**项目编号：LISS2022AQ072216**

**公路管养平台高清视频智能化发现**

**网络安全等级保护测评方案和计划**

|  |  |
| --- | --- |
| **系统名称：** | **公路管养平台高清视频智能化发现** |
| **委托单位：** | **上海市浦东新区道路运输事业发展中心** |
| **测评单位：** | **上海交通大学(信息安全服务技术研究实验室)** |
| **方案时间：** | **2022年08月17日** |

网络安全等级测评基本信息表

|  |  |  |  |
| --- | --- | --- | --- |
| **被测对象** | | | |
| **被测对象名称** | 公路管养平台高清视频智能化发现 | **安全保护等级** | 第二级（S2A2G2） |
| **备案证明编号** | 11111111111-11111 | | |
| **等级保护对象形态** | |  |  |  |  | | --- | --- | --- | --- | | ☑传统IT系统 | ☐云计算 | ☐采用移动互联技术的系统 | | | ☐物联网 | ☐工业控制系统 | ☐大数据 | ☐其他系统 | | | |
| |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | **被测单位** | | | | | | | **单位名称** | 上海市浦东新区道路运输事业发展中心 | | | | | | **单位地址** | 上海市浦东新区金业路399号 | | | **邮政编码** | 200120 | | **联系人** | **姓名** | 陆国盛 | **职务/职称** | 科员 | | | **所属部门** | 信息科 | **办公电话** | 021-50325566 | | | **移动电话** | 18116081016 | **电子邮件** | 2568285235@qq.com | | | | | |
| |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | **测评单位** | | | | | | | **单位名称** | 上海交通大学(信息安全服务技术研究实验室) | | | **机构代码** | SC202127130010091 | | **单位地址** | 上海市淮海西路125号机械楼201室 | | | **邮政编码** | 200030 | | **联系人** | **姓名** | 李海燕 | **职务/职称** | 中级测评师 | | | **所属部门** | 测评部 | **办公电话** | / | | | **移动电话** | 18256062248 | **电子邮件** | lhycps@sjtu.edu.cn | | | **审核批准** | **编制人** |  | **编制日期** |  | | | **审核人** |  | **审核日期** |  | | | **批准人** |  | **批准日期** |  | | | | | |

被测单位方案确认签字页

|  |  |
| --- | --- |
| 单位名称 | 上海市浦东新区道路运输事业发展中心 |
| 方案确认签字 | 我方认可本项目的技术方案合理，计划安排恰当，允许实施。  被测单位确认人（签字）： |

目录

[网络安全等级测评基本信息表 I](#_Toc41237146)

[目录 II](#_Toc41237147)

[1 概述 1](#_Toc41237148)

[1.1 项目简介 1](#_Toc41237149)

[1.2 测评范围 1](#_Toc41237150)

[1.3 测评过程 2](#_Toc41237151)

[1.4 测评依据 4](#_Toc41237152)

[2 被测等级保护对象情况 5](#_Toc41237153)

[2.1 定级情况 6](#_Toc41237154)

[2.2 承载的业务情况 7](#_Toc41237155)

[2.3 网络结构 8](#_Toc41237156)

[2.4 系统构成 9](#_Toc41237157)

[2.4.1 机房 9](#_Toc41237158)

[2.4.2 网络设备 9](#_Toc41237159)

[2.4.3 安全设备 9](#_Toc41237160)

[2.4.4 服务器/存储设备 10](#_Toc41237161)

[2.4.5 终端/现场设备 11](#_Toc41237162)

[2.4.6 系统管理软件/平台 11](#_Toc41237163)

[2.4.7 业务应用软件/平台 11](#_Toc41237164)

[2.4.8 关键数据类别 12](#_Toc41237165)

[2.4.9 安全相关人员 12](#_Toc41237166)

[2.4.10 安全管理文档 12](#_Toc41237167)

[2.5 前次测评问题整改情况说明 13](#_Toc41237168)

[3 测评对象与指标 14](#_Toc41237169)

[3.1 测评对象选择方法 14](#_Toc41237170)

[3.1.1 测评对象选择结果 15](#_Toc41237171)

[3.1.1.1 机房 15](#_Toc41237172)

[3.1.1.2 网络设备 15](#_Toc41237173)

[3.1.1.3 安全设备 15](#_Toc41237174)

[3.1.1.4 服务器/存储设备 16](#_Toc41237175)

[3.1.1.5 终端/现场设备 17](#_Toc41237176)

[3.1.1.6 系统管理软件/平台 17](#_Toc41237177)

[3.1.1.7 业务应用系统/平台 17](#_Toc41237178)

[3.1.1.8 数据类别 17](#_Toc41237179)

[3.2 测评指标 18](#_Toc41237180)

[3.2.1 安全通用要求指标 18](#_Toc41237181)

[3.2.2 安全扩展要求指标 18](#_Toc41237182)

[3.2.3 其他安全要求指标 19](#_Toc41237183)

[3.3 测评重点 19](#_Toc41237184)

[4 测评方法与工具 20](#_Toc41237185)

[4.1 测评方法 20](#_Toc41237186)

[4.2 主要测评工具 20](#_Toc41237187)

[5 工具测评 21](#_Toc41237188)

[5.1 风险和规避措施 21](#_Toc41237189)

[5.1.1 设备漏洞扫描 21](#_Toc41237190)

[5.1.2 WEB 应用漏洞扫描 22](#_Toc41237191)

[5.1.3 渗透测试说明 22](#_Toc41237192)

[5.2 工具测试接入点说明 24](#_Toc41237193)

[6 测评内容与实施 26](#_Toc41237194)

[6.1 通用安全要求 26](#_Toc41237195)

[6.1.1 安全物理环境测评 26](#_Toc41237196)

[6.1.1.1 测评指标 26](#_Toc41237197)

[6.1.1.2 测评实施 26](#_Toc41237198)

[6.1.2 安全通信网络测评 27](#_Toc41237199)

[6.1.2.1 测评指标 27](#_Toc41237200)

[6.1.2.2 测评实施 27](#_Toc41237201)

[6.1.3 安全区域边界测评 27](#_Toc41237202)

[6.1.3.1 测评指标 27](#_Toc41237203)

[6.1.3.2 测评实施 27](#_Toc41237204)

[6.1.4 安全计算环境测评 28](#_Toc41237205)

[6.1.4.1 测评指标 28](#_Toc41237206)

[6.1.4.2 测评实施 29](#_Toc41237207)

[6.1.5 安全管理中心测评 30](#_Toc41237208)

[6.1.5.1 测评指标 30](#_Toc41237209)

[6.1.5.2 测评实施 30](#_Toc41237210)

[6.1.6 安全管理制度测评 30](#_Toc41237211)

[6.1.6.1 测评指标 30](#_Toc41237212)

[6.1.6.2 测评实施 30](#_Toc41237213)

[6.1.7 安全管理机构测评 31](#_Toc41237214)

[6.1.7.1 测评指标 31](#_Toc41237215)

[6.1.7.2 测评实施 31](#_Toc41237216)

[6.1.8 安全管理人员测评 31](#_Toc41237217)

[6.1.8.1 测评指标 31](#_Toc41237218)

[6.1.8.2 测评实施 31](#_Toc41237219)

[6.1.9 安全建设管理测评 32](#_Toc41237220)

[6.1.9.1 测评指标 32](#_Toc41237221)

[6.1.9.2 测评实施 32](#_Toc41237222)

[6.1.10 安全运维管理测评 32](#_Toc41237223)

[6.1.10.1 测评指标 32](#_Toc41237224)

[6.1.10.2 测评实施 32](#_Toc41237225)

[6.2 扩展安全要求 33](#_Toc41237226)

[6.2.1 安全物理环境测评 33](#_Toc41237227)

[6.2.1.1 测评指标 33](#_Toc41237228)

[6.2.1.2 测评实施 33](#_Toc41237229)

[6.2.2 安全通信网络测评 33](#_Toc41237230)

[6.2.2.1 测评指标 33](#_Toc41237231)

[6.2.2.2 测评实施 33](#_Toc41237232)

[6.2.3 安全区域边界测评 34](#_Toc41237233)

[6.2.3.1 测评指标 34](#_Toc41237234)

[6.2.3.2 测评实施 34](#_Toc41237235)

[6.2.4 安全计算环境测评 34](#_Toc41237236)

[6.2.4.1 测评指标 34](#_Toc41237237)

[6.2.4.2 测评实施 34](#_Toc41237238)

[6.2.5 安全管理中心测评 35](#_Toc41237239)

[6.2.5.1 测评指标 35](#_Toc41237240)

[6.2.5.2 测评实施 35](#_Toc41237241)

[6.2.6 安全建设管理测评 35](#_Toc41237242)

[6.2.6.1 测评指标 35](#_Toc41237243)

[6.2.6.2 测评实施 35](#_Toc41237244)

[6.2.7 安全运维管理测评 36](#_Toc41237245)

[6.2.7.1 测评指标 36](#_Toc41237246)

[6.2.7.2 测评实施 36](#_Toc41237247)

[7 整体测评 37](#_Toc41237248)

[7.1 安全控制间安全测评 37](#_Toc41237249)

[7.2 层面间安全测评 38](#_Toc41237250)

[7.3 区域间安全测评 38](#_Toc41237251)

[7.4 系统结构安全测评 39](#_Toc41237252)

[8 项目组织与实施 40](#_Toc41237253)

[8.1 项目组织 40](#_Toc41237254)

[8.2 进度安排 41](#_Toc41237255)

[9 配合需求 44](#_Toc41237256)

# 概述

## 项目简介

网络安全等级保护测评是依据国家网络安全等级保护制度，按照有关管理规范和技术标准，对已定级备案的非涉及国家秘密的网络（含信息系统、数据资源等）的安全保护状况进行检验评估的活动。

上海市浦东新区道路运输事业发展中心委托上海交通大学(信息安全服务技术研究实验室) （认证证书编号SC202127130010091）对公路管养平台高清视频智能化发现开展网络安全等级测评，通过对目标网络系统的安全技术状态及安全管理状况依据相应网络安全等级保护要求进行测试、评估与分析，并将测评结论作为委托方进一步完善系统安全制度策略及安全技术防护措施依据。

## 测评范围

受上海市浦东新区道路运输事业发展中心委托，上海交通大学(信息安全服务技术研究实验室)于YYYY年MM月DD日至YYYY年MM月DD日对公路管养平台高清视频智能化发现进行了系统安全等级测评工作。本次安全测评的范围主要包括公路管养平台高清视频智能化发现的物理环境、主机、网络、业务应用系统、安全管理制度和人员等。安全测评通过静态评估、现场测试、综合评估等相关环节和阶段，从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等十个方面，对公路管养平台高清视频智能化发现进行综合测评。

## 测评过程

本次等级测评分为四个过程：测评准备过程、方案编制过程、测评实施过程、分析与报告编制过程。具体如图 1-1 所示。其中，各阶段的时间安排如下：

（1）YYYY年MM月DD日～MM月DD日，测评准备过程。

（2）YYYY年MM月DD日～MM月DD日，方案编制过程。

（3）YYYY年MM月DD日～MM月DD日，现场实施过程。

（4）YYYY年MM月DD日～MM月DD日，分析与报告编制过程。

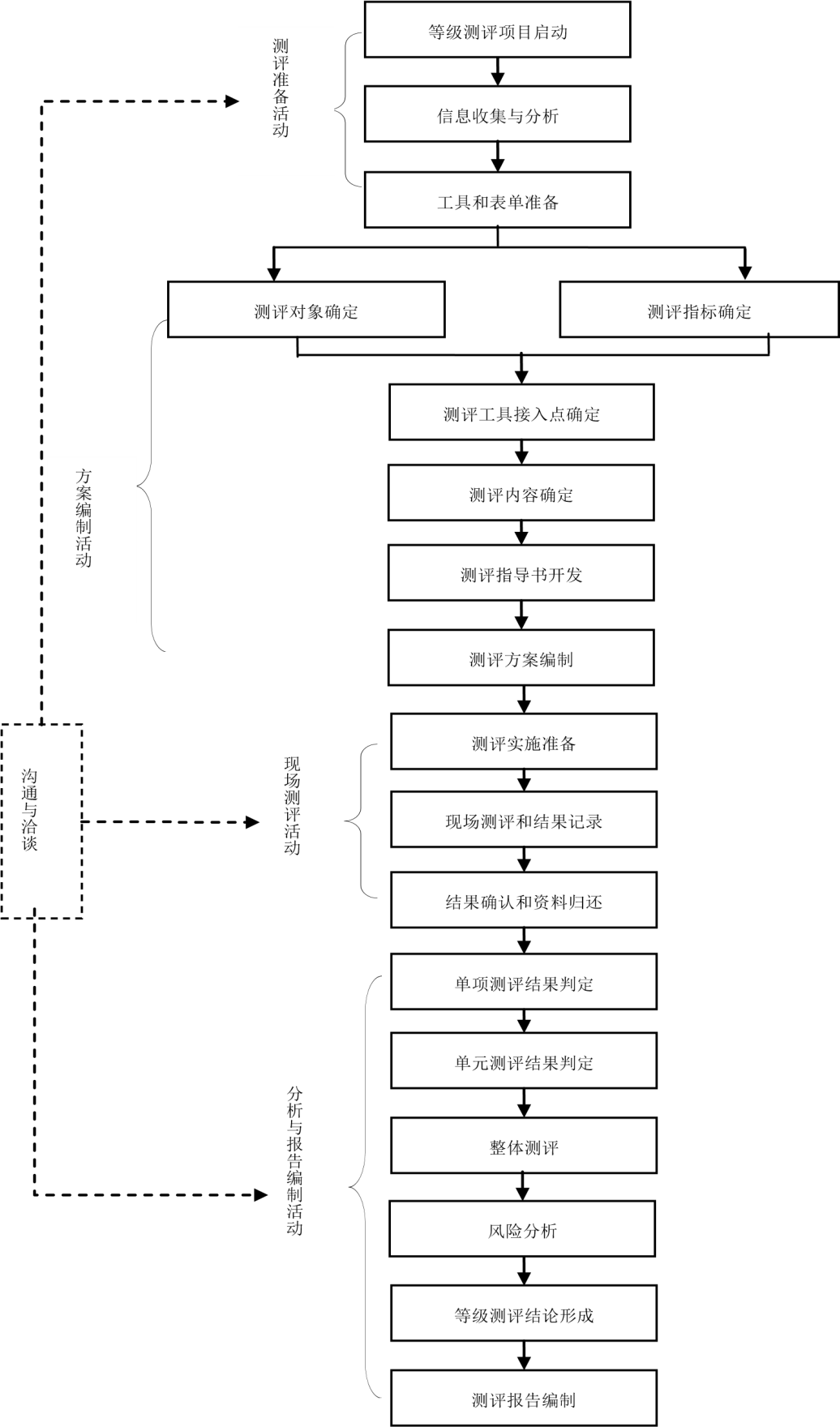


图 1.1 等级保护测评工作流程图

## 测评依据

测评过程中主要依据的标准：

1. GB/T 22239-2019：《信息安全技术 网络安全等级保护基本要求》

# 被测等级保护对象情况

测评过程中主要参考的标准：

公路管养平台高清视频智能化发现升级项目主要针对浦东道运中心对浦东新区全区范围内公路及城市高架道路的安全保障、养护管理的职责，以及公共交通、区域出租、货物运输、汽车维修、停车服务等五个业态的经营者、设施及从业人员日常管理和监督指导的职责。其中：  
1.高清视频接入及扩容：实现将浦东道路视频经由市交警总队和市交通委共享至新区道运发展中心，新区道运发展中心通过使用专用网络访问高清图像资源，包括S20外环高速、中环高架、华夏高架等城市快速路。并相应扩容安全传输通道与流媒体转发性能支持 50 路视频流并发联网。  
2.智慧发现平台：在新区道运发展中心新建一套智慧发现平台，将共享的高清视频资源按中心监管要求分类分析，包括交通运行监测、交通事件监测、道路抛洒物监测、绿化带垃圾监测、占道经营监测、事件告警处置，给中心平台运行人员提供支持，提高工作效率。  
3.监控坐席升级：升级坐席设备，满足高清视频播放的需求。并依托虚拟化的桌面平台，保障信息的安全可靠，包括高清显示器，云桌面服务器等。  
4.大屏坐席协作管理系统：将原大屏控制相关的设备升级为支持数字化和高清化的设施，包括高清输入和输出节点等，以满足高清接入升级的需求。          
本系统名称是公路管养平台高清视频智能化发现升级项目，由浦东新区道路与运输事业发展中心建设和运行，项目相关服务器、存储等硬件均由上海电科市政工程有限公司按照投标文件进行采购和安装调试。  
软件环境包括采购操作系统、数据库、中间件以及引擎产品软件，整体实施部署集成工作以保障系统稳定、安全、高效运行。  
系统部署在浦东新区道路与运输事业发展中心406机房，系统网络划分为浦东新区道路与运输事业发展中心路网。  
浦东新区道路与运输事业发展中心路网主要部署了平台的管理和查看软件、数据库、监控数据等，实现对系统中的设备集中管理。  
本系统部署有虚拟化云桌面终端、服务器等硬件设备，计算机终端通过MvpOperator软件、谷歌、火狐访问登录公路管养平台高清视频智能化发现升级系统。

## 定级情况

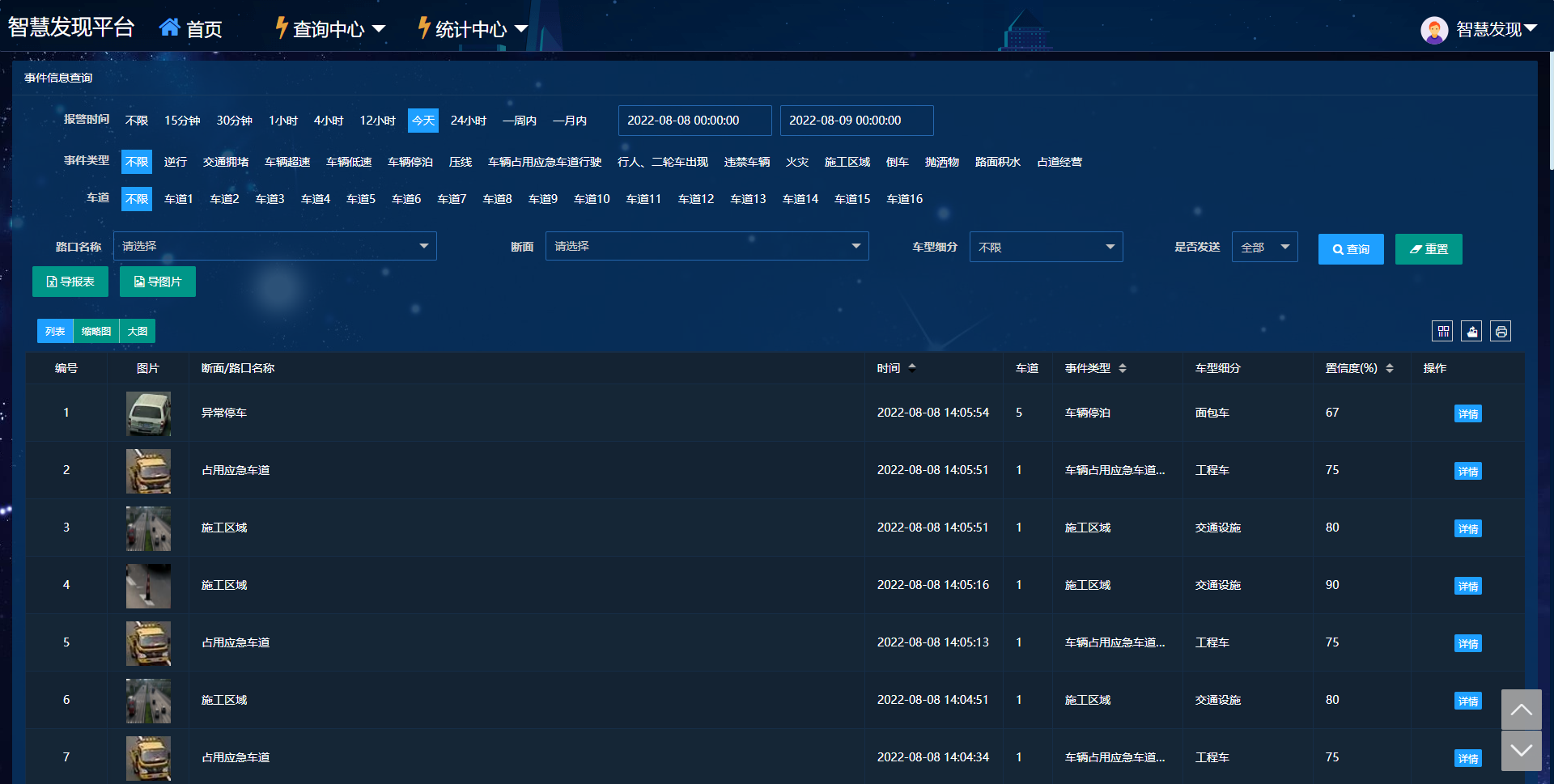
表 2‑1 公路管养平台高清视频智能化发现定级结果

| **被测对象名称** | **安全保护等级** | **业务信息 安全保护等级** | **系统服务 安全保护等级** |
| --- | --- | --- | --- |
| 公路管养平台高清视频智能化发现 | 第二级 | 第二级 | 第二级 |

## 承载的业务情况



图登录页



图业务展示页

## 网络结构

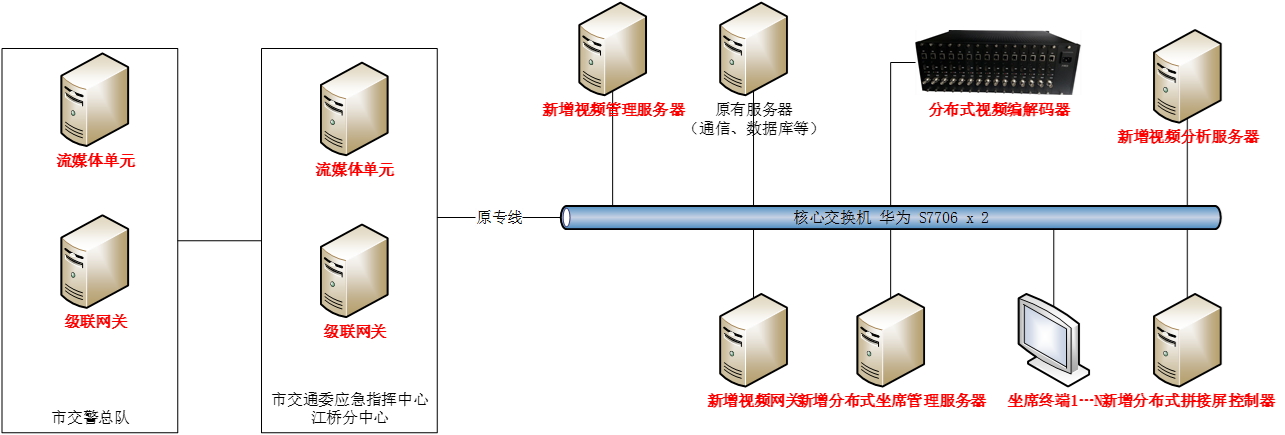


图 2.1 公路管养平台高清视频智能化发现网络拓扑图

如图2-1 公路管养平台高清视频智能化发现网络拓扑图所示，公路管养平台高清视频智能化发现的网络结构主要包括：

本系统名称是公路管养平台高清视频智能化发现升级项目，由浦东新区道路与运输事业发展中心建设和运行，项目相关服务器、存储等硬件均由上海电科市政工程有限公司按照投标文件进行采购和安装调试。  
软件环境包括采购操作系统、数据库、中间件以及引擎产品软件，整体实施部署集成工作以保障系统稳定、安全、高效运行。  
系统部署在浦东新区道路与运输事业发展中心406机房，系统网络划分为浦东新区道路与运输事业发展中心路网。  
浦东新区道路与运输事业发展中心路网主要部署了平台的管理和查看软件、数据库、监控数据等，实现对系统中的设备集中管理。  
本系统部署有虚拟化云桌面终端、服务器等硬件设备，计算机终端通过MvpOperator软件、谷歌、火狐访问登录公路管养平台高清视频智能化发现升级系统。

## 系统构成

### 机房

以列表形式给出被测系统的部署机房。

表 2‑2 机房

| **序号** | **测评对象编号** | **机房名称** | **物理位置** | **重要程度** |
| --- | --- | --- | --- | --- |
| 本系统不涉及 | | | | |

### 网络设备

以列表形式给出被测系统中的网络设备（包括虚拟网络设备）。

表 2‑3 网络设备

| **序号** | **测评对象编号** | **设备名称** | **虚拟**  **设备** | **系统及版本** | **品牌型号** | **用途** | **重要**  **程度** | **备注** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 本系统不涉及 | | | | | | | | |

### 安全设备

以列表形式给出被测系统中的安全设备（包括虚拟安全设备）。

表 2‑4 安全设备

| **序号** | **测评对象编号** | **设备名称** | **虚拟设备** | **系统及版本** | **品牌型号** | **用途** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 本系统不涉及 | | | | | | | | |

### 服务器/存储设备

以列表形式给出被测系统中的服务器和存储设备（包括虚拟设备）。

表 2‑5 服务器/存储设备

| **序号** | **测评对象编号** | **设备名称** | **所属业务应用系统/平台名称** | **虚拟设备** | **操作系统及版本** | **数据库管理系统及版本** | **中间件及版本** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | LISS-SER-001 | 流媒体转发节点 | 高清视频监控管理平台系统 | × | CentOS Linux 7.8 | 高清视频监控管理平台系统数据库 | / | 非常重要 | 172.16.107.2 |
| 2 | LISS-SER-002 | 流媒体单元 | 高清视频监控管理平台系统 | × | CentOS Linux 7.8 | 高清视频监控管理平台系统数据库 | / | 非常重要 | 172.16.107.3, 172.16.107.4 |
| 3 | LISS-SER-003 | 平台级联网关 | 智慧发现平台系统 | × | CentOS Linux 7.8 | 智慧发现平台系统数据库 | / | 非常重要 | 172.16.107.5 |
| 4 | LISS-SER-001 | 视频管理服务器 | 高清视频监控管理平台系统 | × | CentOS Linux 7.8 | 高清视频监控管理平台系统数据库 | / | 非常重要 | 172.16.107.5 |
| 5 | LISS-SER-002 | 云台视频事件检测服务器 | 高清视频监控管理平台系统 | × | CentOS Linux 7.8 | 高清视频监控管理平台系统数据库 | / | 非常重要 | 172.16.107.7 |
| 6 | LISS-SER-003 | 事件检测服务器 | 高清视频监控管理平台系统 | × | CentOS Linux 7.8 | 高清视频监控管理平台系统数据库 | / | 非常重要 | 172.16.107.8 |
| 7 | LISS-DB-001 | 高清视频监控管理平台系统数据库 | 高清视频监控管理平台系统 | × | 视频管理服务器 | mysql 5.1.41 | / | 关键 |  |
| 8 | LISS-DB-002 | 智慧发现平台系统数据库 | 智慧发现平台系统 | × | 视频管理服务器 | mysql 5.1.42 | / | 关键 |  |

### 终端/现场设备

以列表形式给出被测系统中的终端，包括业务终端、运维终端、管理终端和现场设备等，如果使用了移动终端，列出移动终端。

表 2‑6 终端/现场设备

| **序号** | **测评对象编号** | **设备名称** | **虚拟设备** | **操作系统/控制软件及版本** | **设备类别/用途** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 本系统不涉及 | | | | | | | |

### 系统管理软件/平台

以列表的形式给出被测系统中的系统管理类软件或平台，包括数据库、网管软件/平台、安管软件/平台、云计算管理软件/平台等。

表 2‑7 系统管理软件/平台

| **序号** | **测评对象编号** | **系统管理软件/平台名称** | **所在设备名称** | **版本** | **主要功能** | **重要程度** | **备注** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 本系统不涉及 | | | | | | | |

### 业务应用软件/平台

以列表的形式给出被测系统中的业务应用系统（包括服务器端、中间件和客户端软件等应用软件）。

表 2‑8 业务应用软件/平台

| **序号** | **测评对象编号** | **业务应用系统/平台名称** | **主要功能** | **业务应用软件及版本** | **开发厂商** | **重要程度** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | LISS-APL-001 | 高清视频监控管理平台系统 | 桌面云承载平台 | v1.0 | 上海电科市政工程有限公司 | 关键 |
| 2 | LISS-APL-002 | 智慧发现平台系统 | 桌面云发布平台 | v1.0 | 上海电科市政工程有限公司 | 关键 |

### 关键数据类别

以列表形式描述具有相近业务属性和安全需求的数据集合。

表 2‑9 关键数据类别

| **序号** | **数据类别** | **所属业务应用** | **安全防护需求** |
| --- | --- | --- | --- |
| 1 | 鉴别数据 |  |  |
| 2 | 重要业务数据 |  |  |
| 3 | 主要配置数据 |  |  |
| 4 | 重要个人信息 |  |  |

### 安全相关人员

以列表形式给出与被测系统安全相关的人员情况。相关人员包括（但不限于）安全主管、系统建设负责人、系统运维负责人、网络（安全）管理员、主机（安全）管理员、数据库（安全）管理员、应用（安全）管理员、机房管理人员、资产管理员、业务操作员、安全审计人员等。

表 2‑10 安全相关人员

| **序号** | **测评对象编号** | **姓名** | **岗位/角色** | **联系方式** |
| --- | --- | --- | --- | --- |
| 本系统不涉及 | | | | |

### 安全管理文档

以列表形式给出与被测系统安全相关的文档，包括管理类文档、记录类文档和其他文档。

表 2‑11 安全管理文档

| **序号** | **测评对象编号** | **文档名称** | **主要内容** |
| --- | --- | --- | --- |
| 本系统不涉及 | | | |

## 前次测评问题整改情况说明

# 测评对象与指标

## 测评对象

### 测评对象选择方法

公路管养平台高清视频智能化发现等级测评的测评对象种类上基本覆盖、数量进行抽样，重点抽查主要的设备、设施、人员和文档等。结合公路管养平台高清视频智能化发现的网络拓扑结构和业务情况，本次等级测评的测评对象在抽样时主要考虑以下几个方面：

（1）主机房（包括其环境、设备和设施等）和灾备机房；

（2）存储被测系统重要数据的介质的存放环境；

（3）办公场地；

（4）整个系统的网络拓扑结构；

（5）安全设备，包括防火墙等；

（6）边界网络设备，包括路由器、楼层交换机等；

（7）对整个信息系统或其局部的安全性起作用的网络互联设备，如核心交换机、路由器等；

（8）承载业务处理系统主要业务或数据的服务器（包括其操作系统和数据库）；

（9）管理终端和主要XXXX应用系统终端；

（10）能够完成XXXX系统不同业务使命的业务应用系统；

（11）业务备份系统；

（12）信息安全主管人员、各方面的负责人员、具体负责安全管理的当事人、业务负责人；

（13）涉及到信息系统安全的所有管理制度和记录。

抽样原则：在等级测评时，业务处理系统中配置相同的安全设备、边界网络设备、网络互联设备、服务器、终端以及备份设备，每类至少抽查两台作为测评对象。

### 测评对象选择结果

#### 机房

表 3‑1 机房

| **序号** | **机房名称** | **物理位置** | **重要程度** |
| --- | --- | --- | --- |
| 本系统不涉及 | | | |

#### 网络设备

表 3‑2 网络设备

| **序号** | **设备名称** | **虚拟**  **设备** | **系统**  **及版本** | **品牌**  **及型号** | **用途** | **重要**  **程度** |
| --- | --- | --- | --- | --- | --- | --- |
| 本系统不涉及 | | | | | | |

#### 安全设备

表 3‑3 安全设备

| **序号** | **设备名称** | **虚拟**  **设备** | **系统**  **及版本** | **品牌**  **及型号** | **用途** | **重要**  **程度** |
| --- | --- | --- | --- | --- | --- | --- |
| 本系统不涉及 | | | | | | |

#### 服务器/存储设备

表 3‑4 服务器/存储设备

| **序号** | **设备名称** | **所属业务应用系统/平台名称** | **虚拟设备** | **操作系统**  **及版本** | **数据库管理系统**  **及版本** | **中间件及版本** | **重要**  **程度** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 流媒体转发节点 | 高清视频监控管理平台系统 | × | CentOS Linux 7.8 | 高清视频监控管理平台系统数据库 | / | 非常重要 |
| 2 | 高清视频监控管理平台系统数据库 | 高清视频监控管理平台系统 | × | 视频管理服务器 | mysql 5.1.41 | / | 关键 |
| 3 | 流媒体单元 | 高清视频监控管理平台系统 | × | CentOS Linux 7.8 | 高清视频监控管理平台系统数据库 | / | 非常重要 |
| 4 | 智慧发现平台系统数据库 | 智慧发现平台系统 | × | 视频管理服务器 | mysql 5.1.42 | / | 关键 |
| 5 | 平台级联网关 | 智慧发现平台系统 | × | CentOS Linux 7.8 | 智慧发现平台系统数据库 | / | 非常重要 |
| 6 | 视频管理服务器 | 高清视频监控管理平台系统 | × | CentOS Linux 7.8 | 高清视频监控管理平台系统数据库 | / | 非常重要 |
| 7 | 云台视频事件检测服务器 | 高清视频监控管理平台系统 | × | CentOS Linux 7.8 | 高清视频监控管理平台系统数据库 | / | 非常重要 |
| 8 | 事件检测服务器 | 高清视频监控管理平台系统 | × | CentOS Linux 7.8 | 高清视频监控管理平台系统数据库 | / | 非常重要 |

#### 终端/现场设备

表 3‑5 终端/现场设备

| **序号** | **设备名称** | **虚拟**  **设备** | **操作系统/**  **控制软件及版本** | **设备类别/用途** | **重要**  **程度** |
| --- | --- | --- | --- | --- | --- |
| 本系统不涉及 | | | | | |

#### 系统管理软件/平台

表 3‑6 系统管理软件/平台

| **序号** | **系统管理软件/平台名称** | **所在设备名称** | **版本** | **主要功能** | **重要**  **程度** |
| --- | --- | --- | --- | --- | --- |
| 本系统不涉及 | | | | | |

#### 业务应用系统/平台

表 3‑7 业务应用系统/平台

| **序号** | **业务应用系统**  **/平台名称** | **主要功能** | **业务应用软件及版本** | **开发厂商** | **重要**  **程度** |
| --- | --- | --- | --- | --- | --- |
| 1 | 高清视频监控管理平台系统 | 桌面云承载平台 | v1.0 | 上海电科市政工程有限公司 | 关键 |
| 2 | 智慧发现平台系统 | 桌面云发布平台 | v1.0 | 上海电科市政工程有限公司 | 关键 |

#### 数据类别

表 3‑8 关键数据类别

| **序号** | **数据类别** | **所属业务应用** | **安全防护需求** |
| --- | --- | --- | --- |
| 本系统不涉及 | | | |

## 测评指标

### 安全通用要求指标

表 3‑9 安全通用要求指标

| **安全类[[1]](#footnote-1)** | **安全控制点[[2]](#footnote-2)** | **测评项数** |
| --- | --- | --- |
| **安全通用要求** | | |
| 安全计算环境 | 身份鉴别 | 3 |
| 访问控制 | 4 |
| 安全审计 | 3 |
| 入侵防范 | 5 |
| 恶意代码防范 | 1 |
| 可信验证 | 1 |
| 数据完整性 | 1 |
| 数据备份恢复 | 2 |
| 剩余信息保护 | 1 |
| 个人信息保护 | 2 |
| **安全通用要求指标数量统计** | | 23 |

### 安全扩展要求指标

表 3‑10 安全扩展要求指标

| **扩展类型** | **安全类** | **安全控制点** | **测评项数** |
| --- | --- | --- | --- |
| 本系统不涉及 | | | |

### 其他安全要求指标

表 3‑11 其他安全要求指标

| **安全类** | **安全控制点** | **特殊要求描述** | **测评项数** |
| --- | --- | --- | --- |
| 本系统不涉及 | | | |

## 测评重点

无

# 测评方法与工具

## 测评方法

本次等级测评的主要方式有：访谈、核查和测试及综合风险分析。

        ●访谈

        在访谈的广度上，访谈覆盖不同类型的系统运维管理人员，包括系统负责人、机房管理员、系统管理员、网络管理员、开发人员、应用业务人员、文档管理员等。对测评对象采取抽样的形式确定测评数量；在访谈的深度上，访谈包含通用和高级的问题以及一些有难度和探索性的问题。测评人员访谈技术负责人、系统管理员、业务开发人员等系统技术架构的实现及配置；访谈系统负责人系统的整体运行状况、安全管理的执行成效。

        ●检查，包括文档核查及配置核查

       在核查的广度上，数量上采取抽样的形式，基本覆盖系统包含的网络设备、安全设备、主机设备、应用软件、管理制度文档等不同类型对象；在核查的深度上，详细分析、观察和研究除了功能级上的文档、机制和活动外，还包括总体/概要和一些详细设计以及实现上的相关信息。

        ●测试，包括案例验证测试、漏洞扫描测试、渗透性测试。

       在核查的广度上，基本覆盖不同类型的机制，在数量、范围上采取抽样方式；在测试的深度上，功能测试涉及机制的功能规范、高级设计和操作规程等文档及深度验证系统的安全机制是否实现，包括冗余机制、备份恢复机制的实现。

        ●风险分析方法

        本项目依据安全事件可能性和安全事件后果对信息系统面临的风险进行分析，分析过程包括：

        1) 判断信息系统安全保护能力缺失（等级测评结果中的部分符合项和不符合项）被威胁利用导致安全事件发生的可能性；

        2) 判断由于安全功能的缺失使得信息系统业务信息安全和系统服务面临的风险；

        3) 结合信息系统的安全保护等级对风险分析结果进行评价，即对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益造成的风险。

## 主要测评工具

# 工具测评

## 风险和规避措施

### 设备漏洞扫描

**设备包括网络设备、安全设备、主机设备（操作系统），在使用扫描器对目标系统扫描的过程中，可能会出现以下的风险：**

1）占用带宽（风险不高）；

2）进程、系统崩溃。由于目标系统的多样性及脆弱性，或是目标系统上某些特殊服务本身存在的缺陷，对扫描器发送的探测包或者渗透测试工具发出的测试数据不能正常响应，可能会出现系统崩溃或程序进程的崩溃；

3）登录界面锁死。扫描器可以对某些常用管理程序（WEB、 FTP， Telnet，SNMP， SSH， WebLogic）的登录口令进行弱口令猜测验证，如果目标系统对登录失败次数进行了限制，尝试登录次数超过限定次数系统可能会锁死登录界面。

**风险规避方法：**

1）根据目标系统的网络、应用状况，调整扫描测试时间段，采取避峰扫描；

2）对扫描器扫描策略进行配置，适当调整扫描器的并发任务数和扫描的强度，可使减少扫描器工作时占用的带宽，降低对目标系统影响；

3）根据目标系统及目标系统上运行的管理程序，通过与测评委托方相关人员协商，定制针对本系统测试的扫描插件、端口等配置，尽量合理设置扫描强度，降低目标系统或进程崩溃的风险；

4）如目标系统对登录某些相关程序的尝试次数进行了限制，在进行扫描时，可屏蔽暴力猜解功能，以避免登录界面锁死的情况发生。

### WEB 应用漏洞扫描

**在使用 WEB 应用漏洞扫描器对目标系统扫描的过程中，可能会存在以下的风险：**

1）占用带宽（风险不高）；

2）登录界面锁死。 WEB应用漏洞扫描会对登录页面进行弱口令猜测，猜测过程可能会造成应用系统某些帐号锁死。

**风险规避方法：**

1）根据目标系统的网络、应用状况，调整扫描测试时间段，采取避峰扫描；

2）如目标系统对登录某些相关程序的尝试次数进行了限制，在进行扫描时，可屏蔽暴力猜解功能，以避免登录界面锁死的情况发生。

### 渗透测试说明

**渗透性测试根据测试者在测试前掌握被测信息多少的不同可分为：**

* **黑盒测试：**

渗透性测试安全工程师完全处于对系统一无所知的状态，通常这类测试最初信息来自于DNS、Web、Email及各种公开对外的服务器，主要是模拟来自互联网的攻击者。

* **白盒测试：**

渗透性测试安全工程师可以通过正常渠道向被测机构要求，取得各种资料，包括网络拓扑、员工资料甚至网站或其他程序的代码片段，也能够与被测机构内部的其他员工（业务人员、开发人员、管理人员等）进行面对面的沟通。这类测试的目的是模拟组织内部雇员的越权操作，和预防万一组织重要信息泄露，网络黑客能利用这些信息对组织构成的危害。

* **灰盒测试：**

对测试对象有一定的了解，主要是模拟离职的员工或合作伙伴，他们对组织的结构比较了解。但不在公司内部，没有权限访问。

**根据渗透者所处的位置也可以分为：**

* **内部测试：**

渗透测试安全工程师由内部网络发起测试，这类测试能够模拟组织内部违规操作者的行为。最主要的“优势”就是绕过了防火墙的保护。

* **外部测试：**

渗透测试安全工程师完全处于外部网络（如互联网、第三方机构），模拟从组织外部发起的攻击行为，可能来自于对组织内部信息一无所知的攻击者，也可能来自于对组织内部信息一清二楚的攻击者。

## 工具测试接入点说明

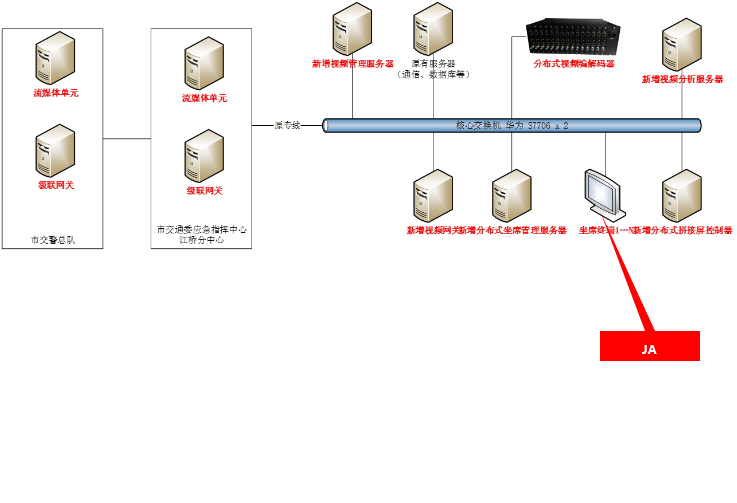


图 5.1 工具接入测试示意图

对公路管养平台高清视频智能化发现进行测评，涉及到漏洞扫描工具、渗透性测试工具集等多种测试工具。为了发挥测评工具的作用，达到测评的目的，各种测评工具需要接入到被测系统网络中，并配置合法的网络IP地址。

针对被测系统的网络边界和抽查设备、主机和业务应用系统的情况，需要在被测系统及其互联网络中设置各测试工具接入点，如图3-1所示：

接入点JA：在单位内网接入，主要目的是，模拟内部恶意用户发现Web应用安全漏洞的过程，并尝试利用以上漏洞实施诸如获取系统控制权（GetShell）、获得大量敏感信息（DragLibrary）等模拟攻击行为。

        以上渗透测试使用明鉴WEB应用弱点扫描器

表 5‑1 接入点扫描的网络设备和服务器设备列表

| **序号** | **接入点** | **设备名称** | **类型/OS** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 测评内容与实施

等级测评的现场实施过程由单项测评和整体测评两部分构成。

对应《基本要求》各安全要求项的测评称为单项测评。整体测评是在单项测评的基础上，通过进一步分析定级对象安全保护功能的整体相关性，对定级对象实施的综合安全测评。

## 通用安全要求

把测评指标和测评方式结合到信息系统的具体测评对象上，就构成了可以具体测评的工作单元。 具体分为安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等方面。

### 安全物理环境测评

#### 测评指标

表 6‑1 安全物理环境（通用要求）测评指标

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
| 本系统不涉及 | | |

#### 测评实施

安全物理环境测评中，测评人员将以文档查阅与分析和现场观测等检查方法为主，访谈为辅来获取测评证据（如机房的温湿度情况），用于评测机房的安全保护能力。

安全物理环境测评涉及的测评对象主要为机房和相关的安全文档。

### 安全通信网络测评

#### 测评指标

表 6‑2 安全通信网络（通用要求）测评指标

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
| 本系统不涉及 | | |

#### 测评实施

安全通信网络测评中，技术检测人员将以安全配置核查、人工验证和网络监听与分析等方法为主，文档查阅与分析等方法为辅来获取必要证据，用于评测系统的安全保护能力。

### 安全区域边界测评

#### 测评指标

表 6‑3 安全区域边界（通用要求）测评指标

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
| 本系统不涉及 | | |

#### 测评实施

安全区域边界测评中，技术检测人员将以安全配置核查、人工验证和网络监听与分析等方法为主，文档查阅与分析等方法为辅来获取必要证据，用于评测系统的网络安全保护能力。

### 安全计算环境测评

#### 测评指标

表 6‑4 安全计算环境（通用要求）测评指标

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
| 1 | 身份鉴别 | a）应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换； |
| 2 | b）应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施； |
| 3 | c）当进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听。 |
| 4 | 访问控制 | a）应对登录的用户分配账户和权限； |
| 5 | b）应重命名或删除默认账户，修改默认账户的默认口令； |
| 6 | c）应及时删除或停用多余的、过期的账户，避免共享账户的存在； |
| 7 | d）应授予管理用户所需的最小权限，实现管理用户的权限分离。 |
| 8 | 安全审计 | a）应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计； |
| 9 | b）审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息； |
| 10 | c）应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。 |
| 11 | 入侵防范 | a）应遵循最小安装的原则，仅安装需要的组件和应用程序； |
| 12 | b）应关闭不需要的系统服务、默认共享和高危端口； |
| 13 | c）应通过设定终端接入方式或网络地址范围对通过网络进行管理的管理终端进行限制； |
| 14 | d）应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求； |
| 15 | e）应能发现可能存在的已知漏洞，并在经过充分测试评估后，及时修补漏洞。 |
| 16 | 恶意代码防范 | a）应安装防恶意代码软件或配置具有相应功能的软件，并定期进行升级和更新防恶意代码库。 |
| 17 | 可信验证 | a）可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。 |
| 18 | 数据完整性 | a）应采用校验技术保证重要数据在传输过程中的完整性。 |
| 19 | 数据备份恢复 | a）应提供重要数据的本地数据备份与恢复功能； |
| 20 | b）应提供异地数据备份功能，利用通信网络将重要数据定时批量传送至备用场地。 |
| 21 | 剩余信息保护 | a）应保证鉴别信息所在的存储空间被释放或重新分配前得到完全清除。 |
| 22 | 个人信息保护 | a）应仅采集和保存业务必需的用户个人信息； |
| 23 | b）应禁止未授权访问和非法使用用户个人信息。 |

#### 测评实施

安全计算环境测评中，技术检测人员主要关注服务器操作系统、数据库管理系统、网络设备、安全设备以及应用系统在身份鉴别、访问控制、安全审计等方面的安全保护能力，将以安全配置核查和人工验证为主，文档查阅和分析为辅来获取证据（如相关措施的部署和配置情况）。

### 安全管理中心测评

#### 测评指标

表 6‑5 安全管理中心（通用要求）测评指标

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
| 本系统不涉及 | | |

#### 测评实施

安全管理中心测评中，技术检测人员将以安全配置核查和人工验证为主，文档查阅和分析为辅来获取证据（如相关措施的部署和配置情况），用于评测系统的安全保护能力。

### 安全管理制度测评

#### 测评指标

表 6‑6 安全管理制度（通用要求）测评指标

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
| 本系统不涉及 | | |

#### 测评实施

安全管理类测评中，技术检测人员将以文档查看和分析为主，访谈为辅获取证据，来评测项目委托单位安全管理类措施的落实情况。安全管理类测评主要涉及安全主管、安全管理人员、管理制度文档、各类操作规程文件和操作记录等。

### 安全管理机构测评

#### 测评指标

表 6‑7 安全管理机构（通用要求）测评指标

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
| 本系统不涉及 | | |

#### 测评实施

安全管理机构测评主要涉及安全主管、相关管理制度以及相关工作/会议记录等技术检测对象。

### 安全管理人员测评

#### 测评指标

表 6‑8 安全管理人员（通用要求）测评指标

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
| 本系统不涉及 | | |

#### 测评实施

安全管理人员测评主要涉及安全主管、相关管理制度以及相关工作/会议记录等检测对象。

### 安全建设管理测评

#### 测评指标

表 6‑9 安全建设管理（通用要求）测评指标

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
| 本系统不涉及 | | |

#### 测评实施

安全建设管理测评主要涉及系统建设负责人、各类管理制度、操作规程文件和执行过程记录等技术检测对象。

### 安全运维管理测评

#### 测评指标

表 6‑10 安全运维管理（通用要求）测评指标

| **序号** | **安全子类** | **测评指标描述** |
| --- | --- | --- |
| 本系统不涉及 | | |

#### 测评实施

安全运维管理测评主要涉及安全主管、各类运维人员、各类管理制度、操作规程文件和执行过程记录等技术检测对象。

## 扩展安全要求

### 安全物理环境测评

#### 测评指标

表 6‑11 安全物理环境（安全扩展要求）测评指标

| **序号** | **扩展类型** | **安全子类** | **测评指标描述** |
| --- | --- | --- | --- |
| 本系统不涉及 | | | |

#### 测评实施

安全物理环境测评中，测评人员将以**文档查阅与分析和现场观测**等检查方法为主，访谈为辅来获取测评证据，用于评测机房针对安全扩展要求方面的安全保护能力。

安全物理环境测评涉及的测评对象主要为机房和相关的安全文档。

### 安全通信网络测评

#### 测评指标

表 6‑12 安全通信网络（安全扩展要求）测评指标

| **序号** | **扩展类型** | **安全子类** | **测评指标描述** |
| --- | --- | --- | --- |
| 本系统不涉及 | | | |

#### 测评实施

安全通信网络测评中，技术检测人员将以安全配置核查、人工验证和网络监听与分析等方法为主，文档查阅与分析等方法为辅来获取必要证据，用于评测系统针对安全扩展要求方面的安全保护能力。

### 安全区域边界测评

#### 测评指标

表 6‑13 安全区域边界（安全扩展要求）测评指标

| **序号** | **扩展类型** | **安全子类** | **测评指标描述** |
| --- | --- | --- | --- |
| 本系统不涉及 | | | |

#### 测评实施

安全区域边界测评中，技术检测人员将以安全配置核查、人工验证和网络监听与分析等方法为主，文档查阅与分析等方法为辅来获取必要证据，用于评测系统针对安全扩展要求方面的网络安全保护能力。

### 安全计算环境测评

#### 测评指标

表 6‑14 安全计算环境（安全扩展要求）测评指标

| **序号** | **扩展类型** | **安全子类** | **测评指标描述** |
| --- | --- | --- | --- |
| 本系统不涉及 | | | |

#### 测评实施

安全计算环境测评中，技术检测人员主要关注服务器操作系统、数据库管理系统、网络设备、安全设备以及应用系统在相关安全扩展要求方面的安全保护能力，将以安全配置核查和人工验证为主，文档查阅和分析为辅来获取证据（如相关措施的部署和配置情况）。

### 安全管理中心测评

#### 测评指标

表 6‑15 安全管理中心（安全扩展要求）测评指标

| **序号** | **扩展类型** | **安全子类** | **测评指标描述** |
| --- | --- | --- | --- |
| 本系统不涉及 | | | |

#### 测评实施

安全管理中心测评中，技术检测人员将以安全配置核查和人工验证为主，文档查阅和分析为辅来获取证据（如相关措施的部署和配置情况），用于评测系统针对安全扩展要求方面的安全保护能力。

### 安全建设管理测评

#### 测评指标

表 6‑16 安全建设管理（安全扩展要求）测评指标

| **序号** | **扩展类型** | **安全子类** | **测评指标描述** |
| --- | --- | --- | --- |
| 本系统不涉及 | | | |

#### 测评实施

安全建设管理测评主要涉及系统建设负责人、各类管理制度、操作规程文件和执行过程记录等技术检测对象。

### 安全运维管理测评

#### 测评指标

表 6‑17 安全运维管理（安全扩展要求）测评指标

| **序号** | **扩展类型** | **安全子类** | **测评指标描述** |
| --- | --- | --- | --- |
| 本系统不涉及 | | | |

#### 测评实施

安全运维管理测评主要涉及安全主管、各类运维人员、各类管理制度、操作规程文件和执行过程记录等技术检测对象。

# 整体测评

系统整体测评主要是在单项测评的基础上，通过测评分析系统在安全控制间、层面间和安全区域间三个方面存在的关联作用验证和分析不符合项是否影响系统的安全保护能力，同时分析系统与其他系统系统边界安全性是否影响系统的安全保护能力，综合测试分析系统的整体安全性是否合理。系统由于运行环境及系统内部结构的关联性，因此需要针对具体的测评单元间的关联关系分析系统整体安全保护能力。具体内容包括：安全控制间安全测评、层面间安全测评、区域间安全测评和系统结构安全测评。**系统整体测评采取风险分析的方式，由测评机构单独完成。**

安全控制间安全测评主要对同一区域内、同一层面上的不同安全控制间存在的功能增强、补充或削弱等关联作用进行测评，同时，也包括对《基本要求》的要求项与同一区域、同一层面上的非《基本要求》要求的安全控制之间的安全测评。依据不同层面对核心业务系统进行划分，分类分析各个层面中安全控制间存在的关联作用，从系统层面上分析考察单元测评中确定的不符合项对系统整体安全保护能力的影响，及不符合项整改的必要性。

## 安全控制间安全测评

安全控制间安全测评主要对同一区域内、同一层面上的不同安全控制间存在的功能增强、补充或削弱等关联作用进行测评，同时，也包括对《基本要求》的要求项与同一区域、同一层面上的非《基本要求》要求的安全控制之间的安全测评。依据不同层面对系统进行划分，分类分析各个层面中安全控制间存在的关联作用，从系统层面上分析考察单元测评中确定的不符合项对系统整体安全保护能力的影响，及不符合项整改的必要性。例如：

在物理安全层面中，物理访问控制与防盗窃和防破坏两个控制点之间具有增强的关系，通常可以通过物理层面上的物理访问控制来增强其安全防盗窃功能等。在网络安全层面中，网络访问控制和边界完整性检查两个控制点之间具有互补和削弱的关系，通常来讲，通过进行边界完整性检查可以检查发现网络访问控制被旁路的可能性。

## 层面间安全测评

层面间安全测评主要考虑同一区域内的不同层面之间存在的功能增强、补充和削弱等关联作用。在进行层面间安全测评时，可以考虑不同层面的两个不同安全控制，也可以同时考虑两个以上不同安全控制的相互作用。对于系统不同层面间相配合的保护措施，需要结合不同层面的安全控制点分析其相互之间存在的关联作用，从而确定某些不符合项对系统整体安全保护能力的影响。例如：

如网络设备防护不符合要求（口令强度不够），该测评项为不符合项，如果网络设备的防护只允许本地登录管理或者限制只能在相应区域内的管理主机上进行网络设备管理，则有可能通过物理安全的访问控制来加强网络设备自身安全防护能力（身份鉴别部分）。

## 区域间安全测评

区域间安全测评主要考虑互连互通（包括物理上和逻辑上的互连互通等）的不同区域之间存在的安全功能增强、补充和削弱等关联作用，特别是有数据交换的两个不同区域。一般边界区域都会和内部某个或某些区域之间发生数据交换；内部不同区域之间也可能因为业务的需要而发生数据交换，需要重点测评这些区域之间的关联作用。

## 系统结构安全测评

系统结构安全测评主要考虑信息系统整体结构的安全性和整体安全防范的合理性。系统结构安全测评的测评范围是整个信息系统，包括被测系统与其他信息系统系统边界之间的安全测评。信息系统整体结构的安全性主要是指从安全的角度，分析信息系统整体结构的安全性（从安全角度看系统）。整体安全防范的合理性主要是指从系统的角度，分析信息系统安全防范的合理性（以系统的观点看安全防范（体系））。

从系统整体结构层面分析系统的安全防范能力，对于外部安全威胁的防范主要可以从物理环境保护、系统网络访问控制和系统外联边界控制等几个方面考虑：在物理环境层面上，确保系统所在的中心机房的物理安全和物理访问控制，严格限制非法人员直接进入机房环境或非法设备通过机房环境直接连入系统；在系统网络层面上，保证系统网络访问控制能力，限制设备访问，防范非法设备从内部接入系统；在系统外联边界上，通过各种防护手段（防火墙、路由控制等）和限制外联的通路（只存在与其它可控安全系统的连接，不存在直接接入Internet或拨号连出的情况），增强系统的安全保护能力。这几个方面的保护措施相结合，可以对系统进行综合保护，从而确保系统内部安全。整体安全防范的合理性，基于目前部署的安全体系，分析安全设备（如防火墙、防病毒）和安全配置（如访问控制列表）在目前系统中部署是否合理，是否符合成本－效益原则，是否存在重复投资和冗余配置，是否在启用安全措施的同时对系统性能和实际业务需求带来较大负面影响。

# 项目组织与实施

## 项目组织

为了保证项目的顺利实施，确保项目质量达到预期目标，上海交通大学(信息安全服务技术研究实验室)将成立项目实施组，以利于加强项目管理和各方面协调合作，使工作和责任更加清晰明确。

项目组组长

质量监督人

技术测试组

管理评估组

渗透测试组

表 8‑1 项目实施组成员表

|  |  |  |  |
| --- | --- | --- | --- |
| **项目组长** | 李海燕 | **质量监督人** | 朱赟 |
| **技术测试组人员** | 段圣雄，王栋、金俊 | | |
| **管理评估组人员** | 李海燕、苏钰琪 | | |
| **渗透测试组人员** | 赵海 | | |

**项目组组长：**负责项目具体实施和管理，制定项目实施计划，掌握项目的每个实施过程，解决项目实施中出现的各种具体问题，项目变化的管理，风险管理，与客户进行及时有效的沟通，定期向用户反馈项目进展情况。

**技术测试组：**负责项目具体的技术测试实施，如网络平台测试、系统平台测试、业务应用测试等，定期向测评组组长反馈技术测试进展情况。

**管理评估组：**负责项目具体的安全管理的评估，实施现场访谈、制度核查、执行记录查阅等，定期向测评组组长反馈管理评估进展情况。

**渗透测试组：**负责汇总技术测试中发现的安全隐患，针对发现的安全漏洞，选择适当的攻击工具及方法，模拟入侵行为。

**质量监督人：**对项目实施全过程的质量监控，动态监控质量体系执行情况，对违反质量管理规范的情况提出改进或否决意见，及时出具质量监控报告或意见。

## 进度安排

下表是项目现场实施的工作周期以及各阶段输出结果，具体的项目进度安排计划将由双方在项目启动会议上由双方确认。

表 8‑2 系统安全测评项目进度表

| **实施项目** | **实施细目** | **测评周期（天）** | **备注** |
| --- | --- | --- | --- |
| **一、测评准备过程** | | 0 |  |
| 现场调查 | | 0 | 需要系统管理员配合访谈 |
| 工具和文档准备 | | 0 |  |
| **第一阶段输出结果：《测评系统基本情况调查报告》** | | | |
| **二、方案编制过程** | | 0 |  |
| 方案及计划制定审核 | | 0 |  |
| **第二阶段输出结果：《系统安全测评方案》、《系统安全测评现场实施计划》** | | | |
| **三、现场实施过程** | | 0 |  |
| 首次会议 | 确认方案和计划，协调测评资源 | 0 | 需要系统方运行相关人员参与 |
| 安全物理环境 | 机房环境 | 0 | 需要机房管理员配合 |
| 安全通信网络 | 网络结构分析 | 0 | 以核查配置文件为主，需要网络管理员配合 |
| 安全区域边界 | 区域边界 | 0 |  |
| 安全计算环境 | 操作系统核查 | 0 | 以核查配置文件为主，需要系统管理员配合；核查并验证安全功能的实现，需要应用系统管理员配合；访谈需要应用系统管理员或开发人员配合 |
| 数据库核查 |
| 终端设备核查 |
| 安全设备核查 |
| 应用安全核查 |
| 数据安全核查分析 |
| 数据安全验证测试 |
| 验证测试 |
| 安全管理中心 | 安全管理中心 | 0 | 以核查配置文件为主，需要系统管理员配合 |
| 安全管理 | 安全管理制度 | 0 | 以核查配置文件为主，需要系统管理员配合 |
| 安全管理机构 |
| 安全管理人员 |
| 安全建设管理 |
| 安全运维管理 |
| 漏洞扫描 | 操作系统 | 0 | 需要系统管理员配合测试 |
| 数据库 |
| 渗透性测试 | 模拟从Ineternet非授权访问系统 | 0 | 需要网络管理员、系统管理员配合测试 |
| 测试结果初步分析 | | 0 |  |
| 末次会议 | 测评结果交流确认、结果审核 | 0 | 需要系统方运行相关人员参与并确认测评结果 |
| **第三阶段输出结果：《系统安全测评记录表》** | | | |
| **四、分析与报告编制过程** | | 0 |  |
| 测评报告书写 | | 0 |  |
| 测评报告审核及签发 | | 0 |  |
| **第四阶段输出结果：《系统安全测评报告》** | | | |
| **总计** | | 0 | 测评实施阶段工作可根据现场情况并行操作 |

# 配合需求

1. 人员配合要求

表 9‑1 配合人员列表

| **配合项目** | **需求说明** |
| --- | --- |
| 总体协调人 | 能够进行各种工作的跨部门组织协调的人员 |
| 网络管理人员 | 对系统的网络架构、网络设备、安全设备、管理平台部署情况较为熟悉的人员，现场配合检查组中网络组人员完成网络方面的测评和调研工作。 |
| 系统管理人员 | 对系统中的各类主机的操作系统、数据库系统、各类数据备份等情况较为熟悉的人员，现场配合检查组中主机组人员完成主机和部分数据测评工作。 |
| 应用系统开发  /运维人员 | 负责各类应用系统情况、熟悉各类应用在系统中实际部署情况的人员，现场配合检查组中应用组人员完成应用的检查工作。 |
| 机房管理人员 | 负责机房管理的人员，现场配合检查组中管理组完成物理安全测评工作。 |
| 安全文档维护人员 | 对所有相关的文档进行整理和管理的人员，现场配合检查组中管理组完成管理测评工作。 |

1. 扫描测试配合要求

表 9‑2 扫描测试配合要求列表

| **配合项目** | **需求说明** |
| --- | --- |
| 配合人员 | 网络管理员，提供：  1、（对于每个接入点）可用的以太网电口以及对应的合法IP地址；  2、监控网络设备的运行状态。 |
| 主机及业务应用管理员，负责在漏洞扫描期间监控相关主机以及业务应用的运行状态。 |
| 安全权限 | 如接入测评设备时需出入机房，则需要测评人员在测评实施期间出入机房的许可。 |
| 针对 WEB 扫描，需要能够访问目标应用所有应用页面的用户权限。 |

1. 文档资料配合要求

表 9‑3 文档资料配合要求列表

| **文档名称** | **具体说明** |
| --- | --- |
| 各类管理制度文档 | 管理制度、工作单 |
| 其他文档 | 应用系统设计、开发文档 |

4) 现场工作环境配合要求

* 相对独立的办公环境，可以容纳 6-8 人左右；
* 工具测试接入及办公电脑互联网接入；
* 提供一个保险柜，用于保存工作中的各类过程文档，以防止丢失；
* 提供一台打印机和打印纸，以便文档的输出。

1. 安全类对应基本要求中的安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理和安全运维管理等10个安全要求类别。 [↑](#footnote-ref-1)
2. 安全控制点是对安全类的进一步细化，在《基本要求》目录级别中对应安全类的下一级目录。 [↑](#footnote-ref-2)