(19)中华人民共和国国家知识产权局

(12)实用新型专利

(10)授权公告号 CN 205584238 U
(45)授权公告日 2016.09.14

(21)申请号 201521128066.5

(22)申请日 2015.12.30

(73)专利权人 北京华大智宝电子系统有限公司
地址 100015 北京市朝阳区高家园一号

(72)发明人 张一帆 巩金亮 梁兵 刘洋

(74)专利代理机构 北京汇思诚业知识产权代理有限公司 11444
代理人 王刚 龚敏

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

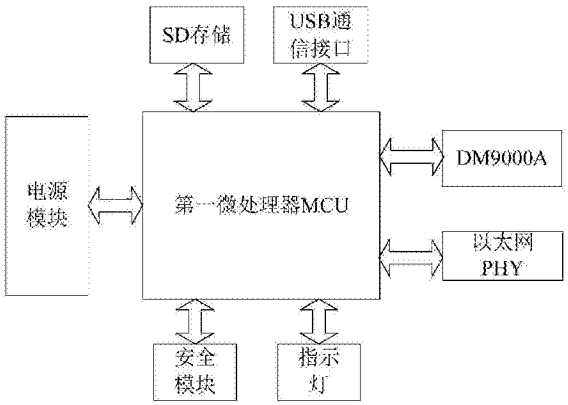
权利要求书1页 说明书4页 附图2页

(54)实用新型名称

一种网络数据加密器

(57)摘要

本实用新型提供一种网络数据加密器，包括：第一微处理器MCU、安全模块、2路工业以太网接口、SD存储、USB通信接口和电源模块；其中，所述第一微处理器MCU分别与所述安全模块、所述2路工业以太网接口、所述SD存储、所述USB通信接口和所述电源模块连接。本实用新型将国密算法引入到工业控制设备中，从数据传输和通讯网络上进行封装处理，解决工控系统中数据泄露和数据篡改的问题，可以很好的保护工控系统的运行安全，而且适用于已有工控系统信息安全等级保护的改造，提升系统的整体安全性。




CN 205584238 U

1.一种网络数据加密器，其特征在于，包括：第一微处理器MCU、安全模块、2路工业以太网接口、SD存储、USB通信接口和电源模块；

其中，所述第一微处理器MCU分别与所述安全模块、所述2路工业以太网接口、所述SD存储、所述USB通信接口和所述电源模块连接。

2.根据权利要求1所述的网络数据加密器，其特征在于，所述网络数据加密器还包括指示灯，所述指示灯与所述第一微处理器MCU连接，所述指示灯用于指示所述网络数据加密器的运行状态。

3.根据权利要求1所述的网络数据加密器，其特征在于，所述安全模块包括：加密单元、认证单元、密钥存储单元和第二微处理器MCU，其中，所述第二微处理器MCU与所述第一微处理器MCU连接，

所述第二微处理器MCU分别与所述加密单元、所述认证单元和所述密钥存储单元连接；

所述密钥存储单元用于保存加密解密运算中用的对称密钥，非对称密钥以及数字证书。

4.根据权利要求1所述的网络数据加密器，其特征在于，所述2路工业以太网接口用于在所述工业以太网中的连接，其中，所述一路接口连接到交换机，所述另外一路接口连接到工控设备。

5.根据权利要求1所述的网络数据加密器，其特征在于，所述电源模块用于为所述网络数据加密器提供稳定供电，并具有电源短路保护功能和过压保护功能。

# 一种网络数据加密器

## 技术领域

[0001] 本实用新型涉及工业信息安全技术领域，尤其涉及一种网络数据加密器。

## 背景技术

[0002] 随着企业信息化的发展和工业综合自动化进程的深入，计算机网络技术越来越多地应用于工业信息控制系统。我国的工业信息系统大多是在引进成套设备的同时进行消化吸收，关键基础设施使用的几乎都是德国Siemens、美国Honeywell、Rockwell和日本横河等国外厂商的控制系统和软件。我国工控领域的高端市场、嵌入式操作系统、嵌入式软件、总线协议和工控软件等核心技术均受制于国外。

[0003] 在为工业生产带来极大效益的同时，也使得针对工业信息控制系统的攻击行为出现大幅度地增长，因此，对工业信息安全的需求变得更加迫切。

[0004] 在工业基础设施中，关键的工业控制系统引发的安全事件不仅会导致系统性能下降、可用性降低、关键控制数据被篡改或丧失、系统失控进而影响生产安全并导致严重的经济损失，而且还可能会进一步导致人员伤亡、环境灾难、危及公众生活甚至国家安全等。因此，工业控制系统的安全运行是确保基础设施正常运行的重要基础，是系统全生命周期内始终需要关注的重要指标。

[0005] 现有工控系统的安全防护措施更多地放在服务器和网络的保护上，并没有从根本上解决工控系统的安全问题，缺乏对设备的身份鉴别和数据传输方面的防护措施，主要存在以下问题：设备的非法接入、协议开放、数据明文传输、非法操作、网络脆弱性和数据篡改等。一旦工业现场的重要控制指令被截取，将对工控系统造成很大的威胁。

## 发明内容

[0006] 因此，为了解决上述技术问题，本实用新型提供一种网络数据加密器，将国密算法引入到工业控制设备中，从数据传输和通讯网络上进行封装处理，解决工控系统中数据泄露和数据篡改的问题，可以很好的保护工控系统的运行安全，而且适用于已有工控系统信息安全等级保护的改造，提升系统的整体安全性。

[0007] 本实用新型提供一种网络数据加密器，包括：第一微处理器MCU、安全模块、2路工业以太网接口、SD存储、USB通信接口和电源模块；其中，所述第一微处理器MCU分别与所述安全模块、所述2路工业以太网接口、所述SD存储、所述USB通信接口和所述电源模块连接。

[0008] 上述方案中优选的是，所述网络数据加密器还包括指示灯，所述指示灯与所述第一微处理器MCU连接，所述指示灯用于指示所述网络数据加密器的运行状态。

[0009] 上述方案中优选的是，所述SD存储用于保存所述网络数据加密器的配置文件和日志信息。

[0010] 上述方案中优选的是，所述安全模块包括：加密单元、认证单元、密钥存储单元和第二微处理器MCU，

[0011] 其中，所述第二微处理器MCU与所述第一微处理器MCU连接，

[0012] 所述第二微处理器MCU分别与所述加密单元、所述认证单元和所述密钥存储单元连接。

[0013] 上述方案中优选的是，所述2路工业以太网接口用于在所述工业以太网中的连接，其中，所述一路接口连接到交换机，所述另外一路接口连接到工控设备。

[0014] 上述方案中优选的是，所述USB通信接口用于配置更新。

[0015] 上述方案中优选的是，所述电源模块用于为所述网络数据加密器提供稳定供电，并具有电源短路保护功能和过压保护功能。

[0016] 上述方案中优选的是，所述安全模块中的所述密钥存储模块用于保存加密解密运算中用的对称密钥，非对称密钥以及数字证书。

[0017] 本实用新型所述的网络数据加密器在不需要更改原有设备的情况下，对设备的数据出口进行加密控制，解决了设备的安全接入和安全访问的问题，可以快速的建立整个安全防护体系，为工业信息等建立强大的安全保护手段，防止数据被非法窃取，篡改与毁坏，保证数据的秘密性，真实性和完整性，采用的主要技术有国密算法、对称加密、非对称加密、签名证书、安全认证和网络通道加密。实现对终端设备的注册、认证和管理，实现“合法终端访问合法网络，合法的平台管理合法的设备”的目标，对防止信息未经过授权使用和误用起到支撑作用。

## 附图说明

[0018] 为了更清楚地说明本实用新型实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图是本实用新型的一些实施例，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。

[0019] 图1是本实用新型所述的一种网络数据加密器的结构示意图。

[0020] 图2是本实用新型所述的一种网络数据加密器中的安全模块的结构示意图。

[0021] 图3是本实用新型提供的如图1所述的网络数据加密器的使用示意图。

## 具体实施方式

[0022] 为使本实用新型的目的、技术方案和优点更加清楚，以下将参照本实用新型实施例中的附图，通过实施方式清楚、完整地描述本实用新型的技术方案，显然，所描述的实施例是本实用新型一部分实施例，而不是全部的实施例。基于本实用新型中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本实用新型保护的范围。

[0023] 本实用新型所述的网络数据加密器以MCU微处理器为核心，辅以强大功能的外围数字电路模块，使网络数据加密器能够与远端认证服务器建立安全数据传输通道，并同时加密或者解密传输的数据。

[0024] 下面对本实用新型提供的技术方案做详细公开的说明，参考图1所示为本实用新型提供的一种网络数据加密器的结构示意图。包括：第一微处理器MCU、2路工业以太网接口(即以太网PHY和DM9000A这两路接口)、安全模块、指示灯、SD存储、USB通信接口和电源模块。

[0025] 其中，第一微处理器MCU采用主频200MHZ的工业级Cortex-M4处理器，该处理器具有丰富的外围接口，可以很好的支撑外围设备的开发。

[0026] 图2是本实用新型所述的一种网络数据加密器中的安全模块的结构示意图。安全模块是该网络数据加密器的核心，采用国家密码检测的国密芯片。它由加密单元、认证单元、密钥存储单元和第二微处理器MCU组成。所述第二微处理器MCU是高度集成的数据安全专用芯片和高性能的微处理器，采用32位CPU内核，具有十年以上数据保持时间，配备硬件随机数发生器，具有硬件SM1、SM2、SM3、SM4等国密算法协处理器以及DES、ECC、AES，其工作温度范围为-40℃～85℃。

[0027] 所述2路工业以太网接口(即图1中的以太网PHY和DM9000A这两路接口)用于工业以太网中的连接。其中，一路连接到交换机，另外一路连接到工控设备，如DCS、PLC等。使得本实用新型所述的网络数据加密器可以直接串联在工控设备与网络设备之间，实现无IP连接。

[0028] 所述SD存储用于保存所述网络数据加密器的配置文件以及关键的日志信息。

[0029] 所述USB通信接口是外部的管理接口，用于配置的更新等。

[0030] 所述指示灯用于指示设备当前的运行状态，例如：运行指示、状态指示或报警指示等。

[0031] 所述电源模块采用单电源输入，使用高端的电源芯片为网络数据加密器提供最大3A的电流，并具有电源短路保护功能和过压保护功能。

[0032] 本实用新型所述的网络数据加密器内嵌实时操作系统，以国密算法为技术核心，根据TCP/IP网络协议规范，应用于工业控制系统的安全防护设备。所述网络数据加密器支持明文数据的加密功能，密文数据的解密功能，工业以太网协议，例如modbus、profinet等。还支持国密算法SM1、SM2、SM3、SM4以及国际算法AES、ECC等。支持USB数据接口的外部管理功能，实现对网路加密器的配置文件的更新。支持密钥在线更新，数字证书的在线更新。具备数字证书功能，能够提供设备的身份认证。通过设置软件旁路功能，实现加密传输和透明传输的灵活切换。本实用新型所述的加密器无IP设置，支持数据应用层加密和数据链路层加密。

[0033] 图3是本实用新型提供的如图1所述的网络数据加密器的使用示意图。所述网络数据加密器利用国密对称算法SM1、SM2和非对称算法SM2，通过数字证书的方式，即通过所述安全模块的认证单元。网络数据加密器在接入网络时通过认证服务器进行统一管理：首先，认证服务器和网络数据加密器进行双向身份鉴别，当设备与设备之间通信时通过数字证书进行身份鉴别。通过双向认证的方式保证数据来源的正确性。

[0034] 所述网络数据加密器利用安全模块中的加密单元，采用SM1或者SM4对称算法，将工业以太网传输过来的数据进行加密或者解密，数据处理完成后MCU再通过另一个端口输出，保证传输数据机密性。

[0035] 所述网络数据加密器将以太网接收到的明文信息经过SM3摘要算法进行计算，利用摘要计算的不可逆原理，在接收端对接收的数据做完整性校验，实现数据的完整性。

[0036] 由于所述网络数据加密器是用在DCS控制器、PLC与交换机之间，如果每台应用都要设置IP的话工作量非常大，而且在每一个网络环境中都会占用IP资源。为了便于现场实施，本实用新型采用无IP连接技术，通过解析TCP/IP协议包，在数据链路层进行解析。并将

数据进行加密。避免了IP层的数据验证。同时按照TCP/IP的数据包格式将加密后的数据进行重新打包发送。

[0037] 在所述安全模块中保存密钥，通过认证单元，即认证服务器，可以设置定期的密钥更新。所述网络数据加密器在通讯协议中可以灵活设置所选用的加密算法和算法密钥，提高数据的保密性。并且具有密钥存储功能，负责保存加密解密运算中用的对称密钥，非对称密钥以及数字证书等。

[0038] 所述网络数据加密器本地就具有存储功能，能够对配置信息及重要日志信息可以进行加密保存。

[0039] 本实用新型所述的网络数据加密器将国密算法这一机密性较高的加密方法应用到网络的数据传输中，有效的解决目前传统网络加密数据容易被破解的问题。同时易于接入已有的网络设备系统，便于实施，提高了工业信息系统的安保水平。

[0040] 以上所述仅是本实用新型的具体实施方式，对于本技术领域的普通技术人员来说，在不脱离本实用新型原理的前提下，还可以做出若干改进和润饰，这些改进和润饰也应视为本实用新型的保护范围。

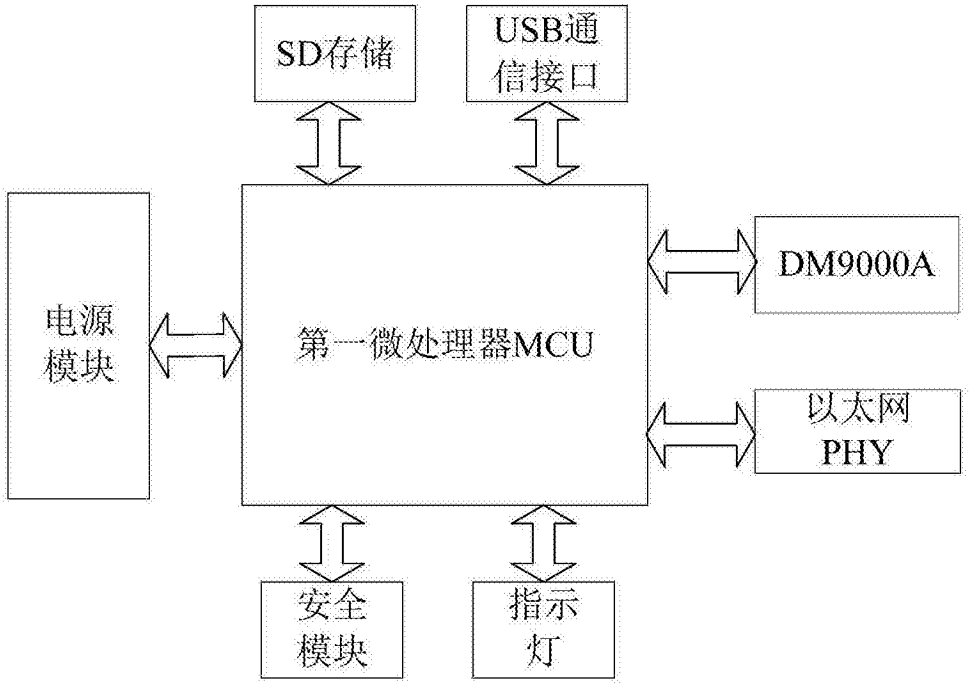

SD存储
USB通信接口
电源模块
第一微处理器MCU
DM9000A
以太网PHY
安全模块
指示灯

图1

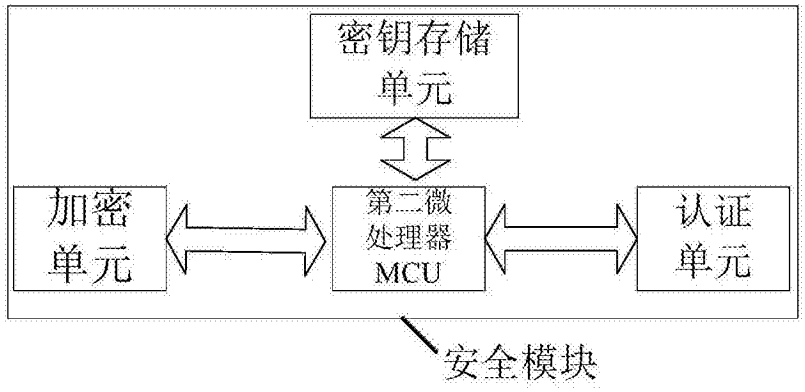

密钥存储单元
加密单元
第二微处理器MCU
认证单元
安全模块

图2

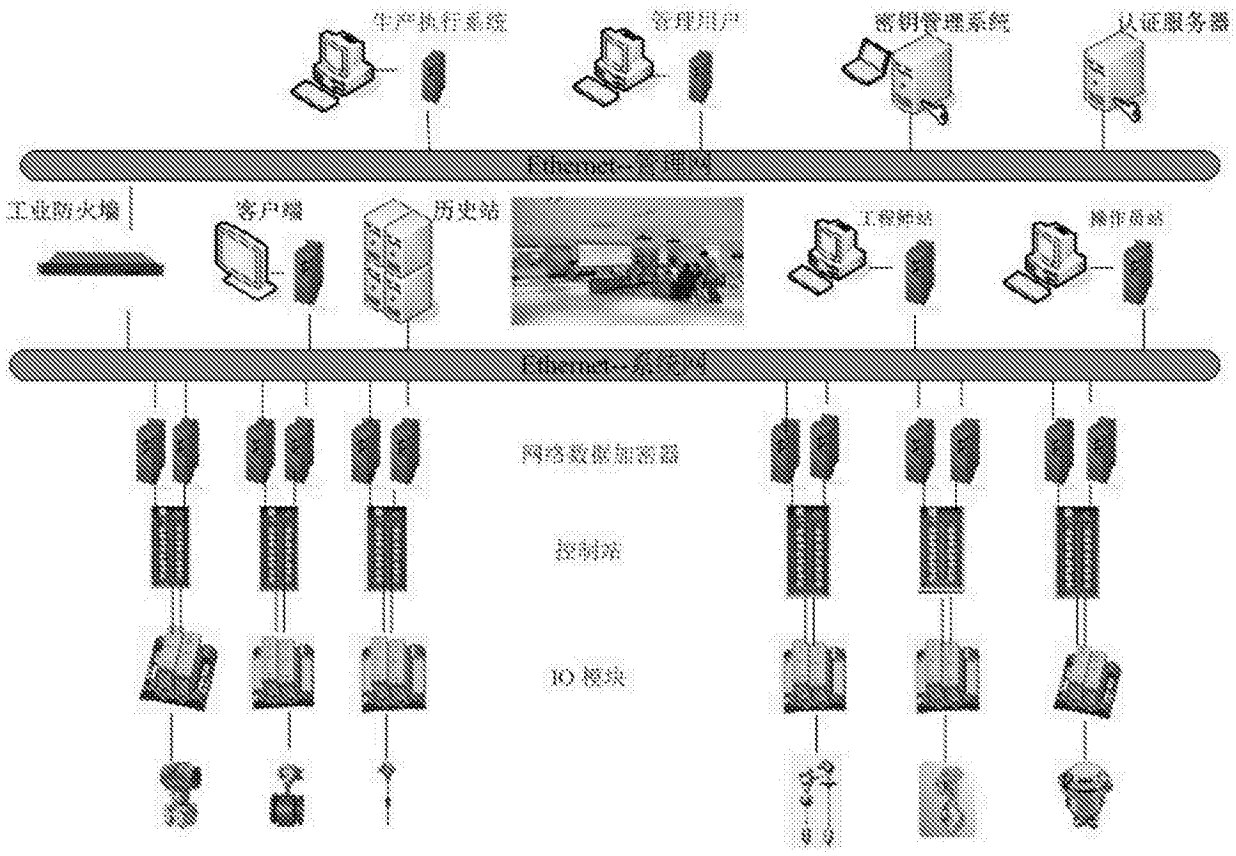



图3