



# (12)发明专利申请

(10)申请公布号 CN 106424506 A

(43)申请公布日 2017.02.22

(21)申请号 201510475363.5

(22)申请日 2015.08.05

(71)申请人 江苏金源锻造股份有限公司  
地址 213300 江苏省常州市溧阳市中关村大道8号

(72)发明人 葛艳明 李明 谢苏

(74)专利代理机构 常州市英诺创信专利代理事务所(普通合伙) 32258  
代理人 王美华

(51)Int.Cl.  
B21J 9/20(2006.01)  
B21K 1/04(2006.01)  
B21K 27/00(2006.01)

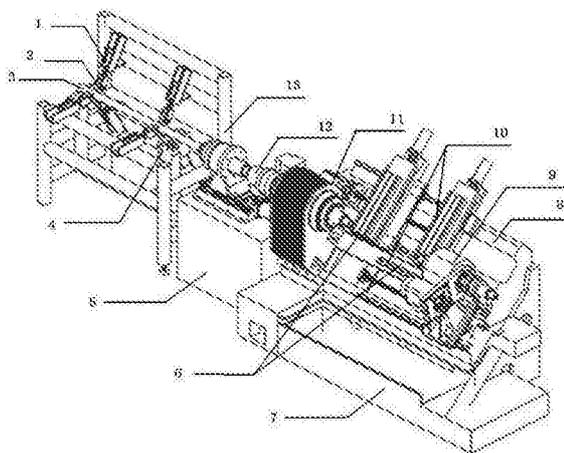
权利要求书2页 说明书5页 附图2页

## (54)发明名称

一种多轴式锻造数控机床

## (57)摘要

本发明公开了一种多轴式锻造数控机床,所述多轴式锻造数控机床具有液压缸,支撑架滚轮,长钢管坯料,固定支撑轮,自动送料底座,刀架部件模块,底座辅助模块,基础支撑模块,副主轴箱部件,进给传动模块,主轴箱部件,自动送料装置,浮动支撑架,当多轴式锻造数控机床加工轴承套圈时,在主轴端的工序完成之后,副主轴与主轴进行动态对接,进而切断坯料,自动送料底座中具有智能控制系统,所述智能控制系统用于控制多轴式锻造数控机床的加工进程,所述智能控制系统还具有权限判定功能,用于为所述多轴式锻造数控机床提供具有权限判定功能的电能供应。



1. 一种多轴式锻造数控机床,所述多轴式锻造数控机床具有液压缸,支撑架滚轮,长钢管坯料,固定支撑轮,自动送料底座,刀架部件模块,底座辅助模块,基础支撑模块,副主轴箱部件,进给传动模块,主轴箱部件,自动送料装置,浮动支撑架,其特征在于:

所述自动送料装置用于实现所述长钢管坯料的自动送料,当多轴式锻造数控机床加工轴承套圈时,在主轴端的工序完成之后,副主轴与主轴进行动态对接,进而切断坯料;

所述自动送料底座中具有智能控制系统,所述智能控制系统用于控制多轴式锻造数控机床的加工进程,所述智能控制系统还具有权限判定功能,用于为所述多轴式锻造数控机床提供具有权限判定功能的电能供应。

2. 根据权利要求 1 所述的一种多轴式锻造数控机床,其特征在于:智能控制系统包括电力供应模块,上级控制模块,权限判定模块,智能电控模块,负载模块;所述负载模块为一种可以消耗电能的机械设备,所述智能电控模块基于来自于权限判定模块的控制信号对可以消耗电能的机械设备的供电回路进行通断控制;当有第三方试图对供电控制进程进行控制时,权限判定模块基于预先设定的权限判定规则,用户认证进程及杀毒进程将第三方阻挡在控制进程之外,以确保供电安全。

3. 根据权利要求 2 所述的一种多轴式锻造数控机床,其特征在于:

所述电力供应模块为市电,UPS 系统,蓄电池组,超级电容器组中的一个或任意个的组合,所述市电,UPS 系统,蓄电池组,超级电容器组中的电能用于提供所需电能消耗;

所述上级控制模块从供电机构和 / 或行政管理部门获取控制信号;

所述权限判定模块基于所述供电机构和 / 或行政管理部门的控制信号进行权限判定;

所述智能电控模块基于权限判定模块产生的权限判定信号实现电能控制;

所述负载模块在智能电控模块的允许下从电力供应模块获取电能;

电力供应模块还具有电源切换模块,所述市电,UPS 系统,蓄电池组,或超级电容器组均连接至电源切换模块的电能输入端口,电源切换模块的电能输出端口电连接至所述智能电控模块的电能输入端口。

4. 根据权利要求 3 所述的一种多轴式锻造数控机床,其特征在于:所述上级控制模块的输入端用于接收所述供电机构和 / 或行政管理部门的控制信号,所述上级控制模块的输出端连接架设为云端服务器的权限判定模块;所述的架设为云端服务器的权限判定模块与所述智能电控模块为两个独立的功能模块;所述的架设为云端服务器的权限判定模块的输出端连接所述智能电控模块的输入端从而将来自于所述上级控制模块的控制信号传送至所述智能电控模块。

5. 根据权利要求 4 所述的一种多轴式锻造数控机床,其特征在于:所述的行政管理部门具有比所述供电机构更高的控制权限,在所述供电机构和 / 或行政管理部门共同进行控制的情况下,所述供电机构所发出的控制信号需要获得行政管理部门的确定,否则被判定为无效命令;或所述的行政管理部门具有比所述供电机构更高的控制权限,在所述供电机构和 / 或行政管理部门共同进行控制的情况下,所述行政管理部门发出的控制信号与所述供电机构所发出的控制信号发生矛盾时,所述的架设为云端服务器的权限判定模块执行所述行政管理部门发出的控制信号。

6. 根据权利要求 5 所述的一种多轴式锻造数控机床,其特征在于:在系统中的功能模块未受到第三方侵入时,所述上级控制模块中的供电机构和 / 或行政管理部门与云端权限

判定模块之间具有通信链路一,用于进行第一通信链路,所述第一通信链路用于交互来自于供电机构和 / 或行政管理部的控制信号以及错误信息反馈信号;所述上级控制模块中的供电机构和 / 或行政管理部与云端权限判定模块之间还具有通信链路二,用于进行与所述第一通信链路不同的第二通信链路,所述第二通信链路用于交互来自于供电机构和 / 或行政管理部的控制信号的真实性的,所述的架设为云端服务器的权限判定模块基于控制信号的真实性的判断是否向所述智能电控模块传递控制信号。

7. 根据权利要求 6 所述的一种多轴式锻造数控机床,其特征在于:所述的与所述第一通信链路不同的第二通信链路执行通信安全等级更高的加密通信协议;所述的与所述第一通信链路不同的第二通信链路基于移动电话通信网络实现第二通信链路。

8. 根据权利要求 7 所述的一种多轴式锻造数控机床,其特征在于:所述架设为云端服务器的权限判定模块在判定供电机构和 / 或行政管理部的控制信号受到第三方挟持的情况下,通过所述第一通信链路以及所述第二通信链路发出所述第一通信链路受到挟持的信号,然后断开所述第一通信链路的通信以及所述第二通信链路的通信,自动切换到基于预设的应急控制程序自主的对智能电控模块进行控制的模式。

9. 根据权利要求 8 所述的一种多轴式锻造数控机床,其特征在于:所述架设为云端服务器的权限判定模块还具有用户认证模块以及杀毒引擎模块用于实现用户认证进程及杀毒进程;所述杀毒引擎模块具有多杀毒引擎,所述多杀毒引擎包括第一引擎和第二引擎,当所述供电机构和 / 或行政管理部发来控制信号时,调用第一杀毒引擎对所述控制信号进行扫描杀毒得到第一结果,根据该第一结果滤除掉一批由第一杀毒引擎扫描得到的病毒文件,之后,调用第二杀毒引擎对基于第一结果的安全文件进行查杀,输出第二结果,在第二杀毒结果显示安全的情况下,再基于用户认证模块对用户进行安全认证,基于用户认证模块的用户认证结果,即在用户验证信息和属性信息与预设的安全信息一致时允许所述供电机构和 / 或行政管理部对判断为安全的文件进行传输,否则当文件不安全或用户认证未通过时拒绝所述供电机构和 / 或行政管理部对文件的传输操作,所述第一杀毒引擎采用虚拟机平台,选择 Vmare 软件搭建虚拟平台和创建虚拟系统,并使用 PEID、OLLYDBG 及 PEInfo 查壳工具对文件病毒进行分析;所述用户认证模块对用户的验证信息和用户的属性进行验证,所述用户的验证信息包括用户的用户名和密码,所述用户的属性信息包括用户的 IP 地址、MAC 地址、操作历史记录及其主机名。

## 一种多轴式锻造数控机床

### 技术领域

[0001] 本发明涉及一种机床,特别是涉及一种多轴式锻造数控机床。

### 背景技术

[0002] 滚动轴承作为典型的标准机械零部件应用范围广、产量大,非常适宜采用高教的自动化生产方式,小型通用类的圆锥滚子轴承、深沟球轴承及部分角接触球轴承的套圈对坯料的内部金属组织要求不高,轴承套圈可采用长管料直接车削成型的加工方式。传统的轴承套圈车削自动化生产线都是基于单轴数控机床的呈流水线式排布,采用工序分散原则进行加工,加工过程需要多次装夹,导致加工精度难以保证、生产成本低、加工效率低等问题。

[0003] 多轴数控机床实现了长管料自动送料、单台设备集中工序加工,能有效地节省设备成本、缩短辅助时间及提高加工效率。多轴式锻造数控机床加工轴承套圈时,当主轴端的工序完成之后,副主轴与主轴进行动态对接,进而切断坯料。

### 发明内容

[0004] 本发明的目的在于克服现有技术不足,提供一种具有能量权限判定功能的多轴式锻造数控机床,实现了长管料自动送料、单台设备集中工序加工,能有效地节省设备成本、缩短辅助时间及提高加工效率它还能够有效地避免第三方对多轴式锻造数控机床运行的影响,同时实现上级管理机构对多轴式锻造数控机床的控制。

[0005] 为了达到上目的,本发明的技术方案是这样的:提供了一种多轴式锻造数控机床,所述多轴式锻造数控机床具有液压缸,支撑架滚轮,长钢管坯料,固定支撑轮,自动送料底座,刀架部件模块,底座辅助模块,基础支撑模块,副主轴箱部件,进给传动模块,主轴箱部件,自动送料装置,浮动支撑架。

[0006] 所述自动送料装置用于实现所述长钢管坯料的自动送料,当多轴式锻造数控机床加工轴承套圈时,在主轴端的工序完成之后,副主轴与主轴进行动态对接,进而切断坯料。

[0007] 所述自动送料底座中具有智能控制系统,所述智能控制系统用于控制多轴式锻造数控机床的加工进程,所述智能控制系统还具有权限判定功能,用于为所述多轴式锻造数控机床提供具有权限判定功能的电能供应。

[0008] 智能控制系统包括电力供应模块,上级控制模块,权限判定模块,智能电控模块,负载模块;所述负载模块为一种可以消耗电能的机械设备,所述智能电控模块基于来自于权限判定模块的控制信号对可以消耗电能的机械设备的供电回路进行通断控制;当有第三方试图对供电控制进程进行控制时,权限判定模块基于预先设定的权限判定规则,用户认证进程及杀毒进程将第三方阻挡在控制进程之外,以确保供电安全。

[0009] 所述电力供应模块为市电,UPS 系统,蓄电池组,超级电容器组中的一个或任意个的组合,所述市电,UPS 系统,蓄电池组,超级电容器组中的电能用于提供所需电能消耗。

[0010] 所述上级控制模块从供电机构和 / 或行政管理部门获取控制信号。

[0011] 所述权限判定模块基于所述供电机构和 / 或行政管理部門的控制信号进行权限判定。

[0012] 所述智能电控模块基于权限判定模块产生的权限判定信号实现电能控制。

[0013] 所述负载模块在智能电控模块的允许下从电力供应模块获取电能。

[0014] 电力供应模块还具有电源切换模块,所述市电,UPS 系统,蓄电池组,或超级电容器组均连接至电源切换模块的电能输入端口,电源切换模块的电能输出端口电连接至所述智能电控模块的电能输入端口。

[0015] 所述上级控制模块的输入端用于接收所述供电机构和 / 或行政管理部門的控制信号,所述上级控制模块的输出端连接架设为云端服务器的权限判定模块;所述的架设为云端服务器的权限判定模块与所述智能电控模块为两个独立的功能模块;所述的架设为云端服务器的权限判定模块的输出端连接所述智能电控模块的输入端从而将来自于所述上级控制模块的控制信号传送至所述智能电控模块。

[0016] 所述的行政管理部門具有比所述供电机构更高的控制权限,在所述供电机构和 / 或行政管理部門共同进行控制的情况下,所述供电机构所发出的控制信号需要获得行政管理部門的确定,否则被判定为无效命令;或所述的行政管理部門具有比所述供电机构更高的控制权限,在所述供电机构和 / 或行政管理部門共同进行控制的情况下,所述行政管理部門发出的控制信号与所述供电机构所发出的控制信号发生矛盾时,所述的架设为云端服务器的权限判定模块执行所述行政管理部門发出的控制信号。

[0017] 在系统中的功能模块未受到第三方侵入时,所述上级控制模块中的供电机构和 / 或行政管理部門与云端权限判定模块之间具有通信链路一,用于进行第一通信链路,所述第一通信链路用于交互来自于供电机构和 / 或行政管理部門的控制信号以及错误信息反馈信号;所述上级控制模块中的供电机构和 / 或行政管理部門与云端权限判定模块之间还具有通信链路二,用于进行与所述第一通信链路不同的第二通信链路,所述第二通信链路用于交互来自于供电机构和 / 或行政管理部門的控制信号的真实性的判断,所述的架设为云端服务器的权限判定模块基于控制信号的真实性的判断是否向所述智能电控模块传递控制信号。

[0018] 所述的与所述第一通信链路不同的第二通信链路执行通信安全等级更高的加密通信协议;所述的与所述第一通信链路不同的第二通信链路基于移动电话通信网络实现第二通信链路。

[0019] 所述架设为云端服务器的权限判定模块在判定供电机构和 / 或行政管理部門的控制信号受到第三方挟持的情况下,通过所述第一通信链路以及所述第二通信链路发出所述第一通信链路受到挟持的信号,然后断开所述第一通信链路的通信以及所述第二通信链路的通信,自动切换到基于预设的应急控制程序自主的对智能电控模块进行控制的模式。

[0020] 所述架设为云端服务器的权限判定模块还具有用户认证模块以及杀毒引擎模块用于实现用户认证进程及杀毒进程;所述杀毒引擎模块具有多杀毒引擎,所述多杀毒引擎包括第一引擎和第二引擎,当所述供电机构和 / 或行政管理部門发来控制信号时,调用第一杀毒引擎对所述控制信号进行扫描杀毒得到第一结果,根据该第一结果滤除掉一批由第一杀毒引擎扫描得到的病毒文件,之后,调用第二杀毒引擎对基于第一结果的安全文件进行查杀,输出第二结果,在第二杀毒结果显示安全的情况下,再基于用户认证模块对用户进

行安全认证,基于用户认证模块的用户认证结果,即在用户验证信息和属性信息与预设的安全信息一致时允许所述供电机构和 / 或行政管理部门对判断为安全的文件进行传输,否则当文件不安全或用户认证未通过时拒绝所述供电机构和 / 或行政管理部门对文件的传输操作,所述第一杀毒引擎采用虚拟机平台,选择 Vmare 软件搭建虚拟平台和创建虚拟系统,并使用 PEID、OLLYDBG 及 PEInfo 查壳工具对文件病毒进行分析;所述用户认证模块对用户的验证信息和用户的属性进行验证,所述用户的验证信息包括用户的用户名和密码,所述用户的属性信息包括用户的 IP 地址、MAC 地址、操作历史记录及其主机名。

[0021] 本发明的有益效果是:实现了长管料自动送料、单台设备集中工序加工,能有效地节省设备成本、缩短辅助时间及提高加工效率它还能够有效地避免第三方对多轴式锻造数控机床运行的影响,同时实现上级管理机构对多轴式锻造数控机床的控制。

### 附图说明

[0022] 图 1 为本发明的多轴式锻造数控机床结构示意图;

[0023] 图 2 为本发明的智能控制系统结构示意图。

[0024] 图中标记为:1- 液压缸,2- 支撑架滚轮,3- 长钢管坯料,4- 固定支撑轮,5- 自动送料底座,6- 刀架部件模块,7- 底座辅助模块,8- 基础支撑模块,9- 副主轴箱部件,10- 进给传动模块,11- 主轴箱部件,12- 自动送料装置,11- 浮动支撑架。

### 具体实施方式

[0025] 下面结合附图和具体实施例对本发明作进一步说明:

[0026] 如图 1 所示,图 1 示出了一种多轴式锻造数控机床,所述多轴式锻造数控机床具有液压缸,支撑架滚轮,长钢管坯料,固定支撑轮,自动送料底座,刀架部件模块,底座辅助模块,基础支撑模块,副主轴箱部件,进给传动模块,主轴箱部件,自动送料装置,浮动支撑架。

[0027] 所述自动送料装置用于实现所述长钢管坯料的自动送料,当多轴式锻造数控机床加工轴承套圈时,在主轴端的工序完成之后,副主轴与主轴进行动态对接,进而切断坯料。

[0028] 所述自动送料底座中具有智能控制系统,所述智能控制系统用于控制多轴式锻造数控机床的加工进程,所述智能控制系统还具有权限判定功能,用于为所述多轴式锻造数控机床提供具有权限判定功能的电能供应。

[0029] 如图 2 所示,图 2 示出了智能控制系统,其包括电力供应模块,上级控制模块,权限判定模块,智能电控模块,负载模块;所述负载模块为一种可以消耗电能的机械设备,所述智能电控模块基于来自于权限判定模块的控制信号对可以消耗电能的机械设备的供电回路进行通断控制;当有第三方试图对供电控制进程进行控制时,权限判定模块基于预先设定的权限判定规则,用户认证进程及杀毒进程将第三方阻挡在控制进程之外,以确保供电安全。

[0030] 所述电力供应模块为市电,UPS 系统,蓄电池组,超级电容器组中的一个或任意个的组合,所述市电,UPS 系统,蓄电池组,超级电容器组中的电能用于提供所需电能消耗。

[0031] 所述上级控制模块从供电机构和 / 或行政管理部门获取控制信号。

[0032] 所述权限判定模块基于所述供电机构和 / 或行政管理部门的控制信号进行权限判定。

[0033] 所述智能电控模块基于权限判定模块产生的权限判定信号实现电能控制。

[0034] 所述负载模块在智能电控模块的允许下从电力供应模块获取电能。

[0035] 电力供应模块还具有电源切换模块,所述市电,UPS 系统,蓄电池组,或超级电容器组均连接至电源切换模块的电能输入端口,电源切换模块的电能输出端口电连接至所述智能电控模块的电能输入端口。

[0036] 所述上级控制模块的输入端用于接收所述供电机构和 / 或行政管理部的控制信号,所述上级控制模块的输出端连接架设为云端服务器的权限判定模块;所述的架设为云端服务器的权限判定模块与所述智能电控模块为两个独立的功能模块;所述的架设为云端服务器的权限判定模块的输出端连接所述智能电控模块的输入端从而将来自于所述上级控制模块的控制信号传送至所述智能电控模块。

[0037] 所述的行政管理部门具有比所述供电机构更高的控制权限,在所述供电机构和 / 或行政管理部门共同进行控制的情况下,所述供电机构所发出的控制信号需要获得行政管理部门的确定,否则被判定为无效命令;或所述的行政管理部门具有比所述供电机构更高的控制权限,在所述供电机构和 / 或行政管理部门共同进行控制的情况下,所述行政管理部门发出的控制信号与所述供电机构所发出的控制信号发生矛盾时,所述的架设为云端服务器的权限判定模块执行所述行政管理部门发出的控制信号。

[0038] 在系统中的功能模块未受到第三方侵入时,所述上级控制模块中的供电机构和 / 或行政管理部门与云端权限判定模块之间具有通信链路一,用于进行第一通信链路,所述第一通信链路用于交互来自于供电机构和 / 或行政管理部门的控制信号以及错误信息反馈信号;所述上级控制模块中的供电机构和 / 或行政管理部门与云端权限判定模块之间还具有通信链路二,用于进行与所述第一通信链路不同的第二通信链路,所述第二通信链路用于交互来自于供电机构和 / 或行政管理部门的控制信号的真实性,所述的架设为云端服务器的权限判定模块基于控制信号的真实性判断是否向所述智能电控模块传递控制信号。

[0039] 所述的与所述第一通信链路不同的第二通信链路执行通信安全等级更高的加密通信协议;所述的与所述第一通信链路不同的第二通信链路基于移动电话通信网络实现第二通信链路。

[0040] 所述架设为云端服务器的权限判定模块在判定供电机构和 / 或行政管理部门的控制信号受到第三方挟持的情况下,通过所述第一通信链路以及所述第二通信链路发出所述第一通信链路受到挟持的信号,然后断开所述第一通信链路的通信以及所述第二通信链路的通信,自动切换到基于预设的应急控制程序自主的对智能电控模块进行控制的模式。

[0041] 所述架设为云端服务器的权限判定模块还具有用户认证模块以及杀毒引擎模块用于实现用户认证进程及杀毒进程;所述杀毒引擎模块具有多杀毒引擎,所述多杀毒引擎包括第一引擎和第二引擎,当所述供电机构和 / 或行政管理部门发来控制信号时,调用第一杀毒引擎对所述控制信号进行扫描杀毒得到第一结果,根据该第一结果滤除掉一批由第一杀毒引擎扫描得到的病毒文件,之后,调用第二杀毒引擎对基于第一结果的安全文件进行查杀,输出第二结果,在第二杀毒结果显示安全的情况下,再基于用户认证模块对用户进行安全认证,基于用户认证模块的用户认证结果,即在用户验证信息和属性信息与预设的安全信息一致时允许所述供电机构和 / 或行政管理部门对判断为安全的文件进行传输,否

则当文件不安全或用户认证未通过时拒绝所述供电机构和 / 或行政管理部门对文件的传输操作,所述第一杀毒引擎采用虚拟机平台,选择 Vmare 软件搭建虚拟平台和创建虚拟系统,并使用 PEID、OLLYDBG 及 PEInfo 查壳工具对文件病毒进行分析;所述用户认证模块对用户的验证信息和用户的属性进行验证,所述用户的验证信息包括用户的用户名和密码,所述用户的属性信息包括用户的 IP 地址、MAC 地址、操作历史记录及其主机名。

[0042] 以上内容仅为本发明的较佳实施方式,对于本领域的普通技术人员,依据本发明的思想,在具体实施方式及应用范围上均会有改变之处,本说明书内容不应理解为对本发明的限制。

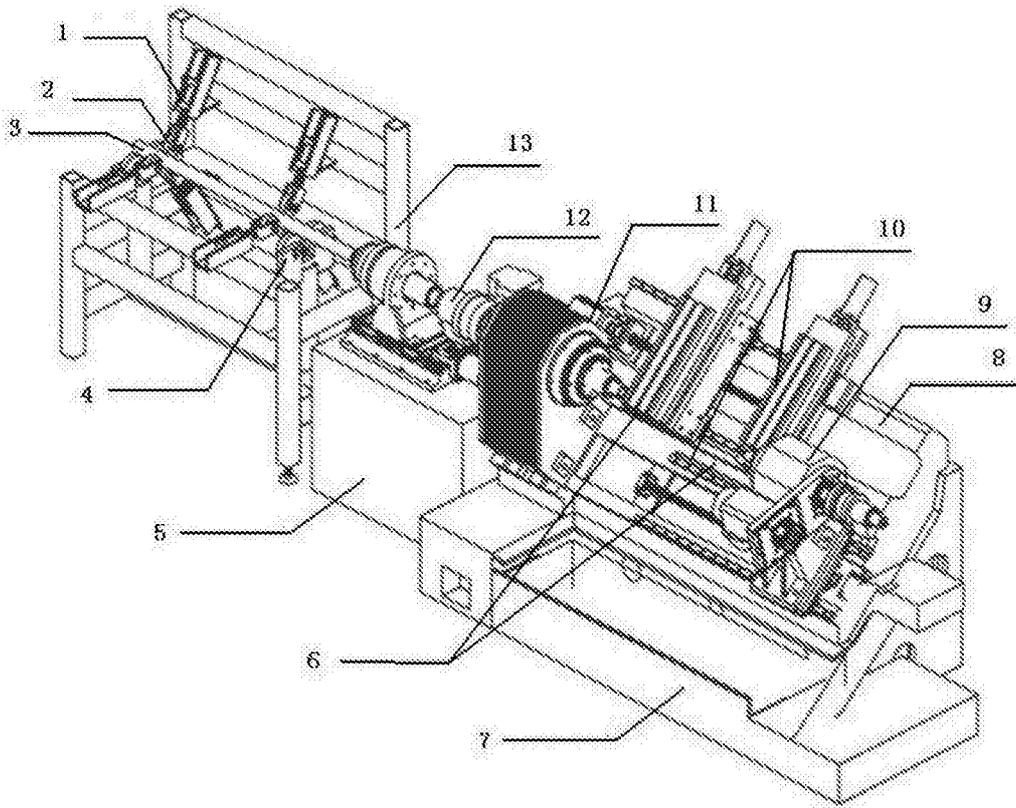


图 1

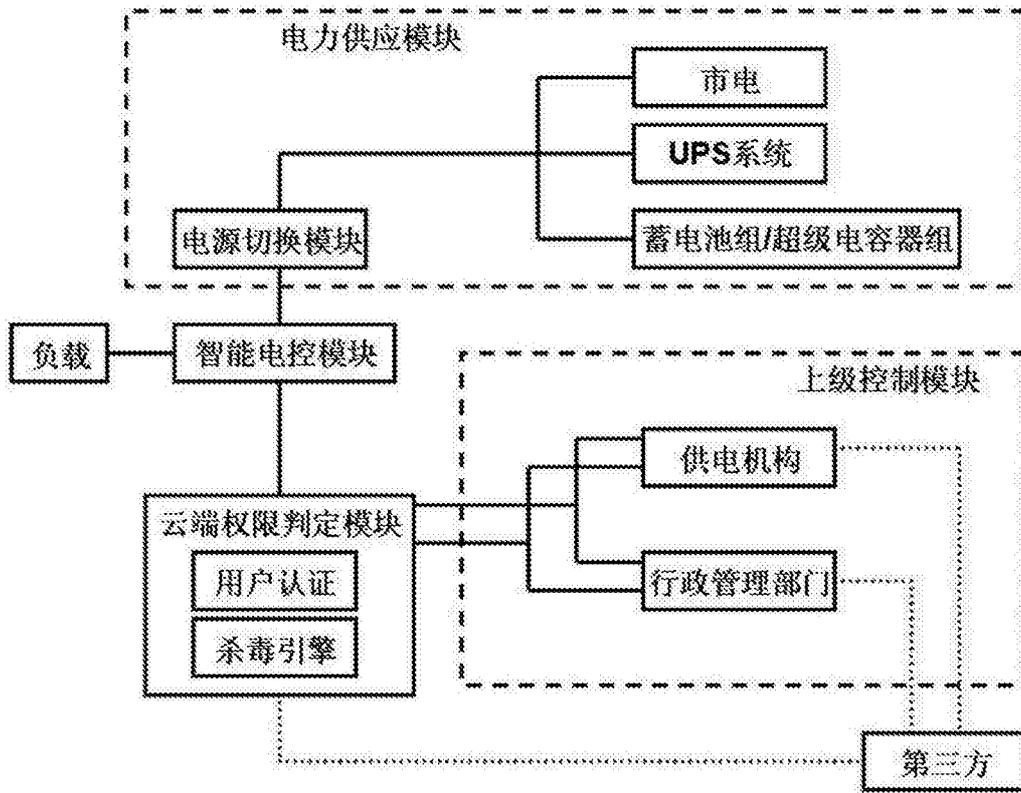


图 2