**人工处置结果上传SDP平台需求**

**<浙江移动一键应急三期>**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 编 写 | 邱辉 | | | | 编写 时间 | | 2020-5-10 | |
| 审 核 |  | | | | 审核 时间 | |  | |
| 审 批 |  | | | | 审批 时间 | |  | |
| 文档管理 | 页码 | 共 页 | 修订次数 | 共 次 | | 版本 | | V1.0 |
| 编号 |  | | | | | | |

目录

[1 总体说明 3](#_Toc40223808)

[1.1 文档目的 3](#_Toc40223809)

[1.2 项目概述 3](#_Toc40223810)

[1.3 基本信息 3](#_Toc40223811)

[1.4 参考文档 3](#_Toc40223812)

[2 总体业务流程 4](#_Toc40223813)

[3 详细功能需求 4](#_Toc40223814)

[3.1 接口参数对应关系 4](#_Toc40223815)

[3.1.1接口信息 4](#_Toc40223816)

[3.1.2平台的处置结果 6](#_Toc40223817)

# 总体说明

## 文档目的

此文档由需求人员编写,主要提供给技术开发部安全管理平台项目组的开发、测试、需求等相关人员进行需求分析、软件设计、软件开发、软件测试。

## 项目概述

浙江移动一键应急三期中将人工应急场景中的封堵和解封堵处置日志上传给SDP平台。涉及的场景是【操作日志】->【应急操作日志】

## 基本信息

|  |  |  |  |
| --- | --- | --- | --- |
| **需求名称** | 浙江移动一键应急三期---人工处置结果需求 | | |
| **需求编号** |  | | |
| **客户联系人** | 何晓明 | **客户联系方式** |  |
| **需求采集人** | 邱辉 | **采集人联系方式** | 13758275340 |
| **需求类型** | 一键应急优化 | **需求类别** | 新增需求 |
| **优先级别** | 高 | **客户期望上线时间** | 2020/5/15 |

## 参考文档

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **文档名称** | **作者** | **来源** |
| 1 |  |  |  |
| 2 |  |  |  |

# 总体业务流程

将人工应急操作日志结果通过接口形式上传SDP平台。

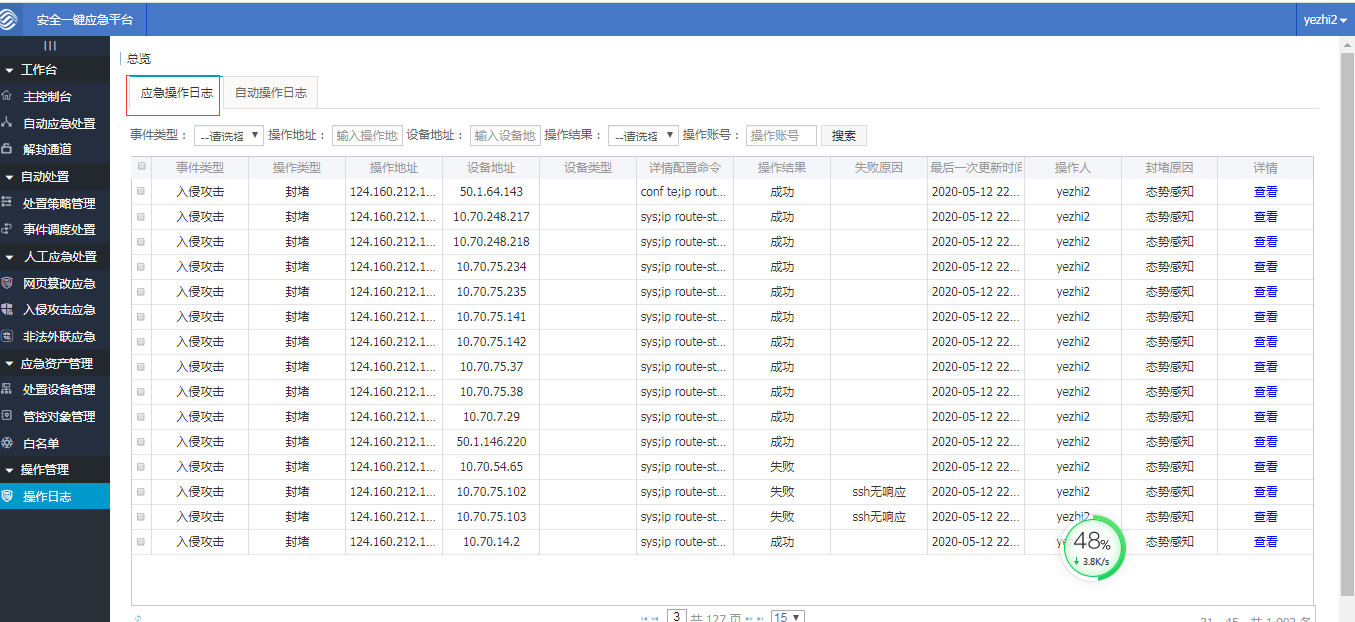
# 详细功能需求

## 接口参数对应关系

### 3.1.1接口信息

|  |  |  |  |
| --- | --- | --- | --- |
| **接口名称** | 安全事件处置结果接收接口 | | |
| **实现功能** | 接收自动处置平台所有处置的安全事件接口 | | |
| **接口地址** | <http://xxxxx:6060/interface/getDisposalReturns?wsdl> | | |
| **接口方法** | getDisposalReturns | | |
| **接口参数** | **参数名称** | **参数类型** | **参数说明** |
| evenId | String | 必填。  处置平台编号，唯一 |
| id | String | 必填。  当evenSrc=0，id= evenId；  当evenSrc=1，id等于SDP平台事件id；  当evenSrc=2，id等于其他平台id或者处置平台id |
| username | String | 必填。  认证账号(asainfo\_px) |
| evenSrc | Int(10) | 必填。  封堵来源：  0 人工处置，处置平台自身发起的封堵事件  1 SDP发起的封堵事件  2其他平台发起的封堵事件 |
| password | String | 必填。  认证密码(sdpEveId+disposalResultSendTime+01)md5值 |
| disposalType | Int(10) | 必填。  处置类型（0封堵、1解封堵） |
| evenType | String | 必填。  入侵攻击/非法外链/ACL清理/网页篡改/其他 |
| evenIp | String | 必填。  操作地址，（IPV4格式的地址和IPV6格式的地址），具体封堵的地址。 |
| ip | String | 必填。  设备地址，封堵设备的地址 |
| disposalResults | Int(10) | 必填。  处置结果（0成功、1部分成功、2失败） |
| disposalSteps | Int(10) | 必填。  处置步骤，数字几下边的详情就需要有几条 |
| disposalDetails |  | 处置详情 |
| disposalID |  | 处置序号(从1开始) |
| disposalAcc | String | 必填。  处置人账号 |
| disposalName | String | 必填。  处置人姓名 |
| disposalPhone | String | 必填。  处置人电话 |
| disposalMail | String | 必填。  处置人邮箱 |
| disposalDate | String | 必填。  处置时间(yyyy-MM-dd hh:mm:ss)2018-5-10 11:22:55 |
| disposalSend | String | 必填。  处置下发内容 |
| disposalReturn | String | 必填。  处置返回内容 |
| disposalResult | Int(10) | 必填。  处置是否成功（0 成功 非0未识别） |
| disposaRemarks | String | 处置备注，识别时写具体识别原因。 |
| disposalResultSendTime | Date | 发送时间(yyyy-MM-dd hh:mm:ss)2018-5-10 11:22:55 |
| **接口返回** | **返回值名称** | **返回值类型** | **返回值说明** |
|  | eveId | String(100) | 处置平台编号，唯一 |
|  | getTaskResult | Int(10) | 任务结果，0为成功,1为认证失败 2 告警处置结果保存失败 3 其他异常 |
|  | failReason | String(100) | 任务失败原因 |

### 3.1.2平台的处置结果



其中需要新增加一个处置编号，处置编号形式是大写字母M+日期+5位数字00001-99999；比如M2020051300001.作为唯一编号上传给SDP。

在前台新增一个字段【处置编号】，同时支持查询即可.

处置编号的查询位置放在【时间类型】前面

