DOI：10.19364/j.1674-9405.2024.06.010

长江委网络安全集中管控平台建设与应用

吴静子，李　歆，谢碧云，徐靖钧

（长江水利委员会网络与信息中心，湖北 武汉 430010）

摘　要：为落实网络安全相关法律法规，提升长江委网络安全防护与管理水平，解决长江委网络安全运维中网络资产不明确、安全设备管理分散、安全策略实施效率低、安全威胁处置响应不够及时、运维体量大等难点和痛点问题，研究应用策略智能适配、安全策略分析模式创新和机器人流程自动化等关键技术，构建由 IT 资产管理、运行维护监控、安全策略管理、安全事件处置和安全知识等中心组成的长江委网络安全集中管控平台。通过在长江委机关网及部分下属单位网络部署运行管控平台，初步实现长江委网络资源和用户的统一监控、访问控制策略的统一管理、网络安全事件的统一分析、网络安全威胁的统一响应，整体提升长江委网络安全纵深防御、监测预警和应急处置能力。

关键词：网络安全；集中管控平台；策略智能适配；安全策略分析；机器人流程自动化；应用成效

中图分类号：TP393.08　　**文献标识码：**A　　**文章编号：**1674-9405(2024)06-0061-05

0　引言

网络安全是事关国家安全的重大战略性问题。国家高度重视网络安全，提出新时代网络强国战略，统筹推进网络安全和信息化工作，推进网络安全和信息化高质量发展[1]。水利领域作为重要行业领域，要加快推进智慧水利建设，不断提升水利信息化水平，为国家水治理体系和能力的现代化提供有力支撑与强力驱动[2]，同时要全面提升网络安全防护能力和安全管理水平[3]。

为贯彻落实新时代网络强国战略、网络安全相关法律法规，水利部不断深化网络安全工作，提出水利网络安全工作必须基于统一的网络安全技术框架，以合规为基础，可控为核心，强调坚持“重点保护、分级管理”“主动防御、强化监管”，并提出网络安全防护能力提升行动，要求强化内外协同及上下联动的主动监测预警、对抗有组织攻击的纵深防御、快速恢复业务的应急处置等能力建设，提升水利网络安全防护水平。

《信息安全技术 网络安全等级保护基本要求》（以下简称等保 2.0）对安全物理环境、通信网络、区域边界、计算环境、管理中心等提出了具体要求[4]，针对持续监测、威胁情报、快速响应类的要求提出了具体落地措施，对风险评估、安全监测、通报预警、态势感知等提出了新的标准。随着信息网络应用和技术的快速发展，云计算、大数据、物联网、互联网等大量新技术的广泛应用，新的脆弱因素和弱点不断被揭示[5]，网络安全潜在威胁造成的危害更趋复杂严峻。

长江水利委员会（以下简称长江委）作为水利部直属最大的流域管理机构，下属单位多且分布在长江沿线，信息系统建设主体多，应用面广且分散，由此产生网络结构复杂，安全体系不统一，以及网络安全风险点多、运营覆盖面广、运维难度大等诸多问题。长江委信息系统及数据资源在数据采集、数据传输、数据存储、应用系统自身、承载应用的基础环境及系统互联等各层面，不断面临着来自内部和外部网络的非授权访问、恶意攻击、数据窃取、数据丢失等复杂安全威胁，潜在威胁造成的危害愈来愈大。同时，在长江委网络安全实际运维管理工作中，存在网络资产不明确、管理界限模糊[6]，网络访问控制策略规则开通效率低、安全威胁处置响应不够及时，以及各安全系统与设施各自为营运维不便且体量大等难点和痛点。目前，市场上运维管理软件、安全产品众多，但没有一款产品可以集中、有效地解决长江委网络安全运营管理中的实际困难。针对难点、痛点和实际困难，研究构建统一、集中的网络安全管控技术体系，建设长江委网络安全集中管控平台（以下简称管控平台），以有效提升长江委网络安全防护能力和管理水平。

收稿日期：2024-01-29

作者简介：吴静子（1991—），女，安徽蚌埠人，工程师，主要从事信息化专业技术工作。E-mail：jingzi_wu@foxmail.com

1 管控平台需求分析

根据《中华人民共和国网络安全法》及网络安全等级保护标准相关要求，从解决实际问题出发，管控平台要实现网络资产统一识别、网络资源与用户统一监控、访问控制策略统一管理、网络安全事件统一分析和网络安全威胁统一响应，达到长江委网络安全集中管控。管控平台设计要充分考虑高扩展性、高可维护性、高可组合性，聚合网络资产管理、设备监控、策略分析、安全威胁处置及应急响应等功能，助力长江委网络安全管理。具体需求分析如下：

1）建立网络资产管理机制，统一识别网络资产。有效识别合规网络资产和管理网络资产，对保障网络安全、提升运营效率具有重要意义。网络资产管理是动态过程，需要精准感知鉴别已在线、新入网、“僵尸”等资产，并保证资产数据的唯一性和可靠性。基于清晰的资产台账，需要进一步收集和分析各类设备的运行状态数据，及时发现故障或异常情况并进行实时告警，从而采取相应的处理措施。

2）建立安全策略采集分析下发机制，统一管理访问控制策略。由于历史原因，长江委信息化发展一直以来采用传统网络安全运维模式，网络安全软硬件设备布署时间不一致，品牌型号多样，各类产品网络安全策略关联交错，日志分散，导致发生异常情况时，故障定位排查困难大，处置效率低下[7]。因此，需要实现对不同安全设备的安全策略采集和统一分析，减少冗余、过期、冲突等策略，并实现策略仿真和一键下发，提高安全运营效率。

3）提升监测预警能力，统一分析安全事件。需要将现有互联网接入区单一区域的网络安全威胁监测预警能力，提升至具备长江委网络多个分区和子网的重要信息系统安全威胁情报收集、网络安全威胁态势感知、重要网站安全监测、通报预警机制支撑等监测预警能力，增强安全事件汇集和分析能力，为长江委机关网的网络安全建设、监督、决策、响应提供有力依据。

4）促进多维度安全可控，统一响应处置网络安全威胁。需要将现有机关网重要信息系统的网络安全防护，提升至以机关网为中心、覆盖全长江委子网络的整体安全防护体系，同时增强虚拟机、代码安全、移动应用等领域安全可控及多平台集成，实现安全策略智能分析一键下发和安全事件分析共享，形成可主动防御、统一处置安全事件的网络安全纵深防御体系，有效抵御各类网络攻击行为。

5）建立平台互联互通机制，强化联防联控应急能力。需要按照水利网络安全标准建设管控平台，统一数据传输、软件接口，保证长江委各子网络管控平台之间、长江委网络安全集中管控平台与水利部网络安全管理平台之间的互联互通和情报共享，提升长江委机关网全域、重要信息系统的应急响应能力，以及与水利部网络安全管理上下联动、协同防御的联防联控能力。

2 管控平台关键技术

管控平台建设的最大难点是实现不同品牌、种类、型号的网络安全设备的统一配置管理和安全事件分析。在管控平台设计、建设过程中，通过策略智能适配、安全策略分析模式创新和机器人流程自动化（RPA）等关键技术的研究应用，解决安全设备策略管理兼容、安全事件智能分析等难点问题。

2.1 策略智能适配技术

策略智能适配技术可解决不同厂家设备间的不兼容问题。在数据采集层使用基于 HTTP 协议和 RESTful API（基于 REST 架构的应用程序编程接口）的数据采集技术，以 JSON 和 XML 作为数据报文格式，实现对策略数据的采集。通过支持多种主流监控协议，实现对来自不同厂商、品类的安全设备和运维监控设备的学习与训练，智能建立丰富策略模型库。横向对比各种类型安全设备指标库，纵向对比不同安全厂家监控模板，根据业务需求自动抽取关注指标，设定监控策略及告警阈值。对新接入的安全产品可通过自动识别自身开放服务，智能匹配最合适的指标库及最相似的监控模板，最终实现各类安全设备和系统的自动识别与适配，打破安全厂家技术壁垒，实现安全策略的统一适配和采集。

2.2 安全策略分析模式创新技术

通过创新安全策略分析模式，解决传统安全策略依靠人员经验配置，存在准确性差及浪费大量人力、物力的问题。结合安全知识库数据，关联设备运行、安全事件、人员处理、知识，生成全过程闭环管理，提供安全事件溯源网络拓扑视图，展示设备暴露服务、协议及端口等，分析目前存在的风险，提出修复建议，不断优化训练策略分析模型。通过 AI 技术自动识别和分析策略中存在的不合理、错误、异常、缺失数据，并对此类数据进行优化和纠正，根据不同场景选择不同的智能算法，最终实现基于 AI 技术的安全策略智能分析，提升安全策略分析的效率和准确率。

2.3　RPA 技术

引入 RPA 技术，帮助管理人员对策略配置进行有效评估，规避操作与管理风险。实现策略下发流程的自动化执行，一键完成下发操作，动画展示执行操作过程等。利用策略模拟，检查存在风险、冲突、违规情况等，设计超时重试等多种失败处置预案。对策略配置版本进行自动化管理，使管控平台具备基线与版本差异分析、配置变更过程管理、策略自动恢复等能力。生成策略变更智能风险评估报告，包括变更前后配置变化、资源需求、影响范围、紧急程度、变更窗口、回退计划等，最终实现策略变更、下发等流程的自动化执行，避免人工干预引发的误操作风险。

3　管控平台设计

管控平台是长江委机关网的网络安全防护与管理中心，既是与各委属单位网络安全管控平台横向集成、纵向贯通、安全信息共享的基础，也是与水利网络安全管理实现上下联动、协同防御、联防联控的枢纽。管控平台由 IT 资产管理、运行维护监控、安全策略管理、安全事件处置和安全知识等五中心组成，具体架构如图 1 所示。管控平台五中心融合发力，做到全局统一、监控严密、响应及时，实现全方位的集中管控。

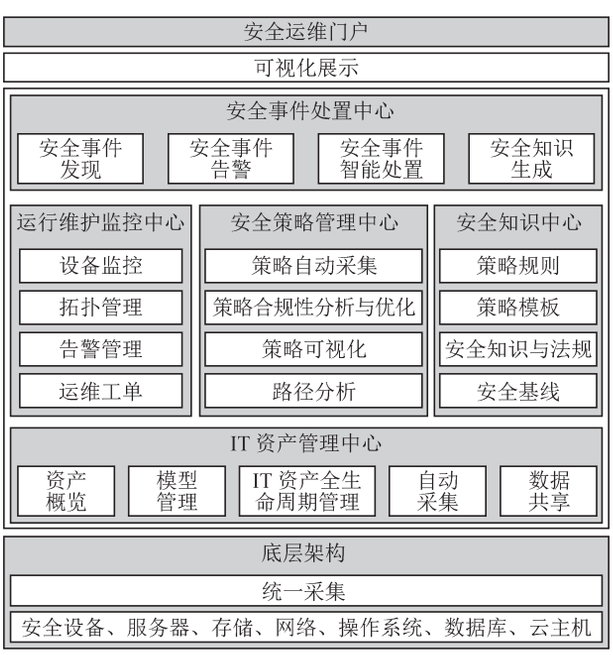

图 1　管控平台架构图

3.1　IT 资产管理中心

IT 资产管理是网络安全管控与运维的基础，IT 资产管理中心主要实现 IT 资产的统一、全生命周期管理及数据的共享。

采用自动发现和比对等算法，实现对 IT 资产信息的自动采集和整合。通过梳理事前、事中、事后资产管理各环节管理要求，建立资产的全生命周期闭环管理体系，实现 IT 资产的一体化信息管理。通过资产管理，清理“僵尸”资产，摸清资产“家底”，发现、统计、整合 IT 资产数据，实现资产数据的一数一源。建立标准化接口，将准确、唯一的资产数据提供给管控平台运行维护监控中心、安全策略管理中心和网络安全威胁感知系统等，提升 IT 资产管理效率，实现对 IT 资产的集中管理。

3.2　运行维护监控中心

运行维护监控中心根据 IT 资产管理中心的基本数据进行配置，实现对各类设备运行状态的监控和告警，并将告警信息通过蓝信发送给资产管理员。在资产明晰的基础上开展运行维护监控，及时了解业务资源和安全设施的运行状况，发现可能导致系统故障的隐患。

运行维护监控中心主要实现设备监控、动态拓扑展示及运维管理。通过对服务器、防火墙等不同类别设备的统一监控，对设备运行的性能、配置、日志、告警等数据进行采集，分析，处理和展示，并根据资产和设备监控等数据，动态生成网络拓扑并进行编辑与展示。监控系统发现设备告警后，自动生成运维工单，并集成蓝信消息推送，提示相关运维人员及时处理，提升运维的及时性。

3.3　安全策略管理中心

安全策略管理中心是网络安全管控的核心，提供安全设备的策略数据及管理，解决网络安全设备庞杂、网络安全策略交错、管理效率低下等问题，统一对网络访问控制策略进行采集、分析与管理，提升安全策略管理效率。

安全策略管理中心主要实现安全策略的统一采集、分析优化、变更风险管理、验证及下发等主要功能。通过定制接口开发，实现对不同品牌、型号的防火墙策略的采集，并反向将策略下发至防火墙设备。定期对存量策略规则进行清理优化，发现隐藏、冗余和可合并等策略，提供处置建议，优化策略规则。实现基于源地址、目的地址、协议、端口等条件的路径仿真分析和可视化呈现，提示对外的暴露面与潜在风险路径等。在策略变更过程中，支持对新增策略进行自动化风险评估，以直观的报告形式支撑安全管理部门的审批工作，实现网络安全策略持续、安全、合规、可控。新的策略生成后，自动使用风险和合规性分析对

策略进行验证及路径仿真模拟，检查是否有重复、冲突、违背安全基线等情况，确保新的策略符合要求，并将策略一键下发到设备。

3.4 安全事件处置中心

安全事件处置中心基于威胁、策略、资产等多维数据，实现安全事件的发现、告警、处置及安全知识生成的闭环管理。

安全事件处置中心与长江委网络安全威胁感知系统等集成，预留与水利网络安全告警、威胁事件统一的处理接口，统一接收安全告警事件，按照安全预案和运维场景分析模型，自动将策略下发到目标设备，实现对安全事件的快速处置，处置流程可自动生成安全知识，为后续事件处置分析与模型优化提供参考。

3.5 安全知识中心

安全知识中心基于安全规则，积累安全知识，为安全事件的处置提供参考，实现对网络安全相关法律、法规、标准，长江委网络安全管理制度，以及策略规则、策略模板、威胁知识、安全管理基线等的统一管理，积淀各类网络安全技术和管理经验，不断优化安全运维管理模型，并与水利网络安全知识平台互联共享，提升网络安全管理能力。

4 管控平台建设及应用成效

管控平台全面实现跨软硬件平台的布署运行。在不同软硬件平台上，网络安全运维管理人员可通过友好的可视化操作界面，对安全设备运行状态进行实时把控，对安全设备策略进行集中采集、分析与展示，便捷管理多台安全设备，最大程度地降低配置、管理、监控及维护安全设备的成本。同时，通过 IT 资产全生命周期管理，帮助信息化部门向业务部门提供有效服务，保障 IT 服务长期正常运作，与长江委网络安全威胁感知系统联动管理，一键处置网络安全威胁。管控平台的建设与应用取得了以下成效：

1）网络安全威胁监测预警能力扩展。管控平台与已建的网络安全威胁感知系统对接集成，可获取长江委机关网各安全域的安全监测预警信息；与水利部数据交换平台集成，可实现长江委机关与水利部及委属单位的网络安全情报整合与共享；与蓝信等平台集成，可采集各设备的性能、配置、日志、告警等数据，进行分析、处理后，将告警通过蓝信推送至相关责任人。管控平台将安全监测预警范围从单一安全域扩展至长江委机关网全域，初步实现了流域内网络安全监测预警信息的共享，极大提升了网络安全威胁监测预警能力。

2）网络安全防护能力提升。a. 厘清资产数据。管控平台将来源于多个单位、项目、建设期的 IT 资产数据及未登记审核的入网资产进行自动感知和统一整合，为网络安全管理部门提供唯一、权威的 IT 资产数据，明确资产归属，隔离非法资产。b. 统一采集分析安全策略。通过接口开发，管控平台与防火墙、云安全管理平台、堡垒机、主机加固系统等不同数据源产品对接，打破设备品牌、类别壁垒，实现基于多类设备的策略统一采集、汇集、查询、清理、下发，并根据策略规则库中预定义的规则进行智能化合规性分析、自动下发和验证；运用知识图谱技术，通过图形化界面实现策略的可视化展示，统一识别分析僵尸、冲突、冗余、过期等策略。c. 一键处置策略变更。管控平台与长江委综合信息门户、统一身份认证系统集成，各安全设备与系统可通过管控平台一键登录，分析研判后可通过管控平台一键处置多个设备的安全策略，不必分别登录各个设备进行配置，运维人员可综合掌控策略情况并迅速准确地完成策略变更，极大提升了安全策略配置的科学性和管理的效率。

3）网络安全应急响应能力提升。管控平台动态接收网络安全事件，根据场景分析模型进行安全事件预警分析，自动获取策略，下发策略，反馈处置结果，实现安全事件从感知到分析再到联动响应的自动化处置，使事件处置更加全面及时，提升了运维管理的及时性和有效性，实现了与委属单位的纵向贯通，并初步实现与水利部网络安全管理平台的信息情报共享，助力上下联动、协同防御、联防联控，有效提升了网络安全事件的应急响应能力。

4）助力全长江委网络安全管理水平提升，效果显现。2021 年，经过实施和打磨，管控平台在长江委中心机房完成布署并投入实际应用；2022—2024 年，管控平台用户逐步扩展至汉江集团、南水北调中线水源有限责任公司等委属单位。委属各单位网络安全管理人员可通过管控平台实现网络安全资产管理和安全情报共享，并可根据长江委网络安全和信息化领导小组办公室的要求进行网络安全工作报告填报，有效助力长江委网络安全的集中控制与统一管理。

截至 2024 年 2 月，管控平台管控全长江委网络设备、服务器、存储及备份设备、安全设备、终端等网络资产 2 000 余台（套），处置网络安全威胁年告警量 16 万余条，网络威胁的感知与处置时长从以前的平均 2 h 缩短到 20 min 内，多次及时发现并阻断了来自

委内单位的横向攻击。尤其在 2021—2024 年湖北省、水利部、公安部网络安全实战演习和重保时期，发挥了有效的预警、防护和应急响应作用。

管控平台的建设运行，有效遏制了长江委网络安全威胁事件，维护了长江委网络安全，保障了长江委重要业务信息系统的稳定连续运行，为长江委防洪、水资源管理等各项业务工作提供了安全有效的信息技术支撑。

5　结语

通过开展管控平台开发建设与应用实践，实现了长江委机关网 IT 资产和网络安全策略的一体化、全生命周期管理，制订了安全设备、网络设备、服务器等硬件上线及安全设备接入基线标准，建立了统一的基线系统，储备了网络安全知识经验，提升了长江委机关网网络安全纵深防御、监测预警和应急处置能力，并在长江委委属相关单位进行了推广应用，整体提高了长江委网络安全防护与管理水平。

随着网络安全形势的日益复杂多变和网络安全技术的迅速发展，网络安全攻击风险仍在持续增长，大规模针对性网络攻击行为、零日漏洞、高级持续性威胁、数据泄露等网络安全风险愈演愈烈[8]。然而，当前的网络安全运维还是过多依赖网络安全运维人员的技术经验，管控平台机器学习、智能分析与处置能力仍然不足，今后需要在人工智能与大数据分析等技术的加持下进一步完善[9]，逐步提升网络安全监测预警的准确性，实现网络安全运营的智能化。

参考文献：

[1] 新华社.习近平在网络安全和信息化工作座谈会上的讲话[J].中国信息安全，2016（5）：23-31.
[2] 水利部网络安全与信息化领导小组办公室.智慧水利总体方案[R].北京：水利部网络安全与信息化领导小组办公室，2019：98-102.
[3] 蔡阳.贯彻《网络安全法》构建水利网络安全保障体系[J].水利信息化，2017（3）：1-4，15.
[4] 全国信息安全标准化技术委员会.信息安全技术 网络安全等级保护基本要求：GB/T 22239—2019 [S].北京：中国标准出版社，2019：26-43.
[5] 张潮，房志刚，郭冉.面向智慧水利的网络安全技术体系构建[J].中国水利，2023（11）：41-44.
[6] 周晔，张春晓，韩东，等.信息化运维与网络安全管理措施改进研究[J].保密科学技术，2023（12）：21-24.
[7] 贾航，王丹.高校网络安全管控平台设计[J].网络安全技术与应用，2024（5）：85-88.
[8] 周敏，陈小东.网络安全运维领域中的实时威胁检测与应对策略研究[J].信息与电脑（理论版），2024，36（3）：219-221.
[9] 王祥，牟亚南.浅谈网络安全检测预警的发展趋势[J].通信与信息技术，2023（增刊 2）：69-72.

Construction and application of centralized cybersecurity control platform for Yangtze River Commission

WU Jingzi，LI Xin，XIE Biyun，XU Jingjun

（*Changjiang Water Resources Commission，Network and Information Center，Wuhan* 430010，*China*）

Abstract： In order to comply with cybersecurity laws and regulations and to enhance the cybersecurity protection and management level of the Yangtze River Commission（YRC），this study addresses various problems faced in the network operation and maintenance of the YRC，including unclear network asset management，decentralized security device management，low efficiency of security policy implementation，delayed response to security threats，and large operational scale. Key technologies such as intelligent policy adaptation，security policy analysis model innovation，and robotic process automation have been researched and applied to construct a centralized cybersecurity control platform consisting of IT asset management，operational maintenance monitoring，security policy management，security incident response，and security knowledge management. By deploying and operating the control platform on the YRC's internal network and some subordinate units，a preliminary unified monitoring of network resources and users has been achieved，along with centralized management of access control policies，unified analysis of cybersecurity incidents，and coordinated response to cybersecurity threats. This initiative significantly enhances the YRC's capabilities in cybersecurity defense，monitoring and early warning，and emergency response.

Key words： cybersecurity；centralized control platform；intelligent policy adaptation；security policy analysis；robotic process automation；application effectiveness

（责任编辑：陆　燕）