ICS XX.XXX.XX
CCS X XX

ZJSEE

浙 江 省 电 力 学 会 标 准

T/ZJSEE XXXX-YYYY

虚拟电厂系统网络安全防护技术规范

Technical Specification for Network Security Protection of Virtual Power Plant Systems

（征求意见稿）

2024-12-1 发布　　2025-01-01 实施

浙 江 省 电 力 学 会　发 布

目　　次

前　　言 II
引　　言 III
1 范围 2
2 规范性引用文件 2
3 术语和定义 2
4 符号、代号和缩略语 3
5 总体原则及要求 3
5.1 总体原则 3
5.2 总体要求 4
6 基础设施安全 4
7 体系结构安全 4
7.1 总体架构要求 4
7.2 安全分区 4
7.3 网络专用 5
7.4 横向隔离 5
7.5 纵向认证 5
8 本体安全 5
8.1 基础软件安全 5
8.2 操作系统安全 5
8.3 计算机和网络及监控设备的安全 5
8.4 可信安全免疫 6
9 数据安全 6
9.1 数据存储安全 6
9.2 安全加密方式 6
9.3 安全加密要求 6
10 应急备用 6
10.1 冗余备用 6
10.2 应急响应 6
11 全面安全管理 6
11.1 安全生产管理体系 6
11.2 人员安全管理 6
11.3 设备及系统的安全管理 6
11.4 全生命周期安全管理 7
参　考　文　献 8

前　言

为规范虚拟电厂技术支持系统建设，保证后续源网荷互动的系统本质安全、信息传播安全和信息内容安全，为系统建设提供安全防护的指导，制定本标准。

本标准按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件（或本部分或本指导性技术文件）由浙江省电力学会提出。

本文件(或本部分或本指导性技术文件)由浙江省电力学会电力系统专业委员会技术归口和解释。。

本文件（或本部分或本指导性技术文件）起草单位（包括第一承担单位和参加起草单位，按对标准的贡献大小排列）：

本文件（或本部分或本指导性技术文件）主要起草人（按对标准的贡献大小排列）：

本文件（或本部分或本指导性技术文件）首次发布（或本文件×年×月首次发布，×年×月第一次修订，×年×月第二次修订）。

本文件在执行过程中的意见或建议反馈至浙江省电力学会标准工作委员会（地址：浙江省杭州市南复路 1 号，邮编：310008，网址：http://www.zjsee.org/，邮箱：zjseeorg_bz@163.com）。

引　言

在双碳和建设新型电力系统的目标下，新能源装机容量快速增长，由于新能源发电的强间歇性、波动性、时空性，需要电网提供更多的灵活性调节资源保证电网安全稳定运行。随着虚拟电厂技术在负荷资源聚合调控中的广泛应用，为了加强电力监控系统的安全管理，根据国家发改委 2014 第 14 号令《电力监控系统安全防护规定》和 GB/T 36572-2018《电力监控系统网络安全防护导则》等相关规定制定本标准。

虚拟电厂系统网络安全防护技术规范

1 范围

本文件规定了虚拟电厂技术支持系统的总体架构要求、本体安全要求、网络安全要求、身份认证要求、安全加密方式及安全加密要求等。

本文件（或本部分或本指导性技术文件）适用于参与电网运行的虚拟电厂技术支持系统的系统网络安全防护。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 9361　　计算机场地安全要求
GB/T 20272　　信息安全技术 操作系统安全技术要求
GB/T 20984　　信息安全技术 信息安全风险评估规范
GB/T 22239　　信息安全技术 网络安全等级保护基本要求
GB/T 20273　　信息安全技术 数据库管理系统安全技术要求
GB/T 36572　　电力监控系统网络安全防护导则
GB_T 38318　　电力监控系统网络安全评估指南
GB/T 37934　　信息安全技术 工业控制网络安全隔离与信息交换系统安全技术要求
GB/T 44241　　虚拟电厂管理规范
DL/T 2473.2　　可调节负荷并网运行与控制技术规范 第2部分：网络安全防护
中华人民共和国国务院令第745号　关键信息基础设施安全保护条例
中华人民共和国国家发展和改革委员会令2014年第14号　电力监控系统安全防护规定
国能安全[2015]36号　　电力监控系统安全防护总体方案和评估规范

3 术语和定义

下列术语和定义适用于本文件。

3.1

虚拟电厂　Virtual Power Plant

通过先进的信息通信技术、智能计量以及优化控制技术，将分布式电源、储能、可调节负荷、电动汽车等分布式资源进行集成，构成具备响应电网需求、参与电力市场运行或接受电网优化调度的系统。

[来源：GB/T 44241-2024 3.1]

3.2

网络安全　Cybersecurity

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

[来源：GB/T 22239-2019 3.1]

3.3

虚拟电厂资源　Virtual Power Plant Resources

能向外输出电能量或提供电功率调节能力的分布式设备或系统。

注：包括但不限于分布式电源、分布式储能、可调节负荷及其组合等。

[来源：GB/T 44241-2024 3.2]

3.4

可调节负荷 Adjustable Load

电力系统中具备技术条件并参与电网调度的负荷资源，可以是满足准入条件的大用户，也可以是聚合后的主体。通过车联网平台（电动汽车）、智慧能源服务平台（营销）、第三方独立主体（虚拟电厂）聚合平台、大用户模式接入负荷调控系统，具备按照电网调度指令或既定控制策略参与调节的能力。

[来源：DL/T 2473.2-2022 3.1]

3.5

虚拟电厂运营商 Virtual Power Plant Operator

将具备可调潜力或发电能力的分布式资源、虚拟机组集中在一起，作为整体参与电力市场或电网运行，并代理相关事宜的机构。

[来源：GB/T 44241-2024 3.3]

3.6

虚拟电厂技术支持系统 Virtual Power Plant Technical Support System

由虚拟电厂运营商建设运营的，通过信息双向互动通信为其实施调控策略提供技术支撑的，实现信息处理、运行监控、业务管理、计划监管、控制执行等功能的软硬件系统。

[来源：GB/T 44241-2024 3.4]

3.7

生产控制大区 Production Control Zone

由具有实时监控与采集以及生产控制等相关功能、纵向联接使用专用网络或专用通道的电力监控系统构成的安全区域。

[来源：GB/T 36572-2018 3.3]

3.8

管理信息大区 Management Information Zone

生产控制大区之外的，主要由邀约管理、计划申报以及交易结算等构成的安全区域。

3.9

互联网区 Internet Zone

是由可调节资源数据采集与交互、交易管理等构成的面向对外服务的安全区域。

3.10

横向隔离 lateral Isolation

在不同安全区间禁止通用网络通信服务，仅允许单向数据传输，采用访问控制、签名验证、内容过滤、有效性检查等技术，实现接近或达到物理隔离强度的安全措施。

[来源：GB/T 36572-2018 3.7]

3.11

纵向认证 Vertical Authentication

采用认证、加密、访问控制等技术实现数据的远方安全传输以及纵向边界的安全防护的措施。

[来源：GB/T 36572-2018 3.8]

4 符号、代号和缩略语

下列符号、代号和缩略语适用于本文件。

SM1：对称密码算法，使用 128 比特分组的分组密码算法，用于密钥协商数据的加密保护和报文数据的加密保护

SM2：256 比特 SM2 椭圆曲线密码算法，用于实体验证、数字签名和数字信封等

SM3：密码杂凑算法，用于对称密钥生成和完整性校验。输出为 256 比特

SM4：对称密码算法，使用 128 比特分组的分组密码算法，用于密钥协商数据的加密保护和报文数据的加密保护

5 总体原则及要求

5.1 总体原则

虚拟电厂技术支持系统所采用的软硬件设备、通信技术和网络安全防护技术，应符合国家有关的技术标准、行业标准和有关的国际标准的基本原则。

5.2 总体要求

应满足国家法律法规和国家技术标准的相关要求，如国家网络安全法、数据安全法、GB/T 22239、GB/T 36572 等。

6 基础设施安全

虚拟电厂运营商机房和生产场地应符合 GB/T 36572 的规定，选择在具有防震、防风和防雨等能力的建筑内；机房和生产场地应符合 GB/T 9361 的规定，采取有效防水、防潮、防火、防静电、防雷击、防盗窃、防破坏措施；机房和生产场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁。

虚拟电厂运营商宜在机房供电线路上设置冗余或并行的电力电缆线路为计算机系统供电，宜建立备用供电系统，提供短期的备用电力供应。

7 体系结构安全

7.1 总体架构要求

虚拟电厂并网运行与控制系统总体安全防护架构要求如图 1 所示。

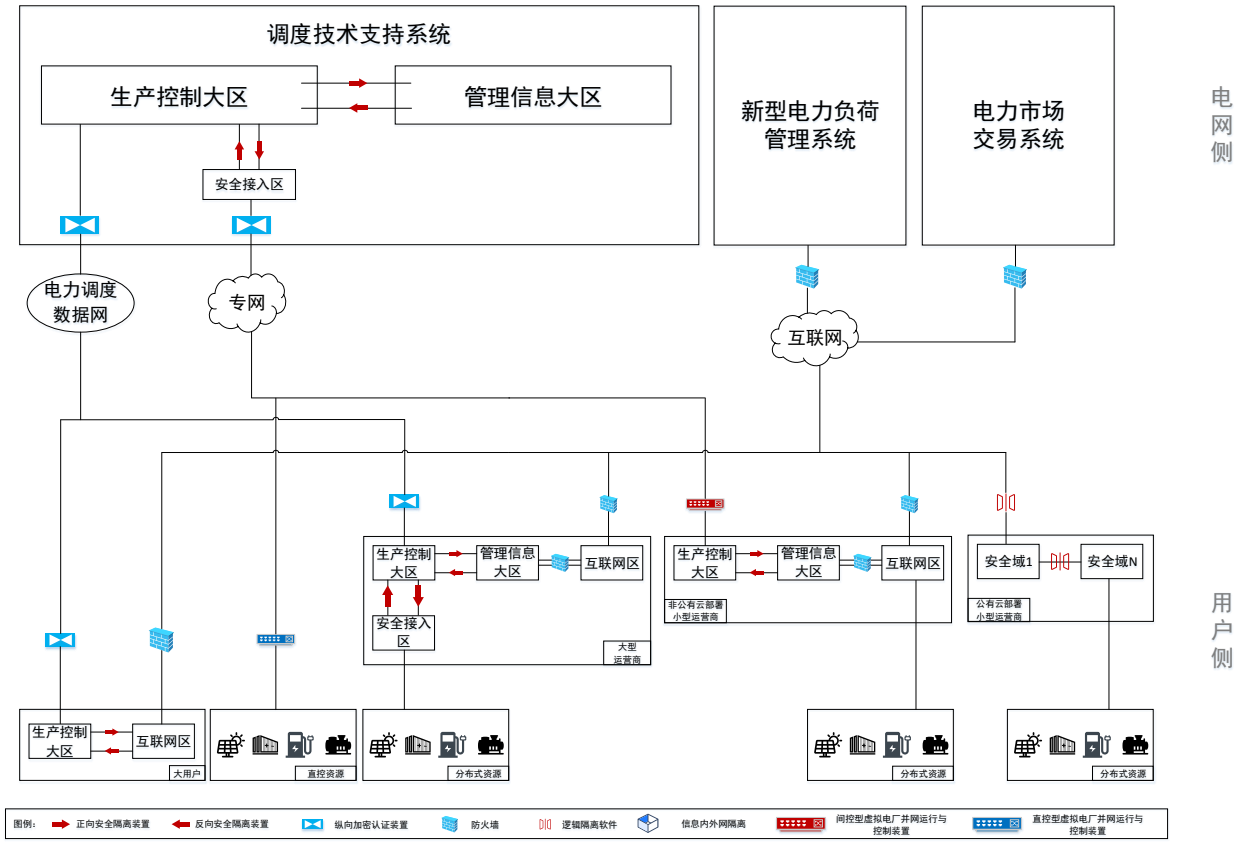

图 1 安全防护架构图

7.2 安全分区

根据电力监控系统的网络安全要求，参与电网运行的虚拟电厂技术支持系统应按照业务功能划分相应的安全分区，宜划分为生产控制大区、管理信息大区和互联网区等。

生产控制大区部署与电网侧实时调控功能相对应的功能模块，涉及实时监控与采集、生产控制等相关功能。管理信息大区部署与电网侧管理类功能相对应的功能模块，涉及虚拟电厂运营商平台邀约管理，

计划申报等相关功能。互联网区用于实现与新型电力负荷管理系统、电力市场交易系统以及各类分布式资源连接，完成数据采集与交互、交易管理等相关功能。对于公有云部署的虚拟电厂技术支持系统应根据功能划分相应的安全区域，不同虚拟电厂技术支持系统应部署于公有云平台的不同区域。

7.3 网络专用

调度机构与虚拟电厂运营商信息交互的网络类型包括调度数据网、专用通信网络。虚拟电厂运营商与新型电力负荷管理系统/电力市场交易系统信息交互的网络类型为专用通信网络、互联网。

负荷调节策略应优先采用调度数据网下发，调度数据网未覆盖到的虚拟电厂运营商与调度机构数据通信宜采用专用通信网络。

对部分负荷聚合规模较大，其负荷波动可能直接影响电网安全稳定运行的虚拟电厂技术支持系统，宜进一步在聚合平台与虚拟电厂终端的边界处部署安全隔离装置，隔离装置须满足 GB／T 37934-2019 的要求。

7.4 横向隔离

虚拟电厂运营商内部生产控制大区与安全接入区之间，应设置经国家检测部门检测认证的电力专用横向单向安全隔离装置，隔离强度应当接近或达到物理隔离。

虚拟电厂运营商内部生产控制大区与管理信息大区之间，应设置经国家检测部门检测认证的电力专用横向单向安全隔离装置，隔离强度应当接近或达到物理隔离。

虚拟电厂运营商内部生产控制大区与互联网区之间，应设置经国家检测部门检测认证的电力专用横向单向安全隔离装置，隔离强度应当接近或达到物理隔离。

虚拟电厂运营商内部管理信息大区与互联网区之间，应采用防火墙等逻辑隔离措施。

公有云部署的虚拟电厂运营商平台，应通过公有云厂商提供的逻辑隔离软件划分不同安全域，并配置访问控制策略，隔离强度应当接近或达到相应的隔离水平。

7.5 纵向认证

虚拟电厂运营商通过调度数据网接入调度机构，应部署纵向加密认证装置或纵向加密认证模块，应具备身份认证、报文过滤和机密性、完整性保护功能。

直控资源或虚拟电厂运营商平台通过并网运行与控制终端接入调度机构时，终端应采用国密加密芯片的独立加密硬件实现数据传输的加密、身份认证和入侵防范功能。

虚拟电厂技术支持系统与可调节负荷之间的控制业务交互宜采取纵向安全加密措施，加密算法应采用国密加密算法。

8 本体安全

8.1 基础软件安全

虚拟电厂技术支持系统使用的数据库、中间件等基础软件应通过国家有关机构的安全检测认证。

生产控制大区业务系统的数据库、中间件等基础软件应符合 GB/T 22239、GB/T 20273 的规定，使用时应合理配置、启用安全策略；操作系统和基础软件应仅安装运行需要的组件和应用程序，并及时升级安全补丁，补丁更新前应进行充分的测试，禁止直接通过因特网在线更新。

8.2 操作系统安全

虚拟电厂运营商的计算机设备应符合 GB/T 20272 的规定，操作系统应通过国家有关机构的安全检测认证，并应符合信息安全等级保护第二级要求的要求。

虚拟电厂运营商应采用“最小特权”等安全机制，重要主机应采用无 root 用户运行模式。

8.3 计算机和网络及监控设备的安全

虚拟电厂技术支持系统中的计算机和网络设备，应通过国家有关机构的安全检测认证，防范设备主板存在恶意芯片。

生产控制大区应采用符合国家相关要求的计算机和网络设备，使用时应合理配置、启用安全策略；应封闭网络设备和计算机设备的空闲网络端口和其他无用端口，拆除或封闭不必要的移动存储设备接

口（包括光驱、USB 接口等），仅保留调度数字证书所需要的 USB 端口。

8.4 可信安全免疫

虚拟电厂运营商的关键应用服务器宜部署安全可信验证模块，对通信设备、边界设备以及计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信认证，并在应用程序的关键执行环节进行动态可信验证。

9 数据安全

9.1 数据存储安全

虚拟电厂运营商应符合数据安全法要求，建立健全全流程数据安全管理制度，组织开展数据安全教育培训，重要数据分级分类，并采取技术措施保障数据安全。

虚拟电厂运营商的合同、交易等关键业务数据应采用加密存储，并采取数据防泄露、水印追踪、防止越权访问与篡改等措施。

虚拟电厂运营商平台的调节策略等敏感数据传输过程应采取加密认证、数据签名等技术。

9.2 安全加密方式

虚拟电厂运营商可使用调度数据网、无线专网等方式接入调度技术支持系统，纵向通信应采用硬加密（如经过国家指定部门检测认证的电力专用纵向加密认证装置或加密认证网关）或软加密（如 https 加密协议），实现双向身份认证、数据加密和访问控制功能。

9.3 安全加密要求

身份认证宜采用国密 SM2 数字签名算法，签名串长度不小于 64 位。

业务报文加密宜采用国密对称加密算法，业务数据报文应采用身份认证、加密等安全防护措施进行保护。

在线更新密钥时，密钥应加密后进行传输。

10 应急备用

10.1 冗余备用

虚拟电厂技术支持系统应实现数据备份及关键设备的冗余备用，建立系统恢复机制，支撑系统故障的快速处理和恢复，保障系统业务的连续性。

10.2 应急响应

应急响应应符合 GB/T 36572 的规定，建立虚拟电厂技术支持系统的应急机制，制定相关制度和应急处理预案，并定期开展应急演练。

11 全面安全管理

11.1 安全生产管理体系

虚拟电厂运营商应按“谁主管谁负责，谁运营谁负责”的原则，建立安全管理制度，健全组织保证体系和安全责任体系。

11.2 人员安全管理

虚拟电厂运营商应对全体人员进行安全管理和培训教育，并应符合 GB/T 22239 的规定。

11.3 设备及系统的安全管理

虚拟电厂技术支持系统的软件模块和硬件设备应建立设备台账，实行全方位安全管理。

虚拟电厂运营商在安全防护设备选型及配置时，应选用国家相关部门检测通过无漏洞和安全风险

的特定系统及设备。

虚拟电厂技术支持系统接入调度机构时应制定接入技术方案、采取相应安全防护措施，接入技术方案须通过调度机构安全管理部门的审核、批准。

虚拟电厂技术支持系统应按 GB/T 20984 和 GB/T 30976.1 的规定，定期开展安全风险评估，针对发现的问题及时整改。

11.4 全生命周期安全管理

虚拟电厂运营商在规划设计、研究开发、施工安装调试、系统改造、运行管理、退役报废等全生命周期阶段应采取相应安全管理措施。

虚拟电厂运营商应采用安全、可控、可靠的软硬件产品，在设备及系统生命期内对此负责，应按国家和行业有关要求做好保密工作。

虚拟电厂聚合资源并网运行与控制相关的重要信息、敏感数据应加强日常运维和安全管理，相关系统和设备退役报废时应按相关要求，销毁含敏感信息的介质和重要安全设备。

参 考 文 献

[1] 中华人民共和国国务院令第 745 号 关键信息基础设施安全保护条例。
[2] 中华人民共和国国家发展和改革委员会令 2014 年第 14 号 电力监控系统安全防护规定。