铁路计算机应用
RAILWAY COMPUTER APPLICATION

铁路供电信息系统安全资源池研究

杨轶杰，许　翔，谢　涛，马俊杰

Security resource pool of railway power supply information system

YANG Yijie, XU Xiang, XIE Tao, and MA Junjie

引用本文:
杨轶杰, 许翔, 谢涛, 等. 铁路供电信息系统安全资源池研究[J]. 铁路计算机应用, 2023, 32(11): 73–76.
YANG Yijie, XU Xiang, XIE Tao, et al. Security resource pool of railway power supply information system[J]. Railway Computer Application, 2023, 32(11): 73-76.

在线阅读 View online: http://tljsjyy.xml-journal.net/2023/I11/73

文章编号：1005-8451（2023）11-0073-04

铁路供电信息系统安全资源池研究

杨轶杰[1]，许　翔[2]，谢　涛[2]，马俊杰[2]
（1. 中国铁道科学研究院集团有限公司　电子计算技术研究所，北京　100081；
2. 中国铁路乌鲁木齐局集团有限公司　工电检测所，乌鲁木齐　830011）

摘　要：为满足铁路供电信息系统的安全防护需求，将安全资源池运用到铁路供电信息系统的安全防护中。文章介绍铁路供电信息系统各子系统的安全防护现状，研究安全资源池的特点，阐述铁路供电信息系统安全资源池的架构、功能和关键技术，从而实现安全资源的动态分配，为铁路供电信息系统安全资源的调度决策提供参考。

关键词：铁路供电信息系统；安全资源池；动态分配；资源调度；网络安全
中图分类号：U223.8 : TP39　**文献标识码：**A　**DOI：**10.3969/j.issn.1005-8451.2023.11.15

Security resource pool of railway power supply information system

YANG Yijie[1], XU Xiang[2], XIE Tao[2], MA Junjie[2]
(1. Institute of Computing Technologies, China Academy of Railway Sciences Corporation Limited, Beijing　100081, China；2. Testing Institute of Track, Communication and Signal, China Railway Urumqi Group Co. Ltd., Urumqi　830011, China)

Abstract: To meet the security protection requirements of the railway power supply information system, the security resource pool is applied to the security protection of the railway power supply information system. This paper introduced the current status of security protection for various subsystems of the railway power supply information system, studied the characteristics of security resource pools, elaborated on the architecture, functions, and key technologies of the security resource pool of the railway power supply information system, thus implemented dynamic allocation of security resources, which provided reference for the security resource scheduling decision-making of the railway power supply information system.

Keywords: railway power supply information system; security resource pool; dynamic allocation; resource dispatching; network security

铁路供电信息系统包括铁路供电远动子系统、铁路供电辅助监控子系统、铁路供电安全检测监测信息综合应用子系统和铁路供电一级子平台等，是电气化铁路运输的重要保障。因此，保障铁路供电信息系统的网络安全是铁路重要的安全保障环节。当前，网络安全形势日益严峻，针对重要信息系统的攻击时有发生。铁路供电信息系统作为专网运行的系统，若受到攻击者入侵，在专网内横向移动，会引发供电故障，甚至造成行车事故。在已有的研究中，研究人员针对铁路供电信息系统的安全运行提出过精准判断和及时恢复的解决方案，但在攻击方式与攻击技术日益升级的环境下，精准判断愈加难以实现[1]；也有研究人员提出对铁路供电信息系统终端实施特殊安全防护，严格准入限制条件，在一定程度上降低了攻击面，但也对这类系统今后可能需要进行的扩展带来了限制[2]。

在网络安全资源日益丰富的背景下，安全资源池可对专网运行的系统提供更加全面的安全防护[3-6]。本文综合考虑已有网络安全防护的不足和安全资源池的优点，提出铁路供电信息系统安全资源池，强化铁路供电信息系统的安全防护。

1　铁路供电信息系统现状

1.1　铁路供电远动子系统现状

铁路供电信息系统以铁路供电远动子系统为主，辅之以铁路供电辅助监控子系统，共同实现铁路供

收稿日期：2023-07-31
基金项目：中国铁路乌鲁木齐局集团有限公司揭榜挂帅重点课题（2022-kj-69）
作者简介：杨轶杰，助理研究员；许　翔，高级工程师。

电的控制与调配。铁路供电远动子系统的主要作用是监视与数据采集。通常情况下，铁路供电远动子系统由调度主站、通信通道、被控站等组成[7]，采用中国国家铁路集团有限公司（简称：国铁集团）、铁路局集团公司、站段的三级结构部署[8]。

国铁集团级铁路供电远动子系统的防护，在网络架构上采用网络链路与设备冗余部署的方式，以保障链路与设备的正常运行；在实际部署中，通过国铁集团主数据中心云平台提供的，客户系统安全审计服务对数据库访问行为进行审计，防止非法入侵，并进行恶意代码检测。

1.2 铁路供电辅助监控子系统现状

铁路供电辅助监控子系统是保障铁路供电远动子系统运行的重要系统，其主要业务是对铁路牵引供电远动系统中的电气设备进行远程监视、测量和控制，包括对其相关信息的采集、处理、传输、显示等功能。

铁路供电辅助监控子系统的网络设备包括防火墙、网闸、交换机、路由器等，其中，防火墙通过访问控制策略实现不同功能区间的访问控制与区域隔离。铁路供电辅助监控子系统的网络区域分为采集交换区、接口交换区、数据域和应用域。通过关闭高危端口、数据库限定主机访问、部署数据库审计服务器和堡垒机等方式，实现网络安全隔离与防护。

1.3 铁路供电安全检测监测信息综合应用子系统现状

铁路供电安全检测监测信息综合应用子系统针对供电段管辖线路的接触网 C1 ~ C6 装置的检测数据，提供检测数据管理、缺陷数据管理、任务分配、数据统计、数据同步等功能，实现跨平台数据访问、数据整合共享和综合分析。该子系统部署模式为 B/S 架构，开发语言为 Java。在安全技术方面，子系统对网络设备、安全设备进行远程管理时，采用 SSH 和 HTTPS 加密协议。

1.4 铁路供电一级子平台现状

铁路供电一级子平台的主要业务为供电信息集中展示和联合分析，预防和处理各供电段接触网和变/配电等专业发生的各种应急事件。在网络架构上，铁路供电一级子平台采用站段级部署为主、工电检测所部署为辅的方式，分级分域实现安全防护。在安全防御上，各安全域间的访问通过防火墙进行逻辑隔离，通过访问控制策略限制业务间的按需访问。该子平台与其他铁路专网间通过安全隔离设备进行边界防护和必要的数据交互。

2 安全资源池简介

安全资源池是安全服务资源的集合[9]，是一个基于软件集成的安全工具集[10]，即一个资源集成平台，可集成目标系统的各种安全防护资源，并开放应用接口，提供与云资源类似、按需获取及弹性使用的安全功能，可从软件和硬件形态上提供安全能力解决方案[11]。

安全资源池由安全资源池分配管理平台和安全资源池资源存储平台组成，通过集中建设、统一资源调配、弹性扩容、按需分配及动态部署功能，实现安全能力利用效率最大化；另外，通过安全资源池分配管理平台的资源分配调度，实现安全能力的动态编排[12-13]。

3 铁路供电信息系统安全资源池

3.1 铁路供电信息系统安全资源池架构

铁路供电信息系统安全资源池架构包括基础环境层、安全防护功能层和安全防护展示层，如图 1 所示。

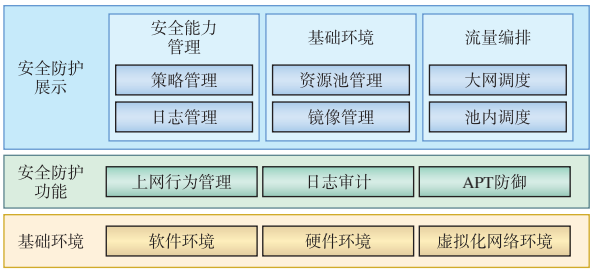

图1 铁路供电信息系统安全资源池架构

3.1.1 基础环境层

主要包括安全资源池运行所需的硬件环境、软件环境及虚拟化的网络环境，需要根据用户需求和

安全能力进行规划部署。硬件环境主要指服务器、交换机、防火墙等硬件设备；软件环境指在硬件环境的基础上，为安全资源池运行提供的操作系统、数据库等基础环境；虚拟化网络环境指在已有硬件设备的基础上，为满足安全资源池连接所需的虚拟网络设备、安全设备等。

3.1.2 安全防护功能层

根据用户安全防护需求，部署相应的安全防护产品，实现上网行为管理、日志审计及APT（Advanced Persistent Threat）防御等功能。上网行为管理和日志审计主要依靠流量安全检测设备来实现；APT防御主要通过流量安全检测设备和静态扫描设备等的联合检测来实现。

3.1.3 安全防护展示层

包括安全能力管理、基础环境管理及流量编排3部分。其中，安全能力管理包括策略管理和日志管理，策略管理主要针对安全资源池自身的安全进行策略配置，日志管理是对安全资源池自身运行状况的日志进行记录；基础环境管理包括资源池管理和镜像管理，对安全资源池的安全防护功能进行动态管理；流量编排包括大网调度和池内调度，是对安全资源池内资源的综合调度，包括单个安全池内的资源分配及多个安全资源池联动时的资源调度。

3.2 铁路供电信息系统安全资源池功能

安全资源池用于铁路供电信息系统后，在保障铁路供电信息系统安全运行的同时，还能做到各个系统间的逻辑隔离。结合对铁路供电信息系统安全资源池架构的研究，铁路供电信息系统安全资源池功能主要包括以下几点。

3.2.1 用户上网行为管理

用户上网行为管理主要针对铁路供电信息系统的各子系统的用户登录、数据访问等，并根据用户属性进行数据访问限制和文件传输限制等。

3.2.2 日志审计

针对铁路供电信息系统各子系统进行日志监控、日志分析及日志事件告警。对各子系统的运行状况进行实时监控，包括监控CPU及内存等关键区域的占用情况。针对日志监控得到的数据，进行日志分类、分组查询。根据铁路供电信息系统各子系统运行中遇到的常见安全问题，定制日志查询规则，利用日志关联性、字段逻辑关系等属性针对性地发现可疑日志，并及时进行告警。

3.2.3 攻击行为防御

针对铁路供电信息系统各子系统的攻击进行实时监测，对可疑行为重点监控，针对APT攻击实现快速响应和有效溯源。攻击行为防御还具备推理能力，能够从用户行为中发现非正常的访问行为，例如：出现频繁登录、存在撞库可能等，并排查潜在的攻击威胁。

4 关键技术

铁路供电信息系统安全资源池关键技术包括安全资源一体化管理技术和安全资源流量调度技术。

4.1 安全资源一体化管理技术

安全资源一体化管理技术主要包括安全资源动态存储技术和安全资源分配技术等。其中，安全资源动态存储技术指在安全资源池建设与运营过程中对安全资源的存储位置、存储时间、所存储资源的软件包进行升级与控制，可实现安全资源在存储方面的高效、统一；安全资源分配技术指在安全资源池运营过程中针对不同用户的安全服务需求及当前安全资源能够提供的安全服务情况进行安全资源的分配，实现在满足服务需求的同时，节约安全资源的目的。

铁路供电信息系统安全防护需求的安全资源一体化管理技术在安全资源池建设完成后，主要侧重于对安全资源的动态存储资源分配，包括日志审计、数据库审计、终端准入、漏洞扫描、终端防病毒软件资源在安全资源池内的存储及对铁路供电信息系统中不同子系统的分配等。

4.2 安全资源流量调度技术

安全资源的主要作用是提供安全服务，在提供安全服务的过程中，需要根据安全资源的储备情况及用户对安全资源的需求程度进行服务与需求的匹配。在目标防护系统提出安全防护需求后，可通过安全资源池分配管理平台，给出安全资源分配策略，

根据安全需求，通过调用 API 事件，自动触发资源分配流程。

铁路供电信息系统安全资源池的安全资源流量调度技术指安全资源池中安全资源能够满足铁路供电信息系统安全防护需求的条件下，达到安全资源充分利用的技术，包括综合分析铁路供电信息系统的安全防护需求和已有的安全资源池中安全资源的服务能力，达到完全匹配的效果。

5 结束语

本文结合铁路供电信息系统现状及安全资源池的应用现状，研究铁路供电信息系统安全资源池，给出了铁路供电信息系统安全资源池的架构、功能及关键技术，实现安全资源的动态分配，为铁路供电系统安全资源的调度决策提供参考。在接下来的研究中，需要针对铁路供电信息系统的实际部署架构及需要补强的安全防护功能，调整安全资源池的功能，以适用于具体的安全防护需求。

参考文献

[1] 刘 军，朱继强，闫占强，等. 铁路局集团公司供电设备安全综合分析系统的研究 [J]. 铁路计算机应用，2021，30（2）：26-29.

[2] 栗会峰，刘 哲，李宣义，等. 高速铁路牵引变电站电力监控系统安全防护策略 [J]. 河北电力技术，2020，39（5）：1-3，33.

[3] 王 伟，牛昌平，张 超，等. 面向城轨云的安全资源池设计方案与实践 [J]. 铁路技术创新，2023（3）：177-182.

[4] 程子栋. 安全资源池安全组件服务编排研究与实践分析 [J]. 信息安全与通信保密，2023（6）：66-80.

[5] 张永华，林孔升，冯淞耀. 安全资源池数据节点异常自动挖掘方法研究 [J]. 自动化与仪器仪表，2020（7）：73-76.

[6] 张 华，岳 皓. 基于 SDN 的港口安全资源池建设 [J]. 网络空间安全，2020，11（3）：39-43.

[7] 邓飞虎. 高速铁路供电 SCADA 系统的调试措施探讨 [J]. 内燃机与配件，2017（16）：110-111.

[8] 乔凯庆. 关于铁路供电 SCADA 系统主站技术标准的研究 [J]. 电气化铁道，2022，33（1）：8-12.

[9] 陈 霖，刘文韬，张进军，等. 安全资源池在运营商关键信息基础设施中的防护应用 [J]. 通信企业管理，2023（3）：40-43.

[10] 方国强，刘一谦，张常亮. 安全资源池在省级气象网络中的部署及优化 [J]. 成都信息工程大学学报，2022，37（6）：651-655.

[11] 王宏鼎，蔺 旋，李长连. 基于 SD-WAN 的 SASE 云安全资源池方案研究 [J]. 邮电设计技术，2022（9）：49-54.

[12] 彭雄杰，余莎莎，陈 宇. 基于资源池化理念的医院网络安全和效率的平衡研究 [J]. 中国数字医学，2023，18（3）：109-113.

[13] 王志辉. 浅谈金融机构私有云安全资源池建设 [J]. 金融科技时代，2020，28（10）：37-40.

责任编辑 李依诺