5G网络运营安全管理系统研究与实践

Research and Practice of 5G Network Operation Security Management System

任若冰/Ren Ruobing[1]，费明/Fei Ming[1]，贾国祖/Jia Guozu[1]，许晨敏/Xu Chenmin[2]，郝振武/Hao Zhenwu[3]
（1. 中国移动通信集团广东有限公司，中国 广州 510623；
2. 北京兴云数科技术有限公司，中国 北京 100176；
3. 中兴通讯股份有限公司，中国 深圳 518057）
(1. China Mobile Group Guangdong Co., Ltd., Guangzhou 510623, China;
2. Beijing Xingyun Digital Technology Co., Ltd., Beijing 100176, China;
3. ZTE Corporation, Shenzhen 518057, China)

DOI：10.12142/ZTETJ.202602012
网络出版地址：https://link.cnki.net/urlid/34.1228.TN.20240926.1042.002
网络出版日期：2024-09-26
收稿日期：2024-06-25

摘要：基于内生安全理念，提出并构建了一个面向5G网络的安全中心，设计并实现了一套5G网络运营安全管理系统。该系统解决了5G安全数据采集的关键问题，能够为5G专网运营提供一套具备智能闭环处置能力的安全运营管理体系。应用结果表明，该系统有效提升了5G网络安全防护效能，保障了5G行业应用与网络基础设施的安全，为5G行业应用的安全落地提供了坚实的技术支撑。

关键词：内生安全；5G网络安全中心；5G安全信息与事件管理（SIEM）；主机安全

Abstract: Based on the concept of endogenous security, a 5G network security center is proposed and constructed, and a security management system for 5G network operation is designed and implemented. This system addresses the key issue of 5G security data collection and provides an intelligent closed-loop disposal mechanism for secure operation management of 5G private networks. Practical application shows that the system effectively enhances the security protection capability of 5G networks, safeguards both 5G industry applications and network infrastructure, and provides solid technical support for the secure deployment of 5G industry applications.

Keywords: endogenous security; 5G network security center; 5G Security Information and Event Management (SIEM); host security

引用格式：任若冰，费明，贾国祖，等. 5G网络运营安全管理系统研究与实践 [J]. 中兴通讯技术，2026，32(2)：81-90. DOI：10.12142/ZTETJ.202602012
Citation：Ren R B, Fei M, Jia G Z, et al. Research and practice of 5G network operation security management system [J]. ZTE technology journal, 2026, 32(2): 81-90. DOI: 10.12142/ZTETJ.202602012

5G将增强移动宽带、高可靠低时延、低功耗大连接三大应用场景作为其核心需求，其泛在的终端接入能力、面向多样化业务的强大承载能力、差异化的安全隔离能力，能够为各类垂直行业客户打造定制化的虚拟专网，满足电力、交通、工业、能源等客户对通信网络的差异化诉求，从而持续不断地推动行业创新业务及商用模式的快速发展。但是，在垂直行业网络中引入5G，打破了企业传统的相对封闭、可信的网络环境，加剧了网络安全风险。

因此，5G在行业的规模化应用，必须按需为5G网络提供安全能力，保证工业互联网、车联网、物联网等网络安全。同时，需要充分灵活地应用5G基础设施以及围绕5G网络的创新所带来的新技术与新能力，使5G网络与垂直行业的安全充分受益。中国移动作为5G网络运营商，必须落实5G网络安全防护职责，研究5G网络运营安全管理策略，打造5G网络运营安全管理体系，建设满足监管要求的安全可靠5G网络。

1 5G网络运营安全挑战

随着5G的规模商用及在垂直行业中的普及，行业应用将吸引更多恶意攻击，诸如电力、交通、工业制造、能源、金融等关键领域的高价值资产将成为首要攻击目标，并可能给国家、社会和企业带来严重的风险。

垂直行业5G专网引入了5G网络切片、网络功能虚拟化（NFV）、多接入边缘计算（MEC）等新技术，在支持智能网络服务定制的同时，也打破了传统企业网络相对封闭可信的环境[1]，引入了新的责任主体，导致信任模型、网络基础设

施及网络边界复杂化。当前，5G网络运营安全面临如下挑战：

挑战1：为大力推动5G行业应用的普及与落地，需落实具备统一管理策略与有效监控手段的5G网络运营安全管理系统，形成一套目标明确、过程规范、多方协同、可复制推广、智能化、自动化的安全运营管理体系，打消各行业客户在使用5G专网产品时的安全顾虑，减少5G推广过程中由新技术、新模式所造成的安全阻力。

挑战2：在5G专网安全运营阶段，明确安全责任边界和识别各环节存在的安全风险至关重要，通过采取有效的安全防护措施确保5G网络稳定运行和资产安全。

挑战3：5G网络安全运营的基础是安全数据采集。全面地采集与分析5G网络安全相关的数据，对于发现和预防网络攻击、提高网络安全性与稳定性具有重要意义。

2 5G网络运营安全管理策略研究

为建设一个安全的5G网络，应对5G引入后带来的安全威胁，必须以中国相关安全政策、标准、规范为指导原则，以纵深防御思想为核心，采用先进设计理念与专业安全设备，形成完善的综合网络安全防护体系，避免来自各种目的的攻击、干扰和非法访问问题，全面满足网络安全等级保护需求及网络安全管理战略目标。

本文基于广东移动5G垂直行业业务场景，结合5G专网运营模式展开研究，提出5G网络运营安全管理总体策略，具体包括：

1）一体化的安全运营体系与管理策略。结合广东移动态势感知平台的能力与规划，提出可融入广东移动5G网络安全运营体系的安全建设方案及安全管理策略。基于三层模式构建一体化5G网络运营安全管理系统，通过大中小三层安全闭环，实现资产管理、脆弱性分析、威胁分析、合规检测等功能。从网络与系统的视角对5G网络中各类资产进行统一安全管理，避免多个系统各自孤立的情况。该系统既能满足广东移动安全管理的需要，也能满足5G网络和行业客户的安全需求。

2）专业的5G网络安全防护策略。开展5G网络安全风险与需求分析，明确安全责任边界，将5G专网划分为不同区域，在不同区域之间实现网络隔离与边界安全防护，并建立安全传输通道，同时通过在关键节点部署安全设备，提高专网网络韧性，从网元接入、边界防护、安全隔离、数据传输、MEC安全等方面开展安全防护策略研究。

3）全面的5G网络安全数据采集与预处理策略。全面采集5G网络安全数据，支持采集5G网络中的5G网元、安全设备、安全系统的资产数据、系统状态、流量数据、日志数据、安全数据等，支持多种协议接口，实现对数据的采集、预处理、分层建模与汇聚，同时具备向上级态势感知平台转发功能，通过算法模型将分析后的数据进行关联分析和汇聚呈现，提高数据共享效率与安全事件响应效率，打造安全合规的5G网络。

2.1 5G网络运营安全管理体系与方案研究

为了解决5G网络缺乏有效安全防护手段、5G安全运营缺乏有效监控手段这两大痛点，本文中我们开展了基于5G网络运营安全管理总体策略的研究，与广东移动安全管理与技术体系相结合，与已建设运营的态势感知平台、大网流量监测等手段相结合，研发5G基础网络设施和5G应用安全防护方案，并在电力、政务等安全要求高的行业专网，开展试点验证，增强5G专网防护水平[2]。同时，在广东移动现有5G网管平台、统一采集平台、态势感知平台的基础上，构建5G网络运营安全管理体系[3]，建设5G网络运营安全管理系统，实现5G专网安全数据采集与威胁检测，实现专网安全“可见可管可控”，如图1所示。

与传统信息技术（IT）网络的态势感知平台不同，5G网络因为虚拟化、网络切片、MEC等新技术，具有云化、非云化等资产的特点。5G网络运营安全管理系统需要深入分析和研究5G网络场景下带来的网络安全风险，梳理和明确省级态势感知平台需要采集的数据。

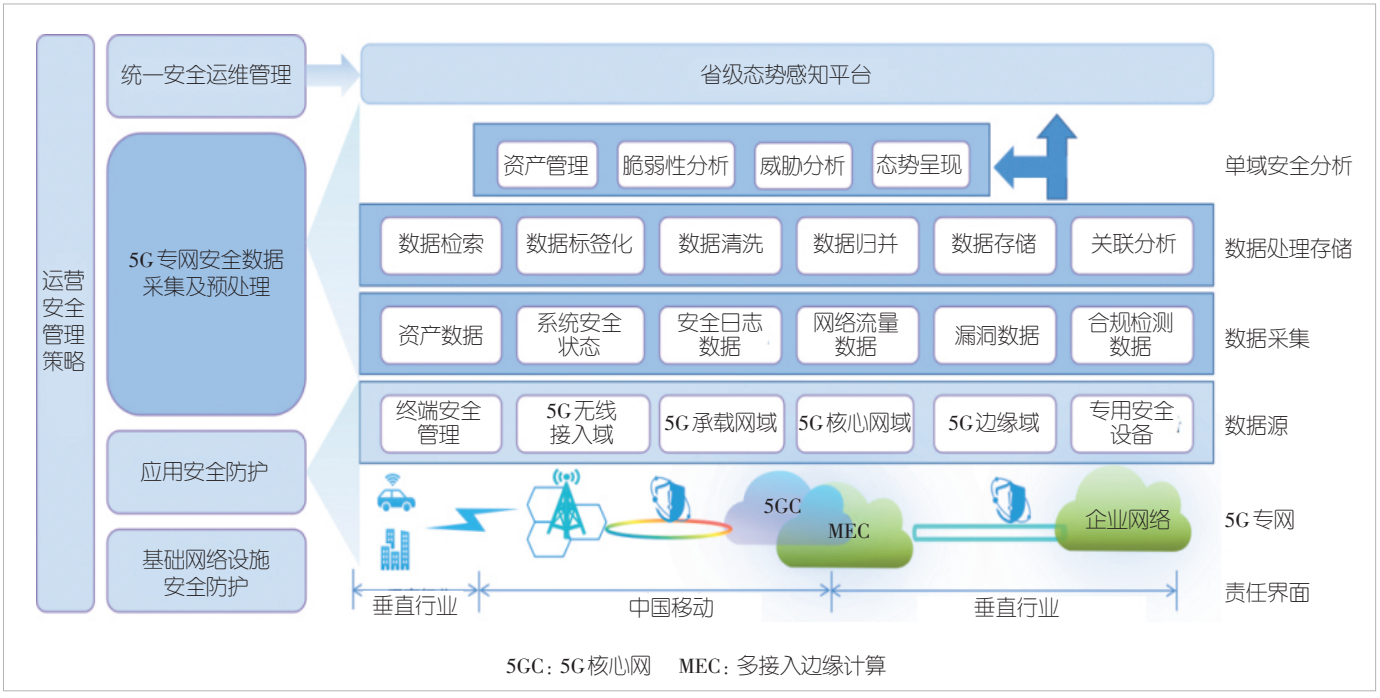
5G网络运营安全管理系统从5G网络网元、安全设备、流量采集探针、资产安全管理平台等采集数据，并与公共漏洞发布平台等对接获取漏洞及威胁情报，然后结合5G网络具体架构与场景进行安全分析，建立评估模型和评估指标，对5G网络进行安全评估、安全态势预警及处置。

我们基于三层模式完成5G网络运营安全管理方案的研究，通过整网端到端全局、单域和设备网元层形成大中小三层安全闭环的能力，完成各个层次下的数据采集方式、能力和要求的研究[4]。结合广东移动5G网络安全运营要求，指导5G网络数据采集能力的实现和5G网络安全运营工作的开展，如图2所示。

其中，三层安全闭环指的是：

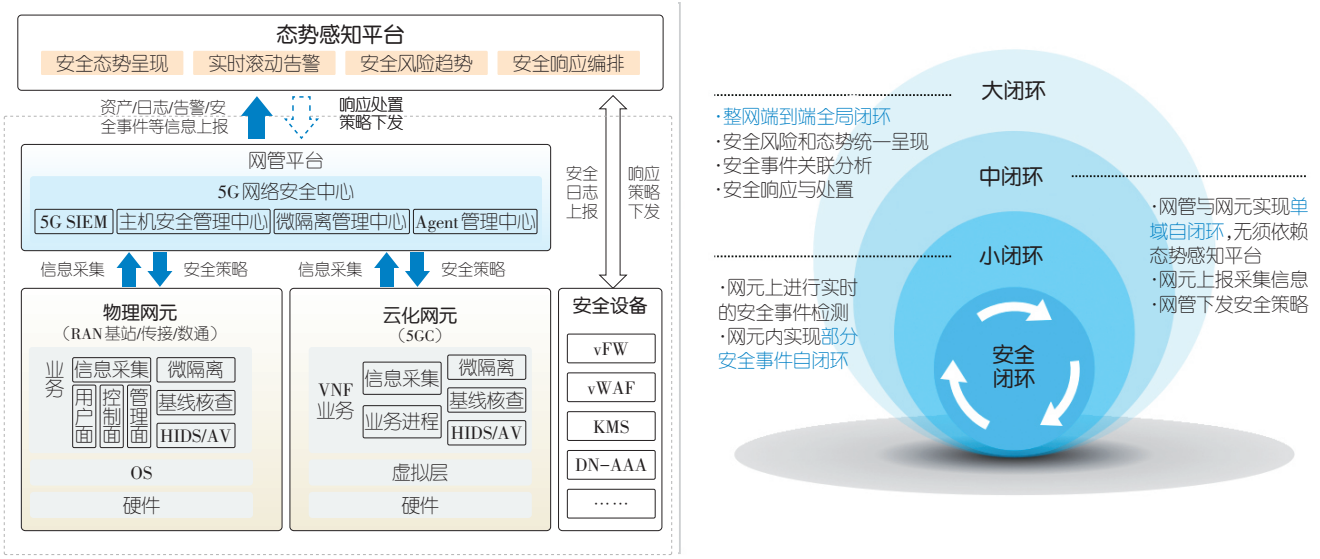
1）大闭环：通过整网端到端的全局闭环，进行安全事件与资产等的关联分析、安全响应与处置联动，实现5G网络安全风险和态势的统一呈现。

2）中闭环：通过网管与网元的单域自闭环，支持网元上报采集信息和网管下发安全策略，无须依赖上级态势感知平台。



5GC：5G核心网　MEC：多接入边缘计算

图1　5G网络运营安全管理体系架构



5GC：5G核心网
AV：防病毒
DN-AAA：数据网络认证、授权与计费
HIDS：主机入侵检测系统
KMS：密钥管理服务
OS：操作系统
RAN：无线接入网
SIEM：安全信息与事件管理
vFW：虚拟防火墙
VNF：虚拟网络功能
vWAF：虚拟Web应用防火墙

图2　基于三层模式的5G网络运营安全管理方案

3）小闭环：通过在网元上进行实时安全事件检测与拦截，在网元内部实现部分安全事件自闭环。

2.2 5G网络安全防护方案研究

针对引入5G专网的企业，我们研究安全责任边界划分，具体如图3所示：

1）运营商界面：园区内从5G空口至MEC站点用户面功能（UPF）网元N6出口之间的端到端5G网络属于运营商资产，包括基站、UPF、MEC平台、传输和承载设备，运营商保证其安全性。

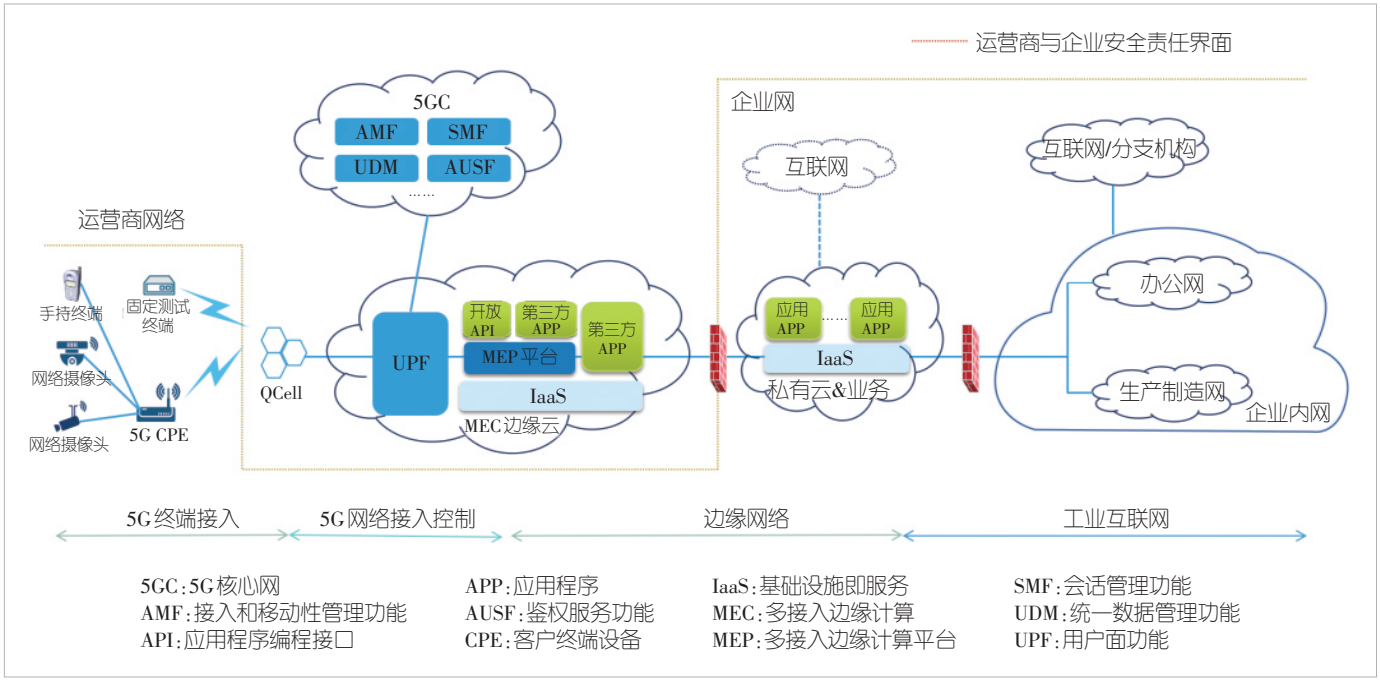


图3　5G专网安全责任边界

2）企业客户界面：园区内的生产设备、5G终端、私有云承载的应用程序（APP）及其虚拟机（VM）属于企业资产，企业保证其安全性。

我们从5个方面对5G网络安全防护方案开展了研究：

1）网元安全防护：MEC、UPF、基站、切片分组网（SPN）等作为组成5G专网的关键网元设备，通过强化N4/N6接口、安全配置核查、异常行为分析、入侵检测、网际协议安全（IPSec）通道认证和加密强度等方式保障网元设备自身安全。

2）网络边界防护：在N3/N4/N6等重要接口和网络边缘、终端侧等风险暴露面，部署防火墙、入侵防御系统（IPS）、蜜罐等安全设备，强化分布式拒绝服务（DDoS）、安全检测以及全流量等防御能力，相关安全告警统一纳入态势感知平台监测分析，强化5G网络边界安全防护手段与管理能力。

3）网络安全隔离：构建彼此隔离的5G网络切片，在无线接入网侧划分无线频谱和基站处理资源，在承载侧采用软隔离和硬隔离技术，在核心网侧采用接入策略控制、相互认证和安全隧道等方式实现安全隔离。

4）网络传输安全防护：对于N3/N6接口通过IPSec对传输的数据进行机密性和完整性保护；对于N4接口通过对传输的信令进行机密性和完整性保护；对于N6/N9接口，数据面承载通过防火墙隔离和保护，以保护核心网网络安全。

5）MEC安全防护：部署云安全管理中心，采用多层接入访问控制、内网隔离等手段，保障行业用户数据安全存储与访问，实现应用和数据全生命周期安全管理。

2.3 5G网络安全数据采集及预处理方案研究

5G网络安全数据采集及预处理方案确定了数据源的采集方案，开展对不同厂家的5G网元、网管、安全设备、安全系统等相关安全数据的研究，依据标准规范完成数据预处理关键技术的试验验证，实现5G网络运营安全管理的总体目标，支撑5G网络运营安全管理系统的建设和演进。

5G网络安全数据采集范围包括：

1）5G网元安全数据采集：支持对5G核心网（5GC）、5G无线接入网（RAN）、MEC、5G终端等网元数据的采集。

2）安全资产数据采集：安全资产数据覆盖范围广泛，需要支持对网元网管设备资产、网络设备资产、主机资产、安全设备资产、物联网资产、办公外设资产、应用系统资产、支撑系统资产、软件类资产等资产数据的采集。

3）单域态势感知数据采集：在网管侧实现内生单域安全运维管理能力，构建支持感知业务的安全检测、响应处置和安全策略编排能力，对网元、网管自身的攻击入侵、软件篡改、恶意操作等安全事件和基线核查结果进行采集。

4）专网平台类产品数据采集：调研分析5G专网场景中的平台类产品，研究并采集具有价值的平台上的数据。

5）非IT类安全数据采集：支持对非云化网元、硬件网络设备等非IT类安全资产上的网络安全基础信息的采集。

2.3.1 应用场景研究

由于不同应用场景组网方式、设备部署等存在差异，需要研究在不同部署场景下采集的数据内容。应用场景可划分为单域态感、多域态感和运营技术（OT）域态感3种，如图4所示。

1）单域态感应用场景：5G网络安全中心作为单域网管的内置组件部署，并在网元中部署安全代理Agent，支持管理单域内的5G RAN网元、5GC网元等。5G网络安全中心与网管集成部署，通过Agent采集单域内网元的资产数据、日志与安全事件，数据经处理、存储与单域安全分析后，支持北向接口上报至运营商省级态势感知平台。

2）多域态感应用场景：当不同域间网络互通时，5G网络安全中心作为独立系统部署，并在网管和网元中部署安全代理Agent，支持管理不同域的网元、网管等。5G网络安全中心与网管分离部署，对接多个网管系统，通过Agent采集不同域的网管、网元的资产数据、日志与安全事件，数据经过处理、存储与多域关联分析后，支持北向接口上报至运营商省级态势感知平台。

3）OT域态感应用场景：5G网络安全中心作为独立系统部署，并在5GC下沉网元、多接入边缘计算平台（MEP）、虚机和业务应用系统中部署安全代理Agent，支持管理5GC下沉网元、终端安全管理系统、NodeEngine、流量探针、安全设备等。5G网络安全中心对接多种系统与安全设备，通过Agent采集5G终端状态、资产和流量数据、日志与安全事件，数据经过处理、存储、威胁分析与响应联动，支持北向接口上报至企业态势感知平台。

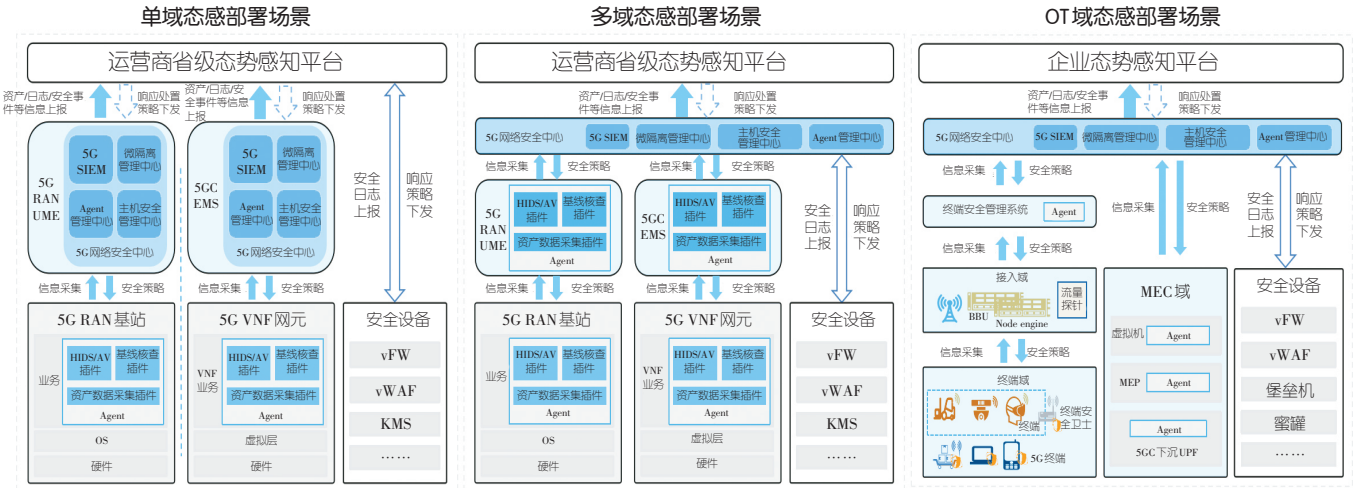
2.3.2 数据采集及预处理策略研究

1）资产采集策略

5G网络架构基于云化部署并采用服务化架构，使得5G网络架构中的资产种类更为广泛，资产逻辑关联关系更为复杂[5]。与传统互联网或办公网的资产类别对比，5G网络中还包括了切片、虚拟网络功能（VNF）网元等多种资产信息。通过采集全面的5G网络资产信息，确定5G网络中关键资产逻辑关系，绘制清晰的网络拓扑关系图，实现5G网络资产的关联管理，及时了解5G网络中漏洞或威胁对资产的波及影响，如图5所示。

2）安全数据采集策略

传统安全分析检测技术都是单一能力的，例如日志检测类产品、操作系统（OS）、安全检测类产品、网络检测类产品等等，这种割裂的技术方案不能直接、准确地获得安全分析结果，而是需要安全运维专家查看多个检测平台并综合分析结果。然而，5G专网网元分布在运营商大网外，网元自身受到大网网管的管理，可在网管侧实现内生单域安全运维管理能力，构建感知业务的安全检测与响应、安全策略编排的能力，对网元、网管自身遇到的攻击入侵、软件篡改、恶



5GC：5G核心网　HIDS：主机入侵检测系统　OS：操作系统　SIEM：安全信息与事件管理　VNF：虚拟网络功能
AV：防病毒　KMS：密钥管理服务　OT：运营技术　UME：统一管理专家　vWAF：虚拟Web应用防火墙
BBU：基带处理单元　MEC：多接入边缘计算　RAN：无线接入网　UPF：用户面功能
EMS：网元管理系统　MEP：多接入边缘计算平台　RRU：射频拉远单位　vFW：虚拟防火墙

图4　5G专网安全数据采集应用场景

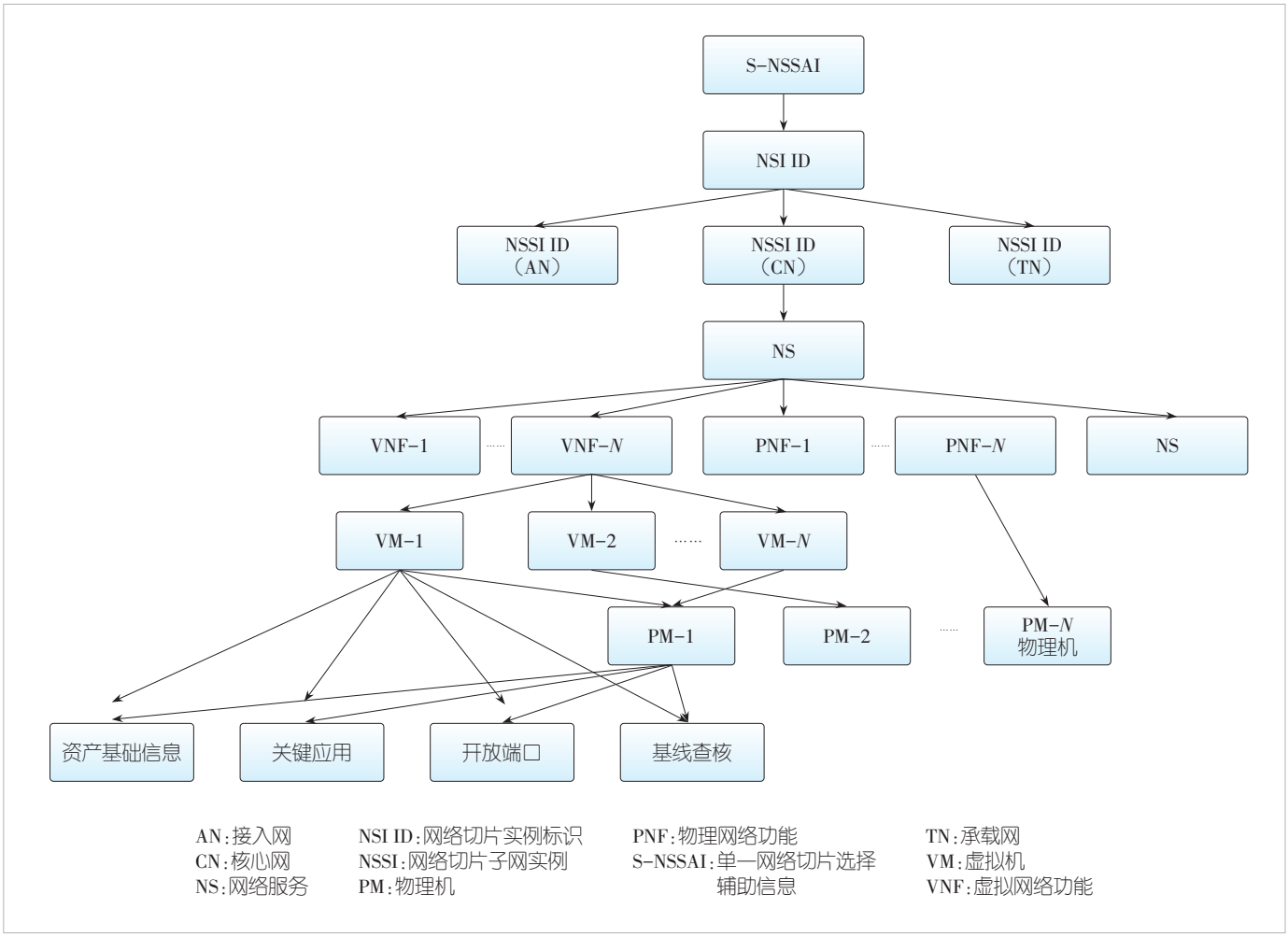


图5　5G网络中关键资产逻辑关系

意操作等安全事件，实现“分钟级”的快速感知，提高对业务和系统的安全配置合规管理能力。

5G网元作为5G网络关键业务设备，需要采集的安全数据主要包括以下两种：

（1）按IT类安全资产上报的5G安全数据，具体包括：云化部署的网元、网管系统、通信技术（CT）云主机等。其中，云化部署的网元和系统一般包含虚拟机，为了清楚标注网元或系统和虚拟机的关系，故单独归类。因此，IT类安全资产按照部署形式，可分为云化部署的网元和系统，以及CT云主机两类，分别采用不同的格式上报5G安全数据。

（2）按非IT类安全资产上报的5G安全数据，具体包括：非云化网元、非云化网管系统和网络设备。

3）日志采集与解析策略

5G网络运营安全管理系统需要支持各种日志的采集与解析，包括从主机、网元采集的系统日志，从数据库、中间件、Web应用采集的应用日志，从5G RAN、承载网、核心网等管理维护系统采集的告警日志、操作日志等，从防火墙、IPS、入侵检测系统（IDS）、Web应用防火墙（WAF）、堡垒机、蜜罐等安全设备采集的会话审计日志、主机操作日志、门户登录日志、流量元数据、信令元数据、告警数据和日志数据等。

4）数据预处理策略

针对5G网络运营安全管理系统采集的不同厂家，不同类型的5G网元、5G网管、网络安全设备、安全系统等数据通过数据预处理，可以将数据的类型、内容、格式进行规范化，实现安全数据共享。

该策略的设计思路如下：

（1）数据采集预处理：即从各个数据源将数据采集汇聚并加以归一化、标准化等预处理。

（2）数据清洗和标准化：支持对采集的日志数据进行清

洗和标准化。

（3）日志清洗：能够对数据存在的错误、不完整、无效等问题进行清洗。支持配置日志过滤规则实现对日志的过滤清洗。过滤规则可存在多种方式：关键字或关键字组合、条件运算、正则匹配、表达式计算等。

（4）日志标准化：支持对采集的各类异构日志进行统一格式化处理，并保存原始数据。支持分隔符、键值对、JavaScript对象表示法（JSON）等多种格式日志解析，并可通过正则表达式对格式不规则日志进行解析。支持根据每类日志的标准定义字段规则，对日志解析提取到的字段进行标准化。

5）数据上报策略

5G网络运营安全管理系统应能将5G网络资产信息、安全事件、日志等信息上报给上级态势感知平台，上报方式包括：

（1）安全文件传输协议（Sftp）方式：系统将资产信息按JSON格式存为文件，提供Sftp服务供上层系统调用。资产文件定期更新，可反映最新资产状态。

（2）具有表述性状态转移特性的（RESTful）接口方式：支持实时查询当前资产信息，包括资产类型、属性、状态等。除了资产信息，还能够查询资产漏洞和威胁信息等。

（3）Syslog接口方式：除了提供查询接口外，系统应能提供信息主动上报功能，在安全事件发生时，以syslog形式上报事件信息，信息内容包括事件名称、类型、互联网协议（IP）地址等。

3 5G网络运营安全管理系统实践

广州南方电网5G专网是典型的5G下沉专网，是“5G+数字电网”垂直行业应用标杆。根据前文的策略研究，我们选择在广州南方电网5G专网进行5G网络运营安全管理系统试点实践。其中，5G网络运营安全管理系统包括无线基站、5G核心网网元（下沉L型UPF）、5G RAN统一管理专家（UME）网管、5GC网元管理系统（EMS）网管、5G网络安全中心，以及统一采集平台和省态势感知平台。

广州南方电网试点项目采用多域部署方式，如图6所示，新建一套5G网络安全中心，通过对接5G RAN UME和5GC EMS网管，采集资产数据、基线核查结果与安全事件；北向对接统一采集平台与省态势感知平台，进行数据上报与响应处置策略下发，实现试点5G专网安全状态可感知。

根据内生安全理念，中国移动与中兴通讯等厂商合作，规划设计并落实5G网络运营安全管理系统，推出了5G网络安全中心，通过在网管与网元中内置安全代理（Agent），实现资产管理、基线核查、主机入侵检测、防病毒检测、安全分析、态势呈现等内生安全功能[6]，如图7所示。

5G网络运营安全管理系统如图8所示，其中5G网络安全中心具体包括：

1）安全态势感知中心：实现资产管理、安全信息采集、威胁分析、态势呈现，进一步融入响应处置功能。

2）主机安全管理中心：实现资产数据采集、主机入侵检测、防病毒检测、基线核查等安全插件策略管理。

3）Agent管理中心：实现安全中心策略下发、Agent版本更新与插件管理等功能。

4）安全代理：接收并执行Agent管理中心下发指令，实现数据采集/告警上报等功能。

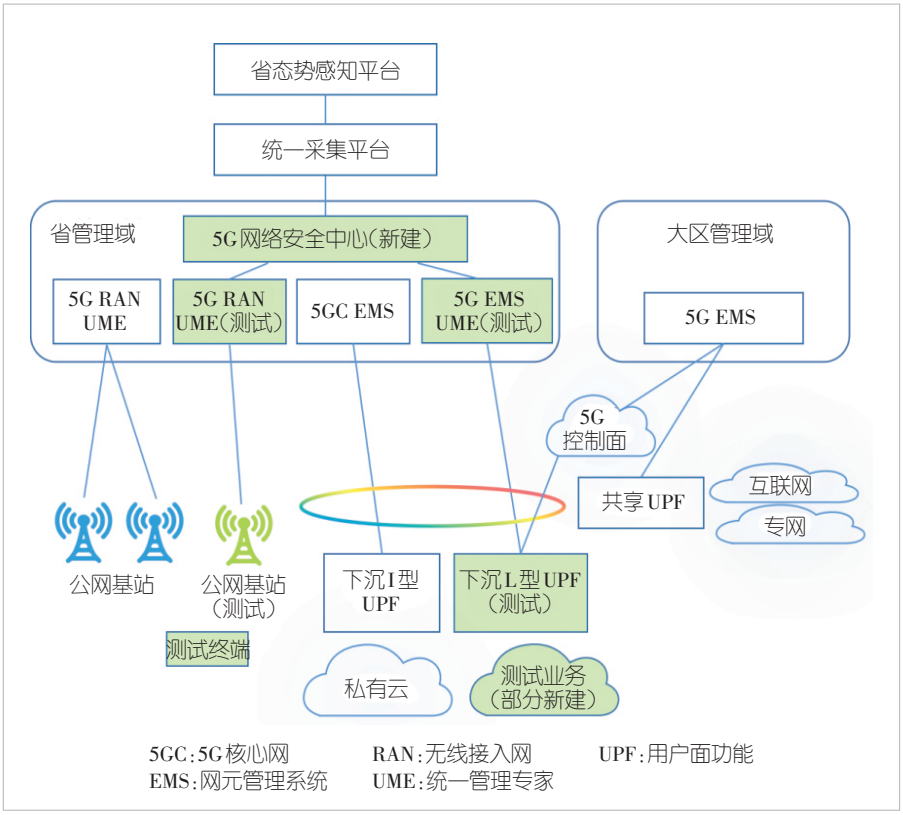


图6　广州南方电网试点项目

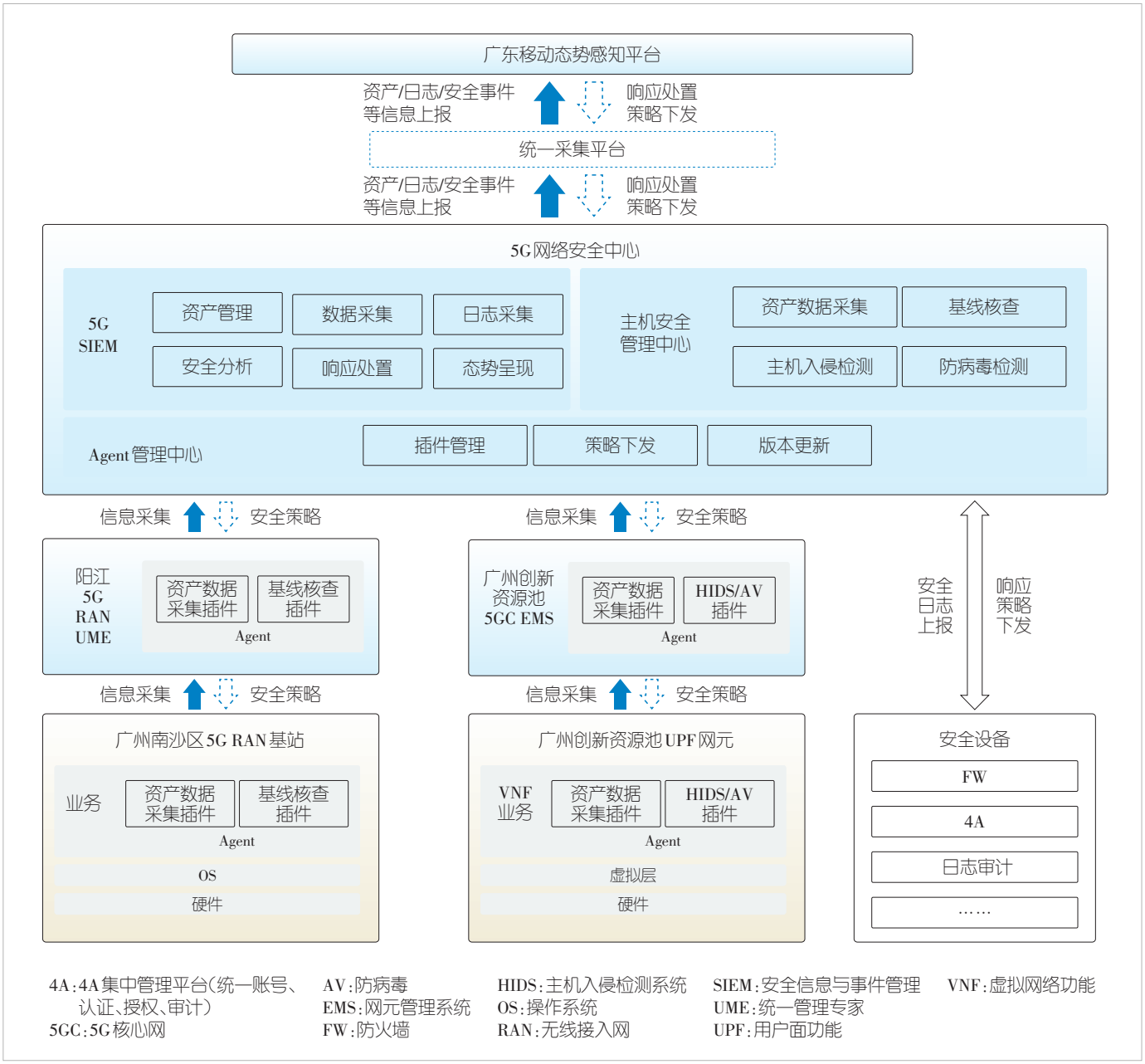


图7　5G网络运营安全管理系统试点项目落地部署架构

5）主机入侵检测系统（HIDS）/防病毒（AV）插件：在应用层执行安全中心指令，实现主机入侵检测或防病毒检测功能。

本次试点通过在IP承载网侧配置路由与防火墙策略，实现5G网络安全中心与阳江无线UME网管、广州创新资源池核心网EMS网管的数据交互。在广州南方电网5G专网场景中开展对5G基站、下沉UPF网元、网管的安全数据采集、基线核查、入侵检测、防病毒检测、安全态势呈现与数据上报的功能验证，试点所涉及的94条测试用例全部验证通过，顺利完成5G网络运营安全管理系统的建设工作。

5G网络运营安全管理系统的成功落地实践，明确了广州南方电网5G专网场景的安全责任边界，解决了5G网络安全数据采集问题，通过全面采集与分析5G网络安全数据，及时发现网络攻击，提升5G网络主动安全防御能力以及安全运维效率，为5G专网运营提供一套智能闭环处置的安全运营管理体系，保障5G行业应用和5G网络基础设施安全。

图8　5G网络运营安全管理系统界面

同时，为推动5G网络安全运营的普及与落地带来以下积极影响[7–8]：

1）促进5G行业应用的安全普及。该系统不仅保障了广州南方电网5G专网的安全运营，更为其他行业树立了安全管理的典范，增强了社会各界对5G网络安全性的信心，促进更多行业敢于并愿意采用5G技术，加速了5G技术在智能制造、智慧城市、智慧医疗等领域的广泛应用和普及。

2）提升公共安全与应急响应能力。5G网络的高速率、低延迟特性使得其在公共安全领域具有巨大潜力。该系统的成功实践，为应对突发事件、自然灾害等紧急情况提供了更加快速、可靠的信息传输与决策支持能力，有助于提升5G专网乃至整个社会的应急响应速度和效率，增强公共安全意识。

3）促进网络安全技术创新与产业发展。该系统的研发与实施，不仅解决了当前5G网络安全运营管理领域的一些关键技术难题，还带动了网络安全技术创新与产品研发的活跃度。未来更多类似项目的开展和成功经验的积累，将有力推动网络安全产业的快速发展，形成更加完善的网络安全产业链与生态体系[9–10]。

综上所述，广州南方电网5G网络运营安全管理系统的成功落地实践，不仅提升了企业自身的网络安全防护能力与运营效率，更在社会层面产生了广泛而深远的影响，为5G技术的普及应用、公共安全的提升以及数字社会的构建贡献了重要力量。

4 结束语

本文通过对5G网络运营安全管理策略的深入研究，设计并落实5G网络运营安全管理系统，依据内生安全理念，提出了5G网络安全中心，打造5G网络运营安全管理体系，增强5G网络安全防护水平，建设满足监管要求的安全可靠5G网络，实现网络安全与5G业务的深度融合。通过孵化5G网络运营安全解决方案，携手生态企业，协同研发相关产品，可陆续在能源、交通、工业、医疗、教育等行业复制推广，助力5G应用的健康发展，奠定企业数字化转型所必需的5G网络基础设施能力。

未来，5G网络运营安全管理系统及其相应模式将成为5G专网产品推广应用过程中必不可少的组成部分，增强各行业客户基于5G进行产业升级的安全信心，为5G面向行业应用的迅速普及带来积极的推动作用。

参考文献

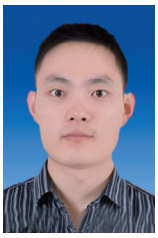
[1] 苗守野. 关于5G网络内生安全的思考 [J]. 信息通信技术, 2023, 17(4): 56–62
[2] 王瀚洲, 刘建伟. 网络内生安全研究现状与关键技术 [J]. 中兴通讯技术, 2022, 28(6): 2–11. DOI: 10.12142/ZTETJ.202206002

[3] 何国锋, 段赟, 刘东鑫, 等. 面向未来网络的高可信内生安全体系研究 [J]. 网络安全与数据治理, 2023, 42(4): 45-50. DOI: 10.19358/j.issn.2097-1788.2023.04.008
[4] 马铮, 闫新成, 周继华, 等. 网络5.0内生安全可信体系 [J]. 信息通信技术与政策, 2023, 49(12): 40-47. DOI: 10.12267/j.issn.2096-5931.2023.12.005
[5] 曾梦岐, 石凯. 基于动态信任的内生安全架构 [J]. 通信技术, 2022, 55(8):1036-1043.
[6] 韩永刚. 基于内生安全框架的面向数字化转型的网络安全防御体系 [J]. 中兴通讯技术, 2022, 28(6): 29-35+56. DOI: 10.12142/ZTETJ.202206006
[7] 袁超颖, 白景鹏, 袁淑美, 等. 新一代电信云网内生安全架构研究 [J]. 中兴通讯技术, 2025, 31(3): 3-8. DOI: 10.12142/ZTETJ.202503002
[8] 粟栗, 闫茹, 马宇威. 6G 网络内生安全体系运行机制研究 [J]. 中兴通讯技术, 2025, 31(3): 44-49. DOI: 10.12142/ZTETJ.202503008
[9] 马红兵, 姚戈, 张曼君, 等. 6G网络安全架构展望 [J]. 中兴通讯技术, 2025, 31(3): 56-61. DOI: 10.12142/ZTETJ.202503010
[10] 陆海涛, 周强, 代九龙, 等. 面向6G 的天地一体化网络安全技术 [J]. 中兴通讯技术, 2025, 31(6): 75-83. DOI: 10.12142/ZTETJ.202506011

作 者 简 介

任若冰，中国移动通信集团广东有限公司高级工程师；主要研究方向为5G应用安全、网络安全管理支撑系统等；参与多个省部级重大专项。

费明，中国移动通信集团广东有限公司工程师；主要研究方向为网络运维、5G行业应用等。



贾国祖，中国移动通信集团广东有限公司高级工程师；主要研究方向为物联网与5G专网等；发表论文5篇，申请专利10项，拥有软件著作权4项。

许晨敏，北京兴云数科技术有限公司工程师；主要研究方向为AGV、5G网络安全、内生安全等；发表论文2篇，申请专利1项。

郝振武，中兴通讯股份有限公司规划总工；主要研究方向为5G网络安全、工业互联网安全、内生安全等。