识别，AIS融合对比、船舶抓拍等。

船舶特征及行为分析：航向轨迹跟踪、空重载识别、船舶尺度检测、吃水检测、船名异常告警、AIS异常告警、超载监管、未封蔽、违规锚泊、非法捕鱼等船舶违规行为智能识别与监管。

船岸协同：作为岸测边缘节点，助力船舶辅助驾驶，远程驾驶。

桥梁智能防撞预警：超高、偏航检测，声光报警，信息发布。

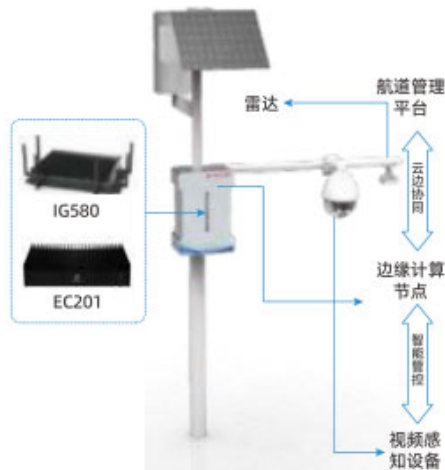


图2 岸测一体杆构造图

表1 岸测一体杆集成网关设备参数表

名称	IG580工业级物联网边缘AI网关	EC201
AI算力	扩展keembay, 8Tops	扩展keembay, 16Tops
通信	4G/5G、802.11a/b/g/n/ac	
软件功能	内置边缘计算框架，提供容器监控、函数计算、规则引擎、流式计算，并提供T320、T350等系列网关管理功能和物联网平台的云边协同功能、支持Modbus-RTU/TCP、MQTT等终端接入	提供AI基础框架，支持多算法融合，集视频管理、存储、智能于一体

2. 骨干传输网

骨干传输网为岸侧到数据中心的数据通信通道，主要用于外场感知设备、港航部门与数据中心的通信，宜采用光纤网络。骨干传输网在其他行业已有广泛应用，但是并不能很好的复制到水运行业。城市轨道交通、高速公路行业目前采用传统的SDH、MS-OTN或PTN设备组成光纤环网的方案，解决多个业务系统不同网络质量不同带宽及高可靠的通信需求。这些传统传输产品以其硬隔离技术，冗余的硬件设计可以确保各个业务数据流之间相互独立和隔离，提高了网络的安全性、可靠性和性能。但同时这些传输设备也有着诸多的弊端：

- 封闭，兼容异构能力低：传统传输业务编排与规划基本以手工方式为主，缺乏自动化编排和部署的能力。在后期运维阶段缺乏智能化的运维手段，对运维人员的专业技能要求较高。由于技术的封闭性导致传输市场完全被少数厂商垄断。

- 成本高：由于传输系统无兼容异构能力，各家厂商设备均不支持异构组网，极易导致最终用户被设备厂商绑定，大大降低了最终用户的议价能力，投资成本往往居高不下。

另外也有部分行业探索使用价格低廉更加通用的以太网交换机构建骨干环网。业务隔离靠构建多张物理环网实现，因受光模块传输距离的影响往往需要设立中继站点或者仅应用在短距离骨干网建设，同时多张物理环网带来的运维工作量也非常大。

航道建设主要是政府财政资金投入，收入来源低，人员配置少，无论是采用传统传输还是以太网构建航道骨干传输网都有不足。新华三推出的IPRAN骨干承载网方案可以兼顾传统传输高可靠性，业务数据隔离和以太网易管理的特点，同时有比传输更低的成本，是航道行业骨干传输网不错的技术选择。

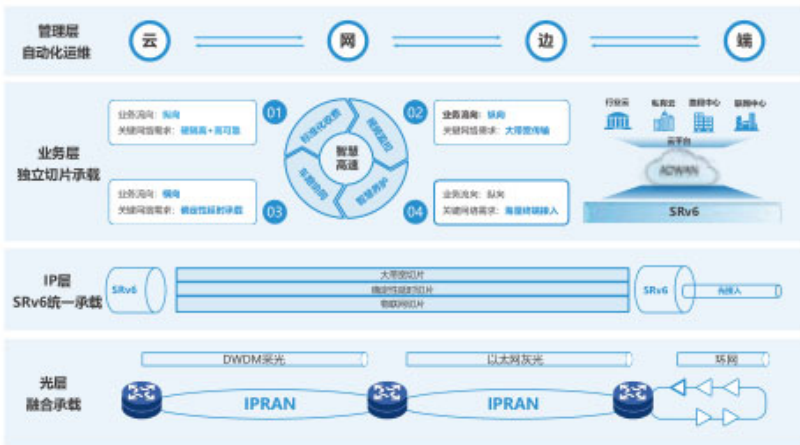


图3 新华三智慧航道骨干传输网

IPRAN技术以SRv6为主要协议，同时支持MPLS-SR协议。SRv6是IPv6作为内核，使用IPv6 DIP和IPv6扩展头指导转发的技术，支持与MPLS-SR互通，具有良好的兼容性和可扩展性。IPRAN技术平滑演进，整体架构并没有出现大的变化，由全球运营商、各行业一同推动演进，主要是利用IPv6优秀的可扩展性，形成了大量的IPv6+智能应用场景，如iFIT、SFC、APN、网络切片等，使得使用IPRAN技术的网络可以感知业务对网络的需求、对安全的需求、业务真实的体验等，提供更加真实、灵活、智能的网络。

IPRAN技术支持并配置FlexE硬管道接口，实现航道收费、AIS、VHF、雷达、视频、会议、办公等不同业务系统数据的物理隔离，同类业务硬件层独享带宽，即使在通信网络业务出现流量拥塞时，也不会影响业务数据的稳定承载，从而在保证业务安全的基础上通过一张物理网络承载航道各业务系统的关键应用。

IPRAN技术基于IP网络，天然的更关注于具体的业务承载情况，通过iFIT技术直接测量业务报文来得到业务的真实丢包率和时延等信息，可以为运维人员提供更加精细化的业务承载状态信息，基于iFIT技术可以引入新的更加智能化的运维手段提升运维效率。只需要省市级航道云数据中心的运维人员远程查看、配置就可以完成大部分的骨干网设备的运维工作，降低沿线区域站点人员的运维技术要求，提高网络设备故障处理效率，减少对航道运营的影响，进而提高航道通航效率。

3. 智慧航道支撑平台

3.1 航道云平台

无论是部水运局发布的数字航道工程建设技术规范还是各省发布的智慧航道建设指南都达成了共识，建立省市统一航道云平台，为智慧航道相关应用提供基础服务支撑。现在云的部署形式有公有云、私有云、混合云、边缘云、还有最新的分布式云，在智慧航道我们应该选择怎样的部署方式，那么就需要看航道业务数据的现实情况是怎么样的。



图4 智慧航道的业务数据特点和需求

支撑智慧航道应用的数据类型类型多，量大，且存在地理分散的特点，船岸系统需要超高速度的数据传输处理，船闸收费调度控制业务需要高稳定性，视频雷达数据需要本地预处理减少对骨干网带宽的影响。基于智慧航道的业务数据特点和需求，新华三提出了“云边端”一站式解决方案，构建智慧航道云计算框架。



图5 智慧航道云计算框架

“云”指的是省市级航道中心云，主承担流域内的各项智慧应用，包括云统一接入、云共享服务、视频云服务、云基础服务等；“边”指航道区域中心边缘云，接受中心云统一管理和下发，同时承载中心业务的降级使用；“端”指航道外场终端设备，进行初步的边缘数据计算预处理。三级设备构成智慧航道业务的计算体系。该框架有以下五大特点：

- ◆统一管理：中心云统一入口，统一运营运维，统一权限管控。
- ◆异构兼容：X86/ARM/FPGA/GPU等多种异构设备多池部署。
- ◆云边协同：应用协同、数据治理协同、AI协同，一次构建，随处部署。
- ◆弹性扩展：云边资源跨域弹性调度，解决应用扩展问题。
- ◆分布式网络：全局SDN，管理面协同，数据面按需打通，支持多出口。

该计算体系模式可以避免航道流域内各个区域中心重复建设，降低建设成本，简化流域内数据互通屏障，同时方便系统维护，提升了整个航道运行效率。

3.2 数据平台

目前智慧航道建设最大的挑战就是数据资源利用差，平台支撑不足。对于智慧航道技术构架缺乏完整的构建，信息化建设项目独立、建设碎片化，使得技术应用于实际的建设过程出现相脱节的情况。没有强大而完善的技术设计，智慧航道建设就不能实现各项信息资源的整合。平台不统一，造成航道各相关部门沟通不协调，一切的智慧化应用建设都将浮于表面，真正的价值发挥可能不足十分之一。新华三绿洲数据平台由数据融合集成平台和数据运营平台构成，主要包括数据采集、数据处理、数据治理、数据交换、数据共享等从汇集到应用的全流程服务能力，可以解决数据质量低、价值密度小、集成难度大（数据不可连、数据标准不统一、数据结构复杂）、数据不可控（安全机制不健全带来大数据应用的隐私和风险问题）、共享联动慢等问题。

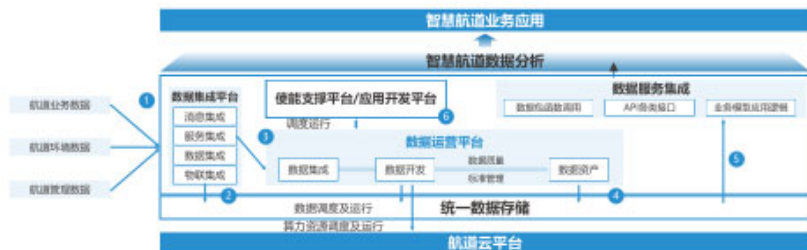


图6 智慧航道绿洲数据平台

绿洲的数据集成平台可以将航道业务数据、环境数据、管理数据等进行消息集成、服务集成、物联集成进行统一接入；数据运营平台将人、物、事时空整合在一起，针对人船物环境进行数据建模，提供各类主题库、专题库，对外提供数据服务，可以方便让开发者快速使用基本数据，让数据发挥价值。

智慧航道数据平台可以提供统一标准和统一规范封装服务和数据；实现数据跨区域、跨系统的可靠交换，系统服务和数据资源的集中统一组织、管理、服务，并为应用系统运行提供集成环境；服务于航道运行管理等智慧航道相关应用，为其提供完备的数据支撑。让各智慧应用发挥智慧基因，切实提高内河航运安全性及航行效率。

结语

航道基础设施建设发展到一定阶段后，航道将由等级提高必然转向管理服务提升，向智能、绿色、安全、高效的现代化服务方向发展，将会进一步深化技术应用。通过更加智能化的航道管理系统和设备，提高航道的实时监测、预测和预警的准确性和效率，航道信息感知将更为全面、透彻；航道信息交互更为通畅、友好；航道信息服务更为实时、便捷；航道管理与养护更为科学、低碳。

通过智慧航道的建设，一方面智慧化系统可以为船舶和驾驶员提供更精细化的环境、服务引导等信息，可以提升航道区域段的安全航速标准，降低因信息获取不全导致的事故发生率，进而提升航道通航效率和安全性。另一方面各项智慧化给航道管理者带来诸多便利，无论是在为船舶、船员服务的流程时效性上，还是应急突发事件处理响应的及时性上都得到大大提升，进一步提升了航道通航效率和安全性。



06

行业探索

第42章 全新视角下的IPRAN	270
第43章 AIGC时代，核心算力基础GPU技术与应用场景解读	277
第44章 AIGC在交通规划领域的应用探讨	284

全新视角下的IPRAN

文/刘术伟

IPRAN定义：IPRAN（IP Radio Access Network）是一种融合了传统无线接入技术和互联网协议优势的通信网络技术。它主要特点包括提供高效的数据处理和传输、增强网络的灵活性和可扩展性，同时在降低运营成本方面具有显著优势。IPRAN尤其适用于高带宽和低延迟需求场景，尤其适用于移动互联网接入和企业网络连接。作为现代通信网络的关键组成部分，IPRAN旨在提供更高效、可靠和灵活的网络服务，以应对当前通信领域的挑战和需求。

IPRAN产品具备完善的SDN能力、丰富的云业务特性、电信级网络可靠性保障等路由器的全部特性，同时也具备灵活切片、精密时钟同步、高可靠性OAM等传输技术。

IPRAN产品在路由器基础上融合了传输产品能力，支持了硬管道（颗粒度10M）、高可靠（故障收敛<50ms）、大带宽（400G）、远距离传输，部分场景可以替代传输技术如SDH、MSTP、PTN、SPN、OTN。

一、IPRAN的前世今生

IPRAN的发展史展示了无线通信技术从其起步阶段到成为现代网络架构重要组成部分的演变过程。从1990年代初的模拟基础和2G网络的萌芽，经历了GPRS和EDGE技术的引入，IPRAN开始从单纯的语音传输网络转型为能够支持初步数据服务的通信系统。进入21世纪，随着3G技术的出现，无线网络技术发生了革命性的变化，不仅数据传输速率得到显著提升，而且移动互联网体验也得到根本性改善。此时，IP技术在无线网络领域的应用逐渐加强，预示着IPRAN概念的逐步成型。

2000年代中后期至2010年代，是IPRAN概念形成和实现的关键时期。在这一时期，无线网络架构的深度融合IP技术成为了现实，这一变革不仅提升了网络的数据处理能力，也为网络管理带来了前所未有的灵活性。特别是4G LTE技术的推广，标志着IPRAN从理论走向实践的重要一步，为实现高速数据传输和高效网络管理铺平了道路。IPRAN技术得到了全球范围内的快速发展，逐渐成为支撑日益增长的数据需求和服务多样化的关键技术。

进入2020年代，随着5G网络的推出和物联网技术的兴起，IPRAN面临着新的挑战和机遇。5G网络对带宽、延迟和连接密度提出了新的更高要求，推动IPRAN技术不断演进以适应新

的网络环境。同时，5G的到来也为IPRAN带来了新的应用领域，如边缘计算、网络切片和更加广泛的业务支持，从而拓宽了IPRAN的应用景观。中国运营商如中国电信和中国联通开始全面推进“固移融合”、“云网融合”，使用IPRAN技术和产品综合承载城域内所有固定网络和移动网络的2H、2C/2B业务、入云业务，对IPRAN的综合承载能力、可靠性及灵活性提出了更高的要求。

综合来看，IPRAN的发展历程不仅是对通信技术持续创新的见证，也是对满足市场和用户需求不懈努力的体现。从最初的模拟网络到集成了IP技术的现代网络架构，IPRAN在全球通信领域中的重要性日益凸显，预示着其在未来通信网络发展中将持续扮演关键角色。随着技术的进一步发展和创新，IPRAN有望继续引领无线通信网络向更高效、更灵活和更智能的方向发展。



二、IPRAN技术演进

IPRAN1.0和IPRAN2.0是3G向5G发展过程中无线接入网络的两个发展阶段，每个阶段都有其独特的架构特点和技术优势。以下是这两个版本的IPRAN架构的比较：

1. IPRAN1.0简介

基本架构：IPRAN1.0主要侧重于将IP技术引入传统的无线接入网络，其架构相对简单，主要集中在提供基本的IP连接和数据传输功能。

技术特点：

- 简单的IP路由和转发。

- 基于传统的IP/MPLS技术实现网络连通性。
- 有限的服务质量（QoS）和流量管理功能。

应用场景：主要适用于基础的数据和语音服务，对于高级网络服务和应用的支持有限。

2. IPRAN2.0简介

高级架构：IPRAN2.0在IPRAN1.0的基础上引入了更多先进技术，如SDN（软件定义网络）、FlexE&Slice ID切片、IPv6+等技术，架构更为灵活。

技术特点：

- 高级的IP路由和转发机制，支持更复杂的网络拓扑和策略。
- 改进的QoS和流量管理功能，可以更好地支持多样化的服务需求。
- 集成SDN技术，提高网络灵活性和服务创新能力。
- 引入FlexE和Slice切片技术，业务管道管理更灵活可靠。
- 更强的网络安全性和可靠性，以适应日益增长的网络威胁和挑战。

应用场景：适用于更广泛的应用，包括高速数据服务、复杂的企业应用和新兴的云服务。

3. IPRAN1.0和2.0对比

总体对比，引入FlexE和Slice ID切片技术使IPRAN2.0架构相比IPRAN1.0在网络灵活性、资源优化、带宽管理、服务质量和安全性方面都有了显著提升。这些技术不仅提高了网络的适应性和效率，还为满足日益复杂的网络需求和应对不断增长的数据流量提供了支持。通过这些先进技术的应用，IPRAN2.0能够更好地适应未来通信网络的挑战，满足多样化的业务需求。基于应用感知、算力感知、网络自适应、网络自动调整等技术向自治网络演进。

特性/技术	IPRAN1.0	IPRAN2.0
基础架构	较为简单，主要依赖传统IP/MPLS技术	高级，集成SDN、FlexE、IPv6+等先进技术
性能	200G平台	T级平台
信道化子接口	不支持	支持（异构FlexE互联互通）
网络灵活性	基础端口级的链路灵活性	高度灵活，利用SDN技术及SRv6等动态协议实现网络和资源的动态管理

特性/技术	IPRAN1.0	IPRAN2.0
网络切片技术	支持基于VPN的隔离技术	支持FlexE、Slice ID切片, 提供定制化网络服务
网络安全性	基本安全性能	支持SFC等增强的网络安全能力, 可灵活结合安全云等方案适应复杂网络威胁
适应性和扩展性	基本适应性和扩展性	支持APN6、CFN等应用感知、算力感知协议, 实现高适应性和扩展性, 支持多样化的服务需求
确定性	无确定性机制	支持DevNet等确定性协议, 支持构建端到端的确定性网络
技术应用	适用于基础数据和语音服务	支持高速数据服务、复杂企业应用和云服务

4. IPRAN优势

高带宽、远距离

IPRAN支持标准以太网速率, 如10G、50G、100G等, 此外IPRAN支持使用FlexE捆绑技术将多个以太网捆绑成一个大速率FlexE切片。

IPRAN可通过IP+光技术配合光层系统来实现密级波分复用, 提高单条光纤中的传输带宽, 同时提高传输距离。

低时延、安全

使用切片技术来实现业务隔离, 同时保证不同切片的业务质量互不影响。不同切片组成不同的逻辑网络, 确保低时延应用可以以最短路径访问到最优的边缘计算资源。

当前, IPRAN支持5G粒度的FlexE切片、10M粒度的小颗粒切片、1M粒度的SliceID切片。

高可靠

IPRAN支持各类型故障时收敛时间小于50ms要求。

灵活性

IPRAN支持异厂商组网, 且有大量实施案例。

IPRAN支持第三方网管和控制器, 在运营商有实施案例。

时间同步能力

IPRAN支持1588v2和SyncE。

智能运维

IPRAN支持基于APN6技术和智能运维技术识别应用、应用对网络的需求, 按需将业务引入能符合应用需求的隧道、切片中。

IPRAN可基于iFIT检测结果利用智能运维技术, 及时对业务质量劣化事件进行干预, 如发现应用的流量在网络中真实的质量劣化后将应用的业务流量调整至备份路径。

IPv6+能力

IPRAN全面支持IPv6+技术, 如SRv6 (IPv6分段路由)、APN6 (应用感知网络)、SRv6 SFC (SRv6功能服务链)、SRv6 iFIT (基于SRv6的随流检测)、SliceID (基于IPv6源地址的网络切片技术)。

投资成本、投资保护

IPRAN产业开放, 参与厂商众多, 运营商从IPRAN设计之初就推动异厂商解耦, 所以支持异厂商组网, 新建和扩容的投资成本较低。

先进性

IPRAN有中国电信、联通、移动、广电及海外运营商在推进, 也有金融、政府、电力、教育等行业在使用该技术, 提出新的需求, 所以IPRAN方案有较强的先进性。

三、主流无线承载网技术对比

IPRAN1.0与PTN是同一个阶段产品, IPRAN2.0与SPN是5G承载网同一阶段产品。

不同时期的技术解决问题不同, 面对当前复杂的业务场景, 综合承载能力和良好的发展趋势是选择承载网技术的关键, 综合承载势必要求设备向多合一发展, 融合架构中主要技术的演进路线和芯片生态决定该类产品的生命周期。所以, IPRAN是以太网路线向传输融合, SPN以PTN为基础向支持更多功能以太网发展, 当前阶段SPN对SDH业务友好, 但是随着技术发展, 业务IP化达到一定程度SDH需求将大幅度减少。

IPRAN1.0结合了IP/MPLS和增强型以太网技术, 致力于提供灵活的路由和高效的流量管理, 主要服务于移动通信网络的基站回传。相比之下, PTN更侧重于固定网络的数据包传输优化, 提供可靠和高效的网络连接, 适用于大容量、长距离的数据传输任务。

进一步发展至IPRAN2.0, 该技术展示了对先进IP网络技术如SDN的集成, 以及对IPv6+的全面支持和FlexE等切片技术引进, 为5G及物联网应用提供了高度灵活和高效的网络管理。特别是IPRAN2.0在向IP+光方向的发展上展现了其高带宽和低延迟传输的优势, 增强了网络的传输能力和覆盖范围。与此同时, SPN凸显其在同步和时延控制方面的技术特性, 对SDH业务支持较好, 适用于对时延敏感的固定网络应用, 支持5G传输网络的低延迟和高同步要求。

这些对比反映了IPRAN和PTN/SPN在技术实现、应用场景和未来适应性上的根本区别, 显示了它们承载网中的各自技术进步和应用优势。

综上所述, 几类技术对比如表所示:

特性/技术	IPRAN1.0	PTN	IPRAN2.0	SPN
端口类型	以太网接口	STM/E1\以太网接口	E1\以太网接口	STM/E1\以太网接口
带宽	10G、50G	10G、50G	10G/100G/400G	10G/100G/400G
业务承载能力	以太网链路	SDH\以太网链路	L2/L3业务、以太网链路、IPv6+业务	SDH、PCM、L2/L3业务、IPv6业务
时延	<50毫秒	<50毫秒	< 20微妙	< 20微妙
异构组网能力	支持	不支持	支持	有限异构支持
切片能力	不支持	不支持	5G、10M、1M	5G、10M
IPv6特性支持	支持IPv6基础功能	支持IPv6基础功能	全面支持IPv6及IPv6+特性	支持IPv6

结语

在当今快速演进的网络通信领域中, IPRAN的技术发展路线显示出对于现代承载网建设的显著优势, 特别是在IPv6+ (切片、iFIT、SRv6、APN6、BIER等) 和IP+光技术集成方面。IPv6+的引入, 不仅极大地提升了IPRAN的网络性能, 增强了其在故障检测、隔离、路由优化和多点分发方面的能力, 而且通过网络切片技术, 能够为不同业务需求提供定制化的网络环境, 这对于满足5G和物联网时代的多元化服务需求尤为关键。

IPRAN在集成IP+光技术方面的创新, 有效地解决了远距离传输的挑战。通过将IP网络的灵活性与光纤通信的高带宽优势相结合, IPRAN实现了更远距离的数据传输, 同时保持了较低的

网络延迟。对比传统IP+OTN二层甚至三层组网架构, IP+光系统以统一的单层管理平面进行架构设计, 大大减少建设、管理、维护成本。这种技术融合不仅适用于大规模数据流和高速数据传输, 而且对于数据中心间的互联、高清视频传输等应用场景具有重要意义。

面对确定性网络技术的发展, IPRAN在确保确定时延方面同SPN (Slicing Packet Network) 的低时延特性相比较, 同样展现出了竞争力。IPRAN与SPN都专注于低时延和高同步性, 在对时延敏感的应用 (如工业自动化、精确时钟同步) 中表现卓越, IPRAN支持确定性网络技术, 利用多层次确定性网络技术保障业务端到端的质量保障, 为多样化的业务需求提供了灵活和全面的解决方案。

从政策角度看, 工业和信息化部、网信办、国家发改委、教育部、交通运输部、中国人民银行、国务院国有资产监督管理委员会、国家能源局等2023年4月23日发布关于推进IPv6技术演进和应用创新发展的实施意见, 主要目标是“到2025年底, IPv6技术演进和应用创新取得显著成效, 网络技术创新能力明显增强, “IPv6+”等创新技术应用范围进一步扩大, 重点行业“IPv6+”融合应用水平大幅提升。”

长远来看, 在承载网建设领域, IPRAN与SPN各有所长。SPN的主要优势在于其对低时延和高同步性的专注, 使其在特定领域表现出色。IPRAN在IPv6+技术支持、远距离传输能力及对多样化业务的灵活适应性方面的全面优势, 显示出更广泛的应用潜力。尤其是在应对不断增长的数据需求和多变的网络环境时, IPRAN的全面性和适应性使其成为未来承载网建设的更优选择。IPRAN的技术创新和灵活性, 在5G、物联网、云业务接入等场景表现优异, 说明其在未来网络发展中必将发挥核心和关键的作用。

AIGC时代， 核心算力基础GPU技术与应用场景解读

文/王宇

一、GPU需求背景

AIGC作为新一代人工智能技术正在全方位地塑造行业格局，引领行业未来发展趋势。而这些大型人工智能图形计算（AIGC）模型通常涉及到大量的数据和复杂的计算任务，例如深度学习模型和图形处理等。为了满足这些需求，构建AIGC大模型通常需要使用高端的GPU（图形处理单元）芯片。相比于传统的中央处理器（CPU），GPU具有更多的并行处理核心和更高的内存带宽，能够更快速地完成复杂的计算任务。因此，在构建AIGC大模型的过程中，使用高端GPU芯片可以极大地提高计算速度和效率，使得模型的训练和推断等任务能够更加高效地完成。本文将详细解读GPU基本概念及应用场景，探讨GPU并行计算场景下的通信技术。

二、GPU计算技术详解

1. GPU基础概念



GPU是Graphics Processing Unit的缩写，中文翻译为图形处理器。GPU最初是为了提高电脑处理图形的速度而设计的，主要负责图像的计算和处理。GPU通过并行计算的方式，可以同时执行多个任务，大大提高了图形和数据处理的速度和效率。近年来，由于其并行计算的特性，GPU也被应用于一些需要大量计算的领域，如机器学习、深度学习、数据挖掘、科学计算等。在这些领域中，GPU可以加速训练模型、处理海量数据等计算密集型任务，显著提高了计算效率和速度。因此，GPU已成为现代计算机的重要组成部分，被广泛应用于各种领域。

在生活中，我们普遍把GPU叫成显卡。不过事实上，GPU和显卡在术语上有细微差别，GPU指的是负责处理各种任务的那颗芯片，显卡指的是把GPU芯片、显存、接口等集合在一起的那张板卡。GPU根据接入系统的方式分为集成型GPU（Integrated GPU，iGPU）和离散型GPU（Discrete GPU，dGPU）两种，前者就是我们日常所说的集成显卡，后者就是我们日常所说的独立显卡，两种类型GPU均有各自的特点和使用场景。集成显卡通常是指将显存集成在主板芯片组或处理器内部的显卡，这种显卡通常性能较差，适用于一些简单的应用场景，例如

日常办公、网页浏览等。独立显卡通常是指显存独立于主板芯片组或处理器，有自己的显存和显存控制器，这种显卡性能更加强大，适用于游戏、图形处理、科学计算等需要大量显存和计算性能的应用场景。总的来说，集成显卡通常性能较差，适用于简单应用场景，独立显卡性能更加强大，适用于需要大量显存和计算性能的应用场景。

2. GPU与CPU的对比

谈到计算，我们一般都会先想到CPU，CPU的全称是Central Processing Unit，GPU是Graphics Processing Unit的缩写。GPU最初是为了提高电脑处理图形的速度而设计的，主要负责图像的计算和处理。在命名上，这两种器件相同点是它们都是Processing Unit-处理单元；不同点是CPU是“核心的”，而GPU是用于“图像”处理的。在我们一般理解里，这些名称的确非常符合大众印象中它们的用途-一个是电脑的“大脑核心”，一个是图像方面的“处理器件”。但是聪明的人类并不会被简单的名称所束缚，他们发现GPU在一些场景下可以提供优于CPU的计算能力。GPU的工作原理和CPU类似，都是通过执行指令来完成计算任务的。不同的是，CPU是通过串行执行指令的方式来完成计算任务的，而GPU是通过并行执行指令的方式来完成计算任务的。GPU的并行计算方式可以同时执行多个任务，大大提高了计算效率和速度。

CPU和GPU的区别		
	CPU	GPU
组成单元	运算单元、控制单元、缓存单元	阵列
组成占比	25%的ALU（运算单元） 25%的Control（控制单元） 50%的Cache（缓存单元） 	90%的ALU（运算单元） 5%的Control（控制单元） 5%的Cache（缓存单元） 
适用场景	业务部署、信息化等需要复杂逻辑控制的场合	图识学、挖矿、图形学等需要并行计算、无依赖性、互相独立的场合
对于奥数题目的求解能力	单线程计算（比如机器人运动控制），单个芯片性能强劲，计算能力强，能计算出来	单个芯片性能弱，计算能力弱，可能算不出来，或速度很慢
对于1000道算术题目的求解速度	先算第1题，再算第2题，时间为1000XN；速度较慢	可同时计算1000道算术题，时间为M速度很快
形象比喻	相当于1名老教授，奥数题和小学奥数题都会	相当于1000名小学生，只会小学奥数题
能耗	较少，因为只有少量运算单元（文中为4个）无需单独散热风扇	较多，大量运算单元（多达1000个）往往需要单独散热风扇

GPU和CPU的区别主要体现在以下几个方面：

- ◆架构设计不同：CPU的设计注重单线程处理能力，通常有少量的计算核心和更多的高速缓存。GPU则是面向并行处理的设计，通常拥有大量的计算核心，但缓存较小。
- ◆计算方式不同：CPU在处理任务时，主要通过执行指令流的方式进行计算。而GPU则是通过执行大量的线程，同时进行并行计算，以提高计算效率。GPU的并行计算能力可以同时处理许多相似的任务，适用于大规模的计算密集型任务，例如图像处理、机器学习等。
- ◆用途不同：CPU主要用于通用计算任务，例如文件处理、操作系统运行、编程等。GPU则主要用于图形处理、游戏、计算密集型任务，例如机器学习、深度学习等。

3. GPU核心指标

显存

在GPU中，显存是用于存储图形数据的专用高速内存，但它在数据计算中也扮演着重要的角色。在进行数据计算时，显存可以用于存储计算过程中所需的临时数据、变量、模型参数和计算中间结果，以及输入和输出数据。这些数据可能包括训练数据、模型权重、梯度以及其他与计算任务相关的数据。由于显存具有高带宽和快速访问速度，因此在处理大规模数据集和复杂计算任务时，使用显存可以大大提高计算速度和效率。

显存容量：其主要功能就是暂时储存GPU要处理的数据和处理完毕的数据。显存容量大小决定了GPU能够加载的数据量大小。（在显存已经可以满足客户业务的情况下，提升显存不会对业务性能带来大的提升。在深度学习、机器学习的训练场景，显存的大小决定了一次能够加载训练数据的量，在大规模训练时，显存会显得比较重要。

显存位宽：显存在一个时钟周期内所能传送数据的位数，位数越大则瞬间所能传输的数据量越大，这是显存的重要参数之一。

显存频率：一定程度上反应着该显存的速度，以MHz（兆赫兹）为单位，显存频率随着显存的类型、性能的不同而不同。显存频率和位宽决定显存带宽。

显存带宽：指显示芯片与显存之间的数据传输速率，它以字节/秒为单位。显存带宽是决定显卡性能和速度最重要的因素之一。

CUDA Core与Tensor Core

统一计算设备架构（Compute Unified Device Architecture，CUDA），是由NVIDIA推出的通用并行计算架构。解决的是用更加廉价的设备资源，实现更高效的并行计算。NVIDIA® CUDA®工具包提供了一个开发环境，用于创建高性能GPU加速应用。借助CUDA工具包，您可以在GPU加速上开发、优化和部署应用程序嵌入式系统、桌面工作站、企业数据中心、基于云的平台和HPC超级计算机。该工具包包括GPU加速库、调试和优化工具、C/C++编译器和运行时库来部署您的应用程序。

2017年NVIDIA引入Tensor Core，为大模型的出现奠定了坚实的基础，这也是专为深度学习所设计。深度学习所采用的核心计算主要由张量和矩阵组成，而Tensor Core为了他们专门设计了执行单元，Tensor Core在训练方面能够提供高达12倍的teraflops（兆亿浮点计算）峰值，而在推理方面则可提供6倍的leraflops（兆亿浮点计算）峰值。每个Tensor Core在每个时钟周期可执行64次浮点混合乘加（FMA）运算。Tensor Core使用的计算能力要比CUDA Core高得多。

Tensor core和CUDA Core都是运算单元，是硬件名词，其主要的差异是算力和运算场景。CUDA Core是全能通吃型的浮点运算单元，Tensor core专门为深度学习矩阵运算设计。在高精度矩阵运算上Tensor cores吊打CUDA cores。

CUDA内核：每一个GPU时钟执行一次值乘法

1 x 1 per GPU clock

TENSOR核心：每个GPU时钟执行一次矩阵乘法

$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \times \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$ per GPU clock

浮点运算精度

浮点数PF（Floating points）PF后面数值也代表该浮点类型占用内存的比特位数，常用FP16（半精度）、FP32（单精度）和FP64（双精度），把小数点左边（即整数）的位宽和小数点右边（即小数）的位宽固定，这就是一个定点数。1024就能表示成 0.1024×10^4 ，也就是 $0.1024e+004$ ，3.1415926就能表示成 0.31415926×10^1 ，也就是 $.31415926e+001$ ，这就是浮点数。浮点数进行的运算就是浮点运算。打个比方，想象你有两个不同的杯子：一个大杯子（代表单精度，FP32）和一个小杯子（代表半精度，FP16）。这两个杯子都用来盛水，但它们的精度（即能够盛放的水量的精确度）是不同的。大杯子（FP32）：可以非常精确地测量水的量，因为它有更细的刻度线。如果我们精确的水量，我们会选择这个大杯子。但是，它可能会比较重，需要更多的空间，而且需要更长的时间来填满。小杯子（FP16）：它

的刻度线较粗糙，所以测量的水量可能不太精确。但是，它更轻，需要的空间更少，并且可以更快地填满。对于某些任务，我们可能并不需要非常精确的水量，所以这个小杯子是足够的。

回到计算机的世界，这两种“杯子”代表我们如何存储和计算数字。单精度（FP32）可以更精确地存储数字，但它需要更多的资源。而半精度（FP16）需要更少的资源，但它的精度较低。所以，选择哪种“杯子”取决于我们的需求：是需要精确度，还是想要快速和效率。

类别	说明	Bits	精度
FP32 (floating point)	<ul style="list-style-type: none"> 长期用于评估深度学习性能基准值 对于很多HPC科学计算（特别是迭代计算）精度是不够的，会导致误差的累加效应 	32-bit	Single-precision 单精度
TF32 (Tensor Float)	<ul style="list-style-type: none"> A800新的数据精度模式 对AI负载的数据精度要求有足够冗余 格式与FP32相同，可以在FP32运行，无需更改代码 在深度学习和HPC应用加速FP32输入/输出更容易的方式 	19-bit	
FP16	<ul style="list-style-type: none"> 深度学习在倾向于采用FP16而不是FP32，较低的精度计算似乎对神经网络 性能影响不大，额外的精度没有任何好处，同时速度变慢，占用更多内存 	16-bit	Half-precision 半精度
Bfloat16 (Brain floating point)	<ul style="list-style-type: none"> A100是第一款支持此精度的GPU 由Google设计，用于硬件加速机器学习算法 提供与FP32相同的动态范围 有取代FP16的倾向 	16-bit	Half-precision 半精度
FP64	<ul style="list-style-type: none"> 用于精度要求较高的科学计算 通常不用于深度学习计算 	64-bit	Double-precision 双精度

4. GPU通信技术

AIGC大模型的训练对算力的要求是非常庞大的，虽然单卡的计算能力在不断提升，但是对于百亿级参数量的模型，需要利用多台计算设备进行并行计算，增加总体的计算能力，从而提升AIGC大模型的训练性能和准确度。在分布式训练中，不同设备上的计算节点需要共享和传递参数，以保持模型在整个训练过程中的一致性。因此，跨设备的通信是实现参数传递和更新的重要手段。无论是单机多卡还是多机多卡，GPU之间需要有超强的通信支持。

单机多卡GPU通信

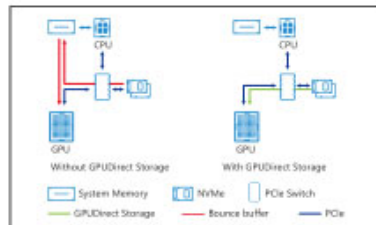
GPU Direct是NVIDIA开发的一项技术，可实现GPU与其他设备（例如网络接口卡（NIC）和存储设备）之间的直接通信和数据传输，而不涉及CPU。

传统上，当数据需要在GPU和另一个设备之间传输时，数据必须通过CPU，从而导致潜在的瓶颈并增加延迟。使用GPU Direct，网络适配器和存储驱动器可以直接读写GPU内存，减少不必要的内存消耗，减少CPU开销并降低延迟，从而显著提高性能。GPU Direct技术包括GPU Direct Storage、GPU Direct P2P、GPU Direct RDMA和GPU Direct for Video。

◆GPU Direct Storage

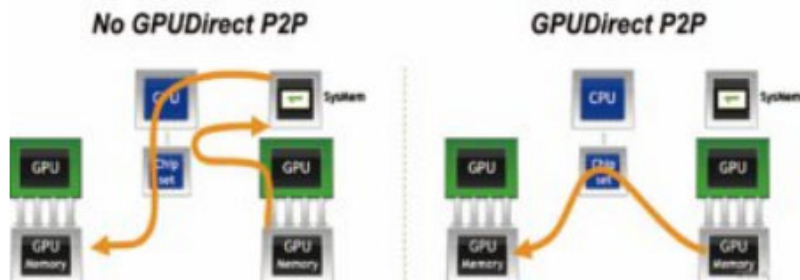
GPU Direct Storage允许存储设备和GPU之间进行直接数据传输，绕过CPU，减少数据传输的延迟和CPU开销。

通过GPU Direct Storage，GPU可以直接从存储设备（如固态硬盘（SSD）或非易失性内存扩展（NVMe）驱动器）访问数据，而无需将数据先复制到CPU的内存中。这种直接访问能够实现更快的数据传输速度，并更高效地利用GPU资源。通过绕过CPU，实现GPU和存储设备之间的直接通信，GPU Direct Storage减少了CPU开销，并释放CPU资源用于其他任务，从而改善了系统的整体性能；消除了数据通过CPU的传输路径，从而最小化了数据传输的延迟。这对于实时分析、机器学习和高性能计算等对延迟敏感的应用非常有益，允许多个GPU同时访问存储设备，这对于需要大规模并行处理和数据分析的应用起到至关重要的作用。



◆GPU Direct P2P

随着运算数据量的不断攀升，GPU间需要大量的交换数据，GPU通信性能成为了非常重要的指标。在没有GPU Direct P2P技术的情况下，来自GPU的数据将首先通过CPU和PCIe总线复制到主机固定的共享内存。然后，数据将通过CPU和PCIe总线从主机固定的共享内存复制到目标GPU，数据在到达目的地之前需要被复制两次，有了GPU Direct P2P通信技术后，将数据从源GPU复制到同一节点中的另一个GPU不再需要将数据临时暂存到主机内存中。如果两个GPU连接到同一PCIe总线，GPU Direct P2P允许访问其相应的内存，而无需CPU参与。前者将执行相同任务所需的复制操作数量减半。



在GPU Direct P2P技术中，多个GPU通过PCIe直接与CPU相连，而PCIe的双向带宽不足，当训练数据不断增长时，PCIe的带宽满足不了需求，会逐渐成为系统瓶颈。为提升多GPU之间的通信性能，充分发挥GPU的计算性能，NVIDIA于2016年发布了全新架构的NVLink。NVLink是一种高速、高带宽的互连技术，用于连接多个GPU之间或连接GPU与其他设备（如CPU、内存等）之间的通信。NVLink提供了直接的点对点连接，具有比传统的PCIe总线更高的传输速度和更低的延迟。但是NVLink技术无法使单服务器中8个GPU达到全连接，为解决该问题，NVIDIA在2018年发布了NVSwitch，实现了NVLink的全连接。

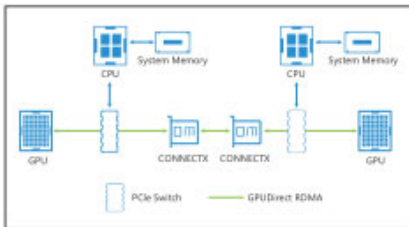
多机多卡GPU通信

AIGC大模型的训练通常需要处理大量的数据，多机多卡的计算是一个常态，多机间的通信是影响分布式训练的一个重要指标。RDMA技术通过绕过操作系统内核，直接将数据从内存中读取并传输到目标内存中，从而大大提高了数据的传输速度和效率。

◆GPU Direct RDMA

GPU Direct RDMA结合了GPU Direct加速计算和RDMA（Remote Direct Memory Access）技术，实现了在GPU和RDMA网络设备之间直接进行数据传输和通信的能力。它允许GPU直接

访问RDMA网络设备中的数据，无需通过主机内存或CPU的中介。GPUDirect RDMA专为满足GPU加速需求而设计，可在远程系统中的NVIDIA GPU之间提供直接通信。这消除了系统CPU和通过系统内存所需的数据缓冲区副本，从而使性能提高10倍。



结语

GPU作为一种高性能并行处理器，已经在众多领域展现了其强大的计算能力和应用潜力。随着人工智能、深度学习、大数据分析等领域的飞速发展，GPU技术将继续向前迈进。GPU技术的发展与国家人工智能、高性能计算和云计算等领域的重视息息相关，各大科技企业和研究机构将加大对GPU技术的研发和创新。

新华三集团作为数字化解决方案领导者，致力于成为客户业务创新、数字化转型值得信赖的合作伙伴，将深入研发GPU服务器，积极拥抱当前开放的市场环境，推动该领域的创新和发展。我们将致力于提供更加强大、可靠和智能的ICT设备和解决方案，为百行百业的进步和发展贡献力量。

AIGC在交通规划领域的应用探讨

文/沈明宇

AIGC（Artificial Intelligence Generated Content），全称人工智能生成内容，无疑是当今IT领域最热门的技术之一。自2022年底OpenAI公司发布ChatGPT以来，基于其开发的应用已多如牛毛，促进了搜索引擎、文本生成、图像生成等领域跨越式发展，已经在互联网、媒体、教育等行业掀起了一轮革新风潮。

AIGC在交通规划领域同样有着广泛的应用前景，不仅可以用于文本编撰、知识问答等基本的办公场景，而且在交通规划数据处理、各种交通方式出行量预测等生产场景也能发挥重要作用。

本文以新华三百万灵犀私域大模型为例，探讨AIGC在交通规划领域的应用。

一、AIGC概述

人工智能的发展历程可以追溯到上世纪50年代，随着计算机技术的发展，人工智能技术也得到了不断的推动和进步。进入21世纪以来，大数据时代的到来为人工智能技术带来了新的挑战 and 机遇。一方面，海量数据的收集和分析需要更加高效和准确的方法和技术；另一方面，大数据也为人工智能的应用提供了更加广阔的领域和前景。在这样的背景下，AIGC应运而生。



AIGC是一种基于Transformer结构的深度学习模型，它通过多层的自注意力机制和前馈神经网络进行训练和学习。其中，Transformer结构是AIGC的核心组成部分，它通过自注意力机制对输入序列进行建模，从而实现了长距离依赖关系的有效捕捉。在预训练阶段，AIGC使用大规模的语料库进行训练，从而学习到丰富的语言知识和表达方式。在生成文本时，AIGC通过解码器生成输出序列，同时利用自注意力机制对输入序列进行建模，从而实现了输入序列的语义理解和生成。

AIGC与以往的机器学习、深度学习等人工智能模型在数据结构与算法、训练方式、应用场景、计算资源要求等方面有明显差异。比如：在应用场景方面，AIGC可以应用于自然语言处理、文本/图像/音视频生成、对话系统等领域，具有更广泛更通用的应用场景。而传统的机器学习模型通常只针对特定的任务进行训练，应用场景相对有限。结合AIGC在自然语言/计算机编程语言处理、对话等方面的能力，以及传统机器学习模型在特定场景下的能力，可以帮助编程能力短缺的交通从业者顺利开展交通运输工程与计算机科学交叉学科的相关研究。

新华三百业灵犀LinSeer私域大模型采用自主研发动态混合专家（Dynamic Mixture of Experts）模型技术，是具备多模态能力的生成式预训练大语言模型，能够根据输入的任务类型和内容，动态地选择和组合不同的专家模型，从而实现更高的预测性能。

二、交通规划领域的“老大难”问题

在交通规划行业的生产领域运用最多的是“四阶段法”，该方法由英国交通工程师高特（Gordon）在1950年提出，并在后来的发展中得到了广泛的讨论和完善，时至今日国内仍有很多交通规划设计院在使用该方法。“四阶段法”是指交通规划的四个阶段，包括交通发生与吸引、交通分布、交通方式划分和交通量分配。

“四阶段法”在交通规划中具有重要地位，它可以帮助规划者了解交通需求和交通流量的变化情况，为道路网络的设计和优化提供依据。然而，这种方法也存在一些问题，一方面在第一阶段需要确定小区居民出行发生量和吸引量与小区土地利用、社会经济特征等变量之间的定量关系，预测的结果可能存在误差，这会影响到后续的交通分配和方式划分；另一方面，在第三阶段确定出行量中各交通方式所占比例时，需要依赖大量的人工调查，成本高却效果不佳。此外，该方法忽略了土地利用、交通网络和其他社会经济因素之间的相互作用，而这些因素可能会对交通需求产生影响。

正是因为影响交通出行的因素繁多，且各因素之间的相互作用关系错综复杂，导致交通规划的误差通常较大。交通规划的不准确给交通基建带来或投资不足或投资浪费的问题，造成要么“路修少了，不能满足人们出行需求”，要么“路修多了没车跑，资源浪费”的尴尬局面。

而大数据技术和AIGC技术分别在处理海量出行数据，以及发现交通出行与交通要素之间繁杂关系有着各自的优势，有望为交通规划者解决交通规划领域的“老大难”问题。该方法相较于“四阶段法”，主要区别如下表所示：

类别	四阶段法	大数据 +AIGC
方式	集计	非集计
数据来源	人口普查数据、土地规划数据、交通调查数据、社会经济数据等	手机信令数据、铁路客票数据、地图数据等
数学模型	重力模型、Logit模型、最短路径模型等	机器学习、深度学习、Transformer模型等
软件工具	TransCAD等	爬虫、ArcGIS、AIGC助手等
基本原理	阶段一、根据土地利用性质计算各交通小区的到发总量 阶段二、使用重力模型计算各交通小区之间的到发量分布情况 阶段三、问卷调查采集数据，使用Logit等离散模型计算二阶段中各小区到发量在不同交通方式的分担率 阶段四、使用最短路径模型将阶段三流量分配到路网	Step1、从运营商获取脱敏后的手机信令数据，包含出行者的基础信息，利用大数据清洗/分析等手段，提取出与交通出行的相关信息 Step2、使用AIGC技术训练出包含出行规律的AI模型 Step3、使用全样本出行者的手机信令数据推理出每次出行的交通方式 Step4、分类统计出行信息，得出交通方式分担率、路网流量等信息

简单而言，结合大数据和AIGC技术，可以将交通规划工作聚焦到每一个出行者身上，让AI刻画出行者的个人特征和交通方式的特征之间的相互关系。通过训练得到一座城市甚至一个城市圈的出行特征大模型，可推理未来的出行数据，从而引导交通规划工作。

三、用AIGC预测城际出行交通方式

本文选定交通规划中的城际出行交通方式划分领域，采用我国西南某两座城市之间的实际出行数据来验证新华三百业灵犀私域大模型在预测城际出行交通方式的能力，并体验使用过程。

1. 城际出行大数据处理

有别于四阶段法中问卷调查的方式预测交通方式划分比例，本文采用大数据技术与AIGC技术进行城际出行方式的预测。本文使用一周内发生过城市A-城市B城际出行行为居民的手机信令数据，原始数据集共计26.2亿条数据，约63G，数据来源于移动运营商。数据经过脱敏处理，用户识别号为完全匿名的加密代码，数据仅用于科学研究，研究结论均以集计的方式呈现，符合个人信息保护法和数据安全法，保证用户的隐私安全。手机信令数据中包含的信息有用户的性别、年龄、套餐费用、与基站进行通信时的时刻、基站的位置信息等。

除此之外，本文从高德地图API接口调取兴趣点数据，包含学校、医院、住宅区、商务区、景区、购物中心等类别的位置信息。使用地理空间数据处理软件ArcGIS对手机信令中基站坐标信息中隐含的城际段出行方式、市内段出行方式、出发时刻、城际段出行时间、出行目的等多个方面进行挖掘，将原始的手机信令大数据转化成为城际出行大数据。

通过对原始数据集进行数据清洗、挖掘、分析等工作后，最终得到22万条有效出行数据。从铁路12306客票系统获取研究时间范围内的客票数据，用以验证大数据处理结果的准确性。通过对比客票数据与经处理后选择铁路方式的手机信令出行数据发现，总体准确率达93.25%。城际出行大数据处理工作的结果优异，处理后的数据集满足使用AIGC预测城际出行方式的研究要求。

用户标号	性别	年龄	出发城市市内段出行方式	城际段出行方式	到达城市市内段出行方式	出发城市市内段出行耗时	城际段出行耗时	到达城市市内段耗时	出行目的	手机套餐资费
1	男	25	地铁	动车	出租车	60分钟	35分钟	20分钟	上学	49元

大数据提取城际出行信息示例

2. 数据集定义与处理

城际出行方式的预测问题可以抽象为一个AI领域的分类问题，即根据影响城际出行方式选择的因素，如出行者的性别/年龄/手机套餐资费、出发城市市内段出行方式、到达城市市内段出行方式等，判别某位出行者在选择城际出行交通方式时应当归属于本文预测范围（小汽车、长途汽车、普速列车和动车组）的哪一类。

将数据集进行定义和编码处理。

变量	变量含义	特征值
x_1	sex	0: 男, 1: 女
x_2	age	1: 20岁以下; 2: 20-30岁; 3: 35-55岁; 4: 55-65岁; 5: 65岁以上
x_3	tool_o2s	1: 公交; 2: 地铁; 3: 出租车和网约车; 4: 私家车; 5: 其他
x_4	time_o2s	1: 30分钟内; 2: 30-60分钟; 3: 60-120分钟; 4: 120分钟以上
x_5	time_cj	1: 1小时内; 2: 1-2小时; 3: 2-3小时; 4: 3-4小时; 5: 4小时以上
x_6	purpose	1: 工作; 2: 上学; 3: 旅游; 4: 就医; 5: 回家; 6: 其他
x_7	tool_s2d	1: 公交; 2: 地铁; 3: 出租车或网约车; 4: 私家车; 5: 其他
x_8	time_s2d	1: 30分钟内; 2: 30-60分钟; 3: 60-120分钟; 4: 120分钟以上
x_9	fee_phone	1: 49元内; 2: 49-99元; 3: 100-199元; 4: 200-299元; 5: >299元

影响因素定义与编码

表中输入变量名的含义分别为，sex表示性别，age表示年龄，tool_o2s表示出发城市市内段出行方式，time_o2s表示出发城市市内段出行耗时，time_cj表示城际段出行耗时，purpose表示城际出行目的，tool_s2d表示达到城市市内段出行方式，time_s2d表示达到城市市内段耗时，fee_phone表示手机套餐价格。其中，age、time_o2s、time_cj、time_s2d和fee_phone本为连续变量，划分为如上表所示的分类水平主要结合其数据分布情况以及实际含义作为依据。

此外，针对sex、tool_o2s、purpose和tool_s2d这4个离散名义变量，需要进行独热编码（One-Hot Encoding）处理。结果如右图所示：



城际段出行方式作为机器学习模型训练数据集中的标签，测试数据集中的预测结果，其编码方式如下表所示：

出行方式	小汽车	长途汽车	普速列车	动车组
Y	0	1	2	3

输出变量编码

输出变量，即标签无需进行独热编码处理，是因为分类模型可以自动识别。但对于本文这样的多分类问题，为适应模型要求通常需要从“0”开始编码。

3. 使用AIGC完成模型训练与推理验证

本文选用解决分类问题效果较好的随机森林模型用于实例分析，借助新华三百业灵犀LinSeer私域大模型AIGC能力，使用AI助手工具用训练数据集完成模型的训练与参数调优，用测试数据验证模型的准确率。过程如下图所示：



输出结果如下表所示：

实际\预测	小汽车	长途汽车	普通列车	动车组
小汽车	30154	0	0	817
长途汽车	0	883	201	434
普通列车	0	0	8385	231
动车组	1209	0	375	23918

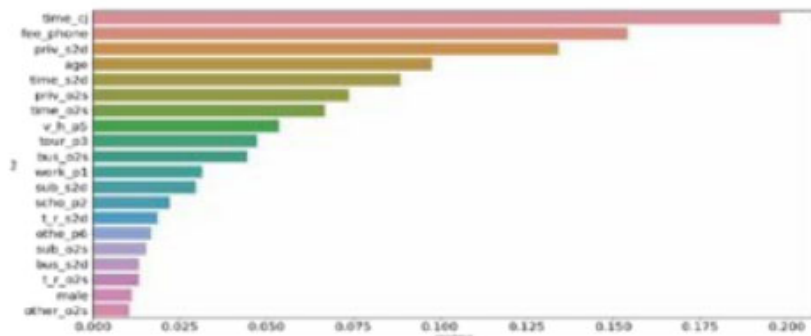
预测结果分析-混淆矩阵

评价指标	accuracy	f1值	运行时间
值	0.9555	0.9546	453.79s

模型评价指标与运行时间

从上述模型的评价指标来看，使用新华三AI助手完成训练与调优的随机森林在测试数据上的预测结果表现优秀，预测准确率达95.55%，f1值（精准率和召回率的调和平均）为95.46%。总体来看，模型预测能力优异，对小汽车的预测准确率最高，对少数类长途汽车的预测准确率最低。

针对已经完成训练和测试的随机森林模型，让AI助手绘制影响因素的排列重要性图：



如上图所示，城际段出行耗时（time_cj）的排列重要性最高，为0.1991，意味着将数据集中的time_cj列随机打乱后将会使随机森林模型的预测准确度下降19.91%，影响最大。主要是因为城际出行耗时作为城际出行方式自身的重要属性，其次，时间成本作为广义费用的一种，是城际出行者选择城际出行方式时考虑的重要因素。

城际出行者手机套餐价格（fee_phone）作为第二重要的影响因素，重要度值为0.1525，主要是因为手机套餐作为一种消费产品，同城际各种交通工具所提供的运输服务类似，具备一定程度地衡量用户经济水平的功能。

priv_s2d是经过独热编码处理后，到达城市市内段出行方式（tool_s2d）的一种，表示的是在到达城市采用私家车的方式完成市内出行，排于第3重要度为0.1336，该特征之所以影响较为显著主要是若到达城市市内段采用私家车的方式出行可以推断城际段、出发城市市内段大概率也采用私家车的方式出行。同样的，排于第6位的priv_o2s重要度高的原因与之类似。

年龄（age）的重要度为0.0979，排在第4位，主要是不同年龄段对于所选的城际出行方式偏好有所不同，且不同年龄群体与不同城际出行方式之间存在一定的映射关系。

排于第5位和第7位的分别是到达城市市内段出行耗时 (time_s2d) 和出发城市市内段出行耗时 (time_o2s), 重要度分别为0.0889和0.0689, 这两个特征反应城际出行者对于时间属性的偏好, 一定程度上潜在的影响着城际出行方式的选择。

从上述分析可以发现, 相较于出发城市的市内交通方式与市内出行耗时, 到达城市的此类特征具有更高的排列重要度。从定性分析的角度, 可以得出城际出行者在发生城际出行行为过程中, 相比于出发城市, 到达城市市内的出行方式与出行耗时会更加显著的影响城际段出行方式的选择。换言之, 在城际出行过程中, 出行者更加注重到达城市的交通条件。

以上是对于各个排列重要度比较高的特征变量的解读, 随着重要度的降低, 代表特征对于城际出行交通方式选择的影响越来越小, 故不再过多描述。

结语

本文结合热点技术——AIGC的特点, 探讨其除基础的文本生成、知识问答等应用之外, 在交通规划专业领域的应用效果。本文融合手机信令、地理空间、POI等多源大数据, 使用数据清洗、数据分析等方法提取城际出行大数据, 借助新华三百业灵犀私域大模型AIGC能力训练出城际出行交通方式预测模型, 一改传统交通规划四阶段法的“老大难”问题。研究的主要结论如下:

- 将城际出行交通方式预测问题研究抽象为分类问题, 使用随机森林模型进行训练调优与推理验证。完成训练调优的城际出行交通方式预测模型准确率达95.55%, 使用该模型并结合运营商的全量手机信令数据即可较为精准地预测城际出行各种交通方式的分担率及交通量, 为交通规划师调整城际间高速公路、高速铁路、普速铁路等的建设方案或开行方案提供参考。利用AI助手绘制的排列重要性图得到了城际段出行耗时 (time_cj) 是影响城际出行交通方式选择程度最强因素的结论。

- 利用AIGC可以实现自动模型构建和优化, 无需手动调参和优化。为非计算机专业的交通行业从业人员提供了一种简化复杂任务的解决方案, 不需要过多关注底层算法和编程细节。新华三百业灵犀私域大模型提供一站式服务平台, 集成AI助手, 帮助交通行业从业者用好大模型, 快速构建智能应用, 实现模型使用自由。AIGC拥有优秀的分类性能和泛化能力, 可以快速准确地处理大量数据和复杂问题, 在处理城际出行方式选择行为这种类似分类问题方面

表现优异。需要注意的是, 虽然AIGC简化了模型构建和调参的过程, 但仍然需要一定的理论基础和背景知识来选择和解释合适的特征, 评估模型性能, 并解释结果。对于非计算机专业人员而言, 了解基本的机器学习和数据分析的概念, 可以更好地利用AIGC, 并与领域专业知识相结合, 发挥其最大的价值。

展望

AIGC在交通行业的应用, 除上文主要讨论的交通规划领域之外, 在专业知识库积累、运维管理、运营计划编制、客票定价策略、应急调度指挥、旅客服务、商业广告等领域也可能发挥其革新作用。

比如, 通过交通行业积累的大量专业资料, 包括专业规范、书籍、文献、论文以及项目经验等, 这些都可以作为专业知识库提供给AIGC私域大模型进行学习训练, 得到交通行业专业知识大模型, 完成专业知识库的积累。

AIGC的发展趋势正在朝向更广泛的应用领域、更高的智能化程度以及更深入的个性化服务拓展。在不久的将来一定会在交通行业中发挥重要作用, 大幅提升效率并创造新的价值。



致谢

《新华三交通行业数字化转型》白皮书历时近一年，30余位专家参与编纂，终于呈现在大家面前。在编纂过程中，我们深感一份责任与挑战。首先，我们要向所有信任并支持本白皮书的行业客户表示最诚挚的感谢。正是因为你们的热情参与和实践分享，我们才得以深入探讨交通行业在数字化热潮中的转型之道。同时，对于与我们肩并肩合作的行业伙伴们，感谢大家的无私支持和通力合作，历经沉淀后终于使得这本白皮书的每一页都充满了智慧与启发。

在交通行业数字化转型的征途上，我们希望这本白皮书能够成为行业同仁探索未知、加速前行的“最佳搭档”。对于其中的不足，我们期待并欢迎广大读者的宝贵意见，让我们共同将这份探究进行到底。再次感谢所有为这本白皮书付出心血和智慧的朋友们，智变大交通二十载，感恩与您一路同行。

精耕务实，为交通赋智慧！

专家名单

肖春喜、胡伯瞳、辛龙超、吕飞、王泽宁、郝亚东
李洋龙、刘铖、刘杰、张一琛、李婧、刘木伟
葛云峰、张仁琳、邵宁、沈明宇、史钰果、王宇
闫泽瑞、童修品、王雪梅、梁宏、王文刚、肖斌
汤贤伟、陈楠、张婷、刘亚茹