(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 106054115 B
(45)授权公告日 2019.01.15

(21)申请号 201610640089.7

(22)申请日 2016.08.05

(65)同一申请的已公布的文献号
申请公布号 CN 106054115 A

(43)申请公布日 2016.10.26

(73)专利权人 中国南方电网有限责任公司电网技术研究中心
地址 510080 广东省广州市越秀区东风东路水均岗8号
专利权人 南方电网科学研究院有限责任公司

(72)发明人 李鹏 胡珊珊 张乐平 肖勇 林伟斌 王吉

(74)专利代理机构 广州华进联合专利商标代理有限公司 44224
代理人 冯右明

(51)Int.Cl.
G01R 35/04(2006.01)

(56)对比文件
CN 105243746 A,2016.01.13,
CN 204904449 U,2015.12.23,
CN 103198575 A,2013.07.10,
CN 203616390 U,2014.05.28,
CN 204925691 U,2015.12.30,
13823608335.费控电能表信息交换安全认证技术要求.《百度文库》.2015,第19-20、27、32、36页.

审查员 尤茜

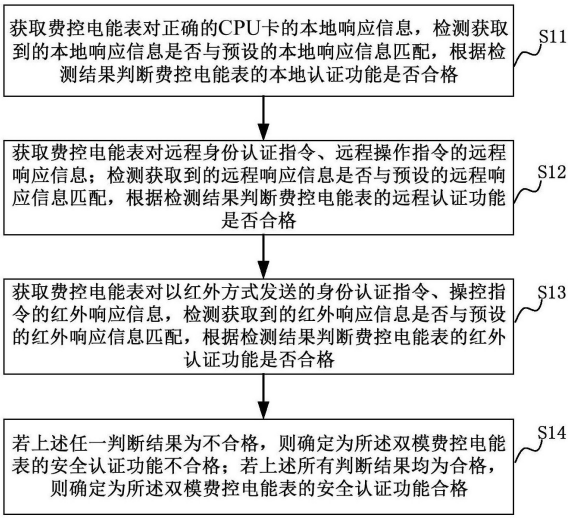
权利要求书4页 说明书8页 附图5页

(54)发明名称

费控电能表的安全认证功能测试方法和系统

(57)摘要

本发明涉及费控电能表的安全认证功能测试方法和系统。所述方法包括:获取费控电能表对正确CPU卡的本地响应信息,判断费控电能表的本地认证功能是否合格;获取费控电能表对远程身份认证指令、远程操作指令的远程响应信息;判断费控电能表的远程认证功能是否合格;获取费控电能表对以红外方式发送的身份认证指令、操控指令的红外响应信息,判断费控电能表的红外认证功能是否合格;若任一判断结果为不合格,则确定为所述双模费控电能表的安全认证功能不合格;若判断结果均为合格,则确定为所述双模费控电能表的安全认证功能合格。通过本发明能够全面准确的检测双模费控电能表的安全认证功能。



CN 106054115 B

1.一种费控电能表的安全认证功能测试方法,其特征在于,包括:

获取费控电能表对正确CPU卡的本地响应信息,检测获取到的本地响应信息是否与预设的本地响应信息匹配,根据检测结果判断费控电能表的本地认证功能是否合格;

获取费控电能表对远程身份认证指令、远程操作指令的远程响应信息;检测获取到的远程响应信息是否与预设的远程响应信息匹配,根据检测结果判断费控电能表的远程认证功能是否合格;

获取费控电能表对以红外方式发送的身份认证指令、操控指令的红外响应信息,检测获取到的红外响应信息是否与预设的红外响应信息匹配,根据检测结果判断费控电能表的红外认证功能是否合格;

若上述任一判断结果为不合格,则确定为所述双模费控电能表的安全认证功能不合格;若上述所有判断结果均为合格,则确定为所述双模费控电能表的安全认证功能合格;

其中,获取费控电能表对以红外方式发送的身份认证指令、操控指令的红外响应信息,检测获取到的红外响应信息是否与预设的红外响应信息匹配,根据检测结果判断费控电能表的红外认证功能是否合格的步骤包括:

在未进行红外身份认证的状态下,通过红外接口向双模费控电能表发送操控指令,检测双模费控电能表对本次操控指令的应答/执行情况是否与预设的第一红外响应信息匹配;

通过红外通信口向双模费控电能表发送正确的身份认证指令之后,在认证时效内向双模费控电能表发送操控指令,检测双模费控电能表对本次操控指令的应答/执行情况是否与预设的第二红外响应信息匹配;

若任一检测结果为不匹配,则判断为费控电能表的红外认证功能不合格;若检测结果均为匹配,则判断为费控电能表的红外认证功能合格。

2.根据权利要求1所述的费控电能表的安全认证功能测试方法,其特征在于,获取费控电能表对正确CPU卡的本地响应信息,检测获取到的本地响应信息是否与预设的本地响应信息匹配的步骤之前还包括:

检测双模费控电能表当前的费控模式,若不是本地费控模式,则将所述双模费控电能表切换为本地费控模式。

3.根据权利要求1所述的费控电能表的安全认证功能测试方法,其特征在于,还包括检测双模费控电能表的MAC挂起功能是否合格的步骤,该步骤包括:

在向双模费控电能表发送第一数量的发送MAC错误的远程指令之后,向双模费控电能表发送修改时间的远程操控指令,检测双模费控电能表对本次操控指令的应答/执行情况是否与预设的第一挂起应答/执行情况匹配;所述第一数量小于启动MAC挂起功能的MAC攻击数;

在向双模费控电能表发送第二数量的发送MAC错误的远程指令之后,向双模费控电能表发送修改时间的远程操控指令,检测双模费控电能表对本次操控指令的应答/执行情况是否与预设的第二挂起应答/执行情况匹配;第二数量大于等于启动MAC挂起功能的MAC攻击数;

监测到双模费控电能表的MAC挂起截止时间到时,向双模费控电能表发送修改时间的远程操控指令,检测双模费控电能表对本次操控指令的应答/执行情况是否与预设的第三

挂起应答/执行情况匹配；

若任一的检测结果为不匹配，则判断为双模费控电能表的MAC挂起功能不合格，若检测结果均为匹配时，判断为双模费控电能表的MAC挂起功能合格；

若双模费控电能表的MAC挂起功能不合格，则确定为所述双模费控电能表的安全认证功能不合格。

4.根据权利要求3所述的费控电能表的安全认证功能测试方法，其特征在于，启动MAC挂起功能的MAC攻击数为200次，所述第一数量属于190～195区间；所述第二数量属于205～215区间。

5.根据权利要求1所述的费控电能表的安全认证功能测试方法，其特征在于，获取费控电能表对正确CPU卡的本地响应信息，检测获取到的本地响应信息是否与预设的本地响应信息匹配，根据检测结果判断费控电能表的本地认证功能是否合格的步骤包括：

获取费控电能表在测试密钥状态下，对正确CPU卡的本地响应信息，检测所述本地响应信息是否与预设的本地响应信息匹配；

若检测结果为不匹配，则判断为费控电能表的本地认证功能不合格；若检测结果为匹配，则判断为费控电能表的本地认证功能合格。

6.根据权利要求1所述的费控电能表的安全认证功能测试方法，其特征在于，获取费控电能表对远程身份认证指令、远程操作指令的远程响应信息；检测获取到的远程响应信息是否与预设的远程响应信息匹配，根据检测结果判断费控电能表的远程认证功能是否合格的步骤包括：

向双模费控电能表发送远程身份认证指令，检测双模费控电能表对本次认证指令的应答状况是否与预设的第一远程响应信息匹配；

向双模费控电能表发送远程身份认证指令，并发送设置身份认证时效为0分钟的指令，检测双模费控电能表对本次时效设置指令的应答/执行情况是否与预设的第二远程响应信息匹配；

向双模费控电能表发送远程身份认证指令，并发送设置身份认证时效为非0的第一时长的指令，检测双模费控电能表对本次时效设置指令的应答/执行情况是否与预设的第三远程响应信息匹配；

向双模费控电能表发送远程身份认证指令，并发送设置身份认证时效为非0的第二时长的指令；监测到所述第二时长届满时向双模费控电能表发送修改日期时间的指令，检测双模费控电能表对本次修改日期时间指令的应答/执行情况是否与预设的第四远程响应信息匹配；

向双模费控电能表发送远程身份认证指令，并发送设置身份认证时效为非0的第三时长的指令，等待设定时间后获取双模费控电能表的认证时效剩余时间，检测每次获取到的认证时效剩余时间是否与对应的参考剩余时间匹配；

向双模费控电能表发送身份认证失效指令之后，发送修改日期时间的指令，检测双模费控电能表对本次修改日期时间指令的应答/执行情况是否与预设的第五远程响应信息匹配；

若上述任一检测结果为不匹配，则判断为费控电能表的远程认证功能不合格；若上述所有检测结果均为匹配，则判断为费控电能表的远程认证功能合格。

7.根据权利要求6所述的费控电能表的安全认证功能测试方法,其特征在于,

所述第一时长大于等于9999分钟;所述第二时长为2～5分钟;所述第三时长为20～30分钟。

8.一种费控电能表的安全认证功能测试系统,其特征在于,包括:

第一测试模块,用于获取费控电能表对正确的CPU卡的本地响应信息,检测获取到的本地响应信息是否与预设的本地响应信息匹配,根据检测结果判断费控电能表的本地认证功能是否合格;

第二测试模块,用于获取费控电能表对远程身份认证指令、远程操作指令的远程响应信息;检测获取到的远程响应信息是否与预设的远程响应信息匹配,根据检测结果判断费控电能表的远程认证功能是否合格;

第三测试模块,用于获取费控电能表对以红外方式发送的身份认证指令、操控指令的红外响应信息,检测获取到的红外响应信息是否与预设的红外响应信息匹配,根据检测结果判断费控电能表的红外认证功能是否合格;

判断模块,用于若上述任一测试模块的判断结果为不合格,则确定为所述双模费控电能表的安全认证功能不合格;若上述所有判断结果均为合格,则确定为所述双模费控电能表的安全认证功能合格;

所述第三测试模块,具体用于:

在未进行红外身份认证的状态下,通过红外接口向双模费控电能表发送操控指令,检测双模费控电能表对本次操控指令的应答/执行情况是否与预设的第一红外响应信息匹配;

通过红外通信口向双模费控电能表发送正确的身份认证指令之后,在认证时效内向双模费控电能表发送操控指令,检测双模费控电能表对本次操控指令的应答/执行情况是否与预设的第二红外响应信息匹配;

若任一检测结果为不匹配,则判断为费控电能表的红外认证功能不合格;若检测结果均为匹配,则判断为费控电能表的红外认证功能合格。

9.根据权利要求8所述的费控电能表的安全认证功能测试系统,其特征在于,还包括:

第四测试模块,用于检测双模费控电能表的MAC挂起功能是否合格的步骤,包括:

在向双模费控电能表发送第一数量的发送MAC错误的远程指令之后,向双模费控电能表发送修改时间的远程操控指令,检测双模费控电能表对本次操控指令的应答/执行情况是否与预设的第一挂起应答/执行情况匹配;所述第一数量小于启动MAC挂起功能的MAC攻击数;

在向双模费控电能表发送第二数量的发送MAC错误的远程指令之后,向双模费控电能表发送修改时间的远程操控指令,检测双模费控电能表对本次操控指令的应答/执行情况是否与预设的第二挂起应答/执行情况匹配;第二数量大于等于启动MAC挂起功能的MAC攻击数;

监测到双模费控电能表的MAC挂起截止时间到时,向双模费控电能表发送修改时间的远程操控指令,检测双模费控电能表对本次操控指令的应答/执行情况是否与预设的第三挂起应答/执行情况匹配;

若任一的检测结果为不匹配,则判断为双模费控电能表的MAC挂起功能不合格,若检测

结果均为匹配时，判断为双模费控电能表的MAC挂起功能合格；

所述判断模块，还用于若第四测试模块的检测结果为不合格，则确定为所述双模费控电能表的安全认证功能不合格。

费控电能表的安全认证功能测试方法和系统

技术领域

[0001] 本发明涉及设备检测技术领域，特别是涉及费控电能表的安全认证功能测试方法和系统。

背景技术

[0002] 区别于普通的费控电能表只具有单一的费控模式，双模费控电能表既可以工作在本地费控模式，也可以工作在远程费控模式，且两种模式之间可以相互切换。所谓的本地费控模式是指本地计量、本地计费、本地开关控制，即电能表可自动根据自身电能计量与设置的电价，自动完成电费结算并按照设置阀值实现剩余金额告警、欠费拉闸、充值后合闸等操作。所谓的远程费控模式是指本地计量、远程主站计费，并通过远程主站实现开关控制，即电能表仅进行电能计量，通过RS485、载波等方式把电能数据传送至远程主站，由远程主站进行电费结算，且根据结算情况下发拉合闸等操作命令。

[0003] 双模费控电能表通过虚拟介质或固态介质(例如射频IC卡)进行初始化、开户、充值、补卡、参数设置、信息返写和拉合闸命令下发等操作，操作过程中须经过硬件安全模块进行安全认证、数据加解密处理。对应的，双模费控电能表的费控功能主要包括：初始化功能、开户功能、充值功能、补卡功能、用户卡返写功能、参数更新功能、密钥更新功能、数据回抄功能、远程控制功能、事件记录功能、清零功能、费控模式切换功能、钱包退费功能、费控结算功能、安全认证功能、防伪造卡攻击功能、软件比对功能等。其中，初始化功能、开户功能、充值功能、补卡功能、用户卡返写功能、钱包退费功能、费控结算功能等7个功能项为本地费控模式独有；参数更新功能、密钥更新功能、数据回抄功能、远程控制功能、事件记录功能、清零功能、费控模式切换功能、安全认证功能、防伪造卡攻击功能、软件比对功能等10个功能项，则是两种模式均具备。

[0004] 然而在目前，无论是国家规范，还是行业规范或企业规范，均没有涉及费控电能表的安全认证功能测试的相关内容，因此存在以下问题：难以评判双模费控电能表的安全认证功能是否符合企业的技术标准要求并给出客观的检测结论，由此给双模费控电能表的使用单位带来了一定的应用风险，难以保障双模费控电能表的对非法远程指令的防攻击能力及挂起功能执行情况。

发明内容

[0005] 基于此，本发明实施例提供费控电能表的安全认证功能测试方法和系统，能够全面准确的检测双模费控电能表的安全认证功能，有利于保证双模费控电能表的防攻击能力。

[0006] 本发明一方面提供费控电能表的安全认证功能测试方法，包括：

[0007] 获取费控电能表对正确的CPU卡的本地响应信息，检测获取到的本地响应信息是否与预设的本地响应信息匹配，根据检测结果判断费控电能表的本地认证功能是否合格；

[0008] 获取费控电能表对远程身份认证指令、远程操作指令的远程响应信息；检测获取

到的远程响应信息是否与预设的远程响应信息匹配，根据检测结果判断费控电能表的远程认证功能是否合格；

[0009] 获取费控电能表对以红外方式发送的身份认证指令、操控指令的红外响应信息，检测获取到的红外响应信息是否与预设的红外响应信息匹配，根据检测结果判断费控电能表的红外认证功能是否合格；

[0010] 若上述任一判断结果为不合格，则确定为所述双模费控电能表的安全认证功能不合格；若上述所有判断结果均为合格，则确定为所述双模费控电能表的安全认证功能合格。

[0011] 本发明另一方面提供费控电能表的安全认证功能测试系统，包括：

[0012] 第一测试模块，用于获取费控电能表对正确的CPU卡的本地响应信息，检测获取到的本地响应信息是否与预设的本地响应信息匹配，根据检测结果判断费控电能表的本地认证功能是否合格；

[0013] 第二测试模块，用于获取费控电能表对远程身份认证指令、远程操作指令的远程响应信息；检测获取到的远程响应信息是否与预设的远程响应信息匹配，根据检测结果判断费控电能表的远程认证功能是否合格；

[0014] 第三测试模块，用于获取费控电能表对以红外方式发送的身份认证指令、操控指令的红外响应信息，检测获取到的红外响应信息是否与预设的红外响应信息匹配，根据检测结果判断费控电能表的红外认证功能是否合格；

[0015] 判断模块，用于若上述任一测试模块的判断结果为不合格，则确定为所述双模费控电能表的安全认证功能不合格；若上述所有判断结果均为合格，则确定为所述双模费控电能表的安全认证功能合格。

[0016] 上述技术方案，通过检查双模费控电能表在不同模式下的安全认证响应情况，全面准确的检测双模费控电能表的安全认证功能，适用于各单位对双模费控电能表安全认证功能进行评价，适用性广。

附图说明

[0017] 图1为一实施例的费控电能表的安全认证功能测试方法的示意性流程图；

[0018] 图2为一实施例的费控电能表的本地认证功能测试举例；

[0019] 图3为一实施例的费控电能表的远程认证功能测试举例；

[0020] 图4为一实施例的费控电能表的红外认证功能测试举例；

[0021] 图5为一实施例的费控电能表的MAC挂起功能测试举例；

[0022] 图6为一实施例的费控电能表的安全认证功能测试系统的示意性结构图。

具体实施方式

[0023] 为了使本发明的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本发明进行进一步详细说明。应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

[0024] 图1为一实施例的费控电能表的安全认证功能测试方法的示意性流程图。

[0025] 如图1所示，本实施例中的费控电能表的安全认证功能测试方法包括步骤：

[0026] S11，获取费控电能表对正确的CPU卡的本地响应信息，检测获取到的本地响应信

息是否与预设的本地响应信息匹配，根据检测结果判断费控电能表的本地认证功能是否合格；

[0027] 本发明实施例中，该步骤的具体实施方式可包括：获取费控电能表在测试密钥状态下，对正确的CPU卡的第一本地响应信息，检测所述第一本地响应信息是否与预设的第一本地响应信息匹配；若检测结果为不匹配，则判断为费控电能表的本地认证功能不合格；若检测结果为匹配，则判断为费控电能表的本地认证功能合格。

[0028] 另一方面，该步骤还可包括：获取费控电能表在正式密钥状态下，对正确的CPU卡的第二本地响应信息，检测所述第二本地响应信息是否与预设的第二本地响应信息匹配；若任一方面的检测结果为不匹配，则判断为费控电能表的本地认证功能不合格；若两个检测结果均为匹配，则判断为费控电能表的本地认证功能合格。

[0029] S12，获取费控电能表对远程身份认证指令、远程操作指令的远程响应信息；检测获取到的远程响应信息是否与预设的远程响应信息匹配，根据检测结果判断费控电能表的远程认证功能是否合格；

[0030] 本发明实施例中，该步骤的具体实施方式可包括：

[0031] 第一方面，向双模费控电能表发送远程身份认证指令，检测双模费控电能表对本次认证指令的应答状况是否与预设的第一远程响应信息匹配；第二方面，向双模费控电能表发送远程身份认证指令，并发送设置身份认证时效为0分钟的指令，检测双模费控电能表对本次时效设置指令的应答/执行情况是否与预设的第二远程响应信息匹配；第三方面，向双模费控电能表发送远程身份认证指令，并发送设置身份认证时效为非0的第一时长的指令，检测双模费控电能表对本次时效设置指令的应答/执行情况是否与预设的第三远程响应信息匹配；第四方面，向双模费控电能表发送远程身份认证指令，并发送设置身份认证时效为非0的第二时长的指令；监测到所述第二时长届满时向双模费控电能表发送修改日期时间的指令，检测双模费控电能表对本次修改日期时间指令的应答/执行情况是否与预设的第四远程响应信息匹配；第五方面，向双模费控电能表发送远程身份认证指令，并发送设置身份认证时效为非0的第三时长的指令，按照预设时间间隔获取双模费控电能表的认证时效剩余时间，检测每次获取到的认证时效剩余时间是否与对应的参考剩余时间匹配；第六方面，向双模费控电能表发送身份认证失效指令之后，发送修改日期时间的指令，检测双模费控电能表对本次修改日期时间指令的应答/执行情况是否与预设的第五远程响应信息匹配。若上述六个方面中任一检测结果为不匹配，则判断为费控电能表的远程认证功能不合格；若上述六个方面的检测结果均为匹配，则判断为费控电能表的远程认证功能合格。

[0032] 优选的，所述第一时长大于等于9999分钟；所述第二时长为2～5分钟；所述第三时长为20～30分钟。

[0033] S13，获取费控电能表对以红外方式发送的身份认证指令、操控指令的红外响应信息，检测获取到的红外响应信息是否与预设的红外响应信息匹配，根据检测结果判断费控电能表的红外认证功能是否合格。

[0034] 本发明实施例中，该步骤的具体实施方式可包括：

[0035] 一方面，在未进行红外身份认证的状态下，通过红外接口向双模费控电能表发送操控指令，检测双模费控电能表对本次操控指令的应答/执行情况是否与预设的第一红外响应信息匹配；另一方面，通过红外通信口向双模费控电能表发送正确的身份认证指令之

后，在认证时效内向双模费控电能表发送操控指令，检测双模费控电能表对本次操控指令的应答/执行情况是否与预设的第二红外响应信息匹配。若该两方面中任一检测结果为不匹配，则判断为费控电能表的红外认证功能不合格；若该两方面的检测结果均为匹配，则判断为费控电能表的红外认证功能合格。

[0036] S14，若上述任一步骤的判断结果为不合格，则确定为所述双模费控电能表的安全认证功能不合格；若上述所有判断结果均为合格，则确定为所述双模费控电能表的安全认证功能合格。

[0037] 进一步的，所述费控电能表的安全认证功能测试方法还可包括检测双模费控电能表的MAC挂起功能是否合格的步骤，该步骤具体实施方式可包括：

[0038] 一方面，在向双模费控电能表发送第一数量的发送MAC错误的远程指令之后，向双模费控电能表发送修改时间的远程操控指令，检测双模费控电能表对本次操控指令的应答/执行情况是否与预设的第一挂起应答/执行情况匹配；所述第一数量小于启动MAC挂起功能的MAC攻击数；另一方面，在向双模费控电能表发送第二数量的发送MAC错误的远程指令之后，向双模费控电能表发送修改时间的远程操控指令，检测双模费控电能表对本次操控指令的应答/执行情况是否与预设的第二挂起应答/执行情况匹配；第二数量大于等于启动MAC挂起功能的MAC攻击数；又一方面，监测到双模费控电能表的MAC挂起截止时间到时，向双模费控电能表发送修改时间的远程操控指令，检测双模费控电能表对本次操控指令的应答/执行情况是否与预设的第三挂起应答/执行情况匹配。若其中任一方面的检测结果为不匹配，则判断为双模费控电能表的MAC挂起功能不合格，若检测结果均为匹配时，判断为双模费控电能表的MAC挂起功能合格。

[0039] 相应的，若双模费控电能表的MAC挂起功能不合格，则确定为所述双模费控电能表的安全认证功能不合格。因此，只有当双模费控电能表的本地认证功能、远程认证功能、红外认证功能以及MAC挂起功能均合格的情况下，才确定为双模费控电能表的安全认证功能合格。

[0040] 需要说明的是，本发明实施例中上述步骤的执行顺序不受限于上述示例的情况，例如，也可先执行步骤S12，再执行步骤S11；或者先执行步骤S13，再执行步骤S12。

[0041] 本实施例的费控电能表的安全认证功能测试方法，可全面准确的检测双模费控电能表的安全认证功能，适用于各单位对双模费控电能表安全认证功能进行评价，适用性广。

[0042] 下面通过一具体示例对本发明的费控电能表的安全认证功能测试方法作进一步的说明。其中，被测试的双模费控电能表具备安全认证功能，可通过双模费控电能表内安全模块采用加密保护方式进行身份认证、红外认证，对传输数据进行加密保护和MAC验证，实现数据机密性和完整性保护，防止重放攻击和非法操作。被测试的双模费控电能表的安全认证功能包括：本地身份认证功能、远程身份认证功能和红外身份认证功能，例如：主站与双模费控电能表之间，交互终端与双模费控电能表之间的认证为远程身份认证；双模费控电能表与CPU卡之间，交互终端与CPU卡之间的认证为本地身份认证；通过红外通信口进行的设备与双模费控电能表之间的认证为红外身份认证。安全认证通过后方可进行双模费控电能表的操作，若安全认证失败或认证失效后，双模费控电能表不允许进行远程充值、参数设置、密钥更新、数据回抄、远程控制、费控电能表清零等操作。

[0043] 对上述所述的被测试的双模费控电能表的安全认证功能进行检测的方式为，在双

模费控电能表上刷用户卡、向双模费控电能表发送远程和红外身份认证指令、远程操控指令，检查双模费控电能表的身份认证时效和身份认证失效的执行情况，还对MAC挂起功能的执行情况进行检查，以测试双模费控电能表对大量非法远程指令的防攻击能力及挂起功能执行情况。下面分别对本地认证功能、远程认证功能、红外认证功能以及MAC挂起功能的测试步骤进行举例说明。

[0044] 如图2所示，本地身份认证功能检测具体流程包括以下步骤：

[0045] 步骤S21：检查双模费控电能表的费控模式状态，若非本地费控模式，则设置为本地费控模式。

[0046] 优选的，由于对于双模费控电能表来说，本地身份认证功能属于本地费控模式，因此需预先检测双模费控电能表当前的费控模式，若不是本地费控模式，则将所述双模费控电能表切换为本地费控模式。

[0047] 步骤S22：测试在测试密钥状态下，测试向双模费控电能表插入正确的参数预置卡(CPU卡的一种)时，双模费控电能读卡响应状况。

[0048] 步骤S23：更新双模费控电能表的密钥，设置为正式密钥。测试向双模费控电能表插入正确的开户卡(CPU卡的一种)时，双模费控电能读卡响应状况；

[0049] 步骤S24：检查步骤S22～S23的检测情况，若任一步骤检测不通过，则本地认证功能的总体检测结论为“不合格”，仅当2个步骤均检测通过，本地认证功能的总体检测结论方为“合格”。

[0050] 如图3所示，远程身份认证功能检测具体流程包括以下步骤：

[0051] 步骤S31：向双模费控电能表发送远程身份认证指令，测试双模费控电能表对指令的应答状况。

[0052] 步骤S32：通过交互终端向双模费控电能表发送远程身份认证指令，测试双模费控电能表对指令的应答状况；

[0053] 步骤S33：向双模费控电能表发送远程身份认证指令，然后发送设置身份认证有效性为0分钟的指令，测试双模费控电能表对指令的应答状况；

[0054] 步骤S34：向双模费控电能表发送远程身份认证指令，然后发送设置身份认证有效性为9999分钟的指令，测试双模费控电能表对指令的应答状况和执行情况；

[0055] 步骤S35：向双模费控电能表发送远程身份认证指令，然后发送设置身份认证有效性为2分钟的指令。等待3分钟后，再发送修改日期时间的指令，测试双模费控电能表对修改日期时间指令的应答状况和执行情况；

[0056] 步骤S36：向双模费控电能表发送远程身份认证指令、和设置身份认证有效性为30分钟的指令，然后读取双模费控电能表的身份认证时效剩余时间并记下作为比对基准。分别等待45秒、90秒后和150秒后，分别读取双模费控电能表的身份认证时效剩余时间，并与比对基准比较，检查数据的正确性；

[0057] 步骤S37：向双模费控电能表发送身份认证时效指令，然后发送修改日期时间的指令，测试双模费控电能表对修改日期时间指令的应答状况；

[0058] 步骤S38：检查步骤S31～S37的检测情况，若任一步骤检测不通过，则远程认证功能的总体检测结论为“不合格”，仅当7个步骤均检测通过，远程认证功能的总体检测结论方为“合格”.

[0059] 如图4所示，红外身份认证功能检测具体流程包括以下步骤：

[0060] 步骤S41，测试在未进行红外身份认证的状态下，通过红外通信口向双模费控电能表发送修改日期时间指令，双模费控电能表对指令的应答和执行情况。

[0061] 步骤S42，通过红外通信口向双模费控电能表发送正确的身份认证指令，然后再发送修改日期时间指令。测试在身份认证指令有效的前提下，向双模费控电能表对修改日期时间指令的应答和执行情况；

[0062] 步骤S43，检查步骤S41～S42的检测情况，若任一步骤检测不通过，则红外认证功能的总体检测结论为“不合格”，仅当2个步骤均检测通过，红外认证功能的总体检测结论方为“合格”。

[0063] 如图5所示，MAC挂起功能检测具体流程包括以下步骤：

[0064] 步骤S51，向双模费控电能表发送有效的远程身份认证指令，然后设置身份认证有效性为30分钟，修改挂起取消时间为零点。

[0065] 步骤S52，等待双模费控电能表时间过零点。向双模费控电能表发送有效的远程身份认证指令，然后连续发送195次MAC错误的远程指令；双模费控电能表的启动MAC挂起功能的MAC攻击数为200次。

[0066] 步骤S53，向双模费控电能表发送将挂起取消时间修改至第二日零点的指令(应预留充足的时间以保障测试步骤S55完成前电能表时间仍未过零点)，测试双模费控电能表对修改时间指令的应答和执行情况。

[0067] 步骤S54，再向双模费控电能表连续发送10次MAC错误的远程指令；

[0068] 步骤S55，双模费控电能表的时间应未过零点，向双模费控电能表发送将修改时间指令，测试双模费控电能表对修改时间指令的应答和执行情况。

[0069] 步骤S56，等待双模费控电能表时间过零点，向双模费控电能表发送有效的远程身份认证指令，然后再发送修改日期时间指令，测试双模费控电能表对修改日期时间指令的应答和执行情况；

[0070] 步骤S57，检查步骤S53、S55和S56的检测情况，若任一步骤检测不通过，则总体检测结论为“不合格”，仅当3个步骤均检测通过总体检测结论方为“合格”。

[0071] 本发明上述示例的费控电能表的安全认证功能测试方法，覆盖了技术标准关于安全认证功能的各项技术要求，测试内容全面；适用于各单位对双模费控电能表安全认证功能进行评价，适用性广。

[0072] 需要说明的是，对于前述的各方法实施例，为了简便描述，将其都表述为一系列的动作组合，但是本领域技术人员应该知悉，本发明并不受所描述的动作顺序的限制，因为依据本发明，某些步骤可以采用其它顺序或者同时进行。

[0073] 基于与上述实施例中的费控电能表的安全认证功能测试方法相同的思想，本发明还提供费控电能表的安全认证功能测试系统，该系统可用于执行上述费控电能表的安全认证功能测试方法。为了便于说明，费控电能表的安全认证功能测试系统实施例的结构示意图中，仅仅示出了与本发明实施例相关的部分，本领域技术人员可以理解，图示结构并不构成对系统的限定，可以包括比图示更多或更少的部件，或者组合某些部件，或者不同的部件布置。

[0074] 图6为本发明一实施例的费控电能表的安全认证功能测试系统的示意性结构图；

如图6所示，本实施例的费控电能表的安全认证功能测试系统包括：第一测试模块610、第二测试模块620、第三测试模块630以及判断模块640，各模块详述如下：

[0075] 所述第一测试模块610，用于获取费控电能表对正确CPU卡的本地响应信息，检测获取到的本地响应信息是否与预设的本地响应信息匹配，根据检测结果判断费控电能表的本地认证功能是否合格；

[0076] 所述第二测试模块620，用于获取费控电能表对远程身份认证指令、远程操作指令的远程响应信息；检测获取到的远程响应信息是否与预设的远程响应信息匹配，根据检测结果判断费控电能表的远程认证功能是否合格；

[0077] 所述第三测试模块630，用于获取费控电能表对以红外方式发送的身份认证指令、操控指令的红外响应信息，检测获取到的红外响应信息是否与预设的红外响应信息匹配，根据检测结果判断费控电能表的红外认证功能是否合格；

[0078] 所述判断模块640，用于若上述任一测试模块的判断结果为不合格，则确定为所述双模费控电能表的安全认证功能不合格；若上述所有判断结果均为合格，则确定为所述双模费控电能表的安全认证功能合格。

[0079] 进一步的，所述费控电能表的安全认证功能测试系统还可包括：第四测试模块650，用于检测双模费控电能表的MAC挂起功能是否合格的步骤，包括：

[0080] 在向双模费控电能表发送第一数量的发送MAC错误的远程指令之后，向双模费控电能表发送修改时间的远程操控指令，检测双模费控电能表对本次操控指令的应答/执行情况是否与预设的第一挂起应答/执行情况匹配；所述第一数量小于启动MAC挂起功能的MAC攻击数；

[0081] 在向双模费控电能表发送第二数量的发送MAC错误的远程指令之后，向双模费控电能表发送修改时间的远程操控指令，检测双模费控电能表对本次操控指令的应答/执行情况是否与预设的第二挂起应答/执行情况匹配；第二数量大于等于启动MAC挂起功能的MAC攻击数；

[0082] 监测到双模费控电能表的MAC挂起截止时间到时，向双模费控电能表发送修改时间的远程操控指令，检测双模费控电能表对本次操控指令的应答/执行情况是否与预设的第三挂起应答/执行情况匹配；

[0083] 若任一的检测结果为不匹配，则判断为双模费控电能表的MAC挂起功能不合格，若检测结果均为匹配时，判断为双模费控电能表的MAC挂起功能合格；

[0084] 相应的，所述判断模块640，还用于若第四测试模块的检测结果为不合格，则确定为所述双模费控电能表的安全认证功能不合格。

[0085] 需要说明的是，上述示例的费控电能表的安全认证功能测试系统的实施方式中，各模块之间的信息交互、执行过程等内容，由于与本发明前述方法实施例基于同一构思，其带来的技术效果与本发明前述方法实施例相同，具体内容可参见本发明方法实施例中的叙述，此处不再赘述。

[0086] 此外，上述示例的费控电能表的安全认证功能测试系统的实施方式中，各功能模块的逻辑划分仅是举例说明，实际应用中可以根据需要，例如出于相应硬件的配置要求或者软件的实现的便利考虑，将上述功能分配由不同的功能模块完成，即将所述费控电能表的安全认证功能测试系统的内部结构划分成不同的功能模块，以完成以上描述的全部或者

部分功能。其中各功能模既可以采用硬件的形式实现，也可以采用软件功能模块的形式实现。

[0087] 本领域普通技术人员可以理解，实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于一计算机可读取存储介质中，作为独立的产品销售或使用。所述程序在执行时，可执行如上述各方法的实施例的全部或部分步骤。其中，所述的存储介质可为磁碟、光盘、只读存储记忆体(Read-Only Memory，ROM)或随机存储记忆体(Random Access Memory，RAM)等。

[0088] 在上述实施例中，对各个实施例的描述都各有侧重，某个实施例中没有详述的部分，可以参见其它实施例的相关描述。

[0089] 以上所述实施例仅表达了本发明的几种实施方式，不能理解为对本发明专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本发明构思的前提下，还可以做出若干变形和改进，这些都属于本发明的保护范围。因此，本发明专利的保护范围应以所附权利要求为准。

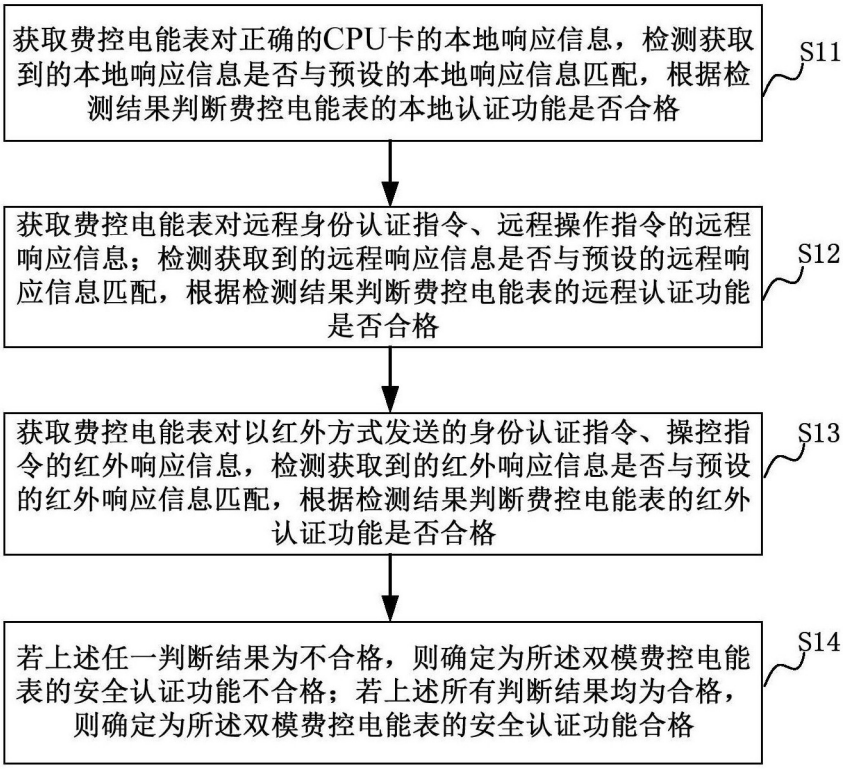

获取费控电能表对正确的CPU卡的本地响应信息，检测获取到的本地响应信息是否与预设的本地响应信息匹配，根据检测结果判断费控电能表的本地认证功能是否合格
S11
获取费控电能表对远程身份认证指令、远程操作指令的远程响应信息；检测获取到的远程响应信息是否与预设的远程响应信息匹配，根据检测结果判断费控电能表的远程认证功能是否合格
S12
获取费控电能表对以红外方式发送的身份认证指令、操控指令的红外响应信息，检测获取到的红外响应信息是否与预设的红外响应信息匹配，根据检测结果判断费控电能表的红外认证功能是否合格
S13
若上述任一判断结果为不合格，则确定为所述双模费控电能表的安全认证功能不合格；若上述所有判断结果均为合格，则确定为所述双模费控电能表的安全认证功能合格
S14

图1

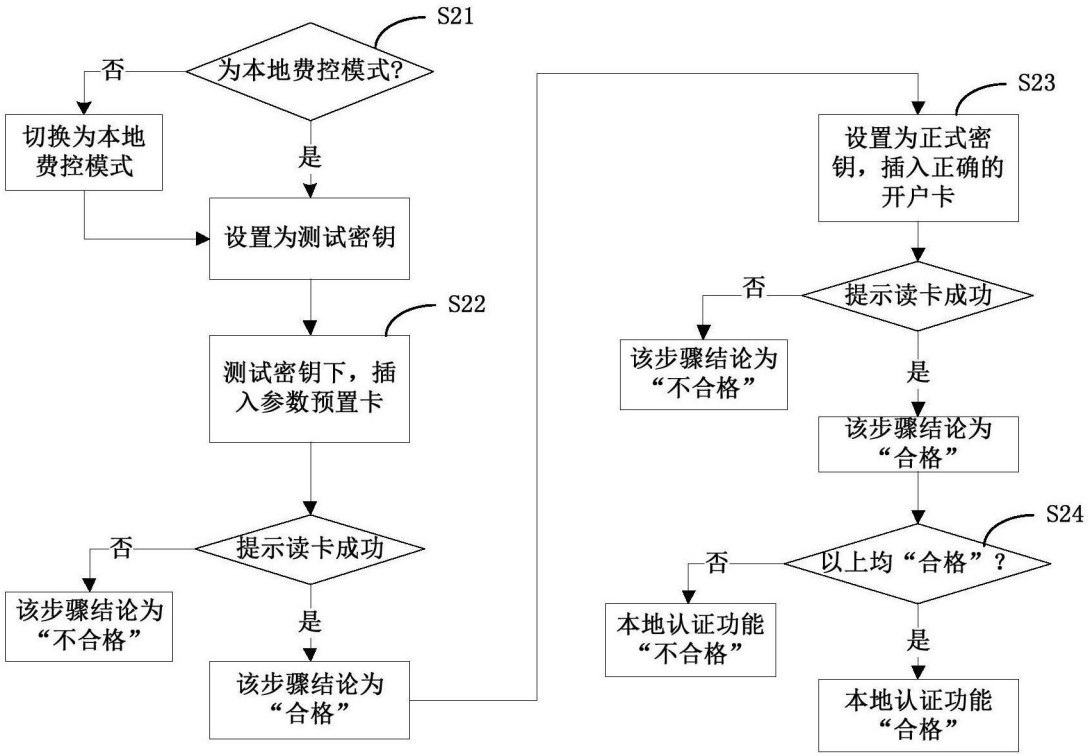

S21
为本地费控模式?
否
切换为本地费控模式
是
设置为测试密钥
S22
测试密钥下，插入参数预置卡
提示读卡成功
否
该步骤结论为“不合格”
是
该步骤结论为“合格”
S23
设置为正式密钥，插入正确的开户卡
提示读卡成功
否
该步骤结论为“不合格”
是
该步骤结论为“合格”
S24
以上均“合格”?
否
本地认证功能“不合格”
是
本地认证功能“合格”

图2

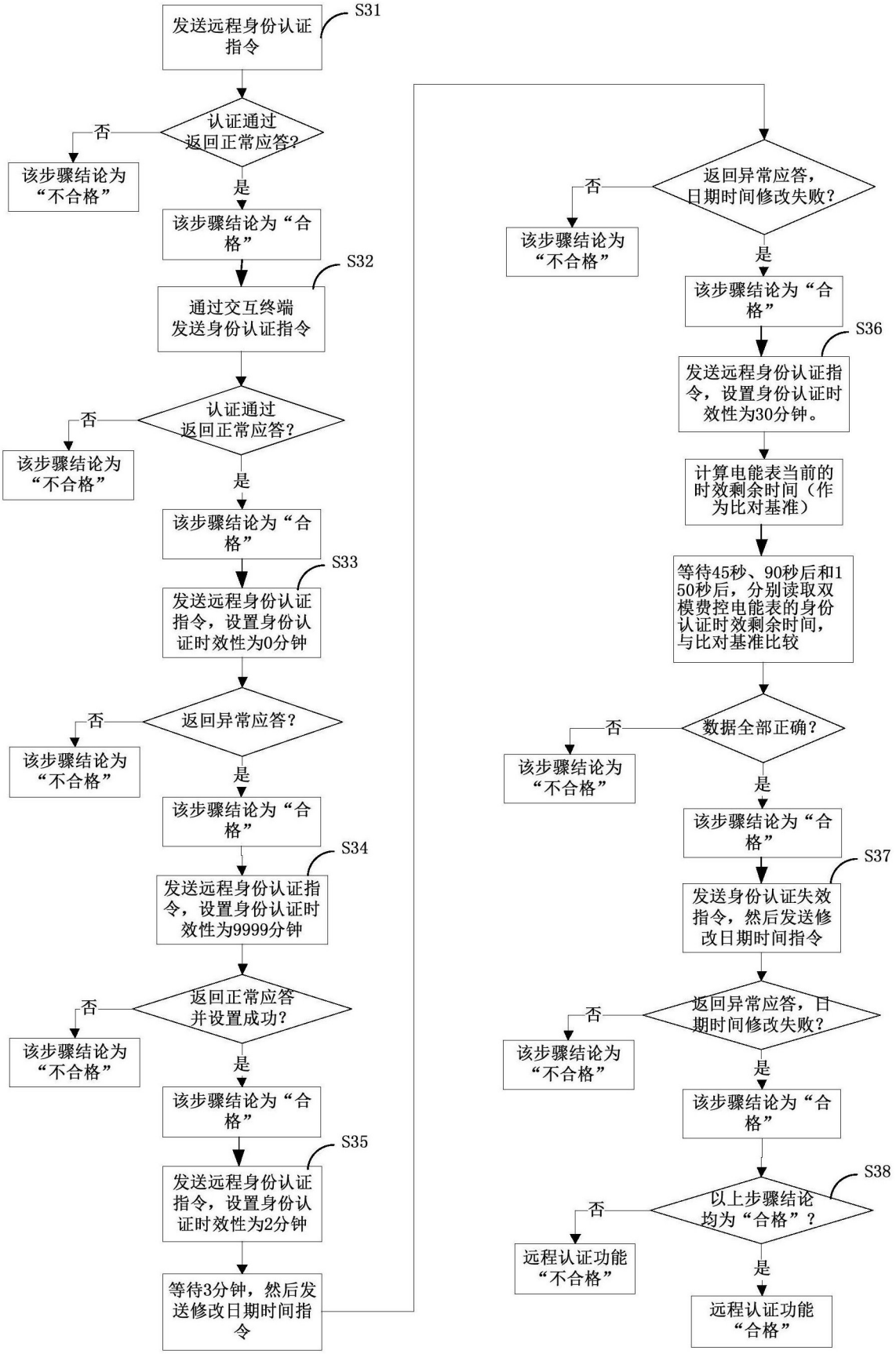

发送远程身份认证指令
S31
认证通过返回正常应答?
否
该步骤结论为“不合格”
是
该步骤结论为“合格”
通过交互终端发送身份认证指令
S32
认证通过返回正常应答?
否
该步骤结论为“不合格”
是
该步骤结论为“合格”
发送远程身份认证指令，设置身份认证时效性为0分钟
S33
返回异常应答?
否
该步骤结论为“不合格”
是
该步骤结论为“合格”
发送远程身份认证指令，设置身份认证时效性为9999分钟
S34
返回正常应答并设置成功?
否
该步骤结论为“不合格”
是
该步骤结论为“合格”
发送远程身份认证指令，设置身份认证时效性为2分钟
S35
等待3分钟，然后发送修改日期时间指令
返回异常应答，日期时间修改失败?
否
该步骤结论为“不合格”
是
该步骤结论为“合格”
发送远程身份认证指令，设置身份认证时效性为30分钟。
S36
计算电能表当前的时效剩余时间（作为比对基准）
等待45秒、90秒后和150秒后，分别读取双模费控电能表的身份认证时效剩余时间，与比对基准比较
数据全部正确?
否
该步骤结论为“不合格”
是
该步骤结论为“合格”
发送身份认证失效指令，然后发送修改日期时间指令
S37
返回异常应答，日期时间修改失败?
否
该步骤结论为“不合格”
是
该步骤结论为“合格”
以上步骤结论均为“合格”?
S38
否
远程认证功能“不合格”
是
远程认证功能“合格”

图3

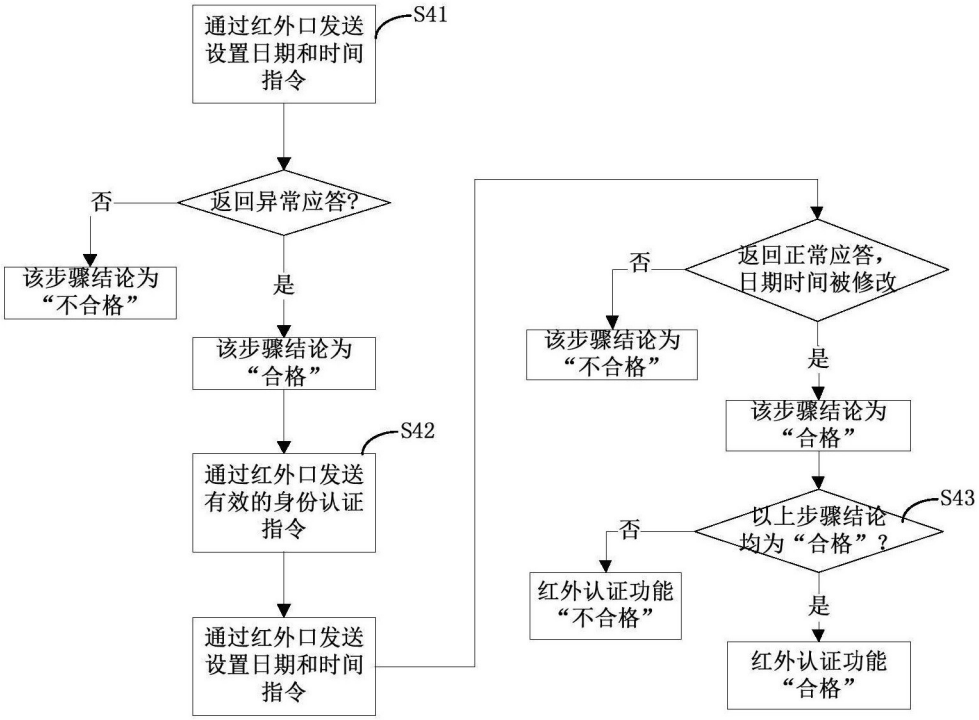

通过红外口发送设置日期和时间指令
S41
返回异常应答?
否
该步骤结论为“不合格”
是
该步骤结论为“合格”
S42
通过红外口发送有效的身份认证指令
通过红外口发送设置日期和时间指令
返回正常应答，日期时间被修改
否
该步骤结论为“不合格”
是
该步骤结论为“合格”
S43
以上步骤结论均为“合格”？
否
红外认证功能“不合格”
是
红外认证功能“合格”

图4

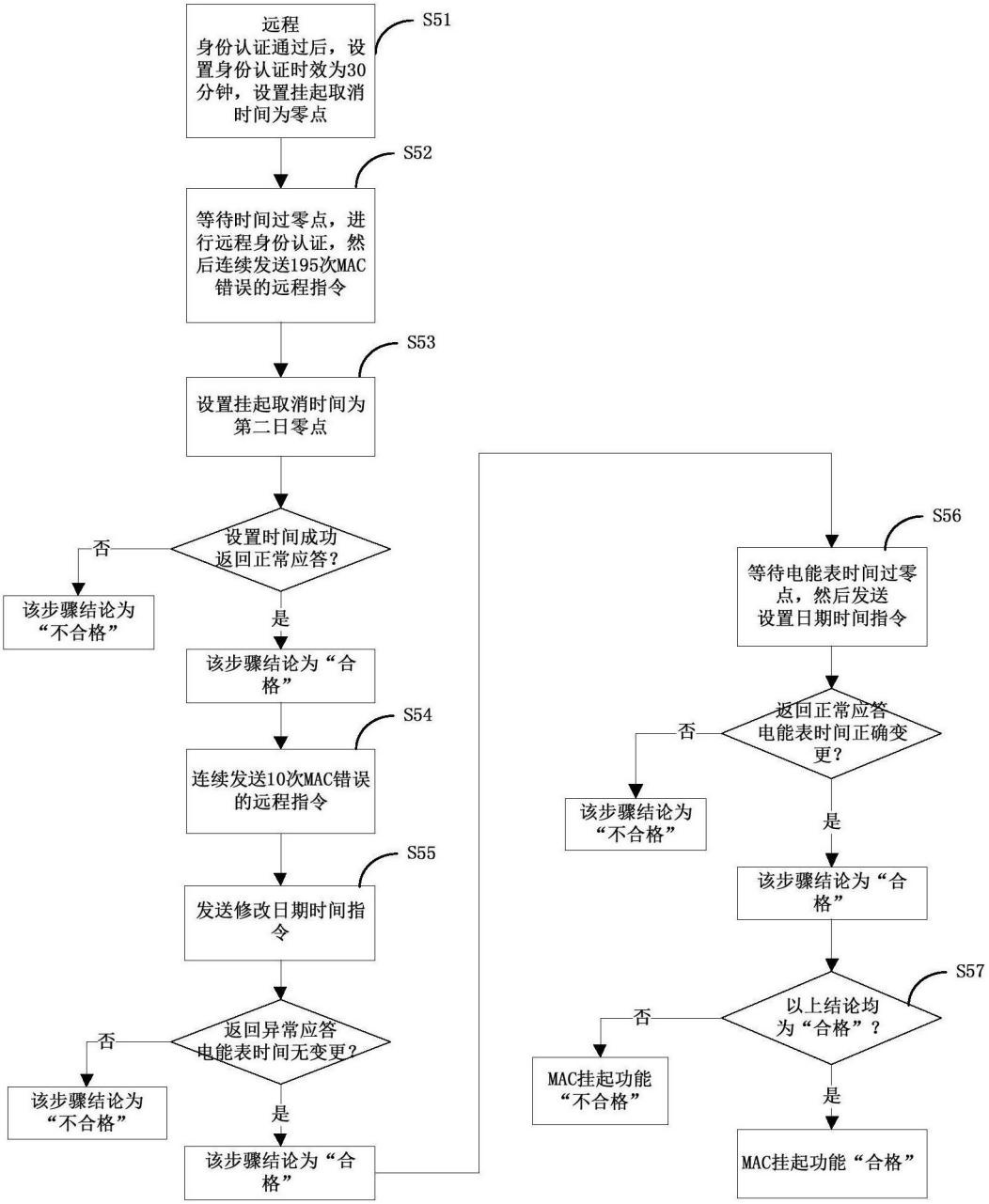

远程
身份认证通过后，设置身份认证时效为30分钟，设置挂起取消时间为零点
S51
等待时间过零点，进行远程身份认证，然后连续发送195次MAC错误的远程指令
S52
设置挂起取消时间为第二日零点
S53
设置时间成功返回正常应答？
否
该步骤结论为“不合格”
是
该步骤结论为“合格”
连续发送10次MAC错误的远程指令
S54
发送修改日期时间指令
S55
返回异常应答电能表时间无变更？
否
该步骤结论为“不合格”
是
该步骤结论为“合格”
等待电能表时间过零点，然后发送设置日期时间指令
S56
返回正常应答电能表时间正确变更？
否
该步骤结论为“不合格”
是
该步骤结论为“合格”
以上结论均为“合格”？
S57
否
MAC挂起功能“不合格”
是
MAC挂起功能“合格”

图5

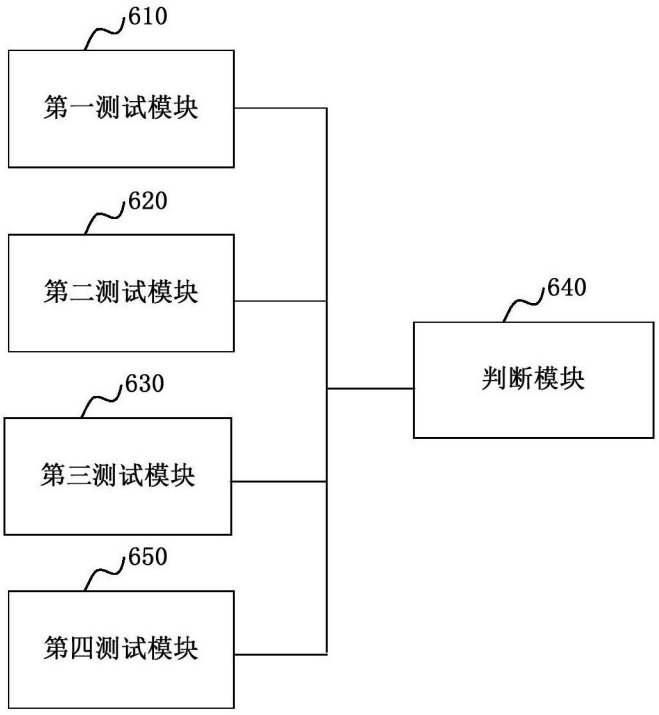


图6