工业数据安全治理探索

马跃强,陈怀源,李 晨
(绿盟科技集团股份有限公司,北京 100089)

摘 要:随着工业企业数字化进程不断加快,工业数据作为新的生产要素,其重要性在生产经营过程中逐渐凸显,但如何确保工业数据在机密性、完整性、可用性的基础上释放潜在价值,是工业企业面临的一大难题。提出一套集管理、技术、运营为一体的治理思路,融合 DSMM 成熟度模型理论,围绕数据采集、传输、存储、处理、分享、销毁等全生命周期,分别从数据安全管理能力、数据安全技术能力以及数据安全运营能力等方面进行全面治理,并通过“知”“识”“控”“察”“行”5 个步骤,将工业数据安全落地,释放潜在价值,为今后工业数据安全治理提供理论参考依据。

关键词:工业数据;安全治理;分类分级;数据资产
中图分类号:TP309.2 文献标识码:A DOI:10.19358/j.issn.2096-5133.2022.04.007
引用格式:马跃强,陈怀源,李晨. 工业数据安全治理探索[J].信息技术与网络安全,2022,41(4):45-51.

Exploration of industrial data security governance

Ma Yueqiang, Chen Huaiyuan, Li Chen
(Nsfocus Technologies Group Co., Ltd., Beijing 100089)

Abstract: With the continuous acceleration of the digitization process of industrial enterprises, the importance of industrial data as a new factor of production has gradually become prominent in the process of production and operation. However, how to ensure that industrial data releases its potential value on the basis of confidentiality, integrity and availability is a major problem faced by industrial enterprises. This paper proposes a set of governance ideas integrating management, technology and operation, integrates DSMM maturity model theory, and comprehensively governs data security management capability, data security technology capability and data security operation capability around the whole life cycle of data collection, transmission, storage, processing, sharing and destruction. Through the five steps of "knowledge", "cognition", "control", "observation" and "action", the industrial data will be safely implemented and the potential value will be released, so as to provide a theoretical reference for the future industrial data security governance.

Key words: industrial data; security governance; classification and grading; data assets

0 引言

工业数据是指工业企业在开展研发设计、生产制造、经营管理、应用服务等业务时,围绕客户需求、订单、计划、研发、设计、工艺、制造、采购、供应、库存、销售、交付、售后、运维、报废或回收等工业生产经营环节和过程所产生、采集、传输、存储、使用、共享的数据[1]。随着工业企业数字化进程不断深化,工业数据作为新的生产要素,贯穿于工业全流程,其地位和重要性不言而喻[2]。然而,随着工业企业组织模式、生产模式和服务模式不断向跨设备、跨系统、跨厂区、跨地区的互联互通转变[3-4],工业数据也面临着重大的安全风险,如数据盗取、数据泄露、数据篡改、敏感数据出境等。那么如何确保工业数据这一生产要素的完整性、机密性、可用性,和在此基础之上能够进行安全有效的采集、传输、存储、使用、共享,是工业企业必须要考虑的问题。

由于工业数据产生源头分散、采集环境恶劣、流转途径多样、业务场景复杂、处理环节粗放等特点,导致工业数据在实时性、时序性、稳定性、连续性、结构化等方面存在较大差异。同时,随着工业互联网与生产制造的不断融合,使得工业数据在研发、采购、生产制造、供应、物流、运维、售后、报废

等环节之间互通互联,加大了供应链数据流向跟踪、数据出境、风险定位、责任追溯等数据管理的难度[5]。

因此,通过对工业数据安全治理探索,帮助工业企业实现数据全生命周期的安全防护,释放工业数据潜在价值,有着重要的意义。

1 工业数据安全治理概述

工业数据作为国家基础性战略资源,是驱动工业数字化转型发展的核心,是构建数字经济的基石。

工业和信息化部陆续出台多项文件,落实党中央、国务院关于加强工业大数据发展的相关精神。《工业互联网发展行动计划(2021-2023 年)》提出实施数据汇聚赋能行动,制定工业大数据标准,促进数据互联互通。2020 年 3 月发布的《工业数据分类分级指南(试行)》以及 9 月发布的《工业和信息化领域数据安全管理办法(试行)》等文件,提出了工业数据安全管理工作制度化、规范化,旨在指导工业企业提升工业数据管理能力和安全保护能力。促进工业数据的使用、流动与共享,释放数据潜在价值,赋能制造业高质量发展。

安全是发挥数据作为生产要素价值的前提条件,工业数据复杂多样性导致其安全不是一个单纯的技术问题,而是涉及组织建设、制度流程、技术工具、人员能力等各方面的系统工程,需要借助数据安全治理理念进行体系化建设[6-7]。构建工业数据安全治理体系,对工业数据在跨系统、跨地域、跨行业间的安全流动、应用有着重要的数据价值。

《数据安全治理实践探索》[6]提出了一套数据安全治理体系架构,围绕数据安全治理实践机制的管理、技术、评估和运营等几个方面逐一展开详细说明,并对数据安全治理实践所涉及的关键措施及技术要求进行了介绍,但是没有给出适用的场景。《装备制造基础数据治理体系建设研究》[7]主要从数据标准、数据架构、数据质量、数据应用以及数据安全防护等方面进行研究。《跨境数据流动安全治理》[8]主要从数据跨境流动方面提出治理的思路、方法以及手段。《工业互联网数据安全分类分级防护框架研究》[10]主要从工业互联网数据分类分级进行研究,给出工业数据分类分级的思路、防护框架以及防护技术。

2 工业数据安全治理探索

本文提出一套集管理、技术、运营为一体的工业数据安全治理参考框架,治理框架如图 1 所示。在法律法规、国家标准、行业标准的框架下,融合 DSMM 成熟度模型理论,围绕数据采集、传输、存储、处理、交换以及销毁等各个阶段的全生命周期,分别从数据安全管理能力、技术能力以及安全运营能力等方面进行全面治理。

2.1 数据安全管理能力

2.1.1 组织治理

工业数据安全治理离不开组织和人力资源的

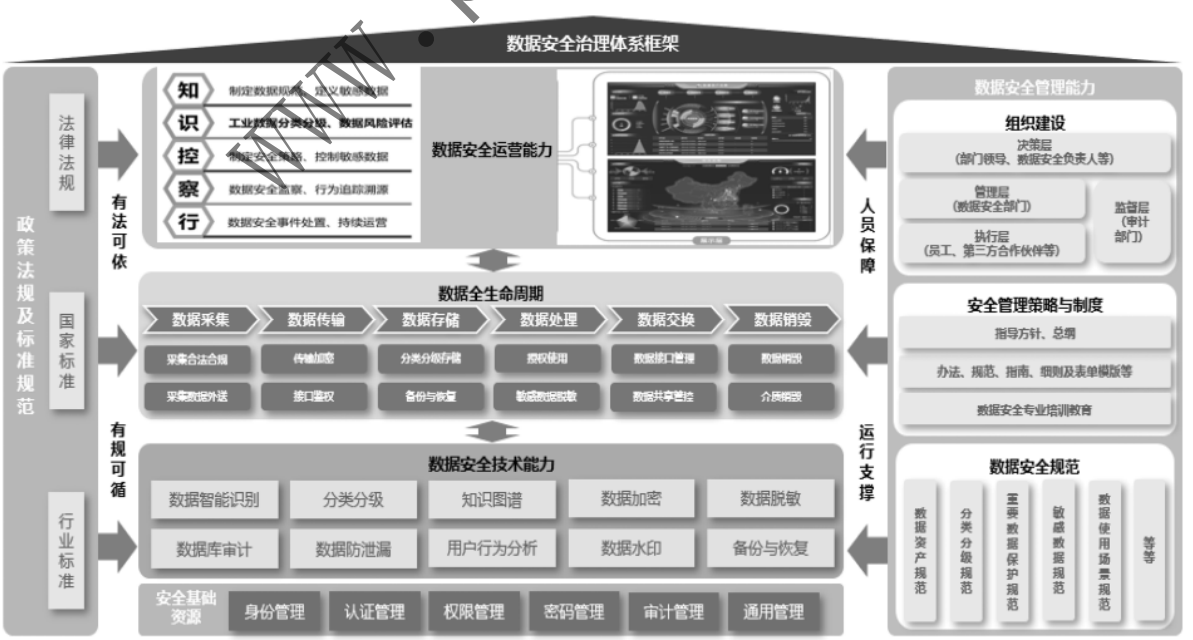

图 1 工业数据安全治理框架

投入。首先建立覆盖本企业相关部门的数据安全工作体系,明确数据安全负责人和管理机构,建立常态化沟通与协作机制。企业法定代表人或者主要负责人是数据安全第一责任人,领导团队中分管数据安全的成员是直接责任人;明确数据处理关键岗位和岗位职责,并要求关键岗位人员签署数据安全责任书。

其次在开展组织建设时,需要设计、研发、测试、生产科、仪表科、数据科、信息中心、财务、审计、人力等相关部门参加到数据安全治理工作中,确保数据安全管理方针、战略、政策等制度得以落地执行。

工业企业数据安全治理组织可采取 5 层组织结构,即决策层、管理层、执行层、监督层和参与层。组织治理结构如图 2 所示。

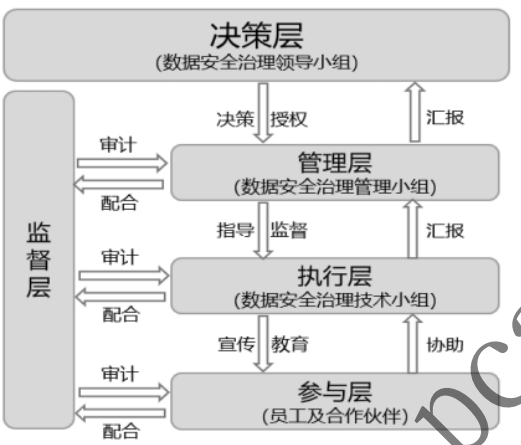

图 2 组织治理结构

决策层,主要由工业企业高层领导参与,构成数据安全治理领导小组,领导小组不少于 2 人,总体负责工业数据安全治理工作的统筹组织、指导推进和协调落实,明确数据安全管理部门,协调机构内部数据安全管理资源调配,包括制定目标、方针、意愿,发布策略、规划、制度规范,提供资源保障和重大事件协调管理。

管理层,主要由工业企业的设计、研发、测试、生产科、仪表科、数据科、信息中心、财务、人力等部门的主要负责人参与,构成数据安全治理管理小组,主要负责工业数据安全治理的相关管理工作、相关政策和制度的制定评审,保障数据安全工作所需资源,并设立数据安全管理专职岗位。包括制定规范、界定职责、开展评估、监督检测、保障运作、组织培训、受理投诉、持续管理。

执行层,主要由工业企业的设计、研发、测试、生产科、仪表科、数据科、信息中心、财务、人力等相关部门落实数据安全执行的人员组成,构成数据安全治理技术小组,主要负责具体数据安全治理相关的技术及管理措施的落实,包括政策、制度、规范的执行,数据安全产品部署及运维,安全事件监控与处置,漏洞排查与修复等日常工作。

监督层,主要由工业企业内部安全审计、督察稽核、法务等部门人员构成,定期对管理层团队、执行层团队、参与层团队在数据安全建设和管理过程中,对于策略和管理要求的执行情况进行监督审核,并向决策层汇报。包括制度落地监督、数据安全工具有效性监督、风险评估、风险监控与审计。

参与层,主要由工业企业内部全部员工及外部合作伙伴参与、配合,遵守企业内部数据安全治理相关要求。

2.1.2 制度规范治理

制度规范治理,需要建立数据全生命周期安全管理制度,针对不同级别数据,制定数据收集、存储、使用、加工、传输、提供、公开等环节的具体分级防护要求和操作规程。

数据安全制度规范体系主要从 4 个层面进行建设,包括:一级文件的数据安全方针、战略;二级文件的数据安全管理制度、办法;三级文件的操作流程、规范、作业指导书、模板等;四级文件的各类表单、记录日志、报告等。数据安全制度规范体系框架如图 3 所示。

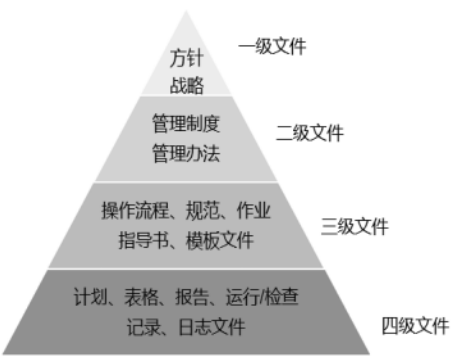

图 3 数据安全制度规范体系框架

一级文件,是企业数据安全方针、战略,属于纲领性的文件,包括数据安全治理的目标、适用范围、治理意义以及指导原则,数据安全各个方面所应遵守的原则方法和指导策略。

二级文件,是从安全方针、战略中规定的安全各个方面所应遵守的原则方法和指导策略引出的具体管理规定、管理办法和实施办法,具有可操作性和落地性。

三级文件,是根据二级文件制定的各个阶段的具体操作流程、规范指南、作业指导书、模板文件等。

四级文件,主要是落地执行三级文件产生的各类记录表单,包括运行日志、检查记录、日志文件、报告等。

2.1.3 数据安全规范治理

工业企业应将数据安全管理要求贯彻到从数据采集、传输、存储、使用、分享、销毁的各个阶段,各业务部门提出各自的数据安全需求,由数据科牵头制定数据安全规范,如《主数据规范》《数据资产识别规范》《数据分类分级规范》《重要数据识别规范》《核心数据识别规范》《敏感数据识别规范》《数据使用场景规范》等。

2.2 数据安全技术能力

数据安全技术能力治理主要是对技术措施的建设,围绕工业数据全生命周期的各个阶段采取相应的安全防护措施,包括智能识别、分类分级、数据库审计、加密传输、数据防泄漏、数据脱敏、数据水印、用户行为分析、知识图谱等。

2.2.1 数据资产识别

通过数据资产识别技术,围绕研发、设计、生产、采购、销售、交付、售后、运维、报废等工业生产经营环节和过程,对所产生、采集、传输、存储、使用、共享以及销毁的数据进行全面智能识别,包括结构化的数据(如设备运行状态)、非结构化数据(如设计图纸),形成数据资产清单和数据资产分布地图,然后进行数据分类分级,识别重要数据和核心数据。同时,对重要数据、核心数据目录进行备案,备案内容包括但不限于数据类别、级别、规模、处理目的和方式、使用范围、责任主体、对外共享、跨境传输、安全保护措施等。

2.2.2 分类分级

依据识别出的数据资产清单,按照《工业数据分类分级指南(试行)》要求,结合企业的生产制造模式、服务运营模式以及行业属性、使用场景、数据流通程度等实际情况,对工业数据进行分类[9-13]。另一方面,根据工业数据遭破坏后,对工业生产经营、公共利益、国家安全等造成的后果,采用“就高不就低”原则,即同一场景下存在多种数据级别的情况下,按照最高级别进行定级,最终形成分类分级清单,为下一步分级定措提供依据。工业数据分类分级示例如表 1 所示。

表 1 工业数据分类分级示例

数据域	行业	一级	二级	三级
研发数据域		开发测试	设计图纸	
生产数据域		控制程序	生产工况	工艺、配方
运维数据域	化工	设备维护	口令账号	
管理数据域		设备资产	模型算法	业务统计
外部数据域		物流信息	生产订单	客户信息

2.2.3 加密传输

避免重要工业数据在三网(生产网、信息网、视频网)混合中传输,必要时通过 IP SecVPN 技术进行隧道加密传输。利用密码技术(如 SM3、SM4、SM9 等),对重要数据传输时进行完整性校验,对数据传输双方身份进行身份鉴别。必要时采用工业专用加密传输协议(如 MODBUS Plus、S7comm Plus 等)或安全传输协议服务(如 TLS、DTLS、HTTPS 等),对传输的数据进行保护,避免来自利用协议脆弱性的破坏攻击。

2.2.4 数据防泄漏

根据工业数据分类分级清单,定义敏感数据,形成工业敏感数据清单和重要数据、核心数据保护清单。在网络、终端主机、邮件服务器、存储服务器等出口边界部署对应的数据防泄漏产品,对含有工业敏感数据的外发进行监控与防护。

2.2.5 数据脱敏

通过数据脱敏技术,对工业企业滥用敏感数据进行治理,防止敏感数据在未经脱敏的情况下从企业流出。既要满足企业保护敏感数据,同时又满足行业监管的合规性。

静态脱敏通过算法将原始数据库中的敏感数据处理成非敏感数据存储至其他位置,供数据访问者直接访问和使用,主要应用在非生产环境,如:系统开发、测试、数据分析等。动态脱敏是在不改变原始数据的情况下,访问者访问敏感数据时,实时对每次访问的数据进行脱敏,防止敏感数据泄露,主要应用在生产环境,比如大屏展示、运维人员工具直连数据库等。同时,也可对脱敏后的数据添加水

印,当数据泄露后,根据水印信息来追溯数据泄露的源头。

2.2.6 数据库审计

通过工业数据库审计技术,对诸如 Siemens 的 SIMATIC-IT-Historian、Honeywell 公司的 PHD、Rockwell 的 RSSQL、北京和利时 HiRIS、浙江中控 ESP-iSYS、北京亚控 KingRDB、三维力控 pSpace 等工业实时数据库以及 Oracle、MySQL、SQLServer、DB2 等关系数据库进行审计。识别出关键操作行为、违规行为,对用户访问数据库行为进行记录、分析和汇报、事故追根溯源。

2.2.7 用户行为分析

通过对于全流量进行采集和分析,利用机器自学习技术对用户日常操作行为进行建模,建立起用户行为基线与数据资产映射,形成用户行为数据资产画像。

2.2.8 知识图谱

利用知识图谱技术,将零散分布的多源异构的工业数据组织起来,对数据资产和物理资产的耦合关系进行深度解析,实现“决策制定、风险预判、事故分析、攻击识别”等能力的智能化辅助和自动化处理,为数据安全的威胁建模、风险分析、攻击推理等提供支持。

2.3 数据安全运营能力

2.3.1 资产安全运营

基于数据资产识别工具,对工业数据进行全面测绘,形成数据资产清单和资产分布地图,通过内置行业分类分级策略模板,将识别出的工业数据进行分类分级,并基于行业属性、业务属性、使用场景对重要数据和敏感数据进行识别,建立起重要数据和敏感数据清单,按照敏感级别进行差异化的安全防护,并通过数据安全运营平台进行持续监控运营。

2.3.2 常态化运营

数据资产的安全,需要持续运营才可以保证。利用数据安全运营平台,从数据合规监管、数据资产、业务场景、数据风险等多个维度进行监测、评估分析、健康指标打分。对运营人员进行实训演练,提升人员技能水平,助力常态化运营持续有效执行。

2.3.3 安全风险运营

安全风险运营的主要内容:基于数据资产、安全漏洞、脆弱性、威胁情报等进行大数据关联分析、态势感知;对特定的人群(如业务人员、第三方运维人员等),涉敏接口建立敏感数据流动基线,监测数据访问异常行为。特别要加强成套进口设备、国外远程运维、设备预测诊断等环节的数据出境风险的监控。直接从工业现场设备、主机、网络、系统等采集的数据被称为“一次数据”;对“一次数据”进行处理、统计、分析、应用所产生的数据被称为“二次数据”。二次数据更能够清晰地表达出工业企业数据的核心内容,往往比一次数据更有价值。因此,特别要加强二次数据的保护力度,对发现数据盗取、破坏、篡改等行为及时告警,并进行通报预警;对发现的安全事件进行应急响应、处置、溯源分析,形成数据安全的闭环。

3 工业数据安全治理实践路线

工业数据安全治理需要通过“知”“识”“控”“察”“行”5 个步骤的治理路线来具体落地。数据安全治理路线如图 4 所示。

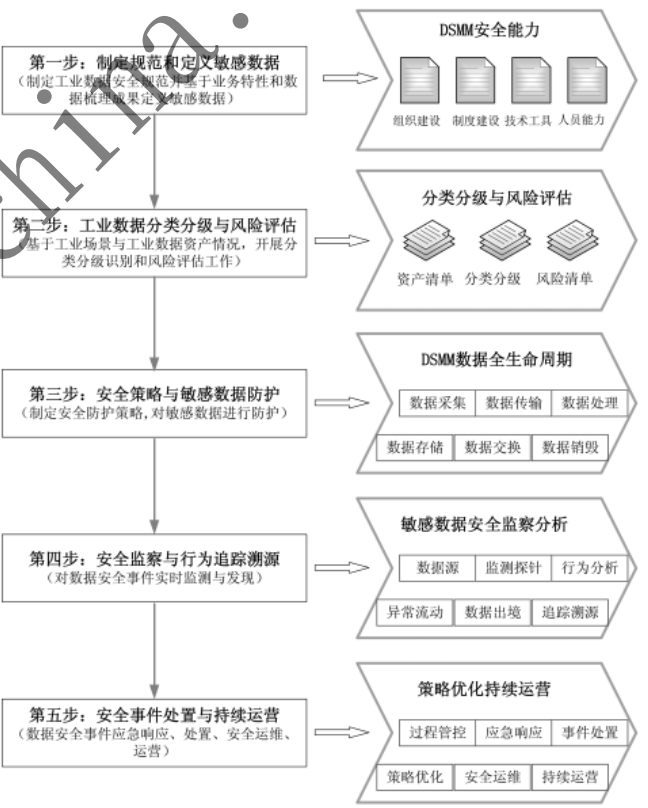

图 4 数据安全治理路线

“知”是指制定规范与定义敏感数据,结合 DSMM 数据能力成熟度模型,从组织建设、制度流程、技术工具和人员能力四个领域开展数据安全的工作,通过对生产业务和组织架构的梳理,制定有针对性的数据资产管理要求、管理办法以及工业数据分类分

级规范。

“识”是指将规范中的要求转化为策略录入到技术工具,实现自动化的数据识别与分类分级。基于数据资产和其关联的应用场景(如成套进口设备数据出境风险)进行分析,发现风险与安全需求,来达到数据风险评估的效果,风险评估中还要包含合规性评估,通过数据风险评估可以全面了解数据资产安全状况。

“控”是指通过风险评估的结果,结合数据生命周期的每一个阶段,制定不同的安全防控策略,控制手段包括对数据库的数据库审计与防护,对应用的数据防泄漏、数据脱敏、数据扫描、数据水印、加密、用户行为分析、备份恢复等技术手段,最终汇聚到数据安全运营平台中进行统一的监管。

“察”是指有了全面的数据资产情况,又有了海量的数据行为日志,数据安全运营平台就可以完成对数据的全面分析,从数据源到数据行为,通过平台底层的大数据分析引擎、UEBA 引擎以及分析检测引擎等机器学习的能力,实现敏感数据的追踪溯源的效果。

“行”是指数据安全运营平台,对数据安全事件进行实时的预警,并实现场景化的展示,让运维人员可以了解到每一个数据安全事件的起因是由于内部操作还是因为外部攻击导致的,通过数据安全运营平台,可由现场的专业人员和云端的专家共同完成安全事件的快速处置以及策略优化,实现持续自适应的数据安全防护能力。

以某化工集团为例,其工业数据安全治理实践路线如图 5 所示。通过“知”“识”“控”“察”“行”5 个步骤的治理路线,将该化工集团的工业数据安全治理成功落地。形成一整套化工行业的工业数据规范标准,识别出化工行业的工业数据资产、数据分布地图,形成分类分级清单、敏感数据清单、重要数据保护目录清单,并进行分级定措防护,建立数据安全运营平台,开展人才培养、实战化运营。

经过近 6 个月的实践效果来看,目前取得了一定成效,发现并阻止应用服务器被攻击 26 次,发现并阻止敏感数据外泄 3 起,内部人员违规操作、误操作 36 次,培养安全人才 9 人,安全事件处置 1 起。

4 结论

本文从安全管理、安全技术以及安全运营三个维度开展工业数据安全治理的探索。通过“知”“识”“控”“察”“行”5 个步骤的治理路线,将某化工集团企业工业数据进行应用实践,产生一定的治理效果。本文对今后工业企业在数字化转型发展过程中实现工业数据跨地域、跨平台、跨行业的安全传输、流动、交换、使用、释放潜在价值,具有现实意义和应用价值。

参考文献

[1] 国家工业信息安全发展研究中心,工业信息安全产业发展联盟.工业互联网数据安全白皮书(2020)[Z].2020-12-07.

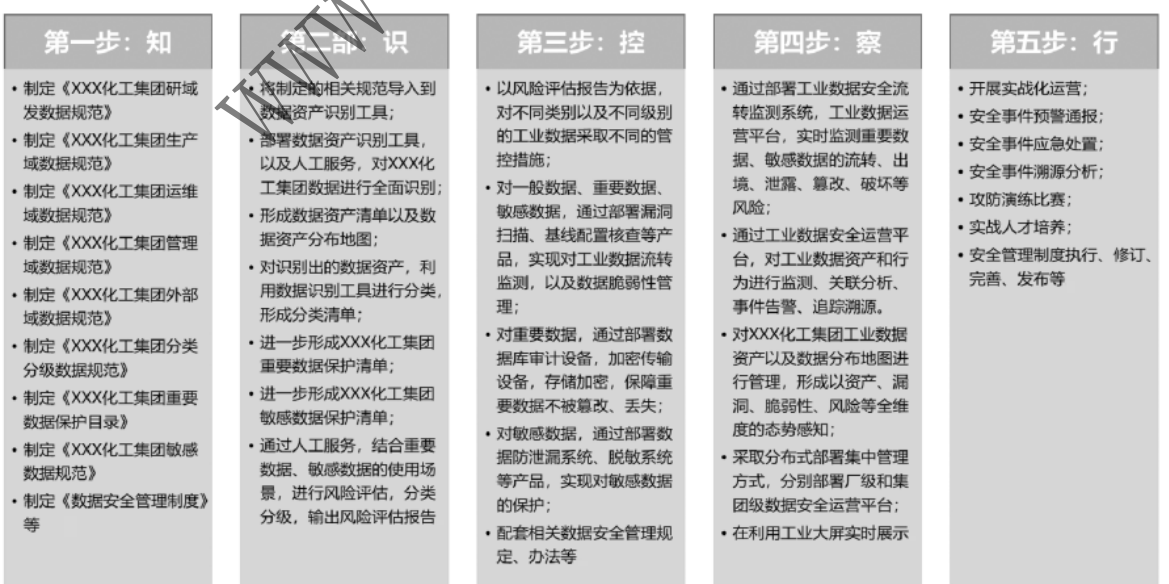

图 5 某化工集团工业数据安全治理实践

[2] 怀进鹏.大数据是国家战略资源[J].中国经济和信息化,2013(8):49-50.
[3] 白龙.工业互联网工业和信息化领域的大革命[J].现代工业经济和信息化,2013(17):72-73.
[4] 国富,石英村,人工智能数据安全治理与技术发展概述[J].信息安全研究,2021,7(2):110-119.
[5] 于成丽.工业互联网安全形势及监管政策浅析[J].保密科学技术,2020(5):16-19.
[6] 胡国华.数据安全治理实践探索[J].信息安全研究,2021,7(10):915-921.
[7] 张莹莹,曹禹.装备制造基础数据治理体系建设研究[J].国防科技,2021(4):28-33.
[8] 董京波.跨境数据流动安全治理[J].科技导报,2021,39(21):9-17.
[9] 朱光亮.探究工业互联网中的数据安全问题及解决方法[J].网络安全技术与应用,2022(1):60-61.
[10] 张雪莹,杨帅锋,王冲华,等.工业互联网数据安全分类分级防护框架研究[J].信息技术与网络安全,2021,40(1):2-9.
[11] 管晓宏.全面提升工业数据管理能力释放数据潜在价值[J].网络安全和信息化,2020(4):6-7.
[12] 陈雪鸿,杨帅锋,柳彩云.工业互联网数据安全分类分级思考[J].网络安全和信息化,2019(8):112-114.
[13] 王大宇,王金星,李云生,等.工程机械行业工业数据分类分级应用分析及研究[J].建筑机械,2020(9):8-11.

(收稿日期:2022-02-22)

作者简介:

马跃强(1984-),通信作者,男,硕士,高级工程师,主要研究方向:工业互联网安全、工控安全、数据安全。E-mail:mayueqiang@nsfocus.com。

陈怀源(1981-),男,本科,高级工程师,主要研究方向:数据安全。

李晨(1983-),男,绿盟科技集团副总裁,中国网络安全产业联盟常务理事,CCF计算机安全专业委员会委员,主要研究方向:网络安全、云计算安全、数据安全等。

(上接第44页)

据监测系统[J].核电子学与探测技术,2006(1):91-94.
[11] 何明,肖利君.智能公交信息服务系统设计[J].山西科技,2008(2):36-37,42.
[12] 王震,杨东超,伊强.基于单片机的车载超级电容测试系统设计与实现[J].电子技术应用,2006,32(9):51-54.
[13] 王常顺,肖海荣,潘为刚.CAN总线的船舶机舱监测报警系统设计[J].自动化与仪表,2010,25(10):24-27,41.
[14] 于建坤.云环境下搜索引擎系统关键技术研究[D].南京:南京邮电大学,2017.
[15] 王建民.工业大数据技术综述[J].大数据,2017,3(6):3-14.
[16] 李建华,肖惠才,高帆.浅谈冶金企业关键设备运行状态在线监测诊断系统构建与实施[J].中国设备工程,2020(1):166-168.

(收稿日期:2022-02-26)

作者简介:

谢利(1974-),男,本科,正高级工程师,主要研究方向:企业信息化建设。

洪晟(1981-),男,博士,副教授,博士生导师,主要研究方向:工业互联网安全、信息网络安全、复杂系统安全性。

谢经广(1980-),男,工程硕士,正高级工程师,主要研究方向:机车产品设计。

版权声明

经作者授权，本论文版权和信息网络传播权归属于《信息技术与网络安全》杂志，凡未经本刊书面同意任何机构、组织和个人不得擅自复印、汇编、翻译和进行信息网络传播。未经本刊书面同意，禁止一切互联网论文资源平台非法上传、收录本论文。

截至目前，本论文已经授权被中国期刊全文数据库（CNKI）、万方数据知识服务平台、中文科技期刊数据库（维普网）、JST 日本科技技术振兴机构数据库等数据库全文收录。

对于违反上述禁止行为并违法使用本论文的机构、组织和个人，本刊将采取一切必要法律行动来维护正当权益。

特此声明！

《信息技术与网络安全》编辑部

中国电子信息产业集团有限公司第六研究所