(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 109120619 A
(43)申请公布日 2019.01.01

(21)申请号 201810938692.2

(22)申请日 2018.08.17

(71)申请人 西安科技大学
地址 710054 陕西省西安市雁塔区雁塔中路58号

(72)发明人 武风波 杨思捷 武文宇

(74)专利代理机构 西安铭泽知识产权代理事务所(普通合伙) 61223
代理人 李振瑞

(51)Int.Cl.
H04L 29/06(2006.01)

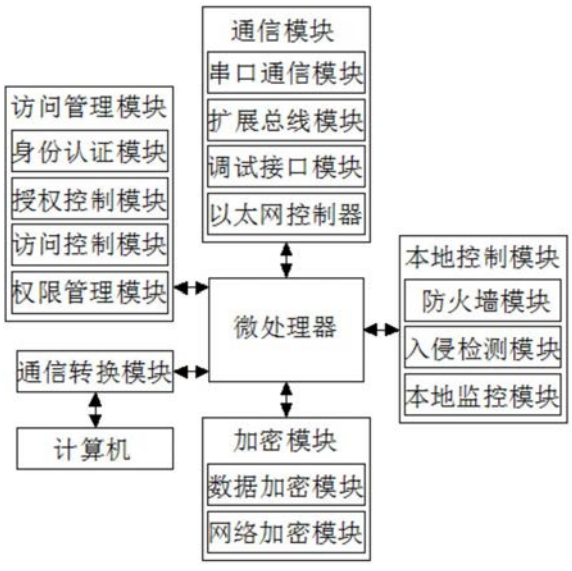
权利要求书1页 说明书3页 附图1页

(54)发明名称

一种计算机网络通信系统

(57)摘要

本发明公开的属于网络通信技术领域，具体为一种计算机网络通信系统，包括微处理器、访问控制模块、加密模块、本地控制模块和通信模块，所述访问控制模块、加密模块、本地控制模块和通信模块均与微处理器连接，所述访问控制模块包括身份认证模块、授权控制模块、访问控制模块和权限管理模块，该发明提出的一种计算机网络通信系统，集成基于主机的访问管理、网络数据加密和本地控制，实现计算机网络的全方位的管理和监控，最大程度的防止了计算机网络受到各种网络攻击，保证数据的安全传输，避免了网络风暴，提高了网络的安全性和可靠性，该发明具有功耗成本低和实时性好的优点。



CN 109120619 A

1.一种计算机网络通信系统,其特征在于:包括微处理器、访问控制模块、加密模块、本地控制模块、通信模块和通信转换模块,所述微处理器、访问控制模块、加密模块、本地控制模块、通信模块和通信转换模块均与微处理器连接,所述通信转换模块连接有计算机;

所述访问控制模块用于对使用者的访问控制,所述访问控制模块包括身份认证模块、授权控制模块、访问控制模块和权限管理模块,所述身份认证模块用于对使用者的身份的确认,所述授权控制模块用于对不同的身份授予不同的访问权限,所述访问控制模块用于对非法用户访问权限的控制,防止网络资源和数据资源被非法使用,所述权限管理模块用于对权限的管理;

所述加密模块包括数据加密模块和网络加密模块,所述数据加密模块基于RSA公开密钥密码体制,实现对数据的加密,所述网络加密模块通过加密机构把各种原始数字信号按照加密算法变换成与明文完全不同的数字信息,提高网络数据传输的安全性;

所述本地控制模块包括防火墙模块、入侵检测模块和本地健康模块,所述防火墙模块实现内部网络与外部网络的安全连接,所述入侵检测模块由于对网络入侵和病毒入侵的检测,所述本地监控模块实现对本机系统、程序和文件的监控;

所述通信模块包串口通信模块、扩展总线模块、调试接口模块和以太网控制,所述通信模块用于计算机主机的网络通信;

所述通信转换模块用于连接所述计算机和微处理器,所述通信转换模块实现所述计算机与CAN通信,所述通信转换模块包括通信接口,所述通信接口双向电性连接单片机,所述单片机双向电性连接CAN控制器,所述CAN控制器双向电性连接光电隔离模块,所述光电隔离模块双向电性连接CAN驱动器,所述CAN驱动器双向电性连接CAN总线;

所述CAN控制器实现区域网络控制,所述单片机对其进行正确的初始化后,通过访问其内部寄存器实现对CAN操作,并完成CAN物理层和数据链路层的所有协议功能,所述CAN控制器与所述光电隔离模块和CAN驱动器构成与所述CAN总线的通道。

2.根据权利要求1所述的一种计算机网络通信系统,其特征在于:所述权限管理模块包括权限增加模块、权限删除模块和权限修改模块。

3.根据权利要求1所述的一种计算机网络通信系统,其特征在于:所述网络加密模块为链路加密模块,所述链路加密模块包括专用电路、电话线、电缆和光缆。

4.根据权利要求1所述的一种计算机网络通信系统,其特征在于:所述防火墙模块采用PBNS2实现所有分布式防火墙、入侵检测策略请求和策略下发功能。

5.根据权利要求1所述的一种计算机网络通信系统,其特征在于:所述微处理器采用提供五级流水线及哈佛结构的32位的ARM920T核的S3C2410A处理器。

6.根据权利要求1所述的一种计算机网络通信系统,其特征在于:所述通信接口包括RS232接口和RS485接口,所述单片机通过所述RS232接口和RS485接口与所述计算机连接,并通过MAX232和MA485进行电平转换,实现连接不同的CAN网络,进行CAN控制器的报文交换。

一种计算机网络通信系统

技术领域

[0001] 本发明涉及网络通信技术领域,具体为一种计算机网络通信系统。

背景技术

[0002] 计算机网络通信技术是通信技术与计算机技术相结合的产物。计算机网 络是按照网络协议,将地球上分散的、独立的计算机相互连接的集合。连接 介质可以是电缆、双绞线、光纤、微波、载波或通信卫星。计算机网络具有 共享硬件、软件和数据资源的功能,具有对共享数据资源集中处理及管理和 维护的能力。随着网络上信息资源的快速增长和网络应用范围的日渐扩大, 人们在生活上和工作上对网络的依赖程度越来越高,而网络面临的安全威胁 却越来越突出,设备故障、软件缺陷、非法访问、计算机病毒、黑客攻击等 问题层出不穷,网络安全已经成为一个全球性和战略性的问题。现有的计算 机网络通信系统的网络安全性差,且解决安全性问题的手段单一,实施起来 比较繁琐,且现有的计算机网络通信系统不能够很好的应用于现场设备和现 场仪表的通信,为此,我们提出一种计算机网络通信系统。

发明内容

[0003] 本发明的目的在于提供一种计算机网络通信系统,以解决上述背景技术 中提出的问题。

[0004] 为实现上述目的,本发明提供如下技术方案:一种计算机网络通信系统, 包括微处理器、访问控制模块、加密模块、本地控制模块、通信模块和通信 转换模块,所述微处理器、访问控制模块、加密模块、本地控制模块、通信 模块和通信转换模块均与微处理器连接,所述通信转换模块连接有计算机;

[0005] 所述访问控制模块用于对使用者的访问控制,所述访问控制模块包括身 份认证模块、授权控制模块、访问控制模块和权限管理模块,所述身份认证 模块用于对使用者的身份的确认,所述授权控制模块用于对不同的身份授予 不同的访问权限,所述访问控制模块用于对非法用户访问权限的控制,防止 网络资源和数据资源被非法使用,所述权限管理模块用于对权限的管理;

[0006] 所述加密模块包括数据加密模块和网络加密模块,所述数据加密模块基 于RSA公开密钥密码体制,实现对数据的加密,所述网络加密模块通过加密 机构把各种原始数字信号按照加密算法变换成与明文完全不同的数字信息, 提高网络数据传输的安全性;

[0007] 所述本地控制模块包括防火墙模块、入侵检测模块和本地健康模块,所 述防火墙模块实现内部网络与外部网络的安全连接,所述入侵检测模块由于 对网络入侵和病毒入侵的检测,所述本地监控模块实现对本机系统、程序和 文件的监控;

[0008] 所述通信模块包串口通信模块、扩展总线模块、调试接口模块和以太网 控制,所述通信模块用于计算机主机的网络通信;

[0009] 所述通信转换模块用于连接所述计算机和微处理器,所述通信转换模块 实现所

述计算机与CAN通信，所述通信转换模块包括通信接口，所述通信接 口双向电性连接单片机，所述单片机双向电性连接CAN控制器，所述CAN控 制器双向电性连接光电隔离模块，所述光电隔离模块双向电性连接CAN驱动 器，所述CAN驱动器双向电性连接CAN总线；

[0010] 所述CAN控制器实现区域网络控制，所述单片机对其进行正确的初始化 后，通过访问其内部寄存器实现对CAN操作，并完成CAN物理层和数据链路 层的所有协议功能，所述CAN控制器与所述光电隔离模块和CAN驱动器构成 与所述CAN总线的通道。

[0011] 优选的，所述权限管理模块包括权限增加模块、权限删除模块和权限修 改模块。

[0012] 优选的，所述网络加密模块为链路加密模块，所述链路加密模块包括专 用电路、电话线、电缆和光缆。

[0013] 优选的，所述防火墙模块采用PBNS2实现所有分布式防火墙、入侵检测 策略请求和策略下发功能。

[0014] 优选的，所述微处理器采用提供五级流水线及哈佛结构的32位的ARM920T 核的S3C2410A处理器。

[0015] 优选的，所述通信接口包括RS232接口和RS485接口，所述单片机通过 所述RS232接口和RS485接口与所述计算机连接，并通过MAX232和MA485进 行电平转换，实现连接不同的CAN网络，进行CAN控制器的报文交换。

[0016] 与现有技术相比，本发明的有益效果是：该发明提出的一种计算机网络 通信系统，集成基于主机的访问管理、网络数据加密和本地控制，实现计算 机网络的全方位的管理和监控，最大程度的防止了计算机网络受到各种网络 攻击，保证数据的安全传输，避免了网络风暴，提高了网络的安全性和可靠 性，基于CAN总线的计算机网络通信系统，连接方便，使用方便，适用范围 广，具有突出的可靠性、实时性和灵活性，该发明具有功耗成本低和实时性 好的优点。

附图说明

[0017] 图1为本发明原理框图；

图2为本发明通信转换模块原理框图。

具体实施方式

[0018] 下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行 清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而 不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做 出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0019] 请参阅图1，本发明提供一种技术方案：一种计算机网络通信系统，包括 微处理器、访问控制模块、加密模块、本地控制模块、通信模块和通信转换 模块，所述微处理器、访问控制模块、加密模块、本地控制模块、通信模块 和通信转换模块均与微处理器连接，所述通信转换模块连接有计算机；

[0020] 所述访问控制模块用于对使用者的访问控制，所述访问控制模块包括身 份认证模块、授权控制模块、访问控制模块和权限管理模块，所述身份认证 模块用于对使用者的身份的确认，所述授权控制模块用于对不同的身份授予 不同的访问权限，所述访问控制模

块用于对非法用户访问权限的控制,防止 网络资源和数据资源被非法使用,所述权限管理模块用于对权限的管理;

[0021] 所述加密模块包括数据加密模块和网络加密模块,所述数据加密模块基 于RSA公开密钥密码体制,实现对数据的加密,所述网络加密模块通过加密 机构把各种原始数字信号按照加密算法变换成与明文完全不同的数字信息, 提高网络数据传输的安全性;

[0022] 所述本地控制模块包括防火墙模块、入侵检测模块和本地健康模块,所 述防火墙模块实现内部网络与外部网络的安全连接,所述入侵检测模块由于 对网络入侵和病毒入侵的检测,所述本地监控模块实现对本机系统、程序和 文件的监控;

[0023] 所述通信模块包串口通信模块、扩展总线模块、调试接口模块和以太网 控制,所述通信模块用于计算机主机的网络通信;

[0024] 所述通信转换模块用于连接所述计算机和微处理器,所述通信转换模块 实现所述计算机与CAN通信,所述通信转换模块包括通信接口,所述通信接 口双向电性连接单片机,所述单片机双向电性连接CAN控制器,所述CAN控 制器双向电性连接光电隔离模块,所述光电隔离模块双向电性连接CAN驱动 器,所述CAN驱动器双向电性连接CAN总线;

[0025] 所述CAN控制器实现区域网络控制,所述单片机对其进行正确的初始化 后,通过访问其内部寄存器实现对CAN操作,并完成CAN物理层和数据链路 层的所有协议功能,所述CAN控制器与所述光电隔离模块和CAN驱动器构成 与所述CAN总线的通道。

[0026] 其中,所述权限管理模块包括权限增加模块、权限删除模块和权限修改 模块,所述网络加密模块为链路加密模块,所述链路加密模块包括专用电路、电话线、电缆和光缆,所述防火墙模块采用PBNS2实现所有分布式防火墙、入侵检测策略请求和策略下发功能,所述微处理器采用提供五级流水线及哈 佛结构的32位的ARM920T核的S3C2410A处理器,所述通信接口包括RS232 接口和RS485接口,所述单片机通过所述RS232接口和RS485接口与所述计 算机连接,并通过MAX232和MA485进行电平转换,实现连接不同的CAN网络, 进行CAN控制器的报文交换。

[0027] 尽管已经示出和描述了本发明的实施例,对于本领域的普通技术人员而 言,可以理解在不脱离本发明的原理和精神的情况下可以对这些实施例进行 多种变化、修改、替换和变型,本发明的范围由所附权利要求及其等同物限 定。

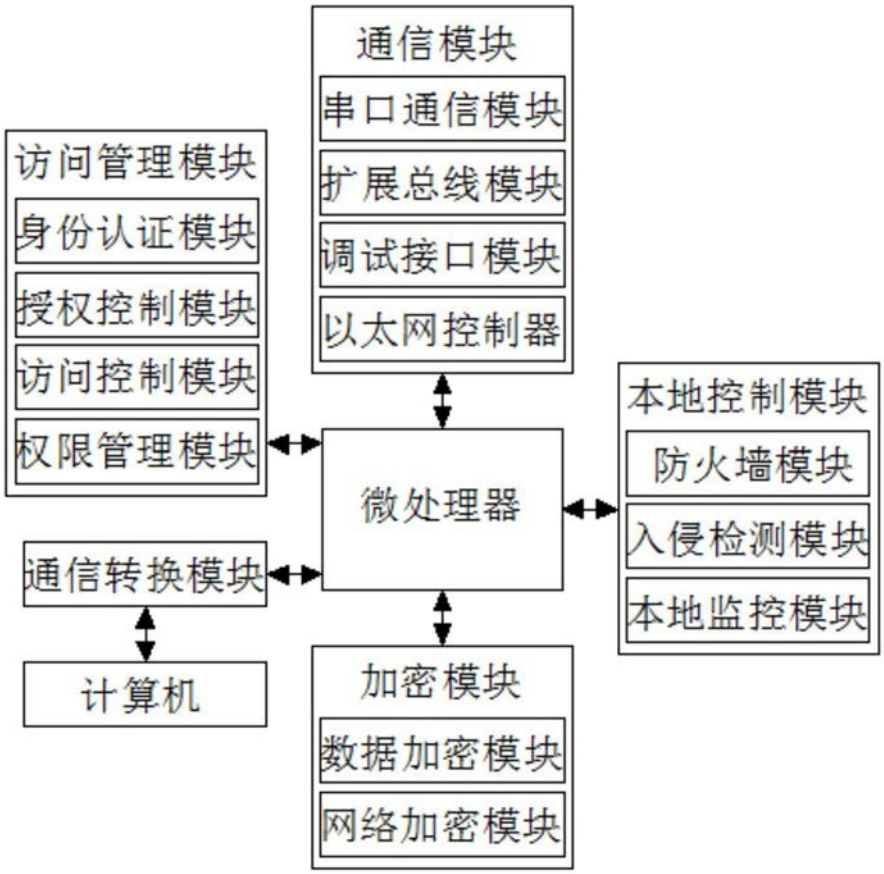

通信模块
串口通信模块
扩展总线模块
调试接口模块
以太网控制器
访问管理模块
身份认证模块
授权控制模块
访问控制模块
权限管理模块
微处理器
本地控制模块
防火墙模块
入侵检测模块
本地监控模块
通信转换模块
计算机
加密模块
数据加密模块
网络加密模块

图1

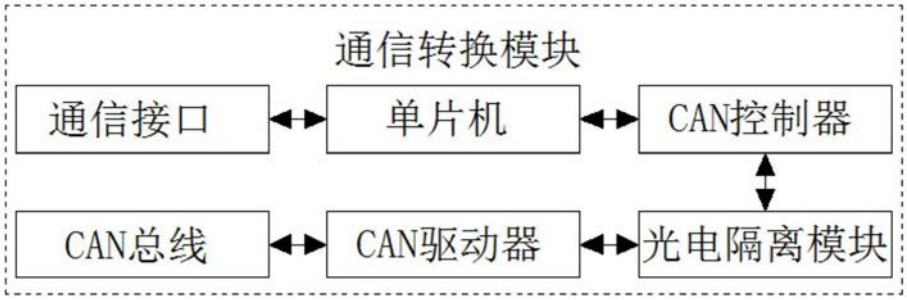

通信转换模块
通信接口
单片机
CAN控制器
CAN总线
CAN驱动器
光电隔离模块

图2