文章编号:1671-4598(2024)10-0228-08 DOI:10.16526/j.cnki.11-4762/tp.2024.10.033 中图分类号:TP393.01 文献标识码:A

基于 openSAFETY 的功能安全通信协议研究

徐建明[1,2], 周家豪[1], 陈 琳[1], 金 瑶[2], 周路顺[2], 张扬扬[2]
(1. 浙江工业大学 信息工程学院, 杭州 310023;
2. 杭州力为科技有限公司, 杭州 311400)

摘要: 针对数据传输可靠性低导致功能安全事故频发的问题, 进行了基于 POWERLINK 的 openSAFETY 功能安全通信协议研究; 在实时工业以太网协议 POWERLINK 的基础上设计了以 PCP-AP 为架构的 openSAFETY 安全节点, 设计了基于 FPGA 软核处理器的 POWERLINK 内核层的软件硬件结构, 设计了基于单片机 MCU 的 openSAFETY 安全应用接口程序以及近底层通信接口程序, 搭建了以贝加莱 PLC 为安全控制节点的功能安全通信实验平台, 依据故障分析设计了电磁干扰实验, 模拟了工业现场中出现不同程度电磁干扰情况下功能安全通信平台的通信情况, 并与非功能安全通信平台进行对比, 验证了安全节点的可靠性和必要性。

关键词: 功能安全; 工业以太网; openSAFETY; POWERLINK; 电磁干扰; FPGA

Research on Functional Safety Communication Protocol Based on OpenSAFETY

XU Jianming[1,2], ZHOU Jiahao[1], CHEN Lin[1], JIN Yao[2], ZHOU Lushun[2], ZHANG Yangyang[2]
(1. College of Information Engineering, Zhejiang University of Technology, Hangzhou 310023, China;
2. Hangzhou Liwei Technology Co., Ltd., Hangzhou 311400, China)

Abstract: Aiming at the problem of frequent functional safety accidents caused by low reliability of data transmission, this paper studies an openSAFETY functional safety communication protocol based on POWERLINK, presents an openSAFETY node with the PCP-AP architecture based on the real-time industrial Ethernet protocol POWERLINK, designs software and hardware structure of POWERLINK kernel layer based on FPGA soft-core processor, achieves the openSAFETY safety application interface program and the near bottom communication interface program based on MCU, and builds a functional safety communication experimental platform with B&R PLC as the safety control node. The electromagnetic interference experiment is designed according to the fault analysis, the communication situation of the functional safety communication platform is simulated in different degrees of electromagnetic interference in industrial fields, and compared with the non-functional safety communication platform, this platform verifies the reliability and necessity of the safety node.

Keywords: functional safety; industrial Ethernet; openSAFETY; POWERLINK; electromagnetic interference; FPGA

0 引言

随着工业互联网的快速发展, 工业化与信息化的不断交融[1], 现场总线技术和以太网技术广泛应用于汽车[2-3]、纺织[4]、核工业[5-6]等产业中。但同时也出现了很多安全事故, 例如: 特斯拉刹车失灵事故, 郑州无人机集体失控坠落事故和甘肃电梯故障导致幼童坠亡事故。为了减少由于自身安全功能不完善而发生的故障, 提出了功能安全的概念。功能安全 (FS, functional safety) 是指在设备或系统的设计、开发和操作中, 保障其在发生故障或异常情况下仍能够安全可靠运行的一种特性。

国际电工委员会提出的 IEC 61508[7-8]提供了一种定量计算安全功能危险失效的安全完整性等级 (SIL, safety integrity levels), 为开发安全设备和安全主控制器提供了明确的安全衡量标准。SIL 分成 1、2、3、4 共 4 个等级, 其对应的残余错误率分别是$<10^{-7}$/h、$<10^{-8}$/h、$<10^{-9}$/h、$<10^{-10}$/h。SIL 为 3 时可以满足大部分工业中对功能安全的要求。我国也出台了功能安全相应的标准 G/T 20438[9]和 GB/T 34040[10]。为了解决功能安全相关的问题, 各大自控公司和相关组织提出了各自现场总线上的功能安全通信协议, 例如西门子推出的 PROFIsafe[11]受限于 PROFInet 和 PROFIbus, 倍福推出的基于 EtherCAT 的故障安全 (FsoE[12], failsafeoverEtherCAT) 受限于 EtherCAT, 都受制于各自的现场总线, 普遍缺少通用性[13]。为此, EPSG 将已达到 SIL3 等级的功能安全通信协议 openSAFETY[14]进行开源。由于采用“黑色通道”原理, 其可以完全独立于

收稿日期:2024-04-28; **修回日期**:2024-05-09。
基金项目:国家自然科学基金面上项目(61374103)。
作者简介:徐建明(1970-),男,博士,教授。
引用格式:徐建明,周家豪,陈 琳,等. 基于 openSAFETY 的功能安全通信协议研究[J]. 计算机测量与控制,2024,32(10):228-235.

以太网或总线[15]，适用于所有现场总线和工业以太网方案。然而，openSAFETY 目前仍缺少大量的实际应用[16]，理论研究还需要进一步的实验证明，对应的系统功能安全设计缺乏完善，缺少相应的实验去验证功能安全的有效性。

本文以开源实时以太网功能安全协议 openSAFETY 为研究对象，根据“黑色通道”原理选择高实时性的现场总线 POWERLINK[17]作为其底层通信，实现了基于 POWERLINK 的安全节点（SN，safety node），并且使用贝加莱公司的 PLC 和安全控制器作为安全控制管理器（SCM，safety configuration manager）提高该系统的实时性，通过电磁干扰实验[18-19]验证了其功能安全的有效性和必要性。

1　功能安全通信的安全措施

在工业现场中，通信系统经常受到不同因素（如电压、阻抗、噪音、电压、电磁干扰等）的干扰[20-22]。在 IEC 61784-3[23-24]中将这些因素干扰表现为以下传输错误现象：1）丢失报文；2）报文出现重复；3）插入其他报文；4）报文顺序错乱；5）报文中数据被破坏；6）报文出现延迟超时；7）安全报文与非安全报文混淆；8）寻址异常。

为了确保通信系统能够实现安全功能，需要采取合适的安全措施，用以控制数据传输中发生的错误现象[25]。

为了应对传输中可能出现的错误，可以采取以下控制措施：

1）报文序列号：在通信中加入报文序列号，以区分不同报文的发送顺序。

2）时间戳：通过记录发送数据的时间信息，确保接收端在正确的时间段内接收数据。

3）时间期望：接收方检查报文到达的时间间隔，以识别通信故障。

4）身份验证：使用唯一的地址代码验证通信设备的身份。

5）反馈报文：接收方向发送方发送反馈信息，确认数据接收情况。

6）数据完整性校验：利用冗余数据和哈希函数检测传输中的位差错。

7）带交叉校验的冗余：通过在不同通道上发送相同或不同的数据并在接收端比对来检测传输错误。

8）数据一致性校验相异性：在同一总线上传输安全和非安全数据时，采用不同的校验方法以确保安全功能不受非安全数据影响。

这些安全措施与各种传输错误密切相关，每种措施都可用于检测一种或多种传输错误。在功能安全通信系统中，为了检测所有可能的传输错误，针对每一种错误至少需要采用一种相应的安全措施或其组合。

openSAFETY 是一个具有里程碑意义的开源功能安全协议[26]，它是世界上首个达到 IEC 61508 功能安全标准的安全完整性等级 SIL3 的协议，由于“黑色通道“原理，openSAFETY 完全独立于现场总线协议，因此原则上适用于所有工业以太网以及现场总线。其设计体系允许标准通信数据和安全通信数据在同一个物理网络中传输，这为工业控制系统的安全性提供了更高的保障。

对于上文提到的工业现场可能出现的通信错误，openSAFETY 提供的安全机制如表 1 所示。

表 1　openSAFETY 安全机制

	时间戳	实时监控	识别码	CRC 校验	交叉检测
重发	√				
丢失		√			
插入			√		
乱序	√				
延迟	√	√			
失真				√	√

在 openSAFETY 通信中，数据帧包含两个字节的时间戳，分别位于连续时间（CT，consecutive time）的子帧 1 和子帧 2 中。这个时间戳标识了数据包的发送时间，接收端通过检查这个时间戳可以验证数据的时效性，从而避免数据帧的重发、乱序和延迟。

openSAFETY 中采用了看门狗模式（watchdog）的实时监控机制。SCM 会定时向 SN 发送监控数据帧，如果处于工作状态的 SN 在设定的超时保护时间内没有收到监控数据帧，那么 SN 会停止工作并进入安全模式。如果 SCM 没有收到 SN 的响应数据帧，SCM 会将 SN 判定为安全失效状态。通过连续实时的监控机制，安全域中的 SCM 可以防止由于数据延迟和丢失而引起的通信错误。

openSAFETY 中有着对数据帧完善的识别机制。帧的识别码（ID，frame identification）字段和部分数据字节（DB，data byte）字段准确标识了各类数据帧类型和报文类型，时间请求区别码（TR，time request distinctive number）字段标识了时间同步服务中各帧的具体排序编号。此外，子帧 2 的数据在编码时异或了安全域码（SDN，safety domain number）和唯一设备码（UDID，unique device identification）编号。安全域中的 SN 可以通过 UDID 区分出不同设备的数据帧，防止其它设备数据插入本设备数据而造成的通信错误。

openSAFETY 的安全数据帧被包含在负载数据（payload）中。每个数据帧由两个子帧组成，这两个子帧包含相同备份的地址和其他字段，以及负载数据。在接收数据时，SN 通过比较两个子帧的数据来确保安全数据的完整性。

每个 openSAFETY 子帧都配备有循环冗余校验（CRC，cyclic redundancy check）码。这个 CRC 码会根据预先确定的海明距进行安全校验，以有效地保护安全数据免受错误影响。

2　功能安全通信平台硬件设计

本文使用 openPOWERLINK 协议栈和 openSAFETY 协议栈搭建 SN。openPOWERLINK 是一个开源的工业以太

网协议栈，分为内核层和用户层，实现了 POWERLINK 协议。本文采用分离用户层和内核层的方式实现 POWERLINK 协议，其中用户层包含 openPOWERLINK 的应用层和应用库，内核层中包含驱动层和驱动库。

2.1 PCP-AP 架构设计

本平台依据 openPOWERLINK 用户层和内核层分离的方式设计了 PCP-AP 架构[27]，POWERLINK 通信处理器端（PCP，POWERLINKcomunicationprocessor）中运行协议栈的内核层，应用处理器端（AP，application processor）实现协议栈中的用户层。采用 PCP-AP 架构将内核层与用户层分离的方式更便于单独移植和调试两部分。由于 openSAFETY 采用了与 POWERLINK 相同的 CANopen 应用层协议，便于在 openPOWERLINK 用户层中移植并实现 openSAFETY 协议，从而实现了基于 POWERLINK 的 openSAFETY 功能安全通信协议。

PCP 端选用 FPGA 实现 POWERLINK 协议内核层，AP 端选用 MCU 实现 POWRLINK 用户层并在其中移植 openSAFETY 协议。PCP 端与 AP 端之间通过串行外设接口（SPI，serial peripheral interface）通信。

本文 PCP 端选用 FPGA 实现有以下几点优势：

1）FPGA 可以通过硬件描述语言节省多种硬件资源，简化平台的硬件结构。

2）FPGA 中的硬件加速功能可以加速实现 POWERLINK 协议通信传输中的自动回复。

3）FPGA 具备高性能数据运算处理能力，可在网络中及时地处理各个节点中的同步信号，实现低延迟、低抖动的网络同步，提升网络通信效率。

本文 AP 端选用 MCU 实现有以下几点优势：

1）只要 FLASH 大小满足要求，MCU 可以以尽量低的成本实现 AP 端，这在冗余方案中效果更为明显。

2）MCU 体积小，结构简单，集成度高，功耗低。

3）MCU 具有较强的处理能力，在一个芯片中可以完成多种复杂任务，完全能够满足 AP 端的需求。

PCP 端向 AP 端提供一个通向以太网的接口，解析从以太网中接收的 POWERLINK 数据帧，将负载数据中的安全数据帧通过 SPI 接口发送给 AP 端，将从 AP 端接收的数据打包成 POWERLINK 数据帧发送到以太网中。AP 端提供接口与用户进行交互。PCP 端为用户数据提供高速稳定的以太网通信接口，AP 端为用户数据提供安全功能。

PCP-AP 架构的硬件设计如图 1 所示。

图 1 中 PCP 端中的 FPGA 选用 Altera 公司的 CycloneIV 系列芯片。通过超高速集成电路硬件描述语言（VHDL，very-high-speed integrated circuit hardware description language）实现了 PCP、PLL 锁相环、openMAC 以太网控制器、SRAM 控制器、EPCS 以及 POWERLINK 主机接口。openMAC 控制 PHY 芯片进行高速以太网数据传输。node_switch 通过拨码开关的方式为该节点设置节点号。POWERLINK 主机接口的具体实现在下一节中详细阐述。

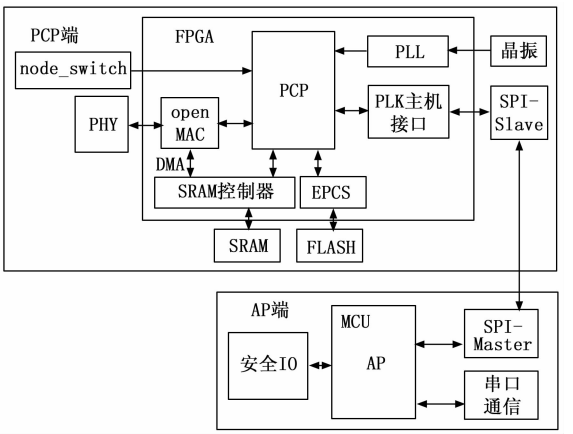

图 1 PCP-AP 硬件结构

FPGA 由 VHDL 语言描述硬件结构之后，其接口信号线如表 2 所示。

表 2 FPGA 接口信号线

信号	描述	I/O
CLK	时钟信号	输入
PHY 接口	PHY 控制接口	输入输出
EPCS	FLASH 控制接口	输入输出
2MBSRAM	SRAM 控制接口	输入输出
SPI	数据通信接口	输入输出
SYNCIRQ	同步中断信号	输出
NODE_SWITCH	节点拨码开关	输入
LED	信号灯	输出

其中每个信号由多条信号线组成，与外设进行连接，达到控制外设的作用。SPI 与 SYNCIRQ 直接与 AP 端进行连接，分别进行数据的传输和同步中断信号的传输。

AP 端中的 MCU 选用意法半导体公司的 STM32 系列芯片。实现了 SPI 主站与 PCP 端进行数据交互，使用串口通信进行调试。

2.2 POWERLINK 接口 IP 核设计

POWERLINK 接口 IP 核提供了用于交换同步进程和/或异步服务数据的不同组件。它由几个子组件组成，其中一些子组件是互斥的。这些子组件可以分为两类核心。为进程或服务数据提供缓冲内存的组件，以及用于从用户应用程序访问该数据的通信核心。

图 2 是该组件的完整概述。虚线分隔了不能在同一设置中使用的组件。SPI 桥核为应用程序提供串行接口，PAR 核为应用程序提供并行接口。

可以使用可用的 IP 核图形用户界面更改 IP 核的配置。该用户界面实例化子组件并将用户配置转发给该组件。因此，POWERLINK 接口 IP 核只是一个简单的配置核心，它简化了配置，并防止用户创建错误的设置。

POWERLINK 接口 IP 核由以下子组件组成：

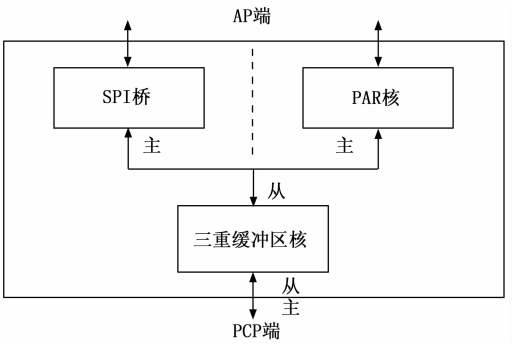

图 2　POWERLINK 接口 IP 核

1）三重缓冲区：为内核提供缓冲存储器。

三重缓冲区核管理 PCP 和用户应用程序之间的缓冲数据传输。它能够实例化多达 32 个缓冲区，如图 3 所示，每个缓冲区可以是生产缓冲区或消费缓冲区。

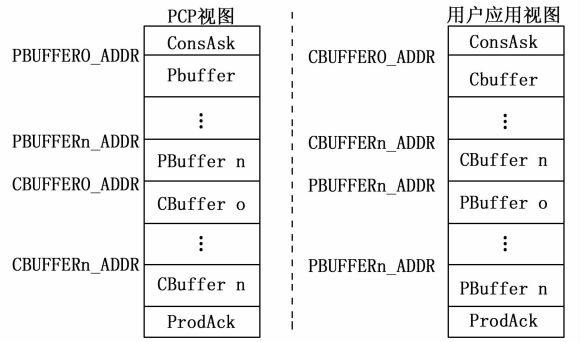

图 3　三重缓冲区

缓冲区的安排方式是，消耗缓冲区（用户应用程序端视图）总是列在内存中的第一个。这允许在连续流中并发访问所有生产和消费缓冲区，通过串行总线接口简化了访问。三缓冲内核本身只提供了一组固定大小的缓冲内存。每个缓冲区内部的详细内存布局不是由 IP 核定义的，而是由使用的软件及其模块提供的。

所有缓冲区的寻址都是连续的，每个缓冲区的偏移量和大小都通过首部（tbuf-cfg. h）转发到用户应用程序。

2）SPI 桥接：为存储器提供串行接口。

这个四线串行接口提供了一个从用户应用程序到内部三重缓冲区的轻量级通信通道。SPI 组件由两个组件组成，第一个组件处理 SPI 从核心功能，第二个组件实现 SPI 协议，如图 4 所示。

核心子组件将输入信号同步到本地时钟，向 SPI 移位寄存器读取/写入数据，并将数据转发到协议组件。协议组件实现了对外部缓冲区的全双工流访问，其中不需要传输额外的命令。

在流式访问时，基本的通信周期从其第一个消费缓冲区的低地址开始，并将数据作为流转发给核心组件。与此同时，它从核心组件读取到达的数据，并将其写入第一个产生缓冲区。因此通信始终是全双工的，在两个流都通过接口传输之前不应该中断。

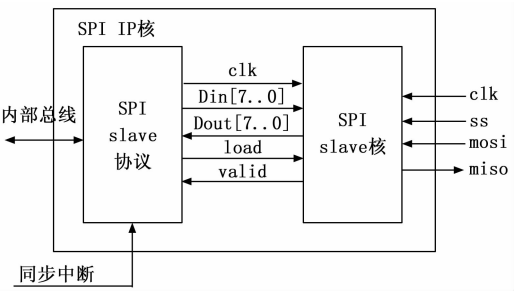

图 4　SPI 桥接组件的内部结构

SS 信号线为 SPI 通信中的片选信号线，如果 SS 信号被重新确认，那么产生和消耗传输都将重新开始。因此，SS 信号需要被激活，直到整个传输完成。

通过该 SPI 接口传输的数据量受到流协议的限制。数据的大小取决于主和从能够处理的最大 SPI 时钟频率。目前 SPI 桥 IP 核能够处理 25 MHz 的最高频率。此外，两次 SPI 访问之间的时间尽可能短也很重要。因此，建议使用具有直接内存访问的 SPI 主控机。这样可以快速读取和写入本地内存，并减少数据传输期间两个字节之间的差距。

3　功能安全通信平台软件设计

在 PCP-AP 架构中，POWERLINK 协议栈与 openSAFETY 协议栈分别运行在 PCP 端的软核处理器以及 AP 端的 MCU 中，如图 5 所示。

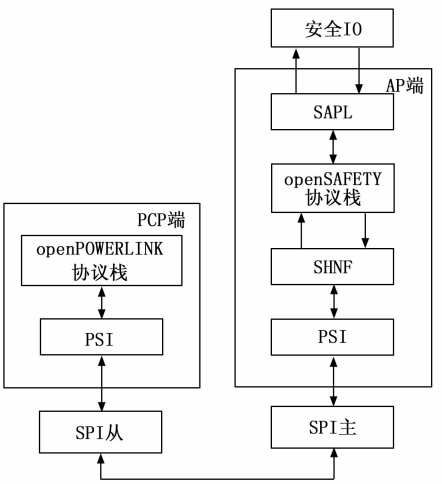

图 5　PCP-AP 软件结构

图 5 POWELRINK 精简接口（PSI，POWERLINK slim interface）模块调用 openPOWERLINK 开源代码中的 POWERLINK 接口库文件，为 POWERLINK 协议栈提供数据传输的接口。PSI 模块为 POWERLINK 协议栈提供了通信接口。安全硬件近固件管理模块（SHNF，safety hardware near firmware managing module）模块为 openSAFETY 协议栈提供了通往底层 PSI 模块的接口。安全应用管理模块（SAPL，safe application managing module）模块提供了用户与 openSAFETY 协议栈之间的接口，用户应用程序提供具有安全功能的 IO 口。

3.1 PSI 模块设计

为了简化用户应用程序的接口，POWERLINK 提供了接口库。为了更加灵活使用 POWERLINK 接口，这个库被分为了几个模块。每个模块都分配了一个三缓冲区。

库的全局配置使用了头文件 triplebuffer. h。该 header 由 tTbufNumLayout 类型组成，如表 3 所示。

表 3 三缓冲区 ID 表

tTbufNumLayout	ID	定义
kTbufAckRegisterCons	0x00	消费者确认寄存器
kTbufNumStatusOut	0x01	状态输出三缓冲区
kTbufNumRpdoImage	0x02	RPDO 三缓冲区映射
kTbufNumSsdoReceive0	0x03	SSDO0 接收缓冲区
kTbufNumStatusIn	0x04	状态输入三缓冲区
kTbufNumTpdoImage	0x05	TPDO 三缓冲区映射
kTbufNumSsdoTransmit0	0x06	SSDO0 输出缓冲区
kTbufNumLogbook0	0x07	日志 0 缓冲区
kTbufAckRegisterProd	0x08	生产者确认缓冲区
kTbufCount	0x09	三缓冲区计数

该类型为每个缓冲区分配一个软件模块。用户需要修改这个类型，以改变缓冲区的含义。该类型还包括第一个索引的消费者确认寄存器（kTbufAckRegisterCons）和最后一个索引的生产者确认寄存器（kTbufAckRegisterProd）。如果向内核添加一个 buffer 实例，那么缓冲区的计数（kTbufCount）也需要调整为 tTbufNumLayout 类型。

PSI 模块由配置通道模块、内部模块、流模块、过程数据对象（PDO，process data object）模块、安全服务数据对象（SSDO，safety service data object）模块、状态模块以及日志模块组成。每个模块由单独的 C 文件实现。

其中配置通道模块为 PCP-AP 架构配置通信的通道。该模块将来自 PCP 的对象数据经由 OCC 转发到 AP，将来自 AP 的对象数据经由 ICC 转发到 PCP，如图 6 所示。

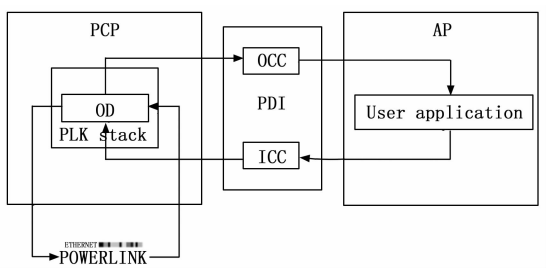

图 6 配置通道

图 6 中，虚线表示服务数据对象（SDO，service data object）通信，实线表示内部通信环。配置通道模块提供了对 POWERLINK 栈的对象字典的几个指定对象的访问。通道本身是通过将内部 PCP /应用程序通信与 POWERLINK SDO 传输分离来实现的。这使得管理节点（MN，manage node）只更新 PCP 上的本地对象字典（OD，object dictionary）。为了获取和设置新数据，本地应用程序使用内部通信循环轮询 PCP 对象字典。内部通信循环中的传输是通过处理预定义的对象列表来完成的。该列表循环交换，最终在应用程序中为 PCP 对象字典提供一致的视图。

当对象通过 SDO 进行外部更新时，此模块实际上并不转发事件。在新数据到达应用程序的对象列表的本地副本之前，可能需要几个周期。因此，用户只能使用相应的 cc _ readObject 函数轮询本地对象列表以获取新信息。

如果需要更新 PCP 的对象字典中的值，可以使用 cc _ writeObject（）函数。请考虑此函数仅更新 PCP 的本地 OD，而没有建立到远程位置的 SDO 传输。

3.2 SHNF 模块设计

SHNF 模块支持 openSAFETY 帧的发送和接收。并在该模块内对帧 CRC 进行了计算。

SHNF 中还包含连续时间模块、硬件近固件（HNF，hardware near firmware）模块和 SHNF 传输模块。其中连续时间模块为安全功能提供连续的时基。HNF 模块与 SHNF 模块提供接口将数据从三缓冲区中提取出来并传输至 openSAFETY 协议栈中。以 SSDO 数据传输为例，其实现如图 7 所示。

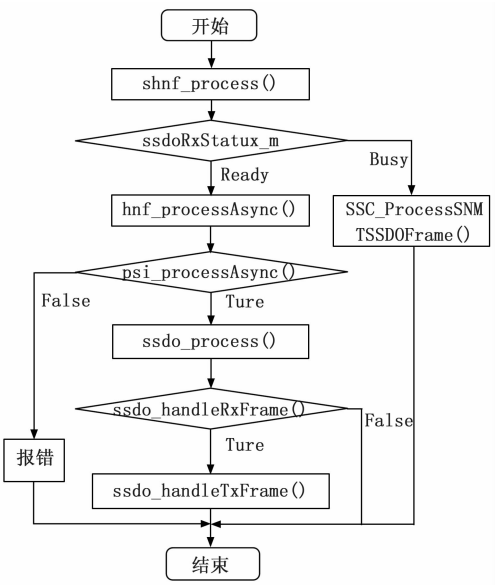

图 7 SSDO 处理流程图

SSDO 处理由多个模块协同工作实现，其中函数名的前部分为该函数的所属模块。当 AP 端的三重缓冲区更新后，PCP 端向 AP 端发送同步中断，shnf _ process（）作为回调函数在接收到同步中断后运行。

在 shnf _ process（）中首先检查 SSDO 接收通道的状态，通过判断全局变量 ssdoRxStatux _ m 是否为 Ready 状态来进行下一步，若为 Ready 则调用 HNF 模块中的 hnf _ processAsync（），此函数名中的 Async 代表此函数处理异步数据，若为 Busy 则调用 openSAFETY 协议栈的接口函数 SSC _ ProcessSNMTSSDOFrame（）并填入空的参数表示无动作发生。

在 hnf _ processAsync（）中调用 psi _ processAsync（）为异步数据传输设置通道并加锁，判断返回为 True 后调用 ssdo _ process（）开始处理 SSDO 数据。若返回 False 则报错并退出。

ssdo _ process（）中先调用 ssdo _ handleRxFrame（）处理接收数据帧，成功则调用 ssdo _ handleTxFrame（）处理发送数据帧，若失败则跳过处理发送数据帧。

在 ssdo _ handleRxFrame（）中通过指针将接收到的数据传送给 SSC _ ProcessSNMTSSDOFrame（），至此，接收数据帧成功将数据从三重缓冲区传输至 openSAFETY 协议栈中。

ssdo _ handleTxFrame（）为发送缓冲区解锁表示 AP 端可以将数据打包发送并增加本地的序列号。

3.3　SAPL 模块设计

SAPL 模块管理固件部分附近的应用程序。它的主要目的是以一种尽可能少消耗时间的方式触发所有 SAPL 子模块。因此，sapl _ process（）函数实现了一个任务调度器，该调度器能够处理 SAPL 所需的任何子任务。该调度器如图 8 所示。

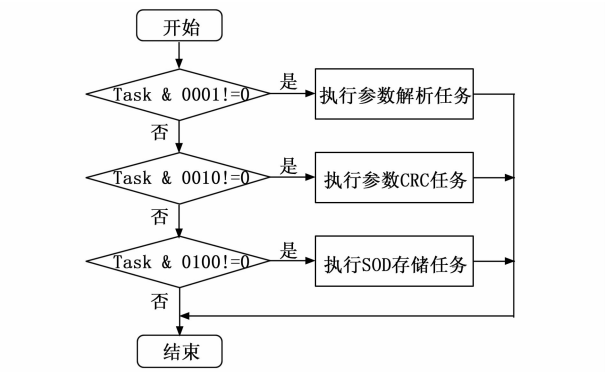

图 8　SAPL 任务调度器

Task 是一个四位二进制数表示正在执行的任务，通过 Task 与子任务对应的掩码按位与是否为 0 判断是否要进行此任务。其中参数解析任务的优先级最高。

参数解析任务将参数流从对象 0x10A1 转发到对象字典中，并对该流进行检查；参数 CRC 任务遍历整个安全对象字典（SOD，safety object direction）并计算所有 CRC 相关对象的校验和；SOD 存储任务存储整个参数设置到非易失性存储器，使 SN 启动时快速启动。

所有子任务都被编写成小块执行的方式，openSAFETY 协议栈可以在每个小块之间进行一些计算。

SAPL 中还包含用户应用模块，该模块实现了用户应用程序的通用部分。这个应用程序用有意义的数据读写 SPDO，然后将这些数据传输到 SCM。该应用程序实现了一个 GPIO 处理示例。

该模块直接与 SN 的 SOD 通信，直接通过读写 SOD 来实现安全 IO。

3.4　SN 启动流程

各模块实现之后可以与 SCM 进行通信，SN 的运行启动流程如图 9 所示。

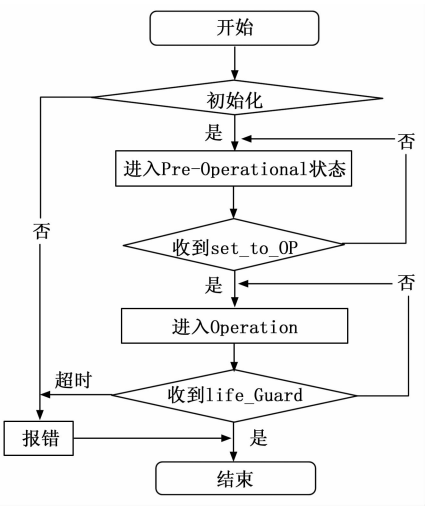

图 9　SN 启动流程图

在系统上电后，SN 自启动初始化程序，进行对象字典等参数的配置。之后，SN 就进入 Pre _ Operational 状态。

Pre _ Operational 状态的节点能够处理来自 SCM 的 SNMT 和 SSDO 帧，从 SCM 下载网络配置参数，包括 SCM 的 UDID、自身的地址、SOD 接入指令等。此时，运行在 SN 中的应用数据都设置为安全状态。同时，SN 也向 SCM 报告自己的运行状态，并等待 SNMT _ SN _ set _ to _ OP 指令。收到指令后，SN 还会进行一轮包括参数校验和时间戳在内的本地自检。如自检不通过，SN 会通知 SCM 要求重新配置参数。当自检通过后，SN 从 Pre _ Operational 切换为 Operational，节点就能够开始周期性地收发 SPDO 数据了。

为了保持在 Operational 状态，节点必须周期性地从 SCM 接收生命周期信号（Life Guarding Sign），即 SNMT _ SCM _ guard _ SN 帧的数据。若 SN 在等待生命周期信号的过程中超时，或者收到的 SNMT _ SN _ set _ to _ PRE _ OP 指令，或在运行过程中产生任务错误指令，都会使其切换回 Pre _ Operational，等待 SCM 的进一步校验和指令。

4　电磁干扰实验

数据传输错误中两大错误源头为网关转发和电磁干扰[28-30]。在工业场景中，被控制的设备和被测量的信号通常分布在不同的位置，而且与控制站之间的距离可能很长。因此，信号线和控制线往往会长距离传输。此外，工业现场通常存在大量的强电设备，它们的启动和运行可能会对测量和控制系统产生严重的干扰影响。

根据实践经验，抗干扰性能是电子测量设备中一个极其关键的问题。电磁干扰可能导致信号线中的电平发生变化，进而导致系统的测量和控制失效，从而降低产品质量，甚至损坏生产设备，引发事故。

而功能安全通信系统可以很好地避免电磁干扰带来的问题。本文设计了一个电磁干扰实验，将安全和非安全通

信平台的信号线置于电磁干扰中，使用 Wireshark 网络检测软件观察电磁干扰对通信的影响，并观察通信平台的现象。

4.1 实验设计

本文选用友晶科技的 DE2-115 教育开发板作为 PCP 端，意法半导体公司的 NUCLEO-F401RE 作为 AP 端，PCP-AP 的架构作为 SN，使用贝加莱公司型号为 X20CP1684 的 PLC 和型号为 X20SL8100 的安全管理控制器作为 SCM，将两者与 PC 机接入同一集线器 HUB 中，并使用串口调试 SN。具有功能安全通信的实验平台如图 10 所示。

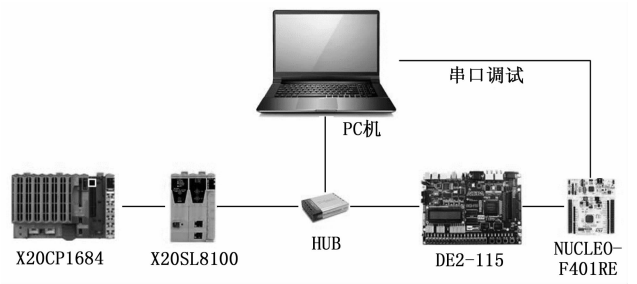

图 10 安全通信平台

将 X20SL1684 与 NUCLEO-F401RE 等安全模块去掉可搭建非安全通信实验平台。

本文选用群脉冲发生器作为电磁干扰发生装置。该设备为三基电子公司的 SKS-0404，可以提供高达 4 500 V 的脉冲试验电压，脉冲频率分为两个档，5 kHz 和 100 kHz，传统上使用 5 kHz 的重复频率测试，然而 100 kHz 更接近于实际情况，本文选择 100 kHz 作为实验的脉冲频率。信号线置于容性耦合夹中。

分别使用非安全通信平台和安全通信平台进行如下实验：

将信号线置于容性耦合夹中，如图 11 所示。

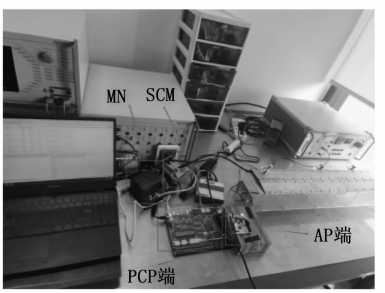

图 11 安全通信平台电磁干扰实验

将重复频率挡位调到 F3（100 kHz）。转动设置电压旋钮从 500 V 开始依次加 500 V，一直加到 4 000 V，每个挡位测完取负再测一遍，每次实验持续 60 s。

4.2 实验结果及分析

非安全通信平台：从报文中几乎看不到任何现象，一直加到 4 000 V 之后会出现断连的情况，一旦断连后需要手动开关电源重新启动。

安全通信平台：在 1 500 V 左右的时候开始出现安全连接断开的情况，断开后主站立马发送 SNMT 请求帧，并开始 SN 的启动流程。实验报文如图 12 所示。

183227 62.270743	DataLogi_08:93:ac	EPLv2_PRes	openSAFETY/Powerlink	60 SPDO Data only - 0x002
183230 62.271745	DataLogi_08:93:ac	EPLv2_PRes	openSAFETY/Powerlink	60 SPDO Data only - 0x002
183233 62.272733	DataLogi_08:93:ac	EPLv2_PRes	openSAFETY/Powerlink	60 SPDO Data only - 0x002
183235 62.272733	B&RIndus_42:cc:91	EPLv2_ASnd	openSAFETY/Powerlink	60 SNMT Assign SADR
183237 62.273740	DataLogi_08:93:ac	EPLv2_PRes	openSAFETY/Powerlink	60 SPDO Data only - 0x002
183240 62.274736	DataLogi_08:93:ac	EPLv2_PRes	openSAFETY/Powerlink	60 SPDO Data only - 0x002
183244 62.275738	DataLogi_08:93:ac	EPLv2_PRes	openSAFETY/Powerlink	60 SPDO Data only - 0x002

图 12 1 500 V 实验报文

3 500 V 以上后，群脉冲发生器启动后，全部连接立刻断开，并在电磁干扰结束后自动开启通信，如图 13 所示。

98428 46.717976	DataLogi_08:93:ac	EPLv2_PRes	openSAFETY/Powerlink	60 SPDO Data only - 0x002
98431 46.718980	DataLogi_08:93:ac	EPLv2_PRes	openSAFETY/Powerlink	60 SPDO Data only - 0x002
98434 46.719978	DataLogi_08:93:ac	EPLv2_PRes	openSAFETY/Powerlink	60 SPDO Data only - 0x002
98437 46.720976	DataLogi_08:93:ac	EPLv2_PRes	openSAFETY/Powerlink	60 SPDO Data only - 0x002
98441 107.703271	DataLogi_08:93:ac	EPLv2_PRes	openSAFETY/Powerlink	60 SPDO Data only - 0x002
98444 107.704020	DataLogi_08:93:ac	EPLv2_PRes	openSAFETY/Powerlink	60 SPDO Data only - 0x002
98447 107.705008	DataLogi_08:93:ac	EPLv2_PRes	openSAFETY/Powerlink	60 SPDO Data only - 0x002

图 13 3 500 V 实验报文 1

由报文数据可知，断连前后正好为 60 s 左右，为电磁干扰作用在信号线上的时间，并且在 10 s 后主站开始向从站发送 SNMT 帧请求通信，开始 SN 的启动流程，如图 14 所示。

126899 117.120433	DataLogi_08:93:ac	EPLv2_PRes	openSAFETY/Powerlink	60 SPDO Data only - 0x002
126902 117.121436	DataLogi_08:93:ac	EPLv2_PRes	openSAFETY/Powerlink	60 SPDO Data only - 0x002
126905 117.122420	DataLogi_08:93:ac	EPLv2_PRes	openSAFETY/Powerlink	60 SPDO Data only - 0x002
126907 117.122420	B&RIndus_42:cc:91	EPLv2_ASnd	openSAFETY/Powerlink	60 SNMT Assign SADR
126909 117.123423	DataLogi_08:93:ac	EPLv2_PRes	openSAFETY/Powerlink	60 SPDO Data only - 0x002
126912 117.124426	DataLogi_08:93:ac	EPLv2_PRes	openSAFETY/Powerlink	60 SPDO Data only - 0x002
126916 117.125427	DataLogi_08:93:ac	EPLv2_PRes	openSAFETY/Powerlink	60 SPDO Data only - 0x002

图 14 3 500 V 实验报文 2

由实验报文得电磁干扰实验现象如表 4 所示。

表 4 电磁干扰实验现象

脉冲试验电压/V	非安全通信平台	安全通信平台
500	无响应	无响应
1 000	无响应	无响应
1 500	无响应	安全状态
2 000	无响应	安全状态
2 500	无响应	安全状态
3 000	无响应	安全状态
3 500	无响应	通信断连后重连
4 000	通信断连	通信断连后重连

SN 节点没有在其生命周期时间内收到 SNMT _ SCM _ guard _ SN 帧信号，或者接收到错误信息时，SN 会从 Operational 状态切换回 Pre _ Operational 状态，所有相关的通信参数都会被强制置为 0，即进入“安全状态”。从实验现象来看，在 1 500 V 之后 3 500 V 之前的电磁干扰实验中，SN 都切换到了 Pre _ Operational 状态，由此可以判断 SN 进入了“安全状态”，此时主站 SCM 仍在不停发送安全过程数据对象（SPDO，safety process data object）数据帧，说明主站并不受影响。而 3 500 V 电压之后由于电磁干扰过大，导致主站 SCM 进入停止状态，停止发送 SPDO 数据帧。在电磁干扰停止 10 s 后，SCM 启动自动成功，开始向 SN 发送 SNMT 请求帧请求进入 Operational 模式。

事实证明在 1500 V 之后就会出现错误帧，而非安全通

信平台无法检测出错误仍在不停通信，这就会导致错误的数据被传输。

实验证明了基于 POWERLINK 的功能安全系统的有效性，避免了错误数据的传输，这在实际的工业现场是非常有必要的。

5　结束语

当前工业以太网技术在工业现场应用中面临着功能安全和信息安全的挑战。传统的网络安全技术已无法满足工业以太网快速、稳定、高效的需求。然而诸多厂商和研究所推出的功能安全技术又受到各自通信协议的限制而无法统一开放的解决方案。对此，本文以基于 POWERLINK 的 openSAFETY 功能安全通信协议为研究对象，进行了 PCP-AP 架构和软硬件的设计，搭建了以 PCP-AP 为架构的安全节点，并以贝加莱 PLC 搭建了具有功能安全的通信实验平台，最后通过实验测试和数据分析，测试了该平台的运行性能，验证了功能安全通信协议的可靠性和必要性。

基于 openSAFETY“黑色通道”原理，其可将安全功能置于任意总线上，包括网络总线中，这意味着需要将功能安全与网络安全相结合[31]，这将是更大的挑战。

参考文献：

[1] 刘燕燕，罗　茵. 工业化与信息化融合促进工业经济转型升级研究 [J]. 现代工业经济和信息化，2023，13 (10)：96－98.

[2] 王田苗，陶　永. 我国工业机器人技术现状与产业化发展战略 [J]. 机械工程学报，2014，50 (9)：1－13.

[3] 方正梁. 工业互联网高质量发展开新篇为加快推进新型工业化增添新动能 [N]. 北京：人民邮电，2023－12－28 (001).

[4] 王永华，常　洁，江　豪. 基于 PROFIBUS 的纺织工业网络架构规划 [J]. 郑州轻工业学院学报，2013，28 (2)：31－35.

[5] 杨安义. 核电厂仪控系统功能安全与网络安全 [J]. 核科学与工程，2023，43 (1)：206－212.

[6] 崔景博，肖安洪，何　伟，等. 核电厂安全级控制系统软件关键性分析 [J]. 核电子学与探测技术，2021，41 (1)：12－17.

[7] 国际电工委员会. 电气/电子/可编程电子安全相关系统的功能安全，第 4 部分：定义和缩略语：IEC 61508-4-2010 [S]. 日内瓦：国际电工委员会，2000.

[8] 国际电工委员会. 电气/电子/可编程电子安全相关系统的功能安全，第 1 部分：一般要求：IEC 61508-1-2010 [S]. 日内瓦：国际电工委员会，2000.

[9] 中华人民共和国国家质量监督检验检疫总局；中国国家标准化管理委员会. 电气/电子/可编程电子安全相关系统的功能安全，功能安全概念及 GB/T 20438 系列概况：GB/Z 29638-2013 [S]. 北京：中国标准出版社，2013.

[10] 中华人民共和国国家质量监督检验检疫总局；中国国家标准化管理委员会. 工业通信网络，功能安全现场总线行规，通用规则和行规定义：GB/T 34040-2017 [S]. 北京：中国标准出版社，2017.

[11] 中华人民共和国国家质量监督检验检疫总局；中国国家标准化管理委员会. 基于 PROFIBUS DP 和 PROFI-NET IO 的功能安全通信行规-PROFIsafe：GB/T 20830－2015 [S]. 北京：中国标准出版社，2015.

[12] EtherCAT Technology Group. ETG. 5100 safety over EtherCAT specification [S]. Germany：EtherCAT Techno-logy Group，2011.

[13] 魏昊旻，王文海. 基于 EPL 的 openSAFETY 平台构架设计 [J]. 计算机测量与控制，2015，23 (3)：889－892.

[14] 贝加莱公司. 通过 openSAFETY 构建系统网络更加安全 [J]. 自动化博览，2013 (5)：78.

[15] 赵　阳，王　坚，薛正卿. openSafety 技术在工业控制网络中的应用研究 [J]. 仪表技术，2011 (2)：39－41.

[16] 宋华振. 智能制造的基础网络平台 [J]. 自动化博览，2017，34 (z1)：58－61.

[17] SOURY A，CHARFI M，GENONCD，et al. Performance analysis of ethernet powerlink protocol：application to a new lift system generation [C] //Luxembourg：IEEE，2015：1－6.

[18] 黄　宇，赵　杰，陈建国. 复杂电磁环境下电子通信信号抗干扰方法 [J]. 计算机仿真，2023，40 (8)：159－163.

[19] 朱俊颖. 开关电源 PCB 电磁干扰的仿真与实验分析 [D]. 成都：电子科技大学，2020.

[20] 国际电工委员会. 工业通信网络协议集，第 3-3 部分：现场总线功能安全，CPF 3 的附加规范：IEC 61784-3-3-2012 [S]. 日内瓦：国际电工委员会，2012.

[21] 国际电工委员会. 工业通信网络，现场总线规范，第 1 部分：对 IEC 61158 和 IEC 61784 系列的总则和指导：IEC 61158-1-2018 [S]. 日内瓦：国际电工委员会，2018.

[22] 国际标准化组织. 道路车辆，互联网协议的诊断通信 (DoIP)，以 IEEE 802. 3 标准为基础的有线车辆接口：ISO 13400-3-2012 [S]. 日内瓦：国际标准化组织，2012.

[23] 史哲烽，陈小华. 符合 IEC61784-3 标准的功能安全通信协议实现及对标准的思考 [J]. 集成电路应用，2019，36 (1)：5－9.

[24] 中国国家标准化管理委员会. 现场设备工具 (FDT) 接口规范，第 5232 部分：通用语言基础结构的通信实现 IEC 61784 CP3/4，CP3/5 和 CP3/6：GB/T 29618. 5232－2018 [S]. 北京：中国标准出版社，2018.

[25] 肖家麒. 功能安全通信中的安全特征 [J]. 中国仪器仪表，2009 (5)：56－59.

[26] AL FRESHER. New OpenSAFETY Protocol [J]. Design News，2010，65 (8)：34.

[27] 魏昊旻. 基于 EPL 的安全工业以太网协议研究及其应用改进 [D]. 杭州：浙江大学，2015.

[28] 郭军华，王维俊，张　敏，等. 小议电磁干扰 [C] //重庆：重庆市电机工程学会，2006：149－152.

[29] 张　琦，白欣鹏，李　凌. 飞机的电磁干扰与抑制策略分析 [J]. 集成电路应用，2023，40 (1)：234－235.

[30] ARMSTRONG K. Techniques and measures to manage functional safety and other risks with regard to electromagnetic disturbances [C] //Luxembourg：IEEE，2018：1－5.

[31] 张刻铭. 大数据背景下网络安全问题及其对策分析 [J]. 网络安全技术与应用，2023 (3)：55－57.