电力现货市场技术支持系统二次安全防护体系研究

常飞

（中国电建集团河南省电力勘测设计院有限公司 郑州 450007）

摘要：随着电力体制改革的全面深化，电力中长期交易规模不断成熟，电力现货交易试点范围的进一步扩大，可以预见在“十四五”期间，电力现货交易将在全国推展。电力现货市场技术支持系统不仅需要为电力现货交易提供计算、存储等基本功能，还需要提供市场出清、风险管控、市场评估等高级功能，在整个电力现货交易中处于至关重要的地位，因此，统的二次安全防护对于系统的运行安全、数据安全就至关重要。本文就电力现货市场技术支持系统的二次安全防护体系进行研究，包含总体安全架构、安全防护要求，提出一套满足要求的安全防护设备配置方案，提升系统的安全性，达到防范、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攻击，确保系统数据安全，保障电力现货市场安全稳定运行的目的。

一、引言

2015 年 3 月，中共中央、国务院出台了《中共中央国务院关于进一步深化电力体制改革的若干意见》（中发〔2015〕9 号），同年 11 月发布了 6 个配套文件，提出了建设相对独立的交易机构、开放增量配电业务、培育售电市场等体制改革措施。此后，国家能源局先后与 2017 年与 2021 年先后确定浙江、山东、江苏、上海、河南等 14 个省（直辖市）为试点地区，电力现货市场建设在我国正有序逐步开展，并取得一定的成效。电力现货市场技术支持系统是整个电力现货市场的大脑，电力现货所有交易都在技术支持系统上进行，所有数据也都存储在技术支持系统上，因此系统的二次安全防护对于系统的运行安全、数据安全就至关重要。

二、总体安全架构

现货市场技术支持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攻击，确保系统数据安全，保障电力现货市场安全稳定运行。

现货市场技术支持系统安全防护遵循“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。

三、安全防火要求

（1）边界防护要求

a）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，也是所其它安全防护措施的重要基础。现货市场技术支持系统边界防护及安全部署如图 1 所示，现货市场技术支持系统边界类型与要求如表 1 所示。

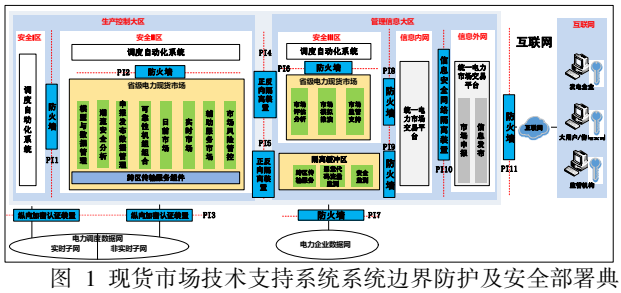

图 1 现货市场技术支持系统系统边界防护及安全部署典型结构示意图

表 1 现货市场技术支持系统边界类型及要求

边界类型	边界安全防护要求
PI1：安全Ⅱ区现货市场技术支持系统与安全Ⅰ区调度自动化系统其它应用的边界	部署硬件防火墙等逻辑隔离设施
PI2：安全Ⅱ区现货市场技术支持系统与安全Ⅱ区调度自动化系统的边界	部署硬件防火墙等逻辑隔离设施
PI3：安全Ⅱ区现货市场技术支持系统与电力调度数据网的边界	部署纵向加密认证装置
PI4：安全Ⅱ区现货市场技术支持系统与管理信息大区的边界	部署电力专用横向单向隔离装置
PI5：安全Ⅱ区现货市场技术支持系统与隔离缓冲区的边界	部署独立的电力专用横向单向隔离装置
PI6：安全Ⅲ区现货市场技术支持系统与安全Ⅲ区调度自动化系统的边界	部署硬件防火墙等逻辑隔离设施
PI7：安全Ⅲ区现货市场技术支持系统与电力企业数据网的边界	部署硬件防火墙等逻辑隔离设施
PI8：安全Ⅲ区现货市场技术支持系统与信息内网统一电力市场交易平台的边界	部署硬件防火墙等逻辑隔离设施
PI9：隔离缓冲区与信息内网统一电力市场交易平台的边界	部署硬件防火墙等逻辑隔离设施
PI10：信息外网现货市场技术支持系统与信息内网的边界	部署信息安全网络隔离装置设施
PI11：信息外网现货市场技术支持系统与互联网的边界	部署硬件防火墙等逻辑隔离设施

b）安全分区

遵照《电力监控系统安全防护规定》（国家发展改革委 2014 年第 14 号令）和《电力监控系统安全防护方案》（国能安全〔2015〕36 号）规定，现货市场技术支持系统主要功能模块布置在生产控制大区安全Ⅱ区和管理信息大区安全Ⅲ区，涉及互联网的功能模块应部署于信息外网。安全分区部署具体如表 2 所示。

表 2 现货市场技术支持系统应用功能分区部署

功能模块	安全Ⅱ区	安全Ⅲ区
市场模型与数据管理	●	
申报发布数据管理	●	
可靠性机组组合	●	

功能模块	安全Ⅱ区	安全Ⅲ区
日前市场	●	
实时市场	●	
辅助服务市场	●	
市场风险管控	●	
市场评估分析		●
市场模拟推演		●
市场监管支持		●
潮流安全分析	●	
数据交换	●	●

备注说明：标记“●”，则可在该区域部署该功能场景。

c）网络专用

现货市场技术支持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。

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。

d）横向隔离

现货市场技术支持系统在安全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。

在安全Ⅱ区部署的现货市场技术支持系统在与安全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。

在安全Ⅲ区部署的现货市场技术支持系统在与安全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。

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。

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。

e）纵向认证

现货市场技术支持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。

现货市场技术支持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。

f）隔离缓冲区

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。

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区现货市场技术支持系统业务之间的数据不落地安全传输。

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。

（2）系统本体安全

a）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。

b）计算机和网络设备安全

现货市场技术支持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。

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。

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）。

c）操作系统和基础软件安全

现货市场技术支持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。

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《电力行业信息系统安全等级保护基本要求》等政策法规要求。

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。

d）应用软件安全

现货市场技术支持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。

现货市场技术支持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。

现货市场技术支持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。

现货市场技术支持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。

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。

现货市场技术支持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。

现货市场技术支持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。

（3）数据保护

现货市场技术支持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。

现货市场技术支持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。

现货市场技术支持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。

（4）运维安全

现货市场技术支持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。

（5）监测预警

结合电力监控系统网络安全管理要求，现货市场技术支持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。

四、安全防护设备配置方案

边界安全防护：系统安全Ⅱ区、安全Ⅲ区与 D5000 系统安全Ⅱ区、安全Ⅲ区之间各部署防火墙 2 台，安全Ⅱ区与安全Ⅲ区之间部署正、向物理隔离装置各 1 台，安全Ⅱ区与隔离缓冲区之间部署正、反向物理隔离装置各 1 台，隔离缓冲区与安全IV 区之间部署防火墙 2 台。

数据安全防护：安全Ⅱ区与管理信息Ⅳ区各部署 1 台加密机，隔离缓冲区部署网络安全监测装置 1 台、恶意代码流量监测 1 台，确保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。

运维安全：安全Ⅱ区、安全Ⅲ区各部署堡垒机 1 台用于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。安全Ⅱ区、安全Ⅲ区运维终端接入交换机与系统服务局汇聚交换机之间各配置防火墙 2 台，实现运维终端与系统服务器的逻辑隔离。

详细设备配置方案可参考图 3。

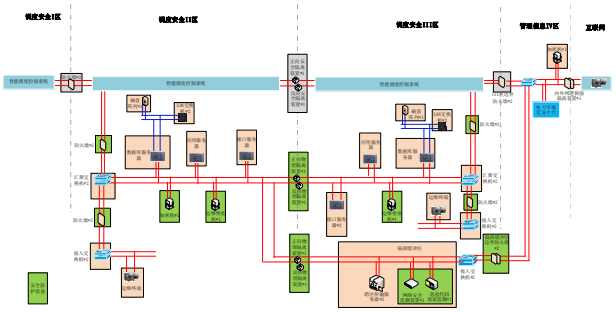

图 3 现货市场技术支持系统安全防护设备配置方案

五、结语

本文通过对电力现货市场技术支持系统安全防护架构、安全防护要求的研究，提出满足要求的二次安全防护设备配置方案，从而实现防范、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攻击，确保系统数据安全，保障电力现货市场安全稳定运行。

参考文献：

[1]蔡宇，肖艳炜，张国芳，昌力，许洪强，常乃超. 省级电力现货市场技术支持系统技术架构设计[J]. 电力系统自动化,2021,45(06).

[2]刘映尚，张昆，顾慧杰，周华锋，彭超逸，胡荣，胡亚平，朱文，许丹莉，何锡祺.南方区域电力现货市场技术支持系统架构及关键技术[J]. 南方电网技术，2018,12(12).

[3]丁恰，昌力，涂孟夫.电力现货市场技术支持系统关键技术探讨[J].电力系统自动化，2018(23)

[4]梁志飞，陈玮,张志翔,丁军策.南方区域电力现货市场建设模式及路径探讨[J]. 电力系统自动化，2017(24).

[5]饶巨为.电力监控系统二次安全防护探讨[J]. 通信电源技术,2019,36(06).

[6]张菁，袁文.电网调度系统二次安全防护策略分析[J]. 中国设备工程,2018,(16).