



(12)发明专利

(10)授权公告号 CN 104683352 B

(45)授权公告日 2018.05.25

(21)申请号 201510118782.3

(56)对比文件

CN 102208982 A, 2011.10.05,

CN 103139058 A, 2013.06.05,

US 2005021839 A1, 2005.01.27,

王博.基于物理隔离技术的网闸系统的设计与实现.《中国优秀硕士学位论文全文数据库信息科技辑》.2014,(第11期),

(22)申请日 2015.03.18

审查员 刘莹

(65)同一申请的已公布的文献号

申请公布号 CN 104683352 A

(43)申请公布日 2015.06.03

(73)专利权人 宁波科安网信通讯科技有限公司

地址 315104 浙江省宁波市江南路586号九
五国际大厦B座826

(72)发明人 周文乐

(74)专利代理机构 北京慕达星云知识产权代理
事务所(特殊普通合伙)
11465

代理人 李冉

(51)Int.Cl.

H04L 29/06(2006.01)

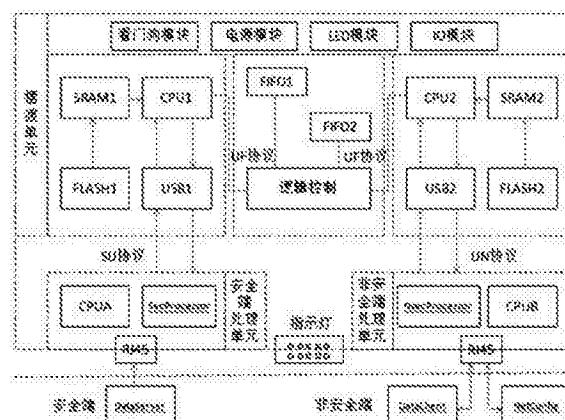
权利要求书1页 说明书5页 附图2页

(54)发明名称

一种具有双通道摆渡的工业通讯隔离网闸

(57)摘要

本发明公开了一种具有双通道摆渡的工业通讯隔离网闸，包括安全端处理单元、非安全端处理单元和摆渡单元；所述安全端处理单元的电路、非安全端处理单元的电路和摆渡单元的电路全独立，且三个单元之间采用USB通讯，所述摆渡单元采用双通道摆渡，双通道为两条独立的单向通道，其中一条为请求通道，负责从非安全端向安全端单向请求，用于配置请求、标签请求，另一条为数据通道，负责从安全端向非安全端单向传输，用于过程数据传输和状态数据传输。该隔离网闸用于工业控制网络与上层信息网络在物理隔离的条件下实现过程数据的单向传输，并实现标签免维护，可远程配置、维护管理的功能，给正常的数据采集和日常维护带来极大的方便。



1. 一种具有双通道摆渡的工业通讯隔离网闸，其特征在于：包括安全端处理单元、非安全端处理单元和摆渡单元；所述安全端处理单元的电路、非安全端处理单元的电路和摆渡单元的电路全独立，且三个单元之间采用USB通讯，安全端处理单元、非安全端处理单元和摆渡单元之间采用各种对应的通讯协议，每种通讯协议都包括协议剥离、校验、解密、封装过程，所述摆渡单元采用双通道摆渡，双通道为两条独立的单向通道，其中一条为请求通道，负责从非安全端向安全端单向请求，用于配置请求、标签请求，另一条为数据通道，负责从安全端向非安全端单向传输，用于过程数据传输和状态数据传输；所述摆渡单元包括两个CPU、两个FIFO缓存和一个逻辑控制电路组成，一个CPU负责接收安全端处理单元发送来的数据包，校验、解密、分析是否符合协议，获取状态数据，通过的数据重新加密、封装成摆渡协议包，写入FIFO缓存，逻辑控制电路负责切断FIFO与当前CPU的连接，重新建立与另一端CPU的连接；另一个CPU对FIFO的数据包进行校验、解密、分析是否符合协议，获取状态数据，通过的数据重新加密、封装成摆渡协议包，通过USB协议传输给非安全端处理单元，非安全端处理单元负责接收协议包，校验、解密、分析是否符合协议，通过对数据重新封装工业通讯协议数据包，并传输给客户端。

2. 根据权利要求1所述的一种具有双通道摆渡的工业通讯隔离网闸，其特征在于：所述安全端处理单元负责与数据源通讯，采集数据并还原成原始数据，并重新加密封装成内部专用协议，通过USB协议传输给摆渡单元；摆渡单元实现安全端处理单元与非安全端处理单元的沟通和隔离。

3. 根据权利要求1所述的一种具有双通道摆渡的工业通讯隔离网闸，其特征在于：所述通讯协议包括：OPC、DNP3、Modbus、Modbus TCP、IEC870-5-101、IEC870-5-104协议。

4. 根据权利要求1所述的一种具有双通道摆渡的工业通讯隔离网闸，其特征在于：所述摆渡单元内部同样采用2+1结构，即安全端处理模块、非安全处理模块、逻辑控制模块组成；安全端处理模块和非安全处理模块有各自的CPU，负责相应的通讯和协议分析功能，逻辑控制模块负责物理链路拆建。

5. 根据权利要求1所述的一种具有双通道摆渡的工业通讯隔离网闸，其特征在于：采用物理链路拆建、多次协议剥离、加密、校验、封装，双通道FIFO缓冲，在非安全端IP层构筑IP过滤机制，仅允许授权的IP才可以访问OPC网闸。

一种具有双通道摆渡的工业通讯隔离网闸

技术领域

[0001] 本发明涉及自动化信息系统的计算机网络技术领域,具体讲是一种具有双通道摆渡的工业通讯隔离网闸。

背景技术

[0002] 数据采集与监控(SCADA)、分布式控制系统(DCS)、过程控制系统(PCS)、可编程逻辑控制器(PLC)等工业控制系统广泛运用于工业、能源、交通、水利及市政等领域,用于控制生产设备的运行。一旦工业控制系统信息安全出现漏洞,将对工业生产运行和国家经济安全造成重大隐患。随着计算机和网络技术的发展,特别是信息化与工业化深度融合,工业控制系统产品越来越多地采用通用协议、通用硬件和通用软件,以各种方式与MIS网络、因特网等公共网络连接,造成病毒、木马等威胁向工业控制系统扩散,工业控制系统安全问题日益突出。2010年发生的“震网”病毒时间,充分反映出工业控制系统信息安全面临严峻的形势。

[0003] 目前,工业控制系统的网络安全保障多大多数还是依靠传统的解决方案,即采用防火墙作为工业控制网络与上层信息网络之间的屏障。实际上,防火墙并不能有效地保障工业控制网络安全,原因如下:

[0004] 一、防火墙由于其自身机理的原因,存在很多先天不足,主要包括:

[0005] (1)由于防火墙本身是基于TCP/IP协议体系实现的,所以它无法解决TCP/IP协议体系中存在的漏洞。

[0006] (2)防火墙只是一个策略执行机构,它并不区分所执行政策的对错,更无法判别出一条合法政策是否真是管理员的本意。从这点上看,防火墙一旦被攻击者控制,由它保护的整个网络就无安全可言了。

[0007] (3)防火墙无法从流量上判别哪些是正常的,哪些是异常的,因此容易受到流量攻击。

[0008] (4)防火墙的安全性与其速度和多功能成反比。防火墙的安全性要求越高,需要对数据包检查的项目(即防火墙的功能)就越多越细,对CPU和内存的消耗也就越大,从而导致防火墙的性能下降,处理速度减慢。

[0009] (5)防火墙准许某项服务,却不能保证该服务的安全性,它需要由应用安全来解决。

[0010] 二、从实际应用来看,防火墙较为明显的局限性包括以下几方面:

[0011] (1)最为广泛应用的工业通讯协议OPC基于DCOM机制,采用动态端口,无法穿透防火墙。

[0012] (2)防火墙不能阻止感染病毒的程序和文件的传输。就是防火墙只能做网络四层以下的控制,对于应用层内的病毒、蠕虫都没有办法。

[0013] (3)防火墙不能防范全新的威胁,更不能防止可接触的人为或自然的破坏。

[0014] (4)防火墙不能防止由自身安全漏洞引起的威胁。

- [0015] (5) 防火墙对用户不完全透明,非专业用户难于管理和配置,易造成安全漏洞。
- [0016] (6) 防火墙很难为用户在防火墙内外提供一致的安全策略,不能防止利用标准网络协议中的缺陷进行的攻击,也不能防止利用服务器系统漏洞所进行的攻击。
- [0017] (7) 由于防火墙设置在内网与外网通信的信道上,并执行规定的安全策略,所以防火墙在提供安全防护的同时,也变成了网络通信的瓶颈,增加了网络传输延时,如果防火墙出现问题,那么内部网络就会受到严重威胁。
- [0018] (8) 防火墙仅提供粗粒度的访问控制能力。它不能防止数据驱动式的攻击。
- [0019] (9) 防火墙正是由于这些缺陷与不足,导致目前被攻破的几率已经接近50%。虽然目前最流行的安全架构是以防火墙为核心的安全体系架构。通过防火墙来实现网络的安全保障体系。然而,以防火墙为核心的安全防御体系未能有效地防止目前频频发生网络攻击。仅有防火墙的安全架构是远远不够的。
- [0020] 网络隔离产品主要的技术原理是从OSI模型的七层上全面断开网络连接,同时采用“2+1”的三模块架构,即内置有两个主机系统,和一个用于建立安全通道可交换数据的隔离单元。这种架构可以实现连接到外网和内网的两主机之间是完全网络断开的,从物理上进行了网络隔离,消除了数据链路的通信协议,剥离了TCP/IP协议,剥离了应用协议,在安全交换后进行了协议的恢复和重建。通过TCP/IP协议剥离和重建技术消除了TCP/IP协议的漏洞。在应用层对应用协议进行剥离和重建,消除了应用协议漏洞,并可针对应用协议实现一些细粒度的访问控制。从TCP/IP的OSI数据模型的所有七层断开后,就可以消除目前TCP/IP存在的所有攻击。
- [0021] 传统网闸产品的主要定位是各行业中对安全性要求较高的涉密业务的办公系统,因此它提供的应用也以通用的互联网功能为主。例如,目前大多数网关都支持:文件数据交换、HTTP访问、WWW服务、FTP访问、收发电子邮件、关系数据库同步以及TCP/UDP定制等。这些网闸产品都不支持工业通讯协议,如OPC、Modbus、DNP3等协议,故不能应用到工业网络安全上。
- [0022] 目前,市场上也有一些工业通讯网闸,用于单向隔离,其配置和标签维护需要分别在安全端和非安全端进行操作,且不能进行远程管理,给正常的数据采集和日常维护带来极大的不便。

发明内容

- [0023] 本发明要解决的技术问题是,提供一种用于工业控制网络与上层信息网络在物理隔离的条件下实现过程数据的单向传输,并实现标签免维护,可远程配置、维护管理的功能,给正常的数据采集和日常维护带来极大的方便的具有双通道摆渡的工业通讯隔离网闸。
- [0024] 本发明的技术方案是,提供一种具有以下结构的具有双通道摆渡的工业通讯隔离网闸,包括安全端处理单元、非安全端处理单元和摆渡单元;所述安全端处理单元的电路、非安全端处理单元的电路和摆渡单元的电路全独立,且三个单元之间采用USB通讯,安全端处理单元、非安全端处理单元和摆渡单元之间采用各种对应的通讯协议,每种通讯协议都包括协议剥离、校验、解密、封装过程,所述摆渡单元采用双通道摆渡,双通道为两条独立的单向通道,其中一条为请求通道,负责从非安全端向安全端单向请求,用于配置请求、标签

请求,另一条为数据通道,负责从安全段向非安全端单向传输,用于过程数据传输和状态数据传输。

[0025] 所述安全端处理单元负责与数据源通讯,采集数据并还原成原始数据,并重新加密封装成内部专用协议,通过USB协议传输给摆渡单元;摆渡单元实现安全端处理单元与非安全端处理单元的沟通和隔离,所述摆渡单元包括两个CPU、两个FIFO缓存和一个逻辑控制电路组成,一个CPU负责接收安全端处理单元发送来的数据包,校验、解密、分析是否符合协议,获取状态数据,通过的数据重新加密、封装成摆渡协议包,写入FIFO缓存,逻辑控制电路负责切断FIFO与当前CPU的连接,重新建立与另一端CPU的连接;另一个CPU对FIFO的数据包进行校验、解密、分析是否符合协议,获取状态数据,通过的数据重新加密、封装成摆渡协议包,通过USB协议传输给非安全端处理单元,非安全端处理单元负责接收协议包,校验、解密、分析是否符合协议,通过的数据重新封装工业通讯协议数据包,并传输给客户端。

[0026] 所述通讯协议包括:OPC、DNP3、Modbus、Modbus TCP、IEC870-5-101、IEC870-5-104协议。

[0027] 所述摆渡单元内部同样采用2+1结构,即安全端处理模块、非安全处理模块、逻辑控制模块组成。安全端处理模块和非安全处理模块有各自的CPU,负责相应的通讯和协议分析功能,逻辑控制模块负责物理链路拆建。

[0028] 采用物理链路拆建、多次协议剥离、加密、校验、封装,双通道FIFO缓冲,在非安全端IP层构筑IP过滤机制,仅允许授权的IP才可以访问OPC网闸。

[0029] 采用上述结构后,本发明与现有技术相比,具有以下优点:采用多重安全技术,采用物理链路拆建、多次协议剥离、加密、校验、封装,双通道缓冲等多种安全技术外,还在非安全端IP层构筑IP过滤机制,仅允许授权的IP才可以访问网闸。综合以上几种安全技术,确保工业通讯网闸成为工业控制网络的坚实堡垒,给正常的数据采集和日常维护带来极大的方便。用于工业控制网络与上层信息网络在物理隔离的条件下实现过程数据的单向传输,并实现标签免维护,可远程配置、维护管理的功能。

附图说明

[0030] 图1为双通道工业通讯网闸硬件组成示意图。

[0031] 图2为双通道数据传输示意图。

[0032] 图3为上半周期双通道链路示意图。

[0033] 图4为下半周期双通道链路示意图。

具体实施方式

[0034] 下面结合附图对本发明具有双通道摆渡的工业通讯隔离网闸作进一步说明。

[0035] 如图1所示,本发明的一种具有双通道摆渡的工业通讯隔离网闸,包括安全端处理单元、非安全端处理单元和摆渡单元;所述安全端处理单元的电路、非安全端处理单元的电路和摆渡单元的电路全独立,且三个单元之间采用USB通讯,安全端处理单元、非安全端处理单元和摆渡单元之间采用各种对应的通讯协议,每种通讯协议都包括协议剥离、校验、解密、封装过程,所述摆渡单元采用双通道摆渡,双通道为两条独立的单向通道,其中一条为请求通道,负责从非安全端向安全端单向请求,用于配置请求、标签请求,另一条为数据通

道,负责从安全段向非安全端单向传输,用于过程数据传输和状态数据传输。

[0036] 所述安全端处理单元负责与数据源通讯,采集数据并还原成原始数据,并重新加密封装成内部专用协议,通过USB协议传输给摆渡单元;摆渡单元实现安全端处理单元与非安全端处理单元的沟通和隔离,所述摆渡单元包括两个CPU、两个FIFO缓存和一个逻辑控制电路组成,一个CPU负责接收安全端处理单元发送来的数据包,校验、解密、分析是否符合协议,获取状态数据,通过的数据重新加密、封装成摆渡协议包,写入FIFO缓存,逻辑控制电路负责切断FIFO与当前CPU的连接,重新建立与另一端CPU的连接;另一个CPU对FIFO的数据包进行校验、解密、分析是否符合协议,获取状态数据,通过的数据重新加密、封装成摆渡协议包,通过USB协议传输给非安全端处理单元,非安全端处理单元负责接收协议包,校验、解密、分析是否符合协议,通过的数据重新封装工业通讯协议数据包,并传输给客户端。

[0037] 采用本发明的工业通讯隔离网闸,替代防火墙,同样位于过程数据服务器(DataServer)和客户端(DataClient)之间,由于网闸在物理层上打断了安全端和非安全端的物理连接,从而保证工业控制网络与上层信息网络之间没有任何的物理连接,从而断绝入侵、恶意攻击、病毒、恶意代码等的攻击通道;采用多次协议剥离、校验、加密、封装,仅允许过程数据和内部专有协议可以单向传输;仅允许DataClient可以访问网闸,增强了堡垒功能;标签来自DataClient的请求,而无需事先定义,这在实际应用中尤其重要,因为标签的维护是经常性的;可以远程维护,查看网闸和过程数据服务器(DataServer)的工作状态,处理故障问题,这在实际的运维工作中是很重要的。通过采用本发明的工业通讯隔离网闸作为工业控制网络与上层信息网络的隔离设备,不仅达到在物理隔离条件下实现单向传输数据的功能外,还不影响原先业务的灵活性。

[0038] 安全端处理单元与过程数据服务器(DataServer)通讯,并将工业通讯协议剥离还原成原始数据保存在内存中等待请求;安全端处理单元与摆渡单元采用USB通讯,从请求通道获取SU协议包,解析请求,做相应处理,将过程数据和配置响应封装成SU协议包,等待下周期送入数据通道。

[0039] 非安全端处理单元与DataClient通讯,并将工业通讯协议还原成原始数据;非安全端处理单元与配置终端(Netconfig)通讯,,并将NC协议还原成原始数据;非安全端处理单元将OPC请求和配置请求重新封装成UN协议包,送入请求通道;非安全端处理单元与摆渡单元采用USB通讯,从数据通道获取UN协议包,解析数据,将过程数据转发给DataClient,将配置数据转发给Netconfig。

[0040] 所述通讯协议包括:OPC、DNP3、Modbus、Modbus TCP、IEC870-5-101、IEC870-5-104协议。

[0041] 所述摆渡单元内部同样采用2+1结构,即安全端处理模块、非安全处理模块、逻辑控制模块组成。安全端处理模块和非安全处理模块有各自的CPU,负责相应的通讯和协议分析功能,逻辑控制模块负责物理链路拆建。

[0042] 采用物理链路拆建、多次协议剥离、加密、校验、封装,双通道FIFO缓冲,在非安全端IP层构筑IP过滤机制,仅允许授权的IP才可以访问OPC网闸。

[0043] 逻辑控制模块用于切换安全端处理模块、非安全端处理模块与数据通道、请求通道的链路连接,从而保证安全端与非安全端的物理上不连接,同时保证数据的传输。逻辑控制模块的工作原理如下:

[0044] 图2为双通道数据传输示意图,数据传输和请求传输分别在数据通道和请求通道中同时进行,传输周期已链路切换为界分为上半周期和下半周期,一个完整的请求数据由2个传输周期完成。

[0045] 图3为上半周期双通道链路状态。此时非安全端处理模块与请求通道FIFO2连接,并将请求包写入FIFO2,置写完状态,安全端处理模块与数据通道FIFO1连接,并将数据包写入FIFO1,置写完状态,控制逻辑根据写完状态开始切换链路,下半周期开始。

[0046] 图4为下半周期双通道链路状态。此时非安全端处理模块与数据通道FIFO1连接,并从FIFO1读取数据包,置读完状态,安全端处理模块与请求通道FIFO2连接,并从FIFO2读取请求包,置读完状态,控制逻辑根据读完状态开始切换链路,新周期开始。自此,数据从安全端到达非安全端,请求从非安全端到达安全端。

[0047] 以上给出的实施用例说明本发明和它的实际应用,并且因此使得本领域的技术人员能够做出和使用本发明。本文并未对本发明作任何形式上的限制,任何一个本专业的技术人员在不偏离本发明技术方案的范围内,依据以上技术和方法作一定的修饰和变更视为等同变化的等效实施例。

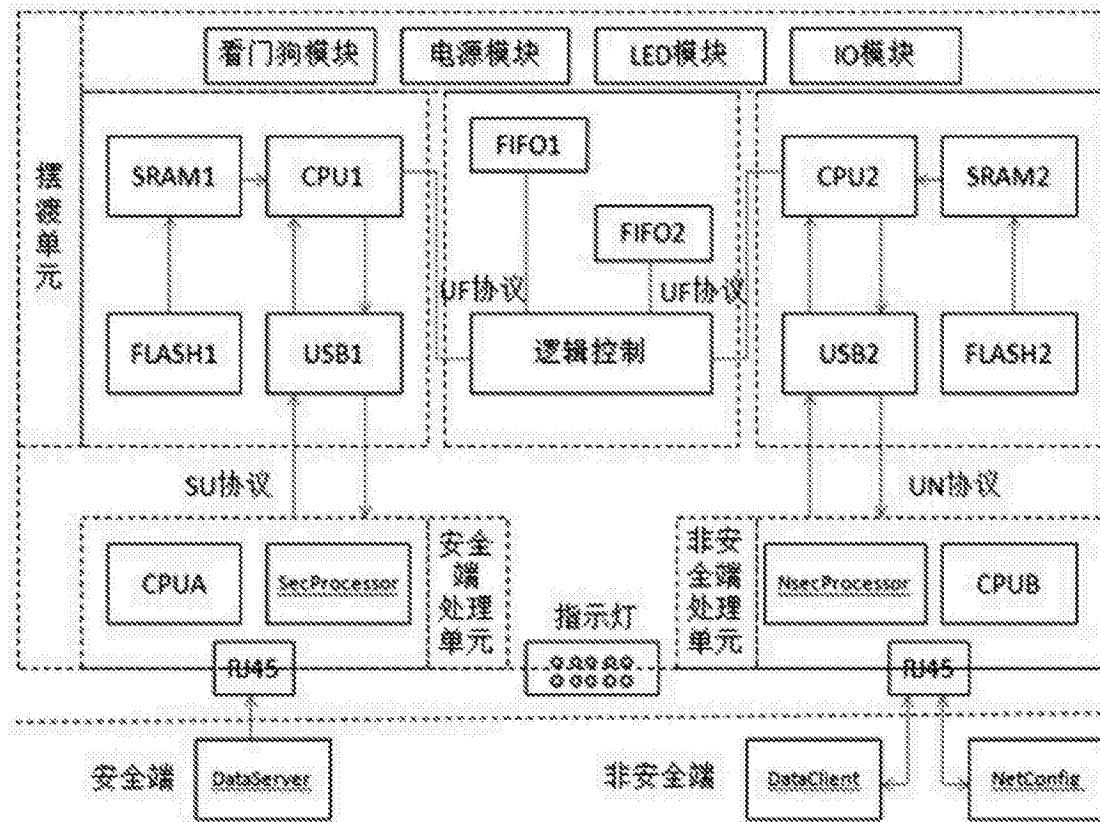


图1

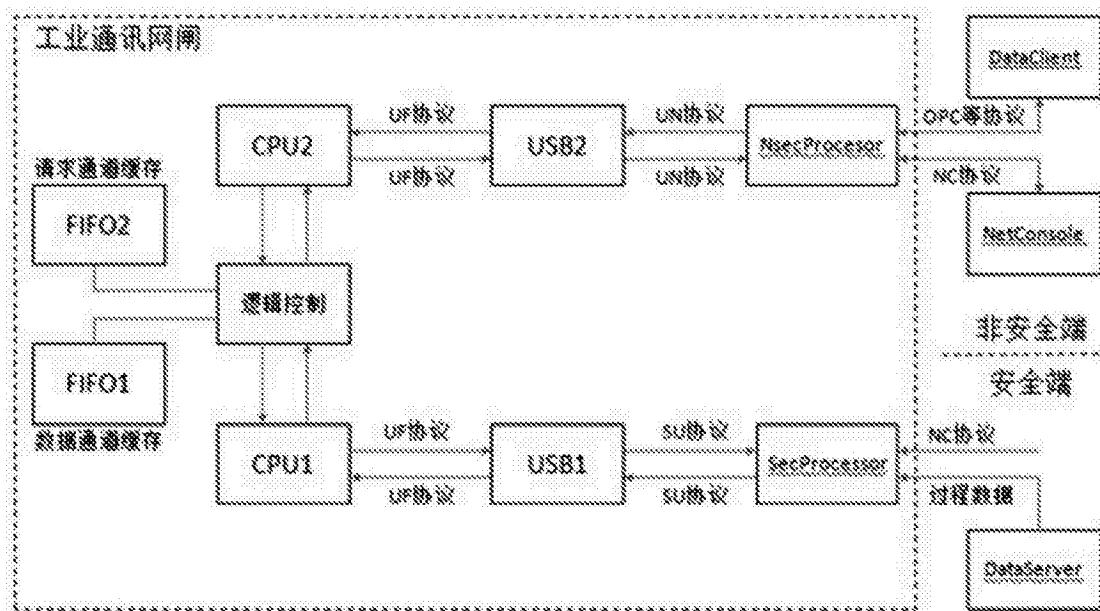


图2

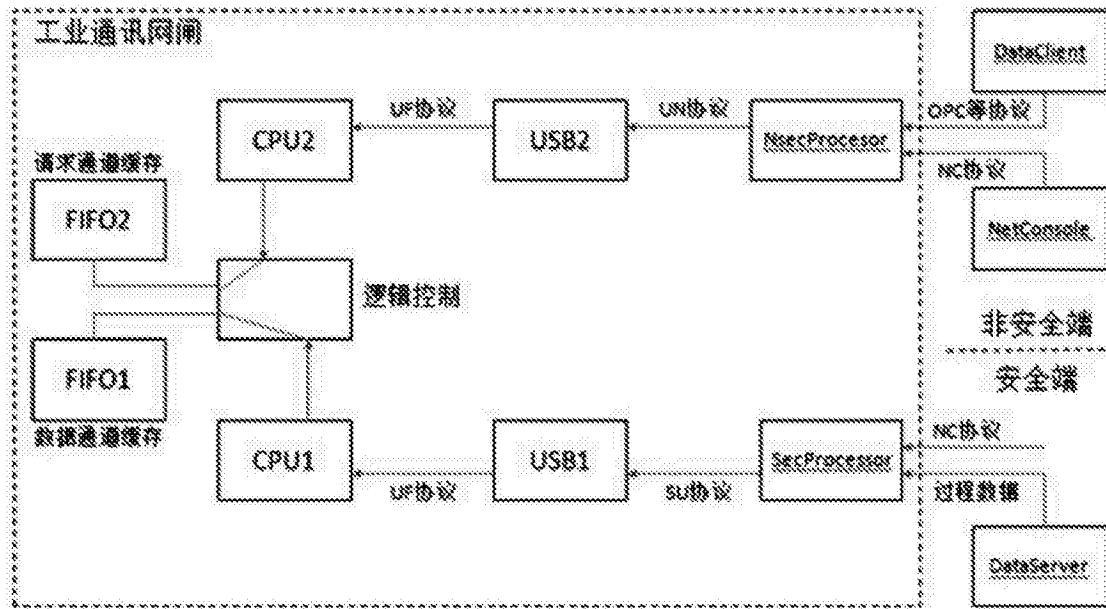


图3

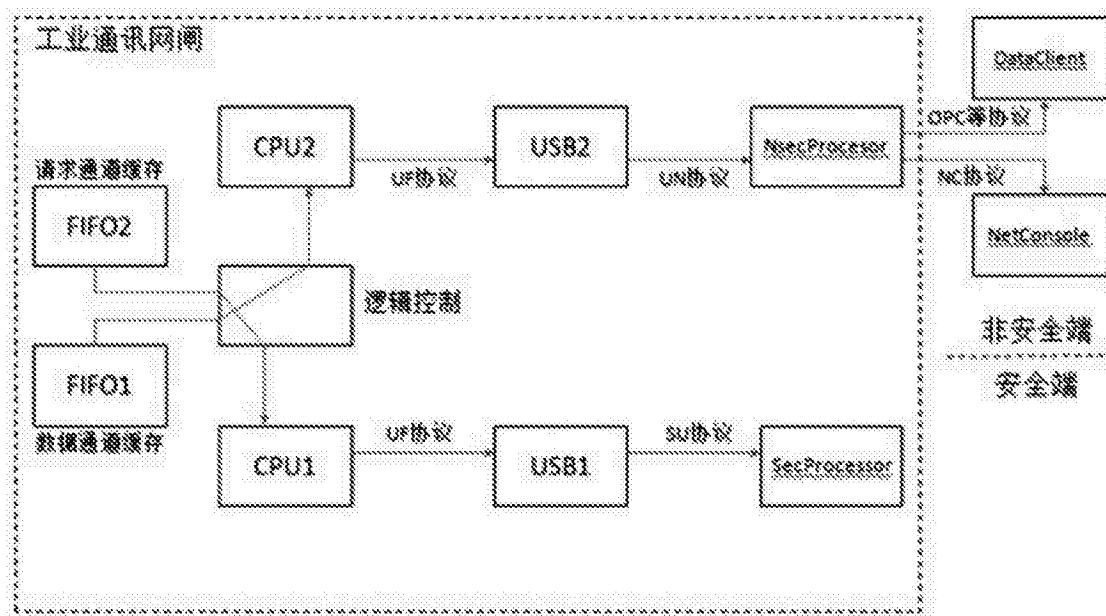


图4