

通信安全解决方案

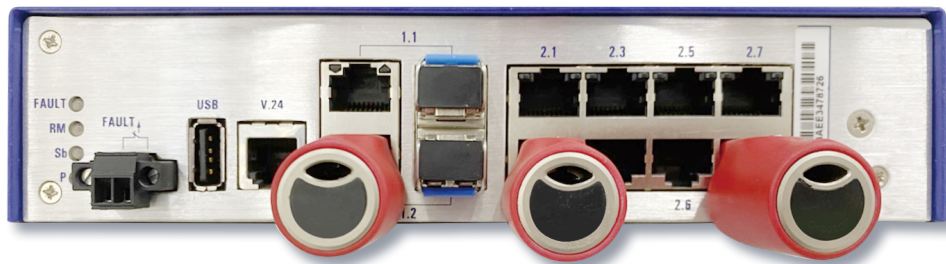
通信接口无管理

纸质记录不清晰

设备操作无记录

开锁信息难追溯

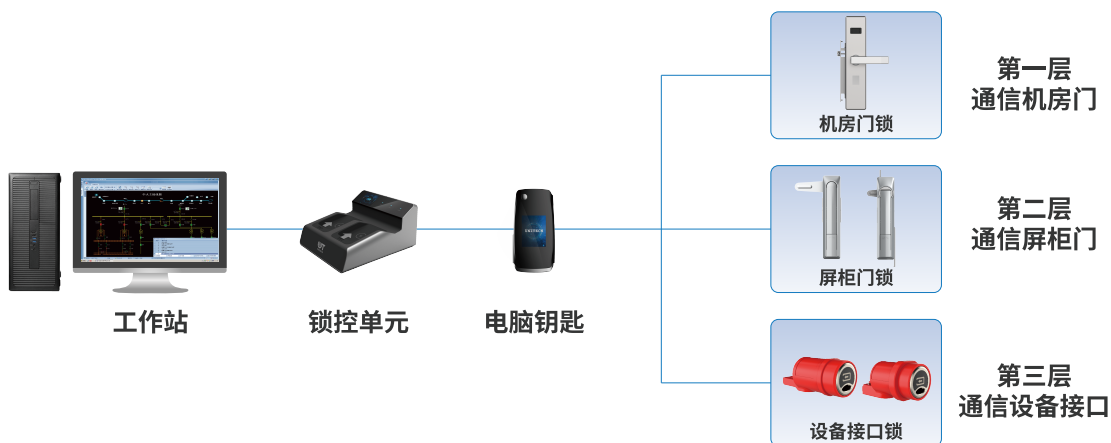
优特科技通信安全管理方案帮您解决问题!



优特科技通信安全管理方案致力于解决通信机房人员进出管理,及机柜内设备通信接口使用信息的无序管理问题。采用机房门锁——屏柜门锁——通信设备接口锁的三层管理结构,全方位增强网络信息安全,提高工作效率。

系统组成

SYSTEM COMPOSITION



• 工作站

用于存贮所有机房锁具信息以及开锁人员信息、管理人员设备权限、生成开锁序列,并发送给锁控单元。同时保存开锁记录,便于浏览和查询。

• 锁控单元

用于和工作站通信,将开锁序列信息传输给电脑钥匙。

• 电脑钥匙

用于读取锁具唯一标识码、开启授权范围内的锁具、自动记录开锁信息的智能化手持设备。

• 锁具

具有统一锁芯结构、唯一标识码。分别对机房门、屏柜门、设备接口进行闭锁。



操作授权

系统具备“临时授权”、“固定授权”功能，经过授权的手持终端才能打开锁具，无授权无法操作，以确保锁具操作的可控性、灵活性。



设备台账管理

锁具的相关信息储存于管理系统中，包括了锁具数量、锁具名称、锁具位置等内容，用图形的方式直接显示在软件界面上，可根据使用习惯自由分类，方便操作管理。



锁具状态采集

电脑钥匙操作时自动记录锁具的开关结果，并可传送到管理系统中。



身份识别

电脑钥匙内存储人员身份信息和锁码信息，可自动识别人员授权范围。



人员权限管理

根据工作人员的职责，系统赋予不同的角色，不同角色的操作权限不同。



分级分区

具备分级分区管理功能，不同区域可设置不同的防护权限。



记录保存与查询

所有的操作记录都自动保存到工作站上，包括操作人、操作时间、被操作设备等信息，可按不同字段进行查询。



锁具安全性高

防技术开启等级达到行业内最高安全等级C级，绑定ID信息，采用国密算法，信息交互安全。锁具本体安全性高，可抗暴力破坏。



一钥多开

一把电脑钥匙可以打开通信机房所有锁具。

应用示例

APPLICATION EXAMPLES



机房房门闭锁案例



服务器屏柜闭锁案例



网络接口闭锁案例



USB接口闭锁案例

工程案例

● 国网安徽蚌埠500kV清流变电站

● 国网浙江金华110kV义门变电站

