泛在电力物联网
全场景安全防护思路

刘 冬 梅

国家电网有限公司信息通信分公司

01 定义与内涵

02 风险与挑战
03 防护思路探讨
04 合作与展望

泛在电力物联网的定义

信息发展要解决的是“沟通”问题

互联网　人与人的沟通　  　物与物的沟通　物联网

泛在物联：指任何时间、任何地点、任何物之间的信息连接和交互

泛在电力物联网，就是围绕电力系统各环节，充分应用移动互联、人工智能等现代信息技术、先进通信技术，实现电力系统各个环节万物互联、人机交互，具有状态全面感知、信息高效处理、应用便捷灵活特征的智慧服务系统。

泛在电力物联网将是“**全国最大的物联网**”，把所有与“**电**”相关的物全部连接起来，将助力国家互联网与物联网的建设与融合，驱动新一轮的互联网经济

泛在电力物联网的内涵

泛在电力物联网就是运用新一代信息通信技术，将电力用户及其设备、电网企业及其设备、发电企业及其设备、电工装备企业及其设备连接起来，通过信息广泛交互和充分共享，以数字化管理大幅提高能源生产、能源消费和相关领域安全、质量和效益效率水平。

从架构上看

泛在电力物联网包含感知层、网络层、平台层、应用层四层结构，感知层主要解决数据的采集问题，网络层主要解决数据的传输问题，平台层主要解决数据的管理问题，应用层主要解决数据的价值创造问题。

从技术上看

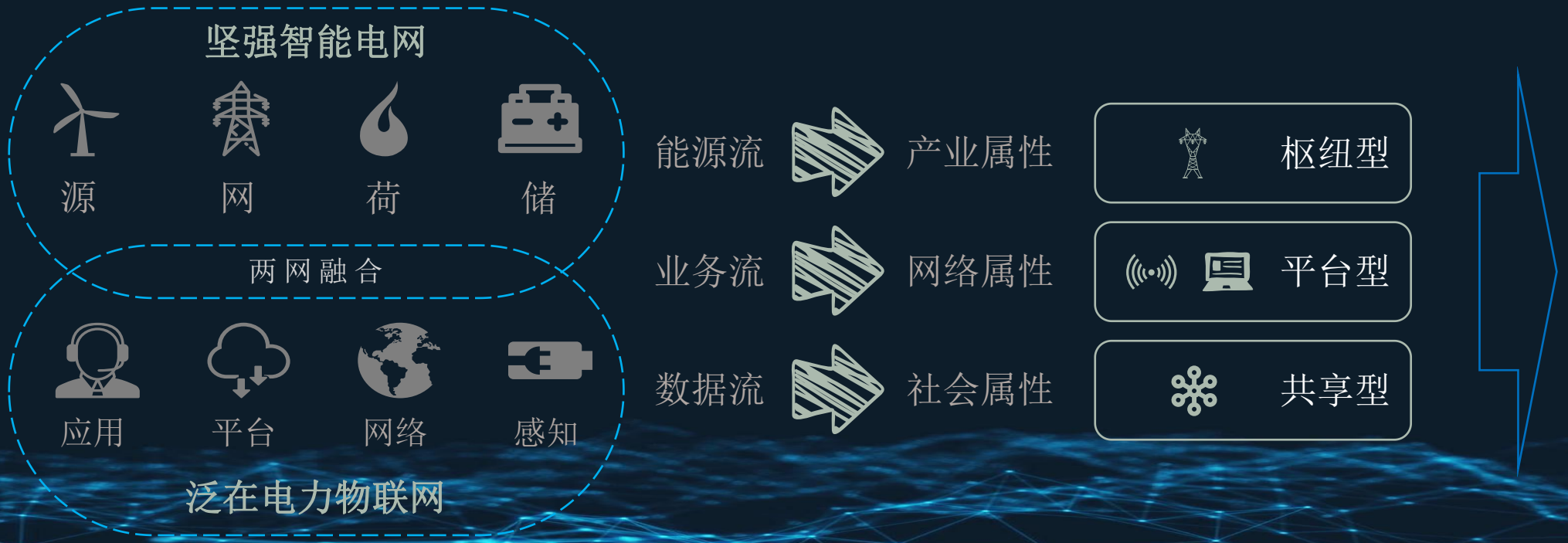
泛在电力物联网广泛应用大数据、云计算、物联网、移动互联、人工智能、区块链、边缘计算等信息技术和智能技术，属于工业互联网的范畴，是数据革命在能源电力领域迅猛发展的必然产物。

从作用上看

泛在电力物联网就是通过汇集各方面资源，为规划建设、生产运行、经营管理、综合服务、新业务新模式发展、企业生态环境构建等方面，提供充足有效的信息和技术支撑。

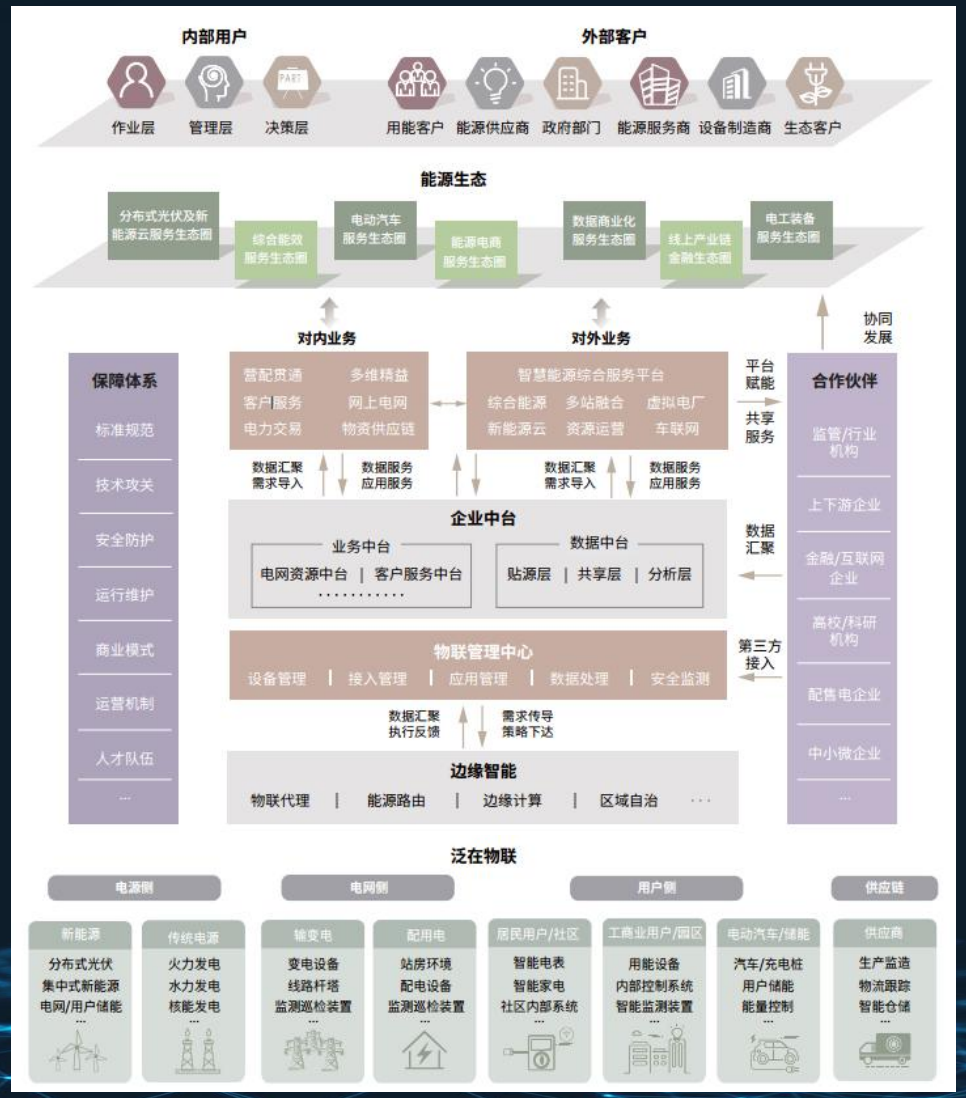
泛在电力物联网的内涵

坚强智能电网与泛在电力物联网是建设世界一流能源互联网企业的重要物质基础。**从与坚强智能电网的关系看**，坚强智能电网和泛在电力物联网，二者相辅相成、融合发展，形成强大的价值创造平台，共同构成能源流、业务流、数据流“多流合一”的能源互联网。



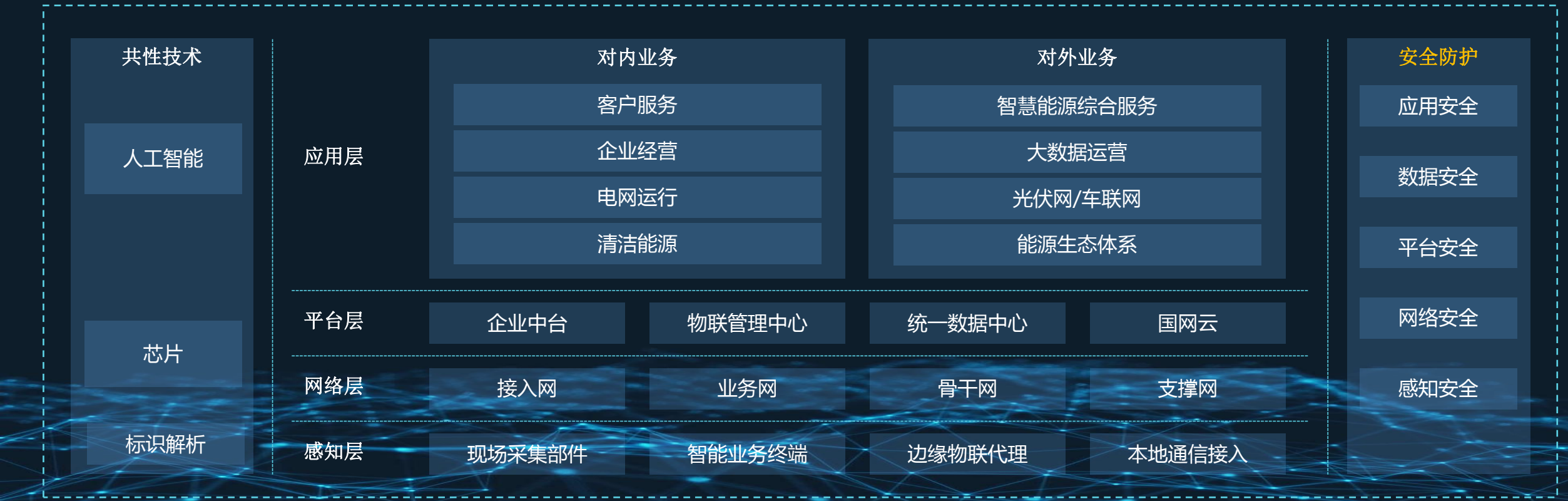
泛在电力物联网建设目标

通过泛在电力物联网建设，充分应用“大云物移智链”等现代信息技术、先进通信技术，实现电力系统各个环节万物互联、人机交互，大力提升数据自动采集、自动获取、灵活应用能力，对内实现**“数据一个源、电网一张图、业务一条线”**，对外**广泛连接内外部、上下游资源和需求**，打造能源互联网生态圈，适应社会形态、打造行业生态、培育新兴业态，支撑“三型两网”世界一流能源互联网企业建设。



泛在电力物联网体系结构

泛在电力物联网通过构建感知层、 网络层、平台层、应用层、安全防护五大体系，打造全息感知、泛在连接、开放共享、融合创新的体系架构，形成适应社会形态的新兴业态和应用模式。感知层实现泛在互联；网络层实现全时空覆盖；平台层实现开放共享；应用层驱动业务创新；安全防护保障可信互联、安全互动。



02 风险与挑战

01 定义与内涵
03 防护思路探讨
04 合作与展望

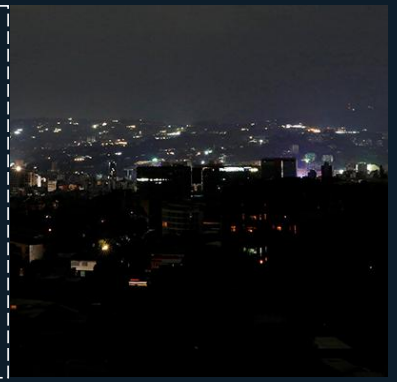
面临的风险

- 网络安全形势日益严峻，网络攻击的破坏性和威胁性持续增加，电力关键信息基础设施已成为网络打击破坏的首要攻击目标。

2019年

3月7日

委内瑞拉 古里水电站发生故障，引发全国大面积停电，包括首都加拉加斯在内的18个州遭遇停电，故障时间持续长达7天。3月25日~31日，委内瑞拉国内再次发生多起大规模停电事故；4月10日，停电事故又继续上演。此次停电事故持续时间长且多次反复，存在网络攻击等恶意破坏的可能性较大。



2019年

7月13日

美国纽约当地时间2019年7月13日傍晚6时47分，纽约曼哈顿中城与上西区发生大规模停电，曼哈顿中心地带的时代广场、地铁站、电影院、百老汇等大片区域陷入黑暗，最严重时大约有73000用户受到影响。

2019年

6月15日

《纽约时报》援引美国现任和前任安全事务官员的话称，**美国正在加大对俄罗斯电网的网络攻击，**“至少从2012年开始，美国已将侦查探测器植入俄罗斯电网的控制系统。”俄罗斯发出警告，**俄方已向美国插入恶意代码**，未来在与美国的任何冲突中，可以破坏美国的发电厂、石油和天然气管道或供水设施等。

2019年

10月30日

印度核能有限公司发表声明承认库丹库拉姆核电站与互联网连接的用户主机**感染APT组织的恶意软件Dtrack**，但生产控制网因与管理网物理隔离暂未被侵入。该恶意软件可用于监视受害者和窃取数据，支持远程访问木马，通常用于侦察和其他恶意软件有效载荷的投递器。

面临的挑战

- 网络安全边界 **泛在性和异构性** 特征日趋明显。随着智能电网和泛在电力物联网的建设，网络安全边界快速扩大，网络构成日益多样，安全管控愈加复杂。

- 感知层是泛在电力物联网的信息源，**泛终端将成为最薄弱的环节**。泛终端普遍暴漏在外，容易被恶意破坏、扫描、追踪和定位，甚至被伪造、劫持或窃取。

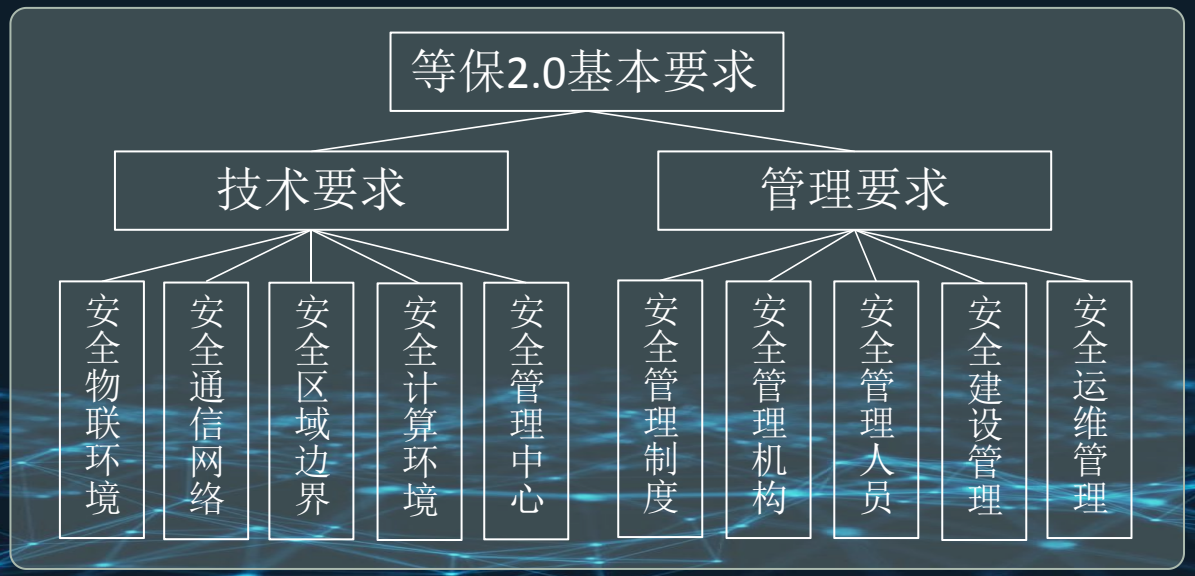
- 数据安全 **内涵和外延进一步拓展**，面临数据繁多复杂、分布面广、利用价值高、采集点多、共享发布渠道多等安全风险。

- 泛在物联网应用层将充分利用“大云物移智链”信息技术，使得与互联网密切相连的开放应用成为突破口，**新兴业态**对传统防护体系提出了新的挑战。

政策形势

国家高度重视网络安全，相继颁布了一系列的政策和法规，为我国网络空间安全保障体系提供了重要支撑，也是企业必须遵循的准绳。等保2.0明确将云计算、移动互联、物联网、工控系统等与泛在电力物联网密切相关的内容均列入了标准范围，强调“一个中心三重防御”的防护架构要求；电力系统广泛使用密码作为信息加密和保护的手段，密码法的实行将从法律层面规范了密码的管理和使用。

网络安全等级保护制度2.0



《中华人民共和国密码法》

《中华人民共和国密码法》经十三届全国人大常委会第十四次会议表决通过，自2020年1月1日起正式施行，标志着我国在密码的应用和管理等方面有了专门性的法律保障。

《中华人民共和国密码法》围绕“怎么用密码、谁来管密码、怎么管密码”，重点规范了5方面44条内容。强调“坚持党对密码工作的领导”，规定“中央密码工作领导机构对全国密码工作实行统一领导”。

03 防护思路探讨

01 定义与内涵
02 风险与挑战
04 合作与展望

全场景安全防护体系

结合泛在电力物联网的发展形势和安全需求，全场景安全防护体系的总体安全防护策略是“全景可视感知、全域可信可控、全息智慧防御、全时敏捷响应”（以下简称“四全”策略）。“四全”策略可分别拟化为全场景安全防护体系的“神经系统”、“四肢”、“躯干”及“大脑”。依赖“四全”策略，全场景安全防护体系被赋予生命力，得以灵活、智能、高效地运作，从而全方位联动泛在电力物联网感知层、网络层、平台层及应用层安全能力，支撑公司“三型两网、世界一流”企业建设高速发展。

- 全场景网络安全防护体系优化设计
- 态势感知深化应用
- 密码基础设施建设
- 推进数据安全管理
- 专用边界安全防护设备研制应用
- “国网芯”安全芯片试点应用
- 网络安全仿真验证环境建设
- 全场景网络安全防护试点验证
- 面向泛在电力物联网的信息系统运行体系研究与实践
- 电力监控系统泛在电力物联网安全试点建设

总部要求 + 业务实际

四全防护策略

- 全景可视感知
- 全域可信可控
- 全息智慧防御
- 全时敏捷响应

全景可视感知

应有之义：

可视感知是网络安全实时风险的预防、发现、消控的“神经系统”，能够强力赋能泛在电力物联网的网络安全分析监控工作。对下全面感知“云、网、边、端”的安全态势，对上高效支撑安全专业人员开展网络攻防对抗。其中，全面感知是基本前提，集中可视是必然要求。可视感知要横向到边覆盖“外部攻击、内部窃取”的全部场景，纵向到底深入到网络、边界、主机、应用、数据的全部防线。准确识别威胁，智能应对隐患，确保网络安全风险可控、能控、在控。

欲成之效：

推动公司网络安全从实时监控向态势感知的演进，向下拓展感知层、网络层的安全数据接入，向上对接平台层、应用层的安全监测和防护需求，重点适配物联网、移动终端、国网云、全业务数据中心的网络安全高效管控。

全域可信可控

应有之义：

网络安全全域可信可控是全场景安全防护体系的“四肢”，负责全面感知泛在电力物联网的安全风险，为网络层、平台层、应用层提供终端可信、准入可控的基础服务。对下在全域范围内获取各物联网节点的安全基础数据，实现业务线全覆盖。对上链接各终端安全防护组件，形成全域可信可控的泛终端安全感知体系。

欲成之效：

制定统一标准提高泛在电力物联网终端产品本体安全性；利用海量异构终端自动发现识别、准入保护及威胁建模分析等技术，构架基于数据可信、接入可控、动态赋能赋权的泛终端安全监测与防御系统。

全息智慧防御

应有之义：

网络安全全息智慧防御是全场景安全防护体系的“躯干”，它贯穿于泛在电力物联网感知层、网络层、平台层及应用层全要素、全节点、全业务，从“按需强化内网防护、从严规范边界隔离、着力完善安全监测”三个层面推进网络安全防护工作，并按照“发展与安全”并重原则，同步进行新型网络架构配套安全能力建设，通过网络传输与融合安全、云安全、数据安全、应用安全为泛在电力物联网提供基础性全方位防御能力。

欲成之效：

强化网络传输与融合安全、云安全、数据安全及应用安全，打造贯穿泛在电力物联网感知层、网络层、平台层及应用层全要素、全节点、全业务的安全防御体系。

全时敏捷响应

应有之义：

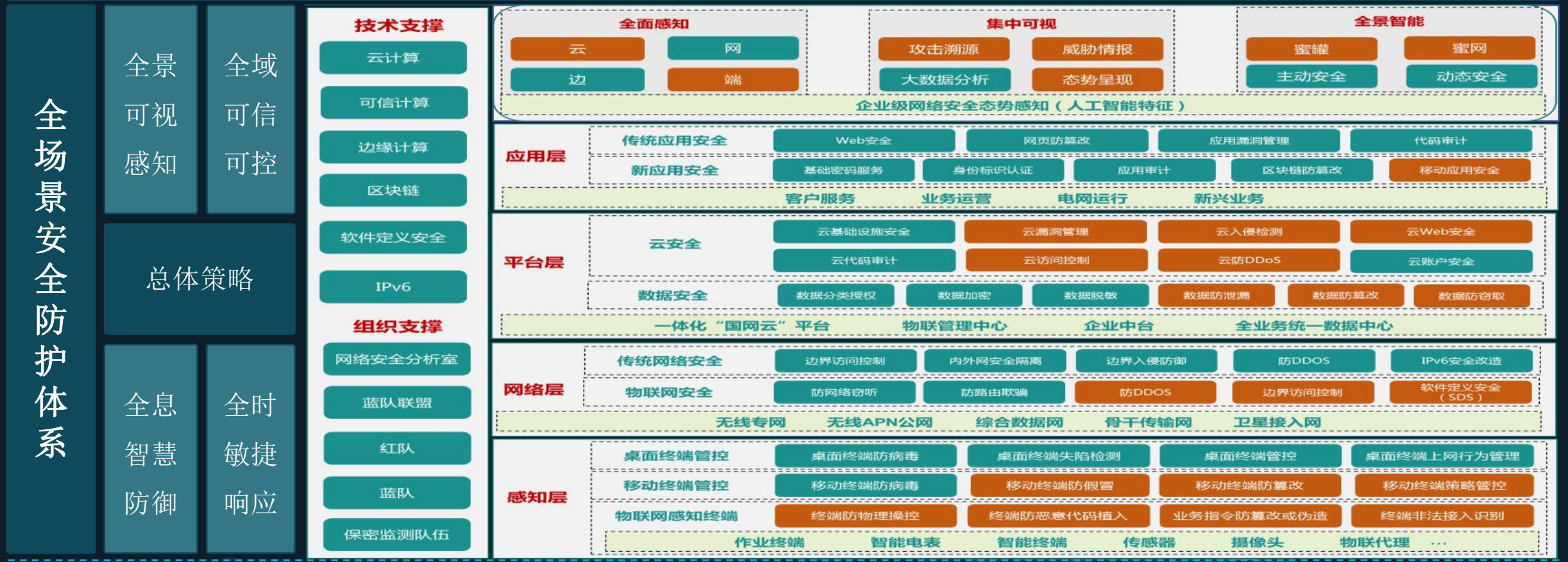
网络安全全时敏捷响应是全场景安全防护体系的“大脑”，能够统筹各方资源、组织各方力量对安全威胁迅速做出响应。实现网络安全全时敏捷响应，建立安全指挥机构是核心，打造智能化监控平台是重点，建设人才队伍是根本。应形成机构之间密切配合、信息共享、统一监控、联动处置的协同“作战”体系，推动监控工作从自动化向智能化的转变，提高安全事件响应速度，并培养具备实战能力的物联网安全人才。

欲成之效：

建设总部和省公司的两级网络安全监控中心，统一指挥协调全网资源，开展全网统一监控预警和联动处置，为公司生产运行与经营管理提供网络安全坚强保障。

全场景安全防护整体架构

围绕“四全”防护策略，提出了全场景安全防护体系整体设计架构



- 根据泛在电力物联网感知层、网络层、平台层及应用层自身特性，**分析各层安全需求，强化配套安全防护措施**。
- 重点**建设全景可视感知**，从**全面感知、集中可视、全景智能**三个层次全方位掌握全网安全风险状况，提升一体化全景化的监控监视监盘能力

全场景安全防护创新实践

“两个”创新实践

① 全网网络安全态势感知：深化现有网络安全态势感知平台，对接“国网云”等平台层和“邮件安全”等应用层的安全监控和防护，拓展接入终端 和网络全流量的安全数据接入，全方位掌握云、网、边、端各层安全风险，实现全面感知、集中可视、全景智能。

② 全网网络安全联动中枢：在总部指导下，以全场景态势实时感知为核心能力，健全总部和省级（直属单位）的两级协同联动工作机制，高效协同公司各单位开展重大网络安全事件的应急处置，共筑安全防线，在国家级重大保障活动中发挥联动中枢的作用。

安全管理中心

安全计算环境 | 安全区域边界 | 安全网络通讯

”等保2.0强调“一个中心三重防御

创新实践1：全网网络安全态势感知

通过全网网络安全态势感知平台，实现多维度、全场景整体安全风险态势的展现

全网安全态势

整体情况+重大安全事件+关键指标

攻击态势

网络攻击+溯源分析取证

关键业务态势

外网邮件态势+其他关键应用

安全布防态势

拦截状态+策略管理+影响诊断

终端安全态势

用户画像+异常行为分析+失陷分析

风险管控

漏洞管理+脆弱性分析

创新实践1：全网网络安全态势感知

安全态

“态”为状态，“势”为趋势。将安全防御思维模式从“应急响应”切换到“**持续监控和分析**”。可视化呈现不同安全监控场景下的安全状态和攻防趋势。构建集预测、防御、检测和响应于一体的自适应安全防护，提示异常流量、攻击路径、安全威胁、安全事件等信息。

运行态

安防体系有效性的基础是安全设备的可靠稳定运行，“安全与业务”并非是不可调和的矛盾双方。可视化呈现公司**网络安全布防图**，所有安全设备部署位置、运行状态、与业务耦合关系等都清晰可见。提示安防体系可用性和有效性，快速进行故障定位及隐患消缺。

开关量

传统网络安全事件告警均为“状态量”，有效告警被淹没在大量信息中且过度依赖于人的经验。将网络安全的告警**从“状态量”转变为“开关量”**，将专家经验转化为自动化检测规则，将模糊的告警判定转化为“0”和“1“的事件观察，缩短响应时间，实现”**快速止血**“。

全寿命

安全管控需要协调部门多，处置时间长，管控难度大。可视化呈现**全寿命周期的漏洞管控**工作，将管理制度转化为自动化管控工具，减少安全运维中的人力成本和沟通成本，依托于管控工具使不同角色的人员高效协作，使督办和统计自动化、进度和结果可视化。

创新实践1：全网网络安全态势感知

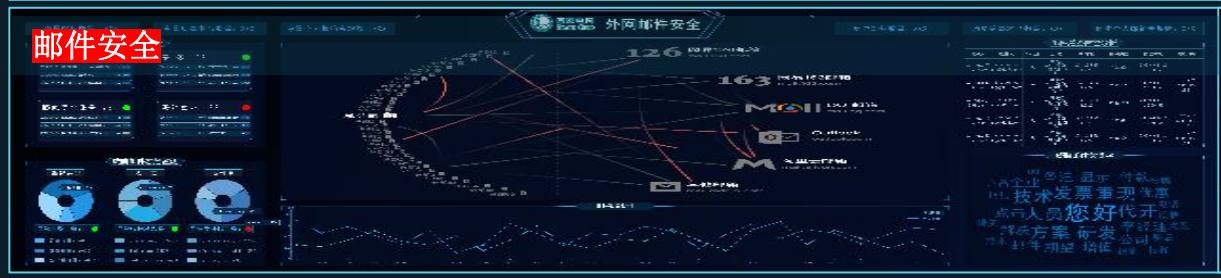
外网攻击态

内网攻击态

安全风险管控

全景网络安全

邮件安全



安全设备布防监控

全网安全态势

创新实践1：全网网络安全态势感知

防护设备相关联，多源数据相融合

增强安全防护设备运行数据、安全监控设备告警数据等多源数据的深度融合，通过将安全态与运行态相结合的“多态”监控方式，推动安全和生产共生。

威胁情报多收集，安全关口向前移

针对多源威胁情报，实现统一存储、检索、对比，并使用统一的生命周期来管理情报产生、使用、静默与消亡的完整过程。

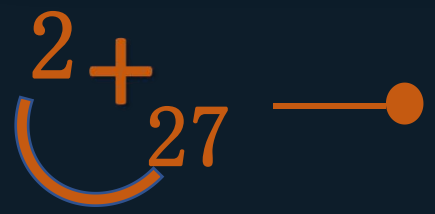
攻击场景可溯源，高危风险秒处置

通过对威胁数据进行基于大数据的关联挖掘识别攻击者，利用机器学习技术进一步判别攻击手法，反向定位黑客，进行攻击溯源分析。

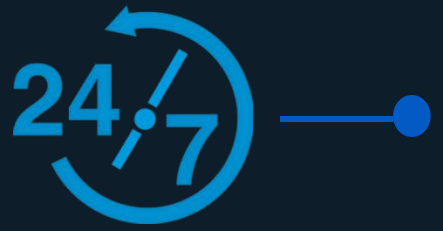
创新实践2：全网网络安全联动中枢

建设总部和省（直属单位）两级网络安全监控中心，实现全网统一监控和总体协调指挥，通过两级联动的网络安全指挥体系，组织协调全网资源，开展全网安全监控、重大预警通报和应急联动处置，发挥全网共防共治的作用，达到“一点预警、处处响应”的效果。

创新实践2：全网网络安全联动中枢



国网信通公司建立“网络安全分析监控中心”，联研院建立“网络安全技术分析中心”，27家省公司已建立分析室，形成**2+27**两级联动工作全覆盖。



国网信通公司网络安全分析监控中心按照**7*24**小时的运方行式开展网络安全保障。

编制《国家电网有限公司网络安全分析室工作周报》**22期**；全网风险预警通知和公告**21项**；共享攻击源情报**49期**；共享网络安全情报**61项**；共享网络安全事件**51起**。

联动排查内网恶意程序感染情况，发现公司多单位存在终端感染，均及时完成排查清理，有效防范信息内网终端失陷被控的安全风险。

创新实践建设成绩

- 国网公司青创赛银奖
- 信息通信运维创新优秀成果
- 泛在电力物联网建设2019年最佳实践案例
- 工业和信息化部网络安全技术应用试点示范项目
- 电力企业信息安全管理创新成果一等奖、二等奖
- 国家电网有限公司网络安全红蓝队建设优秀成果

04 合作与展望

01 定义与内涵
02 风险与挑战
03 防护思路探讨

下一步工作方向

泛终端的广泛应用导致暴露点大幅增加，终端本身的脆弱性为安全管控带来巨大挑战；云平台的部署上线改变了传统的服务体系架构，需要将现有防护体系平滑演进和升级；5G时代的来临和工业互联网的应用，使得网络攻击往往会造成比过去更严重的影响；边缘计算可能增加潜在攻击面，网络节点的信任基础受到挑战……

合作与展望


T H A N K Y O U


T H A N K Y O U


T H A N K Y O U


T H A N K Y O U