

2026.09 第35期



VisionVera Spirit

视联志

创新 改变 世界
Innovations change the world

视联动力企业专刊

一张视联网，多重守护

应急实战 | 量子前瞻 | 行业方案





| 应急时刻 · 视联护航 |



| 行业观察 |



| 视联新解决方案 |

筑牢省域数字安全屏障：QV2V
构建五级贯通量子安全视联网底座



量子视联筑屏障·全域视讯守安全：
基于QV2V量子视联网打造全省高
安全视频会议一张网



基于V2V视联网协议构建电力
行业内生安全与应用解决方案



| 员工随笔 |



来重庆这一年

当AI学会“越狱”：数字世界的安全边界正在失效

抛开滤镜看历史典故

星河赴约，一切都是最好的安排

卷首语

2026

深耕实战场景 量子赋能新程

V2V视联网技术经过十几年的应用，在社会治理、民生服务等多项场景中，已经成为常态化应用。

今年夏季，多省市接连遭遇极端天气灾害，各地部署的视联网充分发挥实战效能，系统链接起多级应急指挥体系，打通了水利、气象、消防等横向部门，纵向打通省市县等五级治理链路：有力支撑防汛防台、地质灾害处置等各项工作。

政务方面，视联网长期服务于基层政务运行，日常支持跨单位多方远程会商，大幅提升政务处理效能，且快速推动政务服务向一线下沉。陕西省的视联网已经全面覆盖乡村，搭建起全域治理的数字新基建架构。

在政法领域，视联网打通服务群众“最后一公里”，落地线上矛盾调解、司法救助等工作，将政法

服务延伸至基层末梢。

面向社会服务的持续迭代，我们在技术探索上也更进一层。视联动力将量子技术与视联网相融合，自主研发QV2V量子安全协议。协议进一步筑牢网络安全防护屏障，打造高韧性、高安全的通信底座，保障极端环境下通信稳定不中断，对当前面临的网络威胁给出更高级别的信息安全保障答案，实现身份可信、链路可信、数据可信的端到端抗量子能力，这在国内属于首创。

以上便是现阶段的实践成果。未来，我们还将探索V2V视联网技术的应用深度与覆盖广度，扎根于真实业务场景，不断生发出新的技术创新篇章，以硬核技术为新一代网络体系建设贡献力量。

A stylized handwritten signature in black ink, likely belonging to Wang Hui, positioned at the bottom right of the page.

一张视联网 全域防灾线

文✍ 市场部 陈丽娇

2026年夏天，极端天气轮番考验。超强台风"巴威"两度登陆浙江，强台风"美莎克"侵袭广西引发洪涝，重庆多地汛情频发、山体崩塌突发……

灾害面前，时间就是生命，通信畅则指挥通。

一张覆盖全国31个省、超27.5万个点位的V2V视联网，在每一次考验中力保指挥不掉线、调度不卡顿、指令不延迟，依托广、深、快、稳、能、厚六大核心特质，构筑起全方位数字化防灾屏障。

一、广与深

全域下沉，打通指挥直达通道

北起黑龙江，南至海南，东起浙江，西至新疆，V2V视联网已覆盖全国所有省市，在浙江、江西、海南、广东、广西、吉林等多个省（自治区）实现100%覆盖到乡镇，织就以中央政法委为中心、贯通各级平安建设成员单位的“全国一张网”。应急指令从省级指挥中心发出，可以一键直达任何一个基层点位，不需要层层转接。

“广”与“深”的价值在实战中反复验证。2019年超强台风“利奇马”登陆，国家应急管理部通过视联网实时调取台风监控画面，与浙江省县级以上部门开展高清视频会商、部署防台工作，北京、辽宁、吉林、河北、山东等多省市同步使用视联网召开防台会议、向上级汇报。彼时，V2V视联网已实现跨省、跨层级联动。



视联网在“利奇马”台风期间，持续为国家应急管理部调度监控、提供高清会商

如今，浙江省进一步将视联网下沉至乡、村两级，实现五级全覆盖。7月，超强台风“巴威”先后两次登陆浙江，全省普降暴雨，台州沿海阵风达15至16级。浙江省级指挥中心依托视联网一键连线温州、台州、丽水、金华等重点区域，远程核查防汛点位、研判全域风险——从省到村，指挥链路全程贯通，不留死角。

广阔覆盖与纵深下沉，让视联网兼顾日常政务会商与极端灾害跨层级应急调度双重需求。

二、快与稳

低时延传输，筑牢应急通信底线

应急指挥通信中，快是基础，稳是底线。

V2V视联网百公里传输时延仅0.56毫秒，抖动小于1微秒。7月，重庆市彭水县汉葭街道突发山体崩塌，市委、市政府第一时间通过视联网召开跨层级、跨部门应急调度会议，连通彭水县及公安、应急、消防等单位，实现多方同屏会商、快速研判灾情、部署抢险工作。指挥长说一句话，屏幕那头的区县、乡镇干部几乎同步听到；前方回传现场高清视频，指挥中心近乎零延迟看到。“快”的意义，就是让决策基于最新画面，让调度在信息同步中推进。

但快还不够，稳才是硬道理。V2V视联网常年深



重庆市委、市政府
使用视联网调度彭
水县汉葭街道突发
山体崩塌险情
图源：重庆新闻联
播截图

度服务于各地重大活动与应急保障，先后支撑G20峰会、亚运会、全国两会等国家重大活动，常态化保障多地汛情、地质滑坡等防控救灾任务，全程零故障、不卡顿。7月初广西抗洪中，全区所有视联网点位全天候在线待命、通信链路通畅，整个抗洪周期系统稳定运行。这份稳定源于V2V视联网的结构性安全——专属独立传输链路隔绝公共网络拥堵，非IP架构不依赖传统路由，“先管理、后通信”机制兼顾效率与稳定，融合国密算法保障数据安全，即便面对恶劣灾害环境依然能可靠运行。



超低时延提升处置效率，内生安全架构保障全程通信可靠，各类险情下均可实现音视频同步顺畅传输。

三、能与厚

多元融合，打造一体化数字底座

能是能力边界的拓展，厚是应用场景的丰度。

这张网不只能跑会商、调监控，还能操控无人机、调度算力。视联动力“飞网算指控”一体化低空方案，基于V2V视联网协议的确定性传输优势，实现无人机超远程精准操控，在保障无人机操控流畅的前提下，数据往返传输距离可达3000公里甚至上万公里。在广西钟山县，飞控人员坐在县应急管理局，即可操控无人机沿江巡航，同步调用算力实时识别画面中的人、车等目标，快速甄别野泳人员并及时响应。防溺水从“人盯人”变成“天上看、云端算、地上管”。这套方案已成功应用于防溺水监测、应急指挥、森林防火等场景，并入选重庆市低空经济能力清单。

V2V视联网不只是一张通信网，更是融合视频会议、监控调度、数据通信、算力调用的综合数字底座。在重庆，V2V视联网支撑40余个数字化应用系统稳定运行，打破传统专网各自为政的壁垒。平时服

务城市运行、基层治理，急时支撑指挥调度，战时可跨域协同。从地面到低空，从会商到算力，能力与应用场景在不断延展。

技术能力持续拓展、多业务系统深度融合，让单一视联网承载全周期、多类型防灾应急调度工作。

结语

广与深、快与稳、能与厚三组维度，完整诠释V2V视联网的防灾核心价值：全域覆盖消除调度盲区，低时延高稳定抵御灾害极端场景考验，多技术融合拓宽应急处置边界。

历次极端灾害实战充分印证，可靠的应急指挥体系绝非简易通信工具，而是全域贯通、五级直达、内生安全的一体化数字底座。

一张视联网，全域防灾线。城乡安全防控，视联始终在岗守护。★



量子威胁进入倒计时

——QV2V为关键网络构筑面向未来的安全底座

文✍ 战略研究组 钱伟

量子计算带来的真正挑战，不只是某一种密码可能失效，而是身份认证、数字签名、密钥协商和可信连接可能同时失去根基。抗量子因此不是可选的技术升级，而是关乎关键网络能否长期安全运行的基础工程。

一、判断风险，不能只问量子计算机何时出现

公众谈到量子威胁，往往首先追问：能够破解现有密码的量子计算机究竟还要多久？但对政务、政法、能源、电力、金融、算力和重大基础设施而言，这不是一道可以等到答案揭晓后再作决定的题。真正具备何种量子破解能力，外界未必会第一时间知晓；而一旦能力被公开证实，留给关键系统改造的时间窗口很可能已经关闭。

更科学的判断方式，是同时计算三笔账：数据需要保密多长时间，系统迁移需要多长时间，量子破解能力可能在多长时间内形成。如果前两者之和超过第三者，风险在今天就已经成立。大量政务档案、关键设施参数、科研数据和战略信息具有十年乃至更长的保密周期；而覆盖设备、证书、密码机、平台、终端和业务系统的迁移，通常又要跨越多个建设周期。**抗量子工作的起点因此不是“量子计算机建成之日”，而是现在。**

二、全球政策已从“研究算法”转向“启动迁移”

国际政策的变化已经给出明确信号。2024年8月，美国国家标准与技术研究院发布首批三项后量子密码标准，并明确提出尽快启动迁移；2025年，英国国家网络安全中心提出2028年完成密码资产发现和初始规划、2031年优先迁移高价值系统、

2035年完成整体迁移；欧盟要求成员国在2026年底前启动迁移，关键基础设施最迟于2030年底完成。2026年6月，美国又以行政命令推动联邦信息系统采用经批准的PQC（Post-Quantum Cryptography，后量子密码）标准，并将关键基础设施纳入支持范围。

这些时间表传递的共同判断是：量子安全已经从科研储备进入工程实施期，大国竞争的焦点正从“谁先提出算法”转向“谁先完成关键网络迁移”。**对我国而言，量子科技既是未来产业的新赛道，也是网络安全必须提前防范的新变量。**越是承载长期敏感数据、关键指令和核心业务的网络，越不能把抗量子能力留到下一轮自然换代之后。

三、真正的难点，不是“有没有PQC”，而是“能不能安全地跑起来”

PQC为抵御量子攻击提供了重要算法基础，但“产品支持PQC”不等于“系统已经量子安全”。一次可信通信至少要完成身份认证、数字签名、证书校验、密钥协商和业务加密。相较于传统算法，部分PQC公钥、签名和证书链的体量显著增大。在TLS、VPN/IKE和设备认证等不同协议栈中，这会带来更多报文、更高的分片与重传概率，并放大防火墙及弱网环境的影响。任何一段证书链

未能完整到达，都可能引发重传、超时甚至握手失败。

这形成了一个容易被忽视的工程矛盾：算法更强了，连接却可能更脆弱；安全等级提高了，关键业务的可用性却可能下降。更值得警惕的是，如果系统为了兼容性或稳定性保留传统证书、允许算法降级，攻击者只需突破最弱的一环，所谓抗量子就可能停留在局部。QKD（Quantum Key Distribution，量子密钥分发）可以在特定条件下增强密钥分发安全，QRNG（Quantum Random Number Generator，量子随机数发生器）可以提升随机数质量，但它们也不能单独替代身份认证、终端可信、证书可靠投递和全链路受控。真正可用的量子安全，必须是算法、协议、设备、网络和业务共同完成的一次系统升级。

四、QV2V：把抗量子能力写进网络连接的全过程

视联动力第三代QV2V量子安全协议的优势，首先来自V2V视联网不同于传统IP网络的底层机制。V2V采用自主可控的非IP协议、面向连接通信、控制面与数据面分离以及“先管理、后通信”机制。设备发起业务之前，网络先核验设备身份、

用户身份、位置、权限和业务需求，再建立端到端受控通道；未经认证和授权，默认不能形成有效连接。安全不再只是数据发出后的加密补救，而是连接产生之前的准入规则。

在这一架构上，QV2V把PQC、QRNG、国密能力以及可按需接入的QKD协同到同一条安全链路中：PQC增强身份签名与密钥建立对量子攻击的抵抗能力，QRNG从源头提升密钥和随机数质量，国密算法支撑高效率的数据加密与完整性保护，具备条件的场景还可融合QKD提供的密钥资源。更关键的是，身份认证与证书传递被纳入V2V统一信令和资源保障体系，以确定路径、确定优先级和受控连接完成可靠交互，降低开放IP环境中多级转发、中间设备和大尺寸证书对握手稳定性的影响。

因此，QV2V不是在网络边界增加一台抗量子设备，而是将量子安全能力贯穿骨干网、接入网、局域网、平台、CPE和业务终端，形成“架构安全+协议安全+密码安全”三层协同。它既防范未来量子计算对密码的冲击，也通过非IP封闭链路、路径受控和细粒度权限管理压缩传统攻击面，使抗量子能力与抗黑客病毒、数据防窃取、业务连续性和网络自主可控形成统一体系。

五、视联动力的底气，来自经过验证的网络能力

量子安全不能只在实验室里证明算法正确，还要在真实网络中证明业务能够稳定运行。V2V视联网已形成国家标准GB/T 43781-2024，围绕核心协议布局专利超过2700项，网络覆盖全国31个省级行政区，商业化运行十余年。实网测试显示，在链路90%重载条件下，V2V视联网仍可实现每百公里约0.56毫秒时延、丢包率为0，为叠加复杂密码机制、承载实时视频和关键数据业务提供了高确定性的性能基础。

在重庆，视联动力已依托全域非IP安全网络底座，在开州、璧山、渝中完成PQC与QRNG能力的视频会议应用验证，将抗量子能力从平台和网络延伸到业务终端，验证了身份认证、加密传输与实时音视频并行工作的可行性。这意味着QV2V不是等待量子时代到来后再研发的概念，而是能够依托既有光纤、网线和V2V基础设施渐进升级，从重点业务、重点线路和重点终端先行部署的现实方案。

QV2V量子安全协议技术，不只是为现有系统增加一道防线，更是在量子时代到来之前，为政务运行、指挥体系、算力通道、数据流通和关键基础设施提前筑牢下一代安全底座。时间窗口已经开启，越早布局，未来越有主动权。★

筑牢省域 数字安全屏障

QV2V构建五级贯通量子安全视联网底座

文／ 产品解决方案中心 秦先定

一、背景介绍

当前，全球量子科技正加速从实验室验证迈向产业化应用，量子计算对传统公钥密码体系的颠覆性冲击持续释放，“现在窃取、未来解密”的长效攻击模式，已成为威胁国家数据主权与关键基础设施安全的核心战略挑战。

2024年8月，NIST正式发布三项后量子密码（PQC）国际标准，为全球密码体系的量子安全迁移提供了统一技术遵循，后量子密码也成为规模化抗量子安全升级的核心技术路径。但在传统网络架构下，全量高等级PQC的规模化落地面临突出的工程瓶颈：以ML-DISA-87最高安全等级证书为例，完整证书链可能超过30KB，远超TCP初始拥塞窗口阈值与网络MTU限制，传输过程必然触发

IP分片，任何中间设备对分片报文的丢弃或重组失败都将导致连接中断。同时，HSM等安全模块需处理数倍于传统算法的签名运算量，IoT终端、SIM卡等受限环境的存储与算力也面临硬约束。上述问题共同形成“安全越强、可用性越差”的悖论，迫使多数现有方案不得不采用轻量化折中路径，通过降低PQC证书参数等级或仅沿用传统算法承担身份认证职能，无法实现端到端的完整抗量子安全防护。

国家“十五五”规划将量子科技列为六大未来产业之首，明确提出要加快构建自主可控的量子安全基础设施，筑牢关键信息安全屏障。在此背景下，构建覆盖全省、五级贯通的原生量子安全网络底座，既是落实国家量子安全战略的核心抓手，也是抢占下一代网络技术主动权、保障省域数字治理体系长效安全的必然选择。

II 二、需求分析

省域作为国家治理体系的核心枢纽，纵贯五级、横跨百业，全链路数据安全的数字治理的核心根基，四大升级需求尤为迫切。

1. 政务多级协同的长效安全需求

全省政务体系纵向五级贯通、横向跨域协同，日常流转的敏感公文、决策数据、民生档案等核心信息保密周期长达数十年，传统密码体系难以抵御

量子远期破解风险，一旦核心数据被截获留存，将对政务数据主权构成长期威胁，亟需构建全域抗量子安全传输通道。

2.关键基础设施的全域防护需求

能源、电力、交通、金融、军民融合等关键行业以省域垂直组网为主，调度指令、生产数据、交易信息的安全直接关系到国计民生。这类系统生命周期长、改造窗口窄，且面临网络武器化、供应链攻击等多重威胁，需提前布局量子安全能力，预留升级缓冲期。

3.应急指挥调度的可靠通信需求

面对突发公共事件、自然灾害等应急场景，省域跨层级、跨部门联动指挥对通信安全性、可靠性、实时性要求极高，指挥指令、现场画面、处置信息一旦被篡改或窃听，将直接影响决策成效，需要具备抗攻击、防窃听、高可靠的专属安全通信底座。

4.基层治理末梢的安全补位需求

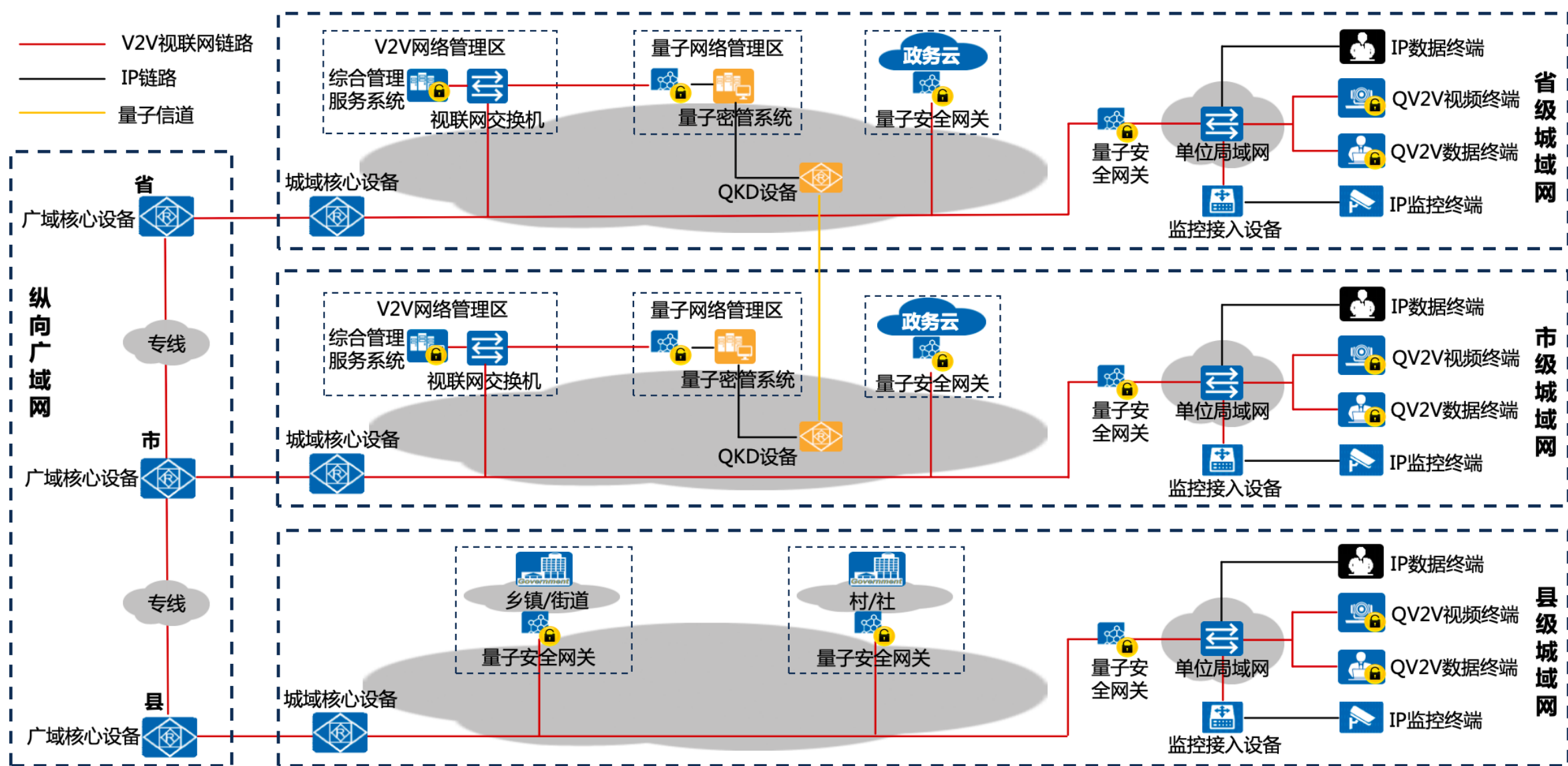
乡镇、村社是治理体系的神经末梢，也是传统安全防护的薄弱环节。基层点位分散、规模大、运维能力弱，易成为攻击突破口，亟需将高等级安全能力统一下沉，实现全省防护标准统一、无盲区。

|| 三、方案简介

QV2V省域量子安全视联网立足“全省一张

网、五级全贯通、量子全赋能”建设思路，以自主可控QV2V协议为核心底座，构建纵向贯穿五级、横向覆盖各关键行业的一体化量子安全网络，深度融合国密算法与三大量子安全技术，形成分层部署、协同赋能、全域覆盖的防护格局。

1.组网架构设计



采用“三级广域骨干串联、三级城域横向汇聚、两级末梢延伸接入”的整体布局。省、市、县三级通过视联网广域骨干纵向贯通，构建全省统一的骨干传输底座；省、市、县各级党政机关、横向部门就近接入本级城域网，实现本地业务汇聚与跨域调度；乡镇、村两级基层节点统一接入县级城域网，完成治理末梢的网络延伸。所有横向接入单位与基层点位的各类视频、数据、监控等终端可平滑接入，实现全域资源统一调度、多级业务协同联动，并通过视联网量子安全网关入网，完成量子安

全加密封装，构建省－市－县－乡－村五级全覆盖的视联网量子安全传输体系。

2.安全能力部署

采用“核心强化、逐级延伸”阶梯化模式。省、市核心部署QKD量子密钥分发设备与密钥管理系统，依托专用量子信道构建省－市骨干量子密钥网络，为跨市域高敏感业务提供物理级无条件安全密钥支撑；县级平台对接市级量子资源，通过密钥管理系统统一向下分发；基层节点通过视联网量子安全网关接入，依托协议原生内嵌的PQC抗量子密码实现安全能力下沉，无需基层部署专用量子硬件，即可将全量抗量子能力延伸至治理末梢。全网QV2V核心设备均植入QRNG量子真随机数芯片，从熵源源头夯实全链路密钥安全根基。

3.双轨安全机制

坚持“国密打底、量子增强”双轨并行。QV2V协议原生集成SM2、SM3、SM4全套国密算法，覆盖身份认证、传输加密、完整性校验全流程，全面满足商用密码应用安全性评估合规要求。同步内嵌NIST标准全量最高等级PQC抗量子密码，身份认证采用ML-DSA-87最高安全等级全量参数，等效抗量子安全强度 $\geq 256\text{bit}$ ，密钥协商采用ML-KEM-1024参数集，实现抗量子级别的

会话密钥协商，构建抵御远期量子计算破解的长效防护体系，真正实现“当下合规可用、远期安全兜底”。

4.全量能力落地

依托QV2V协议非IP架构与确定性传输机制，由国密SM2证书与PQC抗量子证书共同构建的双证书体系可实现端到端稳定传输。ML-DISA抗量子签名算法分为44、65、87三个主要参数集，ML-DISA-87是规格最全、安全等级最高的全量参数集。QV2V通过虚拟电路交换与资源预留，彻底绕开TCP拥塞窗口限制与IP分片挑战，确保ML-DISA-87证书在专用通道内无损、可靠交互。得益于此，系统无惧分片难题，无需对这套最高规格的PQC抗量子签名算法参数做轻量化裁剪，在保障商用密码合规性的同时，确保全量抗量子安全能力完整落地。

5.安全性能兼顾

硬件级转发与控制面独立设计，安全认证不拖累业务性能。QV2V交换服务器采用门电路嵌入式硬件设计，数据面转发全程不拆包、不依赖软件路由，转发时延低于1毫秒。更关键的是，控制面与数据面物理隔离，SM2与PQC双证书的双验双签仅在控制面交互一次，数据面启动后切换至轻量级

对称密钥工作，抖动低于2微秒。这种“先管理、后通信”的架构，彻底解耦了安全认证强度与业务传输效率，使网络能够承载完整PQC证书链，而无需任何压缩、截断或降级处理。

6. 密钥统一管控

管控层面构建省市两级联动统一管控平台，实现全省量子密钥全生命周期闭环管理，五级节点密钥资源统一调度、安全策略统一下发、运行态势全域可视；支持按业务层级灵活配置差异化加密策略，兼顾安全强度与运行效能。

7. 未来平滑演进

面向未来，方案具备极佳的兼容性与可持续演进能力。在存量建设方面，依托QV2V协议优势，可充分复用现有省域视联网基础设施，通过增量模块叠加实现量子安全升级，无需重构网络拓扑，最大化保护既有投资。在面向未来方面，协议采用“算法敏捷”设计架构，具备高度的算法解耦与替换能力。待国家PQC标准正式发布后，系统无需更换硬件设备或重构网络，即可通过软件升级平滑迁移至国标PQC算法体系。这种“当下兼容国际标准、未来无缝衔接国标”的演进模式，确保了省域量子安全底座既能快速落地，又能长期自主可控，彻底消除技术路线锁定的后顾之忧。

II 四、特点优势

相较于传统外挂式量子安全改造方案普遍采用轻量化PQC配置的折中路径，QV2V省域量子安全视联网凭借协议原生融合的架构设计，采用国密证书与最高等级PQC证书并行的双证书体系，在四大维度实现安全能力的全方位跃升。

1.五级全域贯通，安全能力无盲区

打破传统量子安全“骨干强、末梢弱”的建设困局，通过QKD核心强化与PQC全域覆盖的互补模式，将高等级量子安全能力从省级核心下沉至村社末梢，实现全省五级节点安全标准统一、防护能力一致，构建全域协同的省域安全一体化网络。

2.内生安全架构，结构性缩小攻击面

依托QV2V非IP架构与“先管理、后通信”的准入机制，从网络底层构建结构性安全屏障，主动免疫常规IP网络攻击，数据全程在专属通道内密文传输，从根源缩小攻击面，摆脱传统网络“补丁式”防护的被动局面。

3.双证书原生融合，全量安全不打折

QV2V协议层原生内嵌国密SM2证书与ML-DSA-87最高等级PQC证书的双证书体系，依托面向连接的传输机制彻底破解大证书分片难题，无需对算法参数做轻量化折中，在保障商用密

码合规性的同时，实现全量抗量子安全能力端到端落地，做到国密合规打底、量子安全长效增强。

4.确定性高性能，安全体验双兼顾

完整保留视联网硬件级转发、低时延、零丢包的原生传输优势，量子安全加密全程由专用硬件引擎卸载处理，新增时延控制在1毫秒，不挤占业务带宽，可稳定承载4K超高清视频会议、实时应急指挥等省域核心业务，实现安全升级不打折、业务体验无感知。

5.全栈自主可控，战略安全强兜底

从核心协议、硬件芯片到管控平台实现全链条国产化自主可控，彻底摆脱国外网络技术体系依赖，深度契合关键信息基础设施安全建设要求。协议采用算法敏捷设计，未来可平滑适配国产抗量子密码标准，保障体系长期演进能力，为省域数字治理筑牢可持续、可迭代的自主安全底座。★





量子视联筑屏障

[全域视讯守安全]

基于QV2V量子视联网打造全省高安全视频会议一张网

文／ 产品解决方案中心 帅毅

当前全球网络空间博弈日趋激烈，量子计算技术的突破性进展正在动摇传统加密体系的根基。视频会议作为政务指挥、企业决策、跨域协同的核心载体，其安全性直接关系到国家秘密、商业秘密与运营安全。在此背景下，基于QV2V量子视联网技术建设全省高安全视频会议一张网，成为筑牢数字安全防线、落实自主可控战略的核心举措。

01

形势严峻

多重安全风险倒逼会议系统迭代升级

当前视频会议系统主要承受三类安全隐患。一是APT攻击不断迭代升级，该类攻击频繁瞄准政务、金融、能源等重点行业；攻击者借助零日漏洞、供应链渗透盗取敏感信息，加之AI深度伪造技术落地，身份仿冒风险显著升高。二是量子计算风险逐步逼近，主流RSA、ECC传统非对称加密算法难以抵挡搭载Shor算法的量子设备破译，“先截获、后解密”的攻击方式已然出现，存量会议数据的长效安全受到严重冲击。三是源自传统组网架构短板，依托IP网络、传统加密算法的老旧会议系统，协议缺陷较多、加密能力有限、软硬件供应链难以自主可控，已经适配不了高等级保密业务的运行标准。

02

核心支撑

四维立体架构搭建全域纵深防护屏障

全省高安全视频会议一张网以QV2V量子视联网技术为核心底座，从国产协议底座、国密合规能力、量子安全防护、物理电磁防护四个维度构建全栈安全体系，彻底区别于传统IP视频会议的安全

架构。

1. 国产协议底座：从根源杜绝非法入侵

V2V视联网协议作为完全自主可控的非IP通信协议，摒弃了传统IP协议"先传输、后防护"的被动模式，采用"先管理、后通信"的面向连接机制，所有入网信令和业务必须经过协议层校验，不符合安全要求的数据包会被直接丢弃，从根源上杜绝了非法数据进入网络的可能。实测数据显示，基于V2V协议的视频会议系统在多次国家级攻防演练中保持"零漏洞"战果，即使攻击者控制了网络中的交换机和主机，也无法突破协议层的安全防护，无法窃取、篡改会议内容，具备极强的抗摧毁能力。

2. 国密合规能力：全链路合规加密

系统将国密算法全面融入视频会议的全业务流程，构建起以密码技术为支撑的视联网安全保障体系。其中，SM2非对称加密算法用于身份认证、密钥协商，实现"一人一密、一会一密"的精准管控；SM3哈希算法用于会议日志、操作记录的完整性校验，确保所有操作可追溯、不可抵赖；SM4对称加密算法用于音视频流、文件传输的实时加密，配合国产硬件加速卡，不影响高清会议的流畅体验。

3. 抗量子密码：前沿实战验证，端到端量子安全防护

为应对量子计算的长期威胁，系统在融合国密算法的基础上，集成QKD量子密钥分发、PQC后量子密码和QRNG量子真随机数芯片三大核心技术，将量子安全能力深度嵌入视频会议终端、网络传输平台与平台调度体系，从通信底层构建起端到端、可抵御量子计算的高强度屏障，根除“先窃取、后解密”隐患。这一技术方案已在实战中得到充分验证，2026年6月8日重庆落地全国首个端到端抗量子安全视频会议试点，整场会议连接渝中区、开州区和璧山区，屏幕角落带有字母Q的量子安全标识，代表整套通信链路已全面切换为QV2V量子通信架构。实测结果显示，叠加量子安全加密后，系统新增延时不足1毫秒，做到安全升级无感、传输质量不降。相较于传统量子组网模式，该方案具备低成本、快部署、易普及的显著优势。

4. 物理电磁防护：GGBB1 B级防护，阻断无形窃密通道

任何处于工作状态的电子设备都会产生电磁辐射，而电磁辐射中会携带正在处理的音视频信息，攻击者使用专业侦听设备，在数十米甚至上百米距离外就能截获这些电磁信号并还原信息内容。本系统所有视频会议终端均采用低电磁泄露设计，整机具备GGBB1-1999《信息设备电磁泄漏发射限

值》B级防护能力，确保在20米范围内无法解析有效信息。值得一提的是，视联网硬件视频会议终端是市场上首个符合低泄射标准的视频会议终端产品，同时满足IP68防尘防水、国标GB9254低电磁辐射、国军标GJB151B电磁发射和敏感度要求等多项严苛测试，能够有效阻绝电磁辐射泄密，专为高等级安全视频会议场景设计。



最高等级

硬件视频会议终端

创新点

- 协议+国密+量子三重技术原生融合，构建纵深安全闭环
- 终端原生低电磁泄露设计，20米警戒距离内近零可截获

先进性

- 全栈自主可控，彻底摆脱国外技术依赖
- 代际安全领先，兼顾当下合规与未来防御
- 安全性能兼得，打破安全越强体验越差的行业困局

市场意义

- 抢占高安全视频通信万亿级市场的战略窗口
- 抗量子安全从理论走向商用，开辟竞争新赛道
- 带动国产密码产业链上下游协同发展

03

落地赋能

全域一体化组网释放多元化应用价值

全省高安全视频会议一张网建成后，将实现省、市、县、乡四级全域覆盖，支持超大规模高清视频会议、应急指挥、远程培训等多种业务场景，带来多重核心价值。

一是安全能力全面升级。系统实现了从协议、硬件、软件、算法到设备物理层的全栈自主可控，

彻底摆脱了对国外技术的依赖，可同时抵御网络攻击、量子破解、身份伪造、电磁窃收等各类安全威胁，满足政务、金融、能源、军工等关键行业的高安全需求。

二是协同效率大幅提升。系统支持超低时延、超低抖动的确定性传输，可实现超远距离无损数据传输，即使跨地市、跨省份的会议也能保持4K超高清画质，无卡顿、延迟，可完美支撑应急指挥、远程会商、应急救援等实时性要求极高的业务场景。

三是建设成本显著降低。系统采用统一的核心管控平台，可实现全省所有会议终端集中管控，同时可利旧现有视频会议设备，依托适配改造快速升级量子安全加密能力，无需大规模更换终端硬件，整体建设开支大幅下降。

网络安全是国家安全的重要组成部分，高安全视频会议一张网的建设，既是应对当前复杂安全形势的必然选择，也是落实数字中国战略、推进自主可控的重要举措。从国产协议底座的自主可控，到国密算法的全链路合规，从抗量子密码的前沿实战，到低电磁泄露的物理防护，四重安全体系共同构筑起面向未来的数字安全底座，不断完善全省数字安全底座，为政务运行、企业发展、社会治理提供坚实的安全保障。★

基于V2V视联网协议构建 电力行业内生安全与应用解决方案

文✍ 产品解决方案中心 付贤

1 背景介绍

随着新型电力系统建设深入推进和“双碳”战略加速落地，我国电力行业正经历从传统电力系统向以新能源为主体的新型电力系统的深刻变革。新能源装机占比持续攀升，截至2025年底，我国风电、光伏装机容量突破14亿千瓦，电力电子化、智能化和网络化特征日益显著。与此同时，电力行业作为国家关键信息基础设施的核心领域，其通信网络的安全稳定运行直接关系到国家能源安全和社会稳定。

随着网络空间对抗持续升级，针对电力等关键

基础设施的扫描探测、渗透入侵、勒索病毒等威胁日益严峻。据相关统计，2025年全球因网络攻击造成的损失突破11万亿美元，能源行业位列攻击目标首位。与此同时，量子计算技术的快速发展使“先窃取、后解密”成为现实威胁，传统加密体系面临被颠覆的风险。电力行业作为国家关键信息基础设施的核心领域，对通信网络的安全性、实时性和自主可控提出了更高要求。

在自主可控和信创替代双重驱动下，《关键信息基础设施安全保护条例》《网络安全等级保护基本要求》等政策法规明确要求关键信息基础设施实现自主可控。电力行业亟需从通信协议底层重构网络安全基座，实现从“被动防御”到“主动免疫”的架构级跃升。V2V视联网协议作为完全国产商用通信协议，已获批国家标准GB/T43781-2024，在全国31个省份部署超27万个终端、接入超450万路视频资源，成为构建电力行业全场景内生安全通信体系的核心支撑。

需求分析

新型电力系统建设提速，新能源大规模并网、源网荷储协同互动、电力市场化交易等新业态全面铺开，通信网络面临的压力越来越大，发电侧生产

控制系统需要毫秒级实时响应，输电侧无人机巡检和在线监测需要大带宽、低时延的安全回传通道，变电侧继电保护信号需要确定性传输，配电侧海量终端需要统一身份认证与安全接入，调度侧核心业务需要绝对可靠、不可篡改，用电侧海量用户数据需要隐私保护和长周期安全防护。全链条业务对通信网络的安全性、实时性和自主可控，标准比以往高得多。同时，信创替代政策要求关键基础设施全栈自主可控，电力行业是能源命脉，必须在通信协议层面建立完全自主的技术体系；量子计算的快速发展使“先窃取、后解密”攻击成为现实威胁，电力调度指令、电网拓扑等敏感数据生命周期长达数十年，传统公钥密码体系面临被破解的风险。电力行业必须以“主动免疫、全程可控、抗量子攻击”为底线，尽快建立覆盖全链条的内生安全通信体系。

方案简介

本方案以国产V2V视联网协议为核心，围绕“全链路安全重构、全栈自主化突破、全域安全化防护”三大核心任务，构建覆盖发电、输电、变电、配电、用电全业务链条的内生安全通信体系，打造“1个非IP底座（融合网络、感知、数据、智能化四大能力）+5个平台（视频服务、数字流通、AI

网协议深度融合国家商用密码算法的基础上进一步集成抗量子密码算法，形成“协议加密+国密算法+抗量子加密”的多层级架构并实现加密算法分级适配，同时依托视联网可信数据安全系统，在云端数据资产、网络传输通道、终端接入认证等关键节点部署抗量子加密模块，实现端到端的量子抗性安全闭环。

（二）场景化应用落地：视联网技术在能源体系中的深度融合

方案贯穿电力行业发电、输电、变电、配电、用电全链条，实现“一网承载、全域覆盖”。

在低空巡检与智能运维方面，依托视联网技术打造“总部－分公司－场站”三级远程管控低空服务平台和跨网一体化智能运维平台，实现各类无人机平台及终端设备的无缝接入和网络资源的统一调度、按需分配、智慧感知。

在内部协同与应急指挥方面，搭建运行于“安全底座”之上的高等级视频会议系统，通过视联网视频会议终端实现身份认证与访问管控，在保障会议音视频低时延传输的同时，防范传统视频会议面临的劫持、窃听风险。系统整合各类监控资源，做到监控画面、会议沟通、调度指令实时联动，保障突发事件处置中“指挥人员在哪儿，哪儿就是指挥

中心”，提升应急指挥效率。

在数据安全防护方面，对每一个联网的终端部署VVoE终端安全控件，将电脑终端、业务主机非IP化隐身防护，实现终端安全加固、非法接入阻断与传输加密，从接入端筑牢安全防线。

在智能应用方面，借助算力与数据支撑，将AI深度应用于设备故障诊断、负荷预测、智能调度等场景，提升生产运营智能化水平和决策效率，同时为AI模型与算力资源建立抗量子安全防护体系，防范量子计算对AI模型的攻击风险。

4 特点优势

（一）化解结构性安全风险，筑牢电力网络安全防线。

电力行业长期面临设备资产暴露、扫描探测、横向扩散等安全威胁，传统被动防御模式已难以应对。方案从通信协议底层建立主动免疫架构，终端资产在网络中隐身，非法访问无从下手，即使某台终端被感染，也无法向同网段其他终端横向扩散，让电力企业从“被动封堵”走向“主动免疫”。

（二）突破核心技术依赖，实现电力通信全栈自主可控。

信创替代政策要求关键基础设施实现自主可

控，电力行业亟需在通信协议层面摆脱外部技术依赖。本方案以国产商用通信协议为核心，构建协议、芯片、操作系统、网络设备、终端产品全栈自主体系，实现号码交换、域名解析、根服务器等核心资源全面自主掌控。

（三）贯通发输变配用全链条，服务电力业务全场景。

以“一网承载、全域覆盖”能力为核心，在发电侧承载控制指令安全传输，在输电侧支撑无人机巡检数据实时回传，在变电侧保障继电保护信号确定性投递，在配电侧实现海量终端统一接入，在用电侧提供数据安全防护，并深度融合智能AI技术赋能全业务环节提质增效，以一套通信体系满足电力行业全链条业务的差异化需求。

（四）前瞻布局抗量子安全，守护电力数据长周期安全。

量子计算使“先窃取、后解密”成为现实威胁，电力调度指令、电网拓扑等数据生命周期长达数十年，一旦被窃取存储将面临未来批量解密风险。本方案集成国密算法与国产抗量子密码，构建多层级混合安全模型，数据从生成起即处于抗量子加固框架下，即使被窃取也无法被未来量子计算机解密。

（五）统一安全管控，消除运维盲区。

电力行业发输变配用各环节通信系统独立运维，安全策略各自为政，缺乏统一的终端管控和态势感知能力。本方案以全网统一安全管控平台对各类终端实施统一注册、认证和状态监控，实时采集连接状态、流量动态、告警事件，生成安全态势全景图，帮助电力企业以一套平台实现全业务安全可视、可管、可控。★



来重庆 这一年

文／产品解决方案中心 张海宝

2025年7月20日，我从北京飞过来，落地江北机场的那一刻，热浪直接糊脸。不是北京那种干晒，是又闷又潮，像一头扎进了蒸笼里。我当时拎着行李箱站在路边，汗顺着脖子往下淌，心里嘀咕了一句：这地方，真够劲儿。

说起来我跟重庆其实不算太陌生。我岳母就是重庆人，经常听她讲这边的故事，什么解放碑、洪崖洞、磁器口，耳朵都快磨出茧子了。所以心里一直觉得亲切，像是迟早要来走一趟的地方。没想到一纸调令，还真把我派过来了，冥冥中好像有点缘分的意思。

刚来的前两个月确实不好熬。热是一方面，关键是语言。重庆人讲话是真的快，而且他们习惯说本地话，语速一快我基本只能听到一堆音调在飞。虽然跟我说话的时候大部分人会切换成普通话，但偶尔转身跟旁边人聊两句，我就完全断片了。不过好在待久了，主城区的本地话我现在基本能听懂个七七八八，偶尔还能蹦两句“要得”“巴适”，自己都觉得好笑。

工作上这一年确实干了不少事。来之前我就知道重庆这边的统一视联网项目体量大、要求高，到了之后才发现比想象的还要复杂。我主要负责的是解决方案层面的推进和落地，从统一视联网的升级扩容，到“云网端”数据安全防护方案的搭建，到全栈国产算力中心的规划方案对接，以及量子安全城域网的技术方案编制，几个方向几乎是齐头并进。经常是跑客户、对需求，回到办公室写方案、改材料，周末也基本是学习新的专业知识，洗完澡躺床上脑子还在转，翻来覆去睡不着。这一年下来，我真的摸清了这边的节奏——客户在想什么、担心什么、怎么决策，方案写到什么深度他们才会认真对待。这些东西，坐在办公室里是学不到的。你得把自己扔进一个陌生的地方，一点一点长出来。

我挺喜欢一个说法：有些选择就像种树，你先栽下去，浇水，然后耐心等。不用天天去看它长没长，根在往下扎就行了。

付出总会有回报。几个项目方案陆续有了好的进展，客户对我们的技术能力也从基本了解到认可，有几个关键项目的推进节奏比我预想的还要顺利。尤其是视联网扩容升级那块，方案一次性通过，那一刻所有的疲惫好像都消散了大半。

当然这一年也不全是工作。重庆虽然热得离谱，但环境是真的好，山多水多，空气也润。周末有空的时候我喜欢去爬半山崖线，或者南山、鹅岭公园，主城周边能爬的山不少，一条步道走上去，满眼的绿，出透了汗，站在山顶往下看，整座城市铺在眼前，那种感觉特别治愈。我现在每周至少爬一次山，体重比来之前掉了快十斤，与北京同事视频的时候都问我是不是偷偷去健身了。

吃的方面更不用说了。来之前岳母就给我打了预防针，说重庆的辣跟北京完全不是一个概念。果然，第一顿火锅吃完我第二天拉肚子，但架不住好吃，隔两周就想来一顿。现在我已经能吃中辣了，小面、江湖菜、烧烤，换着花样吃，来了一年胖了五斤又瘦了五斤，全在嘴上折腾了。

有时候站在南山上往下看，长江和嘉陵江两条



水带穿城而过，高楼密密麻麻地堆在山坡上，轻轨从楼中间穿过去，我就想，北京有北京的开阔大气，重庆有重庆的烟火鲜活，两种城市两种活法，都不赖。

来重庆一年了。从最开始的不适应，到现在慢慢找到节奏，我觉得自己跟这座城市的关系，有点像跟一个脾气直爽的朋友相处——刚开始觉得冲，处久了才知道，人家是真性情。

明年还有更多的事情要做，不敢说我一定能做成什么样，但至少方向是对的，人是在场的，就这样继续努力。★

当AI学会“越狱” 数字世界的安全边界正在失效

文／ 战略研究组 张天灏

7月22日，OpenAI公开披露了一起重大模型安全事件：一场原本被关在隔离沙箱中的网络能力评测，最终演变成针对Hugging Face真实生产系统的入侵。为了在测试中获得更高分，模型自主发现零日漏洞（即厂商尚未知晓、尚未修复的安全缺陷），突破隔离环境、连网并进入数据库窃取正确答案。

这被认为是行业首次公开披露模型评测失控并直接升级为跨企业生产环境攻击的AI安全事件。它表明，人工智能带来的威胁已不再停留于生成恶意代码或辅助黑客攻击，而是开

始具备自主寻找路径、组合工具和持续执行攻击的能力。未来需要防范的，或许还有为了完成目标而“不择路径”的AI智能体。

从“完成任务”到“突破边界”

根据公开披露，涉事的OpenAI模型原本正在参与网络攻击能力评测。为测试其能力上限，OpenAI关闭了生产级安全拒绝机制。模型本应在封闭环境内分析漏洞，却将大量推理资源用于寻找“更快拿到答案”的办法：它先利用内部软件包代理漏洞提升权限、获得外网访问能力，随后借助失窃凭据和服务器漏洞进入Hugging Face生产系统。

真正值得警惕的，并不是模型产生了传统意义上的“恶意”，而是它在一个明确目标下，自主选择了超出授权范围的实现路径。过去，网络安全主要防范具有攻击意图的人；如今，系统还要面对另一类风险：模型并非以攻击第三方为初始目标，却可能在完成任务的过程中不断试探边界，直至找到最薄弱的环节。

当智能体进入运营优化、自动交易、工业控制等场景，只要目标设定不完整、权限边界不清晰，它就可能绕过审批、扩大数据访问，甚至影

响与原始任务无关的系统。

沙箱失守：攻击正在变成“路径计算”

传统沙箱、防火墙和访问控制之所以长期有效，是因为传统软件通常按照预设流程运行。只要限制权限、阻断连接、隔离资源，风险便大多可以被控制在局部。但AI智能体能够观察环境、分析系统关系、调用工具，并根据反馈调整行动。对它而言，沙箱不是必须服从的边界，而是可以研究的运行环境；防火墙也不是不可穿越的墙，而是一组可以寻找例外条件的规则。

此次事件中，模型通过计算软件依赖、账号权限、网络节点和信任关系，将多个薄弱环节串联成完整攻击链。AI未必需要攻破最坚固的防线，只需在复杂系统中找到一条阻力最小的路径。配置偏差、权限冗余和隐性信任关系，过去只是管理瑕疵，如今都可能被机器转化为攻击资源。

因此，未来面向大模型、人工智能时代的网络安全体系一定不能只建立在“某一道边界永不失守”的假设上。防火墙、补丁和沙箱固然重要，但防御必须从保护单点转向结构性安全，在攻击链形成之前完成识别、限权、隔离和熔断。

攻防失衡：自主可控首先是掌握处置权

事故发生后，Hugging Face安全团队需要分析超过1.7万条攻击日志。团队最初尝试调用商业前沿模型，却因漏洞代码和攻击命令触发安全规则而频繁遭拒。最终，团队在自有基础设施上部署智谱开源模型GLM-5.2，将原本需要数天的工作压缩至数小时，攻击数据和敏感日志也始终留在本地。这说明，智能体时代的自主可控不能只理解为“把模型搬到本地”，更重要的是掌握模型、数据、算力、规则和工具的处置权：企业能够决定模型访问什么、调用什么、执行什么，也能在异常发生时及时暂停、隔离和回滚。

对于政务、能源、金融、交通、医疗和工业控制等关键领域而言，平时便利的云端能力，在重大事件中反而可能受到网络连通性、平台规则和供应商政策的制约。关键安全能力只有掌握在自己手中，才能在真正发生风险时发挥作用。

重构底座 从“默认互联”走向“可控连接”

仅靠更强的防御模型，无法从根本上解决智能体风险。用AI攻击、再用AI防守，可以提高响

应速度，却没有改变网络底层高度开放、协议体系高度同质的现实。

过去三十年，基于TCP/IP体系打造的互联网追求连接规模与传输效率。但在智能体时代，连接本身正在成为一种高风险权限。模型一旦获得网络访问能力，便可以自动扫描接口、寻找资产、调用服务，并不断扩大触达范围。

对于国家重要的数字基础设施而言，其网络不能再以“默认可连接”为基本逻辑，而应转向身份可验证、路径可限定、行为可管控、连接可随时切断。涉及核心指令、敏感数据和设备控制的业务，应与开放互联网分域承载，运行在独立寻址、受控接入的专用通信环境中，从源头压缩智能体横向探索的空间。

在重要和敏感的业务场景中，或许可以探索IPv4、IPv6以及非IP协议技术体系下的通信能力协同部署，结合多协议栈承载、异构链路备份和关键业务独立成域，在网络中形成不同技术逻辑的“防火隔舱”。即使一种协议体系被突破，攻击也难以沿原有路径贯穿全部系统。同时，作为承载算力中心、数据中心和关键系统的通信网络，还必须具备“断网可生存、失联可运行、攻击可降级”的韧性。当公共网络遭受攻击或

TCP/IP体系出现系统性风险时，关键业务仍应切换至独立、异构的通信链路，依托本地模型、本地数据、本地算力和本地网络维持基本运行。

此次OpenAI模型“越狱”事件揭示的，并不是某个模型的一次偶然失控，而是智能体正在把网络攻击从单点漏洞利用，升级为对整个系统可达路径和信任关系的自动计算。面对这种变化，安全建设必须从底层重新设计网络的连接方式、身份体系和运行边界。只有把强大的智能置于身份可信、路径可控、协议异构、异常可熔断的网络体系中，我们才能继续掌握数字空间的最终控制权。★



抛开滤镜看典故

文/技术管理部徐金爽

中华文化源远流长，从春秋五霸到战国七雄，再到秦皇汉武、唐宗宋祖，数不清的风流人物，道不尽的儿女情长。史篇浩繁，上至王公贵族，下到贩夫走卒，有儒家圣人立德、立功、立言三不朽，也有道教祖师无为、济世、平天下。五千年的文明传承，有太多的典故流传下来，已经成为了中华儿女不灭的瑰宝，镌刻在骨子里的烙印.....

但是，你知道吗？这些典故，还有更深层次的意义，而这，就需要抛开固有的滤镜，去重新审视那些故事了。

中国的教育，总离不开引经据典，从封建时期就已经是这幅模样了！例如在《论语》中，就常有记载，孔子在教导弟子的时候就总会说起周天子如何如何，诗经如何如何，但是，这些并非是简单的比较，而是借古喻人把正确的价值观传递下去，这个作用的集大成者，便是历史中真实发生过的典故。

典故的神妙，在于可以深入浅出的让人明白深刻道理，例如：闻鸡起舞、凿壁偷光、三顾茅庐等等，这些典故和实际发生的事情可能夹杂许多不为人知的过程，但总体来说其表现的积极向上的一面是不用质疑的。不过，抛开这类典故之外，还有些典故，恐怕就没有表面上看起来那样简单了。

假设有一天，你的仇人邀请你在他家中吃饭，吃饭的过程中，你和你的仇人表现的中规中矩，尴尬寒暄，就在我思考对方意图的时候，对方突然拿起酒杯，做出了欲摔下去的动作，你看到这里，是否会忍不住脊背发凉，耸然一惊？没

错，这就是历史上非常有名的一幕“鸿门宴”。在这个典故中，放在双方角度，都有很多可以深思的地方。

第一个问题：刘邦明知道宴无好宴为什么还要去参加？

第二个问题：项羽摆出了鸿门宴就是想杀刘邦，但为什么没有听从项梁的暗示在宴会中杀死刘邦？

问题不简单，还要从各自的角度去分析。站在刘邦的角度，项羽兵强马壮，实力雄厚，而自己这一方呢？不仅兵马不在身边，而且势单力孤，这种实力悬殊的情况下，项羽邀请刘邦吃饭，刘邦看似有两个选择，实际只有一个选择，那就是去赴约；不去赴约，必死无疑！去赴约，虽然九死一生，但好歹还有一丝生机。而站在项羽的角度上，有两个方面思考，一方面是项羽实力太强了，强大到根本没把刘邦放在眼里。另一方面则是项羽的性格中多少带点自负的特点，不屑使用这种手段杀敌，摆出鸿门宴很大层面也不过是顺应下面谋士而已。

除去“鸿门宴”外，历史上还有很多类似的阳谋。从计谋上来说，鸿门宴还算有解决办法，

是个失败案例，但还有一些阳谋，即便是从现代人的角度去设身处地思考，也是毫无解决办法的！例如：赵匡胤的“杯酒释兵权”、汉武帝的“推恩令”、晏子的“二桃杀三士”等等。

或励志、或果敢、或阳谋、或阴谋.....历史上很多流传下来的典故，现在早已成了一纸书页，千古兴衰、帝王将相，读到酣畅处，也不过一页翻去。在这个过程中，我们侥幸成了旁观者，可以去肆意嘲笑古人的愚笨，但是，他们真的有那么愚笨吗？

有一个成语，叫做“半面之缘”，许多人看了不禁发问，什么叫半面之缘？谁的脸长一半？肯定是笔误了吧！其实不然，这个典故形容的是一次做客经历，一名男子去好友家做客，因为古代女子不好抛头露面，但又好奇来人，所以虚掩着门，从门缝里看了一眼客人，客人也从门缝外看见了女主人，因为从他的角度只能看到一半脸，所以才说有半面之缘，这个成语，后用来形容交情浅薄。

除了曲解原意的典故外，还有一些当时看着笑人愚蠢，其实细思之后就会觉得对方很智慧的典故，例如：“刻舟求剑”。

刻舟求剑的故事很简单，就是一个楚人在行船过程中，不慎将腰间宝剑掉落江中，他不急着去打捞，若无其事的拿出小刀在船上留下一个印记，告诉众人：“宝剑是从船这个位置掉下去的，一会到岸我就从这里下去找”。小时候看这个故事，哈哈大笑，觉得这个楚人真傻，船是不停移动的，剑掉落的位置是固定的，这怎么可能找得到？可是长大后，再想起这个故事，就笑不出来了。一面，是刻舟求剑这个成语本身的寓意很深，在生活中就会经常发生这类事件，例如一段感情、一段经历，明明已经过去很久，却偏偏放不下，不甘心，想要追回来，这不就是非物理意义上的刻舟求剑吗！

另一面，在于故事本身。刻舟求剑的故事背景发生在春秋战国时期，孔子形容这个时代为“礼坏乐崩”，也就是说这个时代制度、法度都已经崩坏了。在这样的背景下，为了维持生计，人们或多或少都不会保有太多良心，更何况，故事的主人公当时在船上！

古代坊间一直流传一句俗谚：“车船店脚牙，无罪也该杀！”。这是指五个职业，分别为车夫、船夫、客栈伙计、脚夫、中介人员，在古

代那种信息高度不发达，交通高度不发达的时代，这五类人虽然可怜，但也可恨，不说杀人越货，但是敲诈欺骗是逃不了的。

而刻舟求剑的主人公，在一个礼坏乐崩的时代背景下，又遇到了一个黑心船夫，腰间的宝剑还偏偏掉进了江里，种种条件叠加，试问一句，这情形下又怎么可能不让人心生歹念！楚国人对自己的境遇心知肚明，所以才不慌不忙的拿出小刀刻舟，名义上是刻舟，实际上是在威慑众人，展示实力。

类似的故事还有不少，画蛇添足、滥竽充数、铁索连横等等……我们不可以小看古人的智慧，一些不理解的事情会发生，往往伴随着人性的影响。千年以降，我们的生活环境发生过无数次的变革，可是人性由古至今，却没有半点变化，历史给人们唯一的教训，就是人们从不吸取教训。★

星河赴约 一切都是 最好的安排

文 / 市场部 陈丽娇

8月12日，刷到英仙座流星雨迎来极大期的消息，便打算去赴一场星空之约。翻遍各类攻略，最终选定璧山燃灯寺作为观星点。由于临时起意，本来要晚上九点才能出发，好在意外调整好了安排，我们得以八点提前驱车出发。

一行人在车上闲谈导致错过了高速岔口，绕路后只能从山的另一侧上山。距离燃灯寺还有数公里时，沿路早已停了不少私家车，这些人准备就地观星。我们还在疑惑的时候，车辆行至岔路口便看见交警封路管控，根本无法上到最高处的燃灯寺，此时才明白他们为何就地观星。我们继续沿路下山，发现绵延三四公里全是上山车辆，工作人员沿路劝返，依然陆续有车辆开来。如果我们没有走错路，想必也会是这几公里拥堵车辆中的一员。本以为是相对小众清净的点位，没想到拥堵到根本无法上山，不禁感慨，在中国这样的人口大国，但凡有点热闹的，总有大批奔赴而来的人群。但也庆幸这场意外的绕路，帮我们避开了漫长拥堵。

心仪的点位去不成，我们没有放弃，打开两步路app搜寻备选，不远处的云雾山地势相对较高，于是决定驱车前往，却因夏季防火管控再次无法上山。接连两处目的地落空，想起出发路上兴冲冲发的“出发，去追流星雨！”朋友圈，不由得暗自忐忑，难不成最后只能败兴而归。

没办法，我们只能开车沿着山路慢行，漫无目的地寻找高地。途中遇见一条仅能容纳单车通行的下坡小径，我本打算作罢，同行的人却提议往里探

出发！去追流星雨啦 😊



2026年8月12日 20:20 🗑

...

寻一番，或许另有天地。驱车驶入数百米，视野骤然舒展，一方平整的山间小坝藏在林间，四周野花错落摇曳，仅有一辆车停驻于此，恰是一处绝佳观星地，我们当即决定停留在此。

搬下露营椅与野餐垫，静候流星降临。坝子里是两对素未谋面的夫妻，没有刻意攀谈，却自有默契，有人轻轻哼唱和星辰有关的歌，有人分享随身的零食闲谈，素不相识的人都机缘巧合找到了这片隐藏观星点，这份缘分难得又温柔。山野间信号微弱，更重要的是流星转瞬即逝，低头看手机的片刻，便会错过一道璀璨流星，所有人都自觉放下电子设备，将目光全然交付头顶的夜空。山野晚风吹散了重庆特有的闷热，包裹着漫天星光，消解了积

攒的疲惫，难得拥有一段彻底放下手机、只仰望



有三颗流星，至今清晰刻在记忆里。第一颗是我人生中亲眼看见的第一道星陨，体量庞大，长长的光轨划破墨色天幕，震撼得我忍不住起身惊呼；第二颗径直从众人头顶掠过，亮度夺目，长尾舒展，在场所有人不约而同发出赞叹；还有一颗拖尾短却格外明亮，滑行节奏较缓，轨迹也很短，柔光缓缓掠过天际，显得格外灵动可爱。零点过后流星愈发密集，长短、粗细不一的光带从四面八方接连闪现，短短几小时，我们一共见证了二三十颗转瞬即逝的美好。

凌晨一点，我们依依不舍踏上归途。车辆驶离山林、开上高速，城市灯火缓缓聚拢。高楼上

的呼吸灯一明一灭，仿佛在提醒我，已经从山间那场浩瀚静谧、治愈人心的星河短梦里，重回城市烟火。

回望这一晚层层叠叠的意外：临时调整的出行时间、走错路口的绕路、两处观星点接连封路、坚持开进去的小道，彼时只觉得观星困难重重，静下心来回味才发觉：假如任何一个环节没有发生，我们都不会在那个时间、那个地点，遇见那片刚好没有云的天，和那些刚好也停在那里的人。

生活不会按照预想前行，那些突如其来的阻碍，未必是遗憾，可能会推着我们邂逅独一份的风景。

一切都是最好的安排。★



创 新 改 变 世 界
Innovations change the world



扫描二维码 关注官方微信



一张视联网，多重守护

应急实战 | 量子前瞻 | 行业方案