企业数据分类分级自动化路径研究

卢启刚[1]，杨克松[2]，王　建[2]，王思博[2]，吴映波[1]
（1. 重庆大学　大数据与软件学院，重庆　401331；2. 中电数创（北京）科技有限公司，北京　100190）

摘　要：数据分类分级自动化是提升企业数据分类分级效率、促进数据安全管理的重要手段。目前，针对数据分类分级自动化路径的研究还相对较少。结合数据分类分级工作流程，总结企业数据分类分级面临的主要问题挑战，对数据探测、数据预处理、敏感数据识别、分类分级打标等典型自动化技术进行分析，提出了企业数据分类分级自动化的框架和路径，为企业更加高效有序地开展数据分类分级自动化工作提供有效借鉴。

关键词：数据分类分级；数据安全；数据要素
中图分类号：TP29；TP309　　**文献标识码：**A　　**DOI：**10.19358/j.issn.2097-1788.2024.06.007
引用格式：卢启刚，杨克松，王建，等. 企业数据分类分级自动化路径研究［J］. 网络安全与数据治理，2024，43（6）：47-52.

Research on automated paths for enterprise data classification and grading

Lu Qigang[1], Yang Kesong[2], Wang Jian[2], Wang Sibo[2], Wu Yingbo[1]
（1. School of Big Data and Software, Chongqing University, Chongqing 401331, China;
2. China Electronics Digital Innovation, Beijing 100190, China）

Abstract: Automation of data classification and grading is an important means to improve the efficiency of enterprise data classification and grading and promote data security management. At present, there is relatively little research on automated paths for data classification and grading. This article combines the data classification and grading workflow to summarize the main problems and challenges faced by enterprise data classification and grading, analyzes typical automation technologies such as data detection, data preprocessing, sensitive data identification, classification and grading marking, and proposes an automation method for enterprise data classification and grading. The framework and path provide effective reference for enterprises to carry out data classification and grading automation work more efficiently and orderly.

Key words: data classification and grading; data security; data elements

0　引言

我国陆续出台《网络安全法》《数据安全法》《个人信息保护法》等法律法规，提出建设数据分类分级制度，对于数据分类分级的重视程度不断提升。2024 年 3 月 15 日，全国网络安全标准化技术委员会发布《数据安全技术 数据分类分级规则》，给出了数据分类分级的通用规则，用于指导各行业领域、各地区、各部门和数据处理者开展数据分类分级工作。上海、浙江、福建、重庆、贵州等多个地区都出台了政务数据分类分级相关标准指南，金融、工业、医疗、电信、汽车等行业也陆续出台分类分级指南或规范。与此同时，随着数据泄露和隐私保护等问题日益突显，以数据分类分级促进数据安全合规成为企业实现高质量发展的重要工作。

目前，各行业推进数据分类分级的进度和路径不一，多数行业因未发布数据分类分级的标准规范而未开展数据分类分级工作，金融、工业、医疗、电信等领域因分类分级标准规范化工作推进较快，开始探索通过自动化手段支撑数据分类分级工作。总体而言，各行业数据分类分级的自动化路径尚不清晰，自动化水平较低，在数据分类分级过程中仍需要人工进行调整和配置，无法实现全流程的自动化。本文旨在针对数据分类分级自动化开展研究，对数据分类分级面临的问题挑战进行分析，探索提出企业数据分类分级自动化的框架和路径，为企业提升数据分类分级效率提供支撑，促进企业高质量安全合规发展。

1　研究现状

目前，专家学者围绕数据分类分级开展了较为广泛

的研究，主要集中在数据分类分级综合性研究、数据分类分级策略研究、数据分类分级技术研究以及基于数据分类分级的数据安全管理研究等。

（1）数据分类分级综合性研究

李玉亮分析了当前数据分类分级工作的实践，提出对未来数据分类分级工作的建议[1]。张敏等对美国、英国政府数据分类分级管理现状开展研究，同时，对国内政府数据、公共数据、行业数据等分类分级工作进行梳理分析，提出未来完善数据分类分级的路径[2]。严炜炜等对我国数据分类分级学术研究动态进行定量揭示，提炼相关公开政策标准拟定趋势，结合企业实践规律，综合探究我国数据分类分级工作进展[3]。王敏和曹放通过对以 GDPR 为代表的“欧盟标准”、以 CCPA 为代表的“美国标准”的研究分析，为构建“中国标准”提出创新策略，即通过增强制度的适应性、复杂性、主动性、凝聚力提升数据保护能力[4]。Force 等提出了联邦信息系统和组织信息安全和隐私的清单[5]。

（2）公共数据分类分级研究

陈祥玲充分研究政府数据分类分级的理论逻辑、现实困境，提出构建政府数据分类分级的“价值指引—法律体系—配套制度”的理论逻辑框架[6]。周毅和徐梦在具体调查分析公共数据分类分级实践及已有地方性标准基础上，提出公共数据分类分级标准构建的基本原则，构建起我国公共数据分类分级标准模型以及标准核心要素的框架[7]。王跃和苏娜对我国政务数据分类分级实施情况开展系统梳理与量化分析，研究提出我国政务数据分类分级应对策略方案[8]。张晓艺等结合水利、铁路、公安、交通管理、公共资源交易、刑事司法等领域公共数据特点，开展数据分类分级研究[9]。Ross 等认为受控非密信息保护直接影响联邦政府执行基本职能的能力，并提出对受控非密信息分类的建议[10]。

（3）企业数据分类分级研究

董智华分析我国数据分类分级体系现状和存在的问题，提出企业数据分类分级方法[11]。陶镇威聚焦企业敏感涉密数据，总结敏感涉密数据的管理原则，提出开展企业敏感涉密数据分级分类策略[12]。李萌等聚焦重要信息系统数据，通过研究我国数据安全管理法规政策，分析数据遭受破坏后的影响程度、影响对象等因素，提出重要信息系统数据分类分级的治理路径和建议[13]。部分学者针对汽车、电力、航空、银行、港口、烟草、石油化工、工程机械、遥感卫星等行业领域，提出行业数据分类策略、建议等。

（4）数据分类分级技术研究

杜宇骁等对哈佛大学 Datatags 数据分级系统进行研究，分析系统架构原理、数据分级思路、分级模型和应用案例，为科学数据安全共享研究和实践提供新思路[14]。胡挺峰针对传统大数据分类系统对海量数据分类处理结果精确度较低的问题，提出了基于 ML－kNN 算法的大数据分类系统设计[15]。万小博和吴海燕分析了数据分类分级系统应用现状、面临的挑战，从加大需求调研、统一标准、加强技术研发等方面提出数据分类分级系统发展建议及趋势[16]。Mohammadian 等根据组织的数据安全和隐私需求以及政府对数据施加的政策，探讨了模糊逻辑在数据分类中的应用[17]。Wen 等通过对关键数据或重要数据的关联分析，提出了基于数据分类分级的智能数据目录构建[18]。

（5）数据分类分级安全管理研究

闻云霞通过对各行业数据安全防护体系进行分析，总结提出基于数据分类分级的数据安全保护实践路径[19]。周成祖等提出数据安全的两个要素，设计基于数据分类分级和数据安全级别的数据安全防控模型[20]。刘红等建立多维度数据分级分类表达和计算的系统框架，在同一框架下进行多种数据安全分析和管理[21]。张雪莹等从通用安全防护、分类安全防护、分级安全防护三个层面构建工业互联网数据安全防护框架，解决不同层次的工业互联网数据安全问题[22]。袁康等以数据分类分级为基础，对不同重要性和风险等级的数据采取差异化和针对性的管控措施[23]。Singh 通过分析大数据治理中的数据安全问题，提出了补充数据隐私和安全因素的大数据治理框架[24]。

总体而言，伴随着国家层面以及各行业领域数据分类分级政策法规的不断完善，专家学者的研究重点从数据分类分级的框架体系、现状问题、对策建议等综合性问题，进一步细分细化，表现在两方面：一是深化研究细分行业领域的数据分类分级规则，旨在提出各行业领域可参考落地的数据分类分级规则规范；二是加强人工智能、大数据等新技术在数据分类分级领域的应用研究，旨在提出数据分类分级的技术解决方案，帮助各类市场主体提升数据分类分级的能力和效率。其中，针对数据分类分级技术的研究，多数聚焦于新技术在数据分类分级某些重点环节的应用场景，或者基于新技术的数据分类分级智能化系统平台的建设方案。本文重点围绕数据分类分级技术开展研究，尝试以系统工程的视角，围绕数据分类分级的全流程环节，结合人工智能等新技术特点，梳理分析目前可应用于数据分类分级的典型技术，并结合新技术的应用成熟度提出数据分类分级自动化的框架和路径，为各类主体实现数据分类分级工作的自动化提供方案参考。

2 数据分类分级的流程和挑战

2.1 数据分类分级的流程

数据分类分级的工作流程可分为准备、实施及持续运营三个阶段，如图 1 所示。

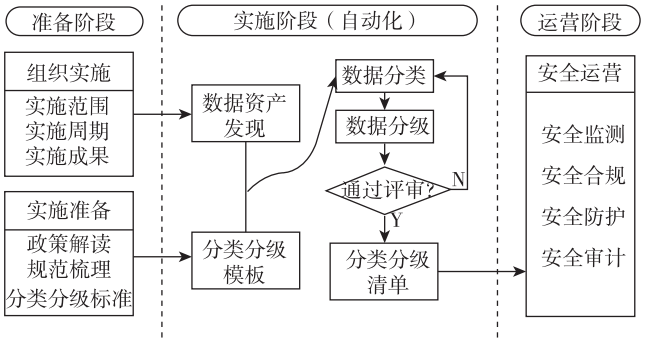

图 1 数据分类分级工作流程图

准备阶段。企业在本阶段需明确实施范围、实施周期等内容，并形成基础方案，为后续的实施工作形成支撑。基础方案包含政策梳理、分类分级标准梳理，形成企业自身的分类分级依据。

实施阶段。首先，采用数据资产探测技术完成数据资产识别；其次，基于前期调研生成模板完成分类分级打标工作，形成数据分类分级清单。

持续运营阶段。企业在本阶段可以将数据分类分级成果用于支撑数据安全监测、安全合规、安全防护、安全审计等数据安全运营工作。同时，可以通过数据接口的方式与其他数据安全产品联动。

2.2 数据分类分级面临的挑战

数据分类分级的工作流程长、涉及范围广，具有较强的专业性和复杂性。数据分类分级整个过程中存在“两难一不高”的问题挑战，亟需充分利用智能化技术促进数据分类分级工作的自动化。

数据资产识别发现难。数据资产扫描是数据分类分级的重要环节，通过数据资产扫描能够实现对企业数据资源的有效盘点，为数据分类分级工作提供高质量数据输入。但企业内部数据量大且种类繁多，数据存储在不同的数据库中，同时跨不同数据库存储的数据存在恶意数据、私有数据、无法追溯数据、不完整数据等数据质量问题，增加了数据资产识别发现的难度，还会降低数据分类分级生成结果的准确度，对数据分类分级模型造成影响。

分类分级模板生成难。分类分级模板是对数据进行打标并进行分类分级的基础，其生成主要依托规则和先验知识。从规则层面看，国家和行业的分类分级标准颗粒度较粗，无法达到表级或字段级的规则生成；其次跨行业的数据分类分级标准差距大，导致数据规则无法复用。从先验知识层面看，不同的行业业务属性差距较大，项目间的可移植性较低，无法通过先验知识实现模板的生成，因此不同行业需要开发不同的模板形成规则库，而且需采用大量人工参与的方式去调整数据分类分级结果的准确度。

分类分级准确率不高。数据分类分级准确率问题依赖于诸多因素。从用户侧来讲，用户对数据资产的把控管理程度、用户所在行业的标准细化程度能够影响数据分类分级的准确率；从厂商侧看，厂商数据安全服务人员的能力、已有项目积累等，均对数据分类分级准确率有影响。因此，需要借助自动化的工具实现对分类分级能力的固化，减少人工的能力对数据分类分级准确率的影响。

3 数据分类分级自动化技术分析

3.1 数据探测技术

数据探测技术是一种结合主动探测与被动探测的综合技术，旨在发现、处理和分析数据资产，提高识别数据资产的效率。在数据资产扫描过程中，该技术不仅能识别结构化数据，还能有效识别非结构化数据。因此，数据探测技术是支撑数据资产盘点的重要手段。

主动探测技术在数据探测过程中占据重要地位，它通过主动向目标发送探测数据包来实现扫描。该技术不仅能够有效探测大多数结构化数据，涵盖 TCP/IP、HTTP、JDBC 等数据包协议，而且能够适配市面上主流的数据库类型，如 MySQL、Oracle、SQL Server、DB2、DM 等。主动探测技术通过对反馈数据进行分析，能够准确判断数据资产的状态，具有高精度和短周期的优点，在数据资产发现过程中发挥着关键作用。

被动探测技术在数据探测过程中虽然占比较小，但在主动探测技术无法适用的场景下，它发挥着关键作用。被动探测技术通过识别流量中的数据库专有协议，能够准确判断数据资产的状态。尽管受限于当前技术水平，被动探测技术目前只能作为辅助类型的探测技术，但它在数据资产发现过程中仍然发挥着不可或缺的作用。

3.2 数据预处理技术

数据预处理技术涵盖了数据清洗、数据转换、特征选择以及关键字提取等一系列方法，是提升数据分析和挖掘效果的关键，其在数据资产发现的过程中发挥着不可替代的作用。首先，通过数据清洗，能够提升数据的质量，减少异常值，增强数据的可靠性。其次，数据转换可以简化数据，统一数据格式，降低数据类型的复杂

性，从而提高数据分析的效率。此外，数据预处理还能辅助人工管理各类数据，提升数据管理效率。然而，目前数据预处理技术仍在发展阶段，面临着一些挑战。对于复杂的数据场景和大型数据集，处理数据的准确率可能会受到影响。

3.3 敏感数据识别技术

敏感数据识别技术通过数据敏感性标识、数据内容分析以及人工识别等多种手段，实现对个人身份信息、个人健康信息以及专有数据等敏感数据的精细管理。现有的敏感数据识别方法主要分为两大类：第一类是人工判断法，它依赖于数据管理员的经验和主观判断，因此识别结果可能带有个人主观性。第二类是基于人工智能的识别技术，包括相似度学习、非监督学习和监督学习三种方法。相似度学习主要运用算法检测各类以文档形式存储的非结构化数据，如 PPT、Word、PDF 等文档；非监督学习则通过算法进行特征提取，如图像关键特征提取和文档数据语义特征提取；而监督学习则通过选择适合的算法，如支持向量机（SVM）、决策树、神经网络等，对数据模型进行训练和打标，进而应用于敏感数据的识别和预测。

3.4 分类分级打标技术

分类分级打标是实现数据自动化管理的重要环节，其核心在于按照“先分类，再分级”的原则，为数据资产打上恰当的标签。这一过程涉及将数据划分为不同的类别和安全等级，并依据这些类别和等级赋予相应的标签。分类分级打标技术依赖于数据资产发现、数据预处理和敏感数据识别等多种技术，并依据数据分类分级模板中的规则实现自动打标。

4 数据分类分级自动化路径

结合数据分类分级自动化技术的发展趋势，数据分类分级自动化主要集中在数据分类分级的实施阶段，可重点推进数据资产发现、分类分级模板生成、敏感数据识别、分类分级打标等环节实现自动化。图 2 所示为数据分类分级实施阶段的自动化路径。

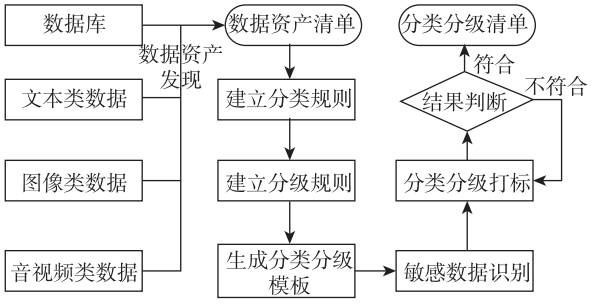

图 2 数据分类分级实施阶段的自动化路径

4.1 数据资产发现自动化

数据资产发现可通过运用数据探测技术促进数据库接入和数据预处理等重点环节的自动化，提升数据资产发现的效率，形成数据资产清单，帮助企业掌握数据资产分布情况。

数据库接入方面。通过接入数据库可以精确地形成表级或字段级的数据资产清单。主动探测技术通过主动向目标数据库发送探测数据包实现对目标数据库的数据资产进行全面扫描。在执行主动探测之前，需人工规划并确认用户所使用的数据库等信息，以确保扫描过程具有明确的目标和针对性。这种主动探测方式能够精准地识别设定范围内所有网络可达的数据资产，为数据分类分级提供有效的基础。

数据预处理方面。数据预处理技术是实现不同类型数据规范化的关键步骤。由于企业涉及的数据类型较多，包括结构化、异构化数据，而数据分类分级主要聚焦于结构化数据，因此利用自然语言处理（NLP）技术，对文本类数据进行全文提取、关键字提取、自动摘要和自动分类等操作，从而实现文本数据的分类分级。对于图片数据，OCR 识别技术通过图像处理和字符识别提取图片中的文本信息，并结合自然语言处理技术进行分类分级。对于音视频数据，特征识别技术则通过提取和分析音视频特征，结合自然语言处理技术完成分类分级。这些技术的结合应用，能够显著提升数据分类分级的准确性和效果。

4.2 分类分级模板生成自动化

分类分级模板是实现分类分级自动化的关键步骤。随着企业对数据分类分级的日益重视，多数行业已形成基础模板库。本文将从数据内容分析、模板选择、机器学习、模板调优等方面探讨如何实现这一目标。

首先，针对企业数据资产清单进行深入的内容分析。这一步骤旨在全面理解企业数据的特点和业务需求，为选择合适的基础模板提供决策依据。通过结合企业数据类型、数据量及业务需求等多维度信息，从模板库选出最符合实际的模板。其次，利用机器学习算法、自然语言处理技术、语料库资源以及血缘关系分析等手段，对所选模板进行优化。这些技术能够有效提升模板的覆盖率和准确率，最终形成一套完善的数据分类分级模板。

4.3 敏感数据识别自动化

敏感数据识别在数据分类分级自动化中扮演着重要的角色，它是确保企业数据安全与合规的关键环节。企业的敏感数据主要聚焦于个人隐私和商业秘密领域，在敏感数据识别自动化的过程中，企业不仅要处理结构化数据，还要应对非结构化数据的挑战。

针对结构化数据，首先通过数据资产发现工具，基于IP地址段或网络流量进行数据资产的全面扫描。随后，依托关键字、正则表达式、机器学习等算法，通过对结构化数据扫描提取数据特征，对比关键字实现特征的匹配，包括字段名称、列注释、样本类型等关键特征信息，从而精确识别出企业的敏感数据类型及其分布情况。

针对非结构化数据，由于其多样性和复杂性，需要借助人工智能技术。通过非监督学习和监督学习算法，识别出文本数据，并依据文本特征、上下文语境等信息，精准判断数据的标签和属性，完成敏感数据识别。

4.4 分类分级打标自动化

分类分级自动打标其核心在于运用分类分级模板进行高效的数据打标处理。在实际操作中，数据的分类工作先于分级工作展开，数据分类打标过程遵循点分类法和面分类法相结合的方式进行。首先，数据分类打标遵循数据分类分级模板中的规则，针对数据进行数据类型的判定，判定完成后会根据既定规则进行标签标注，如个人数据、企业数据、公共数据等。此外，基于数据的业务特征，还会进一步细化为财务数据、生产数据等具体标签。其次，在分类的基础上以匹配的方式完成数据定级。由于不同数据在不同场景中的数据级别不同，因此需结合词向量的方式，基于上下文的其他数据标签，判断该数据的级别并完成打标工作。最后，数据分级要考虑数据量的大小，通过设定阈值的方式实现数据级别的动态调整。

5 结论

当前，针对数据分类分级自动化的理论研究相对较少，但随着数据分类分级工作的开展，推动数据分类分级自动化将是提升企业数据分类分级效率的关键举措。从企业数据分类分级的准备阶段、实施阶段及持续运营阶段来看，当前可重点聚焦实施阶段推进数据资产发现、分类分级模板生成、敏感数据识别、分类分级打标等关键环节的自动化建设，为实现数据分类分级全流程自动化积累经验。然而，局限于当前技术的发展水平，数据分类分级自动化在未来仍有较大的创新探索空间。其中，在数据资产发现方面，自动化识别仍为辅助手段，应加强对图片、视频、音频的数据发现能力研发；在自动化模板生成方面，随着生成式AI技术的发展和先验知识的应用，未来应加强跨行业分类分级模板的研究；在敏感数据识别方面，通过对算法的优化和机器学习的应用，推进敏感数据识别范围和识别精度；在分类分级打标方面，可通过开展分类分级结果评估，针对不同业务场景的业务特征，实现分类分级打标动态调整。通过这些措施，数据分类分级自动化水平将进一步提升，在提高数据管理效率、保障数据安全以及促进数据合规性方面发挥更大的作用。

参考文献

[1] 李玉亮. 数据分类分级的现状与发展 [J]. 中国信息安全，2021 (5)：55－56.

[2] 张敏，魏伟，谭天怡，等. 数据分类分级及其发展路径研究 [J]. 网络安全与数据治理，2022，41 (7)：18－22.

[3] 严炜炜，谢顺欣，潘静，等. 数据分类分级：研究趋势、政策标准与实践进展 [J]. 数字图书馆论坛，2022 (9)：2－12.

[4] 王敏，曹放. GDPR时代数据保护的欧美标准与中国策略 [J]. 新闻大学，2022 (7)：53－64，118－119.

[5] FORCE J T，INITIATIVE T. Security and privacy controls for federal information systems and organizations [J]. NIST Special Publication，2013，DOI：10.6028/NIST.SP.800－53R4.

[6] 陈祥玲. 政府数据分类分级保护的理论逻辑、现实困境与实践路径 [J]. 征信，2023，41 (4)：36－44.

[7] 周毅，徐梦. 公共数据分类分级标准建设探析 [J]. 情报探索，2023 (3)：24－31.

[8] 王跃，苏娜. 我国政务数据分类分级实施关键问题与实践研究 [J]. 大数据，2014，10 (3)：16－26.

[9] 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 (S2)：232－237.

[10] ROSS R，PILLITTERI V，DEMPSEY K，et al. Protecting controlled unclassified information in nonfederal systems and organizations [R]. Gaithersburg，MD：National Institute of Standards and Technology，2019.

[11] 董智华. 企业数据分类分级的研究与思考 [J]. 软件和集成电路，2023 (12)：74－80.

[12] 陶镇威. 企业敏感涉密数据分级分类管理策略探讨 [J]. 现代工业经济和信息化，2019，9 (10)：79－80.

[13] 李萌，李健，徐平洋，等. 重要信息系统数据分类分级的研究与思考 [J]. 信息安全研究，2023，9 (7)：631－636.

[14] 杜宇骁，龚城，伏安娜，等. 哈佛大学Datatags数据分级系统研究及启示 [J]. 图书馆杂志，2019，38 (8)：17－26.

[15] 胡挺峰. 基于ML－kNN算法的大数据分类系统设计 [J]. 信息与电脑 (理论版)，2022，34 (1)：71－73.

[16] 万小博，吴海燕. 基于市场需求的数据分类分级系统应用现状及发展趋势分析 [J]. 数字技术与应用，2023，41 (8)：105－107.

[17] MOHAMMADIAN M，HATZINAKOS D. Data classification process for security and privacy based on a fuzzy logic classifier [J]. International Journal of Electronic Finance，2009，3 (4)：374－386.

[18] Wen Xing, Wang Zheng, Chen Zhenyu, et al. Intelligent data directory construction based on data classification and grading [C]// International Conference on Distributed Computing and Electrical Circuits and Electronics. IEEE, 2023: 1 - 8.

[19] 闻云霞. 基于数据分类分级的数据安全保护实践探索 [J]. 数字经济, 2024 (3): 54 - 57.

[20] 周成祖, 吴文, 蔡晓强. 基于分类分级的数据安全防控策略研究 [J]. 数据与计算发展前沿, 2023, 5 (1): 128 - 135.

[21] 刘红, 张越今, 赵文霞, 等. 多维度数据分级分类安全管理框架 [J]. 信息网络安全, 2021, 21 (10): 48 - 53.

[22] 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.

[23] 袁康, 鄢浩宇. 数据分类分级保护的逻辑厘定与制度构建——以重要数据识别和管控为中心 [J]. 中国科技论坛, 2022 (7): 167 - 177.

[24] SINGH D. Towards data privacy and security framework in big data governance [J]. International Journal of Software Engineering and Computer Systems, 2020, 6 (1): 41 - 51.

(收稿日期：2024 - 05 - 10)

作者简介：

卢启刚 (1981 -)，男，硕士，工程师，主要研究方向：大数据、数据安全流通。

杨克松 (1991 -)，男，硕士，工程师，主要研究方向：数据要素、数据安全、数字政府。

王建 (1990 -)，男，硕士，工程师，主要研究方向：数据要素、数字政府、数字经济。

(上接第 46 页)

[12] 周树桥, 于晖, 黄晓津. 基于 Modbus 协议的通信设计及调试方法研究 [J]. 自动化仪表, 2023, 44 (S1): 158 - 164.

[13] 韩灵山, 姜帅, 江豪, 等. 基于 Modbus 的设备能耗信息化系统设计及应用 [J]. 自动化与仪表, 2016, 31 (11): 47 - 49.

[14] 黄俊杰, 汪涛, 王文烁, 等. 基于嵌入式的工业多信息网络交换系统设计 [J]. 仪表技术与传感器, 2019 (6): 123 - 126.

[15] 董海涛, 张帅涛, 冯建强. 基于模拟伺服的多轴 EtherCAT 协议设计 [J]. 仪表技术与传感器, 2023 (2): 69 - 72, 77.

[16] 中国电子信息产业集团有限公司第六研究所. 基于 SPARC 架构微处理器的 EtherCAT 与 Modbus 协议转换网关: CN201711394712. 6 [P]. 2018 - 04 - 20.

[17] 肖万彪, 董培培, 郭星, 等. 基于三菱 FX PLC 的 MODBUS - RTU 通信协议的应用 [J]. 锻压装备与制造技术, 2018, 53 (6): 75 - 78.

(收稿日期：2024 - 03 - 28)

作者简介：

王永峰 (1990 -)，通信作者，男，硕士，工程师，主要研究方向：工业控制、电路与系统。E-mail: 1049207228@qq. com。

康晋菊 (1989 -)，女，硕士，工程师，主要研究方向：工业软件研发。

胡啸 (1983 -)，男，硕士，工程师，主要研究方向：工业控制、电路设计。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部