《电力系统数据异常处置规范》团体标准编制说明

一、工作简况

1.任务来源

本项目依据团体标准制修订计划立项，项目名称为《电力系统数据异常处置规范》。

随着新型电力系统、城市综合能源系统及能源互联网快速发展，电力系统数字化、网络化、智能化程度不断提高，数据安全、运行安全及网络安全问题日益突出。尤其在电力调度控制系统、电力物联网、新能源综合能源管理系统等场景中，数据异常、网络攻击、异常行为联动风险等问题对系统稳定运行造成较大影响，亟需建立统一、规范的数据异常监测、异常处置与网络安全协同防护技术体系。

目前行业内针对电力系统数据异常检测、网络攻击检测、风险评估及安全联动处置等方面尚缺少统一标准，特别是在城市综合能源系统场景下，缺乏融合“数据异常监测与处置—网络攻击检测与响应—风险评估—安全策略”的一体化技术规范。因此，有必要制定本标准，为电力系统运行安全、网络安全及数字化运维提供标准依据。

本标准由广东电网有限责任公司东莞供电局提出，珠海市自动化学会归口管理，由广东电网有限责任公司东莞供电局、珠海澳大科技研究院等单位联合起草。

计划完成时间为2026年。

2.主要工作过程

（1）预研阶段

项目启动前，起草组针对电力系统数据异常检测、网络攻击监测、工业控制系统安全、电力监控系统风险评估等方向开展了广泛调研，重点分析了当前电力系统在数据质量监测、安全态势感知、异常行为识别及风险联动处置等方面存在的问题。

同时，起草组对国内外相关标准、技术规范及研究成果进行了系统梳理，重点研究了GB/T 36572《电力监控系统网络安全防护技术要求》、DL/T 1970《电力系统数据质量评价规范》、DL/T 2277《电力监控系统网络安全风险评估规范》等标准内容，为本标准编制奠定基础。

（2）起草阶段

在前期调研基础上，起草组确定了标准总体框架、技术路线及主要技术内容，围绕应用模型构建、数据异常处置、网络攻击检测与处置、风险评估、安全策略及事件响应恢复等内容开展标准文本编制工作。

起草过程中，重点结合城市综合能源系统、电力调度控制系统、新能源综合能源管理系统、电力物联网等实际应用场景，对数据异常检测方法、网络攻击识别机制、风险评分模型、安全防护策略等内容进行了系统研究与规范化整理，形成标准草案。

随后，起草组多次组织专题讨论会，对标准结构、术语定义、模型架构、风险等级划分、检测流程及安全策略等内容进行反复论证和修改完善，形成标准征求意见稿。

（3）征求意见阶段

（4）送审阶段

（5）报批阶段

3.主要参加单位和工作组成员及其所做的工作

主要起草单位：广东电网有限责任公司东莞供电局、珠海澳大科技研究院、顺德职业技术大学。

主要起草人：李诗美、罗金满、邹浙湘、汪杰、刘丰瑞、刘景荣、赵善龙、钟志明、梁浩波、梅傲琪、封祐钧、刘丽媛、余凌、张锐、叶思琪、高承芳、李晓霞、王湘女、李祺威、冷颖雄、陈浩玮。

工作分工：广东电网有限责任公司东莞供电局主要负责标准总体框架设计、电力系统运行场景分析、数据异常检测需求研究、风险评估体系设计及标准技术内容统筹。

珠海澳大科技研究院主要负责网络攻击检测模型研究、安全防护策略研究、拓扑展示架构设计及标准技术内容验证。

各参与人员分别承担术语整理、标准条文编写、检测方法研究、案例分析、标准验证、意见汇总及文本修订等工作。

二、标准编制原则和主要内容

1.标准编制原则

本标准为首次制定，严格按照 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》、GB/T 20000《标准化工作指南》、GB/T 20001《标准编写规则》等相关要求进行编制。标准编制遵循“科学性、规范性、适用性、协调性、先进性”的原则。

（1）科学性原则

标准充分结合电力系统运行机理、工业控制系统网络安全理论及风险评估方法，对数据异常检测、网络攻击检测及安全联动机制进行系统规范，确保标准内容具有理论依据和工程支撑。

（2）规范性原则

标准严格依据国家标准化工作要求进行编写，标准结构完整、术语统一、逻辑清晰，符合团体标准编写规范。

（3）适用性原则

标准紧密结合城市综合能源系统、电力调度控制系统、新能源综合能源管理系统、电力物联网等实际应用需求，重点突出工程应用与落地实施能力，具有较强实用性。

（4）协调性原则

标准与现行国家标准、行业标准及网络安全相关规范保持协调一致，不存在冲突和重复，能够与现有电力监控系统安全体系有效衔接。

（5）先进性原则

标准充分结合当前新型电力系统、能源互联网、工业互联网安全及智能运维的发展趋势，融合状态估计分析、时间序列预测、深度包检测、大数据关联分析、态势感知等先进技术，体现较强技术先进性。

2.主要内容的说明

本标准主要规定了电力系统在数据异常及信息网络攻击情况下的应用模型、处置方法和安全策略要求，包括数据异常处置、网络攻击检测与处置、风险评估、安全防护、事件响应与恢复等内容。

标准主要技术内容包括：

（1）范围

明确本标准适用于城市综合能源系统、电力调度控制系统、新能源综合能源管理系统、电力物联网等数字化系统的数据异常监测、网络安全监测与风险评估。

（2）术语和定义

对“数据异常”“信息网络攻击”“风险评估”“入侵检测系统”“潮流数据”等术语进行了统一定义，为标准实施提供统一技术依据。

（3）应用模型

构建“感知—分析—评估—防御”四层逻辑架构，包括数据采集与处理层、智能检测分析层、风险评估层及安全防护响应层，实现能源运行状态与网络安全态势的融合管理。

（4）处置方法

数据异常处置以状态估计残差分析、规则校验、时间序列预测、多元相关分析等方法为基础，实现异常识别、记录、告警和辅助处置。

网络攻击检测与处置采用特征匹配、异常行为分析、深度包检测（DPI）及日志关联分析等方法，实现攻击识别、风险提示和事件响应。

（5）风险评估

建立风险评分模型，对异常事件及攻击行为进行风险量化分析，并结合风险等级划分实现动态风险管理。

（6）拓扑展示内容设计

建立可视化拓扑展示平台，通过潮流监测、异常告警、风险评估等信息的集中展示，实现电力运行状态与网络安全态势的可视化管理。

（7）安全策略

提出网络分区隔离、访问控制、安全监测部署、冗余与容错设计、定期安全审查等安全防护措施。

（8）事件响应与恢复

建立告警通知、隔离切换、故障甄别与溯源、恢复与验证等全过程应急响应机制，提高电力系统面对异常事件和网络攻击时的快速响应与恢复能力。

3.解决的主要问题

本标准主要解决以下问题：

（1）电力系统运行过程中数据异常监测与处置缺乏统一规范的问题。

（2）传统电力监控系统网络攻击检测与运行监测分离的问题。

（3）城市综合能源系统缺少统一安全态势感知与风险评估机制的问题。

（4）异常数据、网络攻击及风险评估缺少统一联动处置机制的问题。

（5）电力运行安全与网络安全融合治理标准缺失的问题。

通过本标准的制定与实施，可进一步提升电力系统数据异常检测能力、网络攻击识别能力及风险防控能力，提高城市综合能源系统安全运行水平。

三、主要试验（或验证）情况

为验证本标准技术内容的合理性、完整性及工程适用性，标准起草组结合电力系统运行特征和网络安全防护需求，依托面向城市综合能源系统网络攻击监测与安全防护平台原型系统，围绕数据异常检测、网络攻击检测、风险评估及安全联动处置等关键技术内容开展了验证分析。

验证工作以典型电力系统运行场景为基础，结合城市综合能源系统、电力调度控制系统、新能源综合能源管理系统及电力物联网等应用环境，构建覆盖数据采集层、分析处理

层、风险评估层及响应处置层的验证体系，对标准规定的技术要求进行了系统性验证。

（一）数据异常检测验证

针对标准第 5 章规定的数据异常检测方法，重点围绕状态估计残差分析、规则校验与阈值判别、时间序列分析与预测、多元相关分析等技术路线开展验证。

验证过程中，模拟电力系统运行过程中可能出现的数值越限异常、时序失准异常、逻辑矛盾异常及数据缺失异常等典型场景，对异常识别能力、异常定位能力及异常告警能力进行了验证分析。

验证结果表明，标准提出的数据异常检测流程能够实现对电力系统运行数据异常状态的有效识别，能够满足电力系统运行监测及异常预警需求，为后续风险分析和安全处置提供可靠的数据支撑。

（二）网络攻击检测验证

针对标准规定的网络攻击检测要求，结合工业控制系统网络安全特点，围绕特征匹配检测、异常行为分析、深度包检测（DPI）及日志关联分析等技术方法开展验证。

验证内容涵盖拒绝服务攻击（DDoS）、端口扫描、命令注入、ARP 欺骗、恶意软件传播、虚假数据注入等典型网络攻击场景，通过构建攻击事件模拟环境，对攻击识别能力、告警响应能力及攻击溯源能力进行了验证。

验证结果表明，标准提出的网络攻击检测机制能够有效支撑电力监控系统网络安全监测需求，实现对典型网络攻击行为的识别、告警及风险提示，为安全事件快速处置提供技术依据。

（三）风险评估验证

针对标准提出的风险评估模型及风险等级划分方法，围绕风险因子识别、风险评分计算、风险等级划分及风险报告生成等内容开展验证。

验证过程中，结合数据异常事件及网络攻击事件信息，对不同风险场景进行了综合评估分析，并对风险等级划分结果与实际风险状况的一致性进行了验证。

验证结果表明，标准建立的风险评估方法能够较好反映电力系统运行风险和网络安全风险状态，具备较好的工程适用性和可操作性，可为运行单位开展风险管理工作提供技术支撑。

（四）安全联动机制验证

针对标准提出的“检测—评估—响应”闭环管理机制，开展异常事件联动处置验证。

通过模拟异常数据触发、攻击事件告警、风险等级变化及安全策略联动等典型过程，

对告警通知、事件分析、风险评估、隔离控制、恢复验证等环节进行了全过程验证。

验证结果表明，本标准建立的数据异常检测、网络攻击检测、风险评估及安全响应联动机制能够实现信息共享与协同处置，提高异常事件发现效率和风险处置效率，具备良好的工程实施基础。

综上验证结果表明，本标准提出的数据异常检测方法、网络攻击检测机制、风险评估模型及安全联动处置流程具有较好的科学性、合理性和工程适用性，能够满足城市综合能源系统、电力调度控制系统、新能源综合能源管理系统及电力物联网等场景的数据异常检测与安全防护需求。

四、标准中涉及专利的情况。

本标准是基于广东电网有限责任公司科技项目“城市综合能源信息物理系统数据异常及网络攻击安全防护技术”（项目编号：031900KC23120066）的研究成果转化形成的。项目执行期间，已围绕本标准涉及的电力系统数据异常检测、虚假数据注入攻击识别、风险评估及安全防护等关键技术方向申请了多项发明专利。

经标准起草单位评估，以下专利申请内容与本标准技术条款存在关联：

序号	专利申请号	专利名称
1	202411539900.3	一种电力系统中应对攻击的评估方法、系统、计算机设备和存储介质
2	202411609902.5	一种电力系统中针对负载-频率控制的最优虚假数据注入攻击方法和系统
3	202510208351.X	一种基于垂直联邦学习的配电网络虚假数据注入攻击检测方法
4	202510217671.1	一种基于鲁棒图自编码器的电网虚假数据注入攻击识别方法
5	202510378512.X	一种基于自适应数据融合的受攻击电网状态估计与控制方法
6	202510388137.7	一种基于对抗性人工智能的电网交流状态估计中盲虚假数据注入攻击方法
7	202510832560.1	一种信息物理电力系统韧性提升优化系统及方法
8	202510951025.8	一种电力系统虚假数据注入攻击防御方法
9	202511174535.5	一种动态线路评级系统的虚假数据注入攻击实时防

		护方法
10	202511200132.3	一种基于 SHAP-LUNAR 的电网中数据攻击防护方法

五、预期达到的社会效益、对产业发展的作用等情况

本标准实施后，将对电力系统安全运行、网络安全防护、能源数字化建设及行业标准化发展产生积极推动作用，具有显著的技术价值、经济价值和社会价值。

（一）提升电力系统安全运行水平

通过建立统一的数据异常检测与处置技术要求，规范电力系统异常数据识别、分析、预警和处置流程，提高电力系统对异常运行状态的发现能力和风险预警能力，降低异常数据对系统安全稳定运行造成的影响。

（二）提升网络安全防护能力

通过构建数据异常检测与网络攻击检测协同分析机制，实现运行安全与网络安全融合监测，提高对网络攻击、异常行为及潜在安全威胁的识别能力，增强关键基础设施安全防护水平。

（三）推动新型电力系统建设

本标准符合新型电力系统数字化、智能化发展方向，可为数字电网、综合能源系统、能源互联网及新型能源基础设施建设提供统一技术依据和标准支撑，促进能源行业数字化转型升级。

（四）促进电力行业标准化建设

本标准围绕数据异常检测、网络攻击检测、风险评估及安全联动处置等关键技术内容形成统一规范，有助于推动相关技术成果标准化、规范化和工程化应用，完善电力行业标准体系建设。

（五）提升企业风险管控能力

通过建立统一的风险识别、风险评估和风险响应机制，提高运行单位对异常事件和网络安全事件的综合管理能力，降低因设备故障、数据异常及网络攻击导致的经济损失和运行风险。

（六）增强能源基础设施安全保障能力

电力系统作为国家重要基础设施，其安全稳定运行关系国计民生。本标准的实施有助于提升能源基础设施安全防护能力，提高应对复杂运行环境和网络安全威胁的能力，对维护社会公共安全和能源安全具有重要意义。

（七）促进科研成果转化应用

本标准将相关研究成果转化为可推广、可实施、可复制的技术规范，有助于推动产学研用深度融合，加快先进技术成果在电力行业中的落地应用，促进相关产业高质量发展。

六、与国际、国外对比情况

目前，国际上围绕工业控制系统安全、关键基础设施保护及能源系统网络安全已形成一系列技术标准和指导文件，主要包括 IEC 62443 工业自动化与控制系统网络安全系列标准、NIST SP 800-82 工业控制系统安全指南、NERC CIP 北美电力可靠性关键基础设施保护标准以及 ISO/IEC 27019 能源行业信息安全管理规范等。

上述标准主要从工业控制系统安全管理、网络安全防护、身份认证、访问控制、风险管理及关键基础设施保护等方面提出要求，为能源行业网络安全建设提供了重要参考。

经对比分析发现，现有国际标准主要关注工业控制系统网络安全管理体系建设和关键基础设施安全保护要求，对于电力系统运行数据异常检测、网络攻击检测、风险评估及联动处置一体化技术要求尚缺少针对性规范。

本标准充分结合我国新型电力系统建设需求以及城市综合能源系统运行特点，重点构建了“数据异常监测与处置—网络攻击检测与响应—风险评估—安全策略”的协同技术体系，实现运行安全与网络安全的融合管理。

与现有国际标准相比，本标准具有以下特点：

（一）面向电力系统运行场景，突出电力行业专业特点；

（二）实现数据异常检测与网络攻击检测协同分析；

（三）建立风险评估与安全响应联动机制；

（四）强化运行安全与网络安全融合治理理念；

（五）兼顾工程实施可行性和实际应用需求。

本标准未采用国际标准，也未修改采用国际标准。但在标准编制过程中充分参考了国际先进技术理念和相关标准体系成果，并结合我国法律法规、行业管理要求及工程实践需求进行了适应性完善，形成了适用于我国电力系统和城市综合能源系统的数据异常检测与安全防护技术规范。

总体来看，本标准具有较好的先进性、适用性和工程实践价值，可为我国新型电力系统和能源数字化建设提供技术支撑。

七、与现行相关法律、法规、规章及标准，特别是强制性标准的协调性

本标准符合《中华人民共和国网络安全法》《中华人民共和国数据安全法》《关键信

息基础设施安全保护条例》等法律法规要求。

同时，本标准与以下标准保持协调一致：

GB/T 18336—2015《信息技术 安全技术 信息技术安全评估准则》

GB/T 25069—2022《信息安全技术 网络安全等级保护基本要求》

GB/T 36572—2018《电力监控系统网络安全防护技术要求》

DL/T 1455—2015《电力系统控制类软件安全性测评技术要求》

DL/T 1970—2019《电力系统数据质量评价规范》

DL/T 2277—2021《电力监控系统网络安全风险评估规范》

本标准是在现有标准基础上的细化与补充，与现行法律法规及相关标准不存在冲突。

八、重大分歧意见的处理经过和依据

在标准起草过程中，起草组针对风险评估模型、攻击检测范围、风险等级划分、拓扑展示内容及安全策略要求等问题进行了充分讨论，并结合行业专家意见进行了修改完善。

相关意见主要集中于：

（1）风险等级划分标准的合理性；

（2）网络攻击检测范围的覆盖程度；

（3）数据异常与网络攻击联动机制的实现方式；

（4）拓扑展示界面的信息密度与可读性；

（5）安全策略与工程实施可行性的协调问题。

起草组通过专题讨论、技术论证及行业调研，对相关内容进行了统一协调，目前未形成重大分歧意见。

九、标准性质的建议说明

建议本标准作为推荐性团体标准发布实施。

十、贯彻标准的要求和措施建议

建议标准发布后，由相关行业协会、科研机构、电力企业及网络安全技术单位联合开展标准宣贯和培训工作，提高标准应用水平。

建议结合实际工程项目开展试点应用，逐步完善相关配套技术体系和实施方案。

建议建立标准实施反馈机制，根据技术发展和行业需求适时开展标准修订工作。

建议推动标准在城市综合能源系统、新型电力系统及能源互联网等场景中的推广应用。

十一、废止现行相关标准的建议

经调研分析，目前尚无与本标准适用范围、技术内容及应用对象完全一致的国家标准、行业标准或团体标准。

本标准是在现有电力系统数据质量管理、网络安全防护及风险评估相关标准基础上的补充和细化，与现行标准不存在替代关系，也不存在重复和冲突情况。

因此，本标准发布实施后，不涉及废止任何现行标准。

十二、其他应予说明的事项

（一）本标准为首次制定。

（二）本标准未采用国际标准，也未采用国外先进标准。

（三）本标准编制过程中充分参考了现行法律法规、国家标准、行业标准以及相关技术资料，确保标准内容与现行标准体系保持协调一致。

（四）截至本标准编制说明形成之日，未发现本标准涉及必须披露的专利内容。如后续发现相关专利事项，将按照国家有关规定进行处理。

（五）本标准为推荐性团体标准，供相关单位结合实际情况自愿采用。

（六）标准实施后，建议结合工程应用情况持续收集实施反馈，根据技术发展和行业需求适时开展修订完善工作。

《电力系统数据异常处置规范》标准工作组

2026 年 6 月 1 日