

NAVIGATE 数字金融

Digital Finance
— 第 03 期 —

铿锵三十年，与金融科技创新相伴而行 P07

为金融行业用心构筑极致服务体验 P15

浅谈智能运维实践 P17

金融IT系统现代化之——智能运维转型 P41

新华三金融智能网点解决方案 P47

人工智能在金融安全中的应用 P55



—— 数字金融 • 智变科技 ——



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 © 2020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含有技术性误差或印刷性错误,
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-201030-20200709-BR-5D-V1.0



目录



CONTENTS



【主办】 新华三集团金融事业部

【总编】 李乔

【编辑】 闫军、纪钟、宿梦婷、张静华

01

卷首语

01 铿锵三十年，与金融科技创新相伴而行
新华三集团副总裁、金融事业部总经理 李乔

05

新华三资讯

05 走进2020领航者峰会，与“智·变”时代同行
11 从芯出发，相约云上！2019-2020紫光集团的年度高光时刻
13 紫光集团成立云与智能事业群 打造全面统一的新紫光云

15

专家解读

15 为金融行业用心构筑极致服务体验
新华三集团副总裁、技术服务部总裁 陈孝毅
文 / 转载金融电子化记者深度解读文章

17

智能化

17 浅谈智能运维实践
23 大型银行自动化运维规划实践
32 新一代智能运维平台建设探讨
36 数字化转型时代、AI重构网络联接
41 金融IT系统现代化之一——智能运维转型
45 通用人工智能计算
47 新华三金融智能网点解决方案
51 金融行业分支网点机房的智慧化之路
55 人工智能在金融安全中的应用
59 金融视觉中枢，推动智慧金融加速落地

刊首语



铿锵三十年， 与金融科技创新相伴而行

新华三集团副总裁、金融事业部总经理 李乔

当前，新一代人工智能正在全球范围内蓬勃发展，为经济社会发展注入了新动能，并深刻改变着人们的生产生活方式。作为高度数据化的行业，金融是智能技术重塑业务价值的最佳场景之一，在大数据、人工智能、物联网、区块链等一系列创新技术的加持下，正在实现管理模式、运营模式、服务模式的全方位重塑，推动自身向智能化方向快速演进。如今，网络支付、供应链金融、智慧网点、开放银行等概念的兴起，赋予了社会发展更加智慧的金融服务，未来的金融业更将进一步实现全面的网络化、数字化、智能化，金融服务将无感知、无摩擦地存在于社会经济生活的方方面面。

在紫光旗下新华三集团看来，透过数据、算法、算力和应用的能力提升，金融企业可以更加平滑的与各类数字化场景对接，从前端的客户服务，到中台的业务决策，再到后台的风险防控，全方位地提供更加个性化、普惠化、智能化的金融服务，使金融服务做到真正的如影随形，从而迎来一个更加智能化的金融服务新时代。

随着数字化进程的深化，金融企业进一步加速金融科技的发展。由各家大中型金融机构科技部门分离出的金融科技公司也像雨后春笋般建立。未来的金融服务将涵盖客户的全生命周期，令产品营销更精准、客户体验更优异、运维更便捷已成为金融企业关注的焦点。智能化技术的应用是解决这些关注点的利器，透过数据、算法、算力和应用的能力提升，金融企业可以更加平滑的与各类数字化场景对接，无缝地为社会提供更多的智能化金融服务，使金融服务做到真正的如影随形！

关注数据的质和量

在金融走向智能化的过程中，数字价值的分析、洞察和汇聚是驱动行业变革的基础。金融企业传统的交易数据品质较高，如会计总账、账户信息、交易流水、客户信息、行情数据、保单信息等都是金融企业宝贵的数据财富。但是随着场景外延的扩展，如票据影像、监控视频、单据合同、运维数据、征信信息、理赔数据等新衍生的海量大数据飞速增长。面对种类繁多且海量的内外部数据资源，金融行业更需要以数据治理来实现数据质量的优化和改善。

AI等智能技术在金融行业的应用中，数据治理是有效实现大数据管理与交互的利器，透过数据治理可以实现对数据服务的统一规划与实施。可以说，数据治理的输出就是金融智能的输入，数据治理可以为金融智能提供高质量、更合规、更有效的数据，为金融智能的精准分析提供了基础，同时金融智能对数据的评价反馈也能更好地推进数据治理的优化工作。新华三在大数据生命周期管理和数据治理领域积累了大量的实践经验和人才，在为金融客户提供丰富存储产品和大数据平台的同时可以为客户提供数据治理、数据生命周期管理、大数据分析等咨询与实施服务。

构建高效的智能化算法支撑平台

人工智能的算法种类繁多，卷积神经网络算法常用于深度学习、贝叶斯算法常用于推理分类、模糊均值FCM算法常用于聚类。面对日新月异的AI创新，尽管开发人员可以从TENSORFLOW、PYTORCH、CNTK等计算框架中直接调用这些算法进行智能金融应用的开发，但开发管理可视化、模型部署一键化、算法库支持平台化等手段，仍然是进一步提升金融应用创新速度的关键，一套高弹性、易扩展的可视化人工智能开发环境，会逐步成为开发智能金融应用的必备要素。

新华三在参与金融行业人工智能应用项目中，先后开发出了应用于深度学习的AIOS支撑平台和应用于推理的AINF支撑平台，能很好地支撑人工智能服务器集群内的跨平台作业调度、模型训练与管理、资源监控和快捷部署，可以有效降低开发复杂度，最终实现提升智能应用的快速创新能力。面向金融科技场景的智能化要求，新华三将依托强大的研发能力展开与金融科技企业的联合共研，助力企业AI能力建设。

依靠先进的计算资源提升算力

在数据和算法之后，算力的升级同样是驱动AI创新的三个支点之一。智慧计算是当前数字基础架构演进的焦点，面向深度学习的专用人工智能服务器、面向推理的通用服务器以及基于AI的边缘计算服务器正在齐头并进，NVLINK、PCIE等高速互联技术逐渐成为关注点。同时，在人工智能集群内，双宽高性能GPU、专用TPU、带宽可达400G以太网骨干、具备ROCE能力的无损以太网技术等一系列创新技术的应用，将更高效地支持集群计算。而在面向推理的人工智能大规模应用场景下，基于单宽GPU、FPGA或ASIC等正成为主流技术。

在GPU和FPGA的应用上，新华三经与金融客户的深度合作，发现GPU比较适合深度学习的应用场景，而在某些算法模型推理的大规模实践上，FPGA却有着低成本和高性能的优势。但FPGA的使用不像GPU简单易用，需要服务器厂家提供底层固件的支撑以及专业的FPGA技术团队。新华三协同第三方合作伙伴尝试帮助金融客户在推理服务器领域由GPU向FPGA转化，在提升算力、降低处理时延的同时降低了用户的采购成本。

金融智能化应用会在多层次展开

金融企业在客户满意度、运行效率、降低总成本、风险控制和高效监管等方面的要求是长期的，通过智能化的引入会大大提升相关能力。从大的分类来看，有面向经营的业务类场景和面向支撑的运维类场景。金融业人工智能已广泛应用于票据识别、身份认证、反洗钱、反欺诈、风险识别与预警、智能客服、信贷决策、价值客户营销、自动化核保与理赔、智能投顾、量化交易等领域，透过特定的算法和推理模型，很多金融企业取得了巨大的市场竞争优势。人工智能的应用本身会涉及到多个领域的生态，新华三一方面推进在自身的IT基础设施相关的ABC业务能力平台和产品中应用，另一方面会支持与各细分领域的第三方金融科技团队合作，一起让智能化技术成为新时代金融科技的基石。

在支撑和运维场景中，人工智能则主要侧重于IT智能运维（AIOps）、基于态势感知的主动安全防护、预测性维护、智能监控、系统和网络洞察等领域，透过人工智能给IT系统赋能，使得IT系统更稳定、安全、敏捷且易于维护。人工智能的应用从计算智能阶段发展到认知智能阶段，可以更敏捷地对趋势进行预判，极大提升了决策精准度和决策速度。相信将来随着人工智能技术的成熟，必将在更多关注效率的金融科技领域承担重要角色。

人工智能的应用本身会涉及到多个领域的生态，新华三一方面推进在自身的IT基础设施相关的ABC业务能力平台和产品中应用，另一方面会支持与各细分领域的第三方金融科技团队合作，一起让智能化技术成为新时代金融科技的基石。

重新定义智能化的金融新时代

如今，走过电子化、信息化、互联网化阶段的金融行业已经构建起智能技术融合应用的丰厚土壤，由各家大中型金融机构科技部门分离出的金融科技公司正像雨后春笋般纷纷涌现。

为了应对当前金融科技创新带来的新挑战和新机遇，新华三以实现最终用户体验最佳为目标，紧贴时代发展新趋势，打造了面向应用的全场景数字金融平台。通过在数字基础设施、双态ABC融合平台、主动安全和统一运维方面的全栈式技术积累，实现数字金融平台的定制开发、升级迭代。在核心产品和解决方案层面提供全场景金融云、关键业务系统、大数据与人工智能平台等一系列云与智能相互融合的独特能力，从而支持智能网点、智能营销、智能风控等一系列金融服务创新的新场景、新应用。

作为中国领先的金融云与金融IT基础设施提供商，新华三以实力领航金融科技创新与变革。在传统金融IT领域，新华三参与了大量的客户数据中心及分支建设。新华三不仅具备传统核心业务承载的广泛实践，在开放核心和云核心平台上也有很多成功实践，满足多场景客户需求。智变时代，新华三践行智能战略AI IN ALL，以云与智能平台作为核心引擎，以向内生智能演进的数字基础设施为基石，全面升级智能的主动安全能力和统一运维能力，致力于成为金融企业数字化转型最可信赖的战略合作伙伴，全面拥抱金融数字化、智能化变革。



李乔 新华三集团副总裁、金融事业部总经理 李乔

李乔（GEORGE LI）先生作为高级管理人员拥有18年丰富的IT行业从业经验，非常熟悉企业级软件、硬件和服务市场，以及IT对客户业务战略的促进，并对金融、互联网、政府等核心行业有深刻理解。

李乔先生从2003年到2016年在杭州新华三工作期间先后历任数据通信产品行销部经理，政府系统部总监等职位，实现所负责领域的快速增长。新华三成立后，李先生于2016年至2017年就职新华三集团副总裁，分管集团技术咨询销售工作，建立了完善的技术咨询服务团队，实现了原惠普中国与原杭州华三两个技术咨询板块的整合优化，自2018年起在金融事业部任职。

新华三资讯

走进2020领航者峰会， 与“智·变”时代同行

2020开年，面对突发的新冠疫情，新华三首次将NAVIGATE领航者峰会移师线上，从4月20日到25日持续6天，本次线上峰会以“智·变”为主题，通过33个专题，超过120场演讲，向百行百业的企业高管、技术专家和行业数字化建设者们详尽展示了新华三在云与智能平台、智能数字基础设施、主动安全、统一运维的一站式数字化解决方案，以及联合生态伙伴共同构建智慧应用的能力。

在4月20日的主论坛上，新华三不仅发布了“AI in ALL”智能战略，彰显“让自身的产品和解决方案更具智能，助力客户的业务与运营更智能”的愿景和目标，更发布了全新升级的“数字大脑计划2020”，以重磅发布的九大新品引领百行百业的数字化转型升级。



紫光云2.0：全栈智能、全域覆盖、全场景应用

云服务的去边界化正成为当前发展的主流趋势。今年，紫光集团整合私有云、公有云、人工智能、视频云、软件服务等领域的整体能力，成立“紫光云与智能事业群”并打造全新的紫光云，实现架构统一、品牌统一、服务统一，提供全栈智能、全域覆盖的能力，以全新的“紫光云”品牌面向市场，倾力发展“云+智能”业务。

- ▶ 全栈智能：通过“AI in ALL”智能战略，把智能全面植入到IaaS、PaaS、SaaS的部件中，筑就全栈智能云。
- ▶ 全域覆盖：提供公有云、私有云、混合云、边缘云的全域覆盖，以及多云管理能力，实现“云边端”协同。
- ▶ 全场景应用：通过丰富的行业理解与深度实践，支持从智慧城市、产业互联网到百行百业全场景的云产品与云服务应用。





U-Center3.0: 智能运维全面上云, 守卫业务加速创新

智能技术正在推动运维服务在能力上向内生智能演进, 在形式上向云化服务演进。新华三运维结合自身在云和AI方面的创新实力, 将原有的U-Center统一运维平台整体迁移上云, 打造了具备云简、云享、云效和精智、专智、全智六大能力的统一运维云, 不仅开创了全新的商业模式, 更为客户的网络、数字基础设施、业务应用、终端和安全带来了全面智能化的运维服务。

U-Center3.0

AD-NET智能网络解决方案: 简化再部署, 智能新升级

万物智联时代, 海量终端快速增长, 网络架构日益复杂, 给网络的管理和运维带来了沉重负担。新华三AD-NET智能网络通过SNA架构升级, 实现了自诊断网络、自动故障隔离、部署极简、运维极简四大亮点, 通过基于意图的闭环网络系统, 在数据中心、广域网、园区网等多个应用场景当中实现管理、控制、分析的融合, 帮助客户实现构建全场景、全域、全生命周期的智能化网络。为数据中心、园区、广域网等三大主要场景及相关衍生场景搭建了高效、灵动的智慧网络。

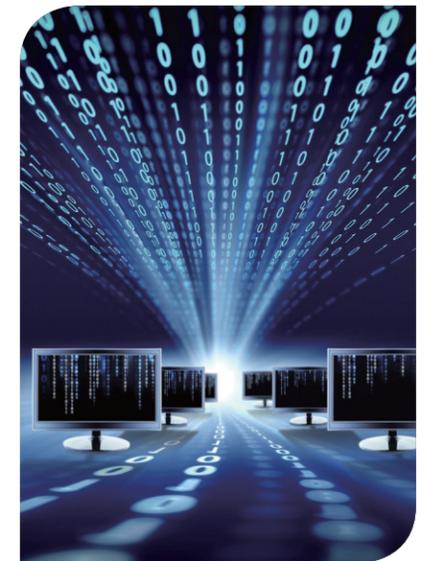
AD-NET



智能核心交换机S9825-64CD: 小盒子开启网络大时代

作为全球首发性能领先的数据中心盒式核心交换机, S9825-64CD从大机箱交换机进化为小盒子, 将摩尔定律发挥到极致, 同时能够实现链路状态精准测量, 网络态势感知与智能调优。作为AD-NET的新成员, S9825-64CD以小盒子的体型提供了64*400GE的强大性能, 实现400%的单位空间性能提升, 50%的平均单端口功耗降低以及分钟级的横向扩展Fabric, 可作为云计算下一代网络核心进行敏捷部署, 为网络的智能化演进打造平台。

S9825-64CD



关键业务智能存储系统Primera: 以智能重新定义存储的体验标准

Primera智能存储系统不仅能预先制止故障, 做到100%的系统可用性, 更拥有比上一代产品122%的性能提升, 简化运维和部署时间高达93%, 为企业创造更领先的数据存储和管理体验。同时, Primera内置AI功能, 能够实现故障预警同步和预判, 控制器的多活架构能够做到自动均衡和自动故障切换。此外, 关键的业务软件和硬件节点在提升性能的同时也实现了更智能化的管理, 全面提升数据管理和存储的效率。

PRIMERA





5G边缘解决方案：以联接的力量，加速产业模式重塑

面对5G与行业应用的融合，新华三5G边缘解决方案全面升级，从Pico RRU、pHUB、BBU到边缘云共有8款新品发布，为工业互联网等当下热门的产业技术提供更高效可靠的联接能力。其中，边缘网关UPF能够实现本地业务分流和统一管控，OTII服务器能够满足边缘机房的部署环境，而按需配置、5G全频段支持、灵活扩展、高效节能等技术优势，更能显著优化客户5G边缘解决方案的体验。



Wi-Fi 6系列7款新品：以创新引领Wi-Fi 6加速企业革新

新华三拥有业界最全的Wi-Fi 6产品组合，在率先实现全场景产品覆盖的基础上，今年新华三新增了7款产品，全部采用业界独家物联融合及具备专利的链式物联技术；软件定义射频可覆盖范围增强30%，并支持按业务需求切换射频功能；旗舰款新品WA6638i具备单机万兆10.75Gbps的最高性能，最大支持1536用户同时接入。



安全AI赋能云安全：主动安全再升级，全面满足等保2.0

新华三着力推动安全AI应用进阶，扩大数据采集广度，不断优化AI算法的使，满足海量安全数据的智能处理，并且在多种维度上持续丰富安全业务模型，从而构建以知识为中心的智能分析体系。本次全新推出的安全AI赋能云安全以云安全管理平台为核心，与SDN以及安全大数据分析器相结合，具备AI能力深度集成与赋能、软件定义的柔性规则、多场景化的安全响应、等保2.0的全面合规四大亮点。同时，新华三针对底层数据采集发布了新型检测系统，同时发布了AI+5G防火墙、AI-ACG、新一代LB等多款产品，进一步强化了安全的全面防护能力。

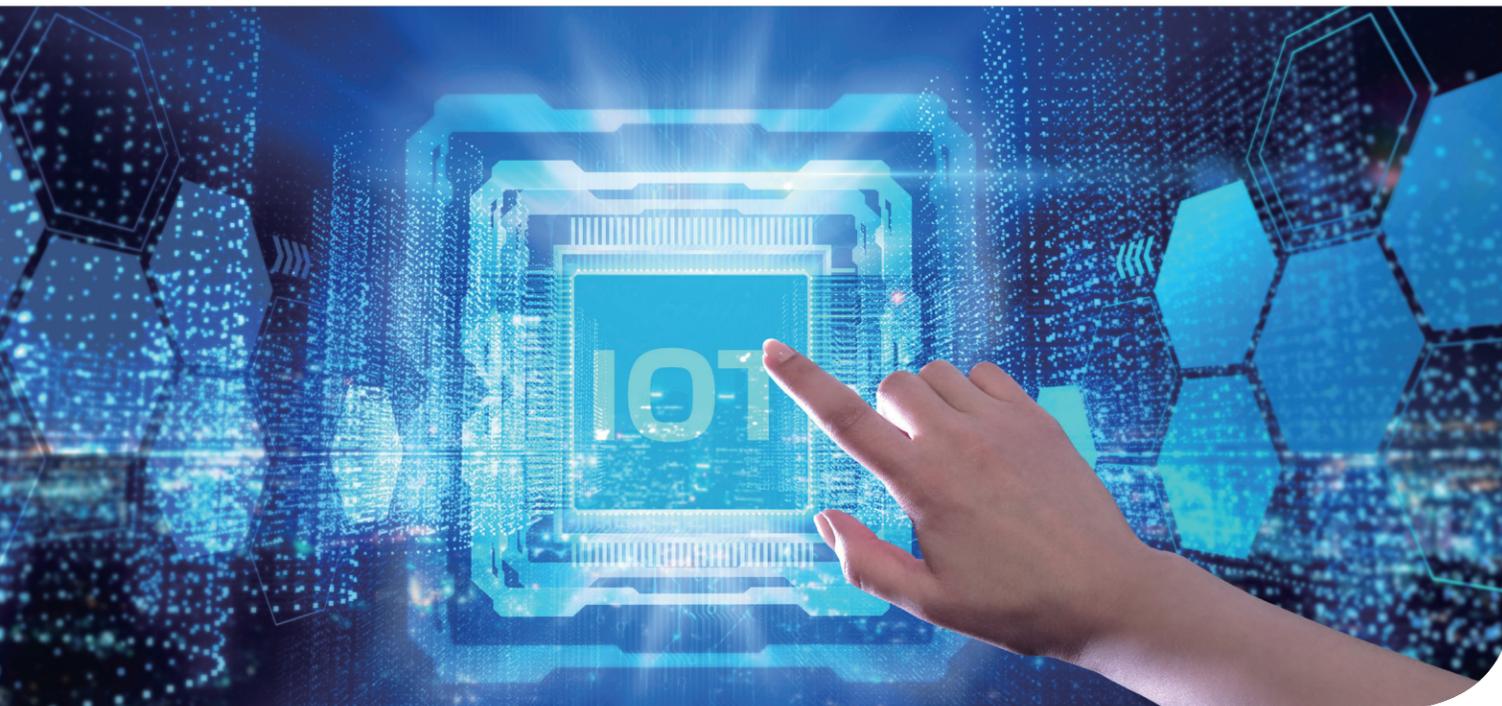


新一代融合云桌面方案：重新定义“远程工作”

H3C Workspace新一代融合云桌面解决方案具备接入灵活、运维便捷、使用安全三大核心特性，基于融合统一的桌面管理、全面升级的用户体验、深度优化的自研协议，能够全面支持金融、政务、医疗等百行百业复工复产，面对超大规模的业务并发挑战也能让远程和现场体验一致，并且能够以云端管控终端，实现软件的无感升级，从而为企业带来焕然一新的工作模式。在疫情期间，新一代融合云桌面方案支持了新华三超过万余名员工的在线远程工作和开发，并保障业务连续不中断。

基于“数字大脑计划2020”在智能数字平台和智慧应用生态方面的革新，新华三将为百行百业的数字化革新提供更具创新性的工具和平台。在金融领域，数字化变革将创造更加个性化、泛在化、智能化的金融服务体验，新华三将和金融创新者们同行同道，以持续迭代的创新技术构建数字金融可靠架构，引领金融业务再造。





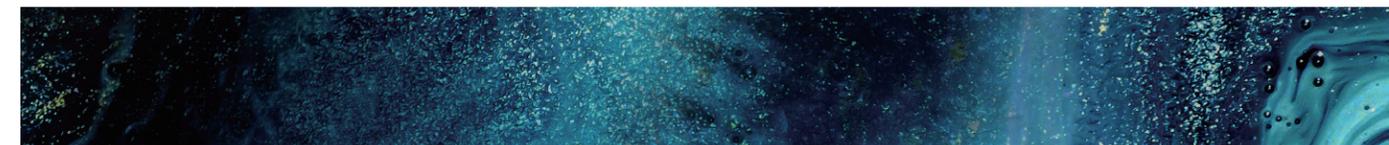
从芯出发，相约云上 ▲

2019-2020紫光集团的年度高光时刻

从智能终端设备联接5G时代的基带芯片，到开创中国存储生态新纪元的3D NAND闪存，再到具备全域融合、全栈智能优势的紫光云与智能事业群，紫光集团在过去的一年中始终在“从芯到云”的战略指引下，以自主创新引领中国科技产业的自我突破，以对于行业和用户的深刻洞察，推动百行百业数字化转型的全面跃进。

紫光展锐5G通信技术平台“马卡鲁”发布

2019年2月26日，紫光展锐在2019世界移动通信大会（MWC）上重磅发布了5G通信技术平台“马卡鲁”及其首款5G基带芯片—春藤510。这标志着紫光展锐迈入全球5G第一梯队，作为领先的5G核心芯片供应商之一，为全球消费者带来5G革命性的连接体验，推动5G商用全面提速。



紫光集团组建DRAM事业群

2019年6月30日，紫光集团决定组建紫光集团DRAM事业群，进一步拓宽紫光集团在存储器领域的相关布局，深化和完善“从芯到云”产业链的建设。在当年8月，紫光DRAM事业群总部、DRAM存储芯片制造工厂落地重庆，极大地带动了重庆市乃至中国集成电路产业的发展，对重庆深入发挥“三个作用”，布局国际国内市场，推动智能产业“补链成群”，推动经济社会高质量发展具有十分重要的战略意义。

长江存储量产基于Xtacking架构的64层256Gb TLC 3D NAND闪存

2019年9月2日，长江存储开始量产基于Xtacking架构的64层256Gb TLC 3D NAND闪存，以满足固态硬盘、嵌入式存储等主流市场应用需求。这是全球首款基于Xtacking架构设计并实现量产的闪存产品，拥有同代产品中最高的存储密度。相比传统3D NAND闪存架构，Xtacking可带来更快的I/O传输速度、更高的存储密度和更短的产品上市周期。

紫光天津芯云产业基地系列项目启动

2019年9月19日，紫光旗下立联信中国工厂暨紫光天津芯

云产业基地系列项目在天津滨海高新区启动，标志着紫光集团布局京津冀区域的第一个产业集群正式拉开帷幕。紫光天津芯云产业基地系列项目预计总投资约220亿元，作为紫光“芯云”战略重要支撑之一，未来将被着力打造成为紫光集团先进技术研发和应用的全国样本。

紫光展锐新一代5G SoC移动平台“虎贲T7520”发布

2020年2月26日，全球领先的移动通信及物联网核心芯片供应商紫光展锐正式发布了新一代5G SoC移动平台“虎贲T7520”，以先进的工艺、新一代低功耗设计，大幅提升的AI算力和多媒体影像处理能力，将为5G智能体验带来更好的选择。虎贲T7520是紫光展锐第二代5G智能手机平台，采用6nm EUV制程工艺，以及多种先进设计技术，性能大幅提升的同时，功耗再创新低。

长江存储128层QLC 3D NAND闪存研发成功

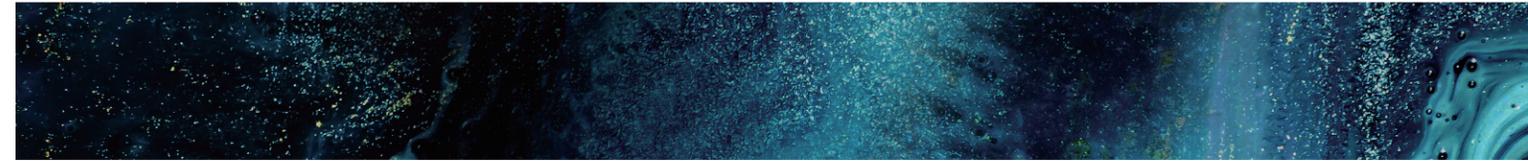
2020年4月10日，长江存储宣布其128层QLC 3D NAND闪存研发成功，并已在多家控制器厂商SSD等终端存储产品上通过验证。作为业内首款128层QLC规格的3D NAND闪存，长江存储X2-6070拥有业内已知型号产品中最高单位面积存储密度，最高I/O传输速度和最高单颗NAND闪存芯片容量，这意味着，我国在存储芯片领域率先进入世界第一梯队。

紫光集团成立云与智能事业群 ▲

打造全面统一的新紫光云

2020年4月8日，紫光集团宣布重大组织架构升级——基于紫光云网板块的整体发展战略，整合旗下公司的私有云、公有云、人工智能、视频云、软件服务能力，成立“紫光云与智能事业群”，紫光集团联席总裁兼新华三首席执行官于英涛出任紫光云与智能事业群总裁。

新成立的紫光云与智能事业群将倾力发展“云+智能”业务，有效整合紫光集团旗下云网板块的新华三集团、紫光云技术有限公司、重庆紫光华山智安科技有限公司以及紫光软件系统有限公司，致力于打造世界级的云网巨头。



发布全面统一的紫光云2.0，成为数字化转型最佳合伙人

紫光集团联席总裁兼新华三首席执行官于英涛表示，“新基建”的加速为数字经济创造了有利的条件和巨大的发展契机，市场将进一步拥抱云与智能。为此，紫光云与智能事业群不断推动“紫光云”的战略升级，以“四个统一、三个全面”为核心，为服务于百行百业的数字大脑打造核心引擎。

以新形象、新内涵出现的紫光云2.0实现紫光云的技术统一、品牌统一、市场统一、服务统一。同时，紫光云2.0还实现了私有云、公有云、边缘云以及多云服务的全域覆盖，并将AI应用于云基础设施、云原生架构、数据中台等各个领域做到全栈智能，为行业用户提供线上线下全面协同的全场景、一站式服务。

基于紫光云2.0，打造全场景金融云平台新能力

随着金融业务的多元化发展，其自身IT架构愈加复杂，在极强的监管要求下，如何实现金融业务的云化创新，如何利用云原生的技术推动业务发展，成为亟待解决的难题。面向未来，金融机构需要改变简易的资源池化管理，搭建真正弹性、便捷、高效、稳定的“金融云”。

紫光云2.0，以自身在私有云领域十年以上的技术储备，充分理解金融行业客户的诉求。在打通传统IT架构的诸项技术弊端后，还可以将已经云化的不同技术架构的私有云和

公有云进行统一管理。同时，紫光云2.0可以将公有云的诸多技术优势与行业生态，同步给本地基础设施已完成云化改造的私有云，形成同构混合云架构，同根同源的软件技术架构带来一致性的最佳体验。

紫光云2.0的私有化部署支持软硬件解耦，分层解耦能力，每一个独立组件都可以与通用的硬件平台，形成单独的解决方案来满足金融行业不同规模，不同场景的需求，每个独立组件都可以与其他云平台适配，可以给金融客户提供更多的技术选择性。

金融用户上云，在关注云平台功能性能否完全覆盖自身需求的同时，还关注是否结合业务个性化定制，是否符合监管机构的安全性要求等诸多问题。紫光云2.0为用户提供非标准的软硬件产品及功能的个性化定制，实现云平台功能及云运营的灵活定制化，各类高端设备的对接适配，形成统一的纳管，实现真正的全数据中心运营运维一体化。

为了让金融用户上云实现真正的最低总拥有成本。基于紫光云2.0，我们选择产品化组件、模块化架构设计，基于自身全面的高成熟度产品，实现任意功能模块组合选择，摆脱传统云服务厂商厚重臃肿的云平台架构限制，实现整体享受最低的总拥有成本。在技术演进连续性方面，可以从极简部署开始，逐步增加功能模块，最后在过渡到同构混合云模式，无需在规模和配套上一步到位。

综上所述，紫光云2.0能够高度结合金融客户的共性需求，满足多类金融场景，不仅能够为金融行业用户提供一致性、连续性的服务，还能够在确保安全性的同时，为金融行业用户提供一个无边界的全球的合格的云。

专家解读

为金融行业 用心构筑极致服务体验

文/转载金融电子化记者深度解读文章

引言

近日，在第三届“双态IT北京用户大会”上，新华三集团副总裁、技术服务部总裁陈孝毅，以《用心构筑极致服务体验》为主题，分享了新华三驱动智能运维转型，护佑金融科技变革的创新和实践经验。

随着互联网金融创新的普及，金融业务对信息系统的依赖程度愈加紧密，使得金融行业对业务连续性的需求不断提高。为保障重要信息系统安全稳定运行，提升业务连续性，实现对运维事件的快速定位、处置、甚至预警，金融行业信息科技部门花费了大量的人力物力建设智能运维管理平台。如何能够充分利用现有数据，提升运维服务的价值，是目前金融机构普遍关注的问题。

在二十余年的IT生涯中，我见证了运维服务从被动保障，向主动防护的颠覆式变革，一个更加智能化的运维服务模式正在揭开帷幕。根据Gartner相关报告预测，智能运维的全球部署将从2017年的10%增加到2020年的50%。科技在加速商业模式创新的同时，也在将云计算、数据分析、人工智能等技术反作用于自身的变革，云服务提供了交付运维服务更便捷的方式，人工智能等分析技术焕发数据背后的价值，达成“多、快、好、省”的运维演进目标。由此，金融行业与智能运维的结合，将开启数字金融变革与发展的新篇章。

为此，新华三为包括金融行业在内的各行各业打造了由运维平台、“运维数字中枢”和运维云组成的技术服务能力集，构建一套统一的监控平台，提供故障预警和快速故障定位，并且顺应运维向智能化的变革，助力行业客户直面运维管理和服务模式的新需求、新挑战。



陈孝毅

新华三集团副总裁、技术服务部总裁

在金融科技无人区奋楫笃行

伴随着金融数字化转型的深化，金融科技的发展已经走进了“无人区”，金融科技的价值必须通过对外的场景创新才能彰显，但在与外部环境的对接中，金融科技面临着交互模式、接入方式、监管标准、风险因素等不同层面的风险挑战。在我看来，如今的运维服务不仅要通过数据驱动，实现与业务价值的广泛融合，同时要实现运维向运营的转型，将成本与快速交付产生的业务价值整合看待，以此来发现运维所能提供的真正价值。

在数据分析和业务价值的驱动下，全栈式管理、业务融合、智能运营分析、知识赋能和模式创新，已经成为了企业在数字时代提升运维能力的关键。无论是在计算、存储、网络等基础架构层面，还是在金融云、大数据、物联网等层面，新华三均有广泛的涉猎和积累，并且具有不同行业和领域的丰富实践以及知识储备，这也是我们提供全栈式运维的核心所在。

目前，基于全面的运维能力和智能技术的融合，金融行业的客户已经能享受到新华三打造的“运维集市”，以CMDB为核心，通过自动化能力和服务流程编排，进行运维平台能力打通，形成覆盖全生命周期的、场景化解决方案，并以APP的形式对外提供。在某客户的应用灾备案例中，新华三通过将不同能力和工具进行集成，实现了跨团队和跨应用的自动化，一键执行，全流程可视化管理与监控，减少手工操作，降低误操作风险，帮助客户更好地达到监管的要求和平稳切换的要求。

我们相信，未来5年的金融科技行业的运维业务将会产生很多新的创新、发展，对整个IT部门来讲，最大的技术创新不一定是在应用侧，更多会在运维侧。

“1+1+1 战略”：释放金融创新价值

传统以人工为主的运维模式，难以适应新时代的需要，自动化的智能运维成为大势所趋。作为金融科技创新的前沿引领者，新华三在金融ICT建设近30年的历史进程中，一直是金融行业最大的ICT基础设施供应商，服务于90%以

上的金融企业客户。2019年初，新华三基于数字大脑的全栈式创新实力，发布了全新的“数字金融架构”，这一架构不仅强调与智能技术相融合，更强调“稳态”和“敏态”的融合，最终为客户提供安全、可靠和弹性的交付能力。

在运维领域，我们正在以“1+1+1”的战略，整合U-Center2.0统一运维平台、一个“运维数字中枢”和一朵运维云，构建数字时代新一代的运维模式和服务生态。U-Center2.0统一运维平台具备AI赋能、全域融合、应用视角、敏捷交付四大能力，为客户提供AIOps智能运维、混合架构全域资源管理、数字化服务体验管理、新一代网络智能运维管理、数据中心自动化运维等领域提供卓越的创新服务。

U-Center2.0不仅是新华三打造的统一运维平台，更蕴藏着面向智能运维的变革理念。这个平台不仅仅是一个软件，更囊括了对运维的理解和对整个IT体系的理解，我们既提供最标准的CMDB、RTSM监控的管理，也支持自动化部署等工具的实现，从而形成对整个用户运维环境的支持。

此外，“运维数字中枢”可以为数据分析和智能决策提供基础，在服务客户的过程中提升多年积累的数据和预测模型价值，推动用户运维质量的提升。在此之上，新华三希望能以SaaS云服务的模式，以更灵活和广泛的模式，为客户提供更专业的服务。智能运维云能够提供“合作伙伴现场技术工程师+智能运维云平台+云端技术运维专家”的服务组合，同时联合合作伙伴，实现运维技术与行业理解的深度整合，通过打造一个完整的云服务生态，提供有效、快捷的云上和本地运维服务。

如今，数字化创新已经渗透到金融行业经营、管理和服务的各个方面，推动智能运维的变革也已经成为影响企业核心竞争力的关键要素。面向未来，新华三将不止为各类用户提供工具、平台和开放性的能力，更将基于自身大量的实践经验以及在数据驱动下的智能化预测分析能力，帮助客户实现主动式的故障防护。在这一战略的驱动下，新华三能够依靠自身对金融业务的深入理解，结合生态合作伙伴的丰富场景化应用，为金融行业打造统一的运维解决方案，助力客户服务管理能力全面升级。

智能化

浅谈智能运维实践

新华三集团技术服务部运维服务业务部 李富

什么是智能运维

AIOps 是IT运营管理的最新发展趋势，目前在国内外领先的互联网公司、金融、运营商等行业头部企业被创新应用。Gartner 在2017年将其重新定位为Artificial Intelligence for IT Operations，即智能运维，以描述使用人工智能应用于IT运维领域的方向。利用大数据、机器学习等技术手段处理运维相关的数据，通过实时、动态、增强等高级分析，使之具备诊断、预测能力，直接或间接提升系统的稳定性、可用性、体验感，实现更高质量、更低成本、更高效的支撑，改善和增强IT运营能力，以提高企业的竞争力。

为什么需要智能运维

IT环境日益复杂化

IT架构复杂化

IT技术飞速发展，现今的IT环境与先前有很大不同。为了提高敏捷性，IT部门正在部署包括虚拟机、容器、微服务和云平台等支持动态变化的IT架构，这些体系架构和技术实现的敏捷性对于企业至关重要；同时系统不同的模块之间依赖、关联、交互，随着时间的推移，功能越来越多，其复杂性日趋增高；IT服务的风险也随之增加。

数据指数增长

随着X86化、容器、微服务和虚拟化技术的采用，监控采集的颗粒度越来越细，同时企业应用也逐渐丰富；数据呈现成倍增长。根据Gartner的说法，IT基础架构和应用程序每年生成的数据量较上一年多出两到三倍。该数据对于企业而言具有巨大的价值，可以利用它来提高效率，降低成本，增强敏捷性，并为企业提供竞争优势。

企业IT要求愈高

SLA要求越来越高

随着互联网、移动互联网的迅猛发展，用户的体验要求越来越高。如银行涉及客户服务的业务停止时长超过30分钟需要上报银监会，以某银行为例，运维的目标是10分钟内定位故障，10分钟内解决故障，这样才能满足半个小时之内把问题解决掉的要求。

数字业务转型

数字化转型正在使企业面对一个动态的、多功能的，同时又复杂的混合多云环境。数字化的出现将会改变运营的本质。它引入了围绕服务可用性、性能和敏捷性的新需求，以满足业务需求和创新。如果管理不善，这些需求可能导致服务质量的恶化、对业务需求的响应延迟以及IT运营成本增加。

传统IT运维难以应对

由于历史及组织分工的原因，传统IT系统的建设多采取竖井式的方式，IT数据也是碎片化和竖井式的，导致无法全面掌握IT资源的使用情况，无法发挥监控数据的真实价值、提供可依赖决策的深度洞察。

IT监控系统只能监控单个IT应用当前及最近的运行状况，只能识别单个组件问题，无法在较长时段内跨本地和云端多个应用层、系统性地检测IT性能异常和故障、提高IT系统和应用的可用性。

现有的工具和流程是被动的，相互关联和分析的过程极其耗时，无法快速确定服务中断的原因，几乎或根本没有能力预先解决可能的问题，更不用谈前瞻性的洞察。

企业的IT运维支持正在变得越来越“力不从心”，本质原因是传统运维所大量依赖的人力决策已经无法应对当前运维所

面临的挑战。企业需要一种新型的技术，通过强大的关联分析和可视化功能使IT运营流程现代化。智能运维具有前瞻性、可预测性，并能够进行数据驱动的决策，从而有助于建立新的、敏捷的业务模型，并支持创新计划，从而保持企业的领先地位。通过对大数据技术的应用，能够初步解决IT与业务之间的断层问题，实现面向业务运维的转型。

智能运维发展趋势

研究报告

专注AIOps研究的Gartner分析师Charley Rich在其报告中预测，到2023年，将有30%的大型企业部署智能运维平台，用于保障数字化新业务的营收，将有40%的DevOps团队将通过IT运营（AIOps）平台的AI增强应用程序和基础架构监控工具，到2024年，将有30%的企业领导者将依靠AIOps平台获取自动洞察来制定与业务相关的决策。得益于国内AI技术的普及和IT数据量的爆发式增长，中国AIOps市场在未来5年的增长速度将领先全球市场34%的复合年增长率。

智能运维价值

现有的企业监控平台很多，但却彼此孤立，通过AIOps工具可以进行监控的统一管控和数据整合。通过AIOps工具增强，可以提升监控实时性和监控效率，升级数据处理能力，这也会扩大数据分析的范围。也正由于智能运维需要数据的拉通、整合，对数据质量有更高的要求，对企业建设和运维的规范也相应提出了更高的标准，有助于减少数据孤岛，开放数据访问，提高企业数据资产质量。通过AIOps可以提供高性能的服务，增强运营的可见性并改善风险管理，同时降低成本和减少漏洞。AIOps还可以减少事件的发生并降低MTTR、消除噪声、确定优先级、确定故障根本原因并进行补救。这些都与企业目标保持高度一致。

智能运维解决方案

构建运维数据智能分析平台中枢

要实现智能化运维，需要具备面向数字化技术的统一运维平台架构。建立运维数据中台，实现性能监控类时序数据、日志非结构化数据、关联关系图类型数据、调用链/跟踪数据、流量数据、事件数据等多元运维数据的整合；通过运维数据治理，实现全域数据融合；将各行业，各技术域的专家经验，进行规则化积累，打造专家系统，通过关联关系、系统画像、知识工程等，构建运维知识图谱，结合机器学习建立各种模型，构建智能运维大脑；以应用视角和业务价值为导向输出智能服务能力，提供异常检测、根因定位分析，关联影响、趋势预测等各专项智能诊断服务；这些AI能力还可以通过便捷的服务编排，赋能容量管理、业务连续性管理、服务台、安全等“监、管、控、防、营”全场景业务，有效提升业务可用性。

运维数据治理“资、治、通、监”

智能运维的本质是以数据驱动算法的智能分析过程。数据质量的高低直接影响智能化的能力输出。大家知道，多数CMDB应用普遍不那么成功，很大原因在于数据质量管理不善，其解决根本的解决之道，需要培养“数据思维”，实现CMDB数据治理及闭环管理；智能运维的数据质量管理也是如此，同样需要运维数据治理。运维数据治理可以抽象概括为“资、治、通、监”。“资”，首先需要摸清我们的家底，有哪些数据资产；“治”，然后通过标准化体系的构建，落实数据治理方案；“通”，实现数据拉通融合，理清数据的使用链路；“监”，在链路上执行数据质量监测，从而实现运维数据质量的不断优化和提升。

AI赋能运维故障治理

AI赋能故障处理

AI技术起起伏伏，发展到今天，可以帮我们解决不少问题，但是它目前的能力还处在擅长解决单领域的问题范围内。需要有充足的数据和知识，信息是确定且完整的，问题定义是清楚的，并明确输入输出。但运维问题非常庞杂，其整体问题已经复杂到AI不擅长解决的程度，基本不可能一步到位解决运维所有的挑战。所以我们采用庖丁解牛的思路。对故障实行事前，事中，事后分段治理（图4-1）。事前做好故障预防，事后做故障复盘，增大故障发生的平均间隔时间，缩短事中故障的平均修复时间。其中事中又可细分解为故障的发现、定位、分析和处理四个阶段，针对每个阶段研发具体的场景算法。如故障的发现就涉及到单KPI、多KPI以及日志的异常检测；为了缩短故障的定位时间，涉及到告警的智能收敛、根因的辅助定位、多维根因定位等场景算法；对于具体领域的故障分析，如数据库、网络故障等，则需要结合专项技术的领域知识，通过算法的组合编排，逐个击破。



图1 故障过程分解图

智能运维场景化实践

场景#1：复杂基础架构系统下的异常检测和异常预测

运维监控通过各种技术工具，如网管、Zabbix、APM、网络抓包等会采集各种监控指标，这些指标通常被存储为时序数据（包含采集时间和指标值）。KPI异常检测对监控指标的时序曲线进行检测，自动发现其反常行为，以便及早发现风险，防止其发展为故障，或及时发现故障，进行止损、诊断和修复。

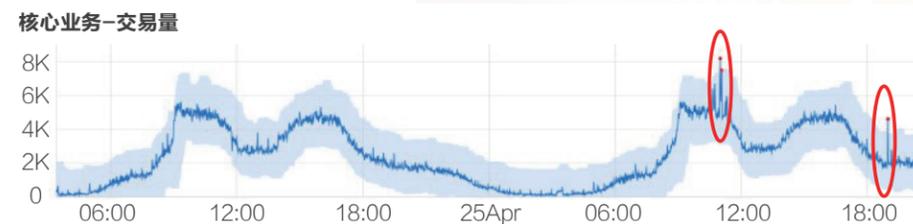


图2 故障过程分解图

常见的单KPI异常检测场景有：

- 业务指标（黄金指标）：交易量、交易响应时间、交易失败数。
- 服务器指标：CPU、内存、网络、磁盘等指标。
- 中间件指标：数据库负载、Web服务器响应时间。

运维挑战

- KPI指标多：系统由大量的组件构成，这些组件都有自己的指标，这些差异化的KPI指标如：业务指标、服务器指标、中间件指标等。
- 阈值设置难：以往基于阈值的设置，通常在低限度预警情况下，无法判断是否有故障，而一旦到达高限度阈值告警，往往故障已经发生。
- 误告漏告多：依赖人力针对数万监控指标配置大量规则，而规则不准确，导致大量误报警，又需要人力过滤，才能筛选出真正要处理的少量有效报警。

解决方案

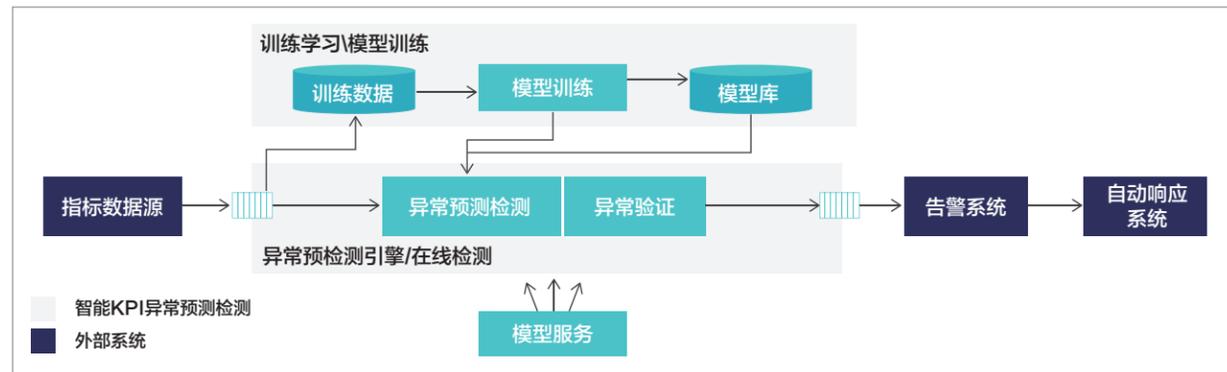


图3 智能KPI异常检测模型

基于学习组件行为模型的异常主动预测：系统运行在一系列组件正常的状态下，当某些组件状态偏离其正常状态，就会产生系统异常。因此，通过大量的历史数据，可以形成每个组件自身的模型，从而判断各种实时监控数据是否即将有异常状态产生的可能性，以此实现故障的主动预测。

场景#2：智能报警事件去噪和收敛

每一个运维工程师都可能被报警风暴所困扰过。我之前负责某运营商系统的运维工作，平均13分钟就会接收一次短信告警，在夜间则是平均37分钟一次，而实际数据统计发现，有效短信告警占比不到14%。因此短信告警的冗余度是非常高的，已经造成了告警疲劳。告警太多的主要原因如下：

➤ 大量监控对象：业务越来越复杂，层次越来越多；x86化，微服务化，容器化，监控的软硬件对象的数量大幅增加，监控粒度越来越细致，每一个监控点都会产生数据指标、状态异常。立体化的监控，带来监控指标的爆炸式增长，也导致越来越多的告警。

➤ 重复告警多：人工配置的监控告警规则，无法适应系统的动态变化，规则不全面不准确，这些都可能会导致误报警；另外告警策略执行周期计算，会持续产生重复告警，部分策略甚至会导致持续告警。

➤ 缺乏关联聚合：传统告警工具只能针对被监控组件本身进行监控和异常告警，无法从相关性和全局性来进行告警的统一处理。如一个网络设备的故障就可能引起“告警风暴”，产生大量的告警，而真正需要处理的告警只有一个。

解决方案

针对上面的这些问题，对现有告警降噪聚合，进行分类梳理、逐个收敛；减少告警数量，使告警通道发出的告警皆为有效告警，告警的信息得以被及时接收并处理；使用智能报警合并策略、基于报警数据挖掘的机房故障分析、报警关注度分析、值班与逐级通告平台和报警回调技术等。

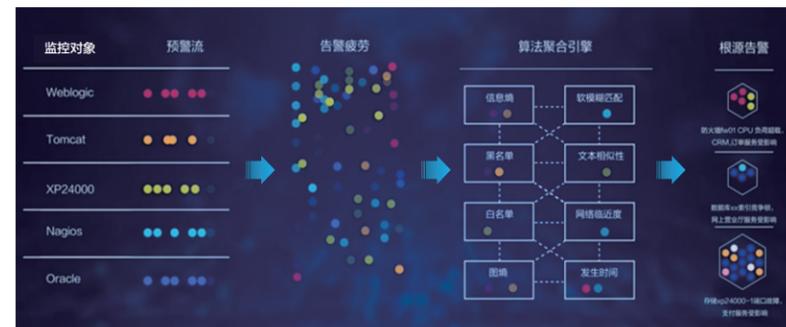


图4 智能告警收敛原理

➤ 告警数据归集：采用统一的事件处理平台，整合不同基础架构监视工具捕获的告警及事件，并将其标准化和利用CMDB等信息增强处理，可以从整个业务和IT中心的视角来进行事件的处理。

➤ 历史告警挖掘：基于历史告警数据挖掘，采用机器学习算法实现告警、异常的关联规则挖掘，形成关联知识库，达到设定的置信度后可形成告警规则表，用于衍生告警的屏蔽、实时告警的合并，避免告警风暴，提高故障解决时效性。

➤ 告警去重降噪：自动剔除假告警和无用告警事件。对大量告警数据进行去重、降噪，产生数量压缩、重要性分级的告警信息，形成聚合事件，相对于原始告警来说数量大大减少。

➤ 算法聚合收敛：基于信息熵、图熵、发生时间、文本相似度、网络临近度等相关性聚类、黑白名单处理，推荐根源告警。

场景#3：多维根因定位

KPI指标（如网页访问量，交易量，失败量，响应时间等）与多维属性（如源系统、交易类型、交易渠道等），是金融、互联网等行业常见而重要的业务监测指标。当某个总指标（如总交易量）发生异常时，需要快速定位到是哪个交叉维度的细粒度指标的异常导致的，以便尽快做修复止损操作，定位出其根因所在的位置是极具挑战性的，尤其当根因是多个维度属性值的组合时。

问题挑战

在实际的场景中，问题的挑战在于其复杂度和及时性，有以下三个方面：

➤ 及时根因定位：业务出现问题，需要在1分钟以内准确定位到根因，若没能及时定位修复，问题的影响和业务的损失很可能会不断扩大。

➤ 准确衡量根因：不同组合的KPI是相互依赖和影响的，真正根因元素的KPI异常，可导致其他元素的KPI也发生变化，很难对影响KPI指标的根因做一个量化的判断。

➤ 搜索空间大：由于KPI拥有多维度的属性，随着维度的增加或粒度的细化，元素的数目往往呈现指数级增长的趋势，可能需要从成千上万的多维属性空间进行搜索。

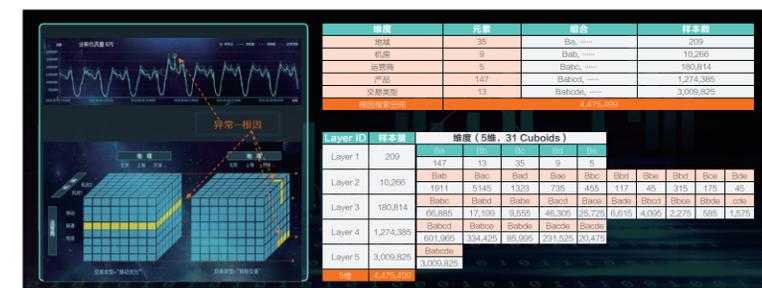


图5 多维根因定位问题图示

传统的根因定位方法依靠人工和BI工具：

➤ 定位不准确：依赖专业的BI工具和训练有素的数据分析人员，利用BI工具不断切片分析，不断细化定位问题，但定位到的可能不是问题的真正根因。

➤ 定位时间慢：人工定位往往滞后，需要数小时甚至更长时间，在复杂的多维度场景，靠人工定位方式几乎无解。

多维根因定位核心采用蒙特卡洛树搜索和分层减枝等算法，蒙特卡洛树搜索中使用了综合根因可能性评价指标，使用这种评价指标对候选根因进行了优选，获得最佳根因。

基于该算法的根因定位，具有以下优点：

➤ 全自动：自动分析总KPI指标，在总KPI异常时，自动启动多维异常定位算法。

➤ 根因准确：基于蒙特卡洛树搜索的机器学习算法，能分析百万级以上多维数据，这是人工所无法实现的。

➤ 秒级定位：定位快速，能实现秒级定位到根因或根因组合，减少因为故障导致的业务损失。

智能运维展望

AIOps的大潮已经来到，多个行业领域都表现出对智能运维的强烈需求。IT运维具备丰富的应用场景和大量的数据，将运维经验、大数据、人工智能相结合，将极大地提高整个运维领域的生产力。面对不确定，拥抱变化，不断探索新兴技术的创新应用，智能运维可以帮助企业管理IT复杂性和风险，确保业务永续及价值创造。

大型银行自动化 运维规划实践

新华三集团技术服务部运维服务业务部 李光

引言

现在大家都在讲智能运维，自动化运维已经逐渐少有提及。智能运维融合大数据、机器学习等先进的分析技术，来提升IT运维的监控、自动化和服务管理能力，实现个性化、动态化、可预测的洞察和处理。目前智能运维尝试主要在监控领域，未来还会在服务管理和自动化领域的AI结合。智能化的实现依赖于成熟的自动化和大数据（智能计算）能力的深度融合。自动化运维已经从一种思潮和探索转变为落地和使用。越来越多企业已经落地自动化运维，而且自动化成熟度相当高，自动化是智能运维强有力的支柱。

金融行业是比较早成功融合IT的行业，经历了几十年的发展，银行业IT已经比较成熟，技术跨越度大。另一方面，银行系统也相对比较复杂，业务连续性要求高，对IT运维也提出更高要求，所以能在大型银行成功落地的案例，极具参考意义，可以作为其它行业的标杆。下文是通过总结提炼银行业自动化运维成功案例的经验，整理出的自动化运维规划实践。当然，这样一套体系未来还将在数字化银行转型过程中，不断地优化提升。

金融行业自动化运维规划实践

在自动化平台搭建前，都是被动式解决问题，在运维中经常被各种问题所困扰，不同岗位的人会从不同角度和维度对运维提出不同需求，比如一线运维人员、室组经理到中心领导，作为运维管理员的你可以回答吗？

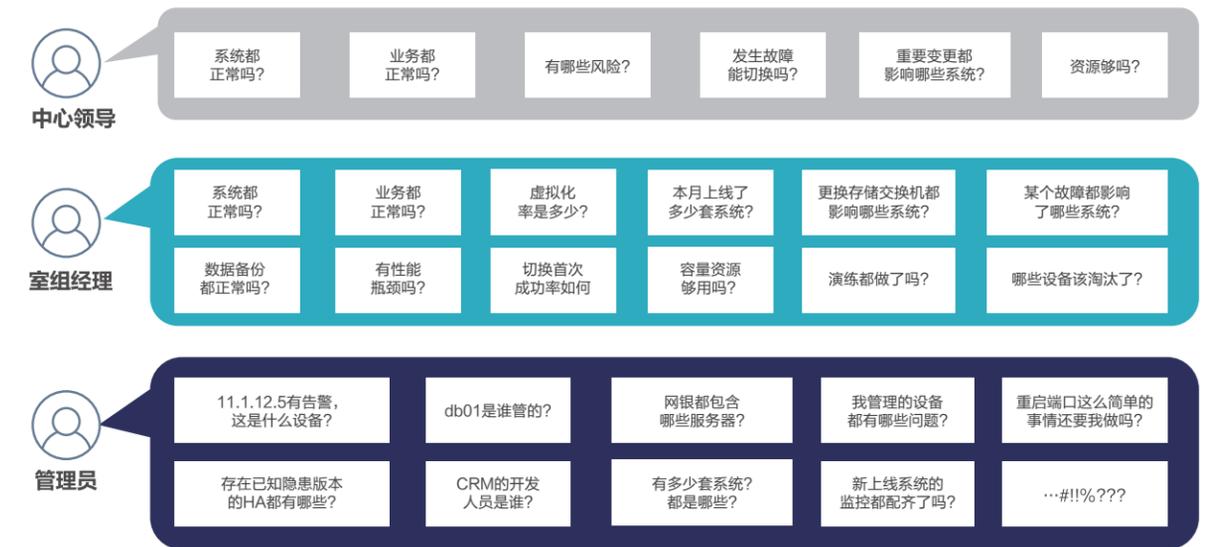


图1 运维管理员常见问题

面临的运维难题很多：信息零散，太多工具及脚本，重复劳动多，繁琐容易出错任务，快速排障和修复，竖井式的团队和不断增长的威胁，不一致的补丁和人工合规巡检。所以需要借助自动化平台来提升运维能力。平台能力主要是面向运维部门的工作平台，运维人员的大部分工作都能在该平台实现。以用户为对象来组织各种功能。可以构建向业务场景的精细化管理平台，比如希望降低产品成本，我们可以建设相应的容量优化平台；希望提升变更效率，可以建设相应的设备扩容调度平台等等。规划重点是针对不同的运维场景给出一套固定的功能组。用户要做什么事，只用选择对应的模块组合就能完成。平台结构设计分为基础设施层、通用能力层、平台能力层、运营能力层。

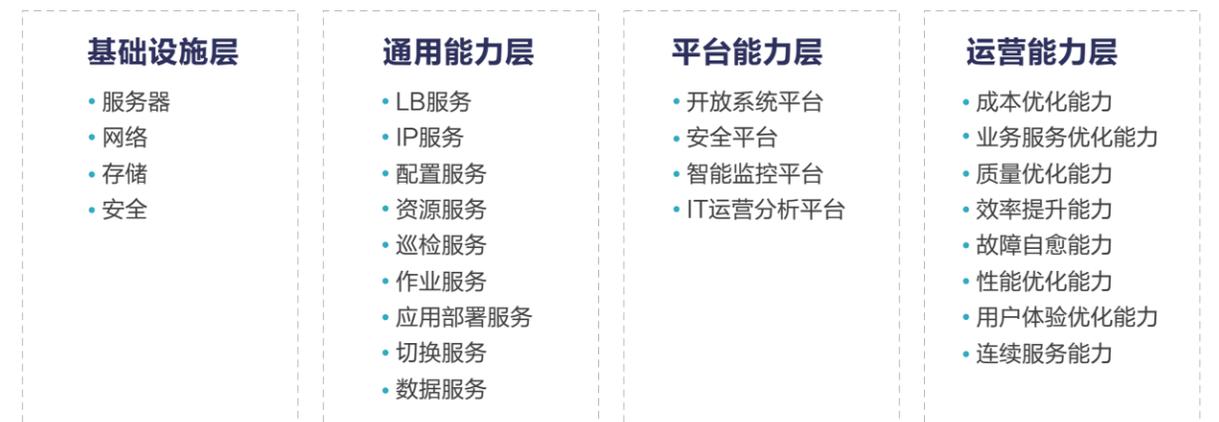


图2 平台架构设计



自动化运维平台的建设是一项持续优化、不断迭代的过程，我们需要一个科学的自动化设计规划路线图来实现这一目标。

在设计自动化运维平台规划的时候，采用“目标愿景 现状评估 差距分析 路线规划”四个步骤。

➤ 第一步：确立目标和愿景

吸收IT业界对数据中心自动化的成熟度和评估标准，结合自身组织结构特点，建立自动化的成熟度模型和评价体系。以成熟度模型为依据，从数据中心整体角度确定确立目标和愿景

➤ 第二步：评估各组现状

数据中心各组的日常具体运维工作存在较大的差异，为了用客观和统一的标准评估各组的现状，对各组的工作进行“分解”并“重组”，具体如下：

首先将各组的日常运维工作进行分解，分解粒度细化到单个的日常运维任务。然后将根据任务的共性进行工作分类，将日常的运维工作划分为若干个维度，最后结合成熟度模型为每个维度确定评价标准，建立数据中心自动化成熟度评估表。

➤ 第三步：分析现状和目标的差距

各组根据自动化成熟度评估表，对自动化现状进行自评，并结合中心的自动化目标，找出各组各项工作距离目标的差距。

➤ 第四步：规划的改进和提升路线

根据差距分析，确定各类工作的改进方向。结合各组的具体情况，确定各项工作的改进次序和方案。

依据该方法，某银行规划和实践过程如下：

先依据IT业界对数据中心自动化的成熟度和评估标准，结合数据中心的组织结构特点，建立自动化的成熟度模型和评价体系。以成熟度模型为依据，从运行中心整体角度确定自动化愿景和确定要达到的目标。

依据《IT运维成熟度模型综合评价表》，从管理与决策、资产与配置、资源与服务、安全与合规以及维护与变更五个类别，来评估现在和将来自动化成熟度，数字越高，表示成熟度越高，建立成熟度模型。

例如：系统组现状评估



分类	工作项	工作内容细分	现状
资源与服务	计算资源管理	建立服务器资源池 资源自动调度	2 2
	资源开通服务	资源申请自服务门户(主要为虚拟机网络、存储、软件)	0
	ITIL服务请求处理	自动化ITIL服务请求，审批后自动执行	2
分析报告	风险分析	建立风险模型 自动采集风险数据 风险分析及报告展现	1 0 0
	统一视图	集中统一的运维视图	2

在IT业界自动化成熟度模型的基础上，结合IT科技部门的组织架构特点，确定IT科技部门的整体自动化成熟度模型，如图3所示：



图3 IT科技部门整体自动化成熟度模型



整体自动化成熟度模型由低到高划分为1至5五个阶段，发展的整体的方向从被动到主动，从分散到统一，从个性到标准化，从任务到服务，从传统运维到云化运维。

根据IT科技部门整体自动化成熟度模型，经历5年发展到达第4阶段的路线图。下表为每阶段规划实施的重点：

平台搭建	<ul style="list-style-type: none"> ◆自动化平台搭建；现有服务器和网络设备的纳管；自动化平台操作培训。 ◆优选人工耗时，自动化技术复杂度低，操作风险低的项目如巡检、合规
运维管理改进	<ul style="list-style-type: none"> ◆二期自动化建设，完成自动化咨询，分析，规划建设，实施投资小，见效快的自动化项目，初步建立自动化体系 ◆对日常运维工作规范化，标准化，储备SOP，为未来加速建设做好准备 ◆规划，设计并建立自动化运维portal ◆其它工具（BSM,ITSM,UCMDB）联动
服务改进	<ul style="list-style-type: none"> ◆三期自动化建设，改进自动化服务管理体系，优化服务流程，将成熟自动化操作，用自助服务方式提供给用户，进一步解放人力。 ◆逐步将标准化的业务流程实现自动化联动 ◆进一步与其它工具普及和联动 ◆各个组普及自动化
IT综合治理	<ul style="list-style-type: none"> ◆在IT治理及自动化成熟度的指引下，将完成监控自动化扩展到各个部门，对整体流程，自动化体系持续改进 ◆整合各工具平台，实现智能可视化运维

经过5年的自动化建设，该行自动化处于金融行业领先水平。再次面对原来的运维难题，借助自动化平台，都有科学的应答，各种运维场景都有高效的解决方案。

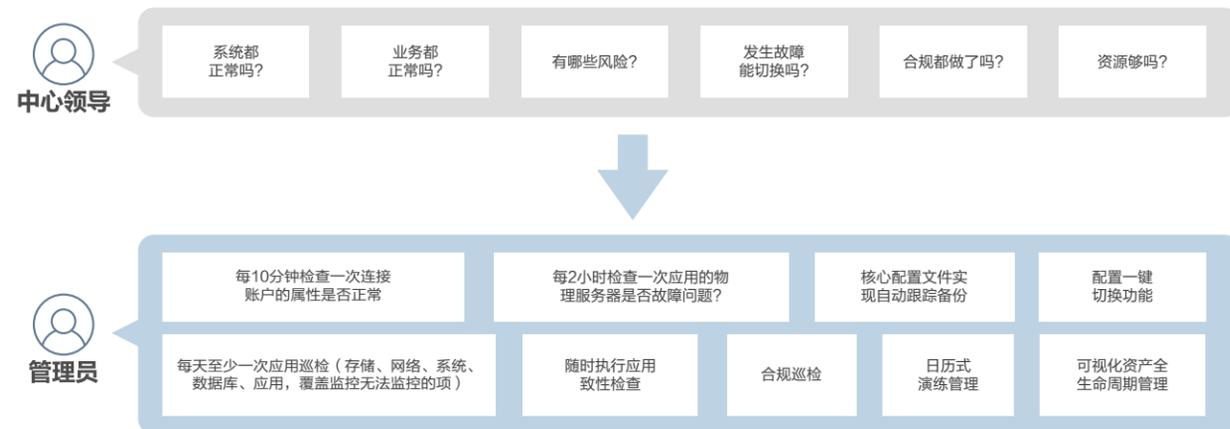
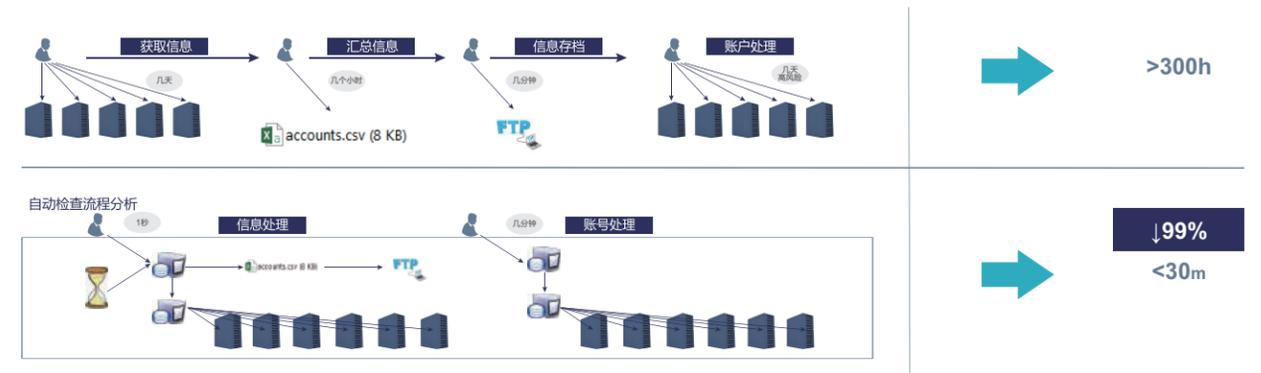


图4 利用自动化平台应答领导关心热点

例如，借助自动化平台对账户检查的需求应对方案。原来通过登录每台服务器，执行脚本，获取账户信息，信息汇总后通过FTP下载到管理员工作机器，通过比对，找出不合规的服务器，然后登录到不合规服务器，创建相应的账户。账号检查人工操作极其繁琐和耗时，为当前痛点作业之一。

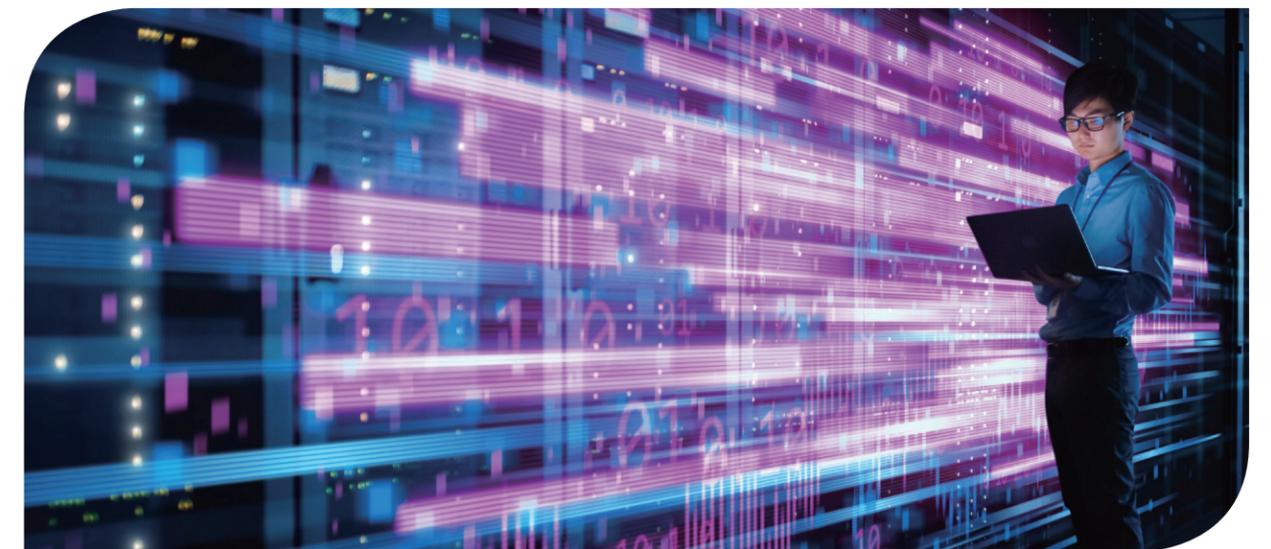
应对方案：通过自动化平台实现服务器账号的定期自动检查，检查服务器是否具备特定账号，对于核检未通过的，进行定期或者按需补救，如新建相应账号，并且自动获取相关信息，生成报告，并存盘。

自动化平台实现账户检查收益分析：



	每台服务器耗时	服务器规模	人力（小时）
Before	10分钟	1500	250
Now	10秒	1500	后台自动运行 半小时出报告

既可以按时检查，也可以按需检查；提高合规率（可以对更多主机进行更频繁的检查）；提高效率（人工操作繁琐耗时）；提高准确率（减少人工检查错误）。



自动化运维平台带来的价值和帮助

自动化整体收益

经过4个阶段的自动化建设，日常运维工作实现规范化，标准化。在自动化成熟度的指引下，完成监管控自动化扩展到各部门，对整体流程，自动化体系持续改进，整合各工具平台，实现可视化运维。

成本控制	资源调度	反应迅速	高效率性能	可视化管理
全局管理水 平提高 管理员： 服务器=1:500	在ITIL中申请资源如 操作系统资源，软 件资源等，自动化 完成资源分配	分钟级容灾切换， 容灾演练保证灾备 中心版本一致	消除70%的由于手 工操作，错误配置 导致的宕机与安全 事件	服务器，网络设备 单点登陆，资产信 息一目了然。所有 运维操作界面化

图6 自动化整体收益

自动化大幅提升协调能力

自动化平台帮助用户把各个部门串联起来，打破部门竖井式的缺陷，真正做到系统作战。

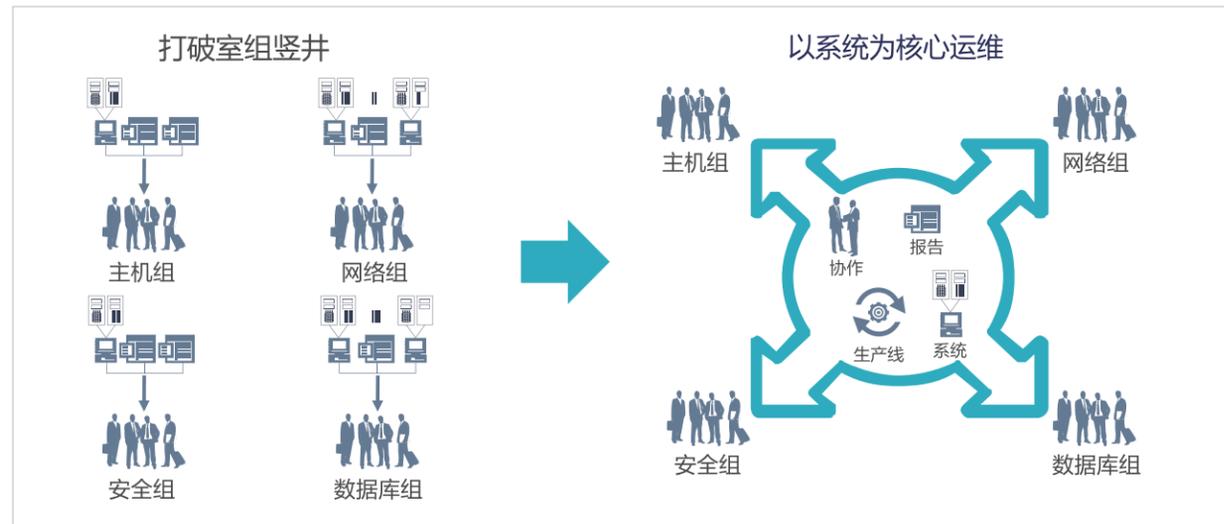


图7 跨室组，系统为核心的运维



自动化大幅提升运维能力

自动化运维平台可以在各项运维场景中提升运维自动化能力。下图总结出了一键功能模块，包括一键部署和一键巡检等7个分支以及43个子场景。



图8 场景化运维工具

自动化改变运维方式

被动解决问题通常是以一个监控告警开始，管理员随即去检测问题，再修复问题。主动解决是为了避免问题的发生，先进行规划（如cpu、内存的利用率并进行预测），再进行优化（回收或扩容），问题发生时自动执行。

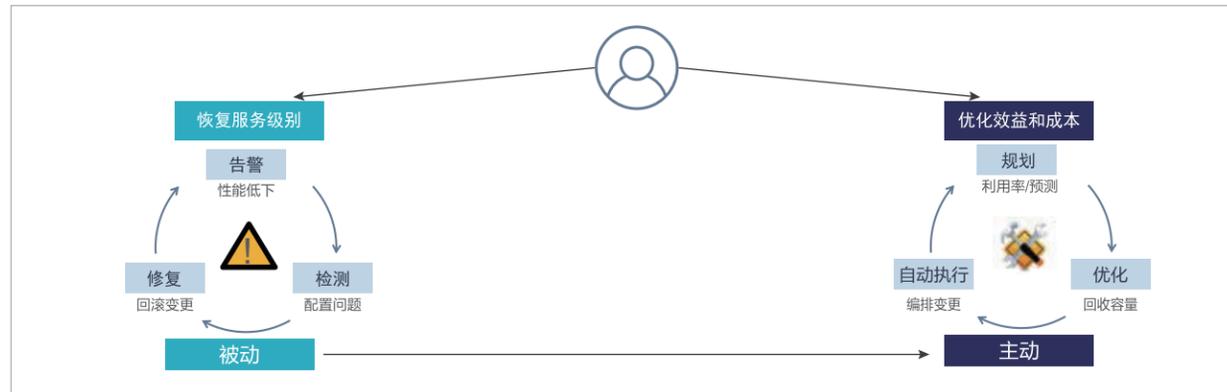


图9 被动到主动的转变

结束语

从IT运维的演进路径可知，运维发展的趋势是走向智能化运维。智能化运维的支柱是自动化，没有成熟的自动化是不可能到智能化的阶段。本文介绍了自动化运维的实践过程，自动化设计规划实践的方法，阐述了该方法论在银行业的实践以及实现的效果。目前金融行业引入大数据、AI、混合云，而本文阐述的自动化运维平台建设实践依然适用，只需要在自动化运维平台上对“平台能力层”和“运营能力层”做出扩展，引入大数据分析平台、智能计算平台等。所以在讲智能运维，自愈运维概念的今天，我们更应提高自动化平台的成熟度。在全面和成熟的自动化平台上引入大数据、机器学习等先进的技术从而实现全面的智能化运维。

新一代智能运维平台

建设探讨

新华三集团技术服务部运维服务业务部 伏三强

前言

在数字化经济转型时期，越来越多的客户认识到IT已经从内部运营支撑工具逐步演进为企业的核心竞争手段。伴随着业务的快速发展，越来越需要保证IT系统能够持续、稳定、高效地运行。传统的监、管、控运维方式已难以满足客户的要求，取而代之的将是采用更加高效、更加智能化的运维方式才能适应客户数字化转型发展。新一代智能运维平台的开发落地势在必行。

平台典型特征

新一代智能运维平台的规划需要考虑企业IT运维的全应用场景，原有平台架构的优势及不足，同时还要充分考虑ITOM领域技术发展的新动向，以便打造出能面向未来，覆盖全应用场景的企业级产品。根据自身经验和客户诉求，新一代智能运维平台不但要能满足多机构、多租户、多张网、大容量、分岗分级等应用场景的运维管理要求，还要加强在大数据、自动化、智能化运维场景的应用。

- 从管理对象层面来讲，新一代智能运维平台既要满足对传统IT环境的运维管理，也要能满足对云环境下虚拟资源和多租户的运维管理要求。
- 从业务管理范围来讲，新一代智能运维平台既要涵盖传统的监、管、控领域，满足自动化运维要求，还需逐步向智能化运维转型。
- 从业务逻辑层面来讲，新一代智能运维平台要以资源管理库（即CMDB）为纽带，实现监、管、控产品模块间的数据互联互通，便于关联分析、故障定位等深化分析场景落地支撑。
- 从应用架构层面来讲，新一代智能运维平台应采用能将服务作为独立模块运行，并能被独立开发、独立测试、独立部署的基于Docker化的微服务架构。
- 从数据存储的角度来讲，新一代智能运维平台既要能实现同类数据的集中统一存储，又要能实现

不同种类、不同时段数据的分库存储，以便既可满足大容量的应用场景，又可使平台性能得到保障。

➤ 从数据交互的角度来讲，新一代智能运维平台要能提供丰富的南、北向接口，以便于快速整合第三方系统的数据，也可为第三方系统提供数据消费。

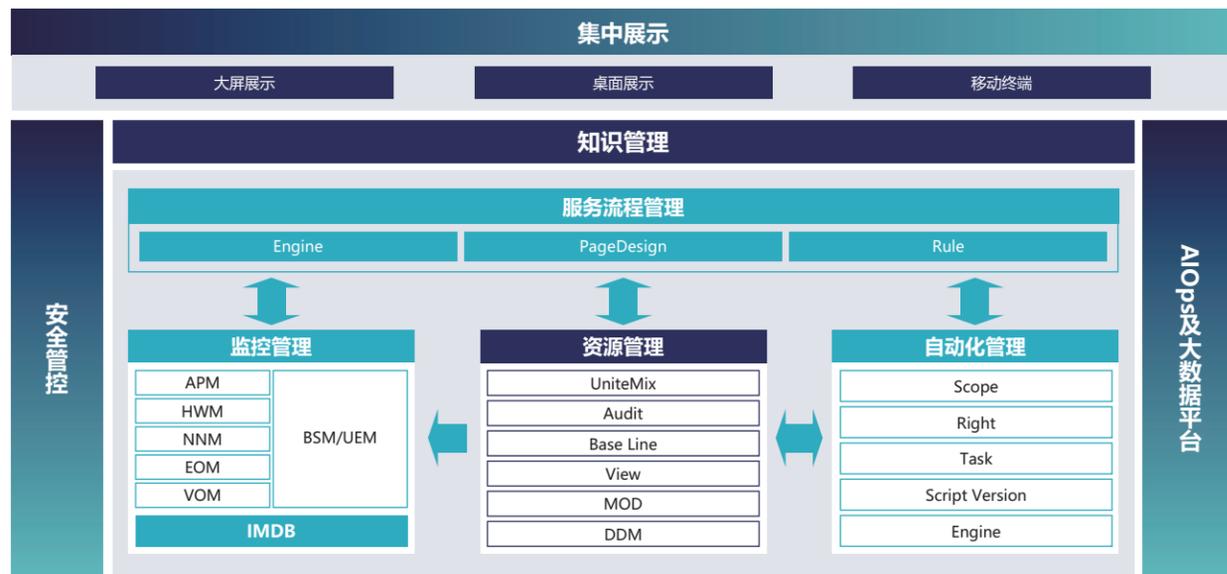
➤ 从知识共享的角度来讲，新一代智能运维平台要提供独立的知识管理模块，其它产品模块既可从知识管理模块中搜索知识条目来帮助解决问题，也可将自已解决问题的方案或经验提交给知识管理模块以形成知识条目。

➤ 从用户体验的角度来讲，新一代智能运维平台在保证业务逻辑和展示风格统一的前提下，要站在使用者的视角来组织菜单和规划页面布局，同时还要做到菜单条目及页面权限的可配置性，以满足不同用户不同应用场景的要求。

核心能力集组成

既然要打造覆盖全场景的企业级软件产品，那么，我们所规划的产品功能就应涵盖IT运维的各个领域，考虑到不同用户需求的差异及综合运维场景要求的不同，新一代智能运维平台将以应用场景来划分产品能力模块、以资源数据为纽带拉通各模块间的数据关联，以用户视角来呈现业务数据。

根据上述设计思想，新一代智能运维平台的核心能力集可归纳为：监控管理、资源管理、自动化管理、服务流程管理、知识管理、安全管控、AIOps及大数据平台、集中展示，共八大模块，总体框架蓝图如下图所示：



上图中，每个模块承载着不同的运维业务和可适用于不同的应用场景。知识管理模块属于公用模块，其它产品模块与知识管理模块间存在双向数据交互；资源管理模块也是属于公用产品模块，其它产品模块中与资源相关的信息都来自于它。

➤ 监控管理：根据管理对象和应用场景的不同，又可分为：视频监控、动环监控、网络监控、硬件监控、软件监控、业务服务管理和用户体验管理七个产品模块。这些产品模块都依赖于统一指标库。

➤ 资源管理：就是ITIL中所说的配置管理库，运维管理的对象和对象之间的关联关系都应集中存放于此。它应具有：自动发现、自动建模、视图管理、基线管理、变更审计和联邦调和等核心能力。

➤ 自动化管理：为日常运维中的装机、应用上线、巡检、配置下发、合规检查等应用提供自动化处理手段，减少人工参与，提升工作效率。它的核心能力包括：范围管理、流程编排、版本管理、任务管理、权限控制等。

➤ 服务流程管理：就是将ITIL中所讲的服务流程落实到不同的企业中，为适应不同企业的组织结构、职责划分、管理文化的差异，它必须要有强大的流程引擎和表单设计器，同时还要且有支持灵活的业务规则自定义。

➤ 知识管理：将日常运维过程中所产生的各类知识和经验进行统一管理，包括知识的收集、分类、审批、入库、发布、检索、查阅、考评、下线、归档等功能。

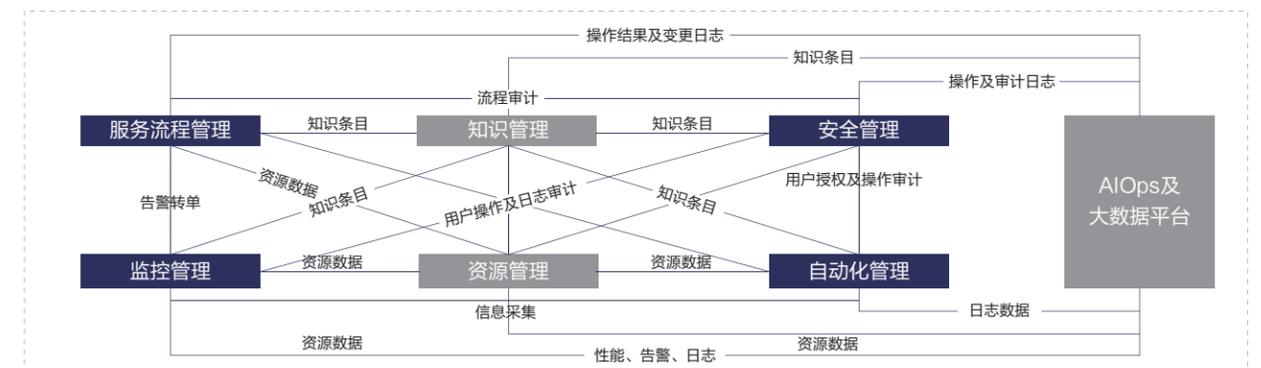
➤ 安全管控：其主要目的是降低运维风险，保障系统持续、稳定地运行，包括身份验证、访问控制、接入审计、合规检查、漏洞扫描等。

AIOps及大数据平台：是将日志、性能、告警、配置、变更记录、网络流量、交易数据进行汇聚，利用人工智能和大数据处理方法进行数据的分析和处理。包括数据采集、数据治理、算法管理、深度学习等功能，具体应用包括：ChatOps、异常检测、根因分析、故障定位、容量预测、关联影响分析等。

➤ 集中展示：在复杂的应用场景中，将各产品模块的数据进行集中展示，为用户提供统一的可视化入口。

新一代智能运维平台构建了以“资源库”、“指标库”、“知识库”为基础的三库模型，意在保证产品模块的规范性和统一性，以及实现各产品模块的互联互通。为满足不同用户和不同应用场景的要求，各产品模块既要能独立部署，也可相互集成，以便可以组合成综合性的解决方案来应对各种复杂的应用场景。

根据前面描述，新一代智能运维平台已根据业务逻辑和应用场景归纳为八大模块，但这些模块都不是孤立存在，相互之间可根据应用场景进行不同的数据交互，如下图所示：



上图只是为了简单地表达各产品模块间是存在信息交互的。具体要交互什么数据，如何交付，需要用较长的篇幅来编写，在此不做赘述。

开发落地实践经验

一个软件产品的开发，需要经历软件工程全生命周期的每个一个环节，要完成新一代智能运维平台所规划的八大类模块的全部开发，更是一个浩大的系统性工程。那么，如何才能有条不紊地按计划完成这项工程呢？如何才能构建好新一代智能运维平台呢？

要完成如此庞大的系统性工程，必须得依靠科学的方法。我们在构建新一代智能运维平台时，遵从的是软件工程CMMI5标准，并引入敏捷开发方法和采用看板的方式进行应用模块的开发，在软件测试和发布过程中，我们遵从DevOps的思想构建了代码的自动化测试和软件包的自动发布框架，从而起到加速软件开发的进度和保证软件交付质量的作用。

下面重点从业务应用、技术架构、数据存储、工程实施等几个方面介绍一下我们在新一代智能运维平台开发中的创新和实践：

▶ 在业务应用方面，整体思想是拉通网络、存储、服务器、操作系统、虚拟资源、应用软件、业务服务的统一管理，构建以资源数据为纽带的大资源管理框架体系，并从业务逻辑、用户体验两个维度重新梳理了平台功能菜单和页面的布局。使得新一代智能运维平台在业务逻辑呈现上更清晰，用户使用起来更容易上手。

▶ 在技术架构方面，采用基于Docker化的微服务架构，将以前基于SOA架构的服务模块进行细化拆分，形成了一个可以独立开发、独立测试、独立部署的功能模块。以便于将来的弹性扩容和满足大规模监控管理的要求，同时，也为将来的持续开发和灰度发布打下坚实的基础。

▶ 在数据存储方面，采用图数据库来存放资源属性及其关联关系，同时采用了时序数据库来存放监控指标数据，并根据采集数据的重要程度、使用频率及时间顺序进行了分级存储。即将一些重要的和使用频度较高的数据定义为一级数据（热数据），存放在Redis内存数据库中，以提高实时查询和计算效率；将实时性要求相对较低的数据定义为二级数据（暖数据），存放在InfluxDB时序数据库中；将一些历史数据和使用频度极低的数据定义为三级数据（冷数据），存放在Hadoop数据库中，为AIOps及大数据应用提供基础。

▶ 在工程实施方面，我们引入了资源归属机构和业务机构的概念，以使得新一代智能运维平台既可满足具有分支机构的大型企业分级分权的管理要求，也可快速满足大型单位新增或合并、拆分机构以及人员离职或换岗的要求，同时，还可减少工程实施人员和系统维护人员的工作量。通过资源归属机构和登录账号所属机构的关联，就可自动进行数据过滤，从而达到控制登录账户的访问权限，免去了维护人员手工分组控制权限的痛苦；通过管理人员的业务机构和资源的所属机构就可满足一些企业跨机构管理的要求；通过变更业务机构就可快速满足人员离职、调岗或机构拆分与合并的要求。引入资源所属机构概念之后，不但能满足多机构运维场景的要求，在与云平台对接后，还能快速满足多租户运维管理的要求。

结束语

由于IT系统构成复杂，IT运维涉及的知识面广，客户环境和组织结构及管理文化又各异，想要用一个平台就能完全满足不同客户全业务的运维不是一件易事。对于客户而言，也不是一个平台能够包打天下，这就要求各软件平台都需要采用开放式的架构，以保证客户业务管理个性化需求的落地。同时，对于很多大型成熟度高的客户而言，开源技术采用越来越普遍，自身自动化和智能化运维开发能力提升的诉求也越来越强烈，运维平台从前台业务到后端技术的开发落地还有很多领域都需要去积极探索。要使运维平台让复杂的IT变得更简单，任重而道远，新华三U-Center也希望能够和客户以及业内同仁充分协同，创新发展。

数字化转型时代、 AI重构网络联接

新华三集团网络产品线ADNET解决方案管理部 唐元武

人类社会经历了农业社会，工业社会的发展，目前进入了数字社会，相对于以往，数字化时代引发了诸多方面的变革，这些变革非常巨大，包括技术、经济、思维、生存等方面都在发生跨时代的改变。在数字化转型的背景下，传统的网络作为数字化转型的基础设施又面临着哪些变化？人工智能下的网络如何直面这些问题？接下来结合目前的现状和大家一起探讨下。

数字化转型下的网络面临巨大挑战

作为数字化的基础设施网络连接来说，在数字化转型后必将面临着巨大的挑战。首先数字化转型后的组织对网络故障的容忍度更低，深度数字化转型对组织而言意味着业务重构，组织重构、流程重构、生产重构，转型之后所有这些系统都会承载在网络之上，因此对于网络的稳定运行的要求更高，最好能做到网络故障的提前预测，提前处理，防患于未然，减少系统的故障宕机时间；其次数字转型带来组织内部的快速反应能力的同时，IT系统为了适应这些变化，自身也在做转型，比较典型的就是从传统的建设模式转换为以云为基础的IaaS或PaaS模式，这些转变为业务提供灵活服务的同时，意味着IT系统建设和维护的复杂度成倍地增加；最后为了应对当前复杂的网络部署和快速的业务变更，网络系统引入SDN等相关的自动化网络技术，实现整个网络部署和变更的自动化，自动化在提升部署和变更效率的同时，对于类似“灰盒系统”的故障定位又成为一个耗时耗力的过程。综上所述数字化转型在对组织内业务、架构、流程做转型的同时，对于数字化的连接基础网络来说已经成为整个企业生产的神经系统，面临着高可靠和快速故障恢复的巨大压力，必须在现有的网络基础之上进行重大能力提升和改善。

人工智能加速网络重构

人工智能近几年的大力发展，在各细分行业如机器视觉、语言翻译等方面取得重大的进展，随着网络的进一步发展，在网络领域的人工智能应用也逐渐走入行业的视野。如何引入AI构建一个智能的网络系统，让网络自身可以智能调整、适应业务的变化，快速的故障定位，甚至于无需人为干预的情况下进行快速的故障恢复，是人工智能引入网络需要重点思考的问题。我们认为网络要达成上述的效果，在现有的网络架构之下难以实现，需要进行网络系统的重构，如图1所示：

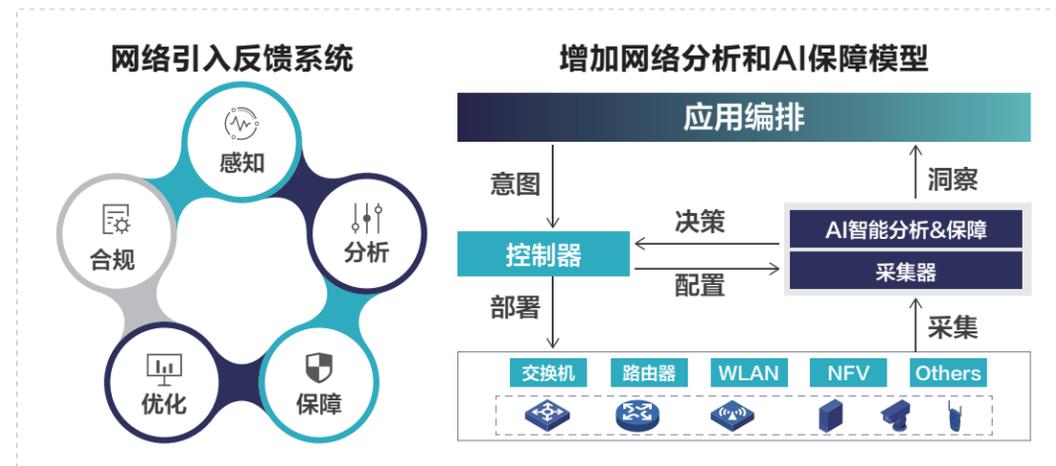
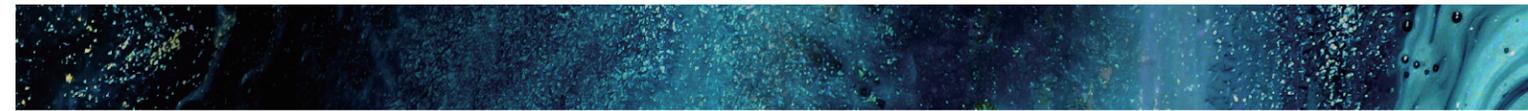


图1 网络系统的重构



首先是引入反馈系统：现有网络从自身系统的运行的角度来看，一直以来都是一个按照严格逻辑运行的开环系统，系统本身缺乏反馈的能力，难以对运行状态进行反馈补偿和修正，要通过AI形成智能控制，首先就需要重构网络系统，使其具备系统级的反馈能力，以便实现网络的感知和补偿；其次是AI能力如何纳入的问题，当前来看比较共识的是通过对网络运行的状态进行实时的精细化的数据采集，然后运用大数据以及AI的技术对采集到的网络数据进行智能分析，构建AI网络运行保障模型、实现场景化的AI网络保障应用。

如图1所示，系统构建具体的需要包含如下几个部分：

➤ 感知是第一步，需要能够做到大量的网络数据采集，可以精准感知网络的运行状态，目前来看Telemetry和ERSPAN是当前比较常用的协议，尤其是gRPC Telemetry实现了网络设备主动推送状态信息的能力，可以收集网络设备的CPU、内存、网络拥塞、网络丢包等信息、是当前对网络设备以及网络运行状态进行采集的最佳手段。

➤ 反馈系统的第二步就是开展网络分析，充分利用大数据的技术对采集到的数据进行综合分析，一方面实现网络的精准的可视化呈现，包括网络状态的可视化、网络设备的可视化、应用的可视化、用户的可视化；另一方面通过数据的分析、实现网络流量、网络运行趋势的预测、以及网络故障的精准定位，这是当前大多数网络引入智能分析之后正在逐步开展的工作，它可以更微观地看清楚当前网络运行的状态，是后续AI网络保障的重要基础。

➤ 第三步是整个利用机器学习、知识图谱等AI相关技术，结合网络相关的行业知识，构建基于AI网络保障模型以及行业知识库。这个部分会是整个AI网络的核心，也会是后续AI网络建设的重点。当前来看，对于园区WLAN网络的网络优化、对于有线网络的常见故障点定位以及优化，对于SDN数据中心网络的Overlay网络的优化，对于广域网针对应用和业务的智能调度是相对比较容易快速落地的场景。

➤ 优化和合规：优化其实主要是对AI保障的模型结果的执行。这一块其实核心就是一个网络自动化的过程，对AI系统给出的指令进行执行，对于SDN网络可能主要是通过网络控制器去执行，对于传统网络可以依赖SNMP、Netconf、命令脚本等多种手段；合规更多是结合各行各业对于信息系统的要求，进行内部的合规检测、避免AI网络智能调整过程中出现安全隐患和违反组织内部的管理规范或者是对生产系统的影响评估等。

新华三面向AI的下一代网络架构

基于AI网络的发展，结合新华三多年来对于网络领域知识、技术和建设运维经验，新华三推出面向AI的下一代网络架构SeerNetwork Architecture，详见图2所示：

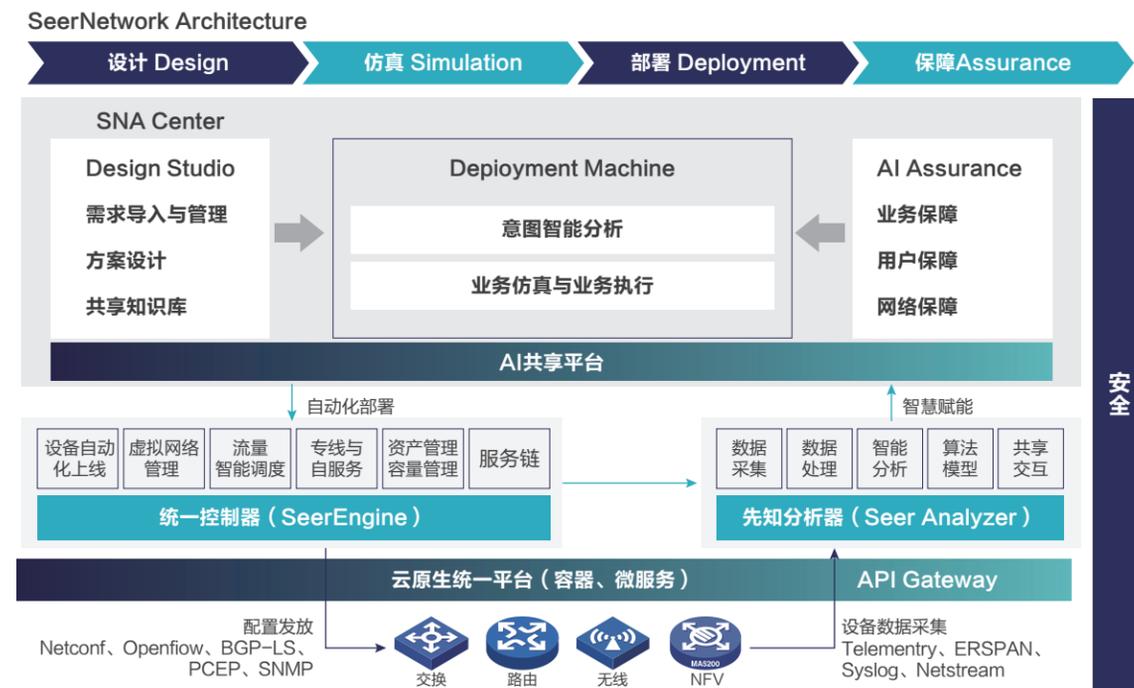


图2 新华三面向AI的下一代网络架构图

新华三面向AI的下一代网络架构，先知网络架构（SeerNetwork Architecture）简称SNA，是专门针对AI网络发展而全新搭建的新一代网络平台。整个网络系统融入了网络分析器SeerAnalyzer、统一网络控制器SeerEngine、统一的网络编排SNA Center以及全部的网络设备或网元节点。构建了包括网络数据采集、数据分析、AI判断和保障、自动化部署和执行在内的完整网络闭环系统，该架构一方面实现了传统企业三大网络场景数据中心、园区、广域网的统一融合，包括多场景控制器产品的融合、AI网络保障的端到端融合，编排层的场景融合；另一方面还实现了传统网络的和SDN网络的融合，为用户网络提供统一的运维、管理、控制。

相对于一般的智能网络系统主要面向网络保障，新华三SNA还提供整个网络全生命周期的管理，可以实现网络设计、网络仿真、网络部署、以及网络先知运维，用户借助SNA可以获取包括但不限于网络架构设计、网络拓扑设计、网络流量设计、网络安全设计以及网络流量仿真、网络故障回放、网络故障预测、和网络精准可视等能力。此外，针对中小型企业以及大型企业的大量分支机构场景在实施AI网络中面临的网络数据不足以及算力成本等问题，SNA还专门搭建了“云享”的AI网络模型，在云端构建全面的先知服务中心，提供高算力、全场景的AI网络分析能力，在靠近用户侧通过先知分析器实现数据的采集、数据的ETL等，然后将整理后的数据送到先知服务中心，由先知服务中心对数据分析，生成相关的网络保障判断模型和策略，然后在返回到先知分析器进行本地执行和处理。

AI网络的发展与演进

同大多数行业一样，网络领域的人工智能终极目标是向整个网络的自动驾驶，实现整个网络在无人干预的情况下能够智能的匹配业务，故障自愈甚至于自我能力提升。但是这个过程并不是一蹴而就的，从目前来看至少应该会经历三个阶段。第一阶段也就是想现在所处的阶段，部分智能化的阶段，是属于智能网络的起步阶段，更多是系统的搭建、数据的采集，AI方面是人工预设决策树模型，提供有选择的单点智能应用模型。第二阶段预计会进入到有条件的智能化阶段，这一阶段网络自学习是基本的特征、同时智能应用会在限定场景中全面展开，比如园区的WLAN应用，广域网络智能应用、数据中心的VXLAN网络等，这个场景典型的特征应该是场景化的变化基本可预测，AI初步具备了特定场景的智能处理能力。第三个阶段是全面的智能化阶段，这一阶段整个网络具备全场景业务识别与资源预测、全场景自我诊断与闭环优化，完全可以在脱离人为的干预下，实现整个网络智能运行，在这个阶段基础网络设备和网络拓扑以及基本的网络连接的技术相比现在都可能发生更大的变化。

新华三基于AI发展的路径以及行业实际发展情况也给出了新华三智能网络的长期规划路径，那就是SDN时代的网络自动化，主要是解决网络的自动配置的问题；第二阶段也就是当前的智能网络阶段，网络自优化的阶段，主要是引入数据分析、机器学习实现网络的预测、洞察与场景化的网络保障；第三个阶段则是智能网络的终极阶段网络自主化的阶段，这个阶段网络完全可以自学习、自配置、自优化、自诊断、自恢复。

在这个数字化转型的时代，我们致力于网络变革、拥抱AI，期待为客户提供更加智能的网络解决方案，夯实客户数字化的网络基础连接！



金融IT系统现代化之 ——智能运维转型

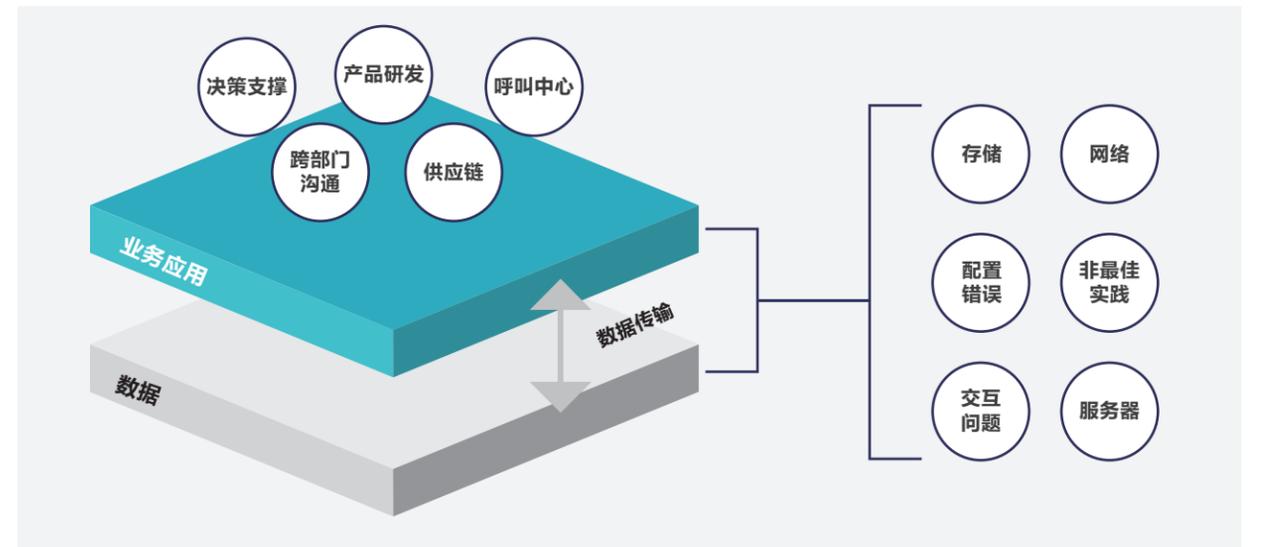
新华三集团智慧计算与存储产品线 杨涛

从Alpha Go围棋智能机器人战胜人类开始，近年来AI的概念在各行各业快速发展，部分领域已经开始落地开花。与此同时，IT设备管理运维的智慧转型也得到了金融企业用户越来越多的关注，部分企业已经开始尝试AI的适用场景。然而IT到底该如何变得更加智慧，如何落地，成为了各企业在智慧转型中的难点。

我们知道，在金融IT初期阶段，IT的供应厂商有限，每个厂商的设备型号也较为单一，即用户可选择的服务器、存储及网络供应商较少，即使全部组合起来也无非就十几种选择。运维工程师只需要掌握这些有限产品型号的特性，就可以相对简易地运维设备、售后维护。即使在设备出现故障时，运维人员也可以凭借对各个产品的运维手册的熟悉，结合已有运维经验，迅速准确的定位问题所在，从而有的放矢地排错。



随着X86取代小型机的趋势越来越明显，IT环境变得丰富和复杂起来。然而这带来的问题是，一旦IT系统发生问题，面临的都是数日甚至数周的排查纠错。但与此相对应的，用户并不会有这么好的耐心。根据第三方调查数据显示，如果用户在一个应用上连续超过3次无法正常访问，消费者很快就会转移到另一个同类应用上。显然，IT保持持续可靠的向业务交付数据，已经是企业核心市场竞争力之一。





但事实是今天的现实情况已经发生了天翻地覆的变化。由于国内外IT供应商的迅速发展及用户应用类型的不断丰富，现代数据中心机房出现了几个典型特征：

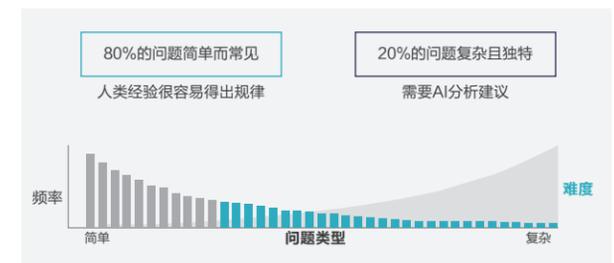
- 机房采用设备供应商数量迅速增多：从之前以IOE为代表的十几个典型供货商，扩展到现在国内外数十家乃至数百家的产品供货商，设备的数量和管理复杂度与日俱增。
- 应用越来越复杂：随着互联网思维在各个行业的落地开花，对各种新应用和新业务的上线速度要求越来越快，要求IT具备更灵活的架构和更简便的管理。
- 随着机房环境越来越复杂，有IT设备发生故障的可能性也越来越高。与IT初期阶段不同，现在的故障可能出现在复杂基础架构的每一个环节。运维工程师如果还坚持过去的处理理念，凭借已有经验只能覆盖10%~20%最常见的错误，我们不得不持续增加运维工程师的数量、不断地学习和培训以增加运维工程师的能力，来应对日益复杂和日益困难的运维任务。

但即使这样，一旦前端业务访问数据出现问题，非常难在第一时间定位问题到底出现在哪里。如下图所示，90%的问题发生在存储层以上，直接排查存储也许只能解决10%的问题。所以现实中，更多的情况是各个系统的运维工程师都需要联合纠察，通过不断尝试排查故障，通过排除法找到问题所在点。毫无疑问，这项工作耗时良久，排查过程也不但是对工程师的能力要求极高，更致命的是排错时间对业务应用的打击。



更令人遗憾的是，即使在某个客户处解决了这个疑难杂症，其故障解决经验也只在排查故障的运维工程师这里积累，无法与其他运维工程师知识共享。这样，同样的故障很可能在全球每一个角落重复上演，却没有办法快速提升解决问题的效率。

对运维工程师来说，大部分常见问题可以凭经验搞定，但还有20%的“疑难杂症”占用了80%的运维精力。HPE/H3C InfoSight正是从这一点出发，可以为这些“疑难杂症”快速提供解决之道，大幅度提升运维效率。

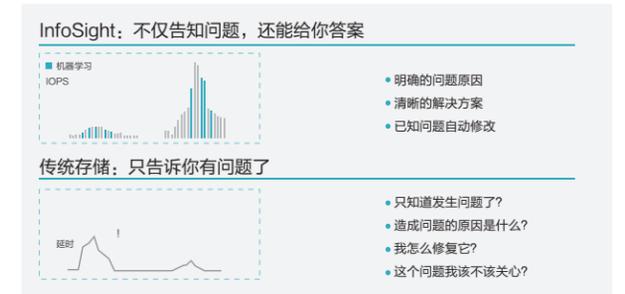


InfoSight是一套融入人工智能机器学习的智能运维系统，可以把全球所有部署InfoSight的硬件设备的运维数据实时共享。全球只要有一台设备发生过这个故障，InfoSight就会把这个故障的征兆以及对应的解决方案记录并共享，一旦其他存储设备遇到类似的情况，InfoSight就可以提前预知故障，甚至主动预防和处理。就像给存储设备打上故障疫苗一样，其他存储设备就不会发生同样的故障了。

这一功能在IT运维领域极其有效。

举例来说，下图是传统存储管理中经常会遇到的情况，在某一时刻，性能曲线图里出现了一次时延显著提升。由于这种时延上升出现的很频繁，我们很容易忽略它，但却不知道背后到底意味着什么深层次的原因。就像我们的身体偶尔感到不舒服一样，也许只是普通感冒，但有时，却意

味着重大的健康隐患。



通过InfoSight，不但会告知用户每次异常时候的状态，还能够分析背后的故障原因，判断究竟是一次普通感冒，还是一个重大的健康隐患！如果经判断只是一次正常性能波动，并没有严重的系统风险，InfoSight则会自动关闭问题，告知你不需要额外关注了。

通过InfoSight，我们可以做到以前的IT运维想不到也做不到的事情：

- 风险预防：立足现在，发生一次问题可以为全球用户免疫，也可以告诉全球客户某种应用下的最佳实践。
- 需求预测：将已知问题发生之前很明显的特征集推送到全球所有设备，提前感知问题，提前给出建议，给出应对计划，避免容量不够、性能不够等问题的发生。
- 应用感知：不但可以感知到存储本身的潜在风险点，还可以感知到服务器、网络等各个层面的传感器信息，第一时间判断问题点到底出现在哪一个硬件层面。

另外，InfoSight在具备在线版本的基础上，现在还支持离线版本，我们可以针对不同应用系统不同的信息安全需求，提供全面的选择。近日，InfoSight在线版本也已经通过了公安三所认证，确保用户数据的私密性。

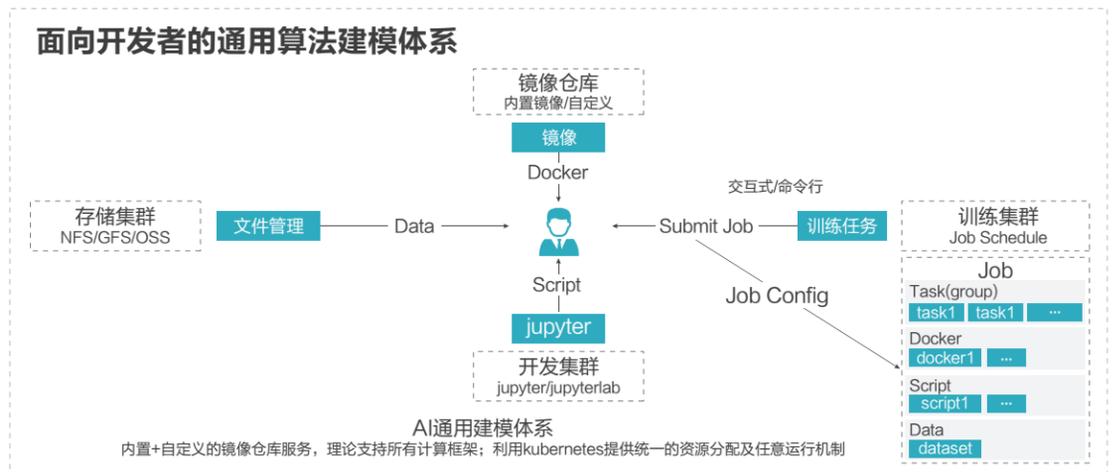
通用人工智能计算

新华三集团研究开发部AI研究院 杨新安、杜鑫

人工智能已成为金融科技一个重要的技术分支。近几年深度学习的成功除大量标记的数据样本、深度学习模型与算法外，尤其需要高性能的系统平台的支撑。深度学习分为线下训练和线上推理两个部分，对线下训练而言，可采用高速网络+分布式并行计算、存储的高性能集群系统架构；平台软件采用高性能分布式弹性架构，能够支持Tensorflow/CNTK/MXNet/Pytorch等多计算框架，支持容器化、微服务业务部署，大幅度提升运算效率。新华三根据深度学习的实际需求，推出了新一代人工智能深度学习支撑平台AIOS。

首先，AIOS平台具备多租户服务能力，不同用户分别具有不同权限，用户可以自动获取计算资源，平台实现了专业开发者使用平台时的自动化和灵活可控性的平衡。平台提供分布式GPU多机多卡训练支持，能够有效利用计算资源、大幅度缩短模型训练的过程、提高资源利用率、节省计算时间；平台还提供环境依赖组件目录、工具集和系统镜像，方便用户个性化定制或者统一规范使用。通过目录管理这个高效的集群管理系统，用户能够实现一键部署，快速安装上线。平台可以帮助用户大幅度提高自动化程度，提升效率，降低人工维护成本。用户采用平台后可以使其计算环境实现按需分配，便捷部署以及维护方便。

其次，AIOS平台是一个可视化的交互开发平台。平台可以实现训练日志及评估指标可视化，支持管理、开发、审计三权分立。平台的API的代码自动补全功能，方便用户随时调整训练脚本，修改网络结构，并及时运行脚本；平台算法组件丰富，无需额外更新算法，算法包括机器学习、深度学习工具和行业模板库。平台具有多种超参搜索能力，能够简化调参，简化代码。平台还可以实时监控训练进度，查看资源利用率图表、损失图表、训练日志等。平台支持从使用的视角进行管理，具备一站式的任务流程导引功能，即“任务流模式”，实现对通用人工智能算法的设计、执行、优化等全过程管理。用户可以根据流程导览图，一步步的完成训练资源申请，AI模型的数据集处理，训练调参直到模型发布部署，如下图所示：



通用算法建模体系



通用算法建模体系



OCR识别模型训练视图

平台条件的运行时环境，并自动执行用户的运行命令，并实时监控作业的运行状态，当达到作业的停止条件时，平台会自动停止作业运行。通过这种通用的作业调度模式，平台理论上可以支持任意的计算框架以及任意的运行方式；另外，平台还在此基础上订制出各种面向特定场景的运行组件，方便用户以更简单的方式进行作业训练。

在该平台上进行的OCR开发实践为例，如下图执行一次COR模型训练，看到的监控界面如下图所示：

平台的任务流引擎，能够为用户带来如下优势：

➤ 满足不同AI工程师对各种计算框架的使用需求，以及作业运行方式的千变万化，设计出通用的作业调度语言，即规范出一个作业统一的行为模式，比如：

- ◆ 作业的运行环境（镜像）
- ◆ 作业的资源使用要求（单节点，多节点，以及多节点间的通信端口）
- ◆ 作业的运行脚本
- ◆ 作业的数据集（不是必须的）
- ◆ 作业的运行命令、停止条件

➤ 平台会根据用户的作业描述配置文件，自动创建满足用

最上面的是训练的进度，中间是各种硬件资源的占用情况，最下面就是训练的准确度和损失函数的调整梯度以及训练的数据集批次（BATCH）。如果想快速完成训练任务就需要申请更多的计算资源。通常这样训练调整参数会反复很多次，直到模型准确度达到期望值。然后把这个模型发布到另外的一个人工智能推理平台上面，就可以执行后面的推理和识别的任务了。

新华三AIOS通用人工智能平台有效降低了相关金融应用开发的复杂度，提升了开发效率和管理能力，相信能在票据识别、生物特征识别、智能投顾、金融风险控制等领域发挥更大的效用。

新华三金融

智能网点解决方案

新华三集团金融事业部金融技术部 叶宗海

金融网点行业趋势

随着金融与科技在业务运营、风险控制等层面不断融合渗透，贴近基层，面向大众的营业网点也向着无人化、智能化、业务云化趋势变化。面对营业网点管理运维复杂，环境设施和广域网智能化程度低、AI能力弱，生物识别新技术引发的边界安全等挑战，新华三有着自己的理解和解决方案。

金融企业的演讲路线目标智能化，实际是服务体系全流程的智能化，而智能化前提是数字化，数字化是智能化的基础。金融网点在数字化转型中经历了四个阶段，从传统的跑马圈地，粗犷的扩展物理网点时代，到ATM自服务、网银等拓展服务时间边界，再到以移动APP支付、掌银的互联网时代，银行业从来没有停止对未来智能化的追求脚步，无人银行和5G银行网点已经开始走进人们的视野和生活。借助人工智能、大数据、5G等新兴技术实现网点自助智慧化，金融网点正在由“交易结算型网点”向“服务营销型网点”转型。

网点数字化转型三个重要的特征

无人自助化

现金服务的需求将越来越少，银行服务的离柜率越来越高，网点的撤并将成为一种趋势。

智慧服务

利用人工智能、生物识别等新兴技术构建人机交互闭环，打造智能型人机协同模式，最终建立“能听会说、能看会学、能理解会思考”的系统智慧服务体系。

全业务云化

业务后台的大集中上收，网点逐渐走向了轻量高端化，一个网点的建设“香不香”，也是一家金融企业形象的象征。

金融网点数字化转型中遇到的挑战

挑战 1—环境智能化不足

➤ 环境智能化不足与网点的特征是密切相关的，网点的特征分散且覆盖范围广，其建设初期往往会涉及空间和供配电等因素的制约，其次网点无专业运维人员。所以整个IT设施的设计和建设周期很长，一体化交付能力弱，很大程度上会影响网点的开业时间。

➤ 常言“三分靠技术，七分靠管理”，一套合规、有效的管理方式是很有必要的，面对众多分散的网点，打造一套可视、分层、及时响应的管理系统是环境智能化的重要基础。

挑战 2—AI 能力不足

现有网点的人机智能能力不足，极大影响了智慧服务体系的建设，在业务指导层面也无法由传统的洞见走向预见。现有网点安防设备的痛点主要有如下几点：

- 传统的视频及安防设备功能单一、面对复杂的应用场景、多业务能力弱，比如像像迎宾、精准获客等能力不足。
- 其次传统安防设备内置算法固化，无法成长、且 算法升级过程中业务中断，会丢失部分节点数据。
- 再者金融企业已部署了大量的安防监控设备，如何保护既有投资？

挑战 3—边界安全问题

金融和新兴技术的融合渗透，衍生出新的应用场景。像大数据、生物识别新技术引入会引发的新的边界安全问题：

- 人脸考勤、门禁、IP电话以及传统的ATM机等物联网终端被仿冒的问题。
- 资产的全生命周期管理问题，如设备无故离线、丢失等资产安全。
- 安防设备自身的安全和考核量化问题，以及处理的工单全流程自动化能力。

挑战 4—广域网自动化能力问题

在信、贷、汇业务分解背景下，产生了上千个“微服务”，分布式多地多DC建设、业务向云化背景下，业务层面要求按需接入，如何打造一张适应业务发展，面向未来的网络保证业务的快速开通、安全稳定、可靠高效和可视化运维，传统WAN技术自动化能力弱瓶颈凸显。主要存在如下问题：

- 业务开通周期长，专线价格昂贵，业务灵活性差
- 网络设备功能单一，多业务扩展性差
- 无法适应快速变化云业务
- 网络运维和可视化能力弱





解决方案

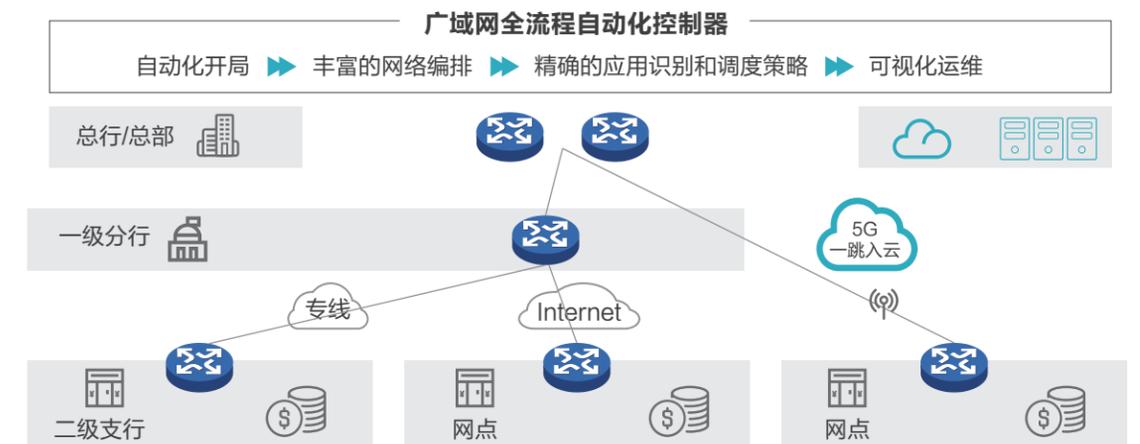
数字化转型过程中，面对以上四个挑战痛点问题，行业趋势目前主要有如下措施：

➤ 通过打破原有安防思路，采用前端软件定义摄像头和智能化前端生物识别设备，筛选并结构化关键数据模型，将海量结构化的数据上送给存储并解析，打造端、边、云全方位的智能安防体系，构建基于数据智能的安防视频云，填补数字化转型过程中AI能力不足的问题。挖掘数据智能的价值既传承了通用安防应用，也可定向开发针对金融行业场景应用，并具备持续开发演进，快速上线的能力。



➤ 针对网点分散、覆盖范围广的特点，需建设一套广域网全流程自动化管理平台，通过该平台构建分行和网点灵活接入的能力，无须做任何繁杂的配置即可接入。

从网点广域网的零配置上线开局，到网络编排，再到上层的关键业务识别保障，线路之间的可视灵活调度，该平台应具备全流程的自动化能力，使得网点的网路接入智能化水平得到了大幅度提升。



➤ 针对新技术应用引发的边界安全挑战，一套安全、可信的网络连接管理系统是很有必要的，通过其内置的边界感知识别特征库，识别所接入端点设备的厂家、ip地址、mac地址等关键信息，将扫描到的信息周期性的与预定义的合法基线策略进行比对，有效的解决了边界物联网设备接入的合规性和资产管理的问题，且针对视频专网这部分，该套系统还具备主动发现和分析视频故障的能力。通过基线比对、主动发现分析手段，确保了整个接入网络的端点可视、可信、可控。

解决方案客户价值

面对营业网点管理运维复杂，环境设施和广域网智能化程度低、AI能力弱，新技术引发的边界安全等挑战，新华三金融智能网点解决方案集成了金融安防视频云、广域网SNA自动化、鹰视网络连接管理，从建设到运维，提供一体化、一站式交付能力，辅以主动安全和可视化运维能力，全面助力网点数字化转型。

在可靠灵活的广域网接入基础上，依托新华三鹰视网络连接管理解决方案为AI安防设备保驾护航，借助新华三金融安防视频云，提高网点智能化程度的同时，也可利用旧原有安防设备，保护客户原有投资。通过整合多张网数据，深度挖掘数据价值。将以人为主导的安防，转变为以机器主导的安防思路，向着“机器研判”、“机器决策”方向演进；安防事件的处置手段，也将从原来的“事后追溯”向“事前预防”发展，先知先觉。



金融行业分支网点 机房的智慧化之路

紫光软件智慧能源事业部 郑鹤

随着IT自动化程度不断提高，移动互联网和云计算产业的迅速发展，对传统数据中心建设模式提出了更高要求。而对于大中型集团企业来说，传统的分支机构数据中心没有统一规划的标准架构、采购部署周期长、本地维护复杂、无法远程统一管控等一系列难题。

对于金融行业来说，分支网点具有数量多、分布广、位置分散等特点，网络系统是分支网点日常业务办理和事务管理的通信载体，是分支网点重要的基础设施之一。网络系统的正常稳定运行直接关系到分支网点的业务开展连续性和客户服务满意度水平，而一个好的环境是信息系统安全稳定运行的必要保障。

在此背景下，针对金融行业分支网点机房，为节省工程投资，缩短建设工期，减少运营成本，提高运维效率，增强机房的安全性和可靠性，紫光软件推出UNIS-IC系列智慧机柜产品，提供一体化机柜级数据中心解决方案，为金融行业分支网点机房建设提供助力。

UNIS-IC系列智慧机柜产品依据微型模块化机房理念，采用密闭式机柜构成一个信息设备运行的空间，柜内集成配电、电源、制冷、监控等4大功能模块，所有组件采用工厂预安装方式，可以实现现场快速组装部署。

依托于紫光UNIS-IC系列智慧机柜的一体化机柜级数据中心解决方案，提供了一种机柜微环境集中监控和机柜基础设施管理的手段，以智慧机柜为基础元素，可以构建安全、可控、智慧的机柜设施，为IT设备安全运行创造条件。

紫光UNIS-IC系列智慧机柜的应用可以为您带来全新的管理提升和体验：

全方位的运行环境监控

紫光UNIS-IC系列智慧机柜才用了机柜级、细粒度、全面

化、精确化监控理念，通过安装与机柜内部的传感器，全方位监控机柜微环境情况，立体展现机柜状态，实时掌控机柜之间的细微差异，实现对全部机柜设施的集中管控。

对于传统的分支网点机房，缺乏全面而有效的智能化监控措施，故障往往是事后很久才能发现，而且故障原因不明，需要浪费很多时间和人力反复排查。通过采用紫光UNIS-IC系列智慧机柜可以实现对分支网点机房设备运行环境的温度、湿度、漏水、烟雾、用电、设备运行状态等实时监控，管理人员通过集中管理软件平台随时随地可以了解每个网点的情况，并且可以精确定位告警故障点，大大提升故障响应和处理效率，提高运维工作效率，降低运维工作成本。

有效的安全提升

紫光UNIS-IC系列智慧机柜采用了更为可靠的机柜级安全

机制与状态监测，提供机柜级电子门禁功能，需要授权刷卡解锁，杜绝非法访问机柜，为提升机柜管理创造条件。同时，实时监测柜门开关状态，避免柜门长开引发的安全风险。

传统分支网点机房，金融分支网点一般没有专业网络运维人员，通常由信息部门一位管理人员管理很多个分散的网点，运维人员开展运维工作周期长，无法掌控机房环境，往往出现了网络系统故障才能发现问题，只能事后处理。

尤其是近年来，随着社区金融网点的普及，分支网点逐渐向小型化、网络化、智能化发展，分支网点的面积也不断缩减。在这种情况下，许多分支网点的机房还被当成了打印复印室、储藏室、休息室来使用，人员进出频繁，物品散乱，这对网络系统带来了安全隐患。通过紫光UNIS-IC系列智慧机柜的应用，由管理人员对各分支网点统一进行管理，通过集中管理平台授权指定机柜、指定时间段的门禁卡，打造安全、规范、有序的机柜应用场景。

可见的管理提升

紫光UNIS-IC系列智慧机柜集中管理平台集中监控下属各分支网点机房/机柜的运行情况，提供可视化界面，人性化的交互操作，管理人员对机柜设施情况一目了然，提供顺畅的操作体验。

分支网点位置分散，且没有专门的信息设备维护人员，一般是一个地区、多个网点由一位技术人员负责信息设备的运维管理，运维人员开展运维工作周期长，无法掌控机房环境，往往出现了网络系统故障才能发现问题，只能事后处理。技术人员对网点信息设备运行环境的实时掌控，是运维管理工作能够及时、准确完成的必要条件。

紫光UNIS-IC系列智慧机柜在机柜内部署温湿度传感器、烟感探测器、水浸传感器、门状态传感器、LED灯条、智能PDU等智能化组件模块，对机柜内的动力、环境进行7*24小时监控并报警。并且监控系统可开放协议，与空调、UPS、智能配电箱等对接，实现动力环境一体化管控。通过部署紫光UNIS-IC系列智慧机柜集中管理平台软件，通过TCP/IP协议，将各网点机柜监控集中接入。可有效监控各网点机柜内部动力、环境等信息，技术人员不需要去现场即可远程在线管理机柜内部环境，方便了技术人员的操作，减少了工作量，提高了工作效率。

高效的预警机制

紫光UNIS-IC系列智慧机柜基于实时数据的告警判断，可以第一时间发出告警，消除安全隐患，保护设备硬件与应用系统运行的安全。

传统分支网点机房，往往是发现网络或者业务中断，才能知道设备出现故障，并需要花费大量时间和人力进行故障排除和处理，造成业务和服务长时间中断。紫光UNIS-IC系列智慧机柜的应用，提供全面的环境和设备状态监控，

发现异常可通过声光告警器、集中管理平台界面弹窗、邮件、手机APP端、短信、语音等多种方式及时告知相关管理人员，便于运维人员及时处理；另外，紫光UNIS-IC系列智慧机柜的应用，可以提供环境和设备状态监控的大数据分析，提前预知系统的使用状态、使用寿命，便于管理人员做好系统扩容、升级、改造、替换的规划，提高系统及业务的连续性、可靠性和安全性。

自愈的环境系统

紫光UNIS-IC系列智慧机柜采用与环境参数联动的环境调节设备和手段，打造一个具备环境自愈功能的系统维持稳定、安全、可靠的设备运行环境，减少人工操作，让您高枕无忧！

传统分支网点机房安装的空调都是家用空调，无法支持长时间持续运行，容易发生故障。同时家用空调不支持来电自启动，停电恢复后，无法提供制冷。尤其是许多分支网点位于写字楼，机房制冷采用写字楼中央空调。但中央空调只在工作时间提供制冷，在夜间和周末不运行。另一方面，写字楼不允许安装空调室外机，无法安装空调。以上情况，都使机房面临空调失效的情况，造成机房温度升高，影响网络系统设备运行安全。紫光UNIS-IC系列智慧机柜的应用，提供了工业级的空调制冷保障，可以365天*24小时不间断运行，并且空调采用无室外机设计，解决了写字楼无法安全室外机的困难。同时，紫光UNIS-IC系列智慧机柜实现了环境监控功能与空调制冷功能的联动控制，通过实时监测设备运行环境温度，联动控制空调启停，提升了空调制冷的及时性和可靠性。

促进节能减排

依据全面的环境数据和能耗管理，紫光UNIS-IC系列智慧机柜可以为用户制定节能减排措施提供决策参考，帮助用户科学实施节能减排，并提供直观的效果展示。

结束语

紫光UNIS-IC系列智慧机柜为标准 19 英寸机架式机柜，通用性强，可安装各类标准服务器、网络设备、工业控制设备等。智慧机柜由机柜柜体、智能监控主机、触摸屏、机柜门禁和相应的传感器以及各外部功能设备组成。

依托于紫光UNIS-IC系列智慧机柜的一体化机柜级数据中心解决方案，是从分支网点实际情况出发，既能解决信息设备要求的技术问题，又能解决金融行业要求的成本和利用率的问题。

紫光UNIS-IC系列智慧机柜的应用为用户带来全面的智慧化提升：

- 全面温度管理：通过机柜前后部上中下共 6 个温度探头，全面监测机柜温度分布。
- 用电监测：监测 PDU 电流、电压，统计整体负载和用电量，协助用电管理。
- 机柜电子门禁：机柜专用一体电子锁，刷卡开门，并记录开门信息，支持远程解锁。
- 资产管理：统计数据中心机柜安装的资产信息，跟踪使用和运行情况。准确的资产位置管理，方便查找设备。
- 空调联动：根据温度自动启停一体机柜空调，无室外机设计，内置冷凝水蒸发装置。
- 在线集中监测：集中展示所有网点环境情况，实时掌控异常信息。
- 分级管理：支持权限分级和分布式部署，方便与管理体保持一致。
- 告警分级：告警分为普通告警、严重告警和紧急告警，可设置针对不同级别告警的告警方式。
- 自动灭火：支持联动气溶胶灭火装置自动灭火。

紫光UNIS-IC系列智慧机柜的应用为用户带来全面的智慧化体验：

- 机柜级机房解决方案：小型美观、紧凑收容，支持多场景、多功能应用，兼容多厂商产品。
- 近端监测、节能减排：根据不同的环境状况，空调自动起停，高效协同。
- 一体设计、快速建设：工厂预安装，现场快速拼装部署，以机柜微模块，侧面并柜，平滑扩容。
- 电信级设计、安全可靠：可靠的组部件，保障设备安全、可靠运行。
- 节约投资、降低成本：采用密闭智慧机柜的一体化机房解决方案相较传统机房建设方式，建设投资可节省30%以上，运营投资可节省50%以上。

人工智能在 金融安全中的应用

新华三集团金融事业部金融科技部 韩喆

有金融科技浪潮下，互联网、大数据、云计算等技术与金融业务有机结合逐步成熟，显著地提升了金融服务效率，降低了服务成本，大幅改变了人们的生产生活方式。然而科技创新也带来了新的风险，当前金融科技创新步伐持续加快，系统的复杂性、用户的多样性、应用环境的差异性对网络安全提出了更高的要求。金融机构应持续优化智慧安全体系，不断提升安全服务和保障能力，提升对未知风险威胁的防范能力。

新华三通过构建主动安全防护体系，为金融科技创新保驾护航。人工智能目前已成为新一轮产业变革的核心驱动力。通过人工智能的应用，构建智能化的网络安全主动防御体系，成为网络安全领域新的发展方向。通过构建“安全大脑”，对全网海量安全信息进行自动分析与深度挖掘，及时掌握安全状况和发展趋势，快速进行自适应联动响应，从而全面增强整体安全防护能力。通过建立基于大数据和人工智能技术的主动防御安全模型，先期发现、主动发现和应对安全威胁，基于用户类别和历史数据对内网用户建立立体化识别方式，可以根据用户的位置、目的、行为、基线等方面形成一个具有判断力、识别力的大脑，确保只有合法用户使用才可以生效，有效识别APT及用户仿冒等攻击，实现更加智能灵活的安全防护。



人工智能在主动安全中的应用方向

随着网络攻击的数量、种类、手段越来越多，充分利用人工智能、机器学习等技术，对传统数据挖掘、统计计算、关联分析方法进行革新与丰富，将成为发现安全威胁与异常的新利器。

通过在一定时间及空间范围内感知所发生的网络安全事件，针对海量安全数据进行综合处理，分析全网受到的攻击行为，评估网络的整体安全状态和预测未来的安全趋势，展现全网的“全局视图”。人工智能及机器学习的主要应用方向包括海量数据分析、未知威胁发现、潜在风险预测和自适应联动响应等。

海量数据分析

从大量结构繁多、来源不同且类型复杂多样的安全日志数据中挖掘隐藏规律，实现从海量安全日志数据向有价值威胁告警的转化。

未知威胁发现

结合外部威胁情报，在数据级、特征级、决策级三个层面利用机器学习算法进行分析处理，从海量的原始安全数据中定位威胁线索，实现对未知威胁的及时发现。

潜在风险预测

通过对全网网络资产、行为、流量和用户全方位、多维度动态分析，从大量的安全事件之中发掘隐藏的相关性，判断潜在的风险。

自适应联动响应

进行自适应决策并实时生成控制策略下发，通过联动响应对攻击源进行控制、阻断和溯源，实现全过程闭环反馈。

基于人工智能的主动安全体系

为了有效地掌控全网安全状态、风险和趋势，依照数据管理、特征管理、特征工程、模型训练和测试评估等流程步骤，利用业务模型完成未知威胁发现、风险预测和自适应联动响应等应用，从而提升安全防御能力，优化安全防护体系。

系统框架

基于人工智能来构建“安全大脑”，对一定时间及空间范围内大范围样本数据进行智能化分析，根据基线或模型发现威胁风险并预判趋势，系统框架如图1所示：

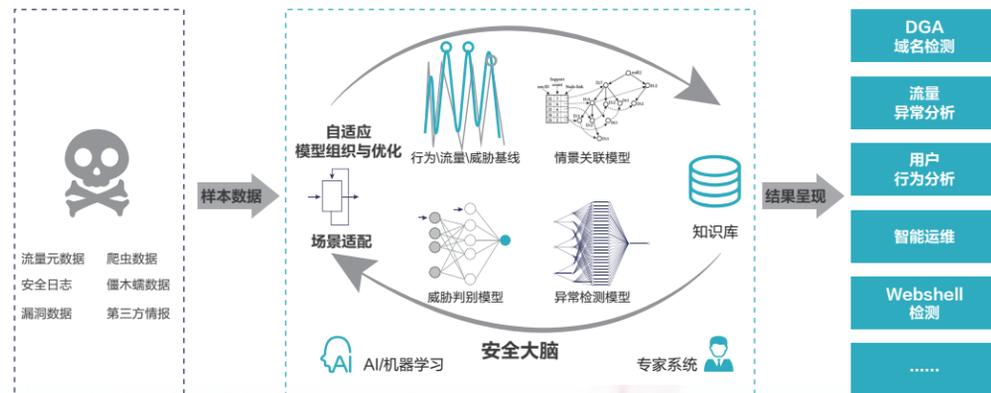


图1 基于人工智能的系统框架

针对实际网络中安全数据的海量、多格式、多梯度的特点，系统主要完成如下3个部分功能：

- 数据预处理：安全系统的输入来自不同数据源，不同数据源对网络安全事件的定义通常具有不同的格式，通过报文分类和范式处理将数据归一化为统一格式，然后进行去除冗余及噪声数据。
- 智能分析：根据业务逻辑不同，利用不同的机器学习算法（如分类算法、聚类算法、关联规则挖掘算法、深度学习算法）训练出相应的网络流量分类、异常流量检测、威胁行为分析和流量趋势预测模型，然后根据训练出的模型进行结果输出。
- 评估优化：根据知识库中的安全量化指标体系，对分析输出的结果进行量化评估，通过学习和分析用户使用过程的历史数据反馈，用来改进模型和算法参数，从而不断提高模型的准确率，减低安全事件的误报率并有效发现潜在威胁。

业务模型

威胁发现模型

在建立目标威胁模型时，分析影响威胁度的若干因素，需要选择合适维度的特征参数，可以采用粗糙集理论中知识约简方法选择目标的最优特征子集；然后利用支持向量机建立威胁判断模型，通过对知识样本的学习，采用SVM算法获取威胁值与特征参数的非线性量化关系，从而估算出目标的威胁程度。

风险预测模型

基于FARIMA模型和混沌时间序列模型对网络流量进行建模，在BP神经网络预测模型中引入小波多分辨分析方法，将小波变换独特的多分辨分析与神经网络的自学习自适应和非线性逼近功能相结合，建立小波神经网络预测模型，预测准确率可达到90%以上，再根据网络流量和行为的歷史数据对未来流量和行为的風險实现预测。

联动响应模型

构建以“知识”为中心的、以控制网络行为为目的框架模型。通过引入上下文管理模块，用于加强已知控制策略的保存和自学习，当网络态势及业务目标等发生变化时，在知识库和策略库的支撑下，可利用基于案例的推理（CBR）方法自适应生成和调整控制策略，从而消除或减轻由累积错误导致的系统可靠性不高的问题。

价值体现

利用人工智能技术，可以对成千上万的网络日志、威胁情报等信息进行自动分析处理与深度挖掘，从海量数据中提取出真正有用的信息，对网络安全状态进行分析评价，感知网络中的异常事件与风险威胁，并对全网的趋势进行预测和预警。

从“结果可视化”向“过程可视化”的转变

通过机器学习引擎，对隐藏在网络流量、各种设备及系统日志中的海量的正向样本和恶意样本进行分析，针对全过程攻击链中攻击者留下的任意线索进行多维拓展，可视化

绘制出完整的攻击链条，从而提前进行防范，实现对威胁全过程的可视化溯源追踪。

从“主机IP识别”向“用户行为识别”的转变

通过传统的IP访问控制已经无法应对复杂的安全事件，新华三采用机器学习技术对用户行为进行检测，通过多维度行为特征对用户进行画像，首先通过用户的歷史交易数据、用户信息特征进行梳理分析和数据搜集、挖掘，形成用户交易基线，加载到安全策略管理中心，由安全策略管理中心根据不同账户进行安全策略调整，当具体用户行为发生的变化超过设定的阈值时候，自动进行告警和分析发生异常的原因。

从“安全产品化”向“安全服务化”的转变

为了应对网络安全的挑战，VPN、防火墙、IDS、身份认证、数据加密、安全审计等安全防护系统得到了广泛应用，但这些产品大部分功能分散，各自为战，形成了互相隔离的“安全孤岛”。通过在云端上应用机器学习等新技术，为用户提供相应的安全AI服务，让每个SaaS企业都能拥有自己的“安全大脑”，实现云化防护。

结束语

为了有效应对日益高级和复杂的攻击手段，以安全情报为驱动构建“安全大脑”，充分利用云端的检测能力，对海量的安全信息进行自动分析与深度挖掘，及时掌握网络的安全状况和趋势，提前制定有预见性的应急预案，对金融用户的业务交易进行全方位、全流程的交易监控，预警交易中的潜在风险，并联动自动化的应对机制和人工参与等处置措施，完成风险交易智能化处理，全面提升应对网络安全威胁的能力。

金融视觉中枢， 推动智慧金融加速落地

2015年，公安部更新中华人民共和国公共安全行业标准GA38-2015（银行营业场所安全防范要求），作为公安部下发的强制标准，在人防、物防、技防上面提出了很多规范性要求，是指导和加强通过银行业安全防范设施建设、审批、验收、日常检查、安全评估提供了工作依据。

目前，银行技防系统经过近20多年的发展，已经非常稳定、可靠，并且大部分银行实现省、市、县三级联网，各子系统也实现了相互联动，随着GA38-2015银行业标准、GA745-2016自助行标准、银行安全评估标准的颁布，老一套的技防系统已经到了急需改进的地步，存在以下几点问题：

清晰度不高

以模拟视频监控系统为主力军的当代金融安防系统，在走过将近20年的发展之路后，渐渐步入瓶颈。随着金融体系的发展，如今的金融安防，面临着越来越多的问题。

前端模拟摄像机依然存在“看不清”、“看不对”、“看不见”的种种问题，随着GA38-2015新标准的实施，提出看清人物的面部特征、车牌颜色、车牌号码等更高的要求，就目前的安防系统来说，前端模拟摄像机基本上都是标清产品，在实地测试过程中，这些产品的清晰度，不能满足标准的要求。

未实现多层次架构，系统架构单一

随着视频高清化改造，在营业网点均采用传统DVR或NVR设备，银行多个营业网点、支行、分行、总行的视频未实现多层次架构互联，硬件资源及数据因物理分散形成了孤

岛，无法实现资源的弹性复用及数据共享，系统架构组成单一容易形成单点故障。

缺少智能化改造，视图数据未产生价值

受制于前端设备点位的高清质量及系统架构单一，银行营业网点的视图数据处理手段单一，缺少智能化处理手段，例如车辆识别、人脸识别、人体识别等。即便单个网点引入了一些智能分析功能，多个营业网点间的数据未实现数据共享，亦造成视图数据价值未能体现，无法对多个营业网点间的数据做到有效低统筹分析。银行对于安防的监控要求之高，急需改善目前视频仅作为事后查证的处理模式，需经过统一地规划，实现银行视频监控由“事后取证”向“事前预防”为主的转变。

网点带宽不足，应急指挥难度大

一般网点安防与业务系统公用一个网络，并且在保障银行业务顺利进行之后才会考虑安保的带宽需求，在进行远程应急指挥时，往往需要调出多个摄像机来看清前端实况，这时由于带宽的原因，会出现部分视频无法调阅的情况，从而影响应急预案的实施。

“全行一朵云”，新华三携手紫光华智推动智慧金融加速落地

对当前金融网点视频建设应用中存在的视频图像资源零散孤立、视频智能化应用不足、视频计算资源不足和缺乏统一调度手段等问题，新华三联合紫光华智推出金融视觉中枢解决方案，推动智慧金融加速落地。

紫光华智金融视觉中枢基于人工智能、云计算、大数据等前沿技术作为牵引，采用软件与硬件解耦、应用与数据解耦、让业务“百花齐放”的设计理念，同时遵循银行营业场所建设规范对视频监控相关标准，以海量感知数据的汇聚、数据共享与能力开放为目标，总体逻辑架构如下图所示：

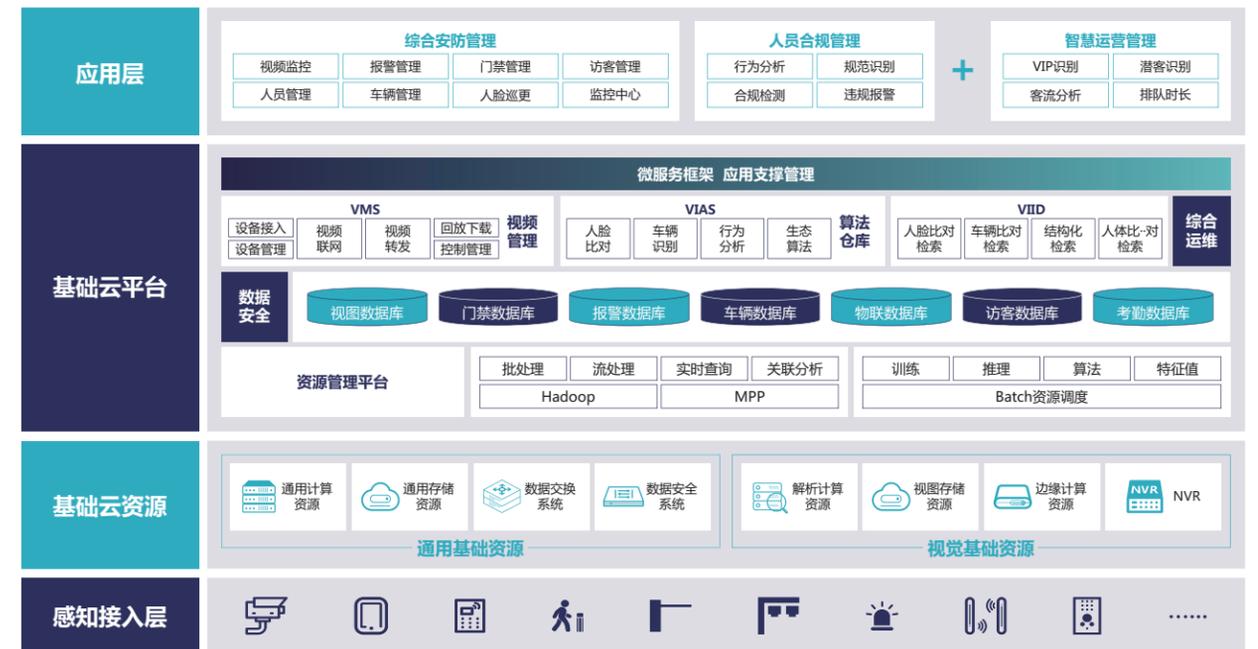


图1 逻辑架构图

总体架构分为感知接入层、基础云资源、基础云平台、视频应用层

感知接入层

进一步满足银行营业网点、大楼等公共安全视频监控覆盖范围，在营业网点进出口、大楼进出口、银行大楼及周边、营业厅关注区域等公共区域部署设备，实现视频、人脸图像、车辆图像的多维数据采集。按照GA38-2015标准中门前场所的要求，达到20米范围回放图像清晰显示人员的面部特征和车辆号牌，50米范围回放图像能显示人员体貌特征和车辆颜色、车型。

基础云资源

主要包含通用基础资源，如通用服务器、通用存储、数据交换网络、数据安全设备，以及视觉基础资源，如解

析计算资源、视图存储资源、边缘计算资源等，将传统方案中的计算、存储、网络、安全等资源进行云化，实现高效利用。

基础云平台

是整个架构的核心层，负责承接原始数据并解析梳理，得到有效数据，还负责整体云资源的容器编排和微服务治理，以及管理中间件等，并承接处理后的有效数据，进行分类汇聚，向上提供接口，为各个应用提供数据。

视频应用层

是整个方案的最终展示层，为金融视频联网提供各类丰富的综合应用，如视频监控、报警、门禁、监控中心展示，并且基于视频+AI提供基于智能化的内控合规管理、风险防控管理、银行智慧运营管理等。

金融视觉中枢技术实现

金融视觉中枢的建设应实现各级互联，全省总行、分行、支行、营业网点的统一管理，实现“物理分散、逻辑统一、按需共享”的“全行一朵云”。在此之下，单个营业网点视频云既能实现区域自治，同时支持多级管理的能力。各级视频云在和上级脱离时，能够进行独立的业务发放操作和运维操作。在与上下级互联时，能够实现任务协同、资源协同以及数据协同。



图2 部署架构图

此外，金融视觉中枢充分发挥紫光华智视频云平台的全时解析、全网应用、安全共享、实时可控等核心优势，可有效破解传统安防重建轻应用、信息数据孤岛、软硬不解耦等应用瓶颈，重点覆盖金融营业网点、办公大楼、数据中心等相关场景。



方案价值

基于云化技术构建视频底层资源，夯实视频应用基础支撑

建设视频监控系统的云化基础设施，支持CPU/GPU等各类计算资源和存储资源的统一调度管理，满足分析资源按需提供、业务服务自动部署的实战应用需求。

构建视频能力开放体系，强化视频处理和分析能力

基于统一的视频云应用支撑平台，把视频图像调阅、解析、大数据检索等应用部署在云端，构建开放、共享、稳定、弹性的系统架构体系，为银行其他应用对于视频图像数据的对接应用提供有力支撑。

搭建“视频云+应用”，创新视频大数据应用模式

在云计算基础设施之上，基于大数据支撑框架下的解析和应用支撑服务，与银行其他技防系统及办公应用协同使用，提高银行信息化工作效率。

