Website: ycyk.brit.com.cn　Email: ycyk704@163.com

基于 APP 的卫星地面遥控系统安全性设计

刘　鹏，李　成，刘　超，邵　坤，师　帅
（北京空间飞行器总体设计部　北京　100094）

摘要：目前，我国绝大部分卫星的遥控指令上行操作必须在专用测控网内进行，当卫星发生在轨异常时，相关支持人员必须赶赴测控中心现场进行集中处置，非工作时段时效性较低，不利于紧急情况下的异常快速处置。对基于 APP 的卫星地面遥控系统安全应用方案进行了研究和设计，旨在为我国未来卫星高效运行管理提供一种新的手段，通过原型系统的仿真测试，验证了系统的技术可行性，实现卫星管理相关人员在远离测控中心的情况下也能安全有效地参与在轨异常应急处置。

关键词：APP；卫星；遥控；风控
中图分类号：TP311　　**文献标识码：**A　　**文章编号：**CN11-1780(2022)01-0074-08
DOI：10.12347/j.ycyk.20210604001
引用格式：刘鹏，李成，刘超，等. 基于 APP 的卫星地面遥控系统安全性设计[J]. 遥测遥控, 2022, 43(1): 74–81.

Safety design of ground telecommand system for satellites based on mobile Apps

LIU Peng,　LI Cheng,　LIU Chao,　SHAO Kun,　SHI Shuai
（Beijing Institute of Spacecraft System Engineering, Beijing 100094, China）

Abstract: At present, the telecommand operation of most satellites in our country must be carried out in the dedicated network, when the satellite is abnormal in orbit, relevant personnel must rush to the task center for centralized disposal, which leads to the problem of low timeliness. This article proposes a safety design scheme of ground telecommand system for satellites based on mobile Apps, which is aimed to provide a new method for the efficient operation and management of satellites in the future. Through the test of prototype system, it is verified that the spacecraft management experts can access to the back-end platform and dispose the abnormity through the mobile terminal in a reliable way while being far away from the task center.

Key words: APP; Satellite; Telecommand; Risk control
DOI：10.12347/j.ycyk.20210604001
Citation: LIU Peng, LI Cheng, LIU Chao, et al. Safety design of ground telecommand system for satellites based on mobile apps[J]. Journal of Telemetry, Tracking and Command, 2022, 43(1): 74–81.

引　言

目前，我国绝大部分卫星的遥控指令上行操作必须在专用测控网内进行，操作人员在测控中心编制好遥控指令序列后，由地面加解密设备完成遥控指令的加解密处理[1,2]，通过地面测控网发送至测控站后上行至卫星。因此，当卫星发生在轨异常时，相关支持人员必须赶赴测控中心现场进行集中处置，非工作时段时效性较低，不利于紧急情况下的异常快速处置。而在无人机、电力系统等其他领域，采用移动终端 APP 进行远程遥控操作的应用已较为成熟[3-5]，在确保安全可靠的情况下可有效提高工作效率。

基于上述背景，本文对基于 APP 的卫星地面遥控系统安全应用方案进行了研究和设计，旨在为我国未来航天器高效运行管理提供一种新的手段，实现卫星管理相关人员在远离测控中心的情况下也能有效参与在轨异常应急处置，提高任务快速响应能力和故障处理成效。

收稿日期：2021-06-04　收修改稿日期：2021-06-20

1　系统架构设计

利用普通智能移动终端在公共互联网络上实现遥控指令的安全操作，采用加密传输机制只是最基本的保障。本系统在对移动终端植入安全芯片实现与后端中心系统之间安全认证和加密交互的基础上，结合实际业务需求引入遥控指令二次审批机制，同时参考人工智能在互联网金融风控领域的应用技术路线进行了多维智能风控策略设计。整个系统的逻辑架构如图 1 所示，主要由以下几部分构成。

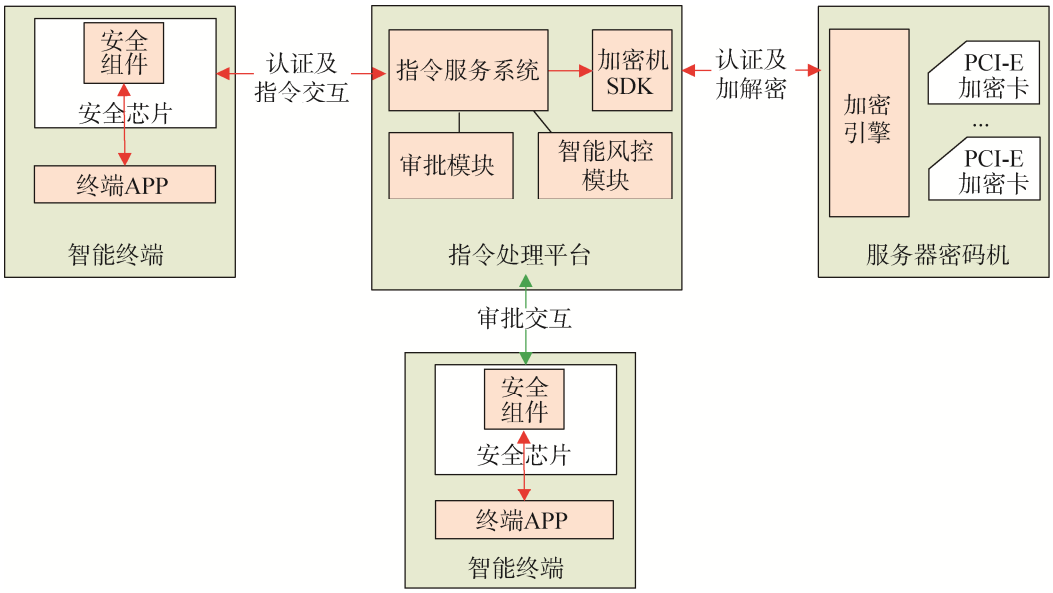

图 1　系统逻辑结构图

Fig. 1　System logical structure

① 安全芯片：自主研发、集成国密算法的独立安全运算单元，可为移动终端系统和应用提供签名/验签、数据加/解密、密钥安全管理等基础安全服务。一般通过在 SIM 卡上贴膜卡或插入 TF 卡的方式为普通智能移动终端植入安全芯片。

② 安全组件：基于安全芯片内部运算资源，将一部分核心指令逻辑直接在安全芯片内部实现，以完成特殊功能操作的软件模块。由于直接在安全芯片内部执行和运算，与终端操作系统和业务软件完全隔离，可以防止终端系统环境不可控对核心指令安全性产生影响。

③ 指令服务系统：用于处理从终端发送过来的指令请求的服务系统，在对指令数据处理前，需要通过调用服务器密码机对应的 SDK 对加密指令数据进行解密、解析、校验，确认数据完整、安全、可信后再进行后续处理。

④ 审批模块：调度不同智能终端协同完成遥控指令的远程二次审批流程。

⑤ 智能风控模块：结合卫星遥控场景的特点和在轨大数据，对指令操作的身份、行为、人物关系、适用场景和在轨状态等多个维度进行实时风险检测和控制，降低风险。

⑥ 服务器密码机：具有数据加解密、签名、验签、MAC、杂凑等功能，内置一个或多个 PCI-E 密码卡，基于 SM1/SM2/SM3/SM4 等国密算法通过光纤或网口对外提供高速密码服务。

⑦ 加密机 SDK：服务器密码机提供的开发服务包，支持安全设备或应用系统方便、快捷的调用服务器加密机实现签名认证、密文指令数据的加/解密等。

2　指令加解密传输设计

系统通过安全芯片实现智能终端 APP 到后端系统之间端到端的通信加密，保证指令数据在传输过程中的机密性和完整性。遥控指令加解密传输流程主要分为设备认证及会话密钥交换、遥控指令传输处理两个阶段，具体流程如图 2 所示。

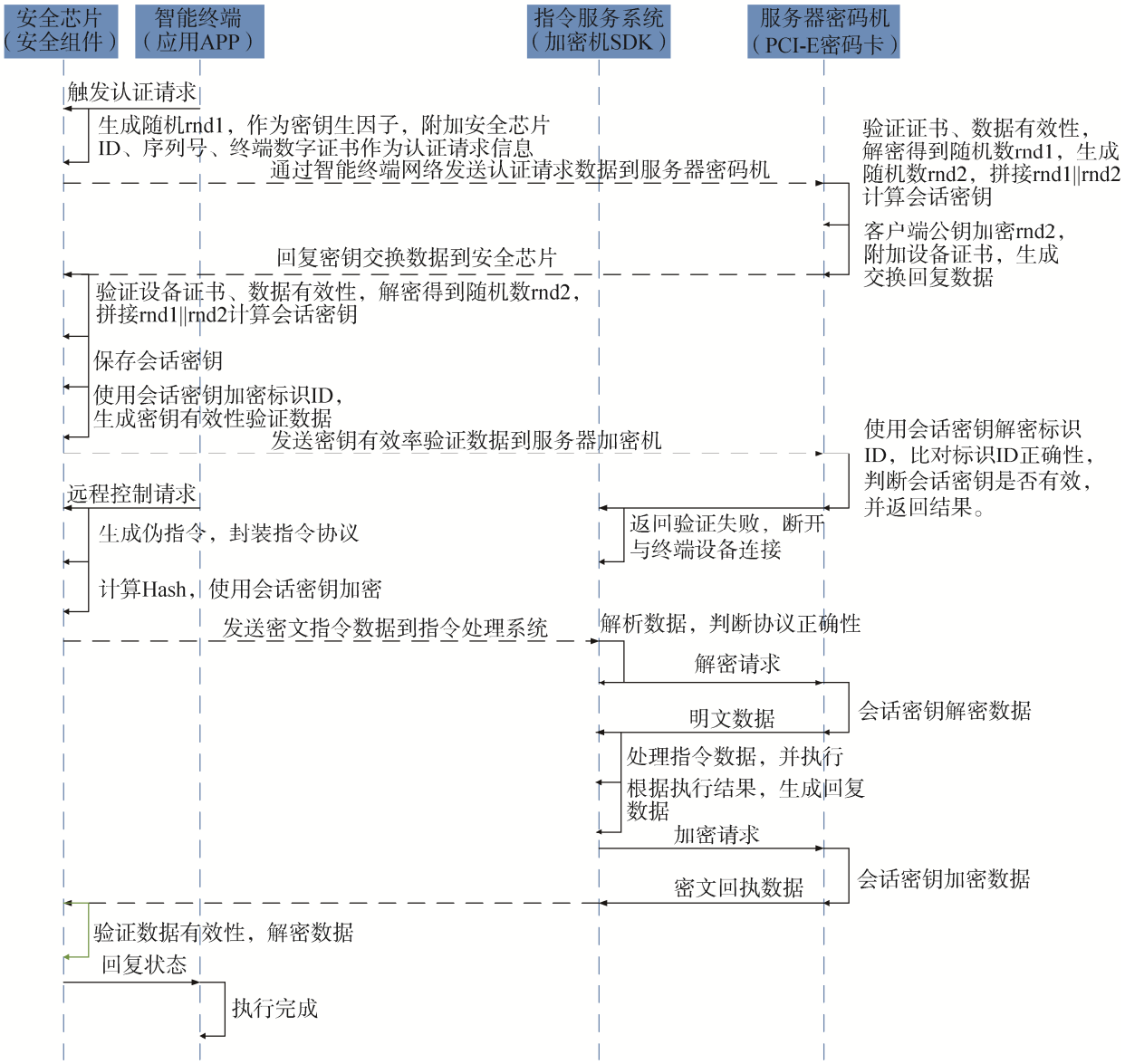

图 2　指令加密传输流程

Fig. 2　Encryption and transmission process of telecommand

2.1　设备认证及会话密钥交换

为确保只有持合法身份的设备才能接入后端系统进行操作，防止非法设备/用户接入。首先需要进行终端设备认证及会话密钥交换，具体流程如下：

① 应用 APP 通过终端设备集成安全芯片驱动，向安全芯片内部安全组件发送认证及会话密钥交换请求。

② 安全芯片内部安全组件收到请求，调用安全芯片随机数发生器生成随机数据 rnd1，并读取芯片 ID，生成序列号 sno1，读取终端设备数字证书，组合成认证请求信息，通过应用 APP 代理转发给指令服务系统。

③ 指令服务系统收到后，根据请求数据协议标识转交给服务器密码机处理。服务器密码机解析请求数据，验证数据协议及客户端证书有效性，取出随机数 rnd1，调用 PCI-E 密码卡生成随机数 rnd2，合并 rnd1 和 rnd2，调用密钥生成函数计算会话密钥。

④ 使用客户端公钥加密 rnd2，附加服务器密码机设备证书、算法标识、序列号作为认证回执信息，

通过指令服务系统转发给智能终端。

⑤ 智能终端收到回复数据后，发送给安全芯片，由安全芯片内安全组件处理。安全组件解析、验证设备数字证书完整性、有效性，并使用芯片内私钥解密 rnd2 密文信息，得到 rnd2。合并 rnd1 盒 rnd2，利用与服务器密码机同样的密钥生成函数计算会话密钥，并存储芯片内密钥文件。

⑥ 安全组件利用生成的会话密钥加密芯片 ID，加密结果作为会话密钥有效性验证数据，通过应用 APP 发送给指令服务系统。

⑦ 指令服务系统收到后根据请求标识发送给服务器密码机处理。服务器密码机通过第一步运算得到的会话密钥解密数据，将得到的明文结果与第一步拿到的芯片 ID 做比对。如果一致，表示会话密钥有效。否则表示会话密钥无效，认证过程失败，将状态反馈给指令服务系统，指令服务系统断开与智能终端的连接。

2.2 遥控指令传输处理

认证过程完成且会话密钥协商成功后，用户可以通过应用 APP 操作界面进行具体控制操作，主要流程包括：

① 安全芯片内的安全组件使用芯片内会话密钥对应用 APP 生成的指令加密，变成密文后返回给应用 APP；

② 应用 APP 将密文指令信息发送给指令服务系统处理，由指令服务系统根据业务标识将密文信息转发给服务器密码机进行解密；

③ 服务器密码机收到后请求后，根据会话信息查询对应会话密钥，并解密数据，将解密结果回复给指令服务系统；

④ 指令服务系统验证明文数据完整性，解析指令并执行；

⑤ 将执行结果通过服务器密码机加密回复给应用 APP；

⑥ 应用 APP 调用安全芯片内安全组件进行解密，得到明文回执，指令执行过程结束。

3 指令二次审批设计

为了保证指令数据完整可靠，系统进一步引入远程审批二次确认的机制。在指令执行前弹出提示窗口，要求操作人员选择需审批确认的其他人员，发送请求至对方终端；审批人员确认指令可以继续执行后，发送审批通过回复至操作人员终端；操作人员点击执行后才能继续发送指令。

指令发起、审批、验证过程中的每一步都进行了签名处理，由下一个处理过程对上一个操作的发起人身份、指令数据、发起时间等信息采用 PKI 签名验签机制进行验证，保证每一个过程发起人身份可信、数据完整有效。具体流程如下：

① 需要审批的指令由终端安全组件进行处理，在原始数据中增加时间戳和唯一序列号，然后调用安全芯片对原始数据进行 HASH 运算，生成摘要值，然后调用芯片内发起人私钥对摘要值进行签名生成签名信息并返回给终端安全组件；

② 终端安全组件拼接指令数据、时间戳、唯一序列号和签名数据，返回给应用 APP，由其发送给后端系统，通过审批模块转发给对应的审批人；

③ 审批人收到审批请求后，调用终端安全组件向服务器验证发起人身份，身份认证通过后获取发起人数字证书并解析出公钥，计算原始指令伪码（含时间戳和唯一序列号）HASH 值，并用公钥解开审批请求数据内附带的签名信息，得到发起人计算的 HASH 值，对比一致，表示数据在传输过程中完整、有效没有被非法篡改和伪造，且是由合法的用户发起，身份信息安全可信，审批人可以对请求进行审批；

④ 审批完成后，应用 APP 会将原始请求与审批动作一同交给安全组件，进行审批过程签名，同样在原始指令数据（含时间戳、唯一序列号）、附加的签名信息基础上，增加审批时间戳和审批信息后进行 HASH 运算，得到摘要数据后调用审批人终端上的安全芯片，使用其私钥对摘要信息进行签名，完成审批签名过程，并把签名数据返回给应用 APP，由其发送到后端系统进行审核；

⑤ 后端系统审批模块收到后，依次验证审批签名信息、发起请求签名信息，保证指令请求在发起过程、审批过程中人员信息安全可信、数据完整可靠，再进行指令数据审核、有效性验证，并发起执行动作，从而保证指令数据全过程安全有效、完整可控。

4　多维智能风控策略设计

目前，互联网金融领域开始利用大数据实现智能风控，通过履约记录、社交行为、行为偏好、身份信息和设备安全等多方面行为“弱特征”，填补传统基于评分卡模型和规则引擎等“强特征”风控模式的不足[6]。本系统参考该技术路线，在采用上述加密和二次审批基础上，结合卫星在轨管理业务场景的特点，进一步设计了多维智能风控策略。

4.1　强特征风控策略

在本系统中，强特征是指身份、行为、人物关系等比较明显的用户特征，即使依赖人工也可快速明确地进行识别。本系统设计了基于“人-卡-机”强关联认证、基于行为自动调整认证级别、基于人物关系图谱的风控等三种强特征风控策略。

①基于“人-卡-机”强关联认证

由于支付宝、微信等移动支付软件可以用账号密码在异地登录，与手机没有强关联绑定，用户 A 可以使用用户 B 的手机以用户 C 的账号密码进行登录，因此存在账号盗用的风险[7]。本系统采用用户特征+安全芯片/数字证书+手机硬件特征（IMEI 号）+SIM 卡唯一编号（IMSI 号）的四码强关联绑定认证，相关操作只能由符合要求的用户通过相匹配的终端完成，不存在异地登录、盗用等风险。遥控指令只能由具备相应权限且通过认证的用户和终端发出。

②基于行为自动调整认证级别

目前，终端及软件的认证方式主要包括传统认证方式，如数字证书、口令、手势等，以及基于生物特性的认证方式，如指纹、虹膜、人脸、声纹等[8]。传统的认证方式存在容易被盗、丢失或者伪造的风险，基于生物特性的认证方式则更加安全可靠。

本系统默认采用数字证书+口令或手势的方式进行认证，但当由访问低密级卫星切换为访问高密级卫星等更敏感信息情况时，系统智能风控模块会启动更高级别身份认证方式进行二次验证，如基于生物特征的指纹、人脸识别等。

③基于人物关系图谱的操作风控

在互联网金融领域，用户的人物关系图谱对于平台方来说预先是不可知的，需要基于大量的历史数据进行学习才能掌握每个用户与其他人物关系图谱。但是对于测控业务来说，以卫星为关联对象，其用户单位、测控单位及研制单位之间各相关责任人是按要求预先设定好的，人物关系图谱对于操作人员和任务中心均是事先知道的。因此，可以基于此特点设计基于人物关系图谱的操作风控。

操作人员通过移动终端执行遥控指令时，对于需要审批才能发送的指令，需要在大量随机人名中选择或直接输入正确的人员姓名进行审批。当不匹配的次数超过一定的阈值，则认为存在较高风险，系统智能风控模块暂时锁定操作，生成告警，管理员电话确认情况后方可解锁。

4.2　弱特征风控策略

在本系统中，弱特征是指指令发送的安全场景是否符合预期等不明显的特征，需要系统基于大量在轨数据进行关联分析才能准确识别。本系统设计了基于指令安全场景、基于在轨基线状态等两种弱特征的遥控操作风控策略。

①基于指令安全场景的操作风控

当航天器在轨运行在某种模式或某种环境下，某些操作是不允许进行的，否则将导致故障发生。例如：在对某通信卫星实施向南位置保持操作时，同时进行星时计数器重置，结果造成偏航姿态异常，导致卫星通信业务出现中断。其原因在于：在卫星处于位保模式并使用太阳敏感器作为偏航基准的条件下，修改了星时计数器，在这两个因素同时发生的情况下，偏航计算公式中一次补偿项时间差计算错误。又

例如：有些低轨航天器要求在侧摆时禁止注入轨道数据[9]。

因此，可以预先充分识别各卫星可能处于的各种在轨运行场景及在该场景下上行操作的影响，然后设置指令安全场景，对指令进行分组，设定各场景下不可发送的禁止指令清单。总体来说，场景至少可分为：

1）外部环境：卫星是否处于或即将进入地月影期或光照期等；

2）任务需求：卫星是否正在或即将进行轨道控制、侧摆成像等常规在轨操作任务；

3）运行状态：卫星是否处于异常报警状态或异常处置过程中；

4）测控条件：卫星是否处于可见跟踪测控范围之内。

系统在后台运行时，自动从在轨数据库中提取各个航天器的实时监测报警信息、历史相似报警信息原因分析结论、在轨遥测数据、指令发送记录、轨道数据、在轨操作事件记录、实际测控跟踪弧段时间、地月影预报、航天器基本信息、在轨异常等多元信息进行关联分析，挖掘出规律信息，识别出航天器当前应该处于的在轨运行场景。例如：系统识别出卫星当前处于地影期内，对于光照期内才能执行的指令则处于非激活状态。

当遥控指令发送至后端系统时，智能风控模块会基于已识别出的航天器当前应该处于的在轨运行场景，根据该场景相关联的禁止指令列表进行指令的发送权限检查，验证指令是否被屏蔽，防止日常操作中蓄意或误发送危险指令。

②基于在轨基线状态的操作风控

在轨基线状态是能够反映卫星上各软硬件当前在轨运行应当所处的状态，包括硬件状态、软件状态、运行模式、装订参数及其对应遥测参数的实际表征值等。需要在系统中，对航天器的在轨基线状态进行实时记录和更新维护。

当遥控指令发送至后端系统时，智能风控模块会与当前相关的单机设备或软件的在轨基线状态进行比对分析，防止出现不合理的操作。例如：当前某发射机 A 机为当班状态，B 机为常驻故障，处于关机状态，当 A 机未锁定时，正常应该发送 A 机复位或重新关开机的指令，当系统检测到当前发送的是 B 机的复位或重新关开机的指令时，则给操作人员和审批人员发送提示信息，告知不合理操作的风险。

5　系统仿真

基于上述设计实现了系统原型，在智能手机上部署了加密膜卡和 APP 软件，针对部分出口商业卫星进行了相关指令的配置，并与后端系统和卫星模拟器进行对接测试，验证了系统的技术可行性。

身份验证通过后，用户可通过 APP 软件自定义编辑指令，包括批量指令和单条指令，通过 4G 无线网络发送至后端系统，经过审批和解密后能够成功发送至卫星模拟器执行。在网络条件良好的情况下，单条指令从发出到成功执行平均消耗时间小于 5 s，效果如图 3 所示。

当指令二次审批时选取对象不匹配的次数超过一定阈值时，基于人物关系图谱的操作风控能够有效识别并锁定操作，生成告警提示，效果如图 4 所示。

图 3　指令编辑及执行效果图

Fig. 3　Telecommand editing and execution

图 4　基于人物关系图谱的操作风控效果图

Fig. 4　Operation risk control based on character relationship graph

当执行不属于当前场景的关键指令，基于指令安全场景的操作风控可有效实现拦截并告警提醒，实现效果如图 5 所示。

当遥控指令与当前相关的单机设备在轨基线状态不匹配时，基于在轨基线状态的操作风控能够有效识别，效果如图 6 所示。

图 5　基于指令安全场景的操作风控效果图

Fig. 5　Operation risk control based on telecommand security scenario

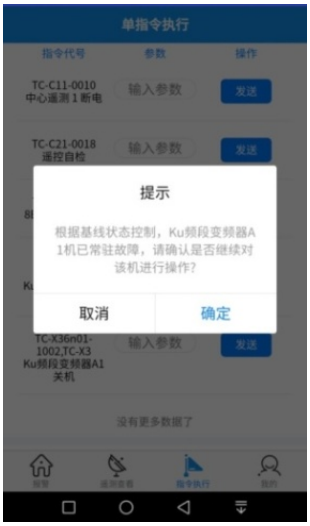

图 6　基于在轨基线状态的操作风控效果图

Fig. 6　Operation risk control based on in-orbit baseline status

6　结束语

本文对基于 APP 的卫星地面遥控系统安全应用方案进行了研究和设计，在对移动终端植入安全芯片实现与后端中心系统安全认证和加密交互的基础上，结合实际业务场景引入遥控指令二次审批机制和多维智能风控策略设计。通过原型系统的仿真测试，验证了系统的技术可行性，实现卫星管理相关人员在远离测控中心的情况下也能有效参与在轨异常应急处置。未来还需要进一步提升软件成熟度，并结合军

民商用卫星不同的应用需求开展适应性评估，在符合保密要求的前提下逐步探索投入应用。

参考文献

[1] 申维和. 新型测控数据加解密平台的设计与实现[D]. 哈尔滨: 哈尔滨工程大学, 2014.
SHEN Weihe. Design and implementation of new platform for encryption and decryption of telemetry and telecontrol data[D]. Harbin: Harbin Engineering University, 2014

[2] 郜晓亮, 王剑, 张权. 测控网安全防护体系研究[J]. 飞行器测控学报, 2013, 32(4): 294–301.
GAO Xiaoliang, WANG Jian, ZHANG Quan. A study on the security architecture of TT&C networks[J]. Journal of Spacecraft TT&C Technology, 2013, 32(4): 294–301.

[3] 胡子杰, 张帆, 沈继忠, 等. 针对民用无人机的遥控数据保护方法[J]. 计算机工程, 2019, 45(4): 100–107.
HU Zijie, ZHANG Fan, SHEN Jizhong, et al. Remote control data protection method for civilian UAV[J]. Computer Engineering, 2019, 45(4): 100–107.

[4] 向军, 朱姣. 电力移动终端系统网络安全的设计与实现[J]. 自动化技术与应用, 2019, 38(5): 101–105.
XIANG Jun, ZHU Jiao. Design and implementation of network security for power mobile terminal system[J]. Techniques of Automation and Applications, 2019, 38(5): 101–105.

[5] 王志贺, 骆钊, 谢吉华, 等. 基于SM2密码体系的SD卡的电力移动终端安全接入方案[J]. 中国电力, 2015, 48(5): 75–80.
WANG Zhihe, LUO Zhao, XIE Jihua, et al. Secure access of electric power mobile terminal using SM2-crypto-system-based SD Card, Electric Power, 2015, 48(5): 75–80.

[6] 刘刚. 大数据时代智能风控体系建设实践[J]. 中国金融电脑, 2018(8): 15–18.

[7] 刘鹏, 王晓晨, 刘超, 等. 基于移动终端和云的航天器在轨监视系统设计[J]. 遥测遥控, 2021, 42(1): 31–39.
LIU Peng, WANG Xiaochen, LIU Chao, et al. Design of in-orbit spacecraft monitoring system based on mobile terminal and cloud platform[J]. Journal of Telemetry , Tracking and Command, 2021, 42(1): 31–39.

[8] 丁玲玲. 移动终端的安全认证技术研究与实现[D]. 南京: 南京理工大学, 2015.
DING Lingling. Research and Implementation of Secure Authentication for Mobile Terminals[D]. Nanjing: Nanjing University of Technology, 2015.

[9] 张国云, 王大鹏, 曹继宏, 等. 航天器在轨运行段遥控作业规范化设计与实现[J]. 遥测遥控, 2020, 41(3): 51–60.
ZHANG Guoyun, WANG Dapeng, CAO Jihong, et al. Design and realization of normalization on telecommand program for spacecraft in operation section[J]. Journal of Telemetry , Tracking and Command, 2020, 41(3): 51–60.

[作者简介]

刘　鹏　1981 年生，硕士，高级工程师，主要研究方向为在轨管理智能技术。

李　成　1986 年生，学士，工程师，主要研究方向为在轨管理智能技术。

刘　超　1984 年生，硕士，工程师，主要研究方向为在轨管理智能技术。

邵　坤　1983 年生，硕士，高级工程师，主要研究方向为在轨管理智能技术。

师　帅　1991 年生，学士，工程师，主要研究方向为在轨管理智能技术。

(本文编辑：潘三英)