(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2022 年 5 月 19 日 (19.05.2022)

WIPO | PCT

(10) 国际公布号
WO 2022/100232 A1

(51) 国际专利分类号:
G06F 15/16 (2006.01)

(21) 国际申请号: PCT/CN2021/116147

(22) 国际申请日: 2021 年 9 月 2 日 (02.09.2021)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202011267117.8 2020年11月13日 (13.11.2020) CN

(71) 申请人: 中车株洲电力机车有限公司 (CRRC ZHUZHOU LOCOMOTIVE CO., LTD.) [CN/CN]; 中国湖南省株洲市石峰区田心高科园, Hunan 412001 (CN)。

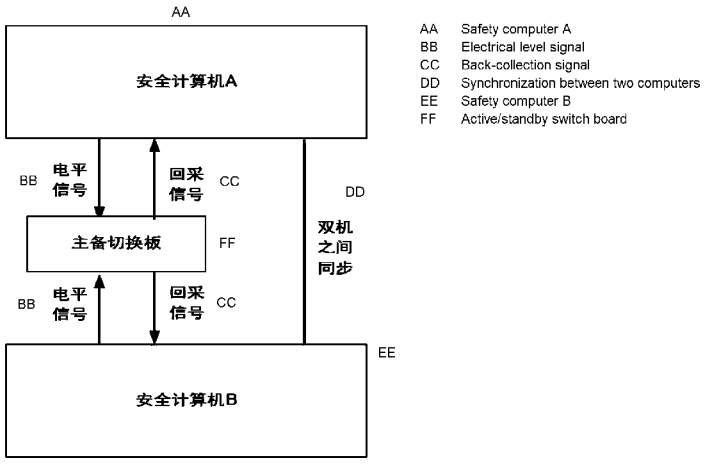
(72) 发明人: 罗显光 (LUO, Xianguang); 中国湖南省株洲市石峰区田心高科园, Hunan 412001 (CN)。 孙俊勇 (SUN, Junyong); 中国湖南省株洲市石峰区田心高科园, Hunan 412001 (CN)。 许晋荣 (XU, Jinrong); 中国湖南省株洲市石峰区田心高科园, Hunan 412001 (CN)。 曾军 (ZENG, Jun); 中国湖南省株洲市石峰区田心高科园, Hunan 412001 (CN)。 陈建林 (CHEN, Jianlin); 中国湖南省株洲市石峰区田心高科园, Hunan 412001 (CN)。 刘宏达 (LIU, Hongda); 中国湖南省株洲市石峰区田心高科园, Hunan 412001 (CN)。 杜求茂 (DU, Qiumao); 中国湖南省株洲市石峰区田心高科园, Hunan 412001 (CN)。

(74) 代理人: 长沙正奇专利事务所有限责任公司 (CHANGSHA ZONEKEY PATENT LAW FIRM); 中国湖南省长沙市岳麓区枫林二路188号向日葵广场7楼, Hunan 410205 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU,

(54) **Title:** DISTRIBUTED-TYPE ON-BOARD SAFETY COMPUTER SYSTEM

(54) 发明名称: 一种分布式车载安全计算机系统



(57) **Abstract:** Disclosed is a distributed-type on-board safety computer system, comprising two safety computers completely equivalent in structure and function and having a two-vote-two structure; a connection is established between the two safety computers by means of an active/standby switch board, and data synchronization between the two safety computers is implemented by means of a communication bus; the active/standby switch board is used for controlling one among the two safety computers to work in an active state and the other to work in a standby state according to configured logic and work data of the two safety computers, or controlling both of the two safety computers to work in a standby state; working in an active state refers to a safety computer being used for receiving and transmitting of data with the outside, and working in a standby state refers to a safety computer only being used for receiving data from the outside but not used for transmitting data to the outside. The present invention has advantages of miniaturization, high performance, high safety, and flexible installation and configuration.

WO 2022/100232 A1

[见续页]

CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布：

— 包括国际检索报告(条约第21条(3))。

(57) 摘要：本发明公开了一种分布式车载安全计算机系统，包括结构和功能完全相同的二取二结构的两套安全计算机，两套安全计算机之间通过主备切换板相连，且两套安全计算机之间通过通信总线实现数据同步；主备切换板用于根据两套安全计算机的工作数据和设定的逻辑，控制两套安全计算机中的一套工作在主系状态而另一套工作在备系状态，或者控制两套安全计算机中的两套均工作在备系状态；工作在主系状态是指安全计算机用于对外接收和输出数据，工作在备系状态是指安全计算机仅用于对外接收数据而不用于对外输出数据。本发明具备小型化、高性能、高安全、安装配置灵活的优点。

一种分布式车载安全计算机系统

技术领域

本发明特别涉及一种分布式车载安全计算机系统。

背景技术

随着无线通信、计算机等技术的快速发展，轨道交通车辆的智能化、自主化水平也越来越高，对传统安全计算机的功能和性能提出了更高的要求。

在传统信号领域，主要由地面设备进行计算，车载安全计算机作为执行单元实现自动运行控制。例如在运行过程中，车辆的车载安全计算机将自身状态位置等信息发送给地面设备，地面设备不仅接收该车辆自身状态位置信息，还接收该地面设备管理的所有车辆的信息，根据这些信息计算后反馈信息（例如限速）给该车辆的车载安全计算机，车载安全计算机再根据反馈信息（例如限速）控制车辆运行，每个控制周期都存在车辆到地面设备以及地面设备到车辆的信息交互，由于信息交互路径长，导致信息交互时间长，影响交互效率，例如交互效率低可能导致车辆不能及时根据限速信息调整其运行。同时，单台地面设备管理多台车载安全计算机，例如单台地面设备最多管理 10 台车载安全计算机，当多辆轨道交通车辆同时处于运行状态时，单台地面设备在进行计算时需要根据该地面设备所管理的且在运行的所有轨道交通车辆发送的信息进行，例如地面设备所管理的轨道交通车辆中有 8 辆处于运行状态，则在每个控制周期地面设备均需要根据 8 辆轨道交通车辆发送的信息来计算，计算量大，影响计算效率，从而影响反馈信息的反馈时间，进一步影响交互效率。

此外，传统的车载安全计算机一般采用 6U 及以上的单机箱设计，机械尺寸较大，不便于车载安全计算机的灵活配置和功能扩展，特别是有轨电车，其空间非常小，对车载安全计算机的配置和扩展影响更甚。

因此，需要一种小型化、高性能、高安全、安装配置灵活的车载安全计算机系统，以满足车辆日益增加的智能化需求。

发明内容

本发明的目的在于，针对上述现有技术中因地面设备与车载安全计算机信息交互路径长导致信息交互效率低的问题，以及车载安全计算机系统体积大影响其配置和功能扩展的问题，提供一种分布式车载安全计算机系统，具备小型化、高性能、高安全、安装配置灵活的优点。

为解决上述技术问题，本发明所采用的技术方案是：

一种分布式车载安全计算机系统，其特点是包括结构和功能完全相同的二取二结构的两套安全计算机，两套安全计算机之间通过主备切换板相连，且两套安全计算机之间通过通信总线实现数据同步；

其中，主备切换板用于根据两套安全计算机的工作数据和设定的逻辑，控制两套安全计算机中的一套工作在主系状态而另一套工作在备系状态，或者控制两套安全计算机中的两套均工作在备系状态；其中，工作在主系状态是指安全计算机用于对外接收和输出数据，工作在备系状态是指安全计算机仅用于对外接收数据而不用于对外输出数据。

本发明中，在每个控制周期，车辆的车载安全计算机系统只需要接收该车辆前、后相邻车辆的数据，并根据前后相邻车辆的数据和自身数据进行计算，再根据计算结果直接控制该车辆的运行，在每个运行控制周期系统与地面设备均无信息交互，系统仅与其前后相邻车辆进行信息交互，大大缩短了信息交互路径，提高了信息交互效率，使车辆能及时调整其运行状态，避免了安全事故的发生；同时，相较于地面设备需要同时计算多辆车辆发送的信息，本发明系统仅需要计算前后相邻车辆的数据，大大降低了数据量，从而降低了计算量，提高了计算效率，进一步提高了交互效率，使车辆更加及时调整其运行状态。

作为一种优选方式，对于两套安全计算机中的一套工作在主系状态而另一套工作在备系状态，两套安全计算机之间的数据同步规则包括：

两套安全计算机之间互相发送心跳帧，若处于备系状态的安全计算机根据心跳帧判断自身的数据状态不同于处于主系状态的安全计算机的数据状态，则处于备系状态的安全计算机发送同步请求帧至处于主系状态的安全计算机，处于主系状态的安全计算机接收到同步请求帧后即发送同步数据至处于备系状态的安全计算机。

作为一种优选方式，每一套安全计算机均包括两块主控板、一块表决板、至少一块 IO 板和若干通信板；

针对单套安全计算机，两主控板相连以用于实现单机内的数据同步，所述主控板、IO 板、通信板均与所述表决板相连，所述表决板与主备切换板相连；两套安全计算机的表决板之间通过通信总线相连。

作为一种优选方式，对于工作在主系状态的安全计算机，两主控板在进行同步数据比较之后并判断两主控板的同步数据一致的情况下，两主控板的同步数据通过表决板输出至工作在备系状态的安全计算机。

作为一种优选方式，对于工作在备系状态的安全计算机，判断两主控板接收到的数据一致的情况下，两主控板才进行数据同步。

作为一种优选方式，主备切换板控制安全计算机工作在主系状态或备系状态的逻辑包括：主备切换板在接收到两套安全计算机在上电后发送的电平信号后，根据获得的两套安全计算机发送的电平信号的先后顺序，锁定先发送电平信号的安全计算机的工作状态为主系状态，锁定后发送电平信号的安全计算机的工作状态为备系状态；两套安全计算机通过从主备切换板回采的信号确定自身的工作状态。

作为一种优选方式，主备切换板控制安全计算机工作在主系状态或备系状态的逻辑包括：当处于主系状态的安全计算机出现故障并停止向主备切换板发送电平信号时，主备切换板将原本处于主系状态的安全计算机的工作状态锁定为备系状态，并将原本处于备系状态的安全计算机的工作状态锁定为主系状态；两套安全计算机通过从主备切换板回采的信号确定自身的工作状态。

作为一种优选方式，所述安全计算机：用于在接收到主备切换板发送的高电平信号时，工作在主系状态；用于在接收到主备切换板发送的低电平信号时，工作在备系状态；

主备切换板控制安全计算机工作在主系状态或备系状态的逻辑还包括：

若原本处于备系状态的安全计算机回采到主备切换板发送的高电平信号，且两套安全计算机之间的数据同步，则原本处于备系状态的安全计算机切换至主系状态，原本处于主系状态的安全计算机切换至备系状态；若原本处于备系状态的安全计算机回采到主备切换板发送的高电平信号，但两套安全计算机之间的数据不同步，则两套安全计算机均进入备系状态；若两套安全计算机均出现故障，则两套安全计算机均进入备系状态。

作为一种优选方式，主备切换板控制安全计算机工作在主系状态或备系状态的逻辑还包括：

针对单套安全计算机，若两个主控板在连续 N 个周期内的同步时长均超过

设定的运算周期，则在本套安全计算机处于主系状态时降级为备系状态；在本套安全计算机处于备系状态时重启系统；

针对单套安全计算机，若一主控板在连续 N 个周期内均未收到另一主控板的有效数据，则在本套安全计算机处于主系状态时降级为备系状态；在本套安全计算机处于备系状态时重启系统。

作为一种优选方式，针对单套安全计算机，还设有硬件看门狗，在喂狗失败时，则在本套安全计算机处于主系状态时降级为备系状态，并释放动态电路且将另一套安全计算机升级为主系状态；在本套安全计算机处于备系状态时重启系统。

与现有技术相比，本发明具有以下有益效果：

1、本发明车载安全计算机系统只需要接收相邻车辆的数据，无车辆与地面设备之间的信息交互，信息交互路径短，信息交互效率高；同时根据接收的数据进行计算时数据量少，计算速度快，进一步提高了交互效率，使车辆能及时调整运行状态，避免了安全事故发生。

2、本发明车载安全计算机系统由两套分布的二取二安全计算机组成，两套安全计算机可以采用集中式机柜安装的方式，也可以采用分布式的安装方式，可以根据不同的车辆情况灵活安装，具备小型化、安装配置灵活的优点。

3、本发明两套安全计算机之间通过独立的主备切换板进行主备切换，保证在任意时刻只有一套安全计算机处于主系状态，并能根据两套安全计算机的工作数据切换主系状态和备系状态，性能和安全性高。

附图说明

图 1 为本发明的组合架构图。

图 2 为本发明的结构框图。

图 3 为单套二取二结构的安全计算机的架构图。

图 4 为两套安全计算机的主备选择流程图。

图 5 为两套安全计算机的主备切换流程图。

图 6 为单套安全计算机的数据流图。

具体实施方式

如图 1 至图 3 所示，本发明的分布式车载安全计算机系统包括结构和功能完全相同的二取二结构的两套安全计算机 A 和 B，两套安全计算机之间通过主备

切换板相连，且两套安全计算机之间通过通信总线实现数据同步。

主备切换板用于根据两套安全计算机的工作数据和设定的逻辑，控制两套安全计算机中的一套工作在主系状态而另一套工作在备系状态，或者控制两套安全计算机中的两套均工作在备系状态；其中，工作在主系状态是指安全计算机用于对外接收和输出数据，工作在备系状态是指安全计算机仅用于对外接收数据而不用于对外输出数据。本实施例中，对外是指分布式车载安全计算机系统以外。

如图 2 所示，每一套安全计算机均包括两块主控板、两块 110V 或 24V 的电源板、一块表决板、至少一块 IO 板和若干通信板；电源板根据具体的安装载体选择不同的电压等级，比如地铁列车选择 110VDC，有轨电车选择 24VDC，无轨电车选择 24VDC，实际安装需要两路独立供电；通信板包括 MVB 通信板、CAN+485 通信板、以太网通信板，可以根据具体情况选择 MVB 通信板、CAN+485 通信板、以太网通信板，同时根据实际的数字量输入输出需求配置合适数量的 IO 模块，具有很强的灵活性。

如图 3 所示，针对单套安全计算机，两主控板相连以用于实现单机内的数据同步，主控板、IO 板、通信板均与表决板相连，表决板与主备切换板相连；两套安全计算机的表决板之间通过通信总线相连，即表决板与主备切换板之间采用硬线连接、两套安全计算机的表决板采用通信总线的连接方式。

两套安全计算机 A 和 B 均采用独立的 3U 标准机箱。主备切换板为单独 1U 设备，或者可以采用插入式板卡形式将主备切换板集成到安全计算机 A 或安全计算机 B 中。U 表示标准机箱外部尺寸单位 unit 的缩写，1U 就是 4.445cm，3U 是 4.445×3cm。相较于传统的 6U 及以上机箱设计，大大降低了机箱尺寸，便于系统的灵活配置和功能扩展。

安全计算机 A、安全计算机 B、主备切换板作为车载设备进行设计，可以根据项目采用一体式上下层机柜、左右并列安装的方式，也可以根据需要安装在不同车辆或不同机柜中，方便灵活，尤其适合有轨、无轨列车等安装空间较为紧张的车辆。

本发明的分布式车载安全计算机系统不仅适用于城市轨道交通车辆，例如地铁、有轨电车、无轨电车等车辆的 SIL4 级高安全设备要求，同时也适用车辆上其他具有安全功能需求的系统。

具体地，本发明包括以下几个部分：

（1）分布式车载安全计算机系统的架构设计

本发明的分布式车载安全计算机系统由两套分布的二取二安全计算机组成，每套独立的安全计算机称为一系，由两块主控板组成二取二结构，并包含两个冗余的电源板、一个表决板、若干 IO 板（根据 IO 点位需求配置板卡数量）和通信板（包括 MVB 通信板、CAN+485 通信板、以太网通信板）组成。两套分布的安全计算机之间有系间同步通道和主备切换板相互联系。

本发明的分布式车载安全计算机系统结构如图 1~图 3 所示，其具有如下特点：

a. 安全计算机 A 和安全计算机 B 分别为独立 3U 小型化机箱，两个设备可以分布放置或者集中式放置，安装灵活，特别适合有轨电车等空间位置紧张的情况。

b. 主备切换板可以作为独立设备，主要实现安全计算机 A 和安全计算机 B 的主从切换，保证在任意时刻两套安全计算机只有一个是主设备，保证了车辆运行控制的安全性。

c. 安全计算机 A 和安全计算机 B 之间通过通信总线实现双机之间的数据同步，保证了车辆运行控制的安全性。

d. 分布式的安全计算机系统配置灵活，应用场景多，两套安全计算机组合构成二乘二取二架构，满足高安全等级的要求（例如 SIL4 级）；单独的一套二取二安全计算机可以作为通用的控制平台满足车辆较低安全等级的需求（例如 SIL2 级）。

e. 根据计算需求对主控板上的控制芯片进行选型，如果单套安全计算机主要用于计算，则选用高性能、运算能力强的控制芯片；如果单套安全计算机用于控制，则选用低功耗、低成本的控制芯片，根据单套安全计算机所要实现的功能进行主控板上控制芯片选型，既能保证功能实现，又能降低功耗和成本。

（2）两套安全计算机的同步切换

两套安全计算机之间通过通信总线进行数据同步，并且根据同步的状态进行主系状态和备系状态的切换：

a.两套安全计算机之间的数据同步规则

① 当安全计算机 A 和安全计算机 B 中一套安全计算机处于主系状态、另一套安全计算机处于备系状态时，安全计算机 A 和安全计算机 B 之间周期性互相发送心跳帧，例如校验数据。

② 当备系根据心跳帧发现自身的数据状态与主系的数据状态不一致时，则备系发送同步请求帧，然后主系接收到同步请求帧后发送同步的数据状态到备系，实现备系与主系之间的数据状态同步。

主系向备系同步的数据状态，首先经过主系的两个主控板进行数据状态比较，当两主控板的数据状态一致的情况下，才向备系输出数据状态。

备系对来自主系的数据状态，只有在备系的两个主控板接收到的数据状态一致的情况下，才进行数据状态的同步，保证备系的状态始终与主系数据状态一致，实现主备无间断切换。

当安全计算机 A 和安全计算机 B 均处于备系状态时，由于两者均是降级状态，均不对外输出数据，无需进行数据状态的同步。

b.两套安全计算机的主备切换逻辑

安全计算机 A 和安全计算机 B 采用冗余设备运行，安全计算机 A 和安全计算机 B 分别通过硬线连接主备切换板，并由主备切换板的互锁电路保证同一时刻只有一个安全计算机处于主系状态，包括主备工作设备选择（见图 4）和主备切换（见图 5）：

① 安全计算机 A 和 B 上电后都向主备切换板持续发送电平信号。

② 主备切换板根据获得的安全计算机 A、B 发送电平信号的先后顺序判断主从，先发送电平信号的安全计算机的工作状态为主系状态，后发送电平信号的安全计算机的工作状态为备系状态；并将切换状态锁定。

③ 安全计算机 A 和 B 的表决板分别通过硬线回采主备切换板的电信号，获得自身的主从状态，回采到高电平信号则为主系，回采到低电平信号则为备系。

④ 当主系检测到故障，则停止发送电平信号，主备切换板进行 A、B 设备的切换并锁定；同时，主系安全计算机的表决板在软件逻辑上进行主系和备系之间的工作状态切换。

⑤ 原工作备系回采到高电平信号，且主备的数据状态同步，则备系升级到主系状态，同时原本处于主系状态的安全计算机切换至备系状态；当备系检测到

主系的数据状态不同步，则两套安全计算机均进入备系状态；若两套安全计算机均出现故障，则两套安全计算机均进入备系状态。

（3）单套安全计算机的同步表决

单套安全计算机包含两个主控板、一个表决板、若干 IO 板和若干通信板，其中 IO 板的数量根据实际应用的需要进行配置，通信板可以根据需要配置 MVB 通信板、CAN+RS485 通信板和以太网通信板。单套计算机各板卡的数据流图如图 6 所示。单套安全计算机的数据同步原理如下：

a.外部数据通过通信板输入。

b.通信板通过通信总线将数据发送给表决板。

c.表决板通过通信总线将相同的数据分别发送到两个主控板。

d.两个主控板之间通过 UART 串行通信或者背板总线的方式进行周期性数据同步：

针对单套安全计算机，若两个主控板同步时长超过设定的运算周期，则计算超过累计时长，当两个主控板在连续 N 个周期内的同步时长均超过设定的运算周期时，则在本套安全计算机处于主系状态时降级为备系状态；在本套安全计算机处于备系状态时重启系统。

针对单套安全计算机，若一主控板在连续 N 个周期内均未收到另一主控板的有效数据，则判断对方同步数据交互不同步，在本套安全计算机处于主系状态时降级为备系状态；在本套安全计算机处于备系状态时重启系统。

e.两个主控板将计算处理后的数据发送到表决板，表决板采用 FPGA 对数据进行表决处理（比较两个主控板发送到表决板的数据是否一致），若数据一致则将输出结果发送到通信板，进而通信板发送数据到外部系统，提高了安全性。

（4）主控板故障诊断

本发明的车载安全计算机系统的主控板在软件、硬件两个层面实现自身故障的诊断：

a.在软件层面：在软件上对非法数据、通信异常、指针越界和任务超时等故障进行判断，一旦发生故障造成两个主控板数据不一致，则主动降级，无法降级时则重启。

b.在硬件层面：在硬件上设有硬件看门狗，如果喂狗失败，则主系降级为备

系状态，另一套安全计算机升级为主系状态；在主系降级的同时，释放动态电路，保证主备正常切换，其中单套安全计算机任意一个主控板释放动态电路则该套安全计算机因失去动态电路而降级。若喂狗失败，且本套安全计算机处于备系状态，则重启系统。本实施例中，动态电路是指主控板上用于产生电平信号的电路，当主系降级为备系时，释放动态电路，使原本工作在主系状态的安全计算机的主控板产生低电平（即不再发送高电平信号），并发送给主备切换板，保证主备切换。

上面结合附图对本发明的实施例进行了描述，但是本发明并不局限于上述的具体实施方式，上述的具体实施方式仅仅是示意性的，而不是局限性的，本领域的普通技术人员在本发明的启示下，在不脱离本发明宗旨和权利要求所保护的范围情况下，还可做出很多形式，这些均属于本发明的保护范围之内。

权利要求

1. 一种分布式车载安全计算机系统，其特征在于，包括结构和功能完全相同的二取二结构的两套安全计算机，两套安全计算机之间通过主备切换板相连，且两套安全计算机之间通过通信总线实现数据同步；其中，

主备切换板用于根据两套安全计算机的工作数据和设定的逻辑，控制两套安全计算机中的一套工作在主系状态而另一套工作在备系状态，或者控制两套安全计算机中的两套均工作在备系状态；其中，工作在主系状态是指安全计算机用于对外接收和输出数据，工作在备系状态是指安全计算机仅用于对外接收数据而不用于对外输出数据。

2. 如权利要求 1 所述的分布式车载安全计算机系统，其特征在于，对于两套安全计算机中的一套工作在主系状态而另一套工作在备系状态，两套安全计算机之间的数据同步规则包括：

两套安全计算机之间互相发送心跳帧，若处于备系状态的安全计算机根据心跳帧判断自身的数据状态不同于处于主系状态的安全计算机的数据状态，则处于备系状态的安全计算机发送同步请求帧至处于主系状态的安全计算机，处于主系状态的安全计算机接收到同步请求帧后即发送同步数据至处于备系状态的安全计算机。

3. 如权利要求 1 或 2 所述的分布式车载安全计算机系统，其特征在于，每一套安全计算机均包括两块主控板、一块表决板、至少一块 IO 板和若干通信板；

针对单套安全计算机，两主控板相连以用于实现单机内的数据同步，所述主控板、IO 板、通信板均与表决板相连，所述表决板与主备切换板相连；两套安全计算机的表决板之间通过通信总线相连。

4. 如权利要求 3 所述的分布式车载安全计算机系统，其特征在于，对于工作在主系状态的安全计算机，两主控板在进行同步数据比较之后并判断两主控板的同步数据一致的情况下，两主控板的同步数据通过表决板输出至工作在备系状态的安全计算机。

5. 如权利要求 3 所述的分布式车载安全计算机系统，其特征在于，对于工作在备系状态的安全计算机，判断两主控板接收到的数据一致的情况下，两主控板才进行数据同步。

6. 如权利要求 1 所述的分布式车载安全计算机系统，其特征在于，主备切换板控制安全计算机工作在主系状态或备系状态的逻辑包括：

主备切换板在接收到两套安全计算机在上电后发送的电平信号后，根据获得的两套安全计算机发送的电平信号的先后顺序，锁定先发送电平信号的安全计算机的工作状态为主系状态，锁定后发送电平信号的安全计算机的工作状态为备系状态；两套安全计算机通过从主备切换板回采的信号确定自身的工作状态。

7. 如权利要求 1 所述的分布式车载安全计算机系统，其特征在于，主备切换板控制安全计算机工作在主系状态或备系状态的逻辑包括：

当处于主系状态的安全计算机出现故障并停止向主备切换板发送电平信号时，主备切换板将原本处于主系状态的安全计算机的工作状态锁定为备系状态，并将原本处于备系状态的安全计算机的工作状态锁定为主系状态；两套安全计算机通过从主备切换板回采的信号确定自身的工作状态。

8. 如权利要求 6 或 7 所述的分布式车载安全计算机系统，其特征在于，安全计算机：用于在接收到主备切换板发送的高电平信号时，工作在主系状态；用于在接收到主备切换板发送的低电平信号时，工作在备系状态；

主备切换板控制安全计算机工作在主系状态或备系状态的逻辑还包括：

若原本处于备系状态的安全计算机回采到主备切换板发送的高电平信号，且两套安全计算机之间的数据同步，则原本处于备系状态的安全计算机切换至主系状态，原本处于主系状态的安全计算机切换至备系状态；

若原本处于备系状态的安全计算机回采到主备切换板发送的高电平信号，但两套安全计算机之间的数据不同步，则两套安全计算机均进入备系状态；

若两套安全计算机均出现故障，则两套安全计算机均进入备系状态。

9. 如权利要求 3 所述的分布式车载安全计算机系统，其特征在于，主备切换板控制安全计算机工作在主系状态或备系状态的逻辑还包括：

针对单套安全计算机，若两个主控板在连续 N 个周期内的同步时长均超过设定的运算周期，则在本套安全计算机处于主系状态时降级为备系状态；在本套安全计算机处于备系状态时重启系统；

针对单套安全计算机，若一主控板在连续 N 个周期内均未收到另一主控板的有效数据，则在本套安全计算机处于主系状态时降级为备系状态；在本套安全

计算机处于备系状态时重启系统。

10. 如权利要求 1 所述的分布式车载安全计算机系统，其特征在于，针对单套安全计算机，还设有硬件看门狗，在喂狗失败时，则在本套安全计算机处于主系状态时降级为备系状态，并释放动态电路且将另一套安全计算机升级为主系状态；在本套安全计算机处于备系状态时重启系统。

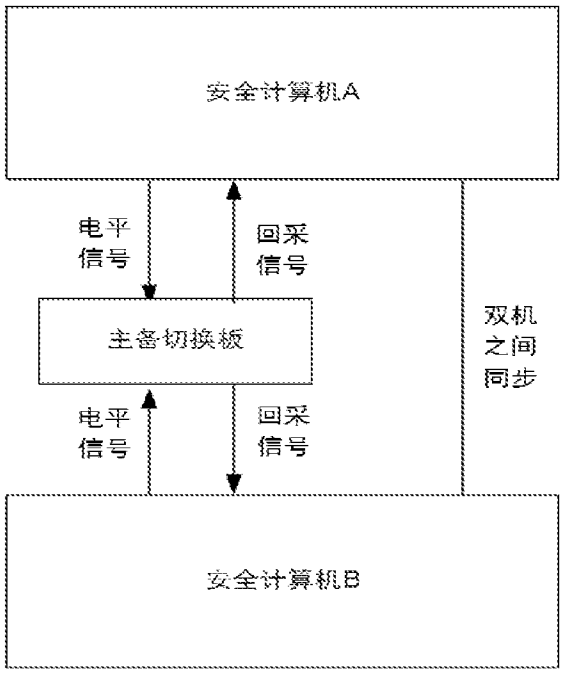


图 1

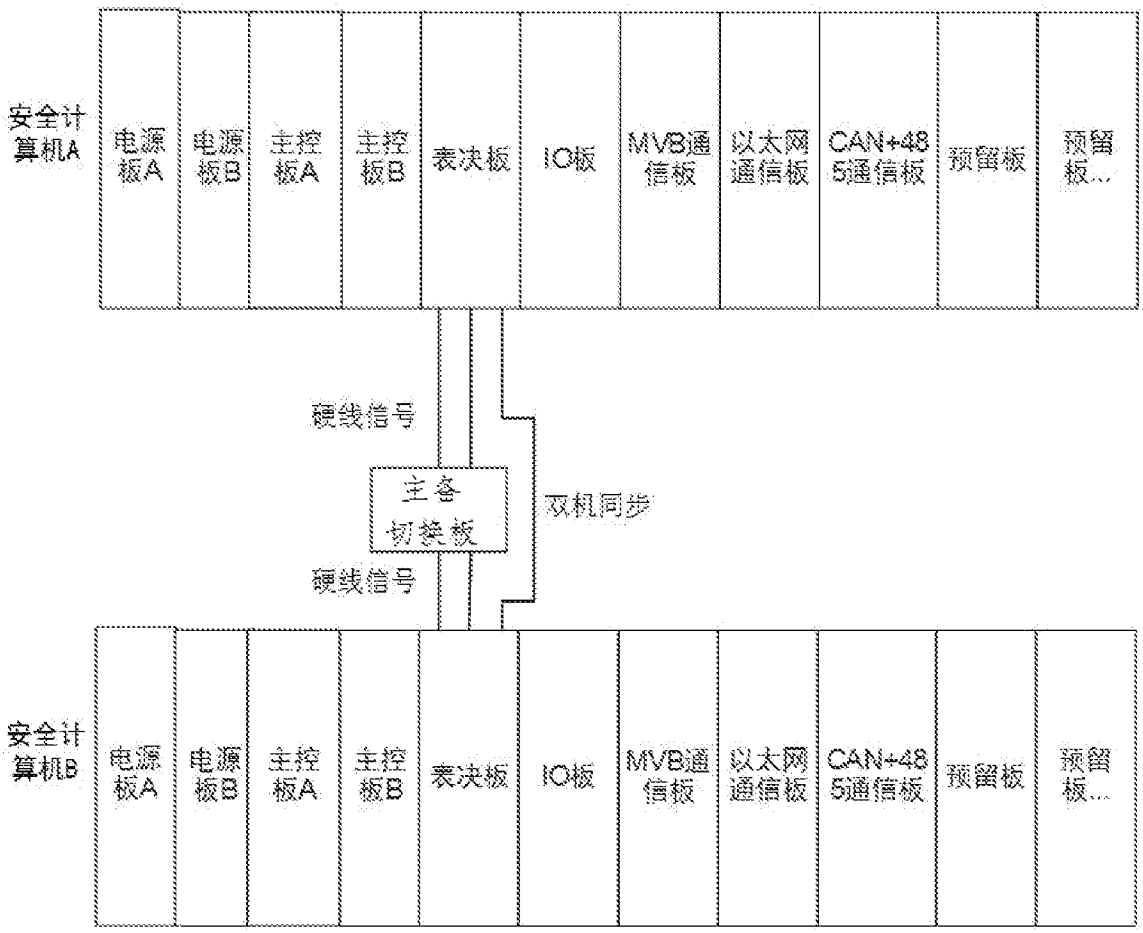

安全计算机A
电源板A
电源板B
主控板A
主控板B
表决板
IO板
MVB通信板
以太网通信板
CAN+485通信板
预留板
预留板...
硬线信号
主备切换板
双机同步
硬线信号
安全计算机B
电源板A
电源板B
主控板A
主控板B
表决板
IO板
MVB通信板
以太网通信板
CAN+485通信板
预留板
预留板...

图 2

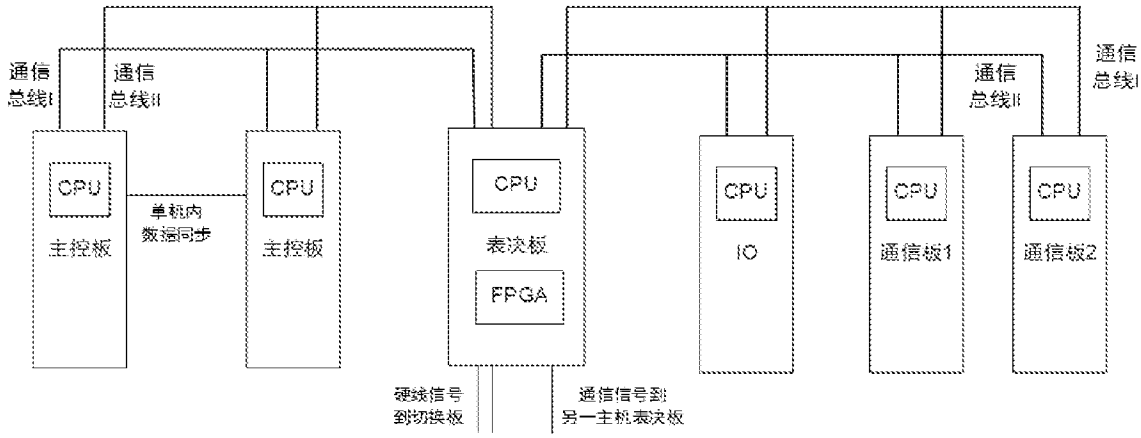

通信
总线I
通信
总线II
CPU
主控板
单机内
数据同步
CPU
主控板
CPU
表决板
FPGA
硬线信号
到切换板
通信信号到
另一主机表决板
CPU
IO
CPU
通信板1
通信
总线II
CPU
通信板2
通信
总线I

图 3

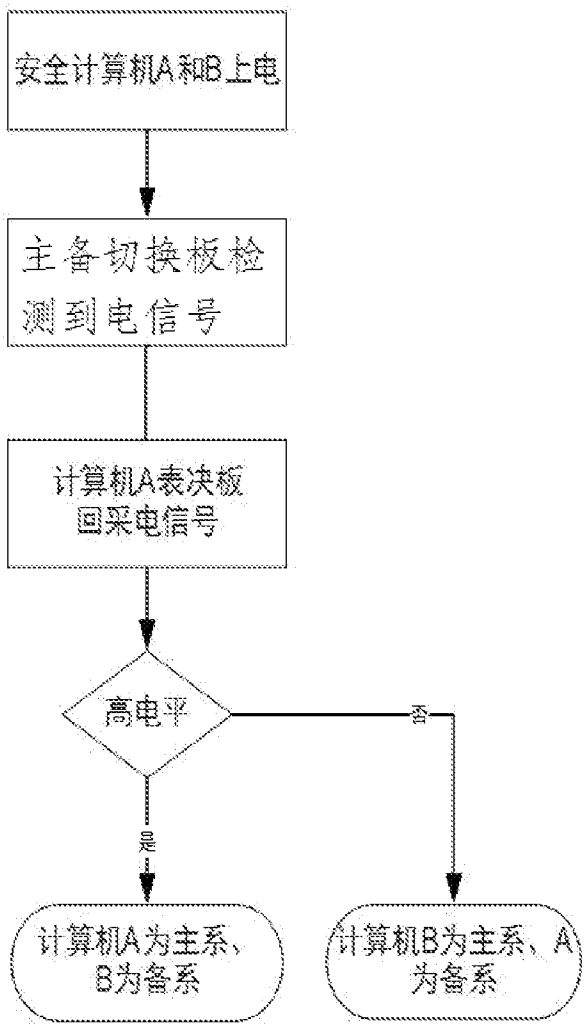

安全计算机A和B上电
主备切换板检
测到电信号
计算机A表决板
回采电信号
高电平
否
是
计算机A为主系、
B为备系
计算机B为主系、A
为备系

图 4

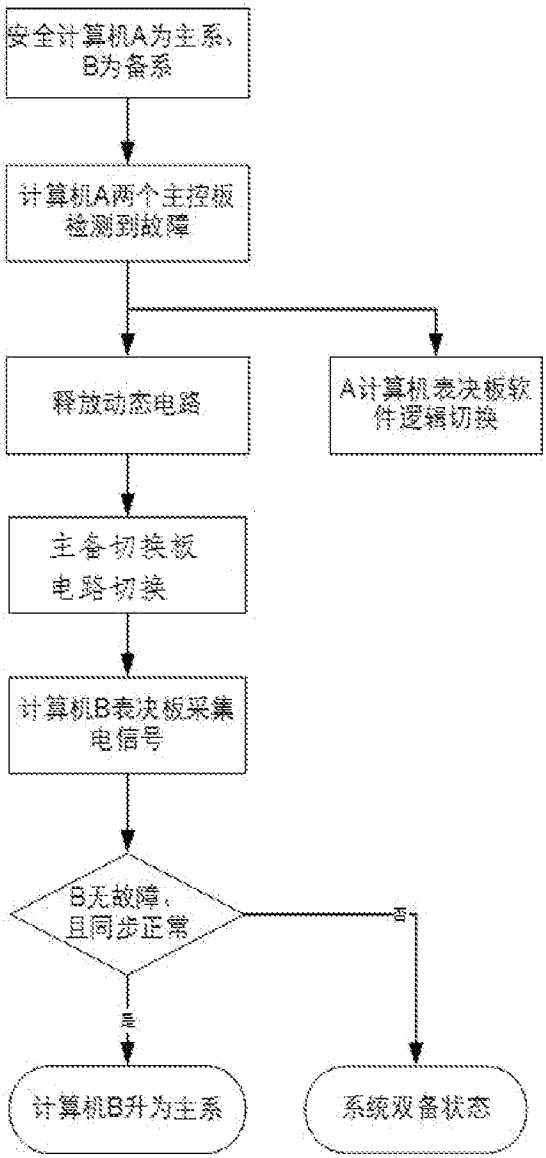

安全计算机A为主系，B为备系
计算机A两个主控板检测到故障
释放动态电路
A计算机表决板软件逻辑切换
主备切换板电路切换
计算机B表决板采集电信号
B无故障，且同步正常
否
是
计算机B升为主系
系统双备状态

图 5

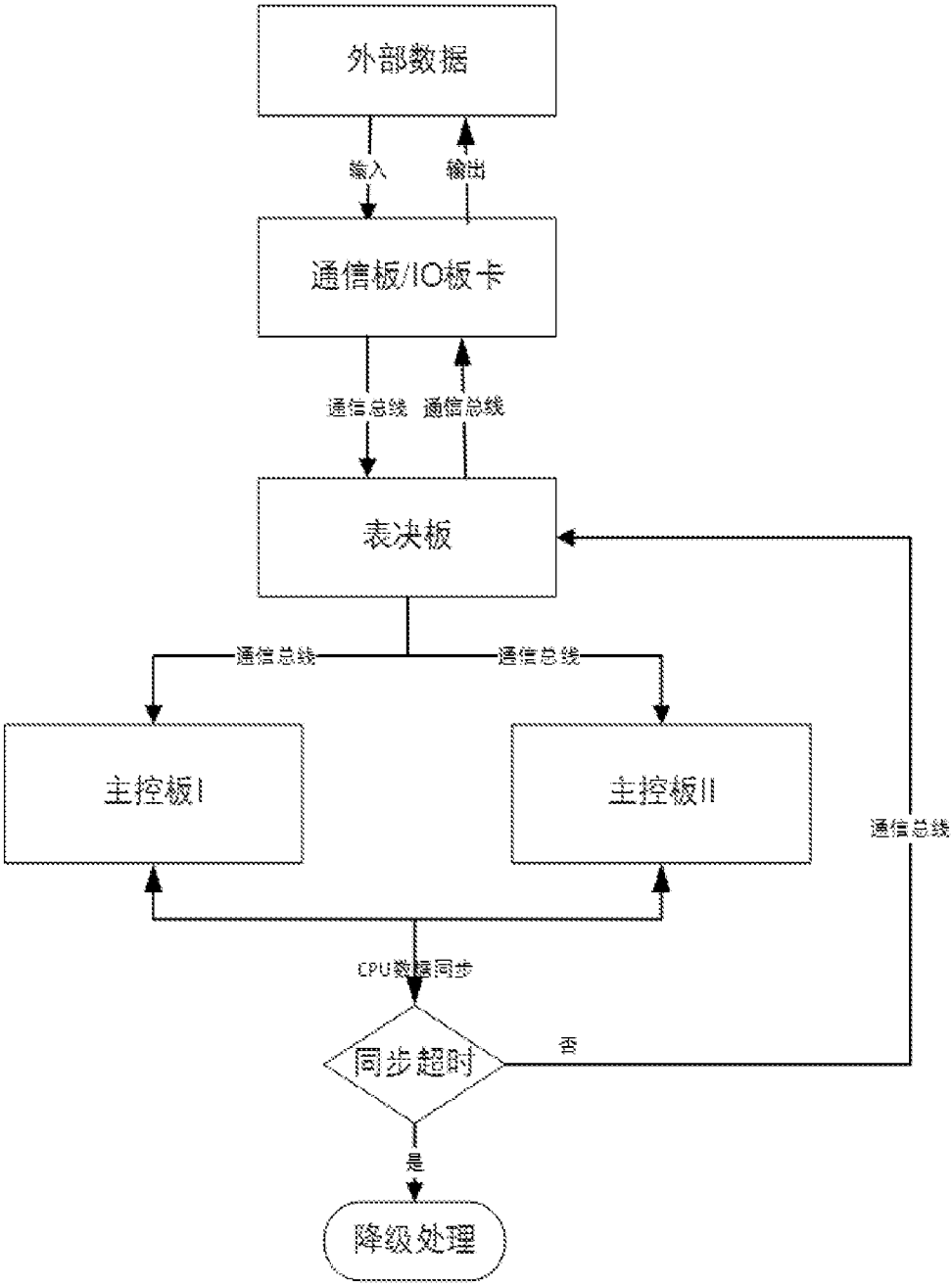

外部数据
输入
输出
通信板/IO板卡
通信总线
通信总线
表决板
通信总线
通信总线
主控板I
主控板II
通信总线
CPU数据同步
同步超时
否
是
降级处理

图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2021/116147

A. CLASSIFICATION OF SUBJECT MATTER

G06F 15/16(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS; CNTXT; WPABSC; VEN; USTXTC; WOTXT; EPTXT; CNKI: 列车, 铁路, 车载, 二取二, 切换, 同步, 主备, 安全, train, railway, vehicle mount, two-to-two, switch, synchronization, main-standby, secure

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 112395236 A (CRRC ZHUZHOU LOCOMOTIVE CO., LTD.) 23 February 2021 (2021-02-23) description, paragraphs 32-73, and figures 1-6	1-10
Y	CN 105159863 A (ZHUZHOU CSR TIMES ELECTRIC CO., LTD.) 16 December 2015 (2015-12-16) description paragraphs 58-76, figure 1	1-10
Y	CN 102945221 A (SHANGHAI HENGJUN SCIENCE & TECHNOLOGY CO., LTD.) 27 February 2013 (2013-02-27) description, paragraphs 24-34, figures 1-4	1-10
Y	CN 111645724 A (HUNAN CRRC TIMES COMMUNICATION SIGNALS CO., LTD.) 11 September 2020 (2020-09-11) description, paragraphs 18-33, and figure 1	1-10
Y	CN 102951182 A (SHANGHAI HENGJUN SCIENCE & TECHNOLOGY CO., LTD.) 06 March 2013 (2013-03-06) description, paragraphs 23-33, and figures 1-4	1-10

☑ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
27 October 2021	**18 November 2021**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088, China** Facsimile No. **(86-10)62019451**	Authorized officer Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2021/116147

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 105388890 A (ZHUZHOU CSR TIMES ELECTRIC CO., LTD.) 09 March 2016 (2016-03-09) entire document	1-10
A	EP 1484681 A2 (SIEMENS AKTIENGESELLSCHAFT) 08 December 2004 (2004-12-08) entire document	1-10

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2021/116147

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 112395236 A	23 February 2021	None	
CN 105159863 A	16 December 2015	None	
CN 102945221 A	27 February 2013	None	
CN 111645724 A	11 September 2020	None	
CN 102951182 A	06 March 2013	None	
CN 105388890 A	09 March 2016	WO 2017107665 A1	29 June 2017
EP 1484681 A2	08 December 2004	DE 10319903 A1	25 November 2004
		DE 10319903 B4	31 May 2007

国际检索报告

国际申请号
PCT/CN2021/116147

A. 主题的分类

G06F 15/16(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNABS;CNTXT;WPABSC;VEN;USTXTC;WOTXT;EPTXT;CNKI:列车,铁路,车载,二取二,切换,同步,主备,安全, train, railway, vehicle mount, two-to-two, switch, synchronization, main-standby, secure

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 112395236 A (中车株洲电力机车有限公司) 2021年 2月 23日 (2021-02-23) 说明书第32-73段，图1-6	1-10
Y	CN 105159863 A (株洲南车时代电气股份有限公司) 2015年 12月 16日 (2015-12-16) 说明书第58-76段，图1	1-10
Y	CN 102945221 A (上海亨钧科技有限公司) 2013年 2月 27日 (2013-02-27) 说明书第24-34段，附图1-4	1-10
Y	CN 111645724 A (湖南中车时代通信信号有限公司) 2020年 9月 11日 (2020-09-11) 说明书第18-33段，图1	1-10
Y	CN 102951182 A (上海亨钧科技有限公司) 2013年 3月 6日 (2013-03-06) 说明书第23-33段，图1-4	1-10
A	CN 105388890 A (株洲南车时代电气股份有限公司) 2016年 3月 9日 (2016-03-09) 全文	1-10
A	EP 1484681 A2 (SIEMENS AKTIENGESELLSCHAFT) 2004年 12月 8日 (2004-12-08) 全文	1-10

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2021年 10月 27日	2021年 11月 18日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国 北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 李腾飞 电话号码 86-(20)-28958130

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2021/116147

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	112395236	A	2021年 2月 23日	无			
CN	105159863	A	2015年 12月 16日	无			
CN	102945221	A	2013年 2月 27日	无			
CN	111645724	A	2020年 9月 11日	无			
CN	102951182	A	2013年 3月 6日	无			
CN	105388890	A	2016年 3月 9日	WO	2017107665	A1	2017年 6月 29日
EP	1484681	A2	2004年 12月 8日	DE	10319903	A1	2004年 11月 25日
				DE	10319903	B4	2007年 5月 31日