

文章编号: 1674—8247(2023)03—0060—05

DOI: 10. 12098/j. issn. 1674 - 8247. 2023. 03. 012

智能开闭器系统的设计与实现

吴小健¹ 罗竣铭² 刘理想³ 喻胜利³ 李磊³

(1. 广西南崇铁路有限责任公司, 广西 崇左 532200;

2. 北京华弘集成电路设计有限责任公司, 北京 100190;

3. 北京思普勒科技有限公司, 北京 101599)

摘 要: 基于铁路供电、信号等专业关键设备开闭管理流程与需求, 分析了智能开闭器系统的功能, 介绍了开闭器系统设计原理及具体实现。将开闭器、蓝牙钥匙通过云端控制系统与 APP 形成一套安全智能开闭器物联网管理系统, 经过高速铁路线路实际应用, 有效实现关键设备开启操作的分级授权、开闭信息可追溯等问题, 形成一套操作便捷、安全稳定、管理闭环的设备闭锁系统。该系统经过适当的调整, 可以应用于能源、冶炼、供水、供气系统关键设备管理。

关键词: 开闭器; 闭锁系统; 物联网; 分级授权; 可追溯

中图分类号: TM7

文献标识码: A

Design and Implementation of an Intelligent Switch Circuit Controller System

WU Xiaojian¹ LUO Junming² LIU Lixiang³ YU Shengli³ LI Lei³

(1. Guangxi Nanchong Railway Co., Ltd., Chongzuo 532200, China;

2. Beijing Huahong IC Design Co., Ltd., Beijing 100190, China;

3. Beijing Sipule Technology Co., Ltd., Beijing 101599, China)

Abstract: Based on the switching management process and requirements of critical equipment in railway power supply, signaling, and other disciplines, this paper analyzed the functions of the intelligent switch circuit controller system, and introduced the design principle and specific implementation of a switch circuit controller system in detail. Through the cloud control system and app, an Internet of Things management system for the safe and intelligent switch circuit controller was formed. After practical application on high-speed railway lines, functions such as hierarchical authorization of key equipment opening operations and traceability of opening and closing information are effectively realized, forming an equipment locking system with convenient operation, safety and stability, and a closed management loop. After proper adjustment, the system can be applied to the critical equipment management of energy, smelting, water supply, and gas supply systems.

Key words: switch circuit controller; locking system; Internet of Things; hierarchical authorization; traceability

收稿日期: 2023-05-27

作者简介: 吴小健(1991-), 男, 工程师。

引文格式: 吴小健, 罗竣铭, 刘理想, 等. 智能开闭器系统的设计与实现[J]. 高速铁路技术, 2023, 14(3): 60-64.

WU Xiaojian, LUO Junming, LIU Lixiang, et al. Design and Implementation of an Intelligent Switch Circuit Controller System [J]. High Speed Railway Technology, 2023, 14(3): 60-64.

铁路系统中存在电力供应、通信信号、运行调度等环节众多关键设备,使用锁具闭锁设备门和手动操作机构是一种普遍采用的设备闭锁方法,是防范事故风险不可或缺的安全措施。这也就意味着,在日常检修、巡视及倒闸操作过程中要进行大量的开锁、闭锁操作。由于设备锁具操作具有工作量大、重要性高的特点,并且与铁路电力生产的诸多环节密切相关。因此,应用物联网、自动控制技术^[1],不断优化设备闭锁方案、加强设备操作管理,对确保安全生产、提高工作效率、减轻运行人员工作强度具有重要意义。

1 现状

几十年来,经过了几代技术的发展变迁,电气防误操作系统已基本成熟,为防止电气误操作事故起到了关键作用。闭锁对象是设备的箱/柜门(如:保护柜门、监控柜门等)、重要区域出入通道门(如:高压室门、通讯机房门)、构架爬梯及部分手动操作机构等。普通锁具不能形成完整的闭锁系统,普遍存在以下问题:

(1) 存在安全隐患

闭锁锁具大部分由设备自带,基本上是 1 种设备 1 种锁。现有的操作管理方法是通过控制钥匙实现对锁具操作的控制。通常,1 把钥匙开 1 把锁或 1 种钥匙开 1 种锁。由于锁具种类繁多,质量良莠不齐(易生锈、失效),所以经常给操作带来不便。现场调查发现,相当一部分锁具处于损坏或非闭锁状态;还

有一部分应闭锁的设备没有任何闭锁,其中构架爬梯所占比例最大。同时存在走错间隔、错误开启带电设备、外单位施工人员误动设备等现象,均会造成人员和设备损毁事故。

(2) 工作效率低

由于需要闭锁的设备门和出入通道门众多、锁具种类繁多,运行人员进行设备操作或设备巡视时需携带多串钥匙,加之对应开启、设备锈蚀等问题,造成工作效率低下。

(3) 无法分级分区管控

传统管理方式是通过控制钥匙实现对锁具操作的控制。这种方式存在管理繁琐,无法进行细致、高效的权限划分,操作没有相应的记录等诸多问题。一旦发生安全问题很难进行深入调查,无法尽快消除隐患。

针对上述问题,本文应用物联网、自动控制等技术,在既安全又高效的原则下,研究设计 1 种具备分时、分区控制,开闭记录可追溯的专用智能开闭器系统^[2],有从而实现有效闭锁,简化操作流程,提高工作效率。

2 系统设计及实现

2.1 方案设计

为提升现有电气防误操作水平,提出智能安全联锁设计方案,如图 1 所示。

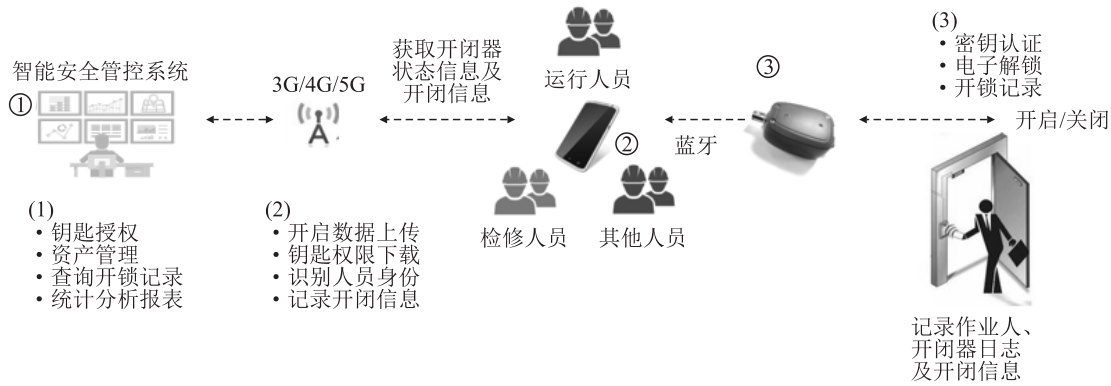


图 1 智能安全联锁设计方案图

作业人员利用无线公网或专网方式与管控系统通过作业终端进行交互,作业终端与智能钥匙通过蓝牙通讯。将人员、组织架构以及关键电力设备通道门、箱柜门等基础档案信息录入系统,智能开闭器及钥匙配置后,作业人员通过作业终端进行钥匙授权,在规定的时

间、区间内进行安全闭锁操作,开闭时间可追

2.2 系统构成

系统由云平台(含 APP)、蓝牙钥匙和智能开闭器组成,各组成部分之间通过私有协议,在认证协商、国密算法加解密的基础上实现互联通讯,共同实现设备远程授权开启、分区域分时间开闭、操作记录追溯等

功能。系统框架如图 2 所示。

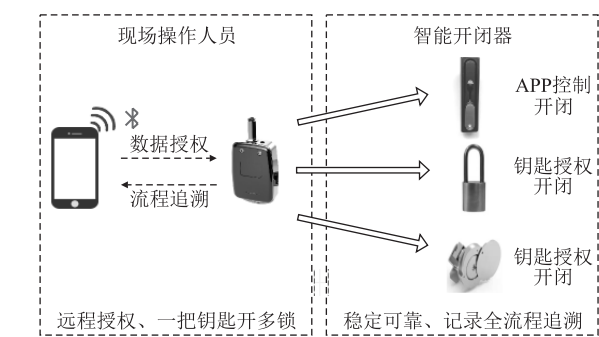


图 2 系统框架图

2.3 功能设计

2.3.1 云平台

云平台是开闭器、蓝牙钥匙操作,以及业务流程控制的大脑,管理人员通过云平台与 APP 完成设备管理、用户管理、系统管理、统计分析等功能。平台主要功能模块设计如图 3 所示。

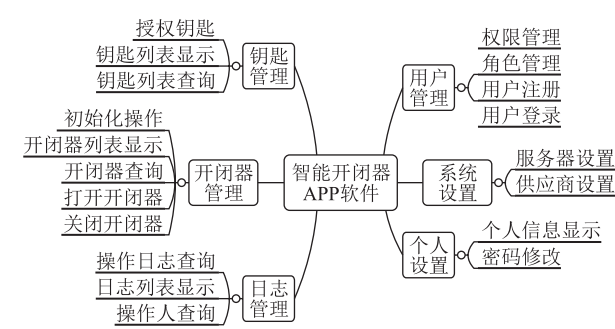


图 3 软件功能模块图

(1) 用户管理

用户管理模块通过角色、权限管理,实现 10 级以内流程权限管理。通过创建不同的角色并分配不同的系统功能权限,满足实际闭锁管理中分级、分角色授权管理需求。系统支持界面化拖拽及外部数据导入方式进行维护设定。

(2) 系统设置

系统设置主要包括云平台服务器地址端口及供应商设置、账号有效期、系统语言等设置。

(3) 个人设置

设置用户名、姓名、手机号码、密码等个人信息。

(4) 钥匙管理

按权限显示用户管理的钥匙信息列表,每条钥匙信息包括钥匙名称、蓝牙名称等信息。同时对钥匙控制的开闭器进行授权操作等功能^[3],确保开闭器操作的全程追溯。钥匙一旦分发给工作人员、无法有效监

控其使用钥匙的时间、地点信息,也无法实时查证工作人员在远程工作区域停留的信息。

(5) 开闭器管理

添加并显示开闭器名称、编号、状态、安装位置、类型,初始化开闭器,控制开闭器的开闭等功能。云平台可通过上传数据监控各个智能开闭器,实时远程监控所有开闭器是否已经闭合。系统功能实现界面如图 4 所示。



图 4 开闭器管理界面图

(6) 全流程追溯管理

开闭智能开闭器全流程操作以列表形式显示,列表显示开闭器名称、操作时间、操作类型、操作结果、操作人员、授权情况等信息,按作业人员、设备可统计作业时间,形成设备开闭闭环管理,如图 5 所示。



图 5 全流程追溯管理界面图

2.3.2 钥匙主要功能

与传统机械锁的“通用钥匙”相比,本文中的钥匙为“万能钥匙”,通过密钥认证、分级授权、流程追溯等机制^[4],保证智能开闭器和钥匙的使用更加安全、便捷。紧急情况时,工作人员可申请管辖范围以外设

备的开闭权限,满足应急抢修、复用检修班组等实际需求。

主要操作流程如下:

(1) 搜索蓝牙钥匙

打开钥匙,点击 APP 右上角的蓝牙标志,对钥匙进行蓝牙搜索,APP 进行钥匙连接。

(2) 注册钥匙, 钥匙授权

点击需连接的钥匙,如钥匙未注册,则弹出是否注册界面。注册后进行钥匙授权操作。

(3) 钥匙操作开闭器

点击 APP 右上角的蓝牙图标,蓝牙搜索智能开闭器的钥匙。钥匙首先处于打开状态,然后插入开闭器中,点击需连接的钥匙。点击该智能开闭器,然后弹出该智能开闭器的界面,点击“开闭器开关”即可打开智能开闭器。

2.3.3 开闭器主要功能

(1) 设备开启

正常开锁,当手机 APP 应用软件下发的指令通过密钥认证后,安全主控 MCU 控制电机旋转^[5],智能开闭器打开,并形成追溯日志。应急开锁,通过安全认证并授权后的钥匙直接控制电机开锁。

(2) 设备关闭

直接手动关闭开闭器,开闭器生成闭锁追溯日志同步到 APP 中,支持蓝牙通讯,确保在无信号的情况下正常闭合开闭器。手动无法关锁时,需连接手机 APP 与智能开闭器,下发关闭指令后,再次手动关闭。多种开闭操作即保障了安全性,也确保了智能开闭器高可用性的特点。

(3) 追溯信息存储

滚动存储 500 条开闭操作记录,解决了交叉管理、责任不清,信息化缺失等问题,实现了钥匙分发,提供全流程追溯信息。

2.4 系统实现

2.4.1 硬件实现

硬件电路设计利用高性能处理器作为智能开闭器的核心控制器件,负责系统传输数据的加密、解密、协议解析、协议组建、数据信息存储、驱动结构的驱动控制、通信数据的转换等,本文通过软件方式实现传输数据的加密和解密。智能开闭器中处理器的软件,将关键信息存入存储器中,对通过接口进入到处理器中的数据进行解密处理,并进行协议解析分析判断数据正确性,尽而完成相应的动作和处理;对通过蓝牙接口发送的数据进行加密处理,并将数据进行协议组帧,尽而将数据帧发送;处理器根据接收到的数据解

析完成后根据需要发送驱动指令和驱动控制,来完成电机的运作及内部结构的驱动,开闭器主要参数如表 1 所示。

表 1 智能开闭器主要参数指标表

序号	项目	描述	备注
1	主材质	304 不锈钢	
2	待机开闭次数/次	50 000	
3	防水等级	IP68	可浸泡在水中开锁
4	追溯信息/条	500	循环存储
5	工作环境	-40 ℃ ~ 80 ℃ 20% ~ 98% 湿度	

综合考虑运算处理性能与运行和待机低功耗的应用需求^[6],本文采用低功耗 STM8 系列芯片。16 Mhz 主频、1 KB RAM 可满足设备开闭控制、通信及数据加解密模块毫秒级动作响应;2.95 ~ 5.5 V 工作电压、238 mW 超低功耗,满足蓝牙钥匙一次充电 15 d 以上常规巡检开闭设备的需求,硬件结构如图 8 所示。

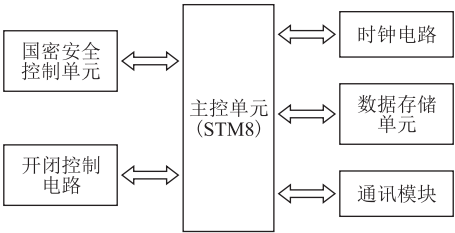


图 8 开闭器硬件结构图

2.4.2 控制协议实现

(1) 通讯协议

原始数据传输格式如表 2 所示。

表 2 原始数据传输格式表

<i>S</i>	<i>T</i>	<i>L</i>		<i>V</i>	<i>C</i>
同步字	指令字	data	data	数据内容	校验位
2 字节	1 字节	2 字节		长度为 length	2 字节

(2) 协议内容:

安全协商协议 4 条;

初始化协议 2 条;

数据安全通信协议 10 多条。

其中数据安全通信协议涵盖开闭器安全开闭操作 2 种方式、开闭器信息设置及读取等,日志读取等。

(3) 安全实现

采用非对称国密 SM 系列安全加密算法^[7],对系统间数据进行加解密,实现开闭器操作的安全保障。具体设计为通过 2 段 32 位以内任意长度的口令,生

成128位根密钥;钥匙、开闭器出厂时下装根密钥;设备侧数据发送前,获取设备IMEI值,参与加密计算;云平台(APP)软件侧在时间戳有效期(默认5 min、可调)内进行验证、解密。通过该算法及流程设计,实现“一设备一密钥”,降低破解风险,提高系统通信安全性。

2.5 应急措施

系统设置了高权限应急授权的软件功能与超级物理钥匙。系统管理员以及应急管理员角色,可对任何智能钥匙进行应急授权,被授权为应急模式的智能钥匙,可开启本辖区内所有开闭器,开闭操作上传至系统及应急管理员;超级物理钥匙以班组为单位,提前进行授权的物理钥匙,可开启本辖区所有开闭器。

2.6 外部接口

系统支持综合自动化系统、作业管理等系统对接,通过工单、工况信息交互共享,实现智能闭锁管理。根据安全、延迟等需求,本系统采用API方式提供外部交互接口,基于HTTP协议,支持签名(sign)、系统调用凭证(token)安全交互方式,防止信息泄露与篡改。API包括开闭器档案信息、开闭时间、作业人员档案信息、授权信息获取,以及作业人员、开闭时间等授权设置接口。

3 应用

本系统在云南、山东铁路公司某供电段进行了试点应用,据现场反馈,主要成效为:“一把智能钥匙走天下”,只需远程授权,即可开启不同开闭器;开闭器采用无孔设计、数字加密技术,安全可靠;云平台、APP操作管理便捷,无源设计、无需布线,无需管理多种量大机械钥匙、高效快捷;管理人员可通过追溯功能监测工人员状态、工作时长,考核有据。

4 结束语

本文将开闭器、蓝牙钥匙通过云端控制系统与APP形成一套安全智能开闭器物联管理系统,经过系统实现与现场试用,本系统达到了设计目标,实现了关键设备闭锁的闭环管理,节省了人力物力、提高了设备运行安全。下一步,将结合铁路检修作业延期/

超时主动预警、作业环境监控预警等需求,继续开展低功耗有源开闭器,温湿度、流量等传感器物联监测,智能预警策略相关研究。

参考文献

- [1] 谢毅,肖杰. 高速铁路发展现状及趋势研究[J]. 高速铁路技术, 2021, 12(2): 23-26.
XIE Yi, XIAO Jie. Research on Development Status and Trend of High-speed Railway [J]. High Speed Railway Technology, 2021, 12(2): 23-26.
- [2] 赵洋洋,王勃,于洋. 智能牵引变电所五防系统设计[J]. 电气化铁道, 2018, 29(5): 11-15.
ZHAO Yangyang, WANG Ren, YU Yang. Design of Five Prevention Systems for Intelligent Traction Substation [J]. Electric Railway, 2018, 29(5): 11-15.
- [3] 齐永虎,汪娜娜,王帆,等. 基于物联网的智能锁群管理系统[J]. 中国科技信息, 2020(20): 65-66.
QI Yonghu, WANG Nana, WANG Fan, et al. Intelligent Lock Group Management System Based on Internet of Things [J]. China Science and Technology Information, 2020(20): 65-66.
- [4] 闵雄,赵力. 基于NFC无源供电技术的防误锁具设计及应用[J]. 机电工程技术, 2022, 51(8): 236-238, 249.
MIN Xiong, ZHAO Li. Design and Application of Error Proof Lock Based on NFC Passive Power Supply Technology [J]. Mechanical & Electrical Engineering Technology, 2022, 51(8): 236-238, 249.
- [5] 陈志明,李澄,程华明,等. 基于RFID技术的智能安防闭锁系统的设计与实现[J]. 计算机测量与控制, 2020, 28(11): 182-186.
CHEN Zhiming, LI Cheng, CHENG Huaming, et al. Design and Implementation of Intelligent Security Locking System Based on RFID Technology [J]. Computer Measurement & Control, 2020, 28(11): 182-186.
- [6] 张震,陈冠彪,樊荣,等. 基于STM32的高压开关柜带电告警及闭锁系统[J]. 山东电力技术, 2018, 45(2): 52-57.
ZHANG Zhen, CHEN Guanbiao, FAN Rong, et al. Live Alarm and Locking System of High Voltage Switchgear Based on STM32 [J]. Shandong Electric Power, 2018, 45(2): 52-57.
- [7] 陈荣茂,王毅,黄欣沂. 国密SM2加密算法的RCCA安全设计[J]. 中国科学(信息科学), 2023, 53(2): 266-281.
CHEN Rongmao, WANG Yi, HUANG Xinyi. RCCA Security Design of State Secret SM2 Encryption Algorithm [J]. Scientia Sinica (Informationis), 2023, 53(2): 266-281.