



(12)实用新型专利

(10)授权公告号 CN 210629540 U

(45)授权公告日 2020.05.26

(21)申请号 201921794424.4

G06F 21/70(2013.01)

(22)申请日 2019.10.24

(ESM)同样的发明创造已同日申请发明专利

(73)专利权人 深圳市永达电子信息股份有限公司

地址 518000 广东省深圳市南山区西丽街
道科技北一路17号摩比天线大楼6楼
601-602室

(72)发明人 戚建淮 曾昌鹏 宋晶 刘建辉
郑伟范 胡金华 彭华

(74)专利代理机构 广州嘉权专利商标事务所有
限公司 44205

代理人 洪铭福

(51)Int.Cl.

H04L 29/06(2006.01)

H04L 9/32(2006.01)

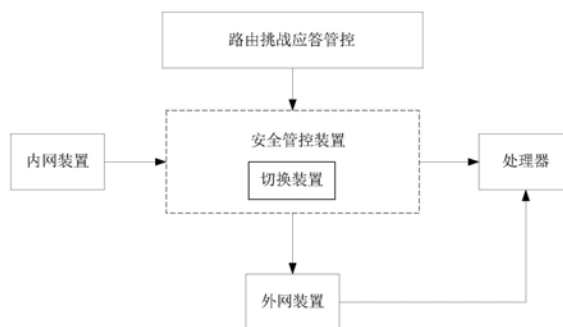
权利要求书1页 说明书4页 附图3页

(54)实用新型名称

一种安全隔离控制计算机系统

(57)摘要

本实用新型公开了一种安全隔离控制计算机系统。其中,安全隔离控制计算机系统包括:安全管控装置、内网装置、外网装置、处理器装置、路由挑战应答管控装置,其中,安全管控装置用于所述外网装置的管控以及外网装置与内网装置的USB通信管控;内网装置,用于与内部网络通信;外网装置,用于与外部网络通信;处理器装置,用于电连接所述外网装置或所述内网装置以构成外网计算机或者内网计算机;路由挑战应答管控装置,用于管控挑战应答,本实用新型通过利用在计算机系统中设置管控装置的技术手段,克服现有技术中存在物理隔离方式占用物理空间大、能耗和成本高,存在安全和泄密隐患技术问题,实现了节省物理空间、能耗和成本,消除安全和泄密隐患的有益效果。本实用新型可广泛应用于信息安全领域。



1. 一种安全隔离控制计算机系统,其特征在于,包括:

安全管控装置、内网装置、外网装置、处理器装置、路由挑战应答管控装置;

所述安全管控装置分别与内网装置、外网装置、处理器装置、路由挑战应答管控装置电连接,用于外网装置的管控、外网装置与内网装置的USB通信管控,所述USB通信管控包括USB通信管控单元;

所述处理器装置与安全管控装置电连接,用于电连接所述外网装置或所述内网装置以构成外网计算机或者内网计算机;

所述路由挑战应答管控装置与安全管控装置电连接,用于与所述安全管控装置之间进行挑战应答。

2. 根据权利要求1所述的一种安全隔离控制计算机系统,其特征在于,所述内网装置包括CPU、EMMC、DDR、内网接口单元、外网装置通信接口管控单元,所述内网装置与所述安全管控装置连接,用于与内部网络通信。

3. 根据权利要求1所述的一种安全隔离控制计算机系统,其特征在于,所述外网装置包括CPU、硬盘、内存、外网接口单元,所述外网装置与所述安全管控装置电连接,用于与外部网络通信。

4. 根据权利要求3所述的一种安全隔离控制计算机系统,其特征在于,所述外网接口单元与所述USB通信管控单元之间包括外网装置通信接口、USB通信接口和切换接口。

5. 根据权利要求3所述的一种安全隔离控制计算机系统,其特征在于,所述安全管控装置包括:切换装置,所述切换装置包括外网开关器件和内网开关器件,用于接收切换指令。

6. 根据权利要求5所述的一种安全隔离控制计算机系统,其特征在于,所述内网开关器件包括第一内网开关器件和第二内网开关器件,所述第一内网开关器件设置在所述内网和所述处理器装置、管控单元之间;所述第二内网开关器件设置在所述内网装置和所述处理器装置之间的第二内网开关器件;

所述外网开关器件包括第一外网开关器件和第二外网开关器件,所述第一外网开关器件设置在所述内网和所述处理器装置之间,所述第二外网开关器件设置在所述外网接口单元和所述处理器装置之间。

7. 根据权利要求1-6任意一项所述的一种安全隔离控制计算机系统,其特征在于,所述处理器装置包括:处理器模块,与所述处理器模块连接的随机存储模块,以及用于复位所述处理器模块以及随机存储模块的复位模块。

一种安全隔离控制计算机系统

技术领域

[0001] 本实用新型涉及信息安全领域,尤其是一种安全隔离控制计算机系统。

背景技术

[0002] 随着计算机的普遍应用及双网办公的迫切需求,以切换器和隔离卡为代表的双网隔离计算机方案得到了一定程度的应用。但是由于架构本身的缺陷,现有安全隔离计算机产品存在严重的安全和泄密隐患,如果继续应用在国家政府机关等对信息保密要求高的重要机构,必然会对我国信息安全造成重大威胁。目前,具有隔离功能的同类产品主要采用网络接口隔离方式、简单物理隔离方式与隔离卡方式。

[0003] 现有技术中现有网络接口隔离方式的缺陷,现有内外网计算机的网线的插头和插座都采用普通的RJ45接口标准,因此,内外网计算机的网线可能会被误插,会直接导致内网主机内的敏感数据通过网线泄露到外网计算机,或者外网计算机的病毒或木马程序通过网线进入内网主机及网络。

[0004] 两台独立的内外网计算机采用简单物理隔离方式的缺陷现有技术中有采用“简单物理隔离”的方式,即使用两台独立的计算机分别联接内网、外网进行工作。但这种方式既增加了物理空间和成本,又不方便使用。为此,人们又采用了双主机加键盘鼠标显示器切换器的方法,这种方案虽然在一定程度上方便了使用,但是仍然存在显著缺点。内网和外网主机缺乏统一的防护系统,不便对用户的操作进行纪录和回溯。需要两套独立的主机和电源,增加了物理空间,能耗和成本。

[0005] 为了解决这些问题,采用隔离卡进行内外网隔离的技术应运而生,主要原理是在计算机上使用一套CPU主板等主要部件,配备两套硬盘等存储设备,分别分配给内网和外网使用。利用隔离卡上的电子开关或电源开关,实现内网和外网的切换和隔离,这样虽然实现了利用一套CPU和主板等主要部件来进行内外网的分时工作,但是存在如下显著缺陷:隔离卡本身存在物理失效的可能,导致内外网信息隔离失败。内外网共享外网等外部存储设备,导致内外网信息隔离失败。内外网共享CPU和主板,它们内嵌存储部件,如CPU内的缓存,主板上的显存,主板上的闪存。前两者是易失性存储器,后者是非易失性存储器。对于非断电切换的第三代隔离卡,这三者都构成了内外网间的隐蔽信道。对于断电或重启切换的第三代隔离卡,非易失性存储器也构成了内外网间的隐蔽信道,不满足国家对物理隔离相关标准的要求。

实用新型内容

[0006] 本实用新型旨在至少在一定程度上解决相关技术中的技术问题之一。为此,本实用新型的一个目的是提供一种安全隔离计算机系统,能够克服现有技术中存在物理隔离方式占用物理空间大、能耗和成本高、存在安全和泄密隐患技术问题,实现了节省物理空间、能耗和成本,消除安全和泄密隐患的有益效果。

[0007] 本实用新型所采用的技术方案是:

[0008] 本实用新型提供一种安全隔离控制计算机系统,包括:安全管控装置:分别与内网装置、外网装置、处理器装置、路由挑战应答管控装置电连接,用于外网网络的管控、外网装置与内网系统的USB通信管控,所述USB通信管控包括USB通信管控单元;

[0009] 处理器装置:与安全管控装置电连接,用于电连接所述外网装置或所述内网装置以构成外网计算机或者内网计算机;

[0010] 路由挑战应答管控装置:与安全管控装置电连接,用于与管控装置之间进行挑战应答。

[0011] 进一步地,内网装置包括CPU、EMMC、DDR、内网接口单元、外网装置通信接口管控单元,所述内网装置与所述安全管控装置连接,用于与内部网络通信。

[0012] 进一步地,外网装置包括CPU、硬盘、内存、外网接口单元,所述外网装置与所述安全管控装置电连接,用于与外部网络通信。

[0013] 进一步地,其中,外网接口单元与所述USB通信管控单元,包括外网装置通信接口、USB通信接口和切换接口。

[0014] 进一步地,其中安全管控装置包括:切换装置,所述切换装置包括外网开关器件和内网开关器件,用于接收切换指令。

[0015] 进一步地,所述内网开关器件包括设置在所述内网和所述处理器装置、管控单元之间的第一内网开关器件和设置在所述内网接口单元和所述处理器装置之间的第二内网开关器件;

[0016] 所述外网开关器件包括设置在所述内网和所述处理器装置之间的第一外网开关器件和设置在所述外网接口单元和所述处理器装置之间的第二外网开关器件。

[0017] 进一步地,所述处理器装置包括:处理器模块,与所述处理器模块通信连接的随机存储模块,以及用于复位所述处理器模块以及随机存储模块的复位模块。

[0018] 本实用新型通过利用在计算机系统中设置管控装置的技术手段,克服现有技术中存在物理隔离方式占用物理空间大、能耗和成本高,存在安全和泄密隐患技术问题,实现了节省物理空间、能耗和成本,消除安全和泄密隐患的有益效果。

附图说明

[0019] 图1是本实用新型一种安全隔离控制计算机系统实施例1示意图;

[0020] 图2A-2C是本实用新型实施例一种安全隔离控制计算机系统实施例1管控系统IO部分连接电路图;

[0021] 图3是本实用新型实施例一种安全隔离控制计算机系统实施例1系统原理详细框图。

具体实施方式

[0022] 需要说明的是,在不冲突的情况下,本申请中的实施例及实施例中的特征可以相互组合。

[0023] 实施例1:本实用新型一种安全隔离控制计算机系统,如图1所示,安全管控装置:分别与内网装置、外网装置、处理器装置、路由挑战应答管控装置电连接,用于外网网络的管控、外网装置与内网系统的USB通信管控,所述USB通信管控包括USB通信管控单元;内网

装置：内网装置包括CPU、EMMC、DDR、内网接口单元、外网装置通信接口管控单元，上述内网装置与安全管控装置连接，用于与内部网络通信；外网装置：外网装置包括 CPU、硬盘、内存、外网接口单元，上述外网装置与所述安全管控装置电连接，用于与外部网络通信；处理器装置：与安全管控装置电连接，用于电连接外网装置或内网装置以构成外网计算机或者内网计算机；路由挑战应答管控装置：与安全管控装置电连接，用于与管控装置之间进行挑战应答。

[0024] 其中，外网接口单元与所述USB通信管控单元，包括外网装置通信接口、USB通信接口和切换接口。

[0025] 其中内网开关器件包括设置在内网装置和所述处理器装置、安全管控装置之间的第一内网开关器件和设置在内网接口单元和所述处理器装置之间的第二内网开关器件，用于电连接内网显示装置和所述处理器装置以及安全管控装置。

[0026] 其中外网开关器件包括设置在外网装置和处理器装置之间的第二外网开关器件和设置在外网接口单元和所述处理器装置之间的第一外网开关器件，用于电连接外网显示装置和所述处理器装置。

[0027] 其中，在安全管控装置中还包括切换装置，切换装置，包括外网开关器件和内网开关器件，上述切换装置用于接收切换指令；其中的内网开关器件，内网开关器件包括设置在内网 CPU、EMMC、DDR和处理器装置、管控单元之间的第一内网开关器件和设置在内网接口单元和处理器装置之间的第二内网开关器件，用于电连接所述外网装置和处理器装置；上述外网开关器件包括设置在所述内网硬盘、内存、CPU和所述处理器装置之间的第二外网开关器件和设置在所述外网接口单元和所述处理器装置之间的第一外网开关器件，用于电连接内网显示装置和所述处理器装置。

[0028] 具体的，切换装置用于切换外网显示装置和内网显示装置之间的电连接以及外网显示装置和内网显示装置之间的电连接；用于切换外网触摸装置和内网触摸装置之间的电连接以及内网触摸装置和外网触摸装置之间的电连接；用于切换外网键鼠操作装置和内网键鼠装置之间的电连接以及所述内网键鼠装置和外网键鼠装置之间的电连接；

[0029] 其中的切换装置可以包括设置在内网装置和处理器装置之间的内网继电器组件，以及设置在外网装置和处理器装置之间的外网继电器组件，以及控制上述内网继电器组件和外网继电器组件通断的控制器件。在本实用新型中，也可以采用其他开关器件，例如晶体管、开关管、逻辑开关等开关器件来代替继电器组件。上述外网装置和内网装置可以具有独立的存储单元和操作系统。其中的处理器装置可以包括处理器模块和随机存储模块。例如处理器模块可以采用RK3288，采用Cortex-A17的CPU架构，1.8GHz的CPU频率，最新Mali-T76x系列GPU的芯片。

[0030] 处理器装置是采用了适合Android以及Windows系统开发的CPU，可提供外部连接接口例如USB接口、WIFI接口、蓝牙接口，红外接口，以及显示屏接口、摄像机接口、音频接口、HDM接口和触摸屏接口。

[0031] 实施例2：如图2为管控系统I0电路图，其中图2A为安全管控GPIO整体电路图，用于安全管控装置对输入输出信号的控制。

[0032] 图2B为安全管控装置USB输出到内网或外网装置电路I0图，此电路是通过安全管控 USB通信接口控制内外网的输入输出图，实现了通过安全管控装置控制内外网装置的目的。

的。

[0033] 图2C为挑战应答WIFI模块接口图,因在挑战应答装置和安全管控装置之间需要挑战应答方式建立连接,在安全管控装置中设置挑战应答WIFI模块接口,可以连接WIFI模块,从而释放WIFI热点,以便于挑战应答装置例如手机或者其他移动终端和安全管控装置之间建立通信连接进行相应操作。

[0034] 实施例3:图3为图1所示系统框图的内部系统详细框图,安全隔离计算机系统包括安全管控系统,内网装置、外网装置、处理器装置、路由挑战应答管控装置,其中安全管控系统中设有接口例如USB、网口、HDMI口、I2C接口等,其中USB口用于连接鼠标、键盘等USB接口设备,网口用于连接安全管控装置、外网装置以及内外网切换;HDMI接口用于连接处理器装置中的显示屏以及内网装置中相对应的HDMI接口;I2C接口用于连接触摸屏。

[0035] 对于内网能正常工作,K1、K5断开,K2、K3、K4打开,K6、K7拨到内网通道;

[0036] 对于外围能正常工作,K1、K5导通,K2、K3、K4打开,K6、K7拨到外网通道。

[0037] 本实用新型实施例中,该安全隔离控制计算机系统可以采用以下配置:

基本功能	参数
显示屏	支持 1920mm×1080mm、21.5 寸
触摸显示屏	支持多点触摸（10 点），电容屏，21.5 寸
操作系统	Win7 以上
CPU	J1900 Intel 四核 2.0GHz
内存	4GB DDR3 （可选 2GB、8GB）
内部存储	SSD 512GB（可选 64GB、128GB、256GB）
管控器	RK3288 2G DDR3 4G EMMC
外网认证路由	MT7628 DDR2 512Mb W9751G6KB-25
接口	HDMI-IN×1，标准 USB2.0×2（1 个用于鼠标、1 个用于键盘），MINI USB2.0×1（用于连接内网主机）接口，Micro USB2.0×1（用于管控系统升级用），RJ45×1
系统切换按键	系统切换按键，用于内外网系统切换用
开机按钮	一个开机按钮（可以开关机，内网模式的待机唤醒）
指示灯	内外网双色指示灯(1 个双色指示灯，外网模式指示灯为绿色，内网模式指示灯为红灯)，认证指示灯（红/绿）
报警	增加报警器*1 与管控器连接
主板预留端子	升级键，debug 口等常用工程调试接口
立体声喇叭	2×8W
电源接口	DC IN 12V 4A
RTC	RTC

[0039] 以上是对本实用新型的较佳实施进行了具体说明,但本实用新型创造并不限于所述实施例,熟悉本领域的技术人员在不违背本实用新型精神的前提下还可做出种种的等同变形或替换,这些等同的变形或替换均包含在本申请权利要求所限定的范围内。

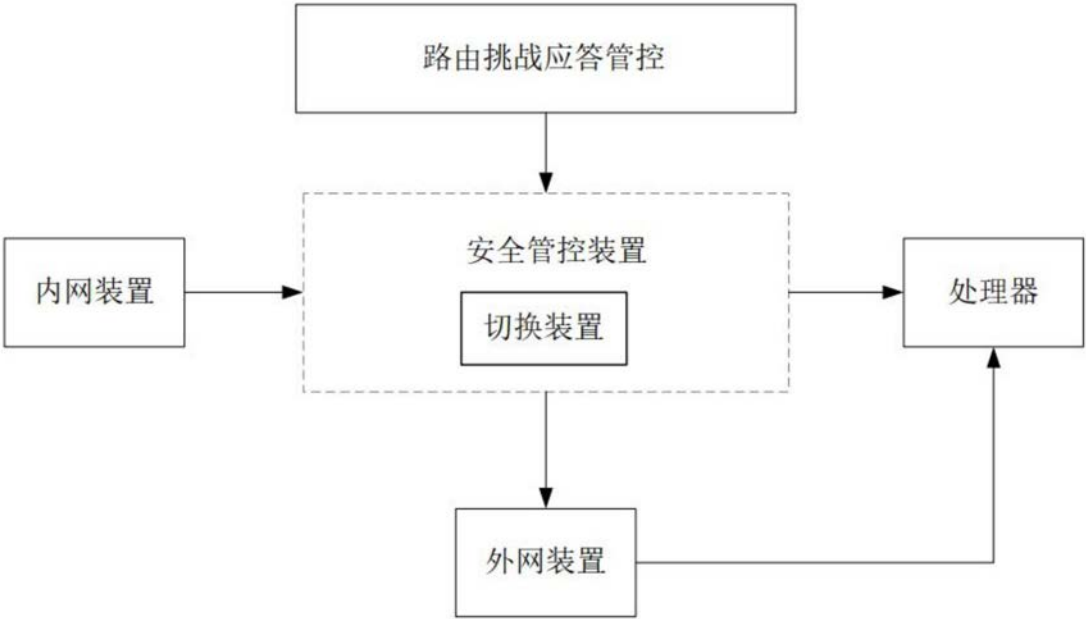


图1

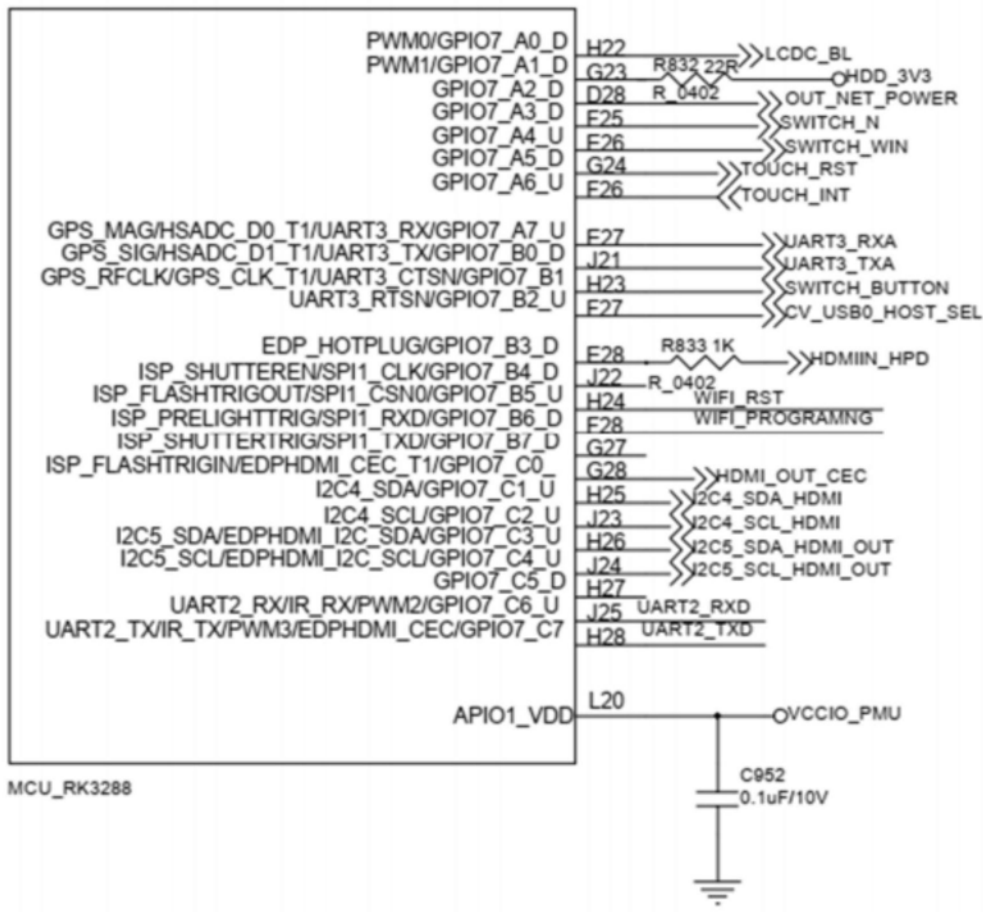


图2A

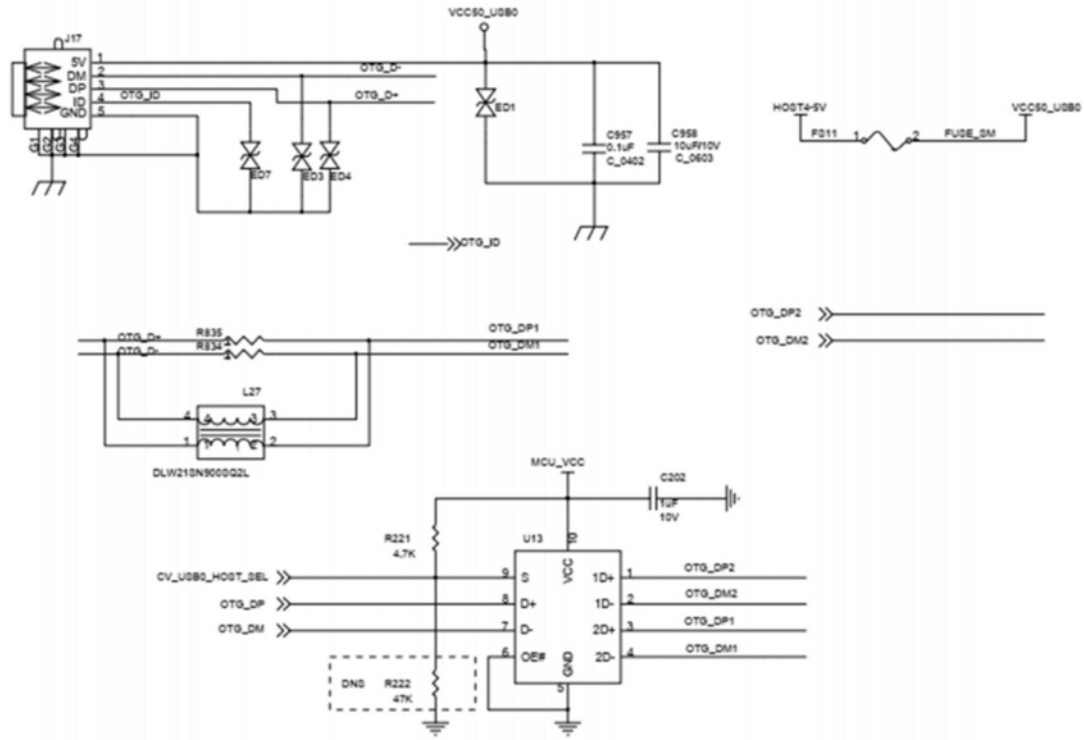


图2B

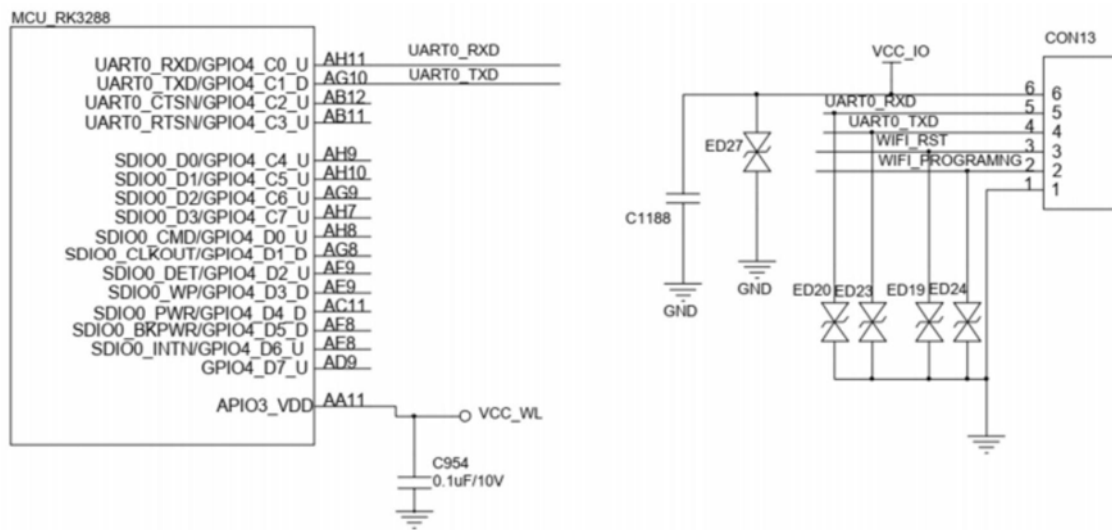


图2C

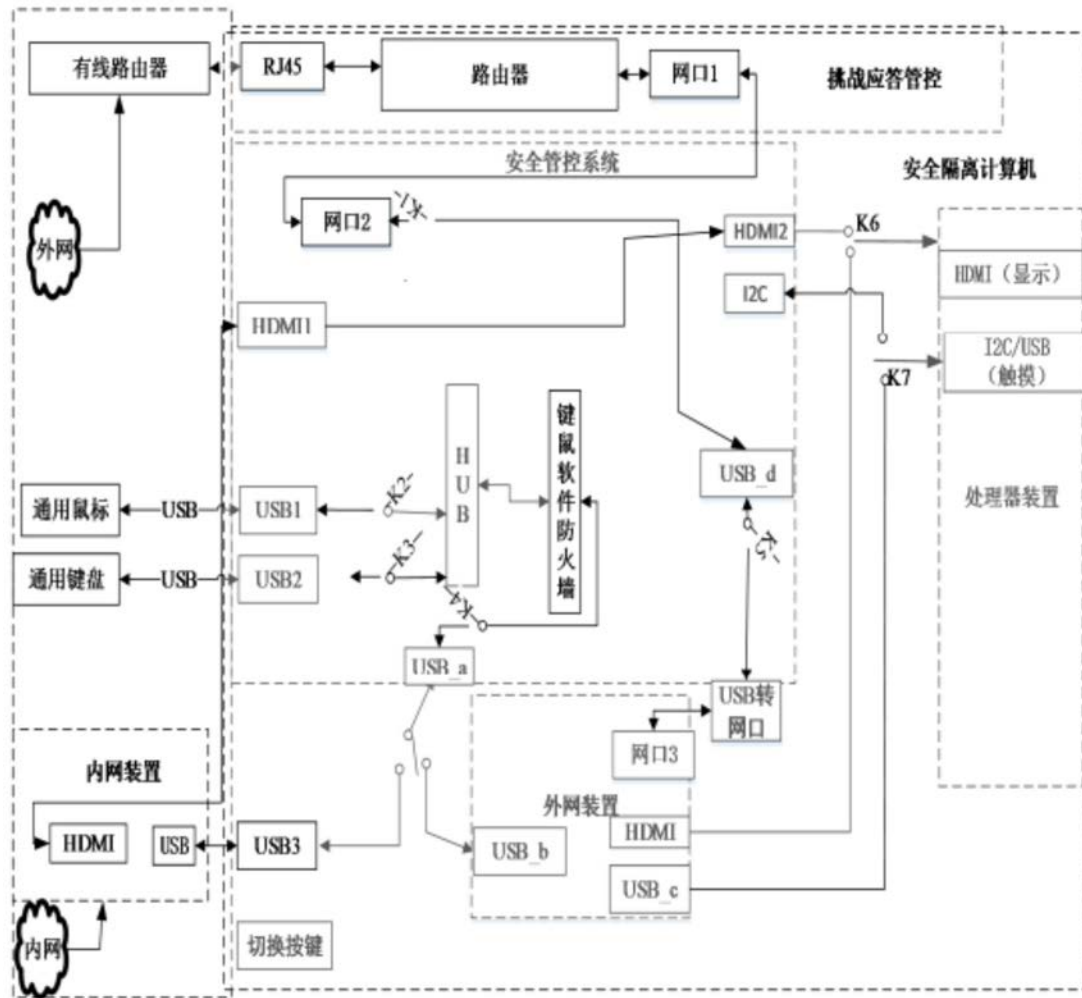


图3