基于 EtherCAT 总线的 Modbus-RTU 主站网关设计

王永峰，康晋菊，胡　啸，张　彪，封成玉
（中电智能科技有限公司，北京　100083）

摘　要： EtherCAT 在国内工控领域被广泛应用，国内许多工业现场采用 EtherCAT 总线作为控制系统总线。Modbus 也是一种标准开放的通信协议，许多仪器仪表、传感器、变频器支持 Modbus 协议，作为 Modbus 从设备被大量地应用于工控现场。为了解决工控现场 EtherCAT 总线与 Modbus 设备通信问题，设计了一种基于 EtherCAT 总线的 Modbus-RTU 主站网关模块，实现 EtherCAT 总线与 Modbus 协议的转化。该模块对外支持 2 路 RJ45 接口和 1 路 DB9 接口，其中 RJ45 接口支持 EtherCAT 协议，DB9 接口支持 Modbus-RTU 主协议。模块通过 2 路 RJ45 接口灵活应用于 EtherCAT 网络中，可以配置链型和环型拓扑结构。

关键词： EtherCAT；Modbus-RTU 主站；协议转化；拓扑结构
中图分类号： TP273　　**文献标识码：** A　　**DOI：** 10. 19358/j. issn. 2097 - 1788. 2024. 06. 006
引用格式： 王永峰，康晋菊，胡啸，等. 基于 EtherCAT 总线的 Modbus-RTU 主站网关设计［J］. 网络安全与数据治理，2024，43(6)：42 - 46，52.

Design of Modbus-RTU master station gateway based on EtherCAT bus

Wang Yongfeng，Kang Jinju，Hu Xiao，Zhang Biao，Feng Chengyu
（Intelligence Technology of CEC Co.，Ltd.，Beijing 100083，China）

Abstract： EtherCAT is widely used in the field of industrial control in China，and many industry fields use it as the control system bus. Modbus is also a standard and open communication protocol，many instruments，sensors，and frequency converters support the Modbus protocol，as Modbus slave device is widely used in industrial control sites. In order to solve the communication problem between EtherCAT bus and Modbus equipment in industrial control field，a Modbus-RTU master station gateway module based on EtherCAT bus is designed，which realizes the conversion between EtherCAT bus and Modbus protocol. The design supports two RJ45 interfaces and one DB9 interface，the RJ45 interface supports the EtherCAT interface protocol，and the DB9 interface supports the Modbus-RTU main protocol. The design can be configured with chain and ring topologies structure through two RJ45 interfaces，so it can be flexibly applied in EtherCAT networks.

Key words： EtherCAT；Modbus-RTU master station ；protocol conversion；topological structure

0　引言

随着现场总线技术的不断发展，各种总线协议层出不穷，目前已经有 20 多种总线协议被纳入 IEC61158 标准[1]。由于不同的厂商设备采用不同的标准协议，因此用户会遇到设备总线不配套不兼容的问题[2]。本文针对 EtherCAT 和 Modbus 总线进行研究，设计了一种 EtherCAT 和 Modbus 总线协议转换的网关模块，解决工控现场 EtherCAT 总线与 Modbus 设备通信问题[3]。

目前市面上有许多关于 EtherCAT 与 Modbus 总线转化的网关模块，但模块的 EtherCAT 大都采用 E-BUS 接口，主要适配定制的系统中，其物理接口为专用的背板总线接口，不具备通用性；或者是模块性能不能满足工控领域，如波特率、延迟时间、寻址范围、带从站的能力等指标。针对此问题，本文设计一种基于 EtherCAT 总线的 Modbus-RTU 主站网关模块，实现 EtherCAT 总线与 Modbus 协议的转化，模块支持标准 Modbus 寻址范围和功能码，支持诊断功能，可以通过在线诊断数据判断通信正常、响应超时、地址错误、CRC 校验错误等状态，通信波特率支持 1 200 ~ 115 200 b/s 配置，输入输出区大小各为 1 KB，最多可以支持 32 个 Modbus 从站，寻址范围为 1 ~ 247 子节点。模块对外接口包含 2 路 RJ45 和 1 路 DB9 接口，其中 RJ45 接口支持 EtherCAT 协议，可以灵活适配

各种系统和场景，配置链型和环型拓扑结构，提高了模块应用性；1 路 DB9 接口为 Modbus-RTU 接口，支持 Modbus-RTU 主协议，与 Modbus 从站设备相连接。模块功能框图如图 1 所示。

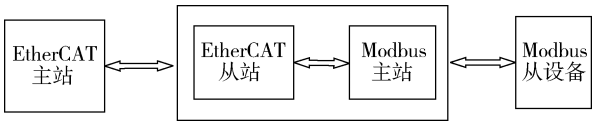

图 1　模块功能框图

1　EtherCAT 与 Modbus 通信原理

1.1　EtherCAT 通信原理

EtherCAT 是 Beckhoff 公司开发的一种实时工业以太网现场总线，其通信速度为 100 Mb/s，具有良好的实时性和同步性。EtherCAT 从站在报文经过其节点时，直接读取相应的数据报文，同时插入需要发送的数据，将消息传到下一个从站，减去了报文的存储、解码、提取过程数据并复制到各个设备的过程，从而降低了对任务数据的处理，提高了网络带宽的利用率，缩短了通信总线传输延时，大大提高了现场总线的性能[4]。

EtherCAT 系统是一个主从站控制系统，在同一网段内采用一个主站多个从站的拓扑结构，从站控制器为专用的集成芯片 ESC，通过双端口存储区实现 EtherCAT 主站与从站本地的数据交换，每个从站按照在通信链路上的物理位置顺序移位对数据帧进行读和写操作[5]。图 2 所示为 EtherCAT 帧处理顺序，从站具有四个数据收发端口，每个端口可以收发数据帧，其中内部传输顺序是固定的，数据从端口 0 进入，然后按照端口 3、1、2、0 顺序传输，如果检测到从站的某个端口上没有外部设备，则自动关闭该端口并转发到下一个端口，因此 EtherCAT 从站至少使用两个数据端口[5]。使用不同端口可以组成各种物理拓扑结构。EtherCAT 协议在数据传输中，发送和接收的以太网帧压缩了大量的设备数据，且双方向的通信都是独立执行的，因此，EtherCAT 具有非常高的带宽速率，并可充分利用 100M 以太网的全双工特性[6]。

1.2　Modbus 通信原理

Modbus 有 Modbus-RTU、Modbus TCP/IP 和 Modbus Plus 等通信方式[7]。经过多年的发展，工控现场设备主要采用 Modbus-RTU 通信模式，如仪器仪表、变频器、伺服电机等设备。

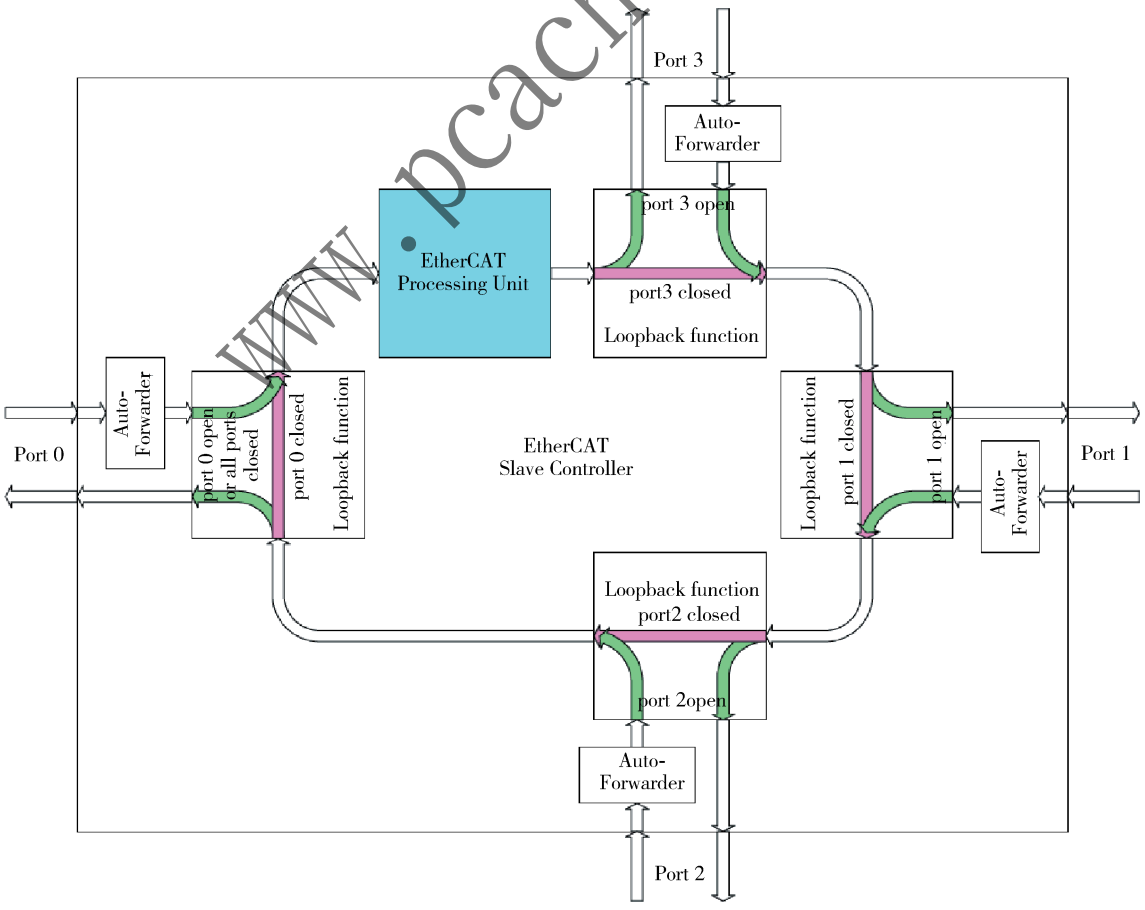

图 2　EtherCAT 帧处理

Modbus 总线技术采用主/从通信方式，即系统中仅有一个主设备，它可以主动发送请求，其他设备为从设备，从设备根据主设备的请求数据做出相应的反应并回复。主设备可以和从设备进行一对一的通信，也可以使用广播的方式与从设备进行一对多的通信。在主设备与从设备通信的过程中，如果通信正常，则从设备发给主机报文中包含请求消息；如果通信异常，返回内容将设置为错误码。图 3 为 Modbus 正常事务处理流程图。

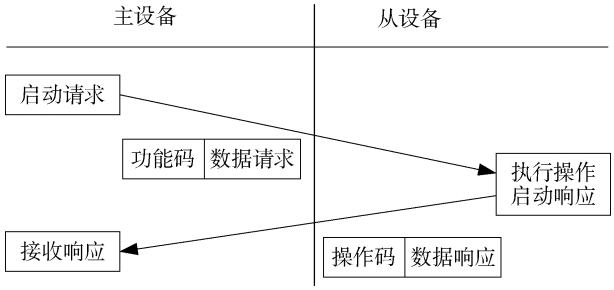

图 3　Modbus 正常事务处理流程

如果发生与请求 Modbus 功能相关的错误，从设备的返回信息中包括一个异常码，主站根据异常码的类型进行相应操作[8]。当从设备响应主设备时，通过功能码数据执行相应的操作[9]。对于一个正常响应来说，从设备仅对原始功能码响应。图 4 为 Modbus 异常事务处理流程图。

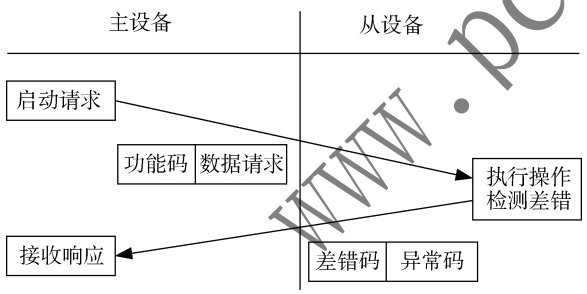

图 4　Modbus 异常事务处理流程

2　硬件电路设计

模块硬件电路主要包括基于 CPU 最小系统、EtherCAT 从站电路、高速光耦隔离、RS485 驱动接口电路、电源电路等部分，模块对外接口包括 2 路 RJ45 接口和 1 路 DB9 接口，其中 RJ45 接口支持 EtherCAT 协议，与 EtherCAT 主站进行连接；DB9 接口实现 Modbus-RTU 通信功能[10]。模块原理框图如图 5 所示。

2.1　CPU 最小系统

MCU 芯片、Flash、SRAM 等组成 CPU 最小系统，用于程序的存储、运行，协议的解析和数据的传输，实现 EtherCAT 与 Modbus 协议间的转化和 Modbus 协议栈功能[11]。在该设计中 MCU 芯片采用基于 SPARC V8 架构的 32 位 RISC 嵌入式处理器，该处理器具有丰富的外设资源。CPU 核心频率可以达到 200 MHz，外设频率为 100 MHz，支持片内 AMBA2.0 总线，支持整型和浮点处理单元，具有丰富的定时器资源，支持外扩 Flash 和 SRAM，支持 DSU 调试接口，集成了 UART16550 接口，接收和发送接口有 64 KB 的 FIFO。

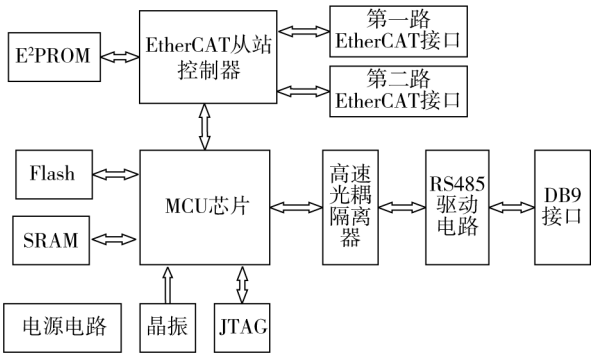

图 5　硬件原理框图

2.2　EtherCAT 从站电路

EtherCAT 从站电路包扩 EtherCAT 从站芯片、E^2PROM、RJ45 接口等电路，原理图如图 6 所示，其中 EtherCAT 从站芯片采用 ET1100，实现 EtherCAT 数据链路层协议，处理 EtherCAT 数据帧；内部集成 2 路 MII 接口和 1 路可选择桥端口，3 个 FMMU 单元，4 个存储同步管理单元，1 KB 的过程数据 RAM[12]。ET1100 与 E^2PROM 通过 I^2C 连接，提供从站配置信息；对内与系统的 CPU 通过 SPI 相连，对外通过 PHY0 和 PHY1 实现 EtherCAT 数据传输，从 EtherCAT 报文提取主站下发给该从站的数据，同时把需要发给主站的数据发给下一个设备，实现从站数据的接收与上传[13]。

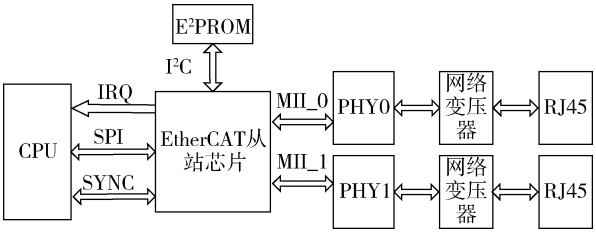

图 6　EtherCAT 从站电路原理图

2.3　RS485 驱动电路

本模块应用于高速、半双工通信场合中，选择了高速 RS485 收发器，与 CPU 侧 UART16550 接口连接，速度高达 10 Mb/s。考虑到主站可以随时接收从站数据，故将 RE 下拉接地；由于发送控制信号 DE 为 CPU 的 GPIO 口控制，上电后状态默认为高，通过加反相器对信号取反，

实现默认工作模式为接收[14]；RS485 芯片后端通过共模电感和磁珠设计，降低 RS485 信号传输过程中的共模干扰和差模干扰。RS485 驱动电路原理图如图 7 所示。

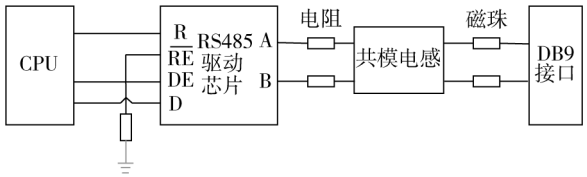

图 7　RS485 驱动电路原理图

3　固件设计

模块固件主要实现的功能包括从 EtherCAT 数据包中获取 Modbus 设备需要的控制数据和参数，组成 Modbus 数据包发送给 Modbus 从站，并将 Modbus 设备返回的数据插入 EtherCAT 数据帧中，上传给 EtherCAT 控制器进行处理。固件设计主要包括 EtherCAT 协议栈、Modbus 协议栈、协议转换功能。

3.1　EtherCAT 协议栈

EtherCAT 协议栈功能框图如图 8 所示，由对象字典、协议栈状态转换、CoE 功能组成，其中对象字典是一个数据存储和操作方式的集合，协议栈状态转换实现从站各状态的切换功能[15]，包括初始化、预运行、安全运行、正常运行四个状态的切换，CoE 为 EtherCAT 应用层协议解析配置信息。

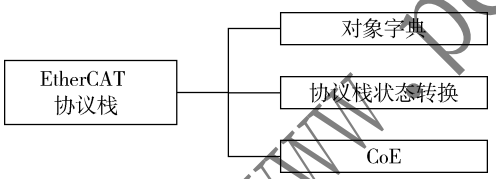

图 8　EtherCAT 协议栈功能框图

3.2　Modbus 协议栈

Modbus 协议栈框图如图 9 所示，包括 Modbus 主站、协议栈运行逻辑、功能码、组织 Modbus 数据帧、解析 Modbus 数据帧、异常处理、数据链路层控制。其中数据链路层控制包括数据收发控制、定时控制、CRC 校验。

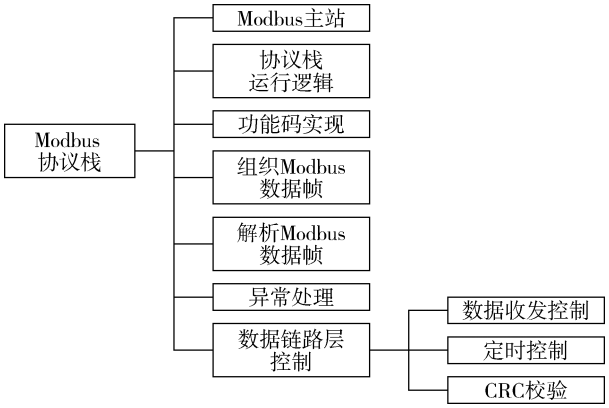

图 9　Modbus 协议栈框图

3.3　协议转化功能

协议转换功能框图如图 10 所示，包括 CoE 配置解析和过程数据搬移。CoE 配置解析包括 Modbus 主站和 Modbus 从站两部分的信息，主站信息包括波特率、校验方式、超时时间、重发次数等信息，从站信息包括站地址、功能码、数据地址、数据长度等信息[16]。过程数据搬移是将输出的过程数据从 EtherCAT 缓存区搬移至 Modbus 协议栈缓存区，将输入的过程数据从 Modbus 协议栈缓存区搬移至 EtherCAT 缓存区。

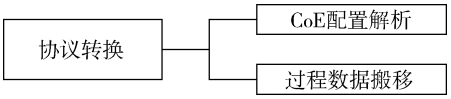

图 10　协议转化功能图

4　网络拓扑

模块对外具有 2 路 RJ45 接口，支持 EtherCAT 协议，可以连接到 EtherCAT 网络中，实现菊花链型和环网的拓扑结构，如图 11 和图 12 所示，满足了工业现场的组网模式，提高模块的灵活性。当采用环网的拓扑结构时，网络中任何一个设备发生故障，主站可以通过环网的两端分别与其他模块进行通信，提高系统的可靠性[17]。

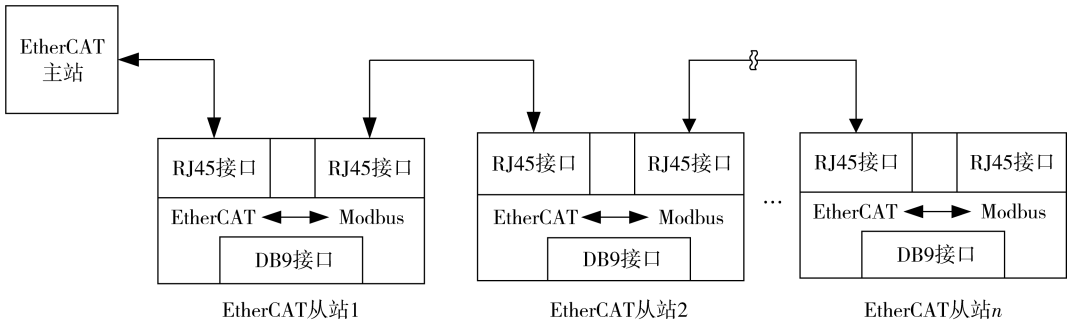

图 11　菊花链型拓扑

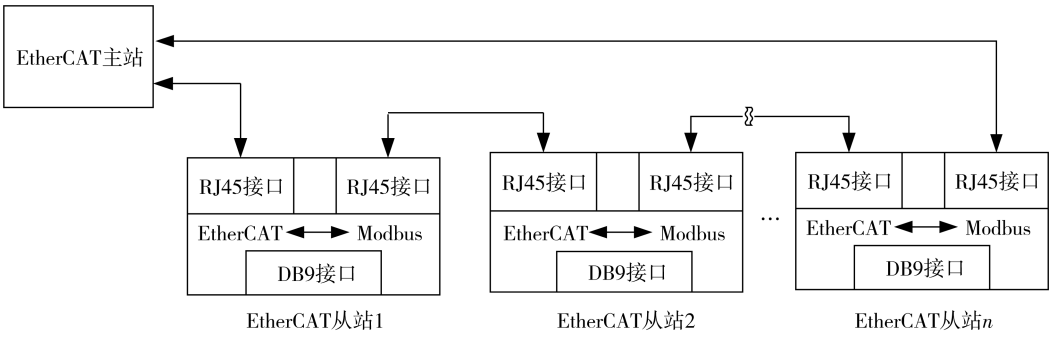

图 12　环网型拓扑

5　功能验证

模块通过与基于 EtherCAT 总线的 PLC 主控器相连接，实现 EtherCAT 主站控制功能，对外与电脑 Modbus-slave 进行通信，验证模块的通信功能。

通过上位机编程软件进行配置，Modbus 所有功能码如图 13 所示，与 Modbus-slave 虚拟从站进行通信，装包数据如图 14 所示，可以验证模块通信正常。

图 13　验证配置

```
000775-Tx:01 04 06 04 89 04 83 04 7D 8E F1
000776-Rx:01 01 00 00 00 03 7C 0B
000777-Tx:01 01 01 00 51 88
000778-Rx:01 02 00 00 00 03 38 0B
000779-Tx:01 02 01 06 21 8A
000780-Rx:01 06 00 00 9B 0A 62 FD
000781-Tx:01 06 00 00 9B 0A 62 FD
000782-Rx:01 10 00 00 00 03 06 00 00 04 83 00 00 16 58
000783-Tx:01 10 00 00 00 03 80 08
000784-Rx:01 03 00 00 00 03 05 CB
000785-Tx:01 03 06 00 00 04 83 00 00 D1 AD
000786-Rx:01 04 00 00 00 03 B0 0B
000787-Tx:01 04 06 04 8A 04 84 04 7E 3B 31
000788-Rx:01 01 00 00 00 03 7C 0B
000789-Tx:01 01 01 00 51 88
000790-Rx:01 02 00 00 00 03 38 0B
000791-Tx:01 02 01 00 A1 88
000792-Rx:01 06 00 00 9C 44 E0 F9
000793-Tx:01 06 00 00 9C 44 E0 F9
000794-Rx:01 03 00 00 00 03 05 CB
000795-Tx:01 03 06 9C 44 04 83 00 00 3C 3E
000796-Rx:01 04 00 00 00 03 B0 0B
000797-Tx:01 04 06 04 8B 04 85 04 7F 96 F1
000798-Rx:01 01 00 00 00 03 7C 0B
000799-Tx:01 01 01 06 D1 8A
000800-Rx:01 02 00 00 00 03 38 0B
000801-Tx:01 02 01 06 21 8A
000802-Rx:01 06 00 00 9D 4C E0 AF
000803-Tx:01 06 00 00 9D 4C E0 AF
```

图 14　装包数据

6　结论

本文设计了一种基于 EtherCAT 总线的 Modbus-RTU 主站网关模块，实现 EtherCAT 总线与 Modbus 协议的转化，拓宽了以 EtherCAT 为总线的设备的应用能力，解决了现场两种总线不兼容的问题。模块支持 2 路 RJ45 和 1 路 DB9 接口，可以配置 EtherCAT 总线链型和环型拓扑结构，提高了模块的易用性。

参考文献

[1] 尹震宇，许鹏，徐福龙. 基于 FPGA SoC 的 EtherCAT 协议栈设计与实现［J］. 小型微型计算机系统，2022，43（8）：1751－1755.

[2] 冯涛，王帅帅，龚翔，等. 工业以太网 EtherCAT 协议形式化安全评估及改进［J］. 计算机研究与发展，2020，57（11）：2312－2327.

[3] 耿英博，杜向阳，张克平，等. 基于 EtherCAT 总线的涂胶机器人控制系统设计［J］. 轻工机械，2018，36（1）：66－70.

[4] 徐健，宋宝，唐小琦. EtherCAT 与 Modbus 协议转换网关的设计及实现［J］. 组合机床与自动化加工技术，2015（4）：71－73，77.

[5] 杨亮. 基于 Modbus 协议的三菱 PLC 与 E700 变频器通信实例［J］. 工业控制计算机，2023，36（8）：45－46.

[6] 林浩，韩庆敏，宋栋，等. 基于实时工业以太网的脉冲发生器［J］. 电子技术应用，2018，44（10）：64－67.

[7] 彭杰，应启戛. 工业以太网的安全性研究［J］. 仪器仪表学报，2004，25（S1）：516－517.

[8] 马保全，姚旺君，刘云龙，等. 基于 FPGA 的 EtherCAT 从站通信链路分析与验证［J］. 电子技术应用，2017，43（8）：95－99.

[9] 黄兵，丰大军，刘云龙，等. 基于 FPGA 的 EtherCAT 协议链路冗余研究［J］. 电子技术应用，2017，43（9）：80－82，86.

[10] 姚旺君，林浩，王永利，等. 基于 FPGA 的 EtherCAT 从站控制器 FMMU 模块设计［J］. 信息技术与网络安全，2018，37（8）：77－82.

[11] 朱斌庚，陈晓曼. 基于 Modbus 协议的边缘计算电能质量网关设计［J］. 现代信息科技，2023，7（22）：174－178.

（下转第 52 页）

[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