

[信息安全]

电网调度自动化厂站端系统安全性分析与防护策略

文/沈嘉杰

国网江苏苏州市吴江区供电分公司

电网调度自动化厂站端系统的安全稳定运行对整个电力系统的安全性和可靠性至关重要。融合安全管理、安全运营、法律法规和安全技术等四个方面，构建电网调度自动化厂站端系统安全治理生态圈。建立和完善一套信息安全管理体制，以确保系统数据和运行的安全性。

电力系统作为现代社会的基础设施之一，对于保障国家能源安全和经济发展具有重要意义。电网调度自动化厂站端系统作为电网运行的关键环节，承担着电力系统安全稳定运行的重要职责，然而随着信息技术的快速发展和电网智能化的推进，电网调度自动化厂站端系统面临着越来越严峻的安全挑战。安全威胁的不断增加，例如网络攻击、恶意软件和人为操作失误等，给电网运行和数据的完整性、可靠性和保密性带来了巨大的风险。

因此，对电网调度自动化厂站端系统的安全性进行深入的分析 and 防护策略的制定显得尤为重要。

电网调度自动化厂站端系统安全治理生态圈

电网调度自动化厂站端系统的安全稳定运行对于整个电力系统的安全性和可靠性至关重要，只有通过综合利用安全管理、安全运营、法律法规和安全技术等手段，全面提升系统的安全性防护水平，才能有效应对各种安全威胁和挑战，确保电力系统的安全稳定运行，为国家经济和社会发展提供可靠的电力支撑。本文从这四个方面进行创新性融合，构建电网调度自动化厂站端系统安全治理生态圈，其结构如图1所示。

1) 安全管理是电网调度自动化厂站端系统安全

治理生态圈的基础。通过建立合规框架和风险评估机制，确保系统运行符合相关规定，并及时识别和应对潜在风险。项目与人员管理也至关重要，包括对项目的规划、实施和监控，以及对人员的培训和权限管理，确保系统运行在合理的框架内，人员具备足够的安全意识和技能。这些措施将有助于建立起一套完善的安全管理体系，为系统安全治理提供坚实的基础。

2) 安全运营是电网调度自动化厂站端系统安全治理生态圈的紧急响应机制。入侵检测、防火墙、防毒墙等安全设备的部署和运行，能够及时发现和阻止潜在的安全威胁，保障系统的正常运行。用户网络行为审计、日志审计和漏洞扫描等技术手段，可以帮助监控用户行为，记录系统运行情况，并及时发现和修复安全漏洞。终端接入控制和其他安全设备的应用，能够有效防范外部攻击和内部威胁，确保系统数据和运行的安全性。

3) 法律法规是电网调度自动化厂站端系统安全治理生态圈的法律基础。网络安全法、数据安全法等相关法规的遵守，为系统安全治理提供了法律保障和规范，确保系统运行在法律框架内，保护用户数据和信息安全。这些措施将有助于建立起一套完善的法律法规体系，为系统安全治理提供法律支持

和保障。

4) 安全技术是电网调度自动化厂站端系统安全治理生态圈的关键手段。数据分类分级、数据脱敏和区块链技术等技术手段,可以有效保护系统数据的机密性和完整性,防止数据泄露和篡改。数据备份恢复、异常行为识别、隐私保护计算、身份认证

和访问授权等技术手段,能够提高系统的抗攻击能力和安全性,确保系统运行的稳定性和可靠性。这些措施将有助于建立起一套完善的安全技术体系,提高系统的安全防护能力,确保系统的安全稳定运行。

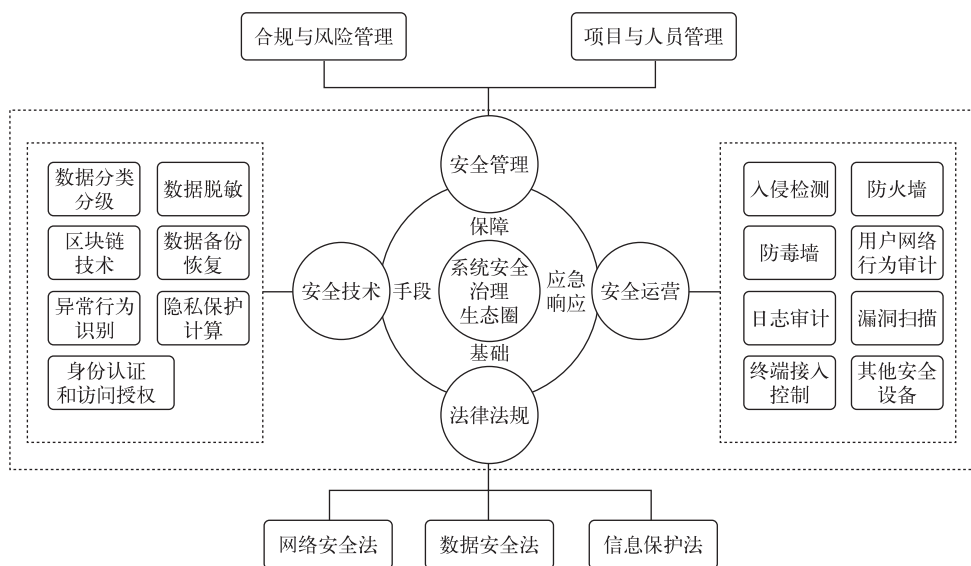


图1 电网调度自动化厂站端系统安全治理生态圈

电网调度自动化厂站端系统信息安全管理体

建立一个完善的信息安全管理体系对于电网调度自动化厂站端系统的安全性和稳定性至关重要。电网调度自动化厂站端系统中包含大量的敏感数据,如电力系统运行数据、设备状态信息等,如果这些数据被恶意攻击者获取或篡改,将会对电力系统的正常运行造成严重影响,甚至引发事故。此外电网调度自动化厂站端系统是电力系统运行的核心控制系统,其稳定性和可靠性直接影响到电力系统的安全性和稳定性。通过建立信息安全管理体

系,可以有效保护系统数据的机密性和完整性,防范网络攻击和恶意破坏,提高系统的可信度和可靠性,确保电网调度自动化厂站端系统的安全稳定运行。

本文创新性地建立和完善了一套电网调度自动化厂站端系统的信息安全管理体

系,在Z坐标系中,基于标准和法律法规,功能体系是信息安全管理体的法律基础。整个信息安全管理体分别涵盖了不同方面的安全管理措施,其架构如图2所示。

整个电网调度自动化厂站端系统信息安全管理体应该是一个综合性、多层次的体系,涵盖系统的各个方面,从结构体系到生命周期管理再到法律法规的遵守。只有在这样的全面体系下,才能有效保护系统的安全性,确保系统数据和运行的安全。因此,建立一个完善的信息安全管理体对于电网调度自动化厂站端系统的安全稳定运行至关重要。

1. 基于分域保护体系框架——结构体系

在电网调度自动化厂站端系统的信息安全管理体中,基于分域保护体系框架,结构体系是至关重要的一部分。这一体系旨在确保系统

在应用安全保护方面,应用系统安全是保障

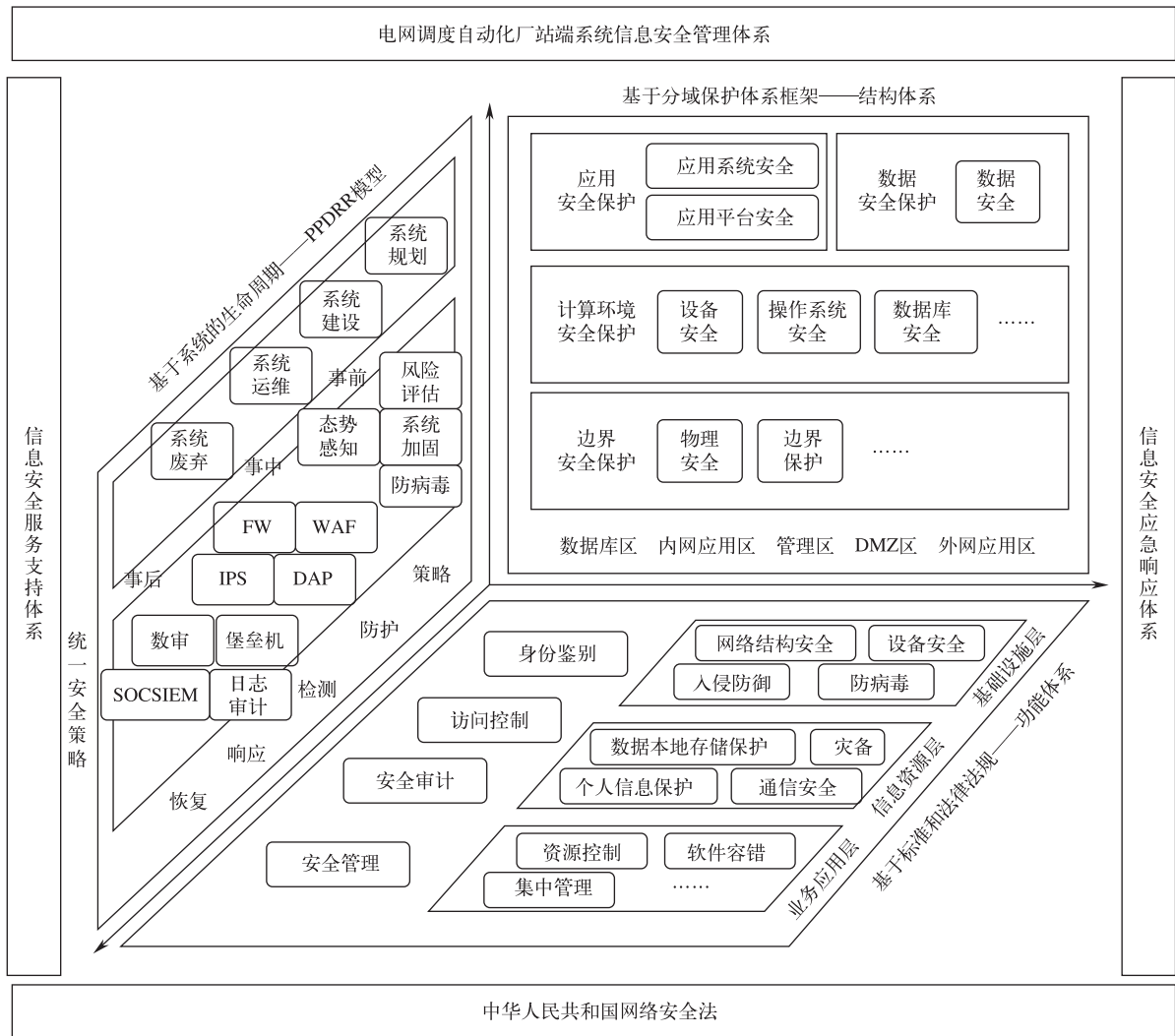


图2 电网调度自动化厂站端系统信息安全管理体

系统正常运行的基础。电网调度自动化系统中的各种应用程序，如调度控制系统、数据采集系统等，都需要具备安全性。通过采用访问控制、身份认证和权限管理等措施，可以确保只有授权人员可以使用系统，并对系统进行合法操作，从而防止未经授权的访问和操作。同时，应用平台安全也是至关重要的，包括对应用平台的安全配置、漏洞管理、安全更新等方面的保护，以确保应用平台不受到恶意攻击和漏洞利用。

2) 在计算环境安全保护方面，设备安全是电网调度自动化厂站端系统安全性的基础。各种设备如服务器、交换机和路由器等需要采取物理和逻辑安全措施，包括设备放置安全、设备访问控制、设备监控和管理等，以确保设备不受到未经授权的访

问和损坏。同时，操作系统安全和数据库安全也是至关重要的，需要采取加固系统、定期更新补丁和加密存储等措施，以防止系统遭受恶意攻击和数据泄露。

3) 在边界安全保护方面，物理安全和边界保护是保障系统安全的重要环节。物理安全包括对服务器机房、控制室等关键场所的严格管控，确保只有授权人员可以进入，并对进出人员和设备进行身份验证。边界保护则包括防火墙、入侵检测系统等网络安全设备的应用，以监控和过滤系统与外部网络之间的数据流，防止恶意流量进入系统，确保系统的安全性。

4) 在数据安全保护方面，数据是电网调度自动化系统中最宝贵的资产之一，需要得到充分的保

护。通过数据加密、数据备份和数据完整性校验等措施，可以确保数据在传输和存储过程中不被篡改或泄露，保障数据的安全性和完整性。此外，还需要建立数据访问控制机制，确保只有授权人员可以访问系统数据，并对数据进行合法操作，避免数据被恶意篡改或删除。

2. 基于系统生命周期的PPDRR模型

在电网调度自动化厂站端系统的工作实际中，基于系统生命周期的PPDRR模型涵盖了系统规划、建设、运维和废弃四个关键阶段，通过事前、事中和事后三个阶段的安全管理措施，确保系统在整个生命周期内的安全性和稳定性。

1) 在事前阶段。包括风险评估、态势感知、系统加固和防病毒等策略。在电网调度自动化系统规划和建设之初，必须进行全面的风险评估，识别潜在的安全威胁和漏洞，及时采取措施加以应对。同时，通过实时的态势感知，监控系统的运行状态和安全事件，及时发现异常情况并做出相应处理。系统加固和防病毒措施则是保障系统在最初阶段就具备足够的安全性，以防范各类安全威胁。

2) 在事中阶段。包括防火墙、Web应用防火墙(WAF)、入侵防御系统(IPS)和数据访问保护(DAP)等防护措施。这些安全设备和技术可以在系统运行时实时监控和阻断潜在的安全威胁，确保系统处于安全状态。防火墙用于监控和过滤网络流量，WAF用于保护Web应用免受攻击，IPS用于检测和阻止入侵行为，DAP用于控制数据访问权限，从而有效防范安全威胁。

3) 在事后阶段。包括安全审计、堡垒机、安全运维与安全事件响应管理(SOCSiem)、日志审计等措施。安全审计可以对系统的安全性进行定期检查和评估，发现潜在问题并及时解决。堡垒机用于加强对系统关键资源的管控和访问控制，防止未经授权的访问。安全运维与安全事件响应管理则是针对安全事件的快速响应和处理，保障系统的连续运行和数据的安全性。日志审计则记录系统的操作和事件，为安全事件的溯源提供重要依据。

3. 基于标准和法律法规的功能体系

在电网调度自动化厂站端系统的安全性分析与防护策略中，基于标准和法律法规的功能体系在确保信息安全管理体系的法律基础上起着至关重要的

作用。这一坐标系涵盖基础设施层、信息资源层和业务应用层三个层级，旨在通过遵守相关标准和法规，建立健全的安全管理措施，保障电网调度自动化系统的安全性。

1) 在基础设施层方面。网络结构安全、设备安全、入侵防御和防病毒是关键的安全措施。网络结构安全包括网络拓扑设计、网络隔离和安全通信协议的应用，以确保系统网络的安全性和稳定性。设备安全涉及硬件设备的安全配置、定期检查和更新，以防止设备被攻击或滥用。入侵防御和防病毒则是通过实时监测和防范网络入侵和恶意软件攻击，保护系统免受安全威胁。

2) 在信息资源层方面。数据本地存储保护、灾备、个人信息保护和通信安全是重要的安全管理措施。数据本地存储保护包括数据加密、备份和恢复机制的建立，以确保数据的完整性和可用性。灾备则是为了应对突发事件或灾难，建立数据备份和恢复计划，确保系统能够快速恢复正常运行。个人信息保护涉及用户数据的隐私保护和合规性管理，遵守相关法律法规对用户数据进行保护。通信安全则是通过加密技术和安全传输协议，保障系统间通信的机密性和完整性。

3) 在业务应用层方面。资源控制、软件容错和集中管理是关键的安全措施。资源控制包括对系统资源的访问控制和权限管理，确保只有授权用户能够访问系统资源。软件容错则是通过容错机制和漏洞修复，提高系统对软件错误和攻击的容忍度。集中管理包括对系统安全策略、日志审计和安全事件响应的集中管理，以便及时发现和应对安全事件。

结束语

电网调度自动化厂站端系统的安全稳定运行对于整个电力系统的安全性和可靠性至关重要。本文从安全管理、安全运营、法律法规和安全技术四个方面进行了创新性融合，构建电网调度自动化厂站端系统安全治理生态圈，并提出一套基于三维架构体系的信息安全管理体系。通过本文的研究，为电网调度自动化厂站端系统的安全性提供全面的分析和防护策略，为电力系统的安全稳定运行提供有益的参考。EA

(收稿日期: 2024-05-07)