(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 106100836 B
(45)授权公告日 2019.02.12

(21)申请号 201610647319.2
(22)申请日 2016.08.09
(65)同一申请的已公布的文献号
申请公布号 CN 106100836 A
(43)申请公布日 2016.11.09
(73)专利权人 中京天裕科技(北京)有限公司
地址 100085 北京市海淀区上地信息路科贸大厦306室
(72)发明人 晏培
(74)专利代理机构 北京汇信合知识产权代理有限公司 11335
代理人 王秀丽
(51)Int.Cl.
*H04L 9/08*(2006.01)
*H04L 29/06*(2006.01)

审查员 陈玲珑

权利要求书2页 说明书5页 附图2页

(54)发明名称

一种工业用户身份认证和加密的方法及系统

(57)摘要

本发明涉及工业信息安全技术领域,具体而言,涉及一种工业用户身份认证和加密的方法及系统。该方法包括:将电子钥匙通过USB接口接入用户终端设备,并通过用户终端设备登录客户端;客户端比对用户终端设备的硬件特征码和电子钥匙绑定的硬件特征码,若一致,且认证服务器验证用户证书具有合法性,则客户端获取工控指令信息并进行加密、封装处理,得到加密的数据包;客户端将所述数据包传输给加密网关;加密网关将所述数据包进行拆包、解密处理,得到解密的工控指令信息,并将其传输给OPC服务器。解决了现阶段工业信息系统数据传输安全性低,无法保证数据包的真实性的问题。


CN 106100836 B

1.一种工业用户身份认证和加密的方法,其特征在于,包括:

步骤1:获取电子钥匙,所述电子钥匙包括用户证书、第一硬件特征码;

步骤2:电子钥匙通过USB接口接入用户终端设备,并启动客户端;

步骤3:客户端获取所述第一硬件特征码以及所述用户终端设备的第二硬件特征码,比对所述第一硬件特征码、第二硬件特征码,若一致,则进行步骤4;否则终止;

步骤4:客户端获取所述用户证书,并将所述用户证书传输给认证服务器;

步骤5:认证服务器验证所述用户证书的合法性,若认证通过,并将通过信息发送至客户端,进行步骤6;否则终止;

步骤6:客户端将工控指令信息进行加密处理,得到加密的工控指令信息;

步骤7:客户端将所述加密的工控指令信息进行隧道封装处理,得到数据包;客户端软件集成工控协议引擎,只有工业控制协议的数据包才进行安全加密和数据封装,其它数据不进隧道,保证传输到服务器端的数据只有工业控制协议的数据包,并且加密算法使用国密算法;

步骤8:客户端将所述数据包传输给加密网关;

步骤9:所述加密网关将所述数据包进行拆包、解密处理,得到解密的工控指令信息;同时,所述加密网关对所述解密的工控指令信息进行过滤处理;

步骤10:所述加密网关将所述解密的工控指令信息传输给OPC服务器。

2.如权利要求1所述的一种工业用户身份认证和加密的方法,其特征在于,所述电子钥匙由证书授权中心统一管理;和/或,

所述电子钥匙还包括:国家密码管理局批准的加密算法、用户基本信息,所述用户基本信息包括用户名、单位、部门、电话号码和邮箱地址。

3.如权利要求1所述的一种工业用户身份认证和加密的方法,其特征在于,所述第一硬件特征码为与唯一用户终端设备绑定的硬件特征码。

4.如权利要求1所述的一种工业用户身份认证和加密的方法,其特征在于,所述认证服务器包括OCSP认证服务器和LDAP认证服务器。

5.如权利要求1所述的一种工业用户身份认证和加密的方法,其特征在于,所述加密网关包括工业控制防火墙设备。

6.一种工业用户身份认证和加密的系统,其特征在于,包括:权利要求1-5任一项所述的客户端、认证服务器、加密网关和OPC服务器;

所述客户端包括:读取模块、验证模块、加密模块、封装模块和传输模块,所述读取模块用于读取电子钥匙中的用户证书、第一硬件特征码信息;所述验证模块用于比对第一硬件特征码与用户终端设备的第二硬件特征码;所述加密模块用于对工控指令信息进行加密处理,得到加密的工控指令信息;所述封装模块用于对所述加密的工控指令信息进行隧道封装处理,得到数据包;所述传输模块用于将所述数据包传输给加密网关;

此外,客户端软件集成工控协议引擎,只有工业控制协议的数据包才进行安全加密和数据封装,其它数据不进隧道,保证传输到服务器端的数据只有工业控制协议的数据包,并且加密算法使用国密算法;

所述认证服务器用于验证用户证书合法性;

所述加密网关用于将所述数据包进行拆包、解密处理,得到解密的工控指令信息;此

外,所述加密网关还用于对所述解密的工控指令信息进行过滤处理;

所述OPC服务器接收所述解密的工控指令信息,并根据所述解密的工控指令信息执行相关操作。

7.如权利要求6所述的一种工业用户身份认证和加密的系统,其特征在于,所述认证服务器包括OCSP认证服务器和LDAP认证服务器。

8.如权利要求6所述的一种工业用户身份认证和加密的系统,其特征在于,所述加密网关包括工业控制防火墙设备。

# 一种工业用户身份认证和加密的方法及系统

## 技术领域

[0001] 本发明涉及工业信息安全技术领域，具体而言，涉及一种工业用户身份认证和加密的方法及系统。

## 背景技术

[0002] 随着信息技术和网络技术在工业系统中应用的普及，开放、互连和标准化已经成为工业信息系统发展的必然趋势，工业系统对信息系统的依赖性也越来越强，所以工业信息系统的安全问题也越来越引起人们的重视，现有的计算机系统、信息网络、业务系统及人们的安全意识已经有一定的安全基础，但对于工业信息系统网络目前还处于快速发展阶段，现有的安全产品比如防火墙、VPN(Virtual Private Network，虚拟专用网)也无法直接用于工业信息系统，虽然目前市场上也有工业控制防火墙专门针对工业协议进行控制，但工业控制防火墙只解决了对数据包的过滤和控制，无法保证数据包的真实性，工业信息系统目前还没有比较成熟的安全解决方案。

[0003] 工业信息安全需求已经迫在眉睫，本发明结合传统安全相关技术，针对工业信息系统的特点，发明一种工业用户身份认证和加密系统，解决工业信息系统数据传输安全问题。

## 发明内容

[0004] 本发明的目的在于提供一种工业用户身份认证和加密的方法及系统，以解决现阶段工业信息系统数据传输安全性低，无法保证数据包的真实性的问题。

[0005] 本发明提供了一种工业用户身份认证和加密的方法，其包括：

[0006] 步骤1：获取电子钥匙，所述电子钥匙包括用户证书、第一硬件特征码；

[0007] 步骤2：电子钥匙通过USB接口接入用户终端设备，并启动客户端；

[0008] 步骤3：客户端获取所述第一硬件特征码以及所述用户终端设备的第二硬件特征码，比对所述第一硬件特征码、第二硬件特征码，若一致，则进行步骤4；否则终止；

[0009] 步骤4：客户端获取所述用户证书，并将所述用户证书传输给认证服务器；

[0010] 步骤5：认证服务器验证所述用户证书的合法性，若认证通过，并将通过信息发送至客户端，进行步骤6；否则终止；

[0011] 步骤6：客户端将工控指令信息进行加密处理，得到加密的工控指令信息；

[0012] 步骤7：客户端将所述加密的工控指令信息进行隧道封装处理，得到数据包；

[0013] 步骤8：客户端将所述数据包传输给加密网关；

[0014] 步骤9：所述加密网关将所述数据包进行拆包、解密处理，得到解密的工控指令信息；

[0015] 步骤10：所述加密网关将所述解密的工控指令信息传输给OPC服务器。

[0016] 在一些实施例中，优选为，所述电子钥匙由证书授权中心统一管理。

[0017] 在一些实施例中，优选为，所述电子钥匙还包括：国家密码管理局批准的加密算

法、用户基本信息，所述用户基本信息包括用户名、单位、部门、电话号码和邮箱地址。

[0018] 在一些实施例中，优选为，所述第一硬件特征码为与唯一用户终端设备绑定的硬件特征码。

[0019] 在一些实施例中，优选为，所述认证服务器包括OCSP认证服务器和LDAP认证服务器。

[0020] 在一些实施例中，优选为，所述步骤9中还包括：加密网关对所述解密的工控指令信息记性过滤处理。

[0021] 在一些实施例中，优选为，所述加密网关包括工业控制防火墙设备。

[0022] 本发明还提供了一种工业用户身份认证和加密的系统，其包括：权利要求1-6任一项所述的客户端、认证服务器、加密网关和OPC服务器；

[0023] 所述客户端包括：读取模块、验证模块、加密模块、封装模块和传输模块，所述读取模块用于读取电子钥匙中的用户证书、第一硬件特征码信息；所述验证模块用于比对第一硬件特征码与用户终端设备的第二硬件特征码；所述加密模块用于对工控指令信息进行加密处理，得到加密的工控指令信息；所述封装模块用于对所述加密的工控指令信息进行隧道封装处理，得到数据包；所述传输模块用于将所述数据包传输给加密网关；

[0024] 所述认证服务器用于验证用户证书合法性；

[0025] 所述加密网关用于将所述数据包进行拆包、解密处理，得到解密的工控指令信息；

[0026] 所述OPC服务器接收所述解密的工控指令信息，并根据所述解密的工控指令信息执行相关操作。

[0027] 针对上述系统，进一步，在一些实施例中，优选为，所述认证服务器包括OCSP认证服务器和LDAP认证服务器。

[0028] 进一步，在一些实施例中，优选为，所述加密网关包括工业控制防火墙设备。

[0029] 本发明实施例提供的工业用户身份认证和加密的方法及系统，与现有技术相比，通过获取电子钥匙，其中电子钥匙与终端设备硬件绑定，只要经过授权的终端设备才有操作权利，防止未授权用户和设备的非法操作。所以客户端进行比对用户终端设备的硬件特征码与电子钥匙绑定的硬件特征码，并且还会通过认证服务器验证所述用户证书的合法性，双重验证处理，可保证数据传输过程中其实设备的安全性和操作权。另外，客户端在将工控指令信息传输之前会对其进行加密封装处理，在意保证了数据传输的安全性。因此，本发明公开的工业用户身份认证和加密的方法有效的解决了现阶段工业信息系统数据传输安全性低，无法保证数据包的真实性的问题。

## 附图说明

[0030] 图1为本发明一个实施例中工业用户身份认证和加密的方法步骤示意图；

[0031] 图2为本发明一个实施例中工业用户身份认证和加密的系统结构示意图。

## 具体实施方式

[0032] 为使本发明实施例的目的、技术方案和优点更加清楚，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，所描述的实施例是本发明的一部分实施例，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的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。

[0033] 针对现阶段工业信息系统数据传输安全性低,无法保证数据包的真实性的问题,本发明提出了一种工业用户身份认证和加密的方法及系统。

[0034] 如图1-2所示,其具体包括:

[0035] 步骤1:获取电子钥匙,电子钥匙包括用户证书、第一硬件特征码。

[0036] 电子钥匙由证书授权中心统一管理,每个电子钥匙里面包含一个用户证书同时集成国家密码管理局批准的相关加密算法;用户证书由证书授权CA中心统一颁发。用户证书里面包含用户基本信息,用户基本信息包括用户名、单位、部门、电话号码和邮箱地址;每个电子钥匙里面还包含一个终端设备的硬件特征码。电子钥匙与终端设备硬件绑定,只要经过授权的终端设备才有操作权利,防止未授权用户和设备的非法操作。

[0037] 步骤2:电子钥匙通过USB接口接入用户终端设备并启动客户端软件。

[0038] 客户端软件安装在用户终端设备上,用户在使用客户端软件时需插入电子钥匙,每个电子钥匙只能和一台终端设备绑定,用户终端设备能从电子钥匙中读取数据;网关设备与用户终端设备进行双向信息交互;户终端设备与认证服务器进行双向信息交互。客户端软件集成工控协议引擎,只有工业控制协议的数据包才进行安全加密和数据封装,其它数据不进隧道,保证传输到服务器端的数据只有工业控制协议的数据包,并且加密算法使用国密算法。

[0039] 步骤3:客户端获取第一硬件特征码以及用户终端设备的第二硬件特征码,比对第一硬件特征码、第二硬件特征码,若一致,则进行步骤4;否则终止。

[0040] 步骤4:客户端获取用户证书,并将用户证书传输给认证服务器。

[0041] 步骤5:认证服务器验证用户证书的合法性,若认证通过,并将通过信息发送至客户端,进行步骤6;否则终止。

[0042] 步骤6:客户端将工控指令信息进行加密处理,得到加密的工控指令信息。

[0043] 步骤7:客户端将加密的工控指令信息进行隧道封装处理,得到数据包。

[0044] 步骤8:客户端将数据包传输给加密网关。

[0045] 步骤9:加密网关将数据包进行拆包、解密处理,得到解密的工控指令信息,加密网关对解密的工控指令信息记性过滤处理。

[0046] 因此,加密网关除负责数据解密和转发外,还负责对解密后的工业控制协议数据的深度过滤,有效控制非法指令的执行。

[0047] 步骤10:加密网关将解密的工控指令信息传输给OPC服务器,OPC服务器收到相关指令信息后执行相关操作,至此一条工业控制指令通过专用隧道安全传输完成。

[0048] 客户端软件的主要功能是:①计算终端设备的硬件特征码;②读取电子钥匙中绑定的硬件特征码并和计算出的硬件特征码做比较;③读取电子钥匙里面的证书并通过认证服务器进行证书认证;④通过工控协议引擎模块实时监听终端设备发送的工控协议数据包;⑤通过电子钥匙中提供的硬件加密算法对数据包加密和封装;⑥发送加密后的数据包。

[0049] 认证服务器用于对证书授权中心统一颁发的用户证书进行用户身份验证,认证服务器包括OCSP(Online Certificate Status Protocol,在线证书状态协议)认证服务器和LDAP(Lightweight Directory Access Protocol,轻量目录访问协议)认证服务器。

[0050] 加密网关包括:工业控制防火墙设备。网关软件安装在加密网关设备上,其主要功

能是:①从用户终端设备接收加密封装后的工控协议数据包;②解密数据包;③查找工控策略;④查找策略路由;⑤转发数据包给OPC服务器。

[0051] 针对上述方法,本发明提供了工业用户身份认证和加密的系统,其包括:权利要求1-6任一项的客户端、认证服务器、加密网关和OPC服务器。客户端包括:读取模块、验证模块、加密模块、封装模块和传输模块,读取模块用于读取电子钥匙中的用户证书、第一硬件特征码信息;验证模块用于比对第一硬件特征码与用户终端设备的第二硬件特征码;加密模块用于对工控指令信息进行加密处理,得到加密的工控指令信息;封装模块用于对加密的工控指令信息进行隧道封装处理,得到数据包;传输模块用于将数据包传输给加密网关。认证服务器用于验证用户证书合法性。加密网关用于将数据包进行拆包、解密处理,得到解密的工控指令信息。OPC服务器接收解密的工控指令信息,并根据解密的工控指令信息执行相关操作。

[0052] 在该系统中,认证服务器包括OCSP认证服务器和LDAP认证服务器。加密网关包括工业控制防火墙设备。其具体原理同上述工业用户身份认证和加密的方法的原理相同,故不作详细陈述。

[0053] 针对上述工业用户身份认证和加密的方法及系统,给出两个具体实施例:

[0054] 实施例1:

[0055] 实施例1中的实现工业用户身份认证和加密系统包括硬件设备和相关软件。硬件设备包括:加密网关、电子钥匙、用户终端设备、认证服务器;相关软件包括:客户端软件和网关软件。

[0056] 客户端软件安装在用户终端设备上,用户在使用客户端软件时需插入电子钥匙,每个电子钥匙只能和一台终端设备绑定,用户终端设备能从电子钥匙中读取数据;网关设备与用户终端设备进行双向信息交互;户终端设备与认证服务器进行双向信息交互。

[0057] 电子钥匙由证书授权中心统一管理,每个电子钥匙里面包含一个用户证书同时集成国家密码管理局批准的相关加密算法;用户证书由证书授权中心统一颁发;用户证书里面包含用户基本信息,所述用户基本信息包括用户名、单位、部门、电话号码和邮箱地址;每个电子钥匙里面还包含一个终端设备的硬件特征码。

[0058] 客户端软件的主要功能是:①计算终端设备的硬件特征码;②读取电子钥匙中绑定的硬件特征码并和计算出的硬件特征码做比较;③读取电子钥匙里面的证书并通过认证服务器进行证书认证;④通过工控协议引擎模块实时监听终端设备发送的工控协议数据包;⑤通过电子钥匙中提供的硬件加密算法对数据包加密和封装;⑥发送加密后的数据包。

[0059] 所述认证服务器用于对证书授权中心统一颁发的用户证书进行用户身份验证,认证服务器包括OCSP认证服务器和LDAP认证服务器。

[0060] 所述加密网关为工业控制防火墙,认证服务器为LDAP服务器。

[0061] 网关软件安装在加密网关设备上,其主要功能是:①从用户终端设备接收加密封装后的工控协议数据包;②解密数据包;③查找工控策略;④查找策略路由;⑤转发数据包给OPC服务器。

[0062] 使用所述工业用户身份认证和加密系统进行信息传输的流程如图2所示,具体为:

[0063] 步骤1:用户终端设备发送一条工业控制指令;

[0064] 步骤2:客户端软件通过使用集成在客户端软件中的工控协议引擎获取工控指令

信息；

[0065] 步骤3：客户端软件计算用户终端设备的硬件编码，然后读取电子钥匙中绑定的硬件编码进行比对，如果一致，则执行第4步操作；否则，终止当前操作；

[0066] 步骤4：客户端软件读取电子钥匙中的用户证书，然后通过认证服务器对证书合法性进行认证，认证通过，则执行第5步操作；否则，终止当前操作；

[0067] 步骤5：客户端软件使用国家密码管理局指定算法对工控指令信息进行加密和隧道封装；

[0068] 步骤6：客户端软件将封装后的工控指令信息发送给加密网关；

[0069] 步骤7：加密网关接收加密后的工控指令信息并解密后转发给OPC服务器，OPC服务器收到相关指令信息后执行相关操作，至此一条工业控制指令通过专用隧道安全传输完成。

[0070] 实施例2：

[0071] 实施例2中的实现工业用户身份认证和加密系统结构与实施例1中的系统相同，区别仅在于：认证服务器为OCSP认证服务器，用户证书采用在线认证方式。

[0072] 使用所述工业用户身份认证和加密系统进行信息传输的流程如图2所示，具体为：

[0073] 步骤1：用户终端设备发送一条工业控制指令；

[0074] 步骤2：客户端软件通过使用集成在客户端软件中的工控协议引擎获取工控指令信息；

[0075] 步骤3：客户端软件计算用户终端设备的硬件编码，然后读取电子钥匙中绑定的硬件编码进行比对，如果一致，则执行第4步操作；否则，终止当前操作；

[0076] 步骤4：客户端软件读取电子钥匙中的用户证书，然后通过认证服务器对证书合法性进行认证，认证通过，则执行第5步操作；否则，终止当前操作；

[0077] 步骤5：客户端软件使用国家密码管理局指定算法对工控指令信息进行加密和隧道封装；

[0078] 步骤6：客户端软件将封装后的工控指令信息发送给加密网关；

[0079] 步骤7：加密网关接收加密后的工控指令信息并解密后转发给OPC服务器，OPC服务器收到相关指令信息后执行相关操作，至此一条工业控制指令通过专用隧道安全传输完成。

[0080] 以上仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

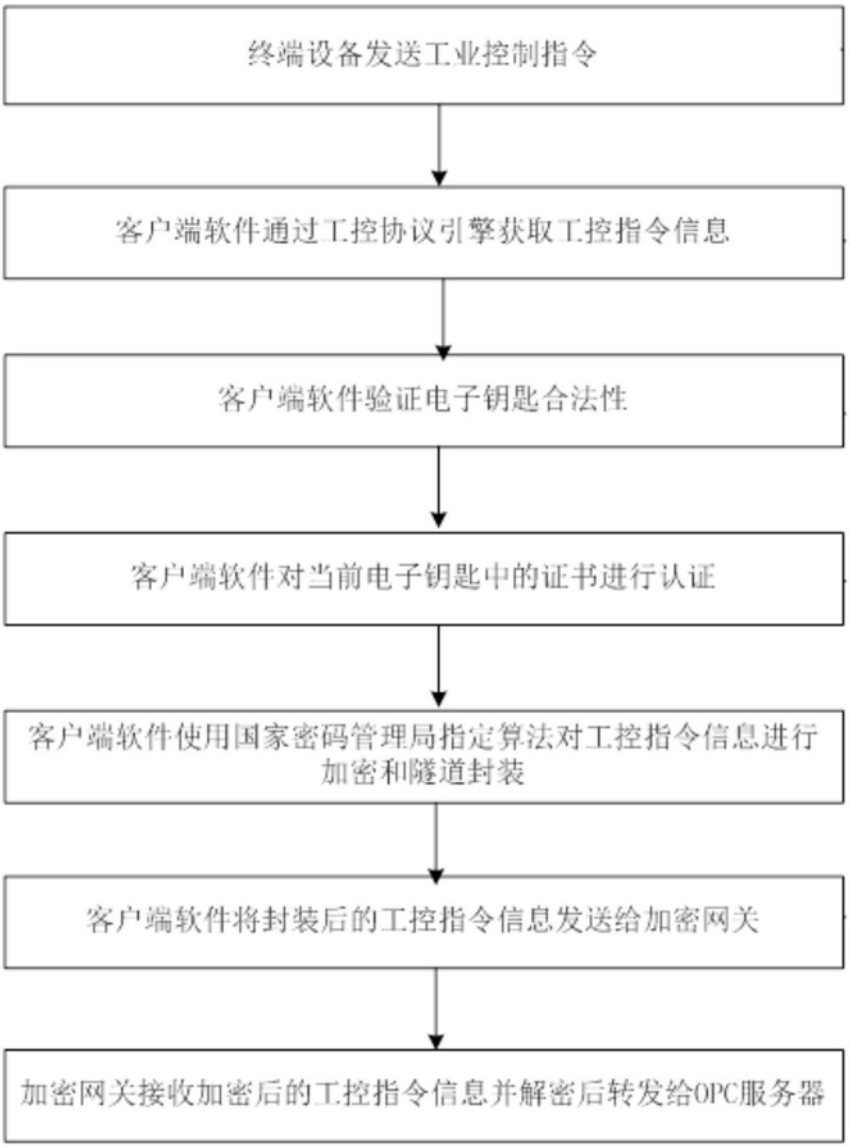
终端设备发送工业控制指令
客户端软件通过工控协议引擎获取工控指令信息
客户端软件验证电子钥匙合法性
客户端软件对当前电子钥匙中的证书进行认证
客户端软件使用国家密码管理局指定算法对工控指令信息进行加密和隧道封装
客户端软件将封装后的工控指令信息发送给加密网关
加密网关接收加密后的工控指令信息并解密后转发给OPC服务器

图1

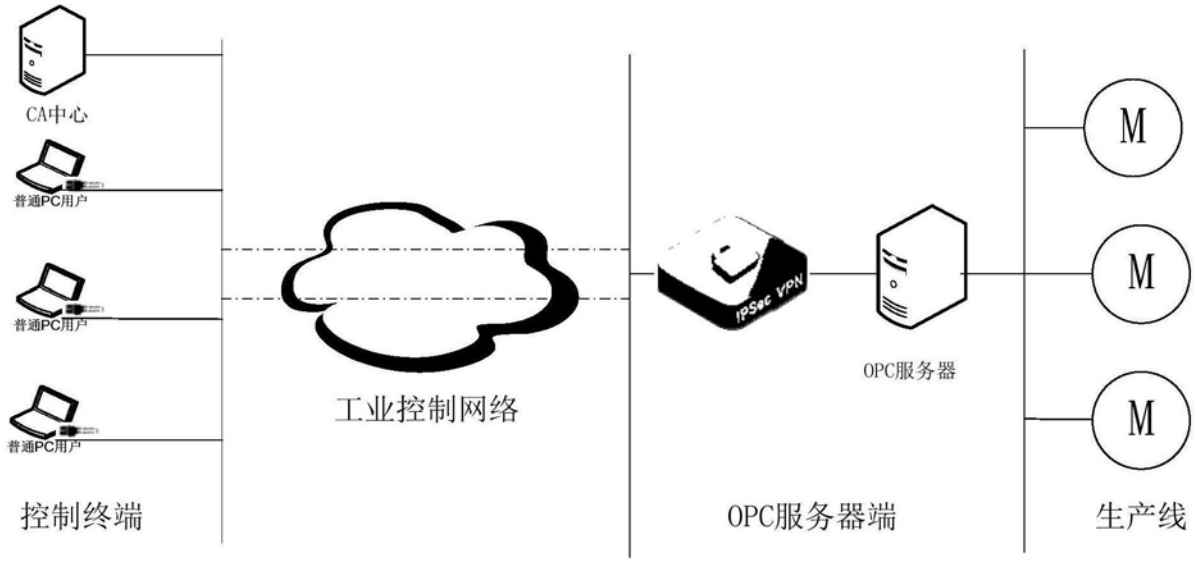
CA中心
普通PC用户
普通PC用户
普通PC用户
工业控制网络
IPSec VPN
OPC服务器
M
M
M
控制终端
OPC服务器端
生产线

图2