



(12) 实用新型专利

(10) 授权公告号 CN 218183360 U

(45) 授权公告日 2022. 12. 30

(21) 申请号 202221114549.X

(22) 申请日 2022.05.07

(73) 专利权人 广西电网有限责任公司

地址 530000 广西壮族自治区南宁市兴宁区民主路6号

(72) 发明人 田君杨 李海勇 巫聪云 蒋连钊

沈梓正 刘斌 黄超 徐晓峰

杨彦 韩冰 黄鹏飞

(74) 专利代理机构 武汉红观专利代理事务所

(普通合伙) 42247

专利代理师 王昌亮

(51) Int. Cl.

H04L 9/40 (2022.01)

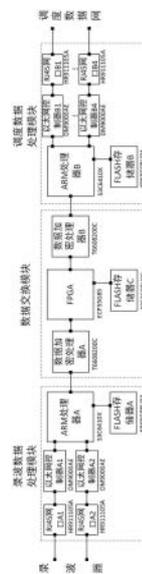
权利要求书2页 说明书7页 附图3页

(54) 实用新型名称

一种录波数据安全交换电路

(57) 摘要

本实用新型提供了一种录波数据安全交换电路,所述录波数据安全交换电路包括:录波数据处理模块、数据交换模块以及调度数据处理模块。本实用新型的录波数据安全交换电路,能够将录波器和调度数据网进行物理隔离,在隔绝安全隐患的同时完成录波数据的安全交换,在传统网闸GAP技术上进行了改良,同时具备物理隔离、高速传输、实时交互和数据过滤等功能,实现变电站录波器的安全隔离和数据传输。



1. 一种录波数据安全交换电路,其特征在于,所述录波数据安全交换电路包括:
录波数据处理模块、数据交换模块以及调度数据处理模块;
所述录波数据处理模块的一端与录波器电性连接,另一端与所述数据交换模块电性连接;
所述数据交换模块的一端与所述录波数据处理模块电性连接,另一端与所述调度数据处理模块电性连接;
所述调度数据处理模块的一端与所述数据交换模块电性连接,另一端与调度数据网电性连接。
2. 根据权利要求1所述的录波数据安全交换电路,其特征在于,所述录波数据处理模块,具体包括:
RJ45网口A、以太网控制器A以及ARM处理器A;
所述RJ45网口A的一端与所述录波器电性连接,另一端与所述以太网控制器A电性连接;
所述以太网控制器A的一端与所述RJ45网口A电性连接,另一端与所述ARM处理器A电性连接;
所述ARM处理器A的一端与所述以太网控制器A电性连接,另一端与所述数据交换模块电性连接。
3. 根据权利要求2所述的录波数据安全交换电路,其特征在于,所述RJ45网口A、以太网控制器A,包括2组,具体包括:
RJ45网口A1、以太网控制器A1为一组,RJ45网口A2、以太网控制器A2为一组,分别与所述录波器、ARM处理器A对应电性连接。
4. 根据权利要求2或3所述的录波数据安全交换电路,其特征在于,所述录波数据处理模块,还包括FLASH存储器A,所述FLASH存储器A与所述ARM处理器A电性连接。
5. 根据权利要求4所述的录波数据安全交换电路,其特征在于,所述数据交换模块,具体包括:
数据加密处理器A、FPGA以及数据加密处理器B;
所述数据加密处理器A的一端与所述ARM处理器A电性连接,另一端与所述FPGA电性连接;
所述FPGA的一端与数据加密处理器A电性连接,另一端与数据加密处理器B电性连接;
所述数据加密处理器B的一端与所述FPGA电性连接,另一端与所述调度数据处理模块电性连接。
6. 根据权利要求5所述的录波数据安全交换电路,其特征在于,所述数据交换模块,还包括FLASH存储器C,所述FLASH存储器C与所述FPGA电性连接。
7. 根据权利要求6所述的录波数据安全交换电路,其特征在于,所述调度数据处理模块,具体包括:
ARM处理器B、以太网控制器B以及RJ45网口B;
所述ARM处理器B的一端与所述数据加密处理器B电性连接,另一端与所述以太网控制器B电性连接;
所述以太网控制器B的一端与所述ARM处理器B电性连接,另一端与所述RJ45网口B电性

连接；

所述RJ45网口B的一端与所述以太网控制器B电性连接,另一端与所述调度数据网电性连接。

8.根据权利要求7所述的录波数据安全交换电路,其特征在于,所述以太网控制器B、RJ45网口B,包括4组,具体包括:

以太网控制器B1、RJ45网口B1为一组,以太网控制器B2、RJ45网口B2为一组,以太网控制器B3、RJ45网口B3为一组,以太网控制器B4、RJ45网口B4为一组,分别与所述ARM处理器B、调度数据网对应电性连接。

9.根据权利要求7或8所述的录波数据安全交换电路,其特征在于,所述调度数据处理模块,还包括FLASH存储器B,所述FLASH存储器B与所述ARM处理器B电性连接。

一种录波数据安全交换电路

技术领域

[0001] 本实用新型涉及数据传输技术领域,具体而言,涉及一种录波数据安全交换电路。

背景技术

[0002] 在电力系统继电保护领域中,录波数据是电网运行监视与事故分析不可缺少的信息支撑。大多数录波器负责对外通信的管理单元仍采用非嵌入式操作系统,易感染病毒或遭受网络攻击。录波器在变电站内完成组网后直接接入调度数据网,当某一台录波器存在网络信息安全隐患时,将会直接威胁到调度数据网及其内大量联网设备的安全。

[0003] 变电站内现有的主要网络信息安全防护设备有以下几种:

[0004] (1) 网络防火墙:分软件防火墙和硬件防火墙,软件防火墙安装在录波器的操作系统内,硬件防火墙安装在变电站内部网络与调度数据网之间。网络防火墙通过对IP、端口、协议等进行数据包过滤,防止网络外部一些陌生设备的入侵,但对网络内部尤其是本身有业务往来的设备很难防范;

[0005] (2) 纵向加密装置:对数据进行加密,防止数据在变电站到调度之间传输的过程中被截取导致信息泄露,不具备网络入侵防护作用;

[0006] (3) 态势感知装置:主要对网络攻击或疑似网络攻击的风险进行监测和告警,属于隐患检测设备,并不能从源头上杜绝隐患的发生。

[0007] 以上设备都处于网络层,不能将录波器与调度数据网从物理层完全隔离,只要存在网络连接,就仍有攻击和被攻击的风险,目前能实现网络物理隔离功能的设备有两种:

[0008] (1) 隔离卡:当一台电脑需要同时连接内网和外网时,隔离卡能够将一台电脑虚拟分割成分别连接内网和外网的两台电脑使用。隔离卡具备连接主板网卡、内网和外网的3个独立网口,以及连接主板SATA接口、内网硬盘和外网硬盘的3个SATA接口,相当于不同的网络、硬盘和操作系统共用一套主板、网卡,实现内、外网的物理分离。由于隔离卡的内、外网硬盘之间数据不能互通,且每次切换时需要手动开关控制并重启或休眠电脑,所以不适合录波器无人值守和数据上送的需求。

[0009] (2) 安全隔离网闸(GAP):网闸是一种独立安装的网络隔离设备,采用双服务主机+隔离硬件的架构,两套服务主机分别连接内网和外网提供数据服务,控制主机则使用私有协议实现两侧服务主机间的数据拷贝。不需要手动切换和重启,即可完成内、外网的数据交换。但是市面上现有的网闸产品由于受数据传输芯片性能的约束,对内、外两端的数据包大小进行了限制,这就要求数据发送端设备对数据包按限定大小进行拆包。而在电力系统中的录波器属于运行设备,难以对已有通信服务程序进行重新设计;另一方面录波器在电网故障时数据量较大,而网闸设备的数据传输效率较低,会延迟录波数据到达录波主站端的时间。

[0010] 以上两种技术方案主要应用在有安全等级差异的两个网络的边界,而录波器与调度主站同处调度数据网,从根本上讲是同等级、同网络的设备,如果使用传统网闸设备,则存在成本高、效率低、适用性不足等问题。

实用新型内容

[0011] 本实用新型解决的问题是：传统网闸设备数据传输效率较低，会延迟录波数据到达录波主站端的时间。

[0012] 为解决上述问题，本实用新型提供一种录波数据安全交换电路，其中，所述录波数据安全交换电路包括：

[0013] 录波数据处理模块、数据交换模块以及调度数据处理模块；

[0014] 所述录波数据处理模块的一端与录波器电性连接，另一端与所述数据交换模块电性连接；

[0015] 所述数据交换模块的一端与所述录波数据处理模块电性连接，另一端与所述调度数据处理模块电性连接；

[0016] 所述调度数据处理模块的一端与所述数据交换模块电性连接，另一端与调度数据网电性连接。

[0017] 优选地，所述录波数据处理模块，具体包括：

[0018] RJ45网口A、以太网控制器A以及ARM处理器A；

[0019] 所述RJ45网口A的一端与所述录波器电性连接，另一端与所述以太网控制器A电性连接；

[0020] 所述以太网控制器A的一端与所述RJ45网口A电性连接，另一端与所述ARM处理器A电性连接；

[0021] 所述ARM处理器A的一端与所述以太网控制器A电性连接，另一端与所述数据交换模块电性连接。

[0022] 优选地，所述RJ45网口A、以太网控制器A，包括2组，具体包括：

[0023] RJ45网口A1、以太网控制器A1为一组，RJ45网口A2、以太网控制器A2 为一组，分别与所述录波器、ARM处理器A对应电性连接。

[0024] 优选地，所述录波数据处理模块，还包括FLASH存储器A，所述FLASH 存储器A与所述ARM处理器A电性连接。

[0025] 优选地，所述数据交换模块，具体包括：

[0026] 数据加密处理器A、FPGA以及数据加密处理器B；

[0027] 所述数据加密处理器A的一端与所述ARM处理器A电性连接，另一端与所述FPGA电性连接；

[0028] 所述FPGA的一端与数据加密处理器A电性连接，另一端与数据加密处理器B电性连接；

[0029] 所述数据加密处理器B的一端与所述FPGA电性连接，另一端与所述调度数据处理模块电性连接。

[0030] 优选地，所述数据交换模块，还包括FLASH存储器C，所述FLASH存储器C与所述FPGA电性连接。

[0031] 优选地，所述调度数据处理模块，具体包括：

[0032] ARM处理器B、以太网控制器B以及RJ45网口B；

[0033] 所述ARM处理器B的一端与所述数据加密处理器B电性连接，另一端与所述以太网控制器B电性连接；

[0034] 所述以太网控制器B的一端与所述ARM处理器B电性连接,另一端与所述RJ45网口B电性连接;

[0035] 所述RJ45网口B的一端与所述以太网控制器B电性连接,另一端与所述调度数据网电性连接。

[0036] 优选地,所述以太网控制器B、RJ45网口B,包括4组,具体包括:

[0037] 以太网控制器B1、RJ45网口B1为一组,以太网控制器B2、RJ45网口B2 为一组,以太网控制器B3、RJ45网口B3为一组,以太网控制器B4、RJ45网口B4为一组,分别与所述ARM处理器B、调度数据网对应电性连接。

[0038] 优选地,所述调度数据处理模块,还包括FLASH存储器B,所述FLASH 存储器B与所述ARM处理器B电性连接。

[0039] 相对于现有技术,本实用新型所述的录波数据安全交换电路具有以下有益效果:

[0040] (1) 本实用新型的录波数据安全交换电路,数据交换模块能够将录波器和调度数据网进行物理隔离,在隔绝安全隐患的同时完成录波数据的安全交换,在传统网闸GAP技术上进行了改良,同时具备物理隔离、高速传输、实时交互和数据过滤等功能,实现变电站录波器的安全隔离和数据传输,传统网闸设备的数据传输速率平均在80Mbps,而录波数据安全交换电路的交换速率可达到 480Mbps,实时性更好、效率更高。

[0041] (2) 本实用新型的录波数据安全交换电路,增加了IEC103和IEC61850规约服务,对电力系统已投运的录波器和调度主站有极好的兼容性,增加了录波数据解析和过滤、调度主站指令解析等功能,更适合录波器及其调度主站业务。

[0042] (3) 本实用新型的录波数据安全交换电路,可封装成独立装置,也可封装成录波器板卡,适应不同的变电站运行环境,制造成本更低。

附图说明

[0043] 图1为本实用新型的录波数据安全交换电路结构示意图;

[0044] 图2为本实用新型的录波数据安全交换电路功能模块图;

[0045] 图3为本实用新型的录波数据安全交换电路工作流程图。

具体实施方式

[0046] 为使本实用新型的上述目的、特征和优点能够更为明显易懂,下面结合附图对本实用新型的具体实施例做详细的说明。

[0047] 实施例一

[0048] 提供一种录波数据安全交换电路,如图1所示,其中,所述录波数据安全交换电路包括:

[0049] 录波数据处理模块、数据交换模块以及调度数据处理模块;

[0050] 所述录波数据处理模块的一端与录波器电性连接,另一端与所述数据交换模块电性连接;

[0051] 所述数据交换模块的一端与所述录波数据处理模块电性连接,另一端与所述调度数据处理模块电性连接;

[0052] 所述调度数据处理模块的一端与所述数据交换模块电性连接,另一端与调度数据

网电性连接。

[0053] 录波数据交换电路沿用了GAP技术的经典2+1结构,即内、外网主机+隔离硬件。由于录波器和调度主站同处调度数据网,不存在内、外网的概念,所以电路主要分为以下几个模块:

[0054] 录波数据处理模块:负责与录波器的通信连接和录波数据的过滤,以及IP、端口调试和安全策略配置;

[0055] 数据交换模块:负责录波数据处理模块与调度数据处理模块之间的网络隔离和数据交换;

[0056] 调度数据处理模块:负责与调度主站的通信连接、调度主站指令处理和录波数据上送。

[0057] 其中,所述录波数据处理模块,具体包括;

[0058] RJ45网口A、以太网控制器A以及ARM处理器A;

[0059] 所述RJ45网口A的一端与所述录波器电性连接,另一端与所述以太网控制器A电性连接;

[0060] 所述以太网控制器A的一端与所述RJ45网口A电性连接,另一端与所述 ARM处理器A电性连接;

[0061] 所述ARM处理器A的一端与所述以太网控制器A电性连接,另一端与所述数据交换模块电性连接。

[0062] ARM处理器A,采用ARM11架构的32位微型处理器(型号S3C6410X),采用嵌入式系统,能够有效阻断录波器端非嵌入式操作系统的病毒、漏洞、非法服务等攻击。

[0063] 其中,所述RJ45网口A、以太网控制器A,包括2组,如图1所示,具体包括:

[0064] RJ45网口A1、以太网控制器A1为一组,RJ45网口A2、以太网控制器A2 为一组,分别与所述录波器、ARM处理器A对应电性连接。

[0065] RJ45网口A1~A2,两个独立网口(型号HR911105A),用于与录波器连接的网线接口,一主一备,支持10Mbps/100Mbps带宽自适应;以太网控制器A1~A2,两个独立网卡(型号DM9000AE),用于与录波器通信,一主一备。

[0066] 其中,所述录波数据处理模块,如图1所示,还包括FLASH存储器A,所述FLASH存储器A与所述ARM处理器A电性连接。

[0067] FLASH存储器A,采用NandFlash技术的FLASH芯片(型号K9K8G08U0A),拥有较高的读写、擦除速度,能够有效提高数据传输效率。FLASH存储器A作为ARM处理器A的外部存储元件,负责功能程序的存储和录波数据的暂存。容量选择为8G,其中4G划分为录波数据暂存空间,采用循环覆盖方式存储。

[0068] 其中,所述数据交换模块,如图1所示,具体包括;

[0069] 数据加密处理器A、FPGA以及数据加密处理器B;

[0070] 所述数据加密处理器A的一端与所述ARM处理器A电性连接,另一端与所述FPGA电性连接;

[0071] 所述FPGA的一端与数据加密处理器A电性连接,另一端与数据加密处理器B电性连接;

[0072] 所述数据加密处理器B的一端与所述FPGA电性连接,另一端与所述调度数据处理

模块电性连接。

[0073] 数据加密处理器A~B,采用国产数据加密芯片,集成32位高性能RISC CPU,支持USB3.0、SATA3.0、GMAC等多种超高速接口,集成多种国密算法。具备可靠的数据安全保障和高效的数据传输能力。

[0074] 数据加密处理器A可对录波数据处理模块的数据进行加密,对调度数据处理模块的数据进行解密。数据加密处理器A与ARM处理器A通过USB OTG 2.0接口连接,传输速率最高支持480Mbps。

[0075] 数据加密处理器B可对调度数据处理模块的数据进行加密,对录波数据处理模块的数据进行解密。数据加密处理器B与ARM处理器B通过USB OTG 2.0接口连接,传输速率最高支持480Mbps。

[0076] FPGA,采用大型可编程逻辑门芯片(型号ECP5-5G-85),支持多通道数据并行处理。用于录波数据处理模块(A端)和调度数据处理模块(B端)的物理隔离和数据交换。FPGA与数据加密处理器之间采用serdes接口连接,serdes接口的传输速率支持270Mbps~3.2Gbps,以数据加密处理器传输速率为上线,即数据交换模块的传输速率最高支持480Mbps。

[0077] 其中,所述数据交换模块,如图1所示,还包括FLASH存储器C,所述FLASH存储器C与所述FPGA电性连接。

[0078] FLASH存储器C(型号K9F2G08U0C),用于程序存储和A/B端数据中转。容量选择为2G,临时存储A/B端数据,即转即删。

[0079] 其中,所述调度数据处理模块,具体包括:

[0080] ARM处理器B、以太网控制器B以及RJ45网口B;

[0081] 所述ARM处理器B的一端与所述数据加密处理器B电性连接,另一端与所述以太网控制器B电性连接;

[0082] 所述以太网控制器B的一端与所述ARM处理器B电性连接,另一端与所述RJ45网口B电性连接;

[0083] 所述RJ45网口B的一端与所述以太网控制器B电性连接,另一端与所述调度数据网电性连接。

[0084] ARM处理器B,采用ARM11架构的32位微型处理器(型号S3C6410X),采用嵌入式系统,能够有效阻断来自调度数据网内的病毒、漏洞、非法服务等攻击。

[0085] 其中,所述以太网控制器B、RJ45网口B,包括4组,如图1所示,具体包括:

[0086] 以太网控制器B1、RJ45网口B1为一组,以太网控制器B2、RJ45网口B2为一组,以太网控制器B3、RJ45网口B3为一组,以太网控制器B4、RJ45网口B4为一组,分别与所述ARM处理器B、调度数据网对应电性连接。

[0087] 以太网控制器B1~B4,四个独立网卡(型号DM9000AE),用于与调度主站通信,主备情况视接入调度主站数量而定,支持省调、地调主站和变电站子站的同时接入;RJ45网口B1~B4,四个独立网口(型号HR911105A),用于与调度数据网交换机连接的网线接口,支持10Mbps/100Mbps带宽自适应。

[0088] 其中,所述调度数据处理模块,如图1所示,还包括FLASH存储器B,所述FLASH存储器B与所述ARM处理器B电性连接。

[0089] FLASH存储器B,采用NandFlash技术的FLASH芯片(型号K9K8G08U0A),拥有较高的

读写、擦除速度,能够有效提高数据传输效率。FLASH存储器B作为ARM处理器B的外部存储元件,负责功能程序的存储和录波数据、调度主站指令的暂存。容量选择为8G,其中4G划分为录波数据和调度指令的暂存空间,采用循环覆盖方式存储。

[0090] 录波数据安全交换电路的功能单元如图2所示:

[0091] 1) 通信规约服务单元:与录波器或调度主站建立通信连接,支持IEC103和IEC61850规约。通信规约服务单元单元可自己完成数据包的粘包和重新拆包工作,因此对录波器和调度主站的数据包大小没有限制,最大程度保证对运行设备的兼容性。

[0092] 2) 病毒、风险检测单元:对录波器、调度数据网和AB端之间传输的数据进行病毒查杀和风险检测,采用白名单制度,只允许白名单配置的IP、端口、协议、服务通过,对非法数据包进行删除并记录日志。

[0093] 3) 录波数据解析单元:解析录波器发送的数据包中的comtrade格式录波文件,检查数据完整性。

[0094] 4) 录波数据过滤单元:通过解析录波文件中cfg格式的配置文件,识别出开关量通道;再通过解析dat格式的数据文件,识别开关量通道是否有变位(通道值是否存在0到1或1到0变化)。对含开关量变位的录波数据设定优先级为高,不含则为低。录波数据处理模块、数据交换模块和调度数据处理模块按照优先级由高到低传输数据,优先级相同的数据按照到达时间由先到后传输数据。

[0095] 5) 安全策略配置单元:RJ45网口A2作为调试接口(出厂默认IP、端口),可通过调试程序对录波数据处理模块和调度数据处理模块的各网口的IP、端口进行配置(当RJ45网口A2的IP、端口发生改变时,会自动改变调试接口的相应配置);对白名单中的对端IP、端口、协议、服务进行配置。

[0096] 6) 数据加/解密单元:采用数据加密处理器芯片自带的私有协议对数据进行加/解密。

[0097] 7) 网络安全隔离:通过FPGA程序控制逻辑链路的通断实现A、B端的物理隔离。即在连接A端接收/发送数据时,B端断开,反之亦然。录波器与调度主站的业务流程采用的是调度主站端发起、录波器响应的模式,所以在空闲状态下默认保持A端断开、B端连接的状态。

[0098] 8) 数据交换:FPGA通过“数据摆渡”的方式实现A、B端的数据交换。

[0099] 9) 主站指令解析:解析调度主站发送的指令。调度指令主要有:建立/断开通信连接、调取录波文件列表、调取录波文件、调取定值、远方启动等。调度数据模块通过指令内容控制数据交换模块工作。

[0100] 10) 数据上送:根据调度主站指令返回相应的调取数据。当因上一次连接中断,调度主站重新调取数据时,优先返回FLASH存储器B已保存的数据,不再向A端重新发起数据传输命令。

[0101] 假设录波数据安全交换电路已完成安全策略配置,并且与录波器和调度主站已建立通信连接,此时电路处于空闲状态,其工作原理如图3所示。

[0102] 本实施例中的录波数据安全交换电路,用于实现变电站录波器的安全隔离和数据传输,具有以下特点:

[0103] (1) 在传统网闸GAP技术上进行了改良,是一种同时具备物理隔离、高速传输、实时交互和数据过滤等功能的录波数据交换电路。传统网闸设备的数据传输速率平均在

80Mbps,而录波数据安全交换电路的交换速率可达到480Mbps,实时性更好、效率更高。

[0104] (2)增加了IEC103和IEC61850规约服务,对电力系统已投运的录波器和调度主站有极好的兼容性,增加了录波数据解析和过滤、调度主站指令解析等功能,更适合录波器及其调度主站业务。

[0105] (3)录波数据安全交换电路可封装成独立装置,也可封装成录波器板卡,适应不同的变电站运行环境,制造成本更低。

[0106] 虽然本实用新型披露如上,但本实用新型的保护范围并非仅限于此。本领域技术人员在不脱离本实用新型的精神和范围的前提下,可进行各种变更与修改,这些变更与修改均将落入本实用新型的保护范围。

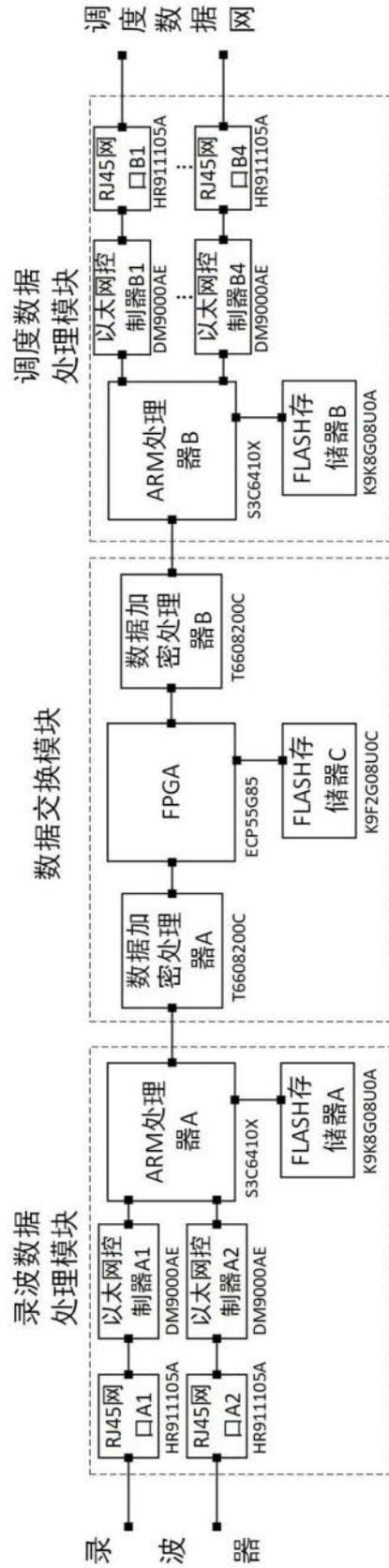


图1



图2

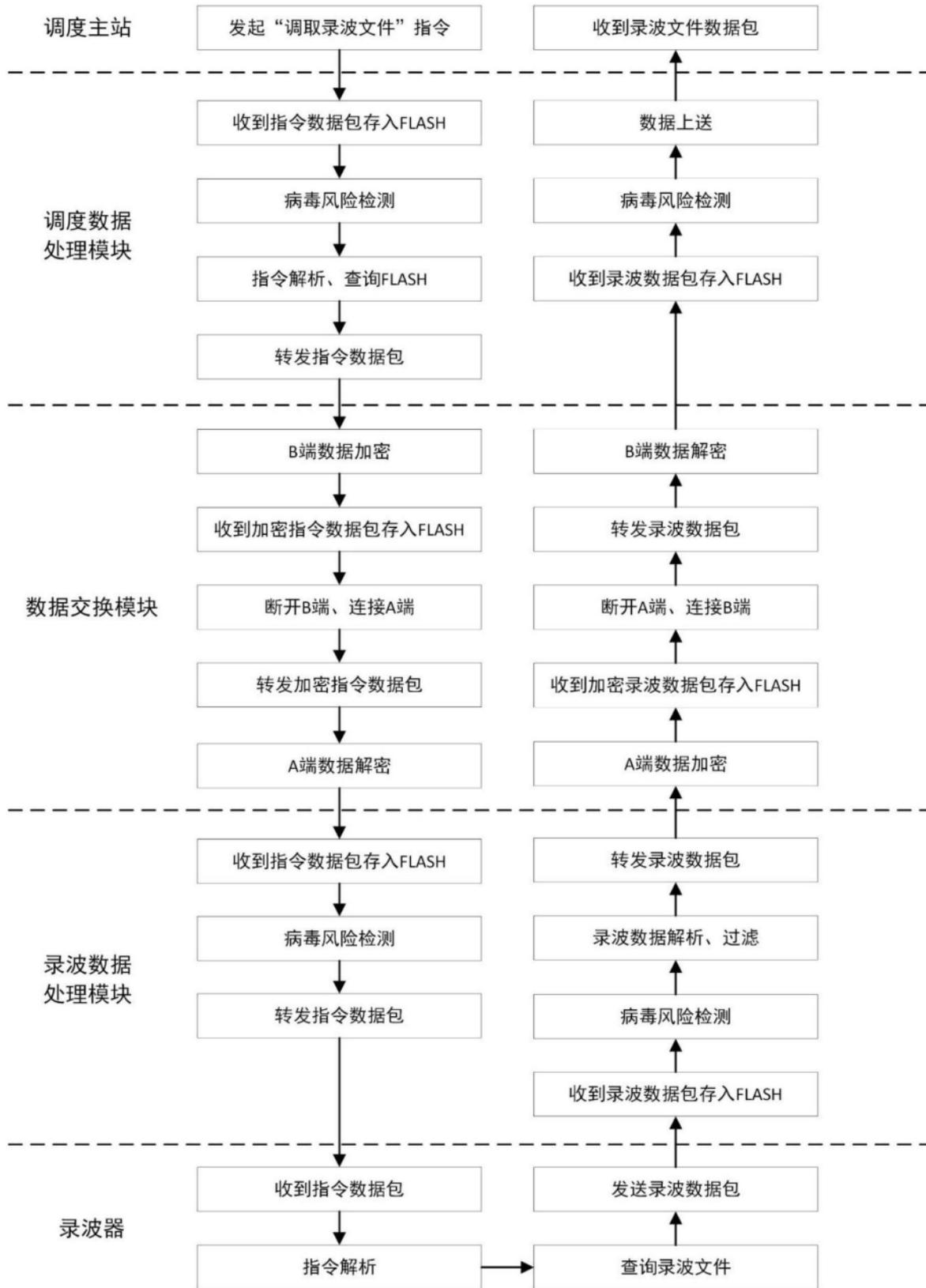


图3