(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2020 年 5 月 7 日 (07.05.2020)

WIPO | PCT

(10) 国际公布号
WO 2020/087782 A1

(51) 国际专利分类号:
*H04L 29/06* (2006.01) *G06F 21/85* (2013.01)
*G06F 21/74* (2013.01)

(21) 国际申请号: PCT/CN2019/072030

(22) 国际申请日: 2019 年 1 月 16 日 (16.01.2019)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201811264762.7 2018年10月29日 (29.10.2018) CN

(71) 申请人: 北京博衍思创信息科技有限公司(**BEIJING BEYONDINFO TECHNOLOGY CO., LTD.**) [CN/CN]; 中国北京市东城区藏经馆胡同17号1幢1291室闫瑞珍, Beijing 100020 (CN)。

(72) 发明人: 杜华 (**DU, Hua**); 中国北京市东城区藏经馆胡同17号1幢1291室闫瑞珍, Beijing 100020 (CN)。 艾伟(**AI, Wei**); 中国北京市东城区藏经馆胡同17号1幢1291室闫瑞珍, Beijing 100020 (CN)。 蔡镇河 (**CAI, Zhenhe**); 中国北京市东城区藏经馆胡同17号1幢1291室闫瑞珍, Beijing 100020 (CN)。 张昊(**ZHANG, Hao**); 中国北京市东城区藏经馆胡同17号1幢1291室闫瑞珍, Beijing 100020 (CN)。

(74) 代理人: 北京清诚知识产权代理有限公司(**BEIJING CHINGCHENG INTELLECTUAL PROPERTY AGENCY LTD.**); 中国北京市朝阳区北苑路168号中安盛业大厦1405号乔东峰, Beijing 100101 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS,

(54) **Title:** EXTERNAL TERMINAL PROTECTION DEVICE AND PROTECTION SYSTEM FOR DATA TRAFFIC CONTROL

(54) 发明名称: 一种数据流量控制的外接式终端防护设备及防护系统

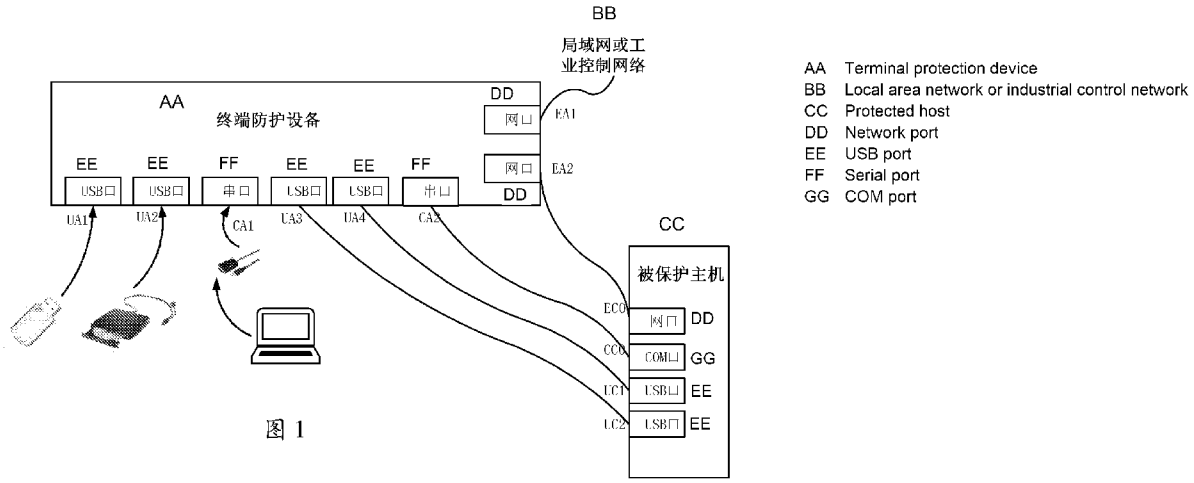



图 1

(57) **Abstract:** Disclosed are an external terminal protection device for data traffic control and a corresponding protection system. The external terminal protection device comprises: an interface control module for providing multiple data interfaces for connecting a protected host and one or more external devices respectively; and a system control module for monitoring in real time the data transmission state of each data interface in the interface control module, and performing traffic control on the data of each data interface. The invention can achieve the functions of performing protocol filtering and auditing on various types of data traffic without installing traffic monitoring and security protection software on a protected host, thereby realizing the effects of low-latency network auditing and high-reliability protocol filtering, and comprehensively eliminating the potential security hazards such as Trojan virus implantation and traffic anomaly that are possibly generated by each interface.

WO 2020/087782 A1

[见续页]

JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

**(84) 指定国**(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

**本国际公布**:

— 包括国际检索报告(条约第21条(3))。

**(57) 摘要**：本发明公开一种数据流量控制的外接式终端防护设备及相应的防护系统，其中所述外接式终端防护设备包括：接口控制模块，用于提供多个数据接口，分别连接被保护主机及一个或多个外部设备；系统控制模块，用于实时监测所述接口控制模块中各个数据接口的数据传输状态，并对各个数据接口的数据进行流量控制。本发明无需在被保护主机上安装流量监控和安全防护软件即可达到对各类型的数据流量进行协议过滤和审计的功能，进而实现低延迟网络审计与高可靠性协议过滤的效果，全面解决了由各个接口可能产生的病毒木马植入以及流量异常等安全隐患。

# 一种数据流量控制的外接式终端防护设备及防护系统

## 技术领域

本发明属于计算机安全技术领域，尤其涉及一种数据流量控制的外接式终端防护设备及相应的防护系统。

## 背景技术

近些年，计算机及网络技术获得高速发展，从而大大促进了网络的普及，当人们日益享受这网络流量带来的便利的同时，也为生产/生活中人们所使用的计算机中的数据流量安全带来了新的威胁，例如常见的有流量攻击、黑客窃取、非授权访问、冒充合法用户、破坏数据完整性、干扰系统正常运行、利用网络传播病毒和中间人窃听等等。

解决内网计算机网络流量管控和信息安全问题的技术手段已有很多，例如在主机中安装和使用流量控制软件、防火墙、防病毒、入侵检测系统等网络安全产品，但采取上述措施后各种网络安全事件仍频频发生。据统计，计算机犯罪的70%是由内部人员非法使用主机等关键资源造成的，真正来自外部的威胁只有30%，内部人员在使用主机时缺乏安全意识，又位于防火墙后端，接入各种外部设备不规范，被植入木马后门，从而导致数据流量异常甚至网络瘫痪，以及系统的误操作或者蓄意的破坏，都会对机关、企事业单位等造成恶劣的影响甚至重大损失。

同时，对于某些特殊设备，如配备有特殊软件控制的主机，某些工业领域的工程师站/工作员站的设备，这些主机/设备往往由于系统特殊性，市面上没有此类系统适配的网络流量控制软件和安全防护软件，或是由于安装流量控制软件或安全类软件容易导致主机原有软件出现兼容性问题，甚至性能受到影响。另外这些工程师站/工作员站的主机上线后基本不会对操作系统进行升级，即使安装流量监控及安全类软件后也往往不及时更新防恶意代码软件版本和恶意代码库，起不到全面的流量控制、网络数据过滤/审计和安全防护作用。

## 发明内容

基于此，本发明提供一种解决上述问题的一种用于数据流量控制的外接式终端防护设备及防护系统，以实现对被保护主机的各个接口的接管，确保使用被保护主机的 USB 接口或串口设备必须通过外接式终端防护设备完成，从而无需在被保护主机上安装安全防护软件即可到达对被保护主机 USB 接口或串口进行防护的目的。

第一方面，本申请提供一种用于数据流量控制的外接式终端防护设备，其包括：接口控制模块，用于提供多个数据接口分别连接被保护主机及一个或多个外部设备；系统控制板，用于实时监测所述接口控制模块中各个数据接口的数据传输状态，并对各个数据接口的数据进行流量控制。

可选地，所述用于数据流量控制的外接式终端防护设备其外接于所述被保护主机上，并将所述接口控制模块与被保护主机的各个数据接口按照类型对应连接。

可选地，所述接口控制模块的多个数据接口进一步包括对内接口、对外接口，以及转发接口；所述对内接口用于与被保护主机的各个数据接口按照接口类型对应连接；所述对外接口用于接入一个或多个外部设备，所述外部设备适于通过所述外接式终端防护设备与被保护主机进行数据交互；所述转发接口用于将各接口类型的数据流量转发给所述系统控制模块。

可选地，所述接口控制模块中进一步包含硬件控制逻辑，用于实现接口控制模块内部各个接口之间物理线路的通断。

可选地，所述系统控制模块进一步包括对外部设备的安全鉴权，以确认所述外部设备是否为许可接入设备。

可选地，当所述系统控制模块对外部设备的安全鉴权后，确认所述外部设备不是许可接入设备时，通过总线通知接口控制模块禁止所述外部设备的数据传输；所述接口控制模块中的硬件控制逻辑保持断开所述

外部设备接入的对外接口与转发接口的物理线路的状态，从而对所述外部设备接入后的数据传输进行过滤禁止。

可选地，当所述系统控制模块对外部设备的安全鉴权后，确认所述外部设备为许可接入设备时，通过总线通知接口控制模块允许所述外部设备的数据传输；所述接口控制模块中的硬件控制逻辑连通所述外部设备接入的对外接口与转发接口的物理线路。

可选地，所述数据接口进一步包括一个或多个网络接口；所述接口控制模块中进一步包含交换芯片，用于获取各个网络接口的寄存器状态，设置接口控制模块的工作模式；所述系统控制模块监测所述交换芯片中网络接口寄存器状态，从而实时获得接口控制模块中各网络接口的连接状态。

可选地，当所述系统控制模块监测到存在一个或多个网络接口的连接状态发生变化时，对相应网络接口状态变化发出告警提示。

可选地，所述系统控制模块通过所述交换芯片设置接口控制模块为流量镜像模式，通过所述接口控制模块中的转发接口，对所述接口控制模块中的对内接口和/或对外接口做流量镜像。

可选地，所述系统控制模块通过所述交换芯片设置接口控制模块为网络协议过滤模式，通过所述接口控制模块中的转发接口，对所述接口控制模块中的对内接口和对外接口之间的数据流量做网络协议过滤。

可选地，所述系统控制模块进一步设定有安全策略，对通过所述接口控制模块接入的外部设备传输进来的数据进行安全性检测；所述接口控制模块将通过安全策略过滤后的数据流量转发给所述被保护主机。

可选地，所述系统控制模块可以是基于 ARM 或 x86 的控制模块。

第二方面，本申请提供一种用于数据流量控制的防护系统，包括：

一个或多个外部设备，所述外部设备适于通过所述外接式终端防护设备与被保护主机进行数据交互；

被保护主机；以及

如上所述的外接式终端防护设备，

其中，所述外接式终端防护设备外接于所述被保护主机上，使得所

述一个或多个外部设备通过所述外接式终端防护设备与所述被保护主机进行接口通信。

通过本发明上述技术方案，至少具有如下一种或多种技术效果：可以实现对被保护主机各个数据接口的接管，确保使用被保护主机各个接口的数据通信都通过外接式的终端完成，从而无需在被保护主机上安装流量监控和安全防护软件即可达到对被保护主机各个类型的数据流量进行协议过滤和审计的功能，进而实现低延迟网络审计与高可靠性协议过滤的效果，同时进一步起到安全防护的目的，并且极大降低了整体系统的网络安全风险，全面解决了由各个接口可能产生的病毒木马植入以及流量异常等安全隐患。

## 附图说明

图 1 为本发明涉及的用于数据流量控制的防护系统的应用场景；

图 2 为本发明涉及的外接式终端防护设备内部构造示意图；

图 3 为本发明涉及的外接式终端防护设备的 USB 数据流量控制的实施例；

图 4 为本发明涉及的外接式终端防护设备的串口数据流量控制的实施例；

图 5 为本发明涉及的外接式终端防护设备的网络数据流量控制实施例；

图 6 为本发明涉及的用于数据流量控制的防护系统的网络部署实施例。

## 具体实施方式

下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了

能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

本文中术语“和/或”，仅仅是一种描述关联对象的关联关系，表示可以存在三种关系，例如，A 和/或 B，可以表示：单独存在 A，同时存在 A 和 B，单独存在 B 这三种情况。另外，本文中字符“/”，一般表示前后关联对象是一种“或”的关系。

本发明提出的数据流量控制的外接式终端防护设备包括接口控制模块和系统控制模块。接口控制模块用于提供多个数据接口分别连接被保护主机及一个或多个外部设备。系统控制模块，用于实时监测所述接口控制模块中各个数据接口的数据传输状态，并对各个数据接口的数据进行流量控制。可见，本发明提供了一种硬件方式的终端防护设备，无需在被保护主机上安装流量监控和安全防护软件即可达到对各类型的数据流量进行协议过滤和审计的功能，进而实现低延迟网络审计与高可靠性协议过滤的效果，全面解决了由各个接口可能产生的病毒木马植入以及流量异常等安全隐患。

需要注意的是，本发明中所称的“模块”为硬件模块，即由电路、数据处理装置、存储器、缓存器等有形电子元件构成的硬件模块。本发明中的接口控制模块和系统控制模块可以是物理上或功能上独立的元件组合，也可以是物理上或功能上整合在一起的整体元件组合。例如，作为一种实施方式，接口控制模块由接口控制板构成，系统控制模块由系统控制板构成，接口控制板和系统控制板均为集成有电子元件的电路板，二者之间通过总线连接。而在其他的实施方式中，接口控制模块和系统控制模块亦可以集成在一个电路板上。因此，本发明的关键在于接口控制模块和系统控制模块之间的控制关系，但不限于组成各自模块的电子元件在空间上或物理连接上的组合方式。

实施例

图 1 所示为本发明涉及的数据流量控制的防护系统的一个实施例的

应用场景。

如图 1 所示，为了对被保护主机的各个数据流量进行控制，需要对被保护主机各个接口进行接管，由此本发明的外接式终端防护设备上设置有与被保护主机各个接口类型对应的对内接口，同时另外还提供类型相应的对外接口，各对内接口用于连接被保护主机，对外接口用于连接需要与被保护主机进行数据交互的外部设备。所述终端防护设备外接于被保护主机上，将需要防护的被保护主机上各个接口（如 USB 口的 UC1、UC2，COM 口的 CC0、网口 EC0）通过各种类型的连接线连接到自身对应类型的对内接口上，比如将被保护主机的接口 UC1 与 UC2 分别连接到外接式终端防护设备的对内 USB 口 UA4 和 UA3 上，将串口 CC0 连接到对内串口 CA2 上，网口 EC0 连接到对内网口 EA2 上。而各种外部设备（U 盘、光驱、串口连接设备等）全部接到所述外接式终端防护设备上各外部接口上，通过外接式终端防护设备才能与被保护主机进行数据通信，从而实现外部设备与被保护主机之间数据流量的控制，比如外部 U 盘设备通过所述外接式终端防护设备的对外接口 UA1 接入，USB 光驱通过对外接口 UA2 接入，串口连接设备通过对外接口 CA1 接入。U 盘、USB 光驱以及串口连接设备这些外部设备需要与被保护主机进行数据通信，都不能直接接入到被保护主机上，必须通过所述外接式终端防护设备相应的对外接口转接通信。

这样，经由外部设备传输的数据，需要首先经过外接式终端防护设备的数据流量控制，从而可以对数据传输进行协议过滤、流量镜像、流量审计及安全性检测等控制。

图 2 所示为本发明的外接式终端防护设备内部构造的实施例。

该实施例中，所述外接式终端防护设备主要由接口控制板 A 和系统控制板 B 构成，接口控制板 A 支持 USB、串口及网络通信，其与系统控制板 B 之间通过控制连接线 E 连接（例如总线），用于控制接口控制板 A 上各个接口，比如 USB 接口、串口及网口的不同工作模式，进而实现对各种外部设备的接入进行安全控制的功能。系统控制板 A 可实现对各个接口的工作模式控制，工作模式包括可用、不可用、网络协议过

滤、流量镜像或流量审计等，但本发明不限于具体的工作模式控制类型。系统控制板 B 可通过 I2C 或 SPI 接口与接口控制板 A 相连，但本发明不限于此类具体的控制连接接口。接口控制板通过各个类型的转发接口（数据连接 F 中的串口、网口、USB 等）将对外接口和对内接口中传输的数据流量转发给系统控制板。

所述外接式终端防护设备中的接口控制板还可接入内部存储器，如图 2 中硬件存储 D，用于转存所述接口控制板上各接口间交换的数据。

当有外部设备通过接口控制板上各种类型的对外接口接入时，系统控制板按照设定的安全策略对接口控制板上不同类型的接口进行安全鉴权，以确认所述外部设备是否为许可接入设备。

在此实施例中，外接式终端防护设备所实现的的安全功能包括但不限于，管理员预先对外接式终端防护设备进行权限设置和安全策略设定；安全策略包括但不限于：使能数据导入（如 USB 接口）、使能数据导出（如 USB 接口）、USB 接入设备限制（如基于 USB 设备的 Vendor ID，即供应商识别码，和/或 Product ID，即产品识别码）、数据导入杀毒策略、数据导出黑白名单控制策略、数据导出格式控制策略、使能串口接入策略、USB 接口插入保护、使能网络通信审计、使能防火墙功能、设置串口命令黑白名单等。

在一种优选的实施方式中，安全策略包括：管理员在设定好各个安全策略后，相关的这些安全策略将被所述外接式终端防护设备逐一执行。

在一种优选的实施方式中，安全策略包括：管理员还控制所述外接式终端防护设备是否进入监控保护模式，此模式将监控与被保护主机间的连接，异常情况下将进行告警。

在一种优选的实施方式中，安全策略包括：当需要记录异常告警或接口访问情况以备后续管理员查询时，内部存储器还用于进一步记录所述告警信息或接口访问日志信息。

在一种优选的实施方式中，所述接口控制板进一步包含硬件控制逻辑，用于实现接口控制板内部各个接口之间物理线路的通断。当所述系统控制板通过安全策略对外部设备进行安全鉴权后，确认所述外部设备

不是许可接入设备时，通过总线通知接口控制板中的硬件控制逻辑保持断开所述外部设备接入的对外接口与转发接口的物理线路的状态，从而对所述外部设备接入后的数据传输进行过滤禁止。当所述系统控制板对外部设备的安全鉴权后，确认所述外部设备为许可接入设备时，通过总线通知接口控制板允许所述外部设备的数据传输；所述接口控制板中的硬件控制逻辑连通所述外部设备接入的对外接口与转发接口的物理线路。

图 3 所示，本发明所涉及的外接式终端防护设备内部一种 USB 数据流量控制的实施例。

接口控制板进一步包含硬件控制逻辑，用于实现接口控制板内部各个接口之间物理线路的通断。接口控制板的对内 USB 接口 UA3 与被保护主机的 USB 口连接，转发接口 UB1、UB2 分别接入系统控制板的 USB 接口 UD3 和 UD4，对外 USB 接口 UA1 插入待接入的外部设备 U 盘或移动存储介质，UB3 插入用于转存数据的内部 USB 存储，CTRL 口作为总线接口连接系统控制板的控制接口。

当外部设备 U 盘中的数据需要导入到被保护主机时，系统控制板通过总线传输控制指令通知接口控制板，以控制所述硬件控制逻辑连通 UA1 与 UB1 之间的物理线路，将 U 盘中的数据 Data1 拷入系统控制板的缓存中，在此期间硬件控制逻辑保持转发接口 UB1（与系统控制板连接）与 UB3（与内部 USB 存储连接）的物理线路处于断开状态，同时保持对内 USB 接口 UA3（与被保护主机连接）与 UB3 的物理线路处于断开状态。

硬件控制逻辑之后断开 UA1 与 UB1 之间物理线路的开关，接通 UB1 与 UB3 之间的物理线路，将 UB3 内部 USB 存储的数据接入 UB1 接口，系统控制板对缓存中的数据 Data1 进行安全性检测，实现在被保护主机隔离状态下，系统控制板对 UA1 插入的 USB 存储进行杀毒等安全性检测。当 Data1 通过安全性检测后，将数据 Data1 拷贝到接口控制板 UB3 接口的内部 USB 存储中，期间硬件控制逻辑控制 UA1 与 UB1、UA3 与 UB3 之间的物理连接处于断开状态。之后，硬件控制逻辑断开 UB1 与

UB3 之间的物理连接，控制 UA3 与 UB3 的物理线路连通，将 UB3 接口上内部 USB 存储中的数据 Data1 通过对内接口 UA3 口发送给被保护主机，期间硬件控制逻辑断开 UA1 与 UB1、UB1 与 UB3 的物理线路。

相应的，当被保护主机中数据需要导出到外部设备 U 盘中时，系统控制板通过总线传输控制指令通知接口控制板，以控制所述硬件控制逻辑控制对内接口 UA3 与 UB3 的物理线路连接，UB3 接口上内部 USB 存储将与被保护主机数据连通，用户操作被保护主机 B 将数据 Data2 导入所述内部 USB 存储中，期间硬件控制逻辑保持对外接口 UA1 与转发接口 UB1、UB1 与 UB3 之间的物理线路处于断开状态。之后，硬件控制逻辑断开 UA3 与 UB3 之间的物理线路，接通 UB1 与 UB3 之间的物理线路，将 UB3 接口上内部 USB 存储中的数据 Data2 通过转发接口 UB1 转发给系统控制板的缓存，系统控制板对缓存中的数据 Data2 进行合规性检查，确认导出数据是否符合设定的合规策略，期间硬件控制逻辑保持对外接口 UA1 与转发接口 UB1、对内接口 UA3 与 UB3 之间的物理线路连接处于断开状态。当确认导出数据 Data2 通过合规性检查后，硬件控制逻辑连通对外接口 UA1 与转发接口 UB1 之间的物理线路，将数据 Data2 拷入 UA1 接口的外部设备 U 盘中，期间硬件控制逻辑保持转发接口 UB1 与 UB3、对内接口 UA3 与 UB3 之间物理线路处于断开状态。至此，完成数据导出过程。

通过本实施例中终端防护设备的数据导入导出的过程经硬件控制逻辑的控制，在任意时刻，只接通一处连接，其他连接处于物理线路断开状态，保证了外部设备接入后与被保护主机之间的数据单向/双向传输全部进行数据流量过滤禁止控制。

图 3 所示的又一实施例中，终端防护设备还可提供一种非存储类 USB 设备直连控制，主要针对一些需要直接接入且非存储类的 USB 设备，例如 USB 光驱，加密狗等。与上述数据导入导出控制类似，设备直连控制通过系统控制板控制接口控制板的硬件控制逻辑实现对 USB 设备的数据流量的控制，硬件连线情况如下：终端防护设备中的接口控制板的对内 USB 接口 UA4 连接被保护主机的 USB 接口，转发接口 UB2

接入系统控制板的USB接口，对外USB接口UA2插入需直连被保护主机B的外部设备（比如USB光驱），接口控制板的CTRL口接入总线连接系统控制板的控制接口。

本实施例中所述终端防护设备对USB设备直连控制方法如下：当终端防护设备的对外USB接口UA2插入需直连被保护主机B的外部设备（比如USB光驱）时，接口控制板通过总线通知系统控制板，系统控制板控制接口控制板的硬件控制逻辑接通接口UA2与转发接口UB2的物理线路，使得UA2接口上插入的USB光驱与系统控制板的USB接口连通，在此期间硬件控制逻辑保持接口UA2与连接被保护主机的对内接口UA4的物理线路处于断开状态。

系统控制板对UA2接口上的USB光驱进行安全鉴权，确认此外部设备是否为许可接入设备，当确认此USB光驱是许可接入设备后，硬件控制逻辑将对外接口UA2与对内接口UA4的物理线路接通，实现UA2接口上插入的USB光驱与被保护主机的连接。

当所述系统控制板监测到存在一个或多个接口的连接状态发生变化时，硬件控制逻辑自动断开所述接口与其他接口的物理线路。例如UA2接口上插入的外部设备接入UA4接口期间，系统控制板将实时监测接口控制板的UA2插入的外部设备连接情况，一旦检测到外部设备拔出接口将自动断开连接。

参见图4，本发明所涉及的外接式终端防护设备内部一种串口数据流量控制实施例，可实现对串口通信数据的过滤及禁止某些非法命令输入。系统控制板通过总线通知接口控制板的硬件控制逻辑控制对外串行接口CA1与转发接口CB1、对内串行接口CA2与转发接口CB2之间物理线路的断开与连通。接入对外串行接口CA1的外部设备首先需要通过系统控制板的安全鉴权，之后串口CD1和CD2实现数据互通，接口控制板的硬件控制逻辑接通串口CA1与CB1、CA2与CB2之间的物理线路，从而实现数据从对外串行接口CA1上的外部串口设备到对内串行接口CA2，进而再到被保护主机间的数据通信。

进一步地，系统控制板通过硬件控制逻辑断开CA1与CB1、CA2

与CB2之间的物理连接，实现对CA1与CA2之间串口通信的线路切断。由于 CA1 与 CA2 间通信均通过 CB1 与 CB2 进行转发，系统控制板可对串口通信数据进行过滤及禁止某些非法命令输入。

参见图 5，本发明所涉及的外接式终端防护设备内部一种网络数据流量控制实施例。本实施例中终端防护设备依赖于交换芯片，尤其是专用网络交换芯片，进而实现网络数据流量控制及审计功能。具体地，在所述终端防护设备中的接口控制板上集成了交换芯片，用于获取各个数据接口的寄存器状态，设置接口控制板的工作模式。接口控制板通过总线（即图示控制线）与系统控制板连接，系统控制板的网口 E5 与接口控制板的转发接口网口 E4 相连。进一步地，本实施例的所述终端防护设备可以采用专用网络交换芯片，在不影响网络延迟的情况下，支持网络流量镜像审计及网络协议过滤的功能。

由于终端防护设备应用于对网络延迟有较高要求的场合，要求接入网络设备对现有网络延迟、结构无明显影响，且对部署方式要求较为灵活。本方案所述终端防护设备网络审计防火墙设计通过依托于专用硬件实现网络数据流控制，进而实现低延迟网络审计与高可靠性协议过滤。

图 5 所示的另一实施例中，所述终端防护设备可具备网线防拔出功能，系统控制板通过读取交换芯片网口寄存器状态，从而获得对外网络接口 E1 与对内网络接口 E2 的连接状态，连接状态描述为链路连接失败/成功。系统控制板通过监测 E1/E2 网口连接状态，获得网口状态信息，进而实现对网线插入或拔出情况的告警。

图 5 所示的又一实施例中，所述终端防护设备可具备网络审计功能。对外接口 E1 接入局域网或工业控制网络，对内接口 E2 连接被保护主机 B 的网口。所述系统控制板基于本地操作指令或远程控制中心的远程网络控制指令，通过交换芯片设置接口控制板为流量镜像模式，通过所述接口控制板中的转发接口 E4，对所述接口控制板中的网络接口 E1 与 E2 做流量镜像。由此网口 E4 可获得来自 E1 及 E2 两个网口间的网络通信数据，而不影响 E1 与 E2 间数据通信，进而可以实现对被保护主机 B 与外部局域网或工业控制网络之间的网络流量审计。同时，此种方式采用

交换芯片设置接口控制板的工作模式，无需改变网络拓扑或添加额外的网络设备。

图 5 所示的再一实施例中，所述终端防护设备可具备网络协议过滤功能。所述系统控制板基于本地操作指令或远程控制中心的远程网络控制指令，通过交换芯片设置接口控制板为网络协议过滤模式，通过所述接口控制板中的转发接口 E4，对所述接口控制板中的对外接口 E1 和对内接口 E2 之间的数据流量做网络协议过滤，从而实现对被保护主机 B 与外部局域网或工业控制以太网络的数据流量做网络协议过滤。

进一步地，系统控制板可以控制交换芯片切换接口控制板的网口工作模式，比如将网络接口 E4 的流量镜像模式切换为网络协议过滤模式，或者将网络接口 E4 的网络协议过滤模式切换为流量镜像模式，或者其他工作模式之间进行切换。

图 6 为本发明的防护系统的一种网络部署实施例。所述防护系统包括一个或多个外部设备；被保护主机；以及外接式终端防护设备，其中，所述外接式终端防护设备外接于所述被保护主机上，使得所述一个或多个外部设备通过所述外接式终端防护设备与所述被保护主机进行接口通信。在此，所述外接式终端防护设备如上所述，此不再赘述。

进一步地，所述防护系统还包括其远程控制所述外接式终端防护设备的控制中心，控制中心由服务器、管理工作站，以及其他节点所组成，通过网络交换节点连接到所述外接式终端防护设备的网口 EA1 上。

在此处所提供的说明书中，说明了大量具体细节。然而，能够理解，本发明的实施例可以在没有这些具体细节的情况下实践。在一些实例中，并未详细示出公知的方法、结构和技术，以便不模糊对本说明书的理解。

类似地，应当理解，为了精简本公开并帮助理解各个发明方面中的一个或多个，在上面对本发明的示例性实施例的描述中，本发明的各个特征有时被一起分组到单个实施例、图、或者对其的描述中。然而，并不应将该公开的方法解释成反映如下意图：即所要求保护的本发明要求比在每个权利要求中所明确记载的特征更多的特征。更确切地说，如下面的权利要求书所反映的那样，发明方面在于少于前面公开的单个实施

例的所有特征。因此，遵循具体实施方式的权利要求书由此明确地并入该具体实施方式，其中每个权利要求本身都作为本发明的单独实施例。

本领域那些技术人员可以理解，可以对实施例中的设备中的模块进行自适应性地改变并且把它们设置在与该实施例不同的一个或多个设备中。可以把实施例中的模块或单元或组件组合成一个模块或单元或组件，以及此外可以把它们分成多个子模块或子单元或子组件。除了这样的特征和/或过程或者单元中的至少一些是相互排斥之外，可以采用任何组合对本说明书（包括伴随的权利要求、摘要和附图）中公开的所有特征以及如此公开的任何方法或者设备的所有过程或单元进行组合。除非另外明确陈述，本说明书（包括伴随的权利要求、摘要和附图）中公开的每个特征可以由提供相同、等同或相似目的替代特征来代替。

此外，本领域的技术人员能够理解，尽管在此所述的一些实施例包括其它实施例中所包括的某些特征而不是其它特征，但是不同实施例的特征的组合意味着处于本发明的范围之内并且形成不同的实施例。例如，在下面的权利要求书中，所要求保护的实施例的任意之一都可以以任意的组合方式来使用。

本发明的各个部件实施例可以以硬件实现，或者以在一个或者多个处理器上运行的软件模块实现，或者以它们的组合实现。本领域的技术人员应当理解，可以在实践中使用微处理器或者数字信号处理器（DSP）来实现根据本发明实施例的文字内容的拍照录入装置、计算设备和计算机可读存储介质中的一些或者全部部件的一些或者全部功能。本发明还可以实现为用于执行这里所描述的方法的一部分或者全部的设备或者装置程序（例如，计算机程序和计算机程序产品）。这样的实现本发明的程序可以存储在计算机可读介质上，或者可以具有一个或者多个信号的形式。这样的信号可以从因特网网站上下载得到，或者在载体信号上提供，或者以任何其他形式提供。

# 权利要求

1、一种数据流量控制的外接式终端防护设备，其包括：

接口控制模块，用于提供多个数据接口分别连接被保护主机及一个或多个外部设备；

系统控制模块，用于实时监测所述接口控制模块中各个数据接口的数据传输状态，并对各个数据接口的数据进行流量控制。

2、如权利要求 1 所述的外接式终端防护设备，其中，

所述接口控制模块与被保护主机的各个数据接口按照类型对应连接。

3、如权利要求 2 所述的外接式终端防护设备，其中，

所述接口控制模块的多个数据接口进一步包括对内接口、对外接口，以及转发接口；

所述对内接口用于与被保护主机的各个数据接口按照接口类型对应连接；

所述对外接口用于接入一个或多个外部设备，所述外部设备适于通过所述外接式终端防护设备与被保护主机进行数据交互；

所述转发接口用于将各接口类型的数据流量转发给所述系统控制模块。

4、如权利要求 3 所述的外接式终端防护设备，其中，

所述接口控制模块中进一步包含硬件控制逻辑，用于实现接口控制模块内部各个接口之间物理线路的通断。

5、如权利要求 1-4 任一项所述的外接式终端防护设备，其中，

所述系统控制模块进一步包括对外部设备的安全鉴权，以确认所述外部设备是否为许可接入设备。

6、如权利要求 5 所述的外接式终端防护设备，其中，

当所述系统控制模块对外部设备的安全鉴权后，确认所述外部设备不是许可接入设备时，通过总线通知接口控制模块禁止所述外部设备的数据传输；

所述接口控制模块中的硬件控制逻辑保持断开所述外部设备接入的对外接口与转发接口的物理线路的状态，从而对所述外部设备接入后的数据传输进行过滤禁止。

7、如权利要求 5 所述的外接式终端防护设备，其中，

当所述系统控制模块对外部设备的安全鉴权后，确认所述外部设备为许可接入设备时，通过总线通知接口控制模块允许所述外部设备的数据传输；

所述接口控制模块中的硬件控制逻辑连通所述外部设备接入的对外接口与转发接口的物理线路。

8、如权利要求 4 所述的外接式终端防护设备，其中，

所述数据接口进一步包括一个或多个网络接口；

所述接口控制模块中进一步包含交换芯片，用于获取各个网络接口的寄存器状态，设置接口控制模块的工作模式；

所述系统控制模块监测所述交换芯片中网络接口寄存器状态，从而实时获得接口控制模块中各网络接口的连接状态。

9、如权利要求 8 所述的外接式终端防护设备，其中，

当所述系统控制模块监测到存在一个或多个网络接口的连接状态发生变化时，对相应网络接口状态变化发出告警提示。

10、如权利要求 8 所述的外接式终端防护设备，其中，

所述系统控制模块通过所述交换芯片设置接口控制模块为流量镜像模式，通过所述接口控制模块中的转发接口，对所述接口控制模块中的对内接口和/或对外接口做流量镜像。

11、如权利要求 8 所述的外接式终端防护设备，其中，

所述系统控制模块通过所述交换芯片设置接口控制模块为网络协议过滤模式，通过所述接口控制模块中的转发接口，对所述接口控制模块中的对内接口和对外接口之间的数据流量做网络协议过滤。

12、如权利要求 8 所述的外接式终端防护设备，其中，

所述系统控制模块进一步设定有安全策略，对通过所述接口控制模块接入的外部设备传输进来的数据进行安全性检测；

所述接口控制模块将通过安全策略过滤后的数据流量转发给所述被保护主机。

13、一种用于数据流量控制的防护系统，包括：

一个或多个外部设备，所述外部设备适于通过所述外接式终端防护设备与被保护主机进行数据交互；

被保护主机；以及

如权利要求 1-12 任一项所述的外接式终端防护设备，

其中，所述外接式终端防护设备外接于所述被保护主机上，使得所述一个或多个外部设备通过所述外接式终端防护设备与所述被保护主机进行接口通信。

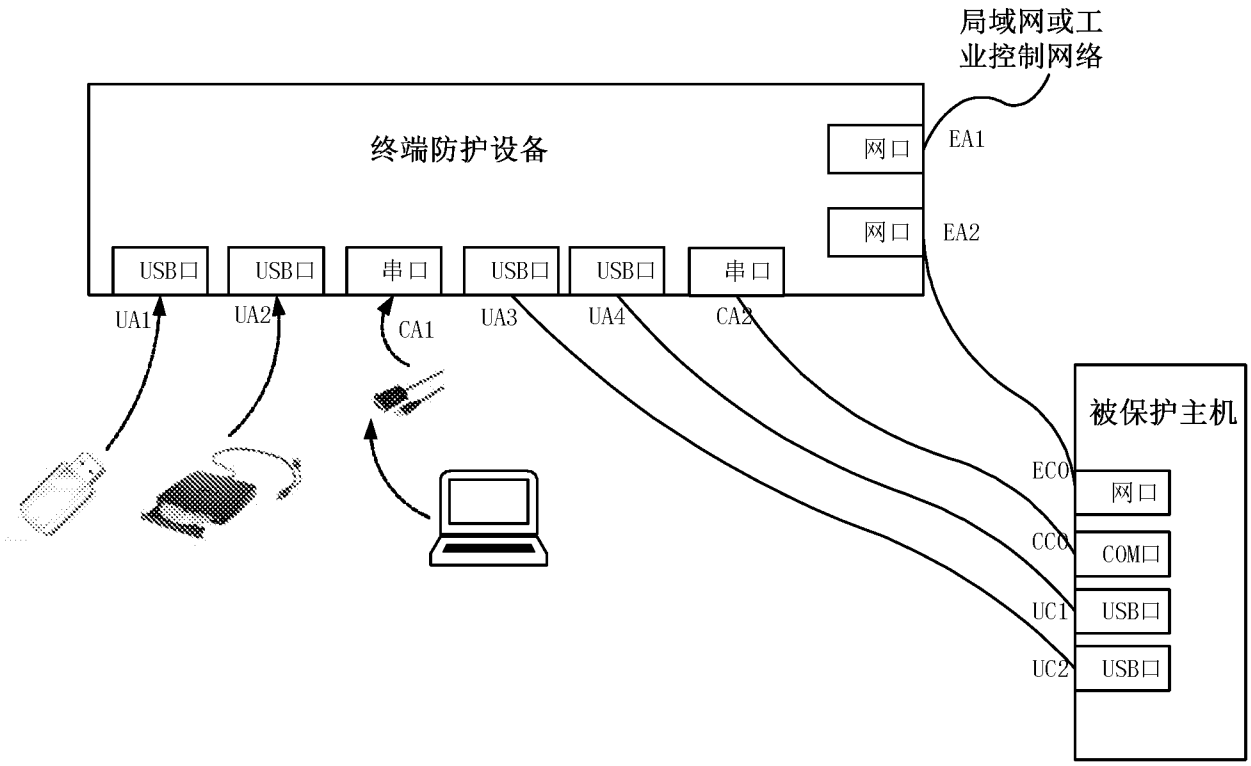

局域网或工
业控制网络
终端防护设备
网口
EA1
网口
EA2
USB口
USB口
串口
USB口
USB口
串口
UA1
UA2
CA1
UA3
UA4
CA2
被保护主机
ECO
网口
CCO
COM口
UC1
USB口
UC2
USB口

图 1

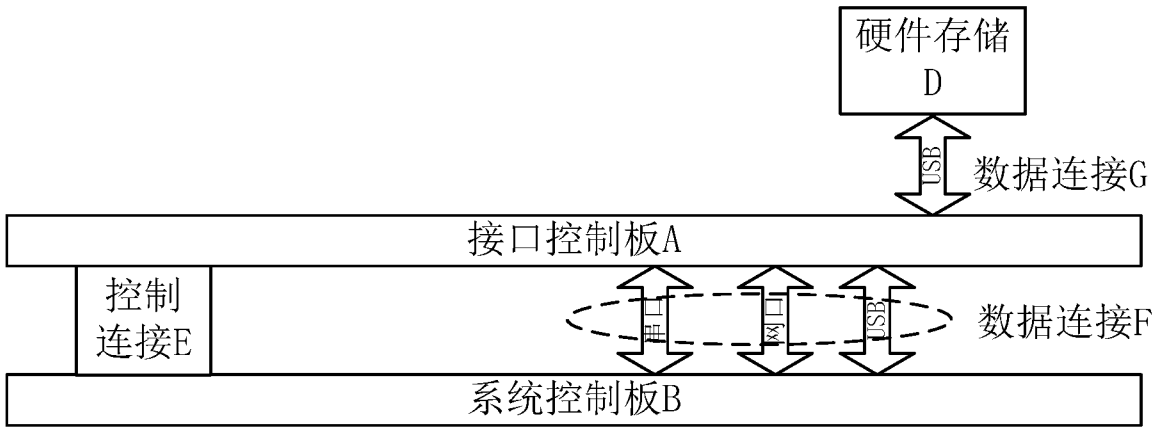

硬件存储
D
USB
数据连接G
接口控制板A
控制
连接E
串口
网口
USB口
数据连接F
系统控制板B

图 2

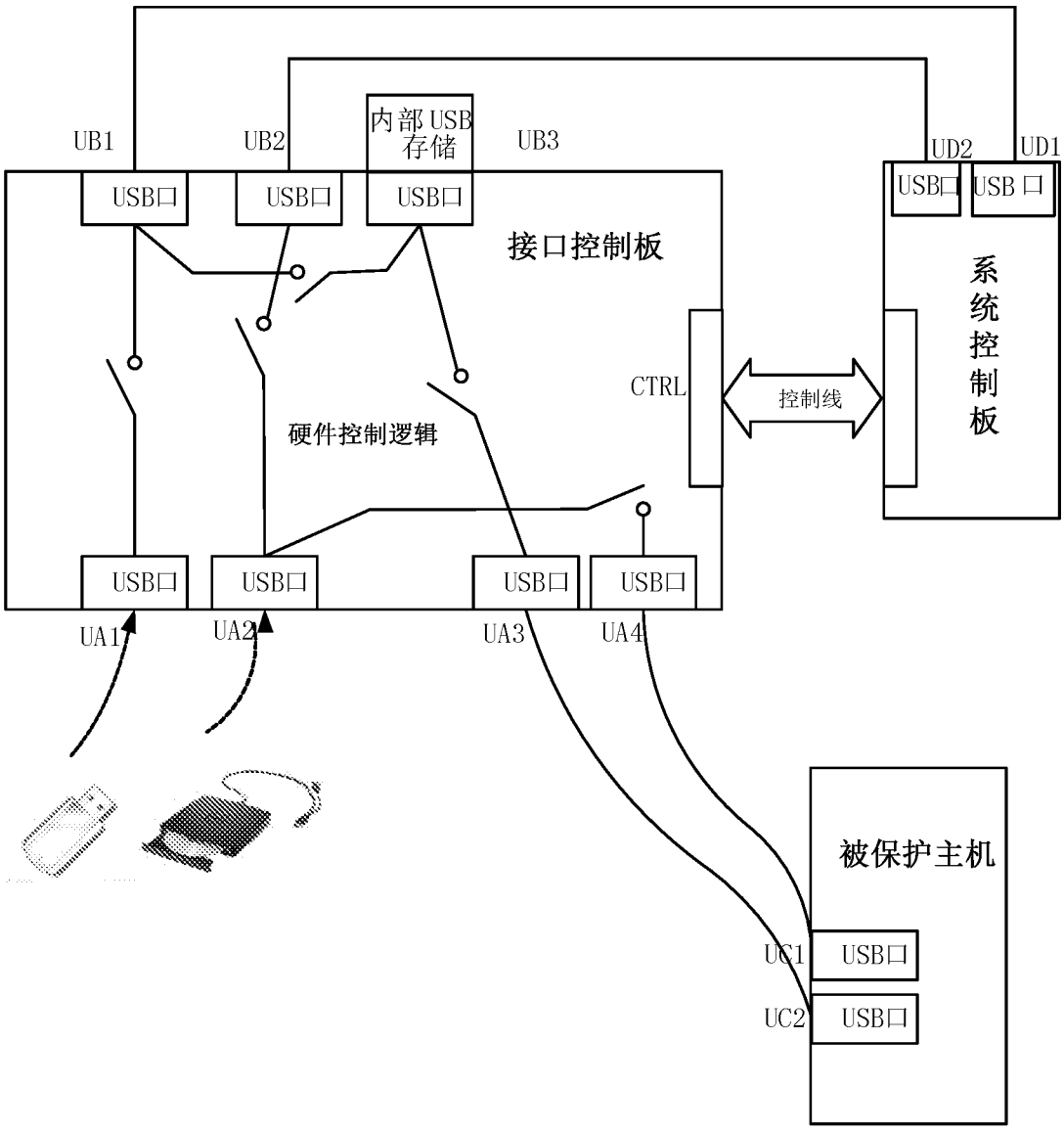

UB1
UB2
内部 USB 存储
UB3
USB口
USB口
USB口
接口控制板
UD2
UD1
USB口
USB 口
系统控制板
CTRL
控制线
硬件控制逻辑
USB口
USB口
USB口
USB口
UA1
UA2
UA3
UA4
被保护主机
UC1
USB口
UC2
USB口

图 3

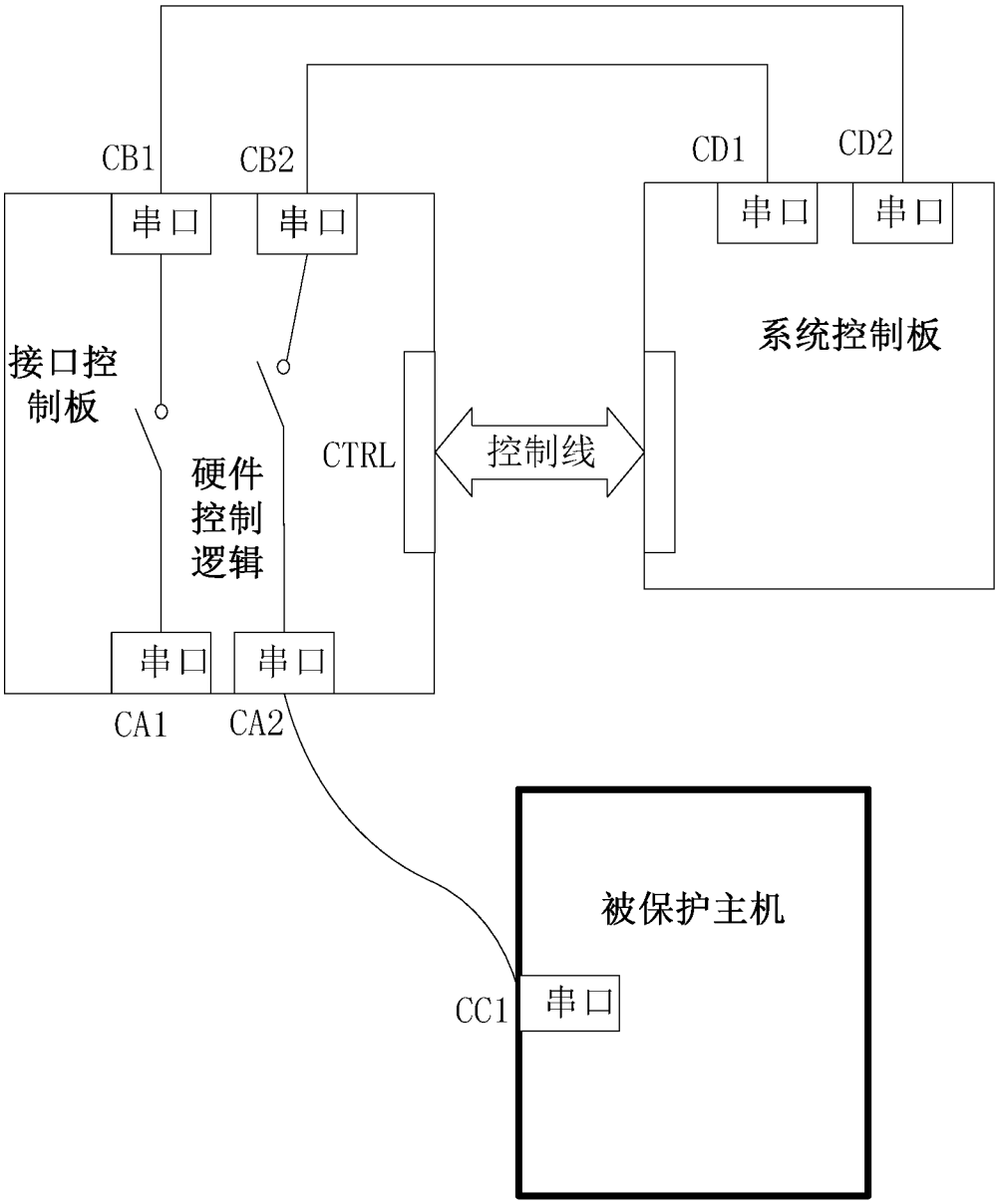

CB1
CB2
CD1
CD2
串口
串口
串口
串口
接口控制板
系统控制板
硬件控制逻辑
CTRL
控制线
串口
串口
CA1
CA2
被保护主机
CC1
串口

图 4

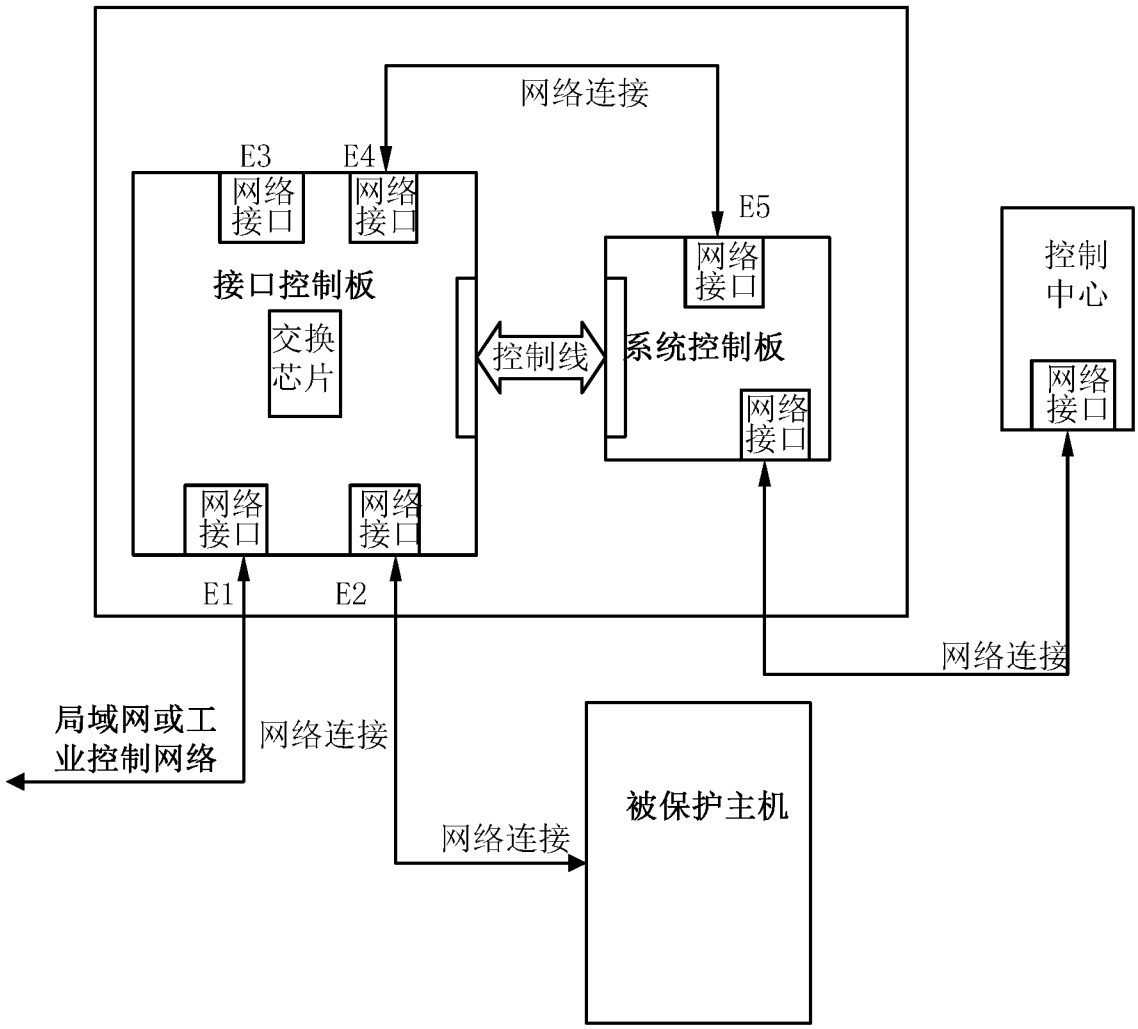

网络连接
E3
E4
网络接口
网络接口
接口控制板
交换芯片
控制线
E5
网络接口
系统控制板
网络接口
控制中心
网络接口
网络接口
网络接口
E1
E2
网络连接
局域网或工业控制网络
网络连接
网络连接
被保护主机

图 5

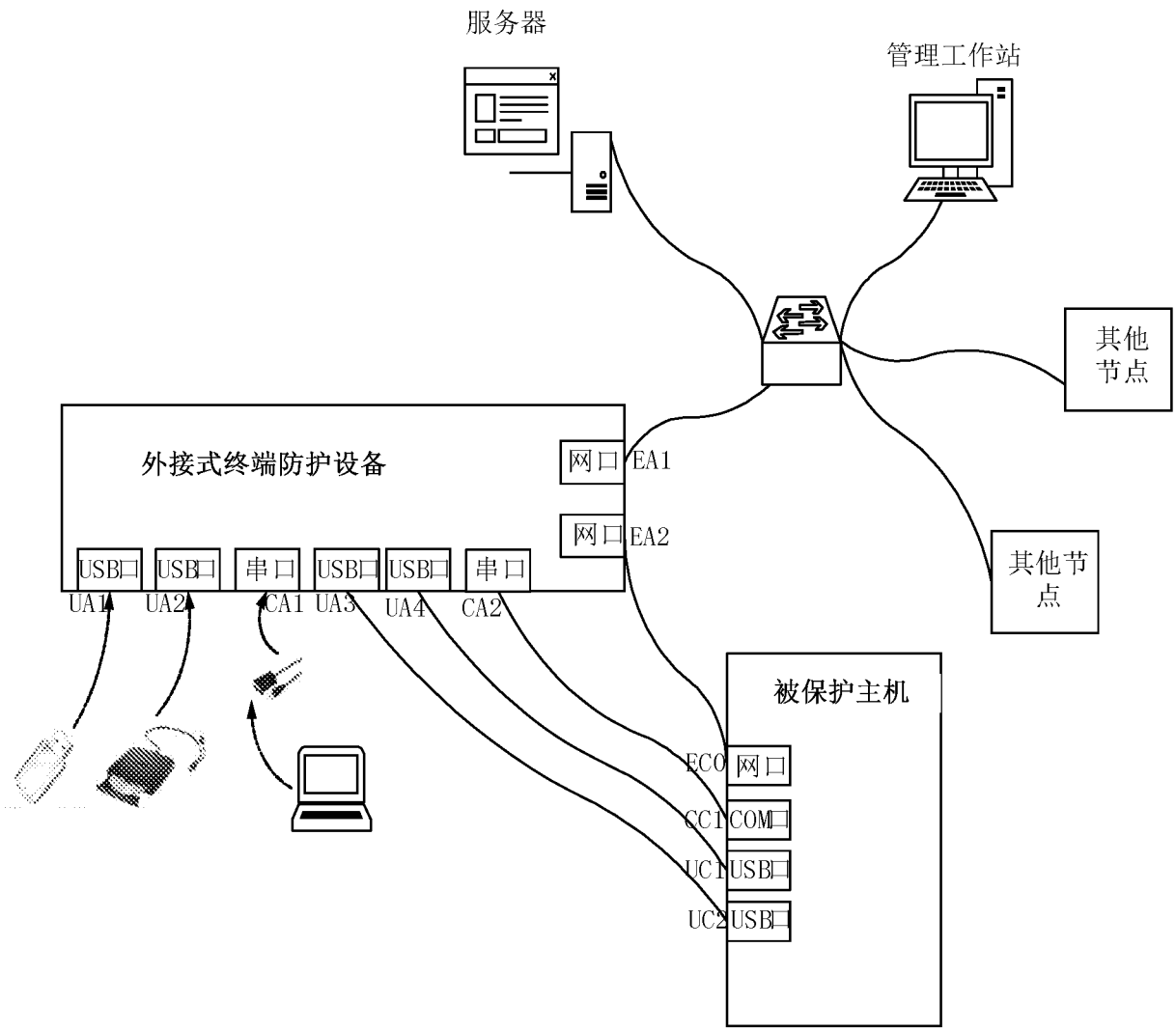

服务器
管理工作站
其他节点
外接式终端防护设备
网口 EA1
网口 EA2
USB口
USB口
串口
USB口
USB口
串口
UA1
UA2
CA1
UA3
UA4
CA2
其他节点
被保护主机
EC0 网口
CC1 COM口
UC1 USB口
UC2 USB口

图 6

# INTERNATIONAL SEARCH REPORT

International application No.
**PCT/CN2019/072030**

## A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06(2006.01)i; G06F 21/74(2013.01)i; G06F 21/85(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L, G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS; CNTXT; VEN; EPTXT; WOTXT; USTXT; CNKI: 保护, 防护, 外部, 外接, 接口, 多个, 流量, 监测, 控制, protect, safety, interface, usb, multiple, flow, monitor, control

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | CN 103020546 A (GUANGZHOU HUABIAO TECHNOLOGY DEVELOPMENT CO., LTD.) 03 April 2013 (2013-04-03)<br>claim 1 | 1-13 |
| X | CN 104915597 A (WANG, XIAONAN) 16 September 2015 (2015-09-16)<br>claims 1-6, and figure 1 | 1-13 |
| A | CN 103778388 A (TIANJIN 707 INSTITUTE OF PRECISION MECHATRONICS SCI & TECH CO., LTD.) 07 May 2014 (2014-05-07)<br>entire document | 1-13 |
| A | CN 205210890 U (REN, JIANLAN) 04 May 2016 (2016-05-04)<br>entire document | 1-13 |
| A | WO 2012106049 A1 (MCCI CORP.) 09 August 2012 (2012-08-09)<br>entire document | 1-13 |

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| **15 May 2019** | **03 July 2019** |

| Name and mailing address of the ISA/CN | Authorized officer |
|---|---|
| **China National Intellectual Property Administration**<br>**No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088**<br>**China** | |
| Facsimile No. **(86-10)62019451** | Telephone No. |

**INTERNATIONAL SEARCH REPORT**
**Information on patent family members**

International application No.
**PCT/CN2019/072030**

| Patent document cited in search report | Publication date (day/month/year) | Patent family member(s) | Publication date (day/month/year) |
|---|---|---|---|
| CN 103020546 A | 03 April 2013 | None | |
| CN 104915597 A | 16 September 2015 | None | |
| CN 103778388 A | 07 May 2014 | CN 103778388 B | 14 September 2016 |
| CN 205210890 U | 04 May 2016 | None | |
| WO 2012106049 A1 | 09 August 2012 | US 8713683 B2 | 29 April 2014 |
| | | EP 2671184 A1 | 11 December 2013 |
| | | US 2014215637 A1 | 31 July 2014 |
| | | US 2013014221 A1 | 10 January 2013 |
| | | US 9021597 B2 | 28 April 2015 |
| | | JP 2014509421 A | 17 April 2014 |

# 国际检索报告

国际申请号
PCT/CN2019/072030

A. 主题的分类

H04L 29/06(2006.01)i; G06F 21/74(2013.01)i; G06F 21/85(2013.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L, G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNABS;CNTXT;VEN;EPTXT;WOTXT;USTXT;CNKI:保护，防护，外部，外接，接口，多个，流量，监测，控制，protect, safety, interface, usb, multiple, flow, monitor, control

C. 相关文件

| 类 型* | 引用文件，必要时，指明相关段落 | 相关的权利要求 |
|---|---|---|
| X | CN 103020546 A (广州市华标科技发展有限公司) 2013年 4月 3日 (2013-04-03)<br>权利要求1 | 1-13 |
| X | CN 104915597 A (王晓楠) 2015年 9月 16日 (2015-09-16)<br>权利要求1-6，图1 | 1-13 |
| A | CN 103778388 A (天津七所精密机电技术有限公司) 2014年 5月 7日 (2014-05-07)<br>全文 | 1-13 |
| A | CN 205210890 U (任剑岚) 2016年 5月 4日 (2016-05-04)<br>全文 | 1-13 |
| A | WO 2012106049 A1 (MCCI CORP) 2012年 8月 9日 (2012-08-09)<br>全文 | 1-13 |

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

| 国际检索实际完成的日期 | 国际检索报告邮寄日期 |
|---|---|
| 2019年 5月 15日 | 2019年 7月 3日 |
| ISA/CN的名称和邮寄地址<br>中国国家知识产权局(ISA/CN)<br>中国北京市海淀区蓟门桥西土城路6号 100088<br>传真号 (86-10)62019451 | 受权官员<br>邓璐<br>电话号码 86-(010)-62089138 |

表 PCT/ISA/210 (第2页) (2015年1月)

# 国际检索报告
## 关于同族专利的信息

国际申请号
PCT/CN2019/072030

| 检索报告引用的专利文件 | | | 公布日<br>(年/月/日) | 同族专利 | | | 公布日<br>(年/月/日) |
|---|---|---|---|---|---|---|---|
| CN | 103020546 | A | 2013年 4月 3日 | 无 | | | |
| CN | 104915597 | A | 2015年 9月 16日 | 无 | | | |
| CN | 103778388 | A | 2014年 5月 7日 | CN | 103778388 | B | 2016年 9月 14日 |
| CN | 205210890 | U | 2016年 5月 4日 | 无 | | | |
| WO | 2012106049 | A1 | 2012年 8月 9日 | US | 8713683 | B2 | 2014年 4月 29日 |
| | | | | EP | 2671184 | A1 | 2013年 12月 11日 |
| | | | | US | 2014215637 | A1 | 2014年 7月 31日 |
| | | | | US | 2013014221 | A1 | 2013年 1月 10日 |
| | | | | US | 9021597 | B2 | 2015年 4月 28日 |
| | | | | JP | 2014509421 | A | 2014年 4月 17日 |