



(12) 发明专利

(10) 授权公告号 CN 108681677 B

(45) 授权公告日 2022. 08. 19

(21) 申请号 201810458381.6

(22) 申请日 2018.05.14

(65) 同一申请的已公布的文献号

申请公布号 CN 108681677 A

(43) 申请公布日 2018.10.19

(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 宋晶 郑伟范 曾昌鹏

(74) 专利代理机构 广州嘉权专利商标事务有限公司 44205

专利代理师 黄春燕

(51) Int.Cl.

G06F 21/62 (2013.01)

G06F 21/34 (2013.01)

(56) 对比文件

CN 103853987 A, 2014.06.11

CN 101521568 A, 2009.09.02

CN 104217177 A, 2014.12.17

CN 103886267 A, 2014.06.25

CN 101739516 A, 2010.06.16

CN 105354504 A, 2016.02.24

审查员 郭瑞

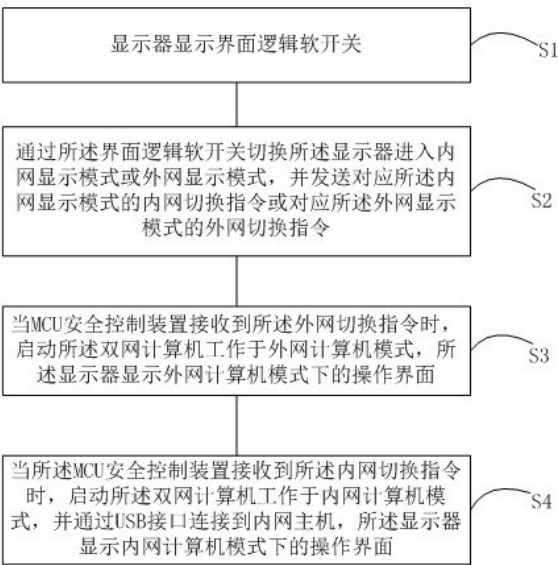
权利要求书4页 说明书12页 附图5页

(54) 发明名称

基于USB接口安全隔离双网计算机的方法、装置及系统

(57) 摘要

本发明实施例公开一种基于USB接口安全隔离双网计算机的方法、装置及系统。该方法包括：显示器显示界面逻辑软开关；通过界面逻辑软开关切换所述显示器进入内网显示模式或外网显示模式，并发送对应所述内网显示模式的内网切换指令或对应所述外网显示模式的外网切换指令；当MCU安全控制装置接收到外网切换指令时，启动双网计算机工作于外网计算机模式，显示器显示外网计算机模式下的操作界面；当MCU安全控制装置接收到内网切换指令时，启动双网计算机工作于内网计算机模式，通过USB接口连接到内网主机，显示内网计算机模式下的操作界面。内网和外网共用显示屏，一键软切换，减少了操作繁琐性，隔离效果好，避免信息泄露和篡网，安全性和可靠性较佳。



1. 一种基于USB接口安全隔离双网计算机的方法,其特征在于,所述方法包括:

双网计算机包括处理器、显示器、MCU安全控制装置、内网存储器和外网存储器;双网计算机通过USB接口与内网主机连接;

显示器显示界面逻辑软开关;

通过所述界面逻辑软开关切换所述显示器进入内网显示模式或外网显示模式,并发送对应所述内网显示模式的内网切换指令或对应所述外网显示模式的外网切换指令;

当MCU安全控制装置接收到所述外网切换指令时,双网计算机进行复位重启,双网计算机的内网计算机模式下的操作系统关机,外网计算机模式下的操作系统启动,显示外网应用界面,工作于外网计算机模式,所有内网计算机模式下的内存全部清零,同时内网计算机模式下的专用硬盘数据被清零,所述显示器显示外网计算机模式下的操作界面;外网显示模式下,处理器用于计算、控制及显示处理,外网存储器用于对应的操作系统运行及存储;

当所述MCU安全控制装置接收到所述内网切换指令时,双网计算机进行复位重启,外网计算机模式下的操作系统关机,内网计算机模式下的操作系统启动,显示内网应用界面,并通过USB接口连接到内网主机,工作于内网计算机模式,所有外网计算机模式下的内存、CPU和外网接口全部断电和清零,并禁用所有外网接口,所述显示器显示内网计算机模式下的操作界面;内网显示模式下,处理器用于图形计算内网主机界面显示处理,内网存储器用于对应的操作系统运行及存储;

内网显示模式下,显示器具有智能显示终端功能,实现内网智能显示,内网主机的显示加密后输出到显示器上;内网智能显示功能包括加密传输功能:为了确保内网计算机模式下的内网主机显示及视频安全性,通过超映射混沌的图像加密算法对明文图像进行Logistic置乱操作,打乱像素点的原始位置,使攻击无法识别有用信息,采用超混沌系统对密文进行置乱操作,并采用置乱后密文图像实现明文图像加密操作,支持对图像的保护且抵抗各种类型的攻击;内网显示控制编辑功能:通过USB接口将智能显示终端的命令下达至内网主机从而达到完全操作内网主机内容的功能。

2. 根据权利要求1所述的基于USB接口安全隔离双网计算机的方法,其特征在于,当所述MCU安全控制装置接收到所述外网切换指令时,启动所述双网计算机工作于外网计算机模式,所述显示器显示外网计算机模式下的操作界面,具体包括:

当所述MCU安全控制装置接收到所述外网切换指令时,所述MCU安全控制装置控制第一继电器、第二继电器断开连接所述内网主机的USB接口,关闭对应所述内网计算机模式的操作系统和断开对应所述内网计算机模式的存储系统;

所述MCU安全控制装置控制第三继电器、第四继电器连通,启动对应所述外网计算机模式的操作系统,建立与外部网络之间的连接,启动对应所述外网计算机模式的存储系统,所述MCU安全控制装置控制电源管理单元复位,并控制所述第一继电器、第二继电器处于断开状态以物理隔离外网计算机模式和内网计算机模式,将所述双网计算机的CPU和RAM存储器清零;

所述显示器显示在外网计算机模式下的操作界面。

3. 根据权利要求2所述的基于USB接口安全隔离双网计算机的方法,其特征在于,当所述MCU安全控制装置接收到所述内网切换指令时,启动所述双网计算机工作于内网计算机模式,并通过USB接口连接到内网主机,所述显示器显示内网计算机模式下的操作界面,具

体包括：

当所述MCU安全控制装置接收到所述内网切换指令时，所述MCU安全控制装置控制第三继电器、第四继电器断开，关闭对应所述外网计算机模式的操作系统，断开所述显示器与外部网络连接的全部接口，断开对应所述外网计算机模式的存储系统；

所述MCU安全控制装置控制第一继电器、第二继电器连通，启动对应所述内网计算机模式的操作系统，采用USB存储器硬件加密并与内网主机进行双向认证，待双向认证通过后，通过USB接口连接内网主机，启动对应所述内网计算机模式的存储系统，所述MCU安全控制装置控制电源管理单元复位，并控制所述第三继电器、第四继电器处于断开状态以物理隔离外网计算机模式和内网计算机模式，将所述双网计算机的CPU和RAM存储器清零；

所述显示器显示在内网计算机模式下的操作界面。

4. 根据权利要求3所述的基于USB接口安全隔离双网计算机的方法，其特征在于，所述MCU安全控制装置为包括可信加密芯片的MCU，所述可信加密芯片为MCU安全控制装置提供加密服务，具体包括：所述可信加密芯片加电后进行自检，完成状态检查；所述可信加密芯片读取双网计算机的BIOS代码，对所述BIOS代码进行度量，并将度量结果存储在所述可信加密芯片中；所述可信加密芯片转移控制权至双网计算机的CPU，所述可信加密芯片成为一个控制器，为MCU安全控制装置提供加密服务。

5. 根据权利要求4所述的基于USB接口安全隔离双网计算机的方法，其特征在于，通过所述界面逻辑软开关切换所述显示器进入内网显示模式或外网显示模式，并发送对应所述内网显示模式的内网切换指令或对应所述外网显示模式的外网切换指令，包括：

启动所述界面逻辑软开关；

依据对所述界面逻辑软开关发出的外网切换指令，包括可信加密芯片的MCU发送第一电平信号控制所述显示器启动外网显示模式；

在所述外网显示模式下启动对应的显示页面；

依据对所述界面逻辑软开关发出的内网切换指令，所述可信加密芯片的MCU发送第二电平信号控制所述显示器启动内网显示模式；

在所述内网显示模式下启动对应的显示页面。

6. 根据权利要求5所述的基于USB接口安全隔离双网计算机的方法，其特征在于，所述第二继电器一端连接双网计算机的USB接口，另一端分别连接双网计算机的CPU和所述MCU安全控制装置。

7. 根据权利要求6所述的基于USB接口安全隔离双网计算机的方法，其特征在于，当所述显示器为触控显示器显示所述界面逻辑软开关时，分以下情况：

当所述MCU安全控制装置接收到所述外网切换指令时，启动所述双网计算机工作于外网计算机模式，所述显示器显示外网计算机模式下的操作界面，包括：

接收用户输入的选择外网显示模式的触控指令时，所述显示器切换到外网显示模式，接收所述用户输入的账户和密码验证信息，所述双网计算机切换到外网计算机模式，然后复位重启显示；

当所述MCU安全控制装置接收到所述内网切换指令时，启动所述双网计算机工作于内网计算机模式，并通过USB接口连接到内网主机，所述显示器显示内网计算机模式下的操作界面，包括：

接收用户输入的选择内网显示模式的触控指令时,所述显示器切换到内网显示模式,所述MCU安全控制装置接收所述用户输入的选择内网显示模式的触控指令后,启动对应内网计算机模式的开机画面,然后对所述用户进行身份验证,待所述身份验证通过后再进入所述双网计算机对应内网计算机模式的内网操作系统,通过USB存储器进行硬件加密和双向认证后,与内网主机通过USB接口建立通信连接。

8. 根据权利要求7所述的基于USB接口安全隔离双网计算机的方法,其特征在于,通过所述USB存储器进行硬件加密和双向认证后,与内网主机通过USB接口建立通信连接,包括:

在所述内网计算机模式下,所述显示器端通过USB存储器存储的内网主机公钥和自身私钥,调用存储在所述可信加密芯片中的加密算法,与内网主机间进行一对一认证;所述加密算法为超映射混沌的图像加密算法。

9. 一种基于USB接口安全隔离双网计算机的装置,其特征在于,包括:

显示模块,控制显示器显示界面逻辑软开关;

切换模块,用于通过所述界面逻辑软开关切换所述显示器进入内网显示模式或外网显示模式,并发送对应所述内网显示模式的内网切换指令或对应所述外网显示模式的外网切换指令;

外网计算机模式工作模块,包括第一外网显示模式处理单元和第二外网显示模式处理单元;第一外网显示模式处理单元用于当MCU安全控制装置接收到所述外网切换指令时,所述MCU安全控制装置控制第一继电器、第二继电器断开连接内网计算机的USB接口,关闭对应所述内网计算机模式的操作系统和断开对应所述内网计算机模式的存储系统;第二外网显示模式处理单元用于所述MCU安全控制装置控制第三继电器、第四继电器连通,启动对应所述外网计算机模式的操作系统,建立与外部网络之间的连接,启动对应所述外网计算机模式的存储系统,所述MCU安全控制装置控制电源管理单元复位,并控制所述第一继电器、第二继电器处于断开状态以物理隔离外网计算机模式和内网计算机模式,将所述双网计算机的CPU和RAM存储器清零;

内网计算机模式工作模块,包括第一内网显示模式处理单元和第二内网显示模式处理单元;第一内网显示模式处理单元用于当MCU安全控制装置接收到所述内网切换指令时,所述MCU安全控制装置控制第三继电器、第四继电器断开,关闭对应所述外网计算机模式的操作系统,断开所述显示器与外部网络连接的全部接口,断开对应所述外网计算机模式的存储系统;第二内网显示模式处理单元用于MCU安全控制装置控制第一继电器、第二继电器连通,启动对应所述内网计算机模式的操作系统,采用USB存储器硬件加密并与内网主机进行双向认证,待双向认证通过后,通过USB接口连接内网主机,启动对应所述内网计算机模式的存储系统,所述MCU安全控制装置控制电源管理单元复位,并控制所述第三继电器、第四继电器处于断开状态以物理隔离外网计算机模式和内网计算机模式,将所述双网计算机的CPU和RAM存储器清零;

内网显示模式下,显示器具有智能显示终端功能,实现内网智能显示,内网主机的显示加密后输出到显示器上;内网智能显示功能包括加密传输功能:为了确保内网计算机模式下的内网主机显示及视频安全性,通过超映射混沌的图像加密算法对明文图像进行Logistic置乱操作,打乱像素点的原始位置,使攻击无法识别有用信息,采用超混沌系统对密文进行置乱操作,并采用置乱后密文图像实现明文图像加密操作,支持对图像的保护且

抵抗各种类型的攻击;内网显示控制编辑功能:通过USB接口将智能显示终端的命令下达至内网主机从而达到完全操作内网主机内容的功能。

10.一种基于USB接口安全隔离双网计算机的系统,其特征在于,包括:双网计算机、USB接口、内网主机以及MCU安全控制装置,所述系统采用权利要求1至8任一项所述的方法实现所述双网计算机的隔离。

基于USB接口安全隔离双网计算机的方法、装置及系统

技术领域

[0001] 本发明涉及计算机信息安全技术领域,尤其涉及一种基于USB接口安全隔离双网计算机的方法、装置及系统。

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,这三种方式存在的不足分别说明如下:

[0003] (1) 网络接口隔离方式的缺陷

[0004] 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。

[0005] (2) 两台独立的内外网计算机采用简单物理隔离方式的缺陷

[0006] 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。

[0007] 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。

[0008] 需要两套独立的主机和电源,增加了物理空间,能耗和成本。

[0009] (3) 隔离卡方式的缺陷

[0010] 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:

[0011] 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。

[0012] 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。

[0013] 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。

发明内容

[0014] 有鉴于此,本发明解决的技术问题是,提供一种基于USB接口安全隔离双网计算机的方法、装置及系统,解决目前双网计算机中内外网存在的安全隔离失效、显示资源泄密和

显示器冗余的技术问题。

[0015] 第一方面,本发明提供一种基于USB接口安全隔离双网计算机的方法,其中,所述方法包括:

[0016] 显示器显示界面逻辑软开关;

[0017] 通过所述界面逻辑软开关切换所述显示器进入内网显示模式或外网显示模式,并发送对应所述内网显示模式的内网切换指令或对应所述外网显示模式的外网切换指令;

[0018] 当MCU安全控制装置接收到所述外网切换指令时,启动所述双网计算机工作于外网计算机模式,所述显示器显示外网计算机模式下的操作界面;

[0019] 当所述MCU安全控制装置接收到所述内网切换指令时,启动所述双网计算机工作于内网计算机模式,并通过USB接口连接到内网主机,所述显示器显示内网计算机模式下的操作界面。

[0020] 较佳地,所述当MCU安全控制装置接收到所述外网切换指令时,启动所述双网计算机工作于外网计算机模式,所述显示器显示外网计算机模式下的操作界面,包括:

[0021] 当所述MCU安全控制装置接收到所述外网切换指令时,所述MCU安全控制装置控制第一继电器、第二继电器断开连接所述内网主机的USB接口,关闭对应所述内网计算机模式的操作系统和断开对应所述内网计算机模式的存储系统;

[0022] 所述MCU安全控制装置控制第三继电器、第四继电器连通,启动对应所述外网计算机模式的操作系统,建立与外部网络之间的连接,启动对应所述外网计算机模式的存储系统,所述MCU安全控制装置控制电源管理单元复位,并控制所述第一继电器、第二继电器处于断开状态以物理隔离外网计算机模式和内网计算机模式,将所述双网计算机的CPU和RAM存储器清零;

[0023] 所述显示器显示在外网计算机模式下的操作界面。

[0024] 较佳地,所述当所述MCU安全控制装置接收到所述内网切换指令时,启动所述双网计算机工作于内网计算机模式,并通过USB接口连接到内网主机,所述显示器显示内网计算机模式下的操作界面,包括:

[0025] 当所述MCU安全控制装置接收到所述内网切换指令时,所述MCU安全控制装置控制第三继电器、第四继电器断开,关闭对应所述外网计算机模式的操作系统,断开所述显示器与外部网络连接的全部接口,断开对应所述外网计算机模式的存储系统;

[0026] 所述MCU安全控制装置控制第一继电器、第二继电器连通,启动对应所述内网计算机模式的操作系统,采用USB存储器硬件加密并与内网主机进行双向认证,待双向认证通过后,通过USB接口连接内网主机,启动对应所述内网计算机模式的存储系统,所述MCU安全控制装置控制电源管理单元复位,并控制所述第三继电器、第四继电器处于断开状态以物理隔离外网计算机模式和内网计算机模式,将所述双网计算机的CPU和RAM存储器清零;

[0027] 所述显示器显示在内网计算机模式下的操作界面。

[0028] 较佳地,所述MCU安全控制装置为包括可信加密芯片的MCU,所述可信加密芯片为MCU安全控制装置提供加密服务,具体包括:所述可信加密芯片加电后进行自检,完成状态检查;所述可信加密芯片读取双网计算机的BIOS代码,对所述BIOS代码进行度量,并将度量结果存储在所述可信加密芯片中;所述可信加密芯片转移控制权至双网计算机的CPU,所述可信加密芯片成为一个控制器,为MCU安全控制装置提供加密服务。

[0029] 较佳地,所述通过所述界面逻辑软开关切换所述显示器进入内网显示模式或外网显示模式,并发送对应所述内网显示模式的内网切换指令或对应所述外网显示模式的外网切换指令,包括:

[0030] 启动所述界面逻辑软开关;

[0031] 依据对所述界面逻辑软开关发出的外网切换指令,所述包括可信加密芯片的MCU发送第一电平信号控制所述显示器启动外网显示模式;

[0032] 在所述外网显示模式下启动对应的显示页面;

[0033] 依据对所述界面逻辑软开关发出的内网切换指令,所述包括可信加密芯片的MCU发送第二电平信号控制所述显示器启动内网显示模式;

[0034] 在所述内网显示模式下启动对应的显示页面。

[0035] 较佳地,在所述第二继电器一端连接双网计算机的USB接口,另一端分别连接双网计算机的CPU和所述MCU安全控制装置。

[0036] 较佳地,当所述显示器为触控显示器显示所述界面逻辑软开关时,分以下情况:

[0037] 所述当MCU安全控制装置接收到所述外网切换指令时,启动所述双网计算机工作于外网计算机模式,所述显示器显示外网计算机模式下的操作界面,包括:

[0038] 接收用户输入的选择外网显示模式的触控指令时,所述显示器切换到外网显示模式,接收所述用户输入的账户和密码验证信息,所述双网计算机切换到外网计算机模式,然后复位重启显示;

[0039] 所述当所述MCU安全控制装置接收到所述内网切换指令时,启动所述双网计算机工作于内网计算机模式,并通过USB接口连接到内网主机,所述显示器显示内网计算机模式下的操作界面,包括:

[0040] 接收用户输入的选择内网显示模式的触控指令时,所述显示器切换到内网显示模式,所述MCU安全控制装置接收所述用户输入的选择内网显示模式的触控指令后,启动对应内网计算机模式的开机画面,然后对所述用户进行身份验证,待所述身份验证通过后再进入所述双网计算机对应内网计算机模式的内网操作系统,通过USB存储器进行硬件加密和双向认证后,与内网主机通过USB接口建立通信连接。

[0041] 较佳地,所述通过USB存储器进行硬件加密和双向认证后,与内网主机通过USB接口建立通信连接,包括:

[0042] 在所述内网计算机模式下,所述显示器端通过USB存储器存储的内网主机公钥和自身私钥,调用存储在所述可信加密芯片中的加密算法,与内网主机间进行一对一认证;所述加密算法为超映射混沌的图像加密算法。

[0043] 第二方面,本发明还提供一种基于USB接口安全隔离双网计算机的装置,其中,包括:

[0044] 显示模块,控制显示器显示界面逻辑软开关;

[0045] 切换模块,用于通过所述界面逻辑软开关切换所述显示器进入内网显示模式或外网显示模式,并发送对应所述内网显示模式的内网切换指令或对应所述外网显示模式的外网切换指令;

[0046] 外网计算机模式工作模块,用于当MCU安全控制装置接收到所述外网切换指令时,启动所述双网计算机工作于外网计算机模式,所述显示器显示外网计算机模式下的操作界

面；

[0047] 内网计算机模式工作模块，用于当所述MCU安全控制装置接收到所述内网切换指令时，启动所述双网计算机工作于内网计算机模式，并通过USB接口连接到内网主机，所述显示器显示内网计算机模式下的操作界面。

[0048] 第三方面，本发明还提供一种基于USB接口安全隔离双网计算机的系统，包括：双网计算机、USB接口、内网主机以及MCU安全控制装置，所述系统采用前面任一项所述的方法实现所述双网计算机的隔离。

[0049] 本发明所提供的基于USB接口安全隔离双网计算机的方法、装置及系统，内网和外网共用显示屏，一键软切换，减少了操作繁琐性，隔离效果好，避免信息泄露和篡网，安全性和可靠性较佳。

附图说明

[0050] 为了更清楚地说明本发明实施例的技术方案，下面将对本发明实施例中所需要使用的附图作简单地介绍，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

[0051] 图1示出了本发明实施例的基于USB接口安全隔离双网计算机的方法流程示意图。

[0052] 图2示出了图1中双网计算机采用界面软切换开关进行切换的示意图。

[0053] 图3示出了实现图1的基于USB接口安全隔离双网计算机的方法的一种硬件结构示意图。

[0054] 图4示出了图1的MCU安全控制装置的控制流程示意图。

[0055] 图5示出了内网计算机模式与外网计算机模式下的切换流程示意图。

[0056] 图6示出了本发明实施例的基于USB接口安全隔离双网计算机的装置结构示意图。

[0057] 图7示出了本发明实施例的基于USB接口安全隔离双网计算机的系统结构示意图。

具体实施方式

[0058] 下面将详细描述本发明的各个方面的特征和示例性实施例，为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细描述。应理解，此处所描述的具体实施例仅被配置为解释本发明，并不被配置为限定本发明。对于本领域技术人员来说，本发明可以在不需要这些具体细节中的一些细节的情况下实施。下面对实施例的描述仅仅是为了通过示出本发明的示例来提供对本发明更好的理解。

[0059] 需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。而且，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括……”限定的要素，并不排除在包括所述要素的过程、方法、物品或者设备中还存在另外的相同要素。

[0060] 请参见图1至图5，本发明实施例的基于USB接口安全隔离双网计算机的方法，对现有技术中采用隔离卡、网络接口的隔离、简单双机隔离的方式进行改进，主要是采用三机双

网的物理架构,完全割裂与内网主机的连接。具体实现方法如下:

[0061] S1、显示器显示界面逻辑软开关;

[0062] S2、通过所述界面逻辑软开关切换所述显示器进入内网显示模式或外网显示模式,并发送对应所述内网显示模式的内网切换指令或对应所述外网显示模式的外网切换指令;

[0063] S3、当MCU安全控制装置接收到所述外网切换指令时,启动所述双网计算机工作于外网计算机模式,所述显示器显示外网计算机模式下的操作界面;这里MCU安全控制装置包括独立于双网计算机的操作系统的安计算机系统,其单独控制,根据用户对显示器界面上的界面逻辑软开关控制选择是外网显示模式还是内网显示模式,依据相应接收到的外网切换指令、内网切换指令进行相关的安全隔离工作。

[0064] S4、当所述MCU安全控制装置接收到所述内网切换指令时,启动所述双网计算机工作于内网计算机模式,并通过USB接口连接到内网主机,所述显示器显示内网计算机模式下的操作界面。

[0065] 本发明实施例的基于USB接口安全隔离双网计算机的方法,主要采用界面逻辑软开关和支持认证加密的MCU安全控制装置,实现内网、外网的隔离切换,内部实现安全隔离内、外网双网络计算机及独立控制双网络安全隔离的安全计算机系统,构成三机双网方案,完全割裂内网主机。通过独立控制双网络安全隔离的安全计算机系统,实现软件定义的安全共享显示器,支持独立可信加密芯片的切换控制、USB接口方式的认证加密、动态缩放和编辑的高清显示。可实现内、外网在安全隔离的情况下,一体化的显示在一个显示器上,解决了目前内、外网存在的安全隔离失效、显示资源泄密及显示器冗余等问题,确保内、外网工作环境的安全隔离。

[0066] 在一个较佳实施例中,前述步骤S3、所述当MCU安全控制装置接收到所述外网切换指令时,启动所述双网计算机工作于外网计算机模式,所述显示器显示外网计算机模式下的操作界面,包括:

[0067] 当所述MCU安全控制装置接收到所述外网切换指令时,所述MCU安全控制装置控制第一继电器、第二继电器断开连接所述内网主机的USB接口,关闭对应所述内网计算机模式的操作系统和断开对应所述内网计算机模式的存储系统;

[0068] 所述MCU安全控制装置控制第三继电器、第四继电器连通,启动对应所述外网计算机模式的操作系统,建立与外部网络之间的连接,启动对应所述外网计算机模式的存储系统,所述MCU安全控制装置控制电源管理单元复位,并控制所述第一继电器、第二继电器处于断开状态以物理隔离外网计算机模式和内网计算机模式,将所述双网计算机的CPU和RAM存储器清零;

[0069] 所述显示器显示在外网计算机模式下的操作界面。

[0070] 进一步地,前述步骤S4、所述当所述MCU安全控制装置接收到所述内网切换指令时,启动所述双网计算机工作于内网计算机模式,并通过USB接口连接到内网主机,所述显示器显示内网计算机模式下的操作界面,包括:

[0071] 当所述MCU安全控制装置接收到所述内网切换指令时,所述MCU安全控制装置控制第三继电器、第四继电器断开,关闭对应所述外网计算机模式的操作系统,断开所述显示器与外部网络连接的全部接口,断开对应所述外网计算机模式的存储系统;

[0072] 所述MCU安全控制装置控制第一继电器、第二继电器连通,启动对应所述内网计算机模式的操作系统,采用USB存储器硬件加密并与内网主机进行双向认证,待双向认证通过后,通过USB接口连接内网主机,启动对应所述内网计算机模式的存储系统,所述MCU安全控制装置控制电源管理单元复位,并控制所述第三继电器、第四继电器处于断开状态以物理隔离外网计算机模式和内网计算机模式,将所述双网计算机的CPU和RAM存储器清零;

[0073] 所述显示器显示在内网计算机模式下的操作界面。

[0074] 具体地,本发明实施例通过USB存储器实现硬件认证、加密,确保内网资源的安全显示。

[0075] 当从外网切换到内网时,外网计算机模式下的操作系统关机,内网计算机模式下的操作系统启动,智能显示内网涉密应用PC机界面,以及相应的安全操作。之前在外网环境中打开的应用全部关闭,外网接口全部断电和清零,并禁用。而且硬盘是独立的,物理隔离的。内存、CPU也清零了,不存在客体重用的问题。用户重新切换到外网环境时,重新开始操作。

[0076] 当从内网切换到外网时,内网计算机模式下的操作系统关机,外网计算机模式下的操作系统启动,显示外网应用界面。所有内网计算机模式下的内存全部清零,同时内网计算机模式下的专用硬盘数据被清零。由于内网计算机采用独立的硬盘,采用易失性方式,在断电重启后全部清零,且物理隔离的,不存在客体重用和隐蔽信道问题,保证了内网的安全性。

[0077] 以上采用一键切换,断电复位。显示器通过界面逻辑软开关确定的工作模式下,内网、外网完全独立运行。在外网工作模式下,内网信息完全清零;内网工作模式下,外网信息安全清零,这样避免了信息泄露、篡网。

[0078] 较佳地,所述MCU安全控制装置为包括可信加密芯片的MCU,所述可信加密芯片为MCU安全控制装置提供加密服务,具体包括:所述可信加密芯片加电后进行自检,完成状态检查;所述可信加密芯片读取双网计算机的BIOS代码,对所述BIOS代码进行度量,并将度量结果存储在所述可信加密芯片中;所述可信加密芯片转移控制权至双网计算机的CPU,所述可信加密芯片成为一个控制器,为MCU安全控制装置提供加密服务。

[0079] 具体来说,所述MCU安全控制装置采用基于独立可信加密芯片TPCM的继电器系统实现内、外网双网计算机的安全隔离,以及独立控制双网隔离的安全计算机系统(MCU安全控制装置),构成三机双网架构。内、外网计算机具有独立的内、外网存储单元、继电器外围电路和操作系统。分别对应外网和内网,具有独立的存储系统,分别为eMMC1、eMMC2。

[0080] 内网计算机模式下根据界面逻辑软开关的状态,内部由独立的嵌入式MCU安全控制装置实现。具体来说,MCU安全控制装置包括独立可信加密芯片TPCM的MCU嵌入式系统,通过继电器实现外网、内网之间的物理隔离,保证外网计算机模式和内网计算机模式分离且安全可靠。

[0081] MCU安全控制装置检测界面逻辑软开关的状态逻辑,控制相应继电器,实现显示器显示外网显示模式和内网显示模式。当MCU安全控制装置检测到软开关状态在外网模式时,基于eMMC1大容量存储与工作电压控制技术,实现外网系统独立的工作体系,确保外网系统工作独立并硬件隔离,保证安全可靠。当MCU安全控制装置检测到软开关状态在内网模式时,基于eMMC2大容量存储与工作电压控制技术,实现内网系统独立的工作体系,保证内网

系统工作独立并硬件隔离,确保内网系统的安全。

[0082] 外网计算机模式下具有独立的操作系统,以及独立的存储硬盘存储外网操作的结果和数据,可实现PAD功能。并通过外网接口,与外部网络进行互联互通。内网计算机具有独立的操作系统,以及专用存储硬盘用于存储内网操作的结果和数据,并通过USB接口支持双向认证和加密通信,保持与内网PC机互联互通。

[0083] 为了确保内网的计算机显示以及图像、视频资料的安全性,本发明前述实施例基于USB存储器的硬件加密方式,调用存储在独立可信加密芯片中的加密算法,在显示器端与内网机间开展双向认证,有效防止非法客户端或者未授权的用户对内网显示资源进行非法接入与访问。此外,以超映射混沌的图像和视频加密算法对明文进行Logistic置乱操作,打乱像素点的原始位置,使攻击无法识别有用信息,采用超混沌系统对密文进行置乱操作,并采用置乱后密文实现明文加密操作,支持对图像和视频的保护且抵抗各种类型的攻击。

[0084] 较佳地,所述通过所述界面逻辑软开关切换所述显示器进入内网显示模式或外网显示模式,并发送对应所述内网显示模式的内网切换指令或对应所述外网显示模式的外网切换指令,包括:

[0085] 启动所述界面逻辑软开关;

[0086] 依据对所述界面逻辑软开关发出的外网切换指令,所述包括可信加密芯片的MCU发送第一电平信号控制所述显示器启动外网显示模式;

[0087] 在所述外网显示模式下启动对应的显示页面;

[0088] 依据对所述界面逻辑软开关发出的内网切换指令,所述包括可信加密芯片的MCU发送第二电平信号控制所述显示器启动内网显示模式;

[0089] 在所述内网显示模式下启动对应的显示页面。

[0090] 较佳地,在所述第二继电器一端连接双网计算机的USB接口,另一端分别连接双网计算机的CPU和所述MCU安全控制装置。

[0091] 较佳地,当所述显示器为触控显示器显示所述界面逻辑软开关时,分以下情况:

[0092] 所述当MCU安全控制装置接收到所述外网切换指令时,启动所述双网计算机工作于外网计算机模式,所述显示器显示外网计算机模式下的操作界面,包括:

[0093] 接收用户输入的选择外网显示模式的触控指令时,所述显示器切换到外网显示模式,接收所述用户输入的账户和密码验证信息,所述双网计算机切换到外网计算机模式,然后复位重启显示;

[0094] 所述当所述MCU安全控制装置接收到所述内网切换指令时,启动所述双网计算机工作于内网计算机模式,并通过USB接口连接到内网主机,所述显示器显示内网计算机模式下的操作界面,包括:

[0095] 接收用户输入的选择内网显示模式的触控指令时,所述显示器切换到内网显示模式,所述MCU安全控制装置接收所述用户输入的选择内网显示模式的触控指令后,启动对应内网计算机模式的开机画面,然后对所述用户进行身份验证,待所述身份验证通过后再进入所述双网计算机对应内网计算机模式的内网操作系统,通过USB存储器进行硬件加密和双向认证后,与内网主机通过USB接口建立通信连接。

[0096] 较佳地,所述通过USB存储器进行硬件加密和双向认证后,与内网主机通过USB接口建立通信连接,包括:

[0097] 在所述内网计算机模式下,所述显示器端通过USB存储器存储的内网主机公钥和自身私钥,调用存储在所述可信加密芯片中的加密算法,与内网主机间进行一对一认证;所述加密算法为超映射混沌的图像加密算法。

[0098] 本发明实施例的基于USB接口安全隔离双网计算机的方法,主要采用界面逻辑的软开关和独立可信的硬方式支持认证加密,实现内网、外网的隔离切换,内部实现物理隔离的内、外网双网络计算机,以及独立控制双网络物理隔离的MCU安全控制装置,构成三机双网架构;通过独立控制的MCU安全控制装置,实现软件定义的安全共享显示器,支持独立可信加密芯片的切换控制、USB接口方式的认证加密、动态缩放和编辑的高清显示。通过实施本发明的上述技术方案,解决目前内外网存在的安全隔离失效、显示资源泄密和显示器冗余等问题,确保内外网工作环境的安全隔离。本发明实施例有效解决现有双网计算机办公应用场景下隔离方法存在的显示资源泄密、显示器冗余和隐蔽信道存在等的安全隐患问题,该显示器采用三机双网的隔离方案,完全割裂内网系统,达到内外网双网办公的安全需要,符合国家标准的安全技术要求。

[0099] 此外,在内网显示模式下,显示器具有软件定义的智能显示终端功能,实现内网智能显示。显示器实现智能终端功能,软件定义的安全共享显示,且通过USB接口将内网系统与显示器连接,将内网的PC机显示加密后输出到显示器上,支持USB接口动态可缩放和编辑的高清显示。同时,通过USB实现智能显示终端下达命令从而操作编辑内网系统内容。该部分的实现均是在内网环境内操作,与外网环境完全物理隔离,符合访问授权与拒绝、不可旁路、客体无法重用的安全要求。主要实现的内网智能显示功能包括安全登录功能、智能内网显示功能、缩放显示功能、内网显示控制编辑功能。前述功能具体描述如下:

[0100] 安全登录功能:内网智能显示安全登录密码限制不可信用户的登录。当用户将拨动开关置于内网环境时,开机后,系统通过摄像头获取使用者人脸数据,并自动识别,通过与本地合法用户数据比对获取对应的权限。如果用户合法并权限匹配,则可显示内网系统内容;否则不能进入显示界面。

[0101] 智能内网显示功能:通过USB接口实现具有图像传输及音频传输的功能,将内网桌面智能的显示到显示器。

[0102] 双向认证功能:显示器端通过USB key以其存储的内网机公钥和自身的私钥,调用存储在独立可信加密芯片中的加密算法,与内网机间进行一对一认证,相互验证显示器端的身份和内网机的身份,防止非法客户端或者未授权的用户对内网显示资源进行非法接入与访问。

[0103] 加密传输功能:为了确保内网计算机模式下的PC机显示及视频安全性,通过超映射混沌的图像加密算法对明文图像进行Logistic置乱操作,打乱像素点的原始位置,使攻击无法识别有用信息,采用超混沌系统对密文进行置乱操作,并采用置乱后密文图像实现明文图像加密操作。支持对图像的保护且抵抗各种类型的攻击。

[0104] 缩放显示功能:通过识别用户手势,进行图像的缩放。当用户将两手指滑动拉开距离,图像进行放大,图像可放大4倍,当用户将两手指距离缩小时,可使图像缩小直至原始大小;支持双击进行以触点为中心进行图像放大及恢复。

[0105] 内网显示控制编辑功能:通过USB接口将智能显示终端的命令下达至内网系统从而达到完全操作内网系统的功能,可进行如文件的打开、关闭、编写等编辑操作。

[0106] 现在结合实际的应用实施例来说明本发明实施例的基于USB接口安全隔离双网计算机的方法,主要过程描述如下:

[0107] (1) 安装显示器及双网计算机。

[0108] 首先需要将显示器的相应内、外网操作系统安全成功,物理隔离控制系统安装成功,系统驱动安装成功,显示器能正常工作。

[0109] 其次,将双网计算机部署于涉及内、外网双网办公的环境,相应初始化参数及地址等配置完成。此时,双网计算机仅通过USB接口与内网主机(PC机)连接;可通过WIFI&BT,USB Type-C与外网连接。

[0110] (2) 显示器和双网计算机上电开机

[0111] 主要有显示器启动、隔离控制系统启动、系统初始化成功。

[0112] (3) 显示模式切换选择

[0113] 通过界面逻辑软开关进行显示器外网显示模式和内网显示模式的切换。

[0114] 如图2所示,当显示器100成功启动后,根据双网办公需要,用户触摸界面逻辑软开关101选择需要的内网显示模式和外网显示模式。两种模式通过界面逻辑软开关控制,进行切换。

[0115] 如图3所示,在本发明实施例的实现基于USB接口安全隔离双网计算机的方法的硬件结构中,双网计算机与内网主机通过USB接口连接。双网计算机装置包括:处理器、PMU复位单元、RAM、显示器、MCU安全控制装置、第一继电器、第二继电器、第三继电器、第四继电器、内网存储器eMMC2、外网存储器eMMC1、辅助电子装置、音频控制按键(+、-)、电源输入DC IN、开机键、耳机、复位及TF卡槽等。其中处理器包括CPU,还可以包括GPU(图像处理单元)。PMU复位单元作为电源管理单元,管理电源复位。MCU安全控制装置包括可信加密芯片的MCU,可以是独立可信加密芯片TPCM。MCU安全控制装置的控制流程如下:

[0116] 独立可信加密芯片TPCM首先加电,加电后进行自检,完成状态检查;TPCM读取BIOS代码、对BIOS进行度量,度量结果存储在TPCM中;TPCM将控制权交给CPU,TPCM变为一个控制设备,为MCU检测过程提供密码服务或者可信服务。

[0117] 独立可信加密芯片接收界面切换软开关发出的内、外网切换指令,外网切换指令导向外网显示模式,内网切换指令导向内网显示模式,这里的内网显示模式可以是智能化的,能够主动的判断和输出显示信息。

[0118] 外网计算机模式时,MCU安全控制装置控制第一继电器、第二继电器断开内网设备的连接接口(USB接口),关闭对应内网计算机模式的操作系统,断开内网存储器eMMC2;第三继电器、第四继电器连通,启动对应外网计算机模式的操作系统,恢复外网计算机模式的操作系统,网络外部连接WIFI&BT,USB Type-C及存储器(eMMC1、TF);MCU安全控制装置控制PMU复位及内、外网继电器保证为断电模式,完全物理隔离,CPU和RAM全部清零。

[0119] 内网显示模式时,MCU安全控制装置控制第三继电器、第四继电器断开,关闭对应外网计算机模式的操作系统,断开显示器与外网的所有接口,如外部网络WIFI&BT,USB Type-C及存储器(eMMC1、TF);第一继电器、第二继电器2连通,重启对应内网计算机模式的操作系统,基于USB存储器加密和双向认证完成后,恢复与内网主机连接接口(USB接口)及存储器eMMC2;MCU安全控制装置控制PMU复位及内、外网继电器保证为断电模式,完全物理隔离,CPU和RAM全部清零。

[0120] 当MCU安全控制装置接收到界面切换软开关指令变化时,立即进行模式切换控制;并对双网计算机进行复位重启。

[0121] 本发明实施例的界面切换软开关切换流程如图4所示:

[0122] 显示器上电,当用户触摸软开关为外网时,显示器需要切换到外网显示模式。此时遵循的流程为:

[0123] S11、上电,Android2开机画面启动;

[0124] S12、用户触控界面软切换开关;

[0125] S13、接收用户输入外网用户名密码及切换口令,并验证;

[0126] S14、切换到外网模式,复位重启显示。

[0127] 当接收到用户触摸界面切换软开关选择内网显示模式时,显示器需要切换到内网显示模式。此时遵循的流程为:

[0128] 启动内网显示模式对应的操作系统如Android2,弹出启动页面,MCU安全控制装置接收界面切换软开关发出的内网切换指令,Android2开机画面启动,等待通过面部识别进行身份验证,通过后进入内网Windows操作系统,并执行基于USB存储器的硬件加密和双向认证,确保内网显示资源安全。如果收到界面切换软开关的指令变化时,再切换到外网显示模式,复位重启显示器外网系统。具体还可以是如图5所示那样,启动界面切换软开关,通过I2C总线发送外网切换指令或内网切换指令至可行加密MCU(也就是可信加密芯片的MCU),可信加密芯片的MCU发送高电平启动外网模式,然后相应启动外网模式对应的页面,之后双网计算机检测到检测端口出现高电平,启动外网计算机模式下的开机画面,进行用户校验或者认证,进入外网计算机模式。而当发送低电平时,启动内网显示模式,也是启动内网计算机模式下的开机画面,用户校验,然后进入内网计算机模式。分别在收到切换指令后,复位重启。

[0129] (4) 根据用户选择的界面切换软开关切换对应的显示模式进行智能显示。

[0130] 假设用户先选择了外网显示模式(也可以先选择内网模式,本质上没有区别),则显示器启动外网显示模式对应的操作系统,显示器工作在外网显示模式。该模式下,结合如图3和图4,工作方式为:

[0131] 1) CPU:CPU&GPU正常工作,用于计算、控制及显示处理;

[0132] 2) 内存:RAM正常工作,用于运行应用的缓存;

[0133] 3) 存储:eMMC1正常工作,用于Android1系统运行及存储,断开eMMC2,TF卡正常工作,用于扩充存储空间;

[0134] 4) 网络:WIFI及TYPE-C正常工作,用于连接外网,TYPE-C需外接TYPE-C转RJ45转接线,支持千兆网速;

[0135] 5) 显示:显示屏进行PAD显示,显示Android1界面,断开与PC连接的USB接口;

[0136] 6) 触摸:触摸屏进行PAD触摸操作。

[0137] 假设用户先选择了内网显示模式,则显示器启动外网操作系统,显示器工作在内网显示模式。该模式下,结合如图3和图4,工作方式为:

[0138] 1) CPU:CPU&GPU正常工作,用于图形计算的内网PC机界面显示处理;

[0139] 2) 内存:RAM正常工作,用于运行应用的缓存;

[0140] 3) 存储:eMMC2正常工作,用于Android2系统运行及存储,断开eMMC1、TF,及外网所

有对外接口；

[0141] 4) 显示与编辑：内网PC主机通过USB接口，连接到显示器的USB输入端口，通过硬件加密传输和双向认证后，显示器进行显示处理，显示Windows界面；用户登录认证、自主动态缩放、编辑。

[0142] 5) 触摸：内网主机(PC主机)通过USB接口进行触摸事件通讯。

[0143] 至此，本实施例工作过程完毕。

[0144] 请参见图6，本发明实施例对应上述基于USB接口安全隔离双网计算机的方法还提供一种基于USB接口安全隔离双网计算机的装置，包括：

[0145] 显示模块10，控制显示器显示界面逻辑软开关；

[0146] 切换模块20，用于通过所述界面逻辑软开关切换所述显示器进入内网显示模式或外网显示模式，并发送对应所述内网显示模式的内网切换指令或对应所述外网显示模式的外网切换指令；

[0147] 外网计算机模式工作模块30，用于当MCU安全控制装置接收到所述外网切换指令时，启动所述双网计算机工作于外网计算机模式，所述显示器显示外网计算机模式下的操作界面；

[0148] 内网计算机模式工作模块40，用于当所述MCU安全控制装置接收到所述内网切换指令时，启动所述双网计算机工作于内网计算机模式，并通过USB接口连接到内网主机，所述显示器显示内网计算机模式下的操作界面。

[0149] 其中，外网计算机模式工作模块30，包括：

[0150] 第一外网显示模式处理单元，用于当所述MCU安全控制装置接收到所述外网切换指令时，所述MCU安全控制装置控制第一继电器、第二继电器断开连接所述内网主机的USB接口，关闭对应所述内网计算机模式的操作系统和断开对应所述内网计算机模式的存储系统；

[0151] 第二外网显示模式处理单元，用于所述MCU安全控制装置控制第三继电器、第四继电器连通，启动对应所述外网计算机模式的操作系统，建立与外部网络之间的连接，启动对应所述外网计算机模式的存储系统，所述MCU安全控制装置控制电源管理单元复位，并控制所述第一继电器、第二继电器处于断开状态以物理隔离外网计算机模式和内网计算机模式，将所述双网计算机的CPU和RAM存储器清零；

[0152] 外网操作界面显示单元，用于所述显示器显示在外网计算机模式下的操作界面。

[0153] 进一步地，内网计算机模式工作模块40，包括：

[0154] 第一内网显示模式处理单元，用于当所述MCU安全控制装置接收到所述内网切换指令时，所述MCU安全控制装置控制第三继电器、第四继电器断开，关闭对应所述外网计算机模式的操作系统，断开所述显示器与外部网络连接的全部接口，断开对应所述外网计算机模式的存储系统；

[0155] 第二内网显示模式处理单元，用于所述MCU安全控制装置控制第一继电器、第二继电器连通，启动对应所述内网计算机模式的操作系统，采用USB存储器硬件加密并与内网主机进行双向认证，待双向认证通过后，通过USB接口连接内网主机，启动对应所述内网计算机模式的存储系统，所述MCU安全控制装置控制电源管理单元复位，并控制所述第三继电器、第四继电器处于断开状态以物理隔离外网计算机模式和内网计算机模式，将所述双网

计算机的CPU和RAM存储器清零；

[0156] 内网操作界面显示单元，用于所述显示器显示在内网计算机模式下的操作界面。

[0157] 请参见图7，本发明还提供对应上述基于USB接口安全隔离双网计算机的方法还提供一种基于USB接口安全隔离双网计算机的系统，包括：双网计算机200，USB接口203，内网主机300。双网计算机200内包括MCU安全控制装置202及显示器201。MCU安全控制装置202独立控制，用于实现双网计算机200外网、内网之间的安全隔离。上述系统采用前述基于USB接口安全隔离双网计算机的方法。

[0158] 需要明确的是，本发明并不局限于上文所描述并在图中示出的特定配置和处理。为了简明起见，这里省略了对已知方法的详细描述。在上述实施例中，描述和示出了若干具体的步骤作为示例。但是，本发明的方法过程并不限于所描述和示出的具体步骤，本领域的技术人员可以在领会本发明的精神后，作出各种改变、修改和添加，或者改变步骤之间的顺序。

[0159] 以上所述的结构框图中所示的功能块可以实现为硬件、软件、固件或者它们的组合。当以硬件方式实现时，其可以例如是电子电路、专用集成电路(ASIC)、适当的固件、插件、功能卡等等。当以软件方式实现时，本发明的元素是被用于执行所需任务的程序或者代码段。程序或者代码段可以存储在机器可读介质中，或者通过载波中携带的数据信号在传输介质或者通信链路上传送。“机器可读介质”可以包括能够存储或传输信息的任何介质。机器可读介质的例子包括电子电路、半导体存储器设备、ROM、闪存、可擦除ROM(EROM)、软盘、CD-ROM、光盘、硬盘、光纤介质、射频(RF)链路，等等。代码段可以经由诸如因特网、内联网等的计算机网络被下载。

[0160] 还需要说明的是，本发明中提及的示例性实施例，基于一系列的步骤或者装置描述一些方法或系统。但是，本发明不局限于上述步骤的顺序，也就是说，可以按照实施例中提及的顺序执行步骤，也可以不同于实施例中的顺序，或者若干步骤同时执行。

[0161] 以上所述，仅为本发明的具体实施方式，所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，上述描述的系统、模块和单元的具体工作过程，可以参考前述方法实施例中的对应过程，在此不再赘述。应理解，本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到各种等效的修改或替换，这些修改或替换都应涵盖在本发明的保护范围之内。

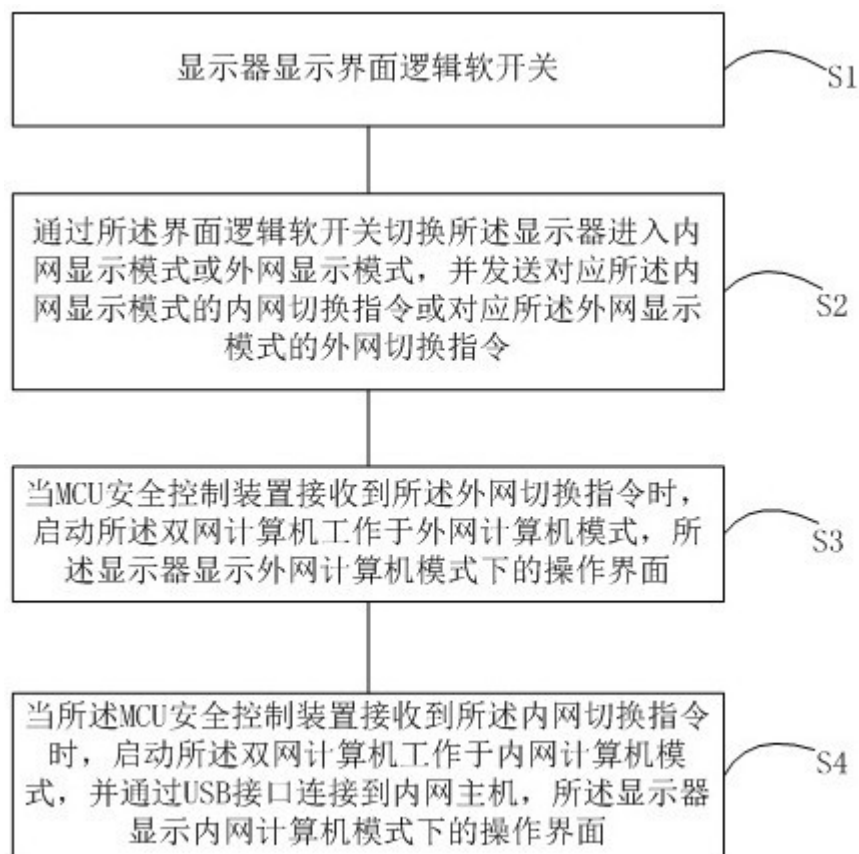


图1

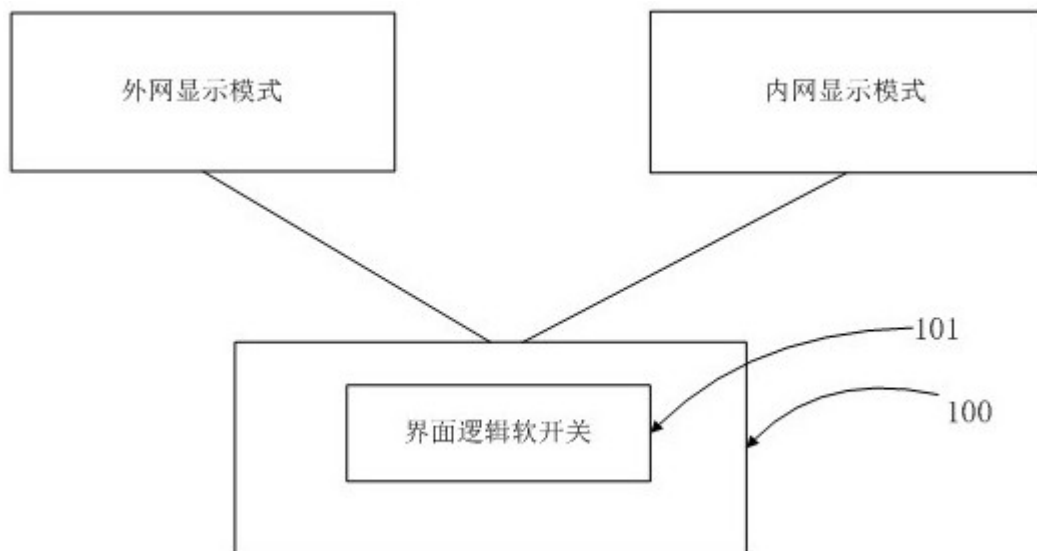


图2

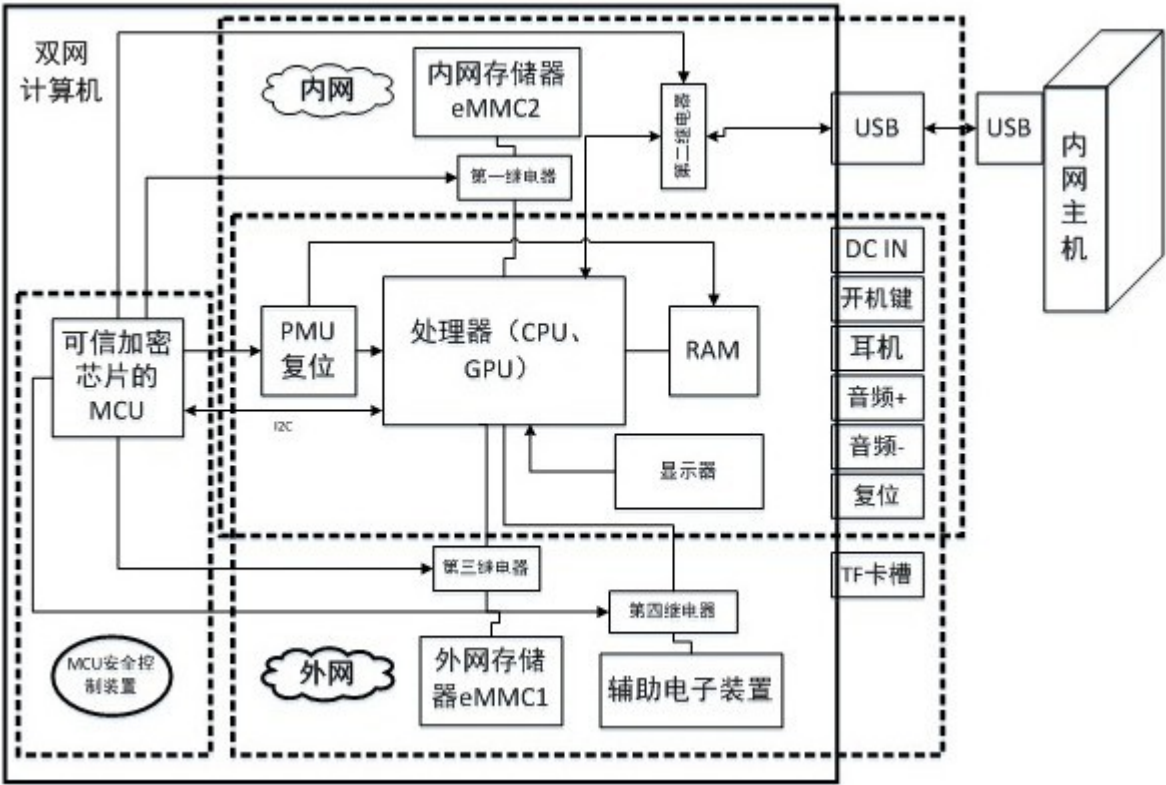


图3

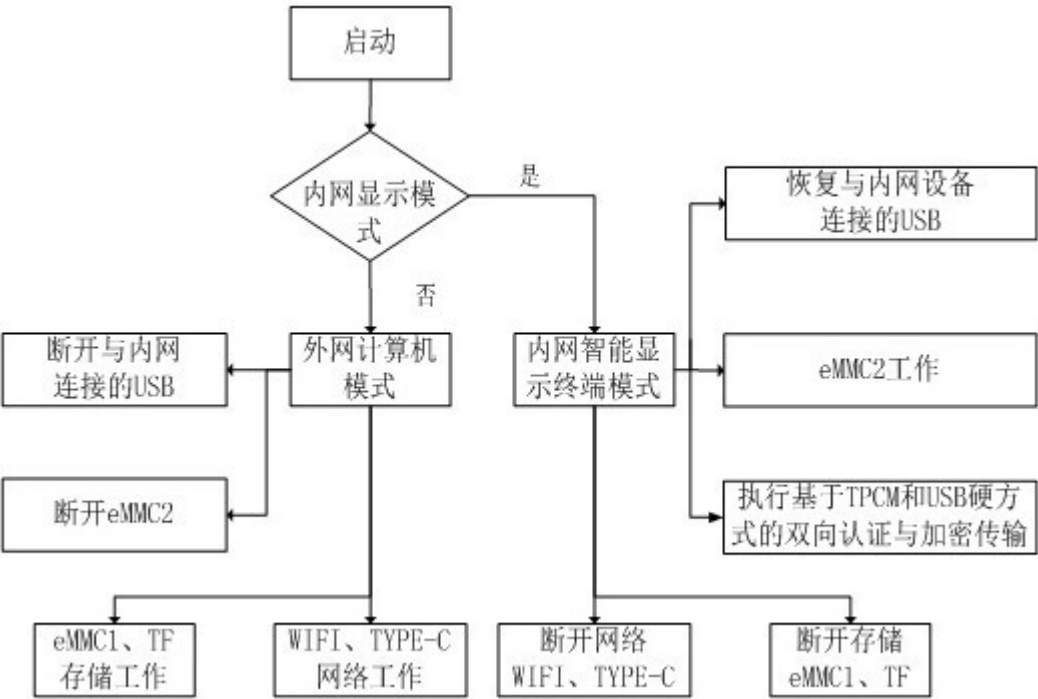


图4

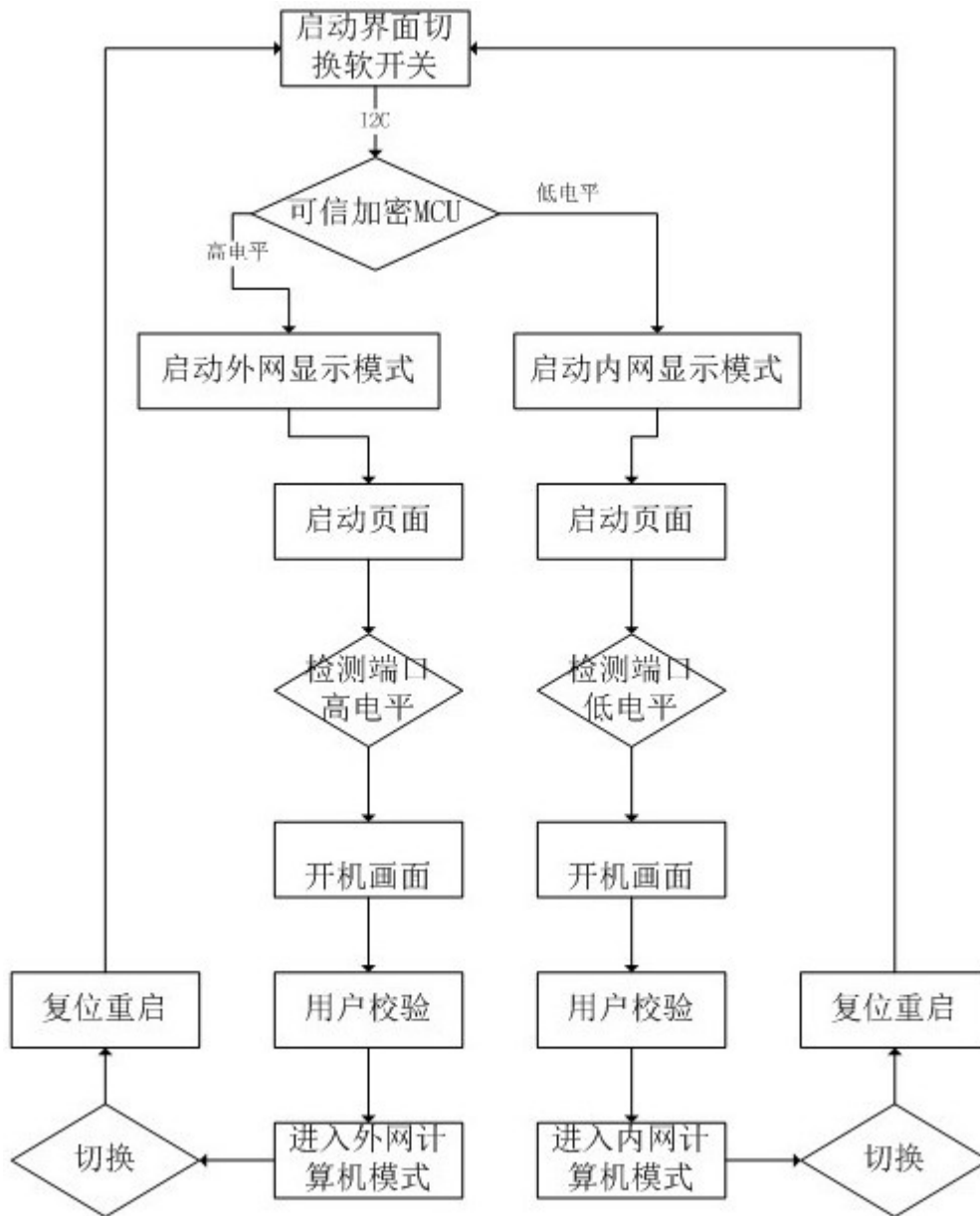


图5

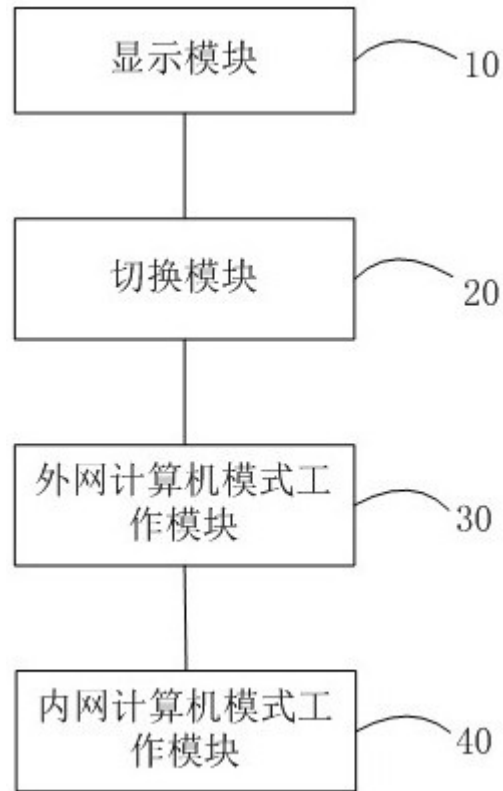


图6

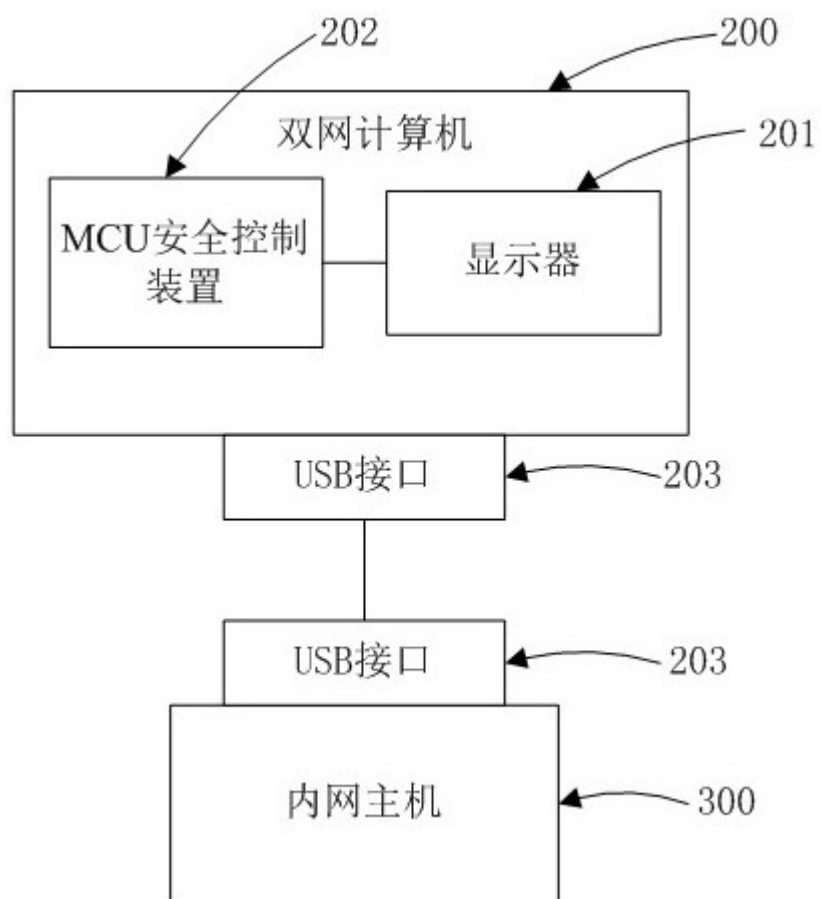


图7