DOI: 10.19666/j.rlfd.202405163

电厂数据安全保护系统原型设计

肖力炀[1]，毕玉冰[1]，刘超飞[1]，刘鹏飞[1]，崔逸群[1]，潘瑞丰[2]
（1.西安热工研究院有限公司，陕西 西安 710054；
2.华能（浙江）能源开发有限公司玉环分公司，浙江 台州 317604）

［摘 要］针对电厂数据信息安全问题及数据资产难以集中管控等现状，设计了一种针对电厂场景下的数据全生命周期安全保护原型系统。首先，详细分析了目前电厂数据保护场景领域特殊性和存在问题；其次，针对电厂数据分类分级没有行业标准的缺点，提出了一种自动化分类分级方法，对电厂数据进行标准化的定级和分类；最后，在系统开发方面根据电厂数据保护范围和功能需求分析，完成了原型系统的功能架构设计和技术架构设计。本系统从数据资产梳理、自动化分类分级、全生命周期管理、安全评估等方面给出了具体的工作步骤，提供了电厂数据安全保护的整套解决方案，为后续有效实现电厂数据全生命周期安全提供了依据。

［关 键 词］数据保护；分级分类；数据安全；网络安全；系统原型

［引用本文格式］肖力炀，毕玉冰，刘超飞，等. 电厂数据安全保护系统原型设计[J]. 热力发电，2025，54(1)：132-144.
XIAO Liyang, BI Yubing, LIU Chaofei, et al. Prototype design of power plant data security protection system[J]. Thermal Power Generation, 2025, 54(1): 132-144.

Prototype design of power plant data security protection system

XIAO Liyang[1], BI Yubing[1], LIU Chaofei[1], LIU Pengfei[1], CUI Yiqun[1], PAN Ruifeng[2]
(1.Xi'an Thermal Power Research Institute Co., Ltd., Xi'an 710054, China;
2.Huaneng (Zhejiang) Energy Development Co., Ltd. Yuhuan Branch, Taizhou 317604, China)

Abstract: To address issues such as data information security and difficulty in centralized management and control of data assets, a prototype system for data lifecycle security protection in power plant scenarios is designed. Firstly, the particularity and existing problems of the current field of power plant data protection scenarios are analyzed in detailed. Secondly, in response to the pain point of the lack of industry standards for data classification and grading in power plants, an automated classification and grading method is proposed to standardize the grading and classification of power plant data. Finally, in terms of system development, based on the analysis of the scope of power plant data protection and functional requirements, the functional architecture design and technical architecture design of the prototype system are completed. This system provides specific work steps from data asset sorting, automated classification and grading, full lifecycle management, security assessment, and other aspects, providing a complete solution for data security protection in power plants, and providing a basis for effectively achieving full lifecycle security of power plant data in the future.
Key words: data protection; grading and classification; data security; cyber security; system prototype

随着数字经济的快速发展和高精尖技术的蓬勃兴起，全球正式进入大数据时代，数据对一个企业乃至国家都属于不可或缺的资源[1]。电力行业是拥有较多关键信息基础设施的重要行业，随着电力企业向数字化、智能化发展，电力行业各设备系统不断融合新技术，逐渐走向互联互通，与此同时数据安全问题亦是日益凸显[2]。电力数据作为关键生产要素，包括营销、财务、物资、生产等海量数据，具有数量多、规模大、覆盖面广、价值高等特点，具备大数据应用条件，对于电厂来说尤

收 稿 日 期：2024-05-28 网络首发日期：2024-11-18
基 金 项 目：中国华能集团有限公司总部科技项目（HNKJ21-H29）
Supported by：Science and Technology Project of China Huaneng Group Co., Ltd. (HNKJ21-H29)
第一作者简介：肖力炀（1996），女，硕士，工程师，主要研究方向为网络安全与信息安全，xiaoliyang@tpri.com.cn。

为重要[3]。然而由于自身网络环境复杂、业务流程特殊、系统结构繁杂等特性，电厂数据安全面临着严峻的威胁与挑战，同时也是网络攻击者的主要窃取目标[4-5]。

2014 年南方电网平台出现了用户敏感信息泄露问题，用户信息被不法分子窃取，对公司绩效和声望均造成了严重影响；2018 年黑客窃取了法国某公司逾 65 G 关于核电站计划和个人信息的文件数据，将该核电站及公司员工置于恐怖主义阴谋等诸多威胁之下；2019 年南非一电力公司遭遇勒索软件攻击，黑客利用病毒加密了所有数据库、应用程序和官方网站数据，造成若干居民区的电力中断；2021 年美国某电力协会遭到网络攻击，导致其 90% 的内部系统瘫痪，25 年的历史数据丢失。国内外大量案例均表明敏感数据的泄漏会对电力企业利益带来巨大损害，包括客户流失、核心技术丢失、声誉受损、法律问题等[6-9]。基于对数据安全的考虑，世界各国政府也相继出台了数据保护相关的法律法规[10]，我国于 2017 年颁布了《中华人民共和国网络安全法》，2021 年开始实施《数据安全法》和《个人信息保护法》，2023 年 10 月国家数据局也正式挂牌成立，这些都表明数据安全问题越来越受到国家和政府的重视[11-12]。

近年来，在电力系统互联互通发展趋势、攻击手段不断升级、数据存储方式愈发依赖联网设备等因素的多重影响下，电力行业数据安全正面临全新的挑战，如数据窃取、数据泄露、数据篡改、数据跨境流动等[13]。数据安全对于电力企业而言不单单是经济损失，更有可能影响到国家安全，导致灾难性的后果[14]。通过攻击电力企业数据获取电力信息系统的关键性、敏感性数据，如系统运行图、网络拓扑图、资产清单等，可以分析出其内部设施设备的运行情况、网络防护的分布情况、生产控制系统的配置情况等，通过篡改关键节点监测预警信息、操作指令等关键数据，可能造成电力系统故障或重大安全事故[15-16]。因此，针对上述存在问题，开展电厂数据保护，完善数据保护体系，增强关键信息安全保护的整体性、针对性和时效性具有非常重要的意义。基于上述背景，并综合对多个电厂的调研分析，本文构思了一种针对电厂场景下的数据全生命周期安全保护原型系统，集资产管理、自动化分类分级、全生命周期保护、安全评估管理、系统管理于一体，构建全局视角下的数据安全能力。

1 电厂数据保护面临现状

1.1 场景特殊性

发电企业数据保护存在如下特殊性：1）电厂采用内外网隔离方式，对数据采集、传输等带来了挑战；2）生产连续性要求高，监管考核处罚力度大，系统对第三方应用的扰动敏感，系统接入难度大；3）电厂普遍缺乏专业的数据工作和管理人员，这对数据全生命周期各环节自动化和智能化提出了更高要求；4）电厂中有大量工控系统存在，这些系统往往不具备改造条件，对数据采集、接入等增加了困难；5）现有设备系统分散，日志之间关联少，无法协作，缺少推理总结性描述等业务维度分析；6）电厂数据来源于信息管理系统、web 应用、生产控制、生产监管等各类系统，涉及服务器、主机、移动终端、数据平台、工控设施、传感控制装置等一系列设备，数据来源广泛，管理难度极大。

1.2 存在问题

针对上述发电场景特殊性，电厂数据保护主要面临以下几个问题：

1）电厂分类分级没有行业标准。目前没有专门针对电厂数据的分类分级解决方案及规范，导致以电厂数据安全为主的数据防泄露、防篡改、数据脱敏、数据流转管控、数据分级保护等都难以得到有效开展，存在引起电力系统故障或重大安全事故的风险。

2）数据安全能力碎片化。电力生产管理过程中产生的各种生产数据、管理数据、运营数据、个人数据等分散在大量的不同信息系统、办公计算机、运维设备、移动终端中，各电厂业务系统各自孤立，防护设备管理分散[17]，导致数据资产分布情况不明，设备之间缺乏联动，无法对数据进行有效管理。

3）数据访问及流向不清。信息系统中转移到物理界的数据缺少访问控制机制，数据流向、数据访问缺少有效记录；生产控制大区内部、管理信息大区内部、生产控制大区和管理信息大区之间的数据访问依托接口控制，但存在接口未采用身份认证、鉴权和加密情况，无法判断、跟踪数据访问历史路径等。

4）缺乏针对电厂场景下的数据保护系统。电力企业至今没有适合电力生产和管理数据安全保护的系统，电厂缺乏数据分类分级能力，且没有合适工具支持，多以传统 IT 资产管理方式为主，缺乏

有效的可视化、跟踪、加密、身份认证、脱敏等技术监控和保护。市面上已有方案没有结合电力生产场景进行考虑，现有产品难以满足电厂实际需求。

1.3 整体设计

本文首先对电厂数据进行资产梳理，全面清晰地厘清数据资产，形成可实施的数据安全分类分级方法，再根据分类分级结果，对数据全生命周期进行保护管理，保障数据全生命周期安全，最后进入数据安全运营阶段。整体方案设计如图 1 所示。

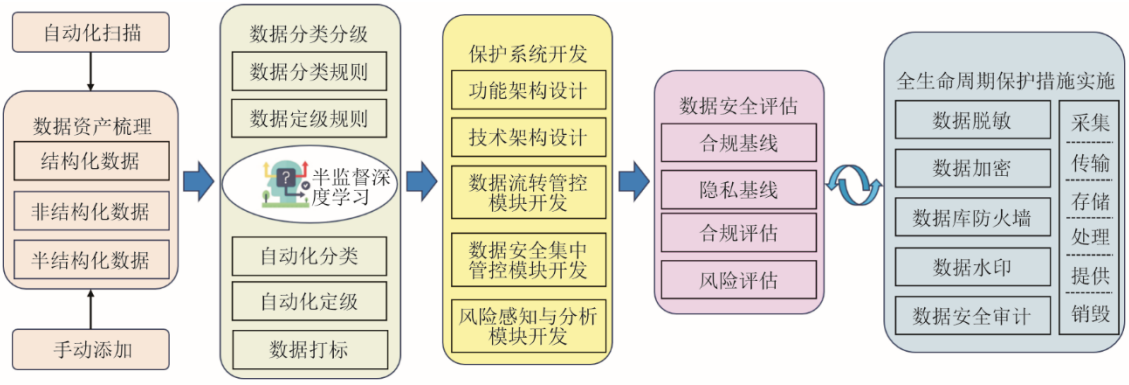

图 1 整体方案设计

Fig.1 Overall scheme design diagram

2 方案设计

2.1 电厂数据资产梳理

为使数据资产管理工作规范化，可以按照职能部门划分，落实数据资产管理责任，面向电厂内各个业务系统开展数据资产盘查，促进电厂对数据资产的有效管理，具体如下。

1）对电厂的结构化数据库、半结构化的接口信息、非结构化的图片和文字等进行全面梳理，形成数据资产库，对不同来源、不同类型的数据资产完成规范化、系统化的归并和整理。

2）通过指定 IP 地址段的自动化扫描、用户手动添加、资产目录的批量导入等多种方式，进行数据资产信息的新增，对已有数据资产信息提供查询、修改、删除、导出等操作。

3）生成数据资产管理台账，明确数据资产的种类、来源、内容和用途及数据资产的权属关系、应用场景，清晰地展示电厂内所有数据资产信息，方便电厂业务人员管理各项数据资产。

4）建立数据资产管理视图，显示内容可包括资产类型、资产数量、资产分布等，为用户直观展示管理效果。

2.2 电厂数据分类分级

2.2.1 数据分类

电厂中业务数据体量庞大，数据类型多样，数据存储呈现碎片化分布特征，数据使用还具有时变性、不确定性等特征，使得数据管理难度极大[18]。为更好地维护和使用数据，本文以火电厂为例，结合电厂内业务系统应用情况，实现对电厂数据的区分和归类。

本文将电厂数据分为研发数据、生产运行数据、运维数据、管理数据和业务服务数据 5 个一级类别，在数据一级划分的基础上[19]，综合考虑数据来源情况、数据存储情况、数据应用情况，进一步细分数据的 17 个二级子类、更细的三级子类等细类。其中，数据来源具体包括产生部门、产生场景、获取方式及频率等，数据存储具体包括存储方式、存储位置、数据格式、数据规模等，而数据应用情况又包括应用场景、应用方式等。具体分类情况详见表 1。

2.2.2 数据分级

电厂中数据在密级程度、可公开性质上具有显著差异，不同重要性的数据应采用不同的保护策略。目前电厂缺乏科学标准的评价体系，对于哪些数据可以使用、哪些数据能对外开放、哪些数据实施应用监管等问题难以掌握厘清。因此，在数据分类基础上，还需进一步对其定级评估，避免数据泄露或不当处理所造成的安全风险[20-21]。表 2 为本文给出的数据安全常规定级规则。

表 1 电厂数据分类
Tab.1 Classification of power plant data

序号	一级子类	二级子类	对应数据
1	研发数据	科技管理数据	科技成果报告、试验测试数据、专利书等
2		规划建设类数据	项目建设方案、批示专利性文件、样机图纸、建筑安装图等
3	生产运行数据	生产监控数据	环境信息、磨煤机数据、给水泵数据、厂用电数据、运行规程、煤仓相关数据等
4		工业控制数据	组态数据、控制指令、稳控系统控制数据、煤质化验数据、负荷调节等
5		工业生产状况信息	锅炉专业数据、汽轮机专业数据、电气专业数据、供热数据、环保数据等
6		生产工艺参数信息	温度、压力、流量、液位、转速、开度等
7		日志信息	服务器日志、安全防护设备日志、缺陷记录、系统自动告警日志等
8	运维数据	网络与系统运维数据	网段、网址、VALN 分配、流量监测、网络系统统计分析数据等
9		网络安全管理数据	安全审计记录、安全评估数据、攻击信息、漏扫缺陷信息等
10		检修管理数据	技术方案及三措两案管理、设备检修与质量管理、热工保护自动装置投退及整定值管理数据等
11	管理数据	企业经营管理数据	岗位标准数据、采购管理数据、财务和审计管理数据等
12		网络与系统管理资源数据	电网辅助通信类数据、传输资源类数据、IT 及工控系统资源数据等
13		设备资产管理资源数据	设备台账、建筑台账、系统台账等
14		个人信息数据	员工基本信息、网络身份标识等
15	业务服务数据	交换类数据	电力交换数据、电网交换数据
16		共享类数据	检修计划、发电情况等
17		交易类数据	交易电量数据等

表 2 数据安全常规定级规则
Tab.2 General grading rules for data security

数据定级要素			数据的一般特征	数据重要程度标识	数据级别标识
影响对象	影响范围	影响程度			
K/S/G	行业	非常严重	①数据安全性遭到破坏后，影响对象是国家、社会或电力市场；影响范围是多个行业或电力行业内多个机构；影响程度一般是“非常严重”； ②只针对特定的人员公开，且只为必须知悉的对象访问或使用	极高	4 级
K/S/G	行业	严重			
G	企业	非常严重			
S	企业	非常严重			
K	企业	非常严重			
K	机构	非常严重			
K/S/G	行业	中等	①数据的安全性遭到破坏后，影响范围一般是电力行业内多个机构或本机构，影响程度一般是“严重”； ②重要业务使用的数据，针对特定的人员公开，且只为必须知悉的对象访问或使用	高	3 级
G	企业	严重			
S	企业	严重			
S	机构	非常严重			
S	机构	严重			
K	企业	严重			
K	机构	严重			
K/S/G	行业	轻微	①数据的安全性遭到破坏后，影响范围一般为本机构，影响程度一般是“中等”； ②一般业务使用的数据，针对部分对象公开；一般用于内部管理或办公，不适合广泛公开	中	2 级
G	企业	中等			
S	企业	中等			
S	机构	中等			
K	企业	中等			
K	机构	中等			
G	企业	轻微	①数据的安全性遭到破坏后，影响范围是本机构，影响程度一般是“轻微”或“无”； ②可被公开或可被公众使用的数据	低	1 级
S	企业	轻微			
S	机构	轻微			
K	企业	轻微			
K	机构	轻微			

注：K 表示客户/个人；S 表示社会秩序/公共利益；G 表示国家安全。

本文给出的数据定级方法分为 5 个步骤，分别是常规定级流程、由数据敏感性定级、由与生产业务关联性定级、由与业务系统关联性定级及最终定级。敏感性定级主要依据电厂的相关规定，先确定

数据的敏感级别，再结合常规定级过程中确定的影响程度，确定数据的安全级别；与生产业务关联性定级主要依据《工业数据分类分级指南》，先确定数据的工业数据等级，然后结合常规定级过程中确定的影响程度，确定数据的安全级别；与业务系统关联性定级主要依据《信息系统安全等级保护定级指南》，先确定数据的业务信息安全等级，然后结合常规定级过程中确定的影响程度确定数据的安全级别。定级流程如图 2 所示。

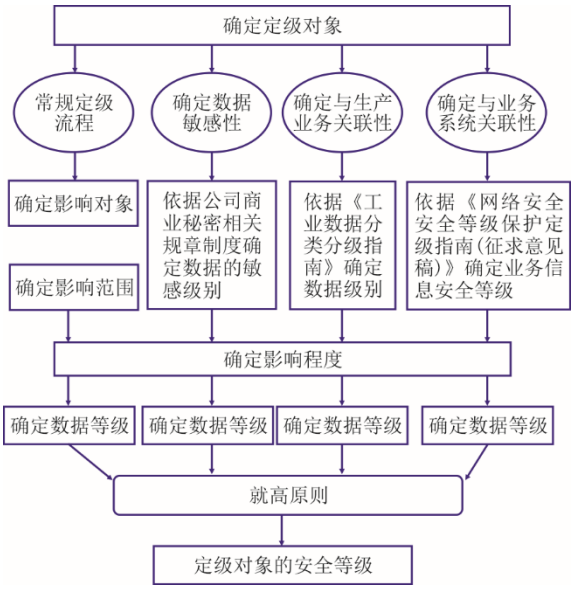

图 2 电厂数据定级流程

Fig.2 Power plant data grading process

通过常规定级、由数据敏感性定级、由与生产业务关联性定级、由与业务系统关联性定级，确定定级对象数据的 4 个安全级别，根据就高原则确定定级对象的最终等级。本文给出数据分级相关信息为：数据分级有 C（公开）、B（普通）、A（敏感）、S（机密）4 级；影响对象有个人、部门、电厂、区域公司、集团公司、电网；影响范围是对象的集合；影响级别有特别严重、严重、一般、轻微。

2.2.3 自动化分类分级

目前数据分类分级方法多为人工手动完成，存在效率低、成本高、主观性强等很多问题[22]。为实现自动化分类分级，本文摒弃传统的数据分类分级方法中人工打标的弊端，提出一种基于深度学习的半监督数据分类分级方法，来完成电厂领域中的海量数据的自动化分类分级。

上节将电厂数据分为研发、生产运行、运维、管理和业务服务 5 个一级类别和若干子类别，数据级别分为 C（公开数据）、B（普通数据）、A（敏感数据）、S（机密数据）4 个级别，本系统通过深度学习技术进行数据自动分类分级，图 3 为自动化分类分级原理。由图 3 可见，首先录入需要扫描的数据源，可采用国产化数据库，支持达梦、海量、PostgreSQL、Mysql 等主流数据库，然后送入半监督学习引擎中进行数据资产的摸底和打标，人工标注少量数据，并通过无监督学习实现其余大量数据的相似字段分析，自动提取数据库字段特征和相似列特征，实现批量化打标，从而建立分类分级标签特征模型，模型采用多层卷积神经网络[23]，并嵌入 Word2Vec 算法[24]对短句等进行词向量训练，对样本间关系进行特征挖掘的同时，学习输入和输出标签之间的相关性，从而自动提取数据库字段特征和相似列特征，有效提取语义及上下文信息，建立分类分级标签特征模型，实现电厂数据的自动化分类分级。

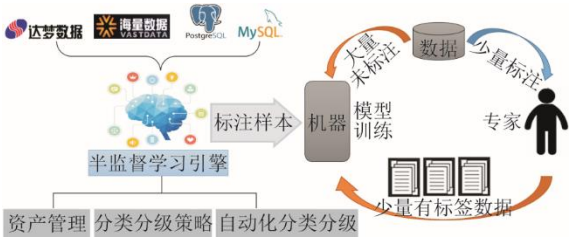

图 3 自动化分类分级原理

Fig.3 Automated classification and grading principle

这种方法不仅可以应对数字、日期、文本等多种数据类型，还能够处理多维度和复杂关系的数据。对于文本等非结构化数据，采用了自然语言处理（NLP）技术，以深度学习模型来理解和分析数据，动态实现对电厂业务数据的自动分类分级。

2.3 数据全生命周期管理

全生命周期管理包括数据采集、传输、存储、处理、提供、销毁的不同生命周期阶段的管理，采用数据库识别与检索、SQL 解析、数据脱敏、数据加密、安全审计、数据库防火墙等技术和差异化保护措施，实现对数据安全保护过程的监视和管理。

2.3.1 数据采集

数据采集包括电厂内部系统之间获取数据、电厂从系统外部获取数据以及安全保护系统从电厂获取数据 3 种形式，数据量庞大、管理难度极高。对此，本文采用抽样采集方式，在部分过程（如数据的接入）定时采集一定比例的最新小样本数据，由于各类数据具有相同表、字段等结构，通过抽样并定期更新的方式，极大降低了后续数据的管理成

本和资源。本文通过建立数据源管理台账，明确数据源类型、接口类型、业务权属、责任主体等，支持自动识别和手动录入等方式，对电厂内部数据源进行统一管理；根据电厂实际情况，制定数据采集规则和接口管理方案，支持规则的灵活配置，管理包括 WebService、OPC、RPC、RESTful、HTTP 在内的多类型接口；对采集数据的合规性和可靠性验证，避免垃圾数据和脏数据采集入库；对采集数据的分类分级校验，对数据定级异常进行告警，同步更新数据的分类分级结果；建立数据采集管理制度，明确数据采集的渠道、范围、方式、周期等内容，规范从电厂外部获取数据的审批、备案流程。

其次，采集到本系统设备的数据仅能通过系统自身部署的数据代理 Agent、API 接口采集，采集过程中使用了代理注册、接口鉴权、身份认证、白名单等措施，确保只有被系统设备注册为合法的数据代理、API 接口才能上传数据，能有效防范设备篡改、中间人攻击；传输过程采用了数据加密技术、数字签名技术，能有效防范恶意数据注入、数据截取和窃取攻击；本设备主要用于电厂管理大区、生产控制大区内部，不与互联网连接，内部的防 DDOS、DOS 等拒绝服务攻击的措施，依赖于电厂管理大区或生产控制大区的防拒绝服务攻击措施。

2.3.2 数据传输

电厂生产控制大区与信息管理大区之间虽然采用网络分区的管理模式，但跨区域网络的数据传输依然存在很多风险隐患。在数据传输过程中，可能存在非法旁路监听导致核心或重要数据的泄露，也可能有中间人等恶意攻击导致业务数据被篡改，在大数据交互的复杂传输网络中，难以跟踪、记录数据传输路径。

本文通过对采集到的小样本数据传输加密保护，包括 API 加密、传输协议加密等，对核心数据、重要数据使用差异化的加密措施，防止数据传输过程中的重要信息泄露；对数据传输过程的异常监测，包括系统连接断开、恶意流量请求等，形成告警清单，避免因系统故障、网络故障或恶意攻击等原因影响数据传输；生成数据流向图，反映数据在各个系统间的流转情况，能够记录数据传输的时间、方式等操作信息，帮助电厂业务人员及时发现数据违规流转、风险流转等隐患；建立身份认证、数据加密、监测预警等相关制度，保障数据传输链路安全；通过制定数据传输规则进行流向比对，对异常数据流向生成告警通知，并对该时段下全部数据进一步采集与分析，提高低成本、可落地的数据管理。

2.3.3 数据存储

电厂内的数据存储介质涵盖各类系统的数据服务器、数据管理平台以及电厂员工的计算机终端、移动终端、移动磁盘等，数据存储分散，管理难度极大。传统数据存储方式是将采集到的数据统一放到数据湖或数据中心进行存储，本文则使用一台一体化的设备存储数据，全量数据仍然存储在各自应用系统中。通过建立数据存储介质管理台账，明确数据存储的介质类型、存储方式、部署位置、加密情况、业务权属、责任主体等，支持自动识别和手动录入等方式，对电厂数据存储介质进行统一管理；定期核验存储介质的使用情况，包括使用人员信息、使用周期、拷贝情况、借调情况等，对可移动存储介质进行跟踪记录；对数据库的漏洞扫描或与第三方漏洞管理平台对接，实现数据库安全统一管理；生成数据分布图，反映数据在各个存储介质的分布情况，能够统计数据库表总量、字段总量、文件总量等信息，可支持单个或多个数据分布的查看；同时制定数据存储制度规则，定时监测发现异常并形成告警通知。

2.3.4 数据处理

电厂中所有信息系统、工控系统的运行都脱离不了数据的加工处理，但在数据使用时缺少全面、系统的监测机制。在数据处理过程中，哪些数据被访问、使用、使用者身份是否合规等都没有相应记录，同时核心数据、重要数据在加工处理时没有对数据进行脱敏处理，难以防止未授权访问后的数据窃取。

传统数据处理是通过平台调接口进行分析，本文采用平台定义处理规则的方式，对核心数据、重要数据进行脱敏处理，在保证数据可用性不变的前提下，清除数据所包含的敏感信息，防止数据处理过程中的重要信息泄露；对数据处理过程中重大突发事件的审计跟踪，形成告警清单并实现应急处置，及时隔离、阻断相应系统的数据接口，避免数据安全事件影响范围的扩大；建立数据访问控制、数据脱敏、操作审计等相关制度，保障数据处理环境安全与过程安全。

2.3.5 数据提供

数据提供涉及内部系统之间或内部系统向外部组织机构及个人传递数据，可能存在的风险体现为对数据提供事务的审批管理欠缺、对数据交互过程的监管记录不够、对递交数据的安全性评估不足。为了保障数据提供的完整性、可靠性和可用性，本文采用建立数据提供台账，明确提供数据的内容、范围、使用期限等，能够对提供数据使用超期等情况进行告警，方便电厂业务人员对数据提供进行管理；对提供数据进行加密保护，支持国产化加密，实现一密一钥，避免提供数据的过度共享与转发；对核心数据、重要数据进行脱敏处理，防止数据提供过程中的重要信息泄露；实现数据资产转移情况的跟踪记录，当数据资产权属变更后同步更新数据资产台账，确保数据资产的账、人、物等信息相符；建立数据提供管理制度，明确数据提供的原则、条件、实施方法、审批流程、备案流程、安全责任等内容，通过系统数据资产地图进行流程比对，如有异常数据及时发布告警，对数据共享、发布、移交、下载等高危敏感操作制定安全防护方案。

2.3.6 数据销毁

电厂内数据体量庞大，在业务运行期间不可避免会有大量数据销毁，现阶段缺乏对数据销毁的监督机制，难以避免数据销毁不完全或存储介质未销毁而导致的敏感数据恢复。数据销毁应当包含对数据本身及数据存储介质的销毁，当业务数据周期结束或数据内容发生改变时，都需要对数据进行合法合规的销毁操作。

本文通过建立数据销毁台账，明确被销毁数据的种类、来源、内容、用途、权属关系、应用场景等，能够关联更新数据资产台账，对达到销毁条件或有销毁需要的数据资产进行管理；建立数据销毁工具台账，明确销毁工具的类型、方式、部署位置、业务权属、责任主体等，能够对销毁工具进行统一管理；对不同级别的数据选择合适的销毁措施，包括对一般数据采取的覆盖式清除，对核心数据、重要数据采取的物理销毁式清除，保证已销毁数据不可再恢复；持委派专人或指定具有认定资质的服务商进行数据资产的销毁，对销毁过程的记录和监督；建立数据销毁管理制度，明确数据销毁的条件、方式、审批流程、销毁流程、归档流程等，形成闭环确认，对于其他系统数据，通过 API 等接入形式，从审批制度、流程等方面进行管理，加强电厂业务人员对数据资产的有效管理。

2.4 电厂数据安全评估管理

电厂中数据产生、流通和应用场景多样化，导致各类安全威胁风险愈加复杂，为促进电厂数据安全规划和发展，亟需开展数据安全评估，发现数据安全隐患，防范数据安全威胁。

建立数据安全合规基线，明确数据合规内容与边界，支持多维度的基线定义，支持基线自由组合和个性化配置，为数据访问控制、违规操作等提供基准；建立数据安全隐私基线，明确数据隐私保护的对象和方法，支持多维度的基线定义，支持基线自由组合和个性化配置，为数据防泄密、隐私保护提供基准；生成数据安全评估报告，能够从管理人员、运维人员、用户等不同角度，全面展示数据安全风险相关信息，支持多种格式的报告导出，帮助电厂安全管理人员及早发现问题，及时整改不足，降低风险隐患给电厂造成的严重危害；能够基于数据安全评估报告生成问题清单，包括问题数量、问题状态、办理时效、涉及资产、办理人员等内容，通过工单的分发为电厂掌握数据安全保护情况提供参考；建立数据安全评估管理制度，明确数据安全评估的依据标准、评估要求、量化指标、评估方式、评估流程、反馈流程等内容，保障电厂在数据资产管理、数据分类分级管理和数据全生命周期管理过程中数据安全工作的落实。

3 数据安全保护系统原型设计

3.1 功能架构设计

数据安全保护原型系统功能架构如图 4 所示，功能架构可分为数据采集层、底层支撑层、安全能力层和管理能力层。

数据采集层 采用静态扫描和动态流量识别，结合和人工经验，实现结构化数据和非结构化数据的全面梳理，为用户建立精准可靠的数据资产台账、形成完整数据分类分级清单。

底层支撑层 针对不同的数据来源，基于权限剥离、可信计算、病毒入侵防范、全面监控的可信底座，开发各类数据接口，采集各类日志信息，完成数据存储。

安全能力层 基于数据资产梳理实现资产的分类分级，形成完整数据分类分级清单。采用数据库动态基线检测技术等实现对数据库所有访问行为的记录、监控、追踪溯源；通过对 web 应用系统

的流量进行旁路（镜像）采集和分析，对 web 应用系统中的操作全审计；采用抑制、泛化、扰乱、随机四大类脱敏技术，满足敏感数据降级使用要求；完成数据库防火墙、数据库加密等安全能力建设。

管理能力层　数据流转管控能力提供文件加密保护、权限控制和外发审计的数据防泄露能力，数据安全集中管控能力是指通过接口对接数据安全相关设备实现对数据安全管控策略统一管理、安全事件统一处置，数据安全风险感知与分析能力是指通过建模与智能学习，对数据安全风险进行研判，进行统一态势感知展示。

图 4　原型系统功能架构

Fig.4 Functional architecture of the prototype system

3.2 技术架构设计

数据安全保护原型系统技术架构如图 5 所示，从系统开发角度，数据安全保护系统可分为数据源层、数据处理层、安全措施层、应用层。

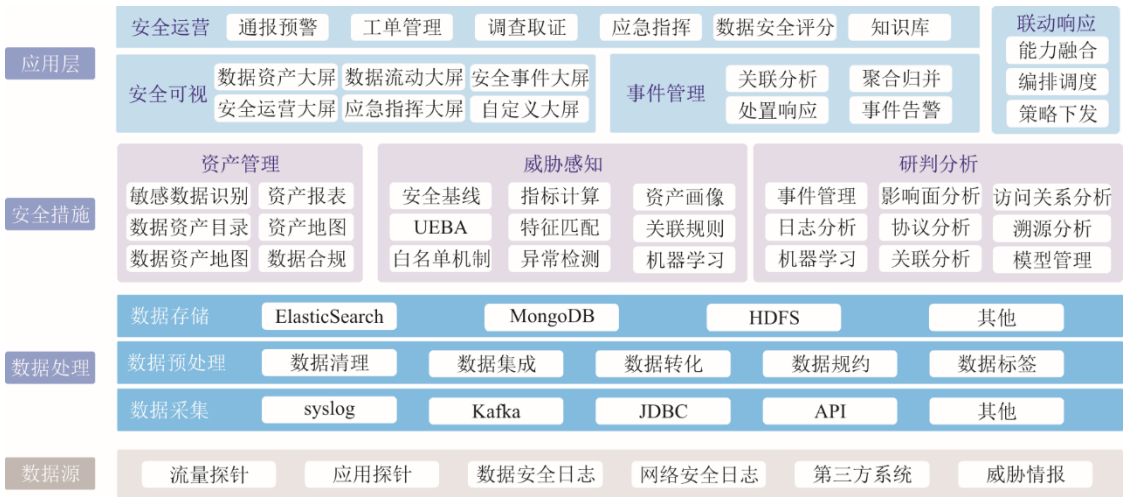

图 5　原型系统技术架构

Fig.5 Technical architecture of the prototype system

数据源层　按数据来源和接口类型对数据进行分类，包括流量探针、应用探针、数据安全日志、网络安全日志、威胁情报等。

数据处理层　采用 syslog、JDBC、API 等方式进行数据采集，经过数据清洗、数据集成、数据转化等预处理后，存入 ElasticSearch、MongoDB、HDFS

等数据库。

安全措施层 针对数据全生命周期的各个环节，采取对应的敏感数据识别、指标计算、关联分析等技术措施，实现数据资产管理、威胁感知和研判分析。

应用层 为用户提供数据资产大屏、数据流转大屏等数据安全可视化和事件告警、聚合归并等事件管理功能，实现日常的数据安全运营，在发生数据安全事件时实现联动响应。

3.3 原型系统平台设计

3.3.1 部署说明

本文采用 JAVA Spring 框架作为数据安全保护系统的开发框架，前端采用 JSP+AJAX 实现后台交互，后端采用 SpringMVC，相关环境设备及配置见表 3。

表 3 环境配置说明
Tab.3 Environmental configuration instructions

设备名称	版本
操作系统	Centos 7.9 标准版
CPU	ARM 8 核 16G
JDK	1.8.1
Tomcat	9.0.46
Redis	5.0.14
Mysql	5.7
Maven	3.8.1
jQuery	3.7.1
Spring	5.3.0

本文所设计原型系统可在电厂进行部署，其中生产环境包括业务服务器和生产库等，部署方式为旁路部署，只需与数据库之间进行网络互通，不影响业务网络，图 6 为数据安全保护原型系统部署。

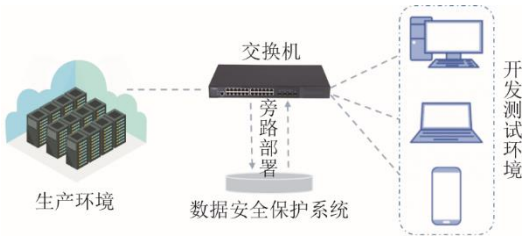

图 6 数据安全保护原型系统部署
Fig.6 Deployment of data security protection prototype system

3.3.2 数据可视化原型

通过对数据安全保护系统中每个模块的关键数据进行提取，将数据资产情况、使用情况（数据采集统计、接口数量）、数据分类分级、数据分布情况、数据的流转情况、数据规模等重要数据，以饼状图、柱状图等多种形式集中展示出来，并将数据安全评估结果、安全风险等用户关心问题进行直观展示[25-27]。

图 7 为本文设计数据安全可视化态势原型界面，该系统支持资产总量、账户总量、数据总量、数据分布等可视化展示，为用户直观展示效果，且便于集中对电厂数据资产进行统计和分析。

图 7 系统可视化界面
Fig.7 System visualization interface

3.3.3 部分界面展示

图 8—图 11 分别为本系统数据资产梳理、分类分级、数据分类分级导图、数据源录入和存储等部分原型展示。

图 8 数据资产梳理原型

Fig.8 Prototype of data asset sorting

图 9 数据分类分级原型

Fig.9 Prototype of data classification and grading

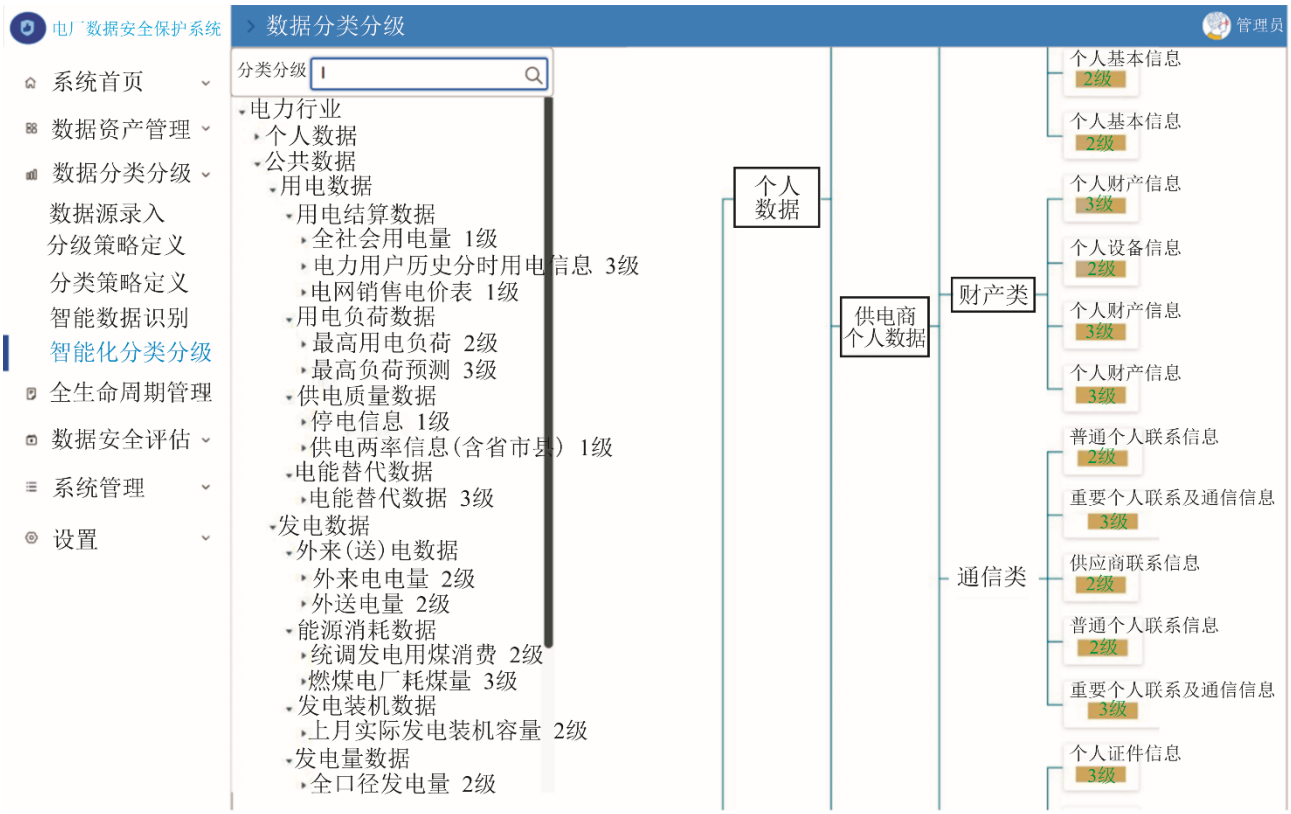

图 10 分类分级导图原型

Fig.10 Prototype of classification and grading map

图 11 数据源录入和存储原型

Fig.11 Prototype of data source input and storage

4 结　语

本文首次为发电行业实现电厂数据的分类分级提供了一套完整可行的方案，为开发电厂数据安全工作相关的系统提供了理论支撑和技术支持。

本文针对电厂的实际情况、当前技术水平和业务需要，采用国产化架构、国密，对标发电侧电力数据的分类分级规范，适用生产控制大区、管理信息大区数据，技术架构成熟，稳定性、可靠性、可扩展性强；从经济角度考虑，本系统没有采用传统的数据湖、大数据中心等方式，而采用小样本抽样的方式，通过结合发电场景的功能设计，可降低数据保护建设的成本、维护成本以及人力成本，为业

界提供低成本、可落地的数据全生命周期安全保护提供了新的思路。

未来本文可针对小样本抽样、流程自动编排等环节做出完善和提高，以及进一步应用于新能源电厂领域的数据全生命周期保护。

［参 考 文 献］

［1］ 中国信息通信研究院. 中国数字经济发展白皮书(2020)[EB/OL]. (2020-12-01) [2024-02-10]. https://baijiahao.baidu.com/s?id=1671829565921459468&wfr=spider&for=pc.

［2］ China Academy of Information and Communications Technology. White paper on the development of China’s digital economy (2020) [EB/OL]. (2020-12-01) [2024-02-10]. https://baijiahao.baidu.com/s?id=1671829565921459468&wfr=spider&for=pc.

［3］ 黄万忠. 数字化转型下的数据安全管理实践[J]. 软件和集成电路, 2022(1): 40-41.
HUANG Wanzhong. Data security management practice under digital transformation[J]. Software and Integrated Circuits, 2022(1): 40-41.

［4］ 陈如明. 大数据时代的挑战 价值与应对策略[J]. 移动通信, 2012(17): 14-15.
CHEN Ruming. The challenges, values, and response strategies in the era of big data[J]. Mobile Communications, 2012 (17): 14-15.

［5］ 龙震岳, 钱扬, 邹洪, 等. 电网企业网络信息安全的威胁与攻防新技术研究[J]. 现代电子技术, 2015, 38(21): 100-104.
LONG Zhenyue, QIAN Yang, ZOU Hong, et al. Threat to network information security and study on new defense technologies in power grid enterprises[J]. Modern Electronics Technique, 2015, 38(21): 100-104.

［6］ YUAN X P, WANG H Y, YUAN Y, et al. Design of an intelligent decision model for power grid fault location and isolation based on topology analysis[J]. International Journal of Thermofluids, 2024(21): 1-10.

［7］ 应欢, 刘松华, 韩丽芳, 等. 电力工业控制系统安全技术综述[J]. 电力信息与通信技术, 2018, 16(3): 56-63.
YING Huan, LIU Songhua, HAN Lifang, et al. Overview of power industry control system security technology[J]. Electric Power ICT, 2018, 16(3): 56-63.

［8］ 吴泽君. 利用数据泄漏防护保护企业数据安全[J]. 计算机安全, 2010(1): 81-85.
WU Zejun. Using data leakage protection to protect enterprise data security[J]. Computer Security, 2010(1): 81-85.

［9］ 赵梦. 基于大数据环境的网络安全态势感知[J]. 信息网络安全, 2016(9): 90-93.
ZHAO Meng. Network security situation awareness based on big data[J]. Netinfo Security, 2016(9): 90-93.

［10］KUMAR S V, ANNAMALAI A, BAPTIST J L A. Cybersecurity challenges in energy sector (virtual power plants): can edge computing principles be applied to enhance security?[J]. Energy Informatics, 2021, 4(1): 1-21.

［11］梅傲, 陈子文. 总体国家安全观视域下我国数据安全监管的制度构建[J]. 电子政务, 2023(11): 104-115.
MEI Ao, CHEN Ziwen. Institutional construction of data security supervision in China from the perspective of overall national security concept[J]. E-Government, 2023(11): 104-115.

［12］何天玲. 电力数据通信网安全防护方案的分析和研究[J]. 电力信息与通信技术, 2020, 18(1): 74-79.
HE Tianling. Analysis and research on network security protection scheme in power data communication network [J]. Power Information and Communication Technology, 2020, 18(1): 74-79.

［13］梅传强, 盛浩. 数据安全刑法保护的模式转换: 从管理安全到利用安全[J/OL]. 重庆大学学报(社会科学版), 2024: 1-18. [2024-11-05]. http://kns.cnki.net/kcms/detail/50.1023.C.20240125.1612.004.html.
MEI Chuanqiang, SHENG Hao. Mode transformation of criminal law protection of data security: from management security to utilization security[J]. Journal of Chongqing University (Social Science Edition), 2024: 1-18. [2024-11-05]. http://kns.cnki.net/ kcms/detail/50. 1023.C.20240125. 1612.004.html.

［14］管磊, 胡光俊, 王专. 基于大数据的网络安全态势感知技术研究[J]. 信息网络安全, 2016(9): 45-50.
GUAN Lei, HU Guangjun, WANG Zhuan. Research on network security situational awareness technology based on big data[J]. Netinfo Security, 2016(9): 45-50.

［15］裘宇超. 基于多源异构大数据的发电厂安全管控系统分析[J]. 集成电路应用, 2023, 40(12): 70-72.
QIU Yuchao. Analysis of power plant safety control system based on multi source heterogeneous big data[J]. Integrated Circuit Application, 2023, 40(12): 70-72.

［16］CHOHWAN O, HYEON D K, IK J L. Application of data driven modeling and sensitivity analysis of constitutive equations for improving nuclear power plant safety analysis code[J]. Nuclear Engineering and Technology, 2023, 55(1): 131-143.

［17］朱磊. 探讨智慧电厂下的数据网络安全体系[J]. 电子元器件与信息技术, 2021, 5(9): 252-254.
ZHU Lei. Exploring the data network security system under smart power plants[J]. Electronic Components and Information Technology, 2021, 5(9): 252-254.

［18］陈驰, 马红霞, 赵延帅. 基于分类分级的数据资产安全管控平台设计与实现[J]. 计算机应用, 2016, 36(增刊 1): 265-268.
CHEN Chi, MA Hongxia, ZHAO Yanshuai. Data security control platform based on hierarchical classification: design and implementation[J]. Computer Applications, 2016, 36(Suppl.1): 265-268.

［19］周亮, 张晓娟, 邱意民, 等. 电力数据分类分级方法研究[J]. 电力信息与通信技术, 2023, 21(4): 25-30.
ZHOU Liang, ZHANG Xiaojuan, QIU Yimin, et al. Research on power data classification and grading method[J]. Electric Power Information and Communication Technology, 2023, 21(4): 25-30.

［20］陈亚茹, 洪鑫, 张红斌, 等. 铁路运输调度领域数据分级及保护策略研究[J]. 铁道运输与经济, 2024, 46(2): 134-141.
CHEN Yaru, HONG Xin, ZHANG Hongbin, et al. Data classification and protection strategy in railway transportation dispatching[J]. Railway Transportation and Economics, 2024, 46(2): 134-141.

［21］张晓艺, 戴逸聪. 水利数据分类分级及安全保护技术[J]. 人民长江, 2023, 54(增刊 2): 232-237.
ZHANG Xiaoyi, DAI Yicong. Water conservancy data classification and security protection technology[J]. People’s Yangtze River, 2023, 54(Suppl.2): 232-237.

[22] 陈韬, 马平男. 基于分类分级的银行数据资产安全管理体系设计[J]. 信息与电脑(理论版), 2023, 35(20): 130-132.
CHEN Tao, MA Pingnan. Design of bank data asset security management system based on classification and grading[J]. Information and Computer (Theoretical Edition), 2023, 35(20): 130-132.
[23] GASPARETTO A, MARCUZZO M, ZANGARI A, et al. A survey on text classification algorithms: from text to predictions[J]. Information, 2022, 13(2): 83.
[24] 王继晔, 张少博, 叶润泽, 等. 基于深度学习的交通运输行业数据自动分级方法研究[J]. 应用科技, 2024, 51(2): 145-150.
WANG Jiye, ZHANG Shaobo, YE Runze, et al. Research on automatic classification method of transportation industry data based on deep learning[J]. Applied Science and Technology, 2024, 51(2): 145-150.
[25] MIKOLOV T, SUTSKEVER I, CHEN K, et al. Distributed representations of words and phrases and their compositionality[J]. Advances in Neural Information Processing Systems, 2013, 3111-3119.
[26] 段丁阳. 数据资产安全管控技术平台的设计与实现[D]. 北京: 北京交通大学, 2017: 1.
DUAN Dingyang. Design and implementation of data assets security management and control platform[D]. Beijing Jiaotong University, 2017: 1.
[27] 林奕夫, 陈雪, 许媛媛, 等. 基于零信任安全模型的电力敏感数据访问控制方法[J]. 信息安全研究, 2024, 10(1): 88-93.
LIN Yifu, CHEN Xue, XU Yuanyuan, et al. Power sensitive data access control method based on zero trust security model[J]. Information Security Research, 2024, 10(1): 88-93.

（责任编辑　杜亚勤）

（上接第 119 页）

[25] 侯一晨, 陈志董, 张宗阳, 等. 基于热负荷均匀分配原则的直接空冷系统轴流风机转速灵活调节策略[J]. 中国电机工程学报, 2024, 44(8): 3125-3137.
HOU Yichen, CHEN Zhidong, ZHANG Zongyang, et al. Flexible speed regulation strategy of axial flow fans in direct dry cooling system based on the principle of uniform distribution of heat load[J]. Proceedings of the CSEE, 2024, 44(8): 3125-3137.
[26] YANG L J, DU X Z, YANG Y P. Space characteristics of the thermal performance for air-cooled condensers at ambient winds[J]. International Journal of Heat and Mass Transfer, 2011, 54(15/16): 3109-3119.
[27] 薛康康. 某 660 MW 超临界机组空冷系统运行优化研究[J]. 汽轮机技术, 2021, 63(4): 311-314.
XUE Kangkang. Numerical investigation of operation optimization of 660 MW supercritical air cooling system[J]. Turbine Technology, 2021, 63(4): 311-314.
[28] 安留明, 安吉振, 刘一帆, 等. 600 MW 直接空冷凝汽器变工况特性研究[J] .发电技术, 2022, 43(6): 935-941.
AN Liuming, AN Jizhen, LIU Yifan, et al. Study on variable working condition characteristics of 600 MW direct air cooling condenser[J]. Power Generation Technology, 2022, 43(6): 935-941.

（责任编辑　杜亚勤）