基于飞腾 E2000 的安全网关设计与实现

黄　武,盛四华,田　炜,蒋增文,李刚锋
(中电工业互联网有限公司,湖南 长沙 410006)

摘　要:在万物互联的大背景下,实现系统的安全可信始终是最核心的目标。随着国产信息系统建设的不断深入,实现系统的安全可信已经成为最迫切的需求。为了解决工业互联网的多接口数据互联和数据安全问题,设计了一款基于飞腾嵌入式 E2000 处理器的安全网关设备。实现了 3G/4G/5G 无线 VPN 路由功能,同时支持以太网、RS232/485 串口,CAN 口接入,并支持 Wifi/蓝牙通信以及 GPS/北斗定位。通过分析 VLAN 协议原理,基于 RTL8367SC 芯片实现了内置网络交换机功能;融合基于 RG200U 的 5G 模块挂载方法,形成了网关的内置 5G 交换机系统,进一步解决了多通道数据互联的问题。通过分析飞腾安全处理器平台架构规范(Phytium Security Platform Architecture,PSPA),设计了网关的安全可信固件制作方法,保证了启动过程执行的所有代码都是安全可信的。通过搭建测试环境进行测试验证,测试结果表明,该系统实现了多种接口的数据互联,并基于多项 E2000 芯片内置安全加密算法,使安全性方面得到了较大提升。

关键词:飞腾 E2000;安全网关;PSPA;RTL8367SC;RG200U
中图分类号:TP393　　**文献标识码**:A　　**文章编号**:1673-629X(2025)02-0048-06
doi:10.20165/j.cnki.ISSN1673-629X.2024.0324

Design and Implementation of Security Gateway Based on Phytium E2000

HUANG Wu,SHENG Si-hua,TIAN Wei,JIANG Zeng-wen,LI Gang-feng
(CEC Industrial Internet Co.,Ltd.,Changsha 410006,China)

Abstract:Under the background of the Internet of everything,to achieve the security and credibility of the system is always the core goal. With the deepening of the construction of domestic information systems,to achieve the security and credibility of the system has become the most urgent demand. In order to solve the problem of multi-interface data interconnection and data security of industrial gateway,a security gateway device based on Phytium embedded E2000 processor is designed. It realizes 3G/4G/5G wireless VPN routing function, while supporting Ethernet,RS232/485 serial port,CAN port access,Wifi/Bluetooth communication and GPS/Beidou positioning. By analyzing the principle of VLAN protocol,the function of built-in network switch is realized based on RTL8367SC chip. The 5G module mounting method based on RG200U is integrated to form a built-in 5G switch system of the gateway,which further solves the problem of multi-channel data interconnection. Based on Phytium Security Platform Architecture (PSPA),a method of making secure and trusted firmware of the gateway is designed to ensure that all the code executed during the startup process is safe and trusted. By building a test environment for test and verification,the test results show that the system realizes the data interconnection of multiple interfaces,and based on a number of E2000 chip built-in security encryption algorithms,the security has been greatly improved.

Key words:Phytium E2000;security gateway;PSPA;RTL8367SC;RG200U

0　引　言

网关设备是一种终端的网络设备,是局域网络智能化的关键,一般需支持虚拟网络接入、Wifi 接入、有线接入等。通过网关可以实现对局域网内各传感器设备、网络设备等的信息采集、输入、输出、控制等功能。网关在物联网时代扮演着非常重要的角色,它将成为连接无线传感网络与传统通信网络的桥梁,完成无线传感网络,传统通信网络以及其他不同类型网络之间的协议转换,实现局域网和广域网的数据互联。

现有网关产品主流选用的是进口芯片开发,当然随着国产芯片研发能力的提升,国产处理器的种类与性能日益增加,采用国产处理器研发的产品种类也是与日俱增,但目前国内自主可控嵌入式芯片也存在着算力不足、功耗较大、安全性低等问题。

收稿日期:2024-08-08　　**修回日期**:2024-12-11
基金项目:湖南省创新型省份建设专项(2021GK4012)
作者简介:黄　武(1987-),男(土家族),工程师,硕士,通信作者,研究方向为嵌入式系统与终端。

安全可信始终是信息系统最基础、最核心的目标。随着国产信息系统建设的不断深入,实现信息系统的安全可信已成为最为迫切的追求。而其中基础处理芯片的安全属性和功能对系统的安全性起到至关重要的作用。

该文提出的安全网关设备使用飞腾新一代嵌入式芯片 E2000 处理器进行设计,相较于进口嵌入式芯片而言,E2000 处理器在性能和安全性方面有了很大提升,采用多项低功耗技术和加密算法,进一步解决了网关设备进行数据采集以及边缘计算时算力不足、安全性低以及功耗较大的问题。

与常规网关设备相比较,该文提出的安全网关设备除了常规网关设备数据传输的基本功能以外,还通过板载 eMMC 和外扩 SD 卡模块增加了本地数据存储功能,并具备多种查询方式,便于进行数据查询与追溯。

该文提出的安全网关设备还具备内置 3G/4G/5G 网络交换机功能[1-2],通过软硬件驱动方案实现多通道数据互联,从而提高生产和监控的自动化水平。

1　系统总体设计

飞腾 E2000 系列是飞腾公司新推出的腾珑系列嵌入式芯片。具备领先的安全特性,支持安全启动,可信计算等多种安全手段。同时兼容可灵活调节的性能与功耗,适应广泛的嵌入式应用场景。

飞腾 E2000 系列集成两个 FTC310 核,兼容 ARM V8 指令系统,支持 64 位和 32 位指令;兼容 ARM V8 虚拟化体系结构,支持 KVM、Xen 虚拟机,同时支持单精度、双精度浮点运算指令,支持 ASIMD 处理指令。同时,该系列芯片还集成了丰富的外设接口和资源,包含 DDR4 控制器、PCIE 接口、支持 SGMII 和 RGMII 的千兆以太网控制器、USB2.0 与 USB3.0 控制器、SD 控制器、QSPI Flash 控制器、SPI Master 控制器、CAN 控制器、UART 控制器和 I2C 控制器等。可应用于电力、轨交、工控等领域。

该系统存储模块选择 DDR4 存储介质,在数据传输速率和读写速度上都优于 DDR3。使用大容量存储介质 eMMC 作为系统存储器,同时支持 SD 卡外接存储。方便进行固件更新、系统加载和数据存储。飞腾 E2000 通过 USB2.0 接口与 4G 模块连接,或通过 USB3.0 接口与 5G 模块连接,同时实现 AT 指令发送与数据传输功能。

另外本安全网关设备还包含 RS232/RS485/CAN 等传感器设备接口,并扩展了 Wifi/蓝牙双模以及 GPS/北斗双模[3]。飞腾 E2000 安全网关系统框图如图 1 所示。

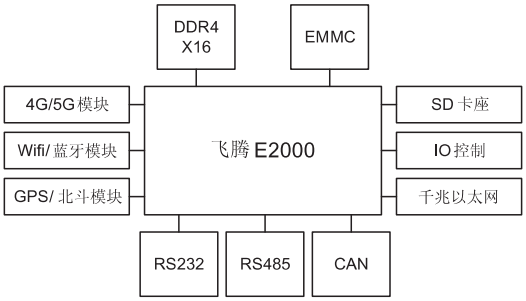

图 1　安全网关系统框图

2　交换系统硬件设计

RTL8367SC 是一款 5+2 端口千兆以太网交换机芯片,五个通用 PHY 接口集成了低功耗 Giga-PHY,每个端口都支持全双工 10/100/1 000 M 连接。RTL8367SC 支持两个额外的高速串行 Giga-MAC 接口,支持 HSGMII/SGMII 接入。芯片集成 SPI 接口,可外扩 EEPROM 芯片或配置成 SPI 从接口与主控芯片进行连接,可对 RTL8367SC 寄存器进行配置。

飞腾 E2000 作为主控芯片,通过 SPI 接口对 RTL8367SC 芯片进行寄存器配置。使用 SGMII 接口与 RTL8367SC 进行数据互联。RTL8367SC 芯片最多可外扩 5 个 RJ45 端口[4](如图 2 所示)。

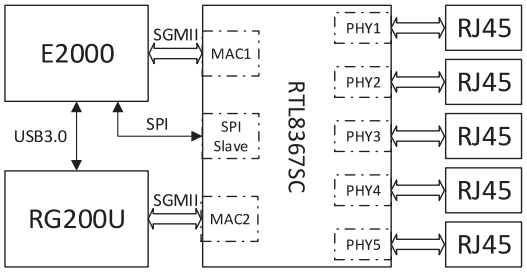

图 2　RTL8367SC 交换机框图

RTL8367SC 支持 IEEE802.1Q 协议,即 Virtual Bridged Local Area Networks(虚拟局域网)。该协议规定了 VLAN 的国际标准实现,从而使得不同厂商之间的 VLAN 互通成为可能[5-6]。802.1Q 协议(见图 3)规定了一段新的以太网帧字段,与标准以太网相比,VLAN 报文在源地址后加了一段 4 字节的 802.1Q 标签。其中包含了两个字节的标签协议标识(Tag Protocol Identifier,TPID)以及两个字节的标签控制信息(Tag Control Information,TCI),TPID 是 IEEE 定义的新的类型,表明这是一个加了 802.1Q 标签的报文。IEEE 802.1Q 以及 VLAN Tagging 属于互联网下 IEEE 802.1 的标准规范,允许多个网桥在信息不被外泄的情况下公开地共享同一个实体网[7]。

因为 LAN 都是处于一个广播域中,所以很容易造成广播风暴。而 VLAN 是虚拟局域网,是将一个物理的 LAN 在逻辑上划分成多个广播域的通信技术。VLAN 内的主机间可以直接通信,而 VLAN 间不能直

接互通,从而将广播报文限制在一个 VLAN 内[8]。

RTL8367SC 支持 VLAN 的 Un-tag 定义[9]。所谓的 Untagged Port 和 Tagged Port 不是讲述物理端口的状态,而是指物理端口所拥有的某一个 VID 的状态,所以一个物理端口可以在某一个 VID 上是 Untagged Port,在另一个 VID 上是 Tagged Port;而一个物理端口只能拥有一个 PVID,当一个物理端口拥有了一个 PVID 的时候,必然也会存在和 PVID 和 TAG 相同的 VID,且在这个 VID 上,这个物理端口必定是 Untagged Port。

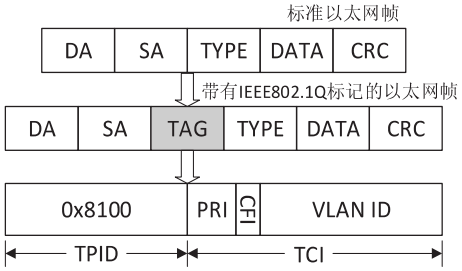

图 3 802.1Q 标签形式

PVID 的作用只是在 RTL8367SC 从外部接收到 Untagged 数据帧的时候给数据帧添加 TAG 标记,在 RTL8367SC 内部转发数据时无作用。拥有和 TAG 标记一致的 VID 的物理端口,不论是否在这个 VID 上是 Untagged Port 或是 Tagged Port,都可以在 RTL8367SC 内部接收标记了这个 TAG 标记的 tagged 数据帧;拥有和 TAG 标记一致的 VID 的物理端口,只有在这个 VID 上是 Tagged Port,在可以接收来自 RTL8367SC 外部的标记了这个 TAG 标记的 tagged 数据帧[10]。不同端口类型对各数据帧处理方法如表 1 所示。

表 1 不同端口类型对各数据帧处理方法

端口	Tag 帧		Untag 帧	
	IN	OUT	IN	OUT
Tag 端口	保持不变		按 PVID 添加 tag 标记	
Untag 端口	丢弃	VLAN ID=PVID 时,去 tag,否则丢弃	按 PVID 添加 tag 标记	保持不变

使用 RTL8367SC 的 VLAN 协议模式,保证了各网口的互通,另外存在 SGMII 接口与 5G 模块进行通信,也保证了各网口能够通过 5G 连接上广域网,真正实现各端口的数据互联。

3 系统软件设计

3.1 RTL8367SC 驱动设计

对于 RTL8367SC 芯片来说,其具备 16 个芯片寄存器配置,对于该交换芯片,其中 MAC 已默认配置为 SGMII 模式,且在默认配置下,相关 PHY 接口已经能够互通,也即不做任何寄存器配置,外部 RJ45 之间都能实现互通。

RTL8367SC 支持特殊的插入 VLAN 标记功能,可在网关应用中将流量与 WAN 和 LAN 端口分开。具体使用时,RTL8367SC 支持每个端口的端口 VID(PVID),并且可以在出口的 VLAN 标记中插入 PVID。使用该功能时,VLAN 标记中携带的 VID 信息将更改为 PVID,且 RTL8367SC 还提供了一个选项,仅允许使用带有特定 PVID 的 VLAN 标记数据包。如果启动此功能,它将丢弃未标记的数据包和具有错误 PVID 的数据包。

RTL8367SC 支持 8 个优先级队列和输入带宽控制。数据包优先级选择可以取决于基于端口的优先级,基于 802.1Q 标签的优先级,基于 IPv4/IPv6 DSCP 的优先级和基于 ACL 的优先级。在 RTL8367SC 中启用多个优先级时,将根据优先级选择表分配数据包的优先级。

因此在飞腾 E2000 端,需使 E2000 内核支持 802.1Q 功能。该方案在 Linux 4.19 版本下进行内核配置,在 kernel 下使用 make menuconfig 进行内核配置,并在 Networking support 中将 802.1Q 相关选项都编进内核。然后加载 RTL8367SC LAN 驱动文件,编译 kernel 并下载到设备。最后进行配置,创建网桥:

```
brctl addbr br0
```

给网桥虚拟网卡配置 IP 段,便于远程控制网桥:

```
ifconfig br0 192.168.1.1
```

将相关 LAN 接口和网桥段进行连接(本例中只使用两个网口):

```
brctl addif br0 eth0
brctl addif br0 eth1
```

再进行设备连接,使用 ifconfig 指令即可看到各 LAN 口配置信息。

当进行千兆网络通信时,E2000 芯片在设备树内将 RTL8367SC 挂载在 SPI 设备下,对交换机完成初始化后,还需配置 rx_delay 与 tx_delay 延时。经测试,配置延时为 20 单位时,E2000 通过 SGMII 接口与 RTL8367SC 芯片实现千兆以太网通讯正常。

广播风暴抑制功能,RTL8367SC 通过设置寄存器来启用或禁用每端口广播/组播/未知 DA 风暴控制(默认为禁用)。广播/组播/未知 DA 数据包的接收速率超过参考速率后,所有其他广播/组播/未知 DA 数据包将被丢弃。参考速率通过寄存器配置进行设置[11]。

3.2 RG200U 驱动设计

RG200U 是上海移远通信的一款专为 IoT/eMBB/URLLC 应用而设计的 5G Sub-6GHz 模块。其同时支

持 5G NSA 和 SA 模式。支持 TDD 和 FDD 两种模式,支持双卡,同时向下兼容 4G/3G。RG200U 模块内置丰富的网络协议,集成多个工业标准接口,并支持多种驱动和软件功能,如 Windows、Linux、Android 等操作系统下的 USB/PCIE 驱动等,极大地拓展了其在 IoT 和 eMBB 领域的应用范围。RG200U 是基于移远的展锐 udx710 平台开发的 5G 模组。在华为被禁,MH5000-31 平台无法使用后,该平台已成为国产 5G 模组不多的选择之一了。

该方案中飞腾 E2000 通过 USB3.0 接口对 RG200U 的 5G 模块进行 AT 指令配置,并可直接进行数据交互。本例中飞腾 E2000 加载的是 Linux 系统,应用中首先在系统启动后通过 dmsg 可以查看 5G 驱动 NCM 挂载情况,如图 4 所示。

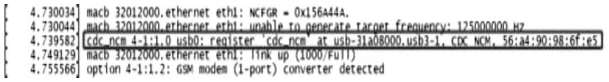

图 4　5G 驱动 NCM 挂载情况

为确定 5G 挂载位置是否正常,通过 ifconfig - a 指令查看网络节点是否挂载正常,如图 5 所示。

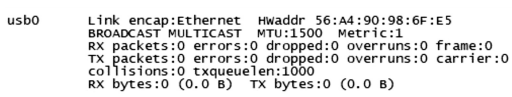

图 5　5G 网络节点挂载情况

通过 USB3.0 发送 AT 配置指令进行 RG200U 配置,发送以下命令进行网卡模式 NCM 配置:

AT+QCFG="usbnet",5

因为 5G 模块 RG200U 用于数据传输时,在 Windows 下使用的是 RNDIS 驱动(对应 AT 指令为 AT+QCFG="usbnet",3),在 Linux 下使用的是 NCM 驱动,因此采用以上驱动配置指令。同时设定网络自动连接:

AT+QNETDEVCTL=2,3,1

中间那个 3 即代表每次开机自动拨号建立连接,这样,只需要配置一次,以后开机就不再需要配置了,每次上电自动建立 cid=2 的数据连接。然后设置自动获取 IP:

udhcpc -i usb0

配置完成后相应打印内容如图 6 所示。

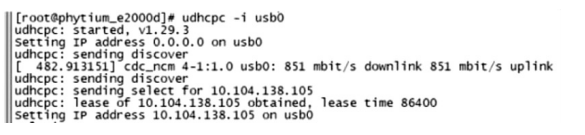

图 6　5G 模块 IP 获取打印内容

系统中 USB3.0 连接会显示 851 Mbps,如果使用 USB2.0 连接,显示的是 425 Mbps。

本方案 RG200U 的 5G 模块与交换机芯片 RTL8367SC 具备直接的 SGMII 接口连接,因此具备直接将 RJ45 网口设备信息转发的能力,使用 5G 直接转发需要对 RG200U 模块进行以下 AT 指令配置:

AT+QIACT=1

该指令为开发 PDP 上下文,必须保证 5G 模块 PDP 上下文有效,后续配置才有意义。之后使能 SGMII 模块:

AT+QSGMIICFG="enable",1

配置网口速度为自动协商:

AT+QSGMIICFG="config",1

完成以上配置后,可以进行网口信息查询,确认网口连接是否正常,查询命令如下:

AT+QSGMIICFG="info"

系统回复 SGMII 网口正常后,即可通过设备 RJ45 网口,直接使用 5G 模块进行数据转发,或者使用 RJ45 网口进行上网操作等。至此,飞腾 E2000 下 5G 模块 RG200U 的驱动加载完毕,此时即可通过 5G 实现无线路由功能,各网口可通过 5G 上网并实现各端口数据互联。

4　安全可信设计

飞腾公司为了统一飞腾系列安全可信处理器的属性和功能,规范软硬件厂商的接口,推出了飞腾安全处理器平台架构规范(Phytium Security Platform Architecture,PSPA)。PSPA 包含密码密钥相关内容,具体为密码加速引擎、密钥管理;包含可信相关内容,具体为可信启动、可信执行环境;包括敏感信息和固件保护的相关内容,具体为安全存储、固件管理;包含芯片生产及全寿命周期管理内容,具体为量产注入、生命周期管理;包含抗物理攻击及硬件漏洞免疫相关内容共计十个方面[12]。

PSPA 在芯片层面实现了安全可信运行,在设计层面需要进行可信固件设计以实现可信启动[13],即保证在处理器启动过程中,所有被执行的代码、引入的数据都是通过度量认证的[14]。

飞腾平台的固件架构分为芯片内置的飞腾启动 ROM(Phytium Boot ROM,PBR)、飞腾基础固件(Phytium Base Firmware,PBF)和系统固件(System Firmware,SFW)三个层次。PBR 保存在飞腾安全处理器芯片内,无法被篡改。其主要功能为在启动过程中验签位于片外非易失存储介质上的 PBF,如果验签通过则加载 PBF。PBF 的主要功能是进行处理器硬件初始化,然后验签、加载 SFW。SFW 按照逐级验签的模式,以此加载、验签、执行后续模块,进而引导操作系统[15-16]。可信启动流程如图 7 所示。

可信固件制作需要由 PBF 对系统引导程序 uboot 进行可信封装。首先需对打包环境进行搭建,主要使

用 GmSSL 工具。GmSSL 是一个开源的密码工具箱，支持 SM2/SM3/SM4/SM9/ZUC 等国密算法，支持国密硬件密码设备，并提供符合国密规范的编程接口与命令行工具，可以用于构建 PKI/CA、安全通信、数据加密等符合国密标准的安全应用。可信固件环境搭建如图 8 所示。

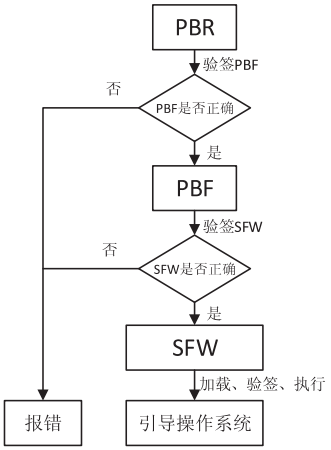

图 7 可信启动流程

1、使用GmSSL工具，在当前工作目录中解压；

2、编译输出到当前目录中：
./Configure – prefix = $(pwd)/output shared no-asm linux

3、使用gcc-linaro交叉编译器make file；

4、执行$ sudo make install；

5、执行$ gmssl version命令行工具，检查安装是否成功；

6、动态链接库到当前目录，即可往下操作打包工具。

图 8 可信固件环境搭建

建立好可信固件环境，需要用到飞腾打包工具将 uboot 引导程序进行打包处理，使用的工具为 image_fix_e2000_v1.07，统一动态链接库，并将做好的 uboot 放置到打包工具中，链接到最终生成的 bin 文件上。执行以下操作：

./my_scripts/fix_parameter.sh

进行 PBF 参数配置。

./my_scripts/image-fix.sh cot

加密 bin 文件。即完成可信固件制作，保证网关系统安全可信加载运行。

5 系统测试

对提出的飞腾 E2000 安全网关进行了实物设计与测试验证，网关系统实物如图 9 所示。

系统搭建如图 10 所示的测试框图。测试在某应用项目进行，E2000 安全网关系统作为终端值守设备，通过 CAN 接口连接进入本地 CAN 总线系统，通过 RS485 或串口连接串口终端与传感器设备，通过以太网连接本地摄像头、便携设备或本地终端等。

图 9 飞腾 E2000 安全网关实物图

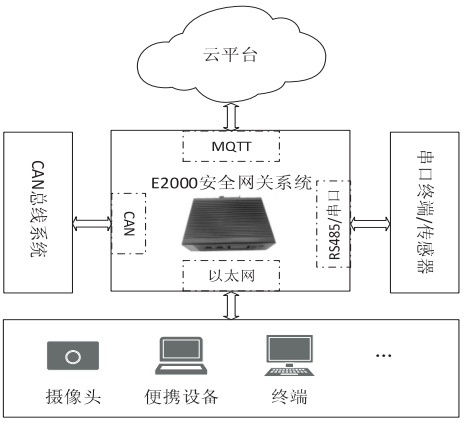

图 10 E2000 网关系统配置框图

摄像头采集的视频信息通过 5G 直接向云平台进行转发，网络端使用拉流工具直接输入流媒体地址进行拉流播放，如图 11 所示，更进一步的，可通过飞腾 E2000 主控芯片实现对视频信息添加 OSD 信息。

图 11 网络端拉流播放

网关系统可直接采集本地数据并进行 MQTT 报文包装，链接上云平台，同时便携设备与本地终端可通过网关内置的交换系统使用 5G 进行上网，实现终端设备互联。

图 12 网关配置工具图

使用自研网关配置软件可远程进行各网关系统参数读取与配置,如图 12 所示。说明 E2000 安全网关系统通过 MQTT 协议向相关物联网平台传输数据连接成功。

6　结束语

该文研究了基于飞腾 E2000 的网关系统架构,并设计了一款内置 5G 交换机功能的安全网关。从硬件层面解读了该网关的设计方案,从软件方面说明了交换机部分与 5G 模块的驱动方案,并基于 PSPA 说明了可信固件生成方式。最后通过实物展示与项目应用验证了 E2000 安全网关的可行性与实用性。

飞腾嵌入式芯片具备国产化优势,设计完全自主可控,搭配其内置加密算法与低功耗设计,将其使用于网关系统具有一定的应用价值;使用提出的内置交换机系统与多接口设计,可以方便地实现各通道数据安全互联,具备较大的推广价值。

参考文献:

[1] 周克勤,罗瑞林,云利军,等. 车载信息安全网关的设计与实现[J]. 云南师范大学学报:自然科学版,2021,41(5):22-27.

[2] 刘　亮,李　卉. 边缘计算网关的功能设计与系统实现[J]. 电测与仪表,2021,58(8):42-48.

[3] 李　鹏,裴丽娜,夏凯旋,等. 一种多协议转换工业智能加密网关[J]. 单片机与嵌入式系统应用,2023,23(2):66-69.

[4] 李万军. Zynq7020 与 BCM5396 的嵌入式数据交换模块设计[J]. 单片机与嵌入式系统应用,2022,22(9):67-70.

[5] 庞韶敏,李亚波. 移动通信核心网[M]. 北京:电子工业出版社,2016:10-12.

[6] 胡天麟. 基于 IPSec 协议的 VPN 安全网关的设计与实现[J]. 通信电源技术,2020,37(3):78-79.

[7] 张　超,王志超,林　岩. 基于 LwIP 协议栈的嵌入式网络控制系统设计[J]. 单片机与嵌入式系统应用,2019,19(2):34-36.

[8] 蓝方力. 虚拟网络技术在计算机网络安全中的应用[J]. 网络安全技术与应用,2020(12):28-29.

[9] 陈海倩,张丽娟,赖宇阳,等. 基于 SSL VPN 技术的电力安全网关设计与实现[J]. 电子设计工程,2020,28(13):97-100.

[10] 沈　鑫,侯若鹏,毛　臻,等. FreeRTOS 和 LwIP 嵌入式设备的以太网通信研究[J]. 单片机和嵌入式系统应用,2023,23(7):29-32.

[11] 宋一杭. 面向物联网弱终端的低功耗通信及接入理论和关键技术研究[D]. 成都:电子科技大学,2022.

[12] NAZARENKO A A, SAFDAR G A. Survey on security and privacy issues in cyber physical systems[J]. AIMS Electronics and Electrical Engineering,2019,3(2):111-143.

[13] NWEKE L O. A survey of specification-based intrusion detection techniques for cyber-physical systems[J]. International Journal of Advanced Computer Science and Applications,2021,12(5):37-45.

[14] ENOCH K, SUBHRAKANTI D, LING S. The performance and limitations of epsilon-stealthy attacks on higher order systems[J]. IEEE Transactions on Automatic Control,2017,62(2):941-947.

[15] YU Zhenhua, GAO Hongxia, GONG Xuya, et al. A survey on cyber - physical systems security[J]. IEEE Internet of Things Journal,2023,10(24):21670-21686.

[16] BRETT M. Exploring phronesis in cyber security, management and resilience[J]. Cyber Security,2023,6(2):154-167.