ICS 35.240.01
CCS L 73

T/EJCCCSE

团　　体　　标　　准

T/EJCCCSE XXXX—XXXX

考虑不确定性的源网荷储协同优化调度系统

Source-grid-load-storage coordinated optimal dispatch system considering uncertainty.

（征求意见稿）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国商业股份制企业经济联合会　　发 布

目　　次

前　言

本文件按照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。

本文件由北京清能互联科技有限公司提出。

本文件由中国商业股份制企业经济联合会归口。

本文件起草单位：北京清能互联科技有限公司。

本文件主要起草人：

考虑不确定性的源网荷储协同优化调度系统

1 范围

本文件规定了考虑不确定性的源网荷储协同优化调度系统的系统平台、应用功能、性能指标、安全防护。

本文件适用于考虑不确定性的源网荷储协同优化调度系统（以下简称“系统”）。

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 12991.1 信息技术 数据库语言 SQL 第1部分:框架

GB/T 22239 信息安全技术 网络安全等级保护基本要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

考虑不确定性的源网荷储协同优化调度系统

对不确定性的刻画与分层逐级消除的各个环节，能够对可再生能源波动等随机性因素引发的安全风险进行量化建模，在风险量化可控前提下给出最优调度决策，为电力系统分析与运行控制提供关键信息支撑。

3.2

通信总线

提供可靠通用的信息交互机制和广域服务机制，实现应用程序之间安全高效的数据通信。

3.3

权限服务

为各个应用提供统一的用户与组织管理服务、资源管理服务、角色管理服务、授权管理服务。

3.4

数据管控理

对风险调度优化计算所需要各类外部数据及市场参数进行集中管理与维护，为后续市场出清计算提供准确、可靠的输入数据。

3.5

源荷不确定评估

基于源荷概率预测技术和资源聚合技术，分析风电、光伏等新能源出力以及负荷的概率分布特性。利用曲线图或者折线图等可视化工具展示源荷出力的预测情况，结合预测误差概率分布特性等统计指标分析源荷预测误差情况，使用出力置信度、条件概率密度等各类不确定性表征参数对出力不确定性进行分析和可视化展示，形象展示和刻画新能源、负荷等的运行特性及多态不确定性。

4 系统平台

4.1 平台架构

系统平台包括数据存储与管理、通信总线、公共服务、人机交互、系统监视与管理等。

4.2 数据存储与管理

4.2.1 关系数据库

4.2.1.1 应使用安全可控数据库。
4.2.1.2 支持遵循 GB/T 12991.1 规定的各类数据类型。
4.2.1.3 支持遵循 GB/T 12991.1 规定的 E-R 关系建模和各类数据操作。
4.2.1.4 提供图形化和命令行的数据库管理工具。
4.2.1.5 提供性能监视和异常报警 API 接口。
4.2.1.6 支持数据库备份和恢复。
4.2.1.7 服务端和客户端均应具有记录日志的能力。
4.2.1.8 满足市场数据持久化保存的要求。
4.2.1.9 应具备加密存储功能。

4.2.2 实时数据库

4.2.2.1 应使用安全可控数据库。
4.2.2.2 支持实时数据的关系描述。
4.2.2.3 具备快速存储和访问能力，提供本地访问接口和远程服务访问接口。
4.2.2.4 提供图形化和命令行方式的数据库管理工具。
4.2.2.5 提供性能监视和异常报警 API 接口。
4.2.2.6 支持实时数据跨安全区同步。
4.2.2.7 服务端和客户端均应具有记录日志的能力。

4.2.3 键值型数据库

4.2.3.1 应使用安全可控数据库。
4.2.3.2 支持键值区分。
4.2.3.3 具备快速存储和访问能力，提供本地访问接口和远程服务访问接口。
4.2.3.4 提供图形化和命令行方式的数据库管理工具。
4.2.3.5 提供水平扩展能力。
4.2.3.6 支持数据跨安全区同步。
4.2.3.7 服务端和客户端均应具有记录日志的能力。

4.3 通信总线

4.3.1 消息总线

4.3.1.1 支持各类实时数据和事件的快速传递。
4.3.1.2 提供消息收发服务，支持不同类型消息的订阅和发布。
4.3.1.3 接收方可根据各自的需求进行消息处理，消息收发互不影响。
4.3.1.4 支持主机间和主机内部进程间的消息传递。
4.3.1.5 支持点对点、一点对多点的消息传递。
4.3.1.6 支持消息注册/撤销，消息发送/接收，消息发布/订阅。
4.3.1.7 支持消息的高可用。

4.3.2 服务总线

4.3.2.1 支持服务的接入和访问。
4.3.2.2 支持应用请求/响应和订阅/发布两种模式的服务访问。
4.3.2.3 支持对服务的查询、监控和定位。
4.3.2.4 支持以命令行或界面方式查询服务有关信息，查询内容包括但不限于：服务位置、服务描述、服务类型、服务当前状态。
4.3.2.5 支持系统间广域数据发送与接收。

4.4 公共服务

4.4.1 统一数据访问服务

4.4.1.1　具备跨编程语言、跨平台能力。
4.4.1.2　支持统一、可定制的数据交换格式，支持按列或按行的取数场景。
4.4.1.3　支持的数据类型包括：结构化数据、半结构化数据和非结构化数据。
4.4.1.4　支持的数据库类型包括但不限于：关系数据库、实时数据库和键值型数据库。

4.4.2　电网统一模型服务

4.4.2.1　支持提供统一模型访问接口从模型数据平台获取电网模型。
4.4.2.2　支持按照设定的电网边界获取剪裁后的电网模型。
4.4.2.3　支持获取未来态电网模型信息。

4.4.3　日志服务

4.4.3.1　日志采集

4.4.3.1.1　应提供统一的日志采集接口，支持方便、快捷地写入日志。
4.4.3.1.2　应提供标准的日志格式，规范和格式化日志数据。

4.4.3.2　日志存储

4.4.3.2.1　根据时效性的不同，支持不同的数据存储方式。
4.4.3.2.2　支持近期数据存储，可按月、按周、按天等设置存储周期。
4.4.3.2.3　支持近期数据存储时限设置，自动清理过期数据。
4.4.3.2.4　支持历史数据存储，可持久化存储日志数据。

4.4.3.3　日志查询

4.4.3.3.1　应提供统一的日志数据在线查询界面。
4.4.3.3.2　应支持自定义的查询条件。

4.4.4　权限服务

4.4.4.1　用户管理服务

4.4.4.1.1　人员信息包括但不限于：姓名、身份证号码、手机号码、所在单位与部门、系统访问限制、人员状态、登录名、密码，具备扩展属性。
4.4.4.1.2　用户组织信息包括但不限于：组织编号、组织名称、父级组织、组织地址、组织性质，具备扩展属性。
4.4.4.1.3　支持对用户与组织的新建、编辑和删除。

4.4.4.2　资源管理服务

4.4.4.2.1　资源属性包含但不限于资源名称、资源编号、资源类型，具备扩展属性。
4.4.4.2.2　提供资源新建、编辑和删除。

4.4.4.3　角色管理服务

4.4.4.3.1　具备角色定义功能，分配角色具有的资源集合。
4.4.4.3.2　角色信息应包括但不限于：角色名称、角色编号、角色类型。
4.4.4.3.3　支持对角色新建、编辑和删除。

4.4.4.4　授权管理服务

4.4.4.4.1　用户管理员根据用户的实际权限，授权分配相应的角色。
4.4.4.4.2　用户管理员审核用户的待分配角色。

4.4.5　文件服务

4.4.5.1　文件管理

4.4.5.1.1　文件管理应提供文件的创建、修改、读取、删除、查询、重命名、复制等功能。

4.4.5.1.2　目录管理应提供目录的创建、删除、查询、重命名等功能。
4.4.5.1.3　支持对文件和目录的操作设置权限控制。

4.4.5.2　文件同步

4.4.5.2.1　应支持跨安全区同步。
4.4.5.2.2　应支持目录级文件过滤同步。
4.4.5.2.3　应支持对同步文件的断点续传和内容校验。
4.4.5.2.4　应支持文件同步任务。

4.4.6　报表服务

4.4.6.1　报表填报

4.4.6.1.1　应提供标准的数据表格用于数据填报。
4.4.6.1.2　应提供常用的报表填报控件，支持但不限于文本框、文本域、数字控件、日期控件、文件控件、列表控件等表单控件。
4.4.6.1.3　应支持填报控件属性校验，如非空、数字、规则库等校验规则。
4.4.6.1.4　支持报表数据分权限填报，支持单元格的编辑权限。

4.4.6.2　报表查询

4.4.6.2.1　支持多条件组合高级查询，查询条件包括：报表分类、展示形式、时间范围等。
4.4.6.2.2　报表查询结果支持以数据列表或文件两种方式返回。

4.4.6.3　数据处理

4.4.6.3.1　应支持对报表数据进行数据整合、数据加工及计算。
4.4.6.3.2　应支持数据处理定时任务管理，支持定时任务对数据进行处理、存储和监视。
4.4.6.3.3　应支持报表数据存储。

4.4.6.4　分析展示

4.4.6.4.1　应支持自定义分析指标。
4.4.6.4.2　应提供多种报表展示方案，包括列表式报表、分组报表、交叉报表、自由报表、组合报表。
4.4.6.4.3　应支持分主题、分类型等多种条件的数据钻取。
4.4.6.4.4　应支持将报表导出为常见文档处理工具文件格式。
4.4.6.4.5　应提供报表配置服务，支持设置报表的生成时间、展示方式和刷新频率。

4.4.6.5　报表打印

应支持报表数据的在线打印，可设置打印属性，如份数、边距等。

4.4.7　时间同步服务

4.4.7.1　支持的时钟源包括但不限于：GPS、北斗二代，可人工指定系统的主用时钟信号来源，支持对时钟信号源的人工切换，切换操作应简便易行。
4.4.7.2　当主时钟源、连接主时钟的机器或者处理主时钟信号的进程出现故障时，应支持时钟源的自动切换。
4.4.7.3　当两个外部时钟源的误差超过设定门槛值、或任意卫星信号接收失败时应发出告警。
4.4.7.4　外部时钟源的时间与系统时间差距超过门槛值时，应放弃与外部时钟的对时，避免系统对时受到影响，同时发出告警。
4.4.7.5　系统内各服务器和工作站应采用 NTP 协议与处理主时钟信号的应用所在机器对时，对时频率不超过 60 次/秒，对时偏差不超过 100 ms。

4.5　人机交互

4.5.1　画面显示

4.5.1.1 支持各应用模块的画面显示，并可灵活切换。
4.5.1.2 支持图形整体及部分区域的缩放和滚动。
4.5.1.3 支持画面的前进、后退，可设定画面主页。
4.5.1.4 支持画面动态数据点的自动刷新。
4.5.1.5 支持在任意工作站的任一监视器的任一窗口上调用任何画面。
4.5.1.6 支持在不同工作站、不同监视器和不同窗口上同时调用和显示同一幅画面。

4.5.2 用户输入与操作

4.5.2.1 应支持通过快捷键进行快速调用与操作。
4.5.2.2 操作应简便易行，常见基础业务单元的操作步骤不超过 3 步，如：画面切换、市场出清、信息录入、数据导出等。
4.5.2.3 用户输入与控制应具有完善的权限控制与管理机制。

4.6 系统监视与管理

4.6.1 系统资源管控

4.6.1.1 应具备对软硬件资源使用情况和业务软件的运行情况监视和记录的功能，并可灵活定义资源使用的告警阀值，超过阈值将发送告警事件。
4.6.1.2 能够自动处置严重故障，保证系统核心业务正常运行。

4.6.2 进程监视与管理

4.6.2.1 应具备实时监视和管理应用进程的运行情况的功能，保证整个系统的正常运行。
4.6.2.2 应具备必要的时候重新启动进程，并实时向系统报告进程运行的状态，使系统可以正确判断出当前进程的运行状态。

4.6.3 应用监视与管理

4.6.3.1 应提供应用的启停、监控和管理工具，实时监视和管理应用的整体运行情况的功能，保证整个系统的正常运行。
4.6.3.2 应支持实时监视应用运行状态并在出现异常时进行告警通知。
4.6.3.3 支持应用主备机切换、应用启停等操作。

4.6.4 流程管理

4.6.4.1 支持设定审批信息，包括审批级数、参与审批流程的账户。
4.6.4.2 支持审批操作，包含建立审批单、审批时间记录、审批意见记录、审批状态进展、审批流转情况等。
4.6.4.3 支持对流程状态的监视及流程可视化展示。

4.6.5 用户权限管理

4.6.5.1 支持系统用户查看和设置不同类型用户的数据查询权限。
4.6.5.2 支持系统用户查看和设置不同类型用户的数据导出权限。
4.6.5.3 支持系统用户查看和设置不同类型用户的业务权限。
4.6.5.4 支持系统用户查看账号拥有的权限范围。

5 应用功能

5.1 模型管理

5.1.1 机组管理

5.1.1.1 支持对发电机组（机组群）进行新增、修改、删除等操作。
5.1.1.2 支持对发电机组的装机容量、最大最小技术出力、爬坡速率、最小连续开停时间、启停曲线、机组开停通知时间等参数进行管理。

5.1.1.3　支持对机组群最大出力、最小出力、发电量、开机台数等参数进行管理。
5.1.1.4　支持对机组（机组群）的管理操作进行日志记录，记录内容至少包括操作人、操作时间、操作内容、操作机器等信息。

5.1.2　储能管理

5.1.2.1　支持对独立储能、抽水蓄能进行新增、修改、删除等操作。
5.1.2.2　支持对独立储能、抽水蓄能的装机容量、最大最小技术出力、最小运行时间、最小停机时间等参数进行管理。
5.1.2.3　支持对独立储能、抽水蓄能的管理操作进行日志记录，记录内容至少包括操作人、操作时间、操作内容、操作机器等信息。

5.1.3　负荷管理

5.1.3.1　持对负荷关联的电网物理节点进行管理维护。
5.1.3.2　支持对负荷信息的管理操作进行日志记录，记录内容至少包括操作人、操作时间、操作内容、操作机器等信息。

5.1.4　联络线管理

5.1.4.1　支持对联络线信息进行管理，维护联络线首末端厂站及送受端电网。
5.1.4.2　支持对联络线信息的管理操作进行日志记录，记录内容至少包括作人、操作时间、操作内容、操作机器等信息。

5.2　数据管理

5.2.1　系统负荷预测数据管理

5.2.1.1　支持对短期系统负荷预测、超短期系统负荷预测数据进行查询、修改、删除等操作。
5.2.1.2　支持系统预测负荷与系统实际负荷对比展示。
5.2.1.3　支持根据历史实测数据和相似日实测数据复制生成。
5.2.1.4　支持对系统负荷预测数据操作进行日志记录，记录内容至少包括操作人、操作时间、操作内容、操作机器等信息。
5.2.1.5　支持基于文件的数据导入导出功能。

5.2.2　母线负荷预测数据管理

5.2.2.1　支持对短期母线负荷预测、超短期母线负荷预测数据进行查询、修改、删除等操作。
5.2.2.2　支持母线预测负荷与母线实际负荷对比展示。
5.2.2.3　支持根据历史实测数据和相似日实测数据复制生成。
5.2.2.4　支持对母线负荷预测数据操作进行日志记录，记录内容至少包括操作人、操作时间、操作内容、操作机器等信息。
5.2.2.5　支持基于文件的数据导入导出功能。

5.2.3　联络线计划数据管理

5.2.3.1　支持对日前联络线计划、实时联络线计划数据进行查询、修改、删除等操作。
5.2.3.2　支持根据历史实测数据和相似日实测数据复制生成。
5.2.3.3　支持对联络线计划数据操作进行日志记录，记录内容至少包括操作人、操作时间、操作内容、操作机器等信息。
5.2.3.4　支持基于文件的数据导入导出功能。

5.2.4　检修计划数据管理

5.2.4.1　支持对日前、临时机组检修计划数据进行查询、修改、删除等操作。
5.2.4.2　支持对日前、临时输变电设备检修计划数据进行查询、修改、删除等操作。
5.2.4.3　支持对检修计划数据操作进行日志记录，记录内容至少包括操作人、操作时间、操作内容、操作机器等信息。

5.2.4.4　支持基于文件的数据导入导出功能。

5.2.5　机组固定出力数据管理

5.2.5.1　支持对日前固定出力、实时固定出力计划数据进行查询、修改、删除等操作。
5.2.5.2　支持根据历史数据和相似日数据复制生成。
5.2.5.3　支持对固定出力数据操作进行日志记录，记录内容至少包括操作人、操作时间、操作内容、操作机器等信息。
5.2.5.4　支持基于文件的数据导入导出功能。

5.2.6　机组可调范围数据管理

5.2.6.1　支持对日前可调出力范围、实时可调出力范围数据进行查询、修改、删除等操作。
5.2.6.2　支持根据历史数据和相似日数据复制生成。
5.2.6.3　支持对机组可调范围数据操作进行日志记录，记录内容至少包括操作人、操作时间、操作内容、操作机器等信息。
5.2.6.4　支持基于文件的数据导入导出功能。

5.2.7　新能源功率预测数据管理

5.2.7.1　支持对短期、超短期新能源功率预测数据进行查询、修改、删除等操作。
5.2.7.2　支持根据历史数据和相似日数据复制生成。
5.2.7.3　支持对新能源功率预测数据操作进行日志记录，记录内容至少包括操作人、操作时间、操作内容、操作机器等信息。
5.2.7.4　支持基于文件的数据导入导出功能。

5.2.8　风险调度配置参数管理

5.2.8.1　支持对风险调度参数进行管理、配置。
5.2.8.2　支持根据风险调度参数用途进行分类管理，参数类别至少包括基本参数、潮流安全分析计算参数、优化计算参数、约束设置参数等。
5.2.8.3　支持风险调度参数的查询、新增、删除、修改等操作。
5.2.8.4　支持对风险调度配置参数操作进行日志记录，记录内容至少包括操作人、操作时间、操作内容、操作机器等信息。

5.3　源荷不确定评估

5.3.1　源荷出力数据管理

5.3.1.1　支持查看单个或多个风电场及光伏电站的短期和超短期历史预测出力和历史实际出力数据。
5.3.1.2　支持查看短期和超短期历史负荷预测和历史实际负荷数据。
5.3.1.3　支持查看选定时间段的风光历史预测出力和历史实际出力数据、历史负荷预测和历史实际负荷数据。
5.3.1.4　支持向概率预测算法和场景生成算法提供相关数据。

5.3.2　源荷出力不确定性分析

5.3.2.1　支持对概率预测算法参数入参文件及出参文件下载。
5.3.2.2　支持对概率预测算法进行管理、配置，参数类别至少包括历史数据开始日、置信度、场景数、典型场景数、极端场景数等。
5.3.2.3　支持执行概率预测算法对短期和超短期的风光出力及负荷进行预测。
5.3.2.4　支持可视化形式展示可选时间段内不同置信度的风光出力、负荷的实际数据和预测数据。
5.3.2.5　支持对源荷出力不确定性分析参数操作进行日志记录，记录内容至少包括操作人、操作时间、操作内容、操作机器等信息。

5.4　源荷场景生成

5.4.1　支持新增自定义场景、导入本地文件场景、导入模板场景等。

5.4.2 支持对自定义推演场景参数进行管理、配置，参数类别至少包括场景日期、场景名称、基准场景选择、场景批量调整、场景页面数据展示等。
5.4.3 支持对场景生成算法参数入参文件及出参文件下载。
5.4.4 支持对场景生成算法参数进行管理、配置，参数类别至少包括历史数据开始日、置信度、典型场景、典型场景数、极端场景数等。
5.4.5 支持执行场景生成算法生成源荷抽样场景。
5.4.6 支持可视化形式展示不同时间段内不同场景下的风光出力、负荷的数据，并支持查询抽样场景方案详情和添加到自定义场景。
5.4.7 支持场景生成算法操作进行日志记录，记录内容至少包括操作人、操作时间、操作内容、操作机器等信息。

5.5 日前风险调度优化

日前风险调度优化功能实现运行日前一天(D-1日)进行的决定运行日(D日)资源计划的优化计算，基于电力市场机制和新型电力系统不确定性下的网源荷储资源协同调控模型和高效求解技术,实现日前风险调度协调优化。日前风险调度优化功能采用案例的模式，支持多使用者多案例同时优化，最终选择结果最合理的案例进行发布，包括以下功能：

a) 案例管理：提供案例信息的统一管理入口，可以进行案例新增和修改，同时支持同步案例数据。
b) 案例模型数据：用于可视化展示送给算法组装的相关约束信息，便于排查问题。按照配置约束的优先级，组织对应算法的各类输入数据用于查看。包括：电网模型参数、电源模型参数、负荷模型参数、储能参数模型等。
c) 案例边界数据：用于展示和修改送给算法组装的相关边界信息。包括：申报数据、预测数据、计划数据、约束数据、计算参数等。
d) 日前风险调度优化计算：日前风险调度优化页面可进行执行计算操作，支持监视当前案例所处环节，展示计算进程与计算中日志信息。
e) 日前优化计算结果：以图表形式展示负荷、供给以及全天电力电量平衡情况。包括：电力平衡、资源优化结果、市场交易结果、潮流优化结果等。

5.6 实时风险调度优化

实时风险调度优化功能根据最新电网运行状态和风险预警信息，每 15 min（周期可设置为 5 min 或 15 min）滚动计算未来 15 min 至 4 h（时间可设置）资源计划，包括案例管理、实时调度优化状况监视、优化计算、结果分析等功能，提高各类资源调度计划编制的科学性。

a) 案例管理：提供案例信息的统一管理入口，可以进行案例新增和修改，同时支持同步案例数据。
b) 案例模型数据：用于可视化展示送给算法组装的相关约束信息，便于排查问题。按照配置约束的优先级，组织对应算法的各类输入数据用于查看。包括：电网物理模型、资源模型参数、市场模型参数、算法参数模型等。
c) 案例边界数据：用于展示和修改送给算法组装的相关边界信息。包括：申报数据、预测数据、计划数据、约束数据、计算参数等。
d) 预处理数据：用于可视化展示送给算法组装的相关约束信息，便于排查问题。按照配置约束的优先级，组织对应算法的各类输入数据用于查看。包括：机组初始状态、机组指定状态、机组固定出力、机组出力限额、预处理配置等。
e) 实时风险调度优化计算：实时风险调度优化页面可进行执行计算操作，支持监视当前案例所处环节，展示计算进程与计算中日志信息。
f) 实时优化计算结果：以图表形式展示负荷、供给以及全天电力电量平衡情况。包括：电力平衡、资源优化结果、市场交易结果、潮流优化结果等。
g) 对比分析：用于对风险调度与确定性调度的结果进行对比分析。包括：对比案例选择、安全性对比分析、经济性对比分析等。

6 性能指标

6.1 总则

6.1.1 技术的先进性

系统配置的方案应采用先进成熟的技术，应保证配置出的系统逻辑结构清晰，易于为系统管理人员所理解。

6.1.2 系统的稳定性要求

6.1.2.1 保证系统能够正常运作。
6.1.2.2 系统应能够 7×24 h 连续不断稳定工作。
6.1.2.3 系统升级或改进应在不影响业务的情况下进行，以保证已有系统和本次新增配置的平稳融合。

6.1.3 系统安全性

6.1.3.1 系统安全性需满足国家发改委 2014 第 14 号令《电力监控系统安全防护规定》及国家能源局文件、国能安全 36 号文《电力监控系统安全防护总体方案》等有关文件要求，为防范黑客及恶意代码等对电力监控系统的攻击侵害，避免由此引发的电力系统事故，保障电力系统的正常稳定运行。
6.1.3.2 应保证实施过程的安全，进而保证实施结果的安全。
6.1.3.3 采用严格的安全体系，保证数据在处理和传输全过程的安全性。
6.1.3.4 系统应该根据安全实体、安全对象、权限、角色、行政区域等进行身份认证之后的统一、有效的权限管理。只有系统管理员有权进行安全权限管理的配置。其他人员均根据各自的角色和所属的安全实体所具有的权限，在规定的行政区域，对规定的安全对象进行规定的操作。

6.2 集中管理

系统应提供集中的管理，以降低管理的成本，提高管理的有效性。

6.3 开发和部署

系统建成后，用户和维护单位应可以进行方便的功能定制、开发、部署与管理。

7 安全防护

7.1 总体安全架构

7.1.1 系统安全防护的目标是防范、抵御黑客及恶意代码等通过各种形式对系统发起的恶意破坏和网络攻击，确保系统数据安全，保障调度系统安全稳定运行。
7.1.2 系统安全防护遵循“安全分区、网络专用、横向隔离、纵向认证”基本原则，在调度中心与交易中心之间应采取对等互信的边界隔离防护措施，构建隔离缓冲区进行数据安全交互，对关键业务数据采取加密签名、安全存储与访问控制措施，强化关键业务数据的安全监管、审计监测和抗抵赖性。加强业务应用安全事件的监视预警、系统运维的安全管控和密码设施的安全管理，提升系统本体和业务终端的安全防护能力。

7.2 边界防护要求

7.2.1 基本要求

边界安全是电力监控系统网络安全防护体系的基础框架，也是所有其它安全防护措施的重要基础。系统边界防护及安全部署如图 1 所示

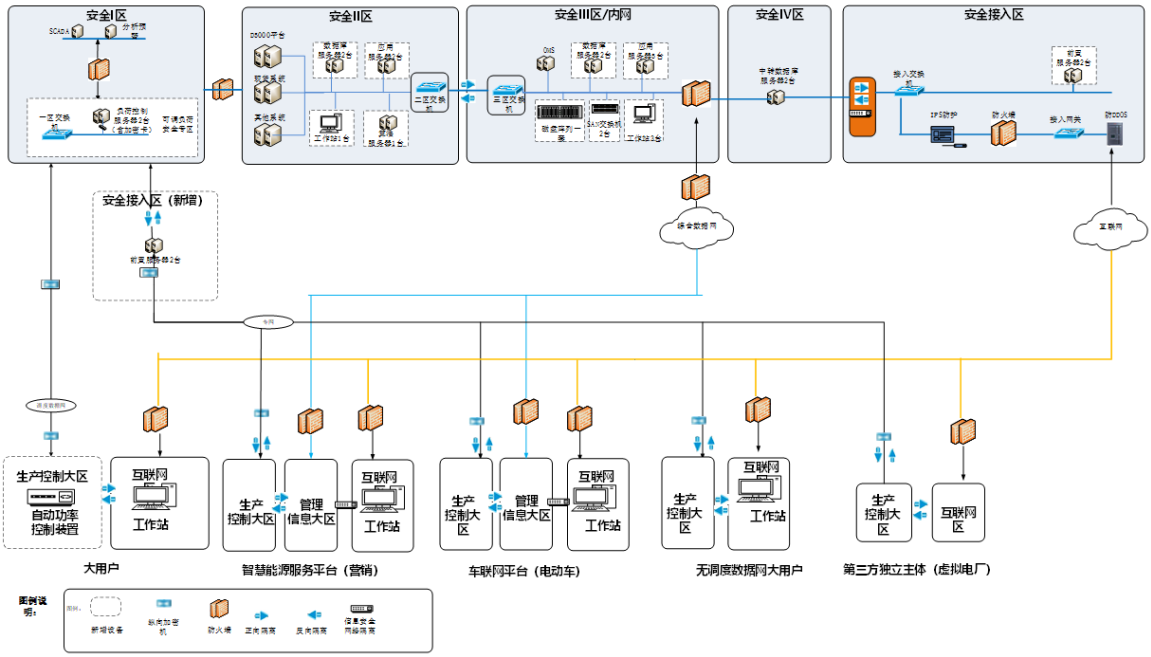

图1　系统边界防护及安全部署典型结构示意图

7.2.2　安全分区

系统涉及安全I区、安全接入区（I区）、安全II区、安全III区和安全接入区（互联网），其安全分区设计如图 2 所示：

a)　系统部署于安全 II 区，接收来自于安全 III 区负荷调控系统的数据，完成风险调度优化计算，并将优化结果发送到安全 I 区负荷调控系统、火电 AGC、新能源 AGC、储能 AGC。

1)　系统与安全 I 区的 SCADA 系统、AGC 系统、负荷调控系统进行数据交互，获取电网模型、机组运行数据、断面控制信息以及实际执行结果，同时向 AGC 系统、负荷调控系统发送实时调度指令；

2)　部署于安全 II 区的系统从新能源综合供电能力预测系统获取新能源出力预测区间数据，从负荷预测系统、调度计划系统、省内/省间现货系统等分别获取母线负荷预测、系统负荷预测、联络线计划、机组发电计划、及省间/省内现货交易结果等数据；

3)　系统与安全 III 区的 OMS 系统等实现数据交互，获取负荷聚合信息、输变电设备检修计划、机组检修计划等数据；

4)　系统从安全 III 区获取短路比结果数据。

b)　负荷调控系统部署于安全 I 区、安全接入区（I 区）、安全 III 区。

1)　负荷调控系统（安全 III 区）：接收有序用电系统中的系统负荷、联络线计划、电力缺口等数据，接收安全接入区的前置互动模块申报数据，将以上数据发送到安全 II 区系统，并接收出清结果；负荷调控系统将有序用电需求发送到有序用电系统，并接收有序用电指令；

2)　负荷控制模块（安全 I 区）：接收网源荷储协同优化出清结果、有序用电等负荷控制指令；将直控大用户的指令通过调度数据网发送到自动功率控制装置；将第三方独立主体（虚拟电厂）的指令通过前置物联模块（安全接入区（I 区））下发执行；接收前置物联模块（安全接入区（I 区））转发的采集信息；

3)　前置物联模块（安全接入区（I 区））：接收负荷控制模块（安全 I 区）的指令，将指令转发到自动功率控制装置；接收自动功率控制装置的采集信息，将采集信息转发到负荷控制模块（安全 I 区）；

4)　前置互动模块（安全接入区（互联网））：接收负荷调控系统（安全 III 区）的发布信息，提供指令查询跟踪、实时监视、中标结果查询等功能；将负荷的申报信息发送到负荷调控系统（安全 III 区）。

c） 自动功率控制装置部署于多元主体的生产控制区，通过调度数据网或专网接收电网调控指令；并采集可调资源状态（功率），上送至安全Ⅰ区的负荷控制模块。

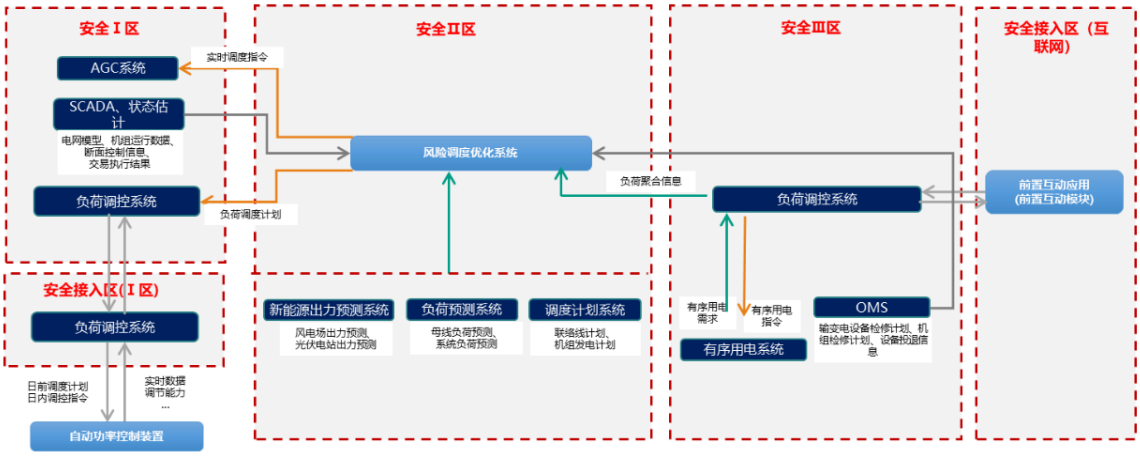

图2 数据架构图

7.2.3 网络专用

7.2.3.1 系统在生产控制大区与其它地区的生产控制大区系统进行通信时，应采用电力调度数据网进行通信。

7.2.3.2 管理信息大区业务应采用电力企业数据网进行通信，电力企业数据网为电力企业内联网。

7.2.4 横向隔离

7.2.4.1 系统在安全Ⅱ区与安全Ⅲ区和隔离缓冲区之间应部署通过国家或行业有关机构检测认证的电力专用横向单向安全隔离装置。

7.2.4.2 在安全Ⅱ区部署的系统在与安全Ⅱ区的其它业务系统之间应部署具有访问控制作用的硬件防火墙或者相当作用的设施，实现逻辑隔离。

7.2.4.3 在安全Ⅲ区部署的系统在与安全Ⅲ区或信息内网的其它业务系统之间应部署具有访问控制作用的硬件防火墙或者相当作用的设施，实现逻辑隔离。

7.2.4.4 在隔离缓冲区部署调度中心与交易中心专用安全接入设施，与交易中心网络之间采用对等隔离措施。

7.2.4.5 在管理信息大区的信息外网与信息内网之间应部署信息网络安全隔离装置等措施。

7.2.5 纵向认证

7.2.5.1 系统在生产控制大区纵向边界处应部署通过国家或行业有关机构检测认证的纵向加密认证装置，通过身份认证、数据加密和访问控制等技术措施，实现业务数据机密性和完整性保护。

7.2.5.2 系统在管理信息大区纵向边界处应采取身份认证、数据加密和访问控制等技术措施，实现业务数据机密性和完整性保护。

7.2.6 隔离缓冲区

7.2.6.1 在管理信息大区可建立隔离缓冲区，采用独立的逻辑隔离措施连通交易中心业务系统网络，通过正反向隔离装置连接生产控制大区。

7.2.6.2 在隔离缓冲区应部署基于可信验证的跨区传输服务，实现交易中心业务与安全Ⅱ区系统业务之间的数据不落地安全传输。

7.2.6.3 在隔离缓冲区应部署恶意代码监测装置和网络安全监测装置，实现对网络流量中的恶意代码进行检测，对内部设备网络安全事件进行统一监视。

7.3 系统本体安全

7.3.1 基本要求

本体安全是构成电力监控系统网络安全防护体系的各个模块应实现自身的安全，系统软硬件应采用安全、可控、可靠的产品，并通过国家有关机构的安全检测认证。

7.3.2 计算机和网络设备安全

7.3.2.1 系统网络安全设施包括网络交换设备（如路由器、交换机等）和网络安全设备（如防火墙、电力专用横向单向隔离装置等），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。
7.3.2.2 关键网络安全设施应提供硬件设备冗余，对设备配置进行安全备份，及时升级安全补丁，禁止选用国家相关部门通报存在漏洞和风险的设备。
7.3.2.3 网络设备和计算机设备使用时应合理配置，启用安全策略，封闭空闲网络端口和其它无用端口，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）。

7.3.3 操作系统和基础软件安全

7.3.3.1 系统设备应采用通过国家或行业有关机构检测认证的安全操作系统、数据库、中间件等基础软件，满足安全可靠要求，并实施严格的访问控制措施，并及时升级安全补丁。
7.3.3.2 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，数据库和操作系统的用户名、口令及其强度应符合 GB/T 22239 的要求。
7.3.3.3 操作系统的管理权限应分别由安全管理员、系统管理员、审计管理员配合实现，并仅授予各用户所需的最小权限。

7.3.4 应用软件安全

7.3.4.1 系统应在设计时融入安全防护理念和措施，业务系统软件应采用模块化总体设计，合理划分各业务模块，并部署于相应安全区，重点保障核心模块安全。
7.3.4.2 系统在生产控制大区的功能模块应采用 C/S 架构；在管理信息大区的功能模块可采用 B/S 架构，但须采用应用层安全防护设施。
7.3.4.3 系统应通过具有测评资质的机构开展安全检测并提供检测报告。
7.3.4.4 系统应采用国家密码管理局认证的密码算法对交易信息进行加密存储及传输，保障交易信息的私密性、完整性和抗抵赖性。
7.3.4.5 应按照用户性质进行实名创建帐号，禁止不同用户间共享帐号，并根据业务需要配置用户帐户所需的最小权限；帐号登录可采用数字证书或生物识别等双因子身份认证措施保障安全性。
7.3.4.6 系统应具有日志审计管理，交易过程应提供可作为法律证据的日志记录，日志记录应采取安全措施保存至少六个月以上。
7.3.4.7 系统中功能模块软件，在部署前应通过国家有关机构的安全性检测和代码安全审计，确保没有恶意软件或恶意代码。

7.4 数据保护

7.4.1 系统申报数据等关键业务数据应采用加密、签名、访问控制等措施，保障数据在存储、传输过程中的保密性、完整性和抗抵赖性。关键业务数据应从源端通过隔离缓冲区采取数据不落地方式传递到安全Ⅱ区的业务系统，传输的数据应通过恶意代码检测。
7.4.2 系统业务数据应采用严格访问控制措施，修改、删除等操作应具备日志记录功能。
7.4.3 系统应具备业务数据备份功能，支持本地和异地数据备份方式，备份数据应采用必要的保护措施，保障备份数据安全。

7.5 运维安全

系统应通过内部专用设施进行维护，运维终端与系统服务器宜采用逻辑隔离措施，应采用有效的措施对运维人员进行身份认证和运维授权，并对系统服务器等关键设备的程序修改、数据库修改、文件修改、文件删除、文件拷贝等操作进行全过程审计，保障系统的运行维护行为可管控、可追溯。

7.6 监测预警

结合电力监控系统网络安全管理要求，系统应部署网络安全监测装置，采集网络运行日志、操作系统运行日志、数据库重要操作日志、安全设备运行日志以及业务应用安全事件信息（包括对业务应用的

登录、访问、关键操作等事件）,全面监视网络空间内计算机、网络设备、安防设备的安全行为，对安全事件进行按分析提供预警信息。

参 考 文 献

[1]《电力监控系统安全防护规定》国家发改委2014第14号令
[2]《电力监控系统安全防护总体方案》国家能源局文件、国能安全36号文