温州瓯江通道建设有限公司

网络安全等级保护差距分析报告

被测单位： 温州瓯江通道建设有限公司

被测系统： 监控系统

报告时间： 2019 年 05 月 28 日

信息系统基本信息表

信息系统					
系统名称	监控系统			**安全保护等级**	三级
被测单位					
单位名称	温州瓯江通道建设有限公司				
单位地址	温州市永嘉县三江街道罗溪村南岩殿(温州北收费站管理中心)			**邮政编码**	325101
联系人	姓名	吕成洲	职务/职称	系统管理员	
	所属部门	温州北管理中心	办公电话	0577-67919270	
	移动电话	18958855597	电子邮件	307210063@qq.com	
测评单位					
单位名称	杭州安信检测技术有限公司			**单位代码**	DJCP2010330088
通信地址	浙江省杭州市滨江区长河路 590 号 4 幢 2 楼 A1-A18、B1-B12 座			**邮政编码**	310052
联系人	姓名	吴智渊	职务/职称	销售经理	
	所属部门	销售部	办公电话	0571-87759285	
	移动电话	15158109776	电子邮件	wzy@axjc.net	
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		

声明

本报告是温州瓯江通道建设有限公司监控系统的技术层面的差距分析报告。

本报告差异分析结果的有效性建立在被测单位提供相关证据的真实性基础之上。

本报告中给出的差异分析结构仅对被测信息系统当时的安全状态有效。当检测工作完成后，由于信息系统发生变更而涉及到的系统构成组件（或子系统）都应重新进行检测，本报告不再适用。

本报告中给出的差距分析结果不能作为对信息系统内部署的相关系统构成组件（或产品）的差距分析结果。

在任何情况下，若需引用本报告中的差距分析结果都应保持其原有的意义，不得对相关内容擅自进行增加、修改和伪造或掩盖事实，不得部分复制本报告，复制本报告未重新加盖本公司检测专用章或公司章无效。

杭州安信检测技术有限公司（加盖单位公章）

2019 年 05 月

目录

1 检测项目概述

1.1 测评目的

本项目是温州瓯江通道建设有限公司网络安全差距分析工作的重要内容。

杭州安信检测技术有限公司受温州瓯江通道建设有限公司的委托，根据温州瓯江通道建设有限公司监控系统定级结果情况，从《信息系统安全等级保护基本要求》（GB/T 22239-2008）中选择相应等级的测评指标，结合温州瓯江通道建设有限公司监控系统的构成特点，确定具体的检测对象，通过访谈、检查和测试等方式判断其安全技术和安全管理的各个方面对测评指标的符合程度，判断被测系统的安全保护能力是否满足国家信息系统安全等级保护要求，找出与国家标准要求之间的差距。根据检测结果出具网络安全等级保护差距分析报告，作为后续安全整改的依据，帮助其达到信息系统安全等级保护三级要求。

1.2 检测依据

《网络安全技术 信息系统安全等级保护基本要求》（GB/T 22239-2008）

1.3 各阶段主要任务

差距分析基本测评过程分为四个：检测准备过程、方案编制过程、检测实施过程、分析及报告编制过程。而检测双方之间的沟通与洽谈应贯穿整个差距分析过程。

检测准备过程

对温州瓯江通道建设有限公司监控系统进行前期调查，掌握信息系统的详细情况，并确定检测对象；根据信息系统的实际情况准备现场检测表与测试工具。

方案编制过程

编制与温州瓯江通道建设有限公司监控系统相适应的检测内容及实施方法。

检测实施过程

按照检测方案的总体要求，严格执行检测实施手册，分步实施所有检测项目；通过单项检测和系统整体检测两个方面，了解系统的真实保护情况，获取足够证据，发现系统存在的安全问题。

分析与报告编制过程

根据现场检测结果和相关标准的有关要求，通过单项检测结果判定和系统整体检测分析等方法，分析整个系统的安全保护现状与相应等级的保护要求之间的差距，综合评价被测信息系统保护状况，并形成差距分析报告文本。

1.4 工作时间节点

检测准备阶段	2019-3-22 至 2019-3-23
方案编制阶段	2019-3-24 至 2019-3-25
检测实施阶段	2019-3-26 至 2019-3-28
报告编制阶段	2019-3-29 至 2019-5-18

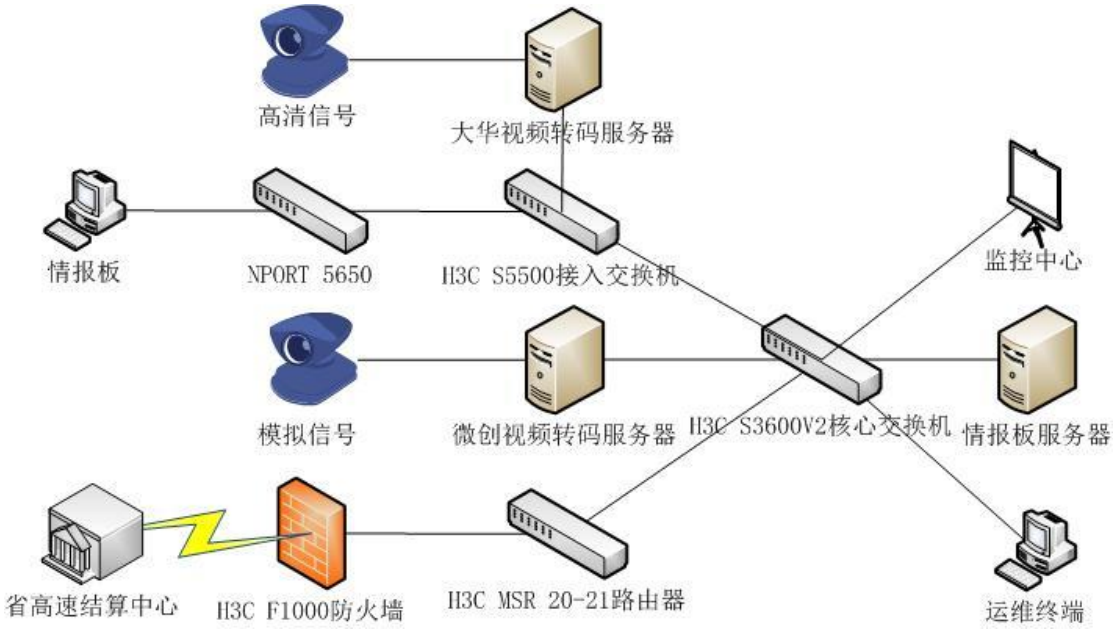
1.5 报告分发范围

本报告一式两份，一份提交被测单位、一份由检测单位留存。

3 被测信息系统情况

3.1 网络基础层描述

温州北管理中心内部部署有路由器、接入交换机、核心交换机、防火墙等设备。在核心交换机与大华视频转码服务器、情报板的链路上部署有接入交换机。微创视频转码服务器、情报板服务器、运维终端和监控中心设备直接核心交换机。省高速结算中心通过防火墙、路由器接入核心交换机。网络拓扑结构如下:



3.2 系统资产

3.2.1 机房

以列表形式给出被测信息系统的部署机房。

序号	机房名称	物理位置
1	视频监控中心	浙江省温州市永嘉县温州北收费站

3.2.2 网络设备

以列表形式给出被测信息系统中的网络设备。

序号	设备名称	操作系统	品牌	型号	用途	数量（台/套）	重要程度
1	核心交换机	Comware	H3C	S3600V2	核心数据交换	1	关键
2	路由器	Comware	H3C	MSR 20-21	出口路由转发	1	重要
3	接入交换机	Comware	H3C	S5500	数据交换	1	重要

3.2.3 安全设备

以列表形式给出被测信息系统中的安全设备。

序号	设备名称	操作系统	品牌	型号	用途	数量（台/套）	重要程度
1	防火墙	Comware	H3C	F1000	安全防护	1	关键

3.2.4 服务器

以列表形式给出被测信息系统中的服务器和存储设备，描述服务器和存储设备的项目包括设备名称、操作系统、数据库管理系统以及承载的业务应用软件系统。

序号	设备名称	操作系统/数据库管理系统	版本	业务应用软件	数量（台/套）	重要程度
1	情报板服务器	Windows 2008 R2/SQL server2008	2008 R2	\	1	关键
2	微创视频转码服务器	Red Hat Enterprise Linux 6.3	Red Hat Enterprise Linux 6.3	VAM 视频监控系统	1	关键
3	大华视频转码服务器	Linux Red Hat 4.4	Red Hat 4.4	Digital Surveillance System	1	重要

3.2.5 终端

以列表形式给出被测信息系统中的终端，包括业务管理终端、业务终端和运维终端等。

序号	设备名称	操作系统	用途	数量（台/套）	重要程度
1	运维终端	windows 7 旗舰版	管理运维	若干	重要

3.2.6 业务应用软件

以列表的形式给出被测信息系统中的业务应用软件（包括含中间件等应用平台软件），描述项目包括软件名称、主要功能简介。

序号	软件名称	主要功能	开发厂商	重要程度
1	Digital Surveillance System	主要提供道路实时预览、录像回放、电子地图、报警管理、视频上墙、语音对讲、车辆查询和行为分析等功能。	浙江大华技术股份有限公司	关键
2	VAM 视频监控系统	主要提供视频调度、串口透传数据调度和音频数据调度。	武汉微创光电股份有限公司	关键
3	诸永高速温州延伸段监控系统	主要提供路段监控，情报板显示内容更改等功能。	武汉微创光电股份有限公司	关键

3.2.7 关键数据类型

以列表形式描述具有相近业务属性（如鉴别数据、管理信息和业务数据等，而业务数据可从安全防护需求（保密、完整等）的角度进一步细分）和安全需求（如保密性、完整性、可用性）的数据集合。

序号	数据类别	所属业务应用	安全防护需求	重要程度
1	系统业务信息	监控系统	完整性、保密性、可用性	关键
2	系统鉴别信息	监控系统	保密性、可用性	关键

3.2.8 安全相关人员

以列表形式给出与被测信息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。

序号	姓名	岗位/角色	联系方式

序号	姓名	岗位/角色	联系方式
1	吕成洲	系统管理员	18958855597

4 检测范围与方法

4.1 检测指标

依据信息系统确定的业务网络安全保护等级和系统服务安全保护等级，选择《基本要求》中对应级别的安全要求作为等级测评的基本指标。

安全层面	安全控制点	测评项数
物理安全	物理位置的选择	2
	物理访问控制	4
	防盗窃和防破坏	6
	防雷击	3
	防火	3
	防水和防潮	4
	防静电	2
	温湿度控制	1
	电力供应	4
	电磁防护	3
网络安全	结构安全	7
	访问控制	8
	安全审计	4
	边界完整性检查	2
	入侵防范	2
	恶意代码防范	2
	网络设备防护	8
主机安全	身份鉴别	6
	访问控制	7

安全层面	安全控制点	测评项数
	安全审计	6
	剩余信息保护	2
	入侵防范	3
	恶意代码防范	3
	资源控制	5
应用安全	身份鉴别	5
	访问控制	7
	安全审计	4
	剩余信息保护	2
	通信完整性	1
	通信保密性	2
	抗抵赖	2
	软件容错	2
	资源控制	7
数据安全与备份恢复	数据完整性	2
	数据保密性	2
	备份和恢复	4
安全管理制度	管理制度	\
	制定和发布	\
	评审和修订	\
安全管理机构	岗位设置	\
	人员配备	\
	授权和审批	\
	沟通和合作	\
	审核和检查	\
人员安全管理	人员录用	\
	人员离岗	\

安全层面	安全控制点	测评项数
	人员考核	\
	安全意识教育和培训	\
	外部人员访问管理	\
系统建设管理	系统定级	\
	安全方案设计	\
	产品采购和使用	\
	自行软件开发	\
	外包软件开发	\
	工程实施	\
	测试验收	\
	系统交付	\
	系统备案	\
	等级测评	\
	安全服务商选择	\
系统运维管理	环境管理	\
	资产管理	\
	介质管理	\
	设备管理	\
	监控管理和安全管理中心	\
	网络安全管理	\
	系统安全管理	\
	恶意代码防范管理	\
	密码管理	\
	变更管理	\
	备份与恢复管理	\
	安全事件处置	\
	应急预案管理	\

4.2 检测对象

4.2.1 机房

序号	机房名称	物理位置	重要程度
1	视频监控中心	浙江省温州市永嘉县温州北收费站	关键

4.2.2 网络设备

序号	设备名称	操作系统	用途	重要程度
1	核心交换机	Comware	核心数据交换	关键
2	路由器	Comware	省财政厅出口路由转发	重要
3	接入交换机	Comware	数据交换	重要

4.2.3 安全设备

序号	设备名称	操作系统	用途	重要程度
1	防火墙	Comware	安全防护	关键

4.2.4 服务器/存储设备

序号	设备名称	操作系统/数据库管理系统	业务应用软件	重要程度
1	情报板服务器	Windows 2008 R2/SQL server2008	\	关键
2	微创视频转码服务器	Red Hat Enterprise Linux 6.3	VAM 视频监控系统	关键
3	大华视频转码服务器	Linux Red Hat 4.4	Digital Surveillance System	关键

4.2.5 终端

序号	设备名称	操作系统	用途	重要程度
1	运维终端	windows 7 旗舰版	管理运维	重要

4.2.6 数据库管理系统

序号	数据库系统名称	版本	所在设备名称	重要程度
1	SQL server	2008	情报板服务器	关键

4.2.7 业务应用软件

序号	软件名称	主要功能	开发厂商	重要程度
1	Digital Surveillance System	主要提供道路实时预览、录像回放、电子地图、报警管理、视频上墙、语音对讲、车辆查询和行为分析等功能。	浙江大华技术股份有限公司	关键
2	VAM 视频监控系统	主要提供视频调度、串口透传数据调度和音频数据调度。	武汉微创光电股份有限公司	关键
3	诸永高速温州延伸段监控系统	主要提供路段监控，情报板显示内容更改等功能。	武汉微创光电股份有限公司	关键

4.2.8 访谈人员

序号	姓名	岗位/职责
1	吕成洲	系统管理员

4.3 检测方法

现场检测方法主要包括访谈、检查和测试等三类，可细分为人员访谈配置核查、现场观测和工具测试等。主要工作过程如下：

1) 使用问卷调查表调阅，对温州瓯江通道建设有限公司信息系统进行初步的系统调研，掌握信息系统的主要功能和业务流程。

2) 采用主机和网络设备配置核查表，从技术角度对主机和网络设备的安全有效性进行手工配置检查。

3) 在用户许可的情况下，对温州瓯江通道建设有限公司信息系统的关键设备和关键系统进行安全漏洞扫描，对网络拓扑结构进行合理性分析，对应用系统进行安全性分析。

5 以下是标准对照（差距分析结果记录）：

5.1 物理安全

5.1.1 信息机房

（一）物理位置的选择

具体要求	现状	差异
a）机房和办公场地应选择在具有防震、防风和防雨等能力的建筑内；	机房位于温州北收费站管理中心 1 层，办公场地位于温州北收费站管理中心 1 层，具有防震、防风、防雨能力。	无差异。
b）机房场地应避免设在建筑物的高层或地下室，以及用水设备的下层或隔壁。	机房位于温州北收费站管理中心 1 层，不在用水设备的下层或隔壁。	无差异。

（二）物理访问控制

具体要求	现状	差异
a）机房出入口应安排专人值守，控制、鉴别和记录进入的人员；	机房有 1 个出入口，已设置电子门禁并安排专人值守。人员进入机房需填写《监控中心来访登记表》，内容包括：日期、入机房时间、出机房时间、姓名、单位名称、人数、工作事由等。	无差异。

b）需进入机房的来访人员应经过申请和审批流程，并限制和监控其活动范围；	来访人员进入机房未经书面审批流程。来访人员进入机房需由监控中心系统管理员全程陪同。	来访人员进入机房未经书面审批流程
c）应对机房划分区域进行管理，区域和区域之间设置物理隔离装置，在重要区域前设置交付或安装等过渡区域；	未对机房划分区域进行管理。	未对机房划分区域进行管理。
d）重要区域应配置电子门禁系统，控制、鉴别和记录进入的人员。	机房出入口已部署电子门禁，能对进出机房的人员进行控制、鉴别和记录。	无差异。

（三）防盗窃和防破坏

具体要求	现状	差异
a）应将主要设备放置在机房内；	主要设备固定在机柜内，放置在机房中。	无差异。
b）应将设备或主要部件进行固定，并设置明显的不易除去的标记；	主要设备固定在机柜内，设置了不易除去的白色标签，标签内容包括名称、编号、起点和终点等。	无差异。
c）应将通信线缆铺设在隐蔽处，可铺设在地下或管道中；	通信线缆敷设在防静电地板下方的管道中。	无差异。
d）应对介质分类标识，存储在介质库或档案室中；	目前未使用移动存储介质，重要纸质文档按照档案分类，通过档案盒进行标识，统一归档至档案室。	无差异。

e）应利用光、电等技术设置机房防盗报警系统；	机房未设置防盗报警系统。	机房未设置防盗报警系统。
f）应对机房设置监控报警系统。	机房未设置监控报警系统。	机房未设置监控报警系统。

（四）防雷击

具体要求	现状	差异
a）机房建筑应设置避雷装置；	机房建筑已设置避雷针。	无差异。
b）应设置防雷保安器，防止感应雷；	机房未设置防雷保安器。	机房未设置防雷保安器。
c）机房应设置交流电源地线。	已设置交流电源地线。	无差异。

（五）防火

具体要求	现状	差异
a）机房应设置火灾自动消防系统，能够自动检测火情、自动报警，并自动灭火；	机房已设置灭火设备：手提式二氧化碳灭火器和手推式干粉灭火器。二氧化碳灭火设备压力正常，但手推式干粉灭火器不适宜用于扑灭机房火灾。机房无火灾自动消防系统。	机房无火灾自动消防系统。
b）机房及相关的工作房间和辅助房应采用具有耐火等级的建筑材料；	机房未采用具有耐火等级的建筑材料。	机房未采用具有耐火等级的建筑材料。
c）机房应采取区域隔离防火措施，将重要设备与其他设备隔离开。	机房未采取区域隔离防火措施。	机房未采取区域隔离防火措施。

（六）防水和防潮

具体要求	现状	差异
a）水管安装，不得穿过机房屋顶和活动地板下；	机房四周无水管穿过。	无差异。
b）应采取措施防止雨水通过机房窗户、屋顶和墙壁渗透；	机房有窗户，采用双层密封玻璃窗，目前未开启。机房不位于顶层，目前暂无雨水渗透隐患。	无差异。
c）应采取措施防止机房内水蒸气结露和地下积水的转移与渗透；	未采取措施防止水蒸气结露。未采取措施防止地下积水转移。	未采取措施防止水蒸气结露。未采取措施防止地下积水转移。
d）应安装对水敏感的检测仪表或元件，对机房进行防水检测和报警。	未对机房进行漏水检测和报警。	未对机房进行漏水检测和报警。

（七）防静电

具体要求	现状	差异
a）主要设备应采用必要的接地防静电措施；	机柜已接地。	无差异
b）机房应采用防静电地板。	机房已采用防静电地板。	无差异

（八）温湿度控制

具体要求	现状	差异

a）机房应设置温、湿度自动调节设施，使机房温、湿度的变化在设备运行所允许的范围之内。	机房部署有 1 台美的冷静星 KFR-120LW/SDY-PA400 空调，具有调节温度的功能，目前运行正常，设定温度为 21℃。但不具备湿度调节功能。	机房不具备湿度调节功能。

（九）电力供应

具体要求	现状	差异
a）应在机房供电线路上配置稳压器和过电压防护设备；	通过施耐德 MGE Galaxy 300i UPS 和 SVC-30kVA 高精度全自动交流稳压器进行智能稳压，但未在机房供电线路上配置过电压防护设备。	未在机房供电线路上配置过电压防护设备。
b）应提供短期的备用电力供应，至少满足主要设备在断电情况下的正常运行要求；	已部署 3 套施耐德 MGE Galaxy 300i UPS。能满足在断电情况下供电 120 分钟。	无差异。
c）应设置冗余或并行的电力电缆线路为计算机系统供电；	未设置冗余或并行的电力电缆线路为计算机系统供电。	未设置冗余或并行的电力电缆线路为计算机系统供电。
d）应建立备用供电系统。	未建立备用供电系统。	未建立备用供电系统。

（十）电磁防护

具体要求	现状	差异

a）应采用接地方式防止外界电磁干扰和设备寄生耦合干扰；	已接地。	无差异
b）电源线和通信线缆应隔离铺设，避免互相干扰；	电源线和通信线缆未隔离铺设，均敷设在防静电地板下方的管道处，无法避免互相干扰。	电源线和通信线缆未隔离铺设。
c）应对关键设备和磁介质实施电磁屏蔽。	采用普通机柜，不具备电磁屏蔽功能。	未对关键设备和磁介质实施电磁屏蔽。

5.1.2 机房差距分析小结

经过对机房的检测，对机房需实现的等级保护 3 级技术要求项共计 32 项，检测结果无差异的占 16，检测结果部分差异的占 3 项。检测结果为有差异的占 13 项。检测结果为不适用的占 0 项。

5.2 网络安全

5.2.1 网络拓扑结构

(一) 网络结构安全

具体要求	现状	差异
a) 应保证主要网络设备的业务处理能力具备冗余空间，满足业务高峰期需要；	在业务高峰时核心交换机的CPU 使用率为 11%,内存使用率为 43%； 防火墙的 CPU 使用率为 5%,内存使用率为 14%；接入交换机的 CPU 使用率为 6%,内存使用率为 67%；路由器的 CPU 使用率为 8%,内存使用率为 73%；能够满足业务高峰期需要。	无差异。
b) 应保证网络各个部分的带宽满足业务高峰期需要；	内部组网带宽为千兆，省高速结算中心光纤接入，满足业务高峰期需求。	无差异。
c) 应在业务终端与业务服务器之间进行路由控制建立安全的访问路径；	采用静态路由协议进行路由访问控制。	无差异。
d) 应绘制与当前运行情况相符的网络拓扑结构图。	已绘制与当前运行情况相符的网络拓扑结构图。	无差异。
e) 应根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段；	该系统服务器与其他系统服务器同一 VLAN。	不同系统的服务器划分在同一网段

f) 应避免将重要网段部署在网络边界处且直接连接外部信息系统，重要网段与其他网段之间采取可靠的技术隔离手段；	在省高速结算中心边界部署了防火墙，但服务器网段与其他网段未隔离。	服务器与其他设备处在同一网段
g) 应按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。	未按业务服务的重要次序分配带宽优先级。	未分配带宽优先级

（二） 边界完整性检查

具体要求	现状	差异
a) 应能够对非授权设备私自联到内部网络的行为进行检查，准确定出位置，并对其进行有效阻断；	未完善非法内联技术。	未完善非法内联技术。
b) 应能够对内部网络用户私自联到外部网络的行为进行检查，准确定出位置，并对其进行有效阻断。	未完善非法外联技术。	未完善非法外联技术。

（三） 入侵防范

具体要求	现状	差异
a) 应在网络边界处监视以下攻击行为：端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等；	未完善入侵检测技术。	未完善入侵检测技术。

b) 当检测到攻击行为时，记录攻击源 IP、攻击类型、攻击目的、攻击时间，在发生严重入侵事件时应提供报警。	未完善入侵检测技术。	未完善入侵检测技术。

（四） 恶意代码防范

具体要求	现状	差异
a) 应在网络边界处对恶意代码进行检测和清除；	未完善防恶意代码技术。	未完善防恶意代码技术。
b) 应维护恶意代码库的升级和检测系统的更新。	未完善防恶意代码技术。	未完善防恶意代码技术。

（五） 网络访问控制

具体要求	现状	差异
a) 应在网络边界部署访问控制设备，启用访问控制功能；	已在省高速结算中心边界部署了防火墙，但未启用访问控制功能。	防火墙未启用访问控制功能
b) 应能根据会话状态信息为数据流提供明确的允许/拒绝访问的能力，控制粒度为端口级；	未按照业务会话配置明确的访问控制策略。	防火墙、核心交换机未配置访问控制策略
c) 应对进出网络的信息内容进行过滤，实现对应用层 HTTP、FTP、TELNET、SMTP、POP3 等协议命令级的控制；	未对进出网络的信息进行过滤。	防火墙、核心交换机未配置访问控制策略
d) 应在会话处于非活跃一定时间或会话结束后终止网络连接；	未限制会话老化时间。	应配置 TCP 超时。

e) 应限制网络最大流量数及网络连接数；	未限制网络最大流量数和连接数。	应限制网络最大流量数及网络连接数。
f) 重要网段应采取技术手段防止地址欺骗；	服务器网段未采取 IP-MAC 地址绑定防止地址欺骗。	重要网段应采取 IP-MAC 地址绑定防止地址欺骗。
g) 应按用户和系统之间的允许访问规则，决定允许或拒绝用户对受控系统进行资源访问，控制粒度为单个用户；	系统无拨号接入用户。	不适用。
h) 应限制具有拨号访问权限的用户数量。	系统无拨号接入用户。	不适用。

5.2.2 核心交换机

(一) 安全审计

具体要求	现状	差异
a) 应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录；	已启用核心交换机的日志功能，对设备的运行情况、网络流量、用户行为进行了日志记录；	无差异。
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；	审计记录内容包括：日期时间、用户、操作、操作结果其他与审计相关的信息；	无差异。
c) 应能够根据记录数据进行分析，并生成审计报表；	未对审计记录进行分析并生成报表。	应根据记录数据进行分析，并生成审计报表。
d) 应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。	审计记录本地保存，不能避免受到未预期的删除、修改或覆盖等。	应对审计记录进行保护。

（二） 网络设备防护

具体要求	现状	差异
a）应对登录网络设备的用户进行身份鉴别；	未对登录设备的用户进行身份鉴别。	应对登录设备的用户进行身份鉴别。
b）应对网络设备的管理员登录地址进行限制；	仅能通过本地登录。	无差异。
c）网络设备用户的标识应唯一；	未设置 console 口登录的用户名和口令。	应设置 console 口登录的用户名和口令。
d）主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别；	未对登录设备的用户进行身份鉴别。	应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别。
e）身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换；	未设置 console 口登录的用户名和口令。	应设置 console 口登录的用户名和口令。口令需满足复杂度要求并定期更换设备的口令。
f）应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；	未配置设备的登录失败处理功能。	应配置设备的登录失败次数和锁定时间。
g）当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；	仅能通过本地登录。	不适用。
h）应实现设备特权用户的权限分离。	未分离设备特权用户的权限分离。	应分为操作员、审计员、安全员等。

5.2.3 路由器

(一) 安全审计

具体要求	现状	差异
a) 应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录；	已启用核心交换机的日志功能，对设备的运行情况、网络流量、用户行为进行了日志记录；	无差异。
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；	审计记录内容包括：日期时间、用户、操作、操作结果其他与审计相关的信息；	无差异。
c) 应能够根据记录数据进行分析，并生成审计报表；	未对审计记录进行分析并生成报表。	应根据记录数据进行分析，并生成审计报表。
d) 应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。	审计记录本地保存，不能避免受到未预期的删除、修改或覆盖等。	应对审计记录进行保护。

(二) 网络设备防护

具体要求	现状	差异
a) 应对登录网络设备的用户进行身份鉴别；	已对登录设备的用户采用用户名口令进行身份鉴别。	无差异。
b) 应对网络设备的管理员登录地址进行限制；	未对网络设备的管理员登录地址进行限制。	应对网络设备的管理员登录地址进行限制。
c) 网络设备用户的标识应唯一；	未设置 console 口登录的用户名和口令。	应设置 console 口登录的用户名和口令。
d) 主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别；	仅采用用户名口令对同一用户进行身份鉴别。	应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别。
e) 身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换；	口令长度 8 位以上，由数字、字母、字符组成，未定期更换口令。	应定期更换设备的口令。

f) 应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；	未配置设备的登录失败处理功能。	应配置设备的登录失败次数和锁定时间。
g) 当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；	采用 telnet 的方式对安全设备进行管理。	应采用加密的方式进行设备远程管理。
h) 应实现设备特权用户的权限分离。	未分离设备特权用户的权限分离。	应分为操作员、审计员、安全员等。

5.2.4 防火墙

（一） 安全审计

具体要求	现状	差异
a) 应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录；	已启用核心交换机的日志功能，对设备的运行情况、网络流量、用户行为进行了日志记录；	无差异。
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；	审计记录内容包括：日期时间、用户、操作、操作结果其他与审计相关的信息；	无差异。
c) 应能够根据记录数据进行分析，并生成审计报表；	未对审计记录进行分析并生成报表。	应根据记录数据进行分析，并生成审计报表。
d) 应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。	审计记录本地保存，不能避免受到未预期的删除、修改或覆盖等。	应对审计记录进行保护。

（二）网络设备防护

具体要求	现状	差异

a) 应对登录网络设备的用户进行身份鉴别；	已对登录设备的用户采用用户名口令进行身份鉴别。	无差异。
b) 应对网络设备的管理员登录地址进行限制；	未对网络设备的管理员登录地址进行限制。	应对网络设备的管理员登录地址进行限制。
c) 网络设备用户的标识应唯一；	未设置 console 口登录的用户名和口令。	应设置 console 口登录的用户名和口令。
d) 主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别；	仅采用用户名口令对同一用户进行身份鉴别。	应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别。
e) 身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换；	口令长度 8 位以上，由数字、字母、字符组成，未定期更换口令。	应定期更换设备的口令。
f) 应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；	未配置设备的登录失败处理功能。	应配置设备的登录失败次数和锁定时间。
g) 当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；	采用 telnet 的方式对安全设备进行管理。	应采用加密的方式进行设备远程管理。
h) 应实现设备特权用户的权限分离。	未分离设备特权用户的权限分离。	应分为操作员、审计员、安全员等。

5.2.5 接入交换机

(一) 安全审计

具体要求	现状	差异

a) 应对网络系统中的网络设备运行状况、网络流量、用户行为等进行日志记录；	已启用核心交换机的日志功能，对设备的运行情况、网络流量、用户行为进行了日志记录；	无差异。
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；	审计记录内容包括：日期时间、用户、操作、操作结果其他与审计相关的信息；	无差异。
c) 应能够根据记录数据进行分析，并生成审计报表；	未对审计记录进行分析并生成报表。	应根据记录数据进行分析，并生成审计报表。
d) 应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等。	审计记录本地保存，不能避免受到未预期的删除、修改或覆盖等。	应对审计记录进行保护。

（二）网络设备防护

具体要求	现状	差异
a) 应对登录网络设备的用户进行身份鉴别；	已对登录设备的用户采用用户名口令进行身份鉴别。	无差异。
b) 应对网络设备的管理员登录地址进行限制；	未对网络设备的管理员登录地址进行限制。	应对网络设备的管理员登录地址进行限制。
c) 网络设备用户的标识应唯一；	未设置 console 口登录的用户名和口令。	应设置 console 口登录的用户名和口令。
d) 主要网络设备应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别；	仅采用用户名口令对同一用户进行身份鉴别。	应对同一用户选择两种或两种以上组合的鉴别技术来进行身份鉴别。
e) 身份鉴别信息应具有不易被冒用的特点，口令应有复杂度要求并定期更换；	口令长度 8 位以上，由数字、字母、字符组成，未定期更换口令。	应定期更换设备的口令。

f) 应具有登录失败处理功能，可采取结束会话、限制非法登录次数和当网络登录连接超时自动退出等措施；	未配置设备的登录失败处理功能。	应配置设备的登录失败次数和锁定时间。
g) 当对网络设备进行远程管理时，应采取必要措施防止鉴别信息在网络传输过程中被窃听；	采用 telnet 和 http 的方式对安全设备进行管理。	应采用加密的方式进行设备远程管理。
h) 应实现设备特权用户的权限分离。	未分离设备特权用户的权限分离。	应分为操作员、审计员、安全员等。

5.2.6 网络差距分析小结

在被测单位信息系统等级保护中需实现的 3 级安全技术要求共有 33 项，检查结果中无差异的占 6 项。检测结果为部分差异的占 4 项。检测结果为有差异的占 21 项。检测结果为不适用的占 2 项。

5.3 主机安全

5.3.1 情报板服务器

（一） 身份鉴别

具体要求	现状	差异
a）应对登录操作系统的用户进行身份标识和鉴别；	通过用户名和口令对操作系统用户进行身份标识和鉴别。数据库采用 Windows 身份验证模式，能对用户进行身份标识和鉴别。	无差异。
b）操作系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换；	已配置 Windows 操作系统密码策略：密码必须符合复杂性要求：已启用，密码长度最小值：0 个字符，密码最长使用期限：42 天，密码最短使用期限：0 天，强制密码历史：0 个记住的密码，用可还原的加密来储存密码：已禁用。目前系统启用的账户有：Administrator，口令为弱口令。未定期更换操作系统用户口令，上次更换密码的时间为 2013/1/14。目前数据库系统启用的账户有：ems2015、ems2015new、sa、zheems，sa 账户和 zheems 账户未勾选“强制实施密码策略”口令设置未满足复杂度要求。	应设置满足复杂度要求的口令，并定期更换。

c）应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；	未配置 Windows 操作系统账户锁定策略。部分 Microsoft SQL Server 账户未勾选“强制实施密码策略”，且未配置 Windows 操作系统账户锁定策略。	应配置账户锁定次数、锁定时间。
d）当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听；	通过 RDP 协议进行远程管理，操作系统版本为 Windows2008 R2，安全层：协商，加密级别：客户端兼容，未设置 Rdp 协议安全层为 SSL。使用 SQL Server 默认远程连接方式进行远程管理。	应采取措施防止操作系统鉴别信息在网络传输过程中被窃听。
e）应为操作系统的不同用户分配不同的用户名，确保用户名具有唯一性；	Windows 中不存在 SID 相同的账户，用户标识具有唯一性。SQL Server 中不存在用户名相同账户，用户标识具有唯一性。	无差异。
f）应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。	仅使用用户名和口令一种鉴别技术对登录服务器的管理用户进行鉴别。	应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。

（二） 访问控制

具体要求	现状	差异

a)应启用访问控制功能，依据安全策略控制用户对资源的访问；	启用了 Windows 操作系统访问控制功能，根据管理人员岗位设置用户权限，目前仅一位管理员使用 administrator 进行管理，已关闭 C$、D$、Admin$等 Windows 默认共享。 启用数据库系统访问控制功能，根据管理员岗位设置账户权限，目前使用 zheems 账户进行管理。已限制应用系统所使用的数据库账户的权限，未授权 DBA 权限。	无差异。
b)应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限；	管理员使用 administrator 账户进行管理，拥有最大权限，未实现操作系统特权用户的权限分离。管理员均使用 zheems 账户进行管理，未实现数据库系统特权用户的权限分离。	应实现特权用户权限的分离。
c)应实现操作系统和数据库系统特权用户的权限分离；	管理员使用 administrator 账户进行管理，拥有最大权限，未实现操作系统特权用户的权限分离。管理员均使用 zheems 账户进行管理，未实现数据库系统特权用户的权限分离。	应实现特权用户权限的分离。
d)应严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令；	已禁用系统默认账户 Guest，已修改 Administrator 默认口令。数据库未禁用无用的默认账户 SA。	应禁用无用的默认账户

e)应及时删除多余的、过期的帐户，避免共享帐户的存在；	目前操作系统中启用的账户有administrator，不存在多余、过期的账户。目前仅有一位管理员，不存在共用账户的现象。数据库存在多余、过期的账户，如SA。目前仅有一位管理员，不存在共用账户的现象。	应删除多余账号。
f)应对重要信息资源设置敏感标记；	未对重要信息资源设置敏感标记。	应对重要信息资源设置敏感标记。
g)应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。	未依据安全策略严格控制用户对有敏感标记重要信息资源的操作。	应对重要信息资源设置敏感标记。

（三） 安全审计

具体要求	现状	差异
a） 审计范围应覆盖到服务器和重要客户端上的每个操作系统用户；	已启用安全审计功能，采用Windows2008R2默认审核策略，审计对象覆盖操作系统上的每个用户。已启用数据库审计功能，对登录事件和操作行为进行记录，审计范围覆盖数据库中所有用户。	无差异。

b）审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；	采用 Windows 2008R2 默认审核策略，对登录、注销、账户锁定、策略更改、系统事件、用户账户管理等进行审计，但未对特权使用进行审计。对 Microsoft SQL Server 用户成功和失败的登录事件以及操作行为进行审计。	合理配置系统审计策略，用户特权使用也应该进行审计。
c）审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；	Windows 审计记录包括时间和日期、任务类别、用户、来源、关键字、事件 ID 等。Microsoft SQL Server 审计记录包括时间和日期、用户、源、消息、事件 ID 等。	无差异。
d）应能够根据记录数据进行分析，并生成审计报表；	未对审计记录进行分析并生成审计报表。	应对审计记录进行分析并生成审计报表。
e）应保护审计进程，避免受到未预期的中断；	无法单独中断 Windows 审计进程。	无差异。
f）应保护审计记录，避免受到未预期的删除、修改或覆盖等。	已合理设置 Windows 日志存储策略，最大日志文件为 100M，按需覆盖。审计记录本地存储，未部署日志服务器或日志审计系统。数据库审计记录本地存储，未部署日志服务器或日志审计系统。	应部署日志服务器或日志审计系统，及时将审计日志转存到此类设备。

（四） 剩余信息包含

具体要求	现状	差异

a)应保证操作系统和数据库管理系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；	未启用“交互式登录：不显示上次登录用户名”。	本地安全选项启用“不显示最后登录的用户名”。
b)应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。	未启用“关机：清除虚拟内存页面文件”。	本地安全选项启用“关机前清除虚拟内存页面”。

（五） 入侵防范

具体要求	现状	差异
a)应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；	主机层面未采取入侵检测措施。	应采取入侵检测措施。
b)应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施；	未对重要程序的完整性进行检测。	应对重要程序的完整性进行检测。

c)操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。	操作系统安装了不必要的程序，如谷歌浏览器，未根据实际应用关闭不必要的服务和端口，如 Print Spooler、Remote Registry、Server、TCP/IP NetBIOS Helper、135、445。未及时更新系统安全补丁，最近补丁安装时间为 2018.5.24，补丁编号为 KB4012212。	应仅安装必要的程序，禁用不必要的服务和端口，并及时更新系统补丁。

（六） 恶意代码防范

具体要求	现状	差异
a) 应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库；	操作系统已安装瑞星 ESM，软件版本 3.0.0.53，特征库版本 30.1121.0001，最近更新时间 2019/3/26，已及时更新恶意代码软件版本和恶意代码库。	无差异。
b)主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库；	网络层未安装防恶意代码软件。	不适用。
c) 应支持恶意代码防范的统一管理。	已安装瑞星 ESM，支持防恶意代码软件的统一管理。	无差异。

（七） 资源控制

具体要求	现状	差异
a)应通过设定终端接入方式、网络地址范围等条件限制终端登录；	仅允许 Windows 远程桌面服务进行管理，但未限制远程登录的地址范围。未限制能够远程登录数据库的地址范围。	应限制远程登录服务器的客户端 IP 地址。

b)应根据安全策略设置登录终端的操作超时锁定；	已设置活动但空间的远程桌面服务会话的时间限制为 15 分钟。已设置 Microsoft SQL Server 数据库连接超时值十五分钟。	无差异。
c)应对重要服务器进行监视，包括监视服务器的 CPU、硬盘、内存、网络等资源的使用情况；	未定期对重要服务器的 CPU、硬盘、内存等使用情况进行监视。	应对重要服务器的 CPU、硬盘、内存等使用情况进行监视。
d)应限制单个用户对系统资源的最大或最小使用限度；	未限制单个账户的资源使用限度。	应限制单个账户的资源使用限度。
e)应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。	未采取措施对系统服务水平进行检测和报警。	应对系统服务水平进行检测和报警。

5.3.2 微创视频转码服务器

（一） 身份鉴别

具体要求	现状	差异
a） 应对登录操作系统的用户进行身份标识和鉴别；	通过用户名和口令对操作系统用户进行身份标识和鉴别。	无差异。

b）操作系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换；	Linux 复杂性策略：未在/etc/pam.d/system-auth 中配置操作系统密码复杂性策略，已为每个账户设置如下参数： PASS_MAX_DAYS 90 PASS_MIN_DAY 0 PASS_MIN_LEN 5 PASS_WARN_AGE 7 目前 root 实际口令由 6 位数字组成，管理员未及时更换口令，root 用户最近口令更改日期：12 月 15, 2014。	应设置满足复杂度要求的口令，并定期更换。
c）应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；	未在/etc/pam.d/system-auth 中配置操作系统账户锁定策略。	应配置账户锁定次数、锁定时间。
d）当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听；	采用 ssh 对服务器进行远程管理。	无差异。
e）应为操作系统的不同用户分配不同的用户名，确保用户名具有唯一性；	不存在 UID 相同的账户，用户标识具有唯一性。	无差异。
f）应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。	仅使用用户名和口令一种鉴别技术对登录服务器的管理用户进行鉴别。	应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。

（二） 访问控制

具体要求	现状	差异

a)应启用访问控制功能，依据安全策略控制用户对资源的访问；	启用了操作系统访问控制功能，根据岗位设置账户权限。已合理设置配置文件权限：/etc/passwd-rw-r--r-- 但未合理设置 Umask 值 ，umask=022。	应合理设置 Umask 值。
b)应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限；	管理员均使用 root 账户进行管理，未实现操作系统特权用户的权限分离。	应实现操作系统特权用户的权限分离。
c)应实现操作系统和数据库系统特权用户的权限分离；	未实现操作系统特权用户的权限分离。	应实现操作系统特权用户的权限分离。
d)应严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令；	已禁用系统默认账户，已修改 root 默认口令。	无差异。
e)应及时删除多余的、过期的帐户，避免共享帐户的存在；	目前操作系统中启用的账户有 root 和 postgres 账户，postgres 为应用账户，不存在多余、过期账户。目前仅有一位管理员，不存在共用账户的现象。	无差异。
f)应对重要信息资源设置敏感标记；	未对重要信息资源设置敏感标记。	应对重要信息资源设置敏感标记。
g)应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。	未依据安全策略严格控制用户对有敏感标记重要信息资源的操作。	应对重要信息资源设置敏感标记。

(三)　安全审计

具体要求	现状	差异

a）审计范围应覆盖到服务器和重要客户端上的每个操作系统用户；	已启用 syslogd 和 auditd 服务，审计范围覆盖操作系统中的所有用户。	无差异。
b）审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；	已启用 Linux syslogd 和 auditd 服务，能够对用户登录、账户管理、重要命令的使用、系统运行状况进行审计。 /etc/rsyslog.conf: *.info;mail.none;authpriv.none; cron.none /var/log/messages authpriv.* /var/log/secure mail.* -/var/log/maillog cron.* /var/log/cron *.emerg * uucp,news.crit /var/log/spooler local7.* /var/log/boot.log /etc/audit/auditd.rules： -D -b 320	无差异。
c）审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；	Linux 审计记录包括事件类型、日期和时间、用户名、UID、命令名称、执行结果等。	无差异。
d）应能够根据记录数据进行分析，并生成审计报表；	未能对日志进行分析，不能生成审计报表。	应对日志进行分析，并能生成审计报表。
e）应保护审计进程，避免受到未预期的中断；	仅 root 账户能够结束审计进程，能够避免未授权的中断。	无差异。

f）应保护审计记录，避免受到未预期的删除、修改或覆盖等。	已合理设置/var/log 下日志文件权限，audit 日志存储策略：num_logs=5、max_log_file=6。审计记录本地存储，未部署日志服务器或日志审计系统。	应保护审计记录，部署日志服务器或日志审计系统。

（四） 剩余信息包含

具体要求	现状	差异
a)应保证操作系统和数据库管理系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；	Linux 满足 TCSEC C2 级	无差异。
b)应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。	Linux 满足 TCSEC C2 级	无差异。

（五） 入侵防范

具体要求	现状	差异
a)应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；	主机层面未采取入侵检测措施。	应采取入侵检测措施。

b)应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施；	未对重要程序的完整性进行检测。	应对重要程序的完整性进行检测。
c)操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。	操作系统仅安装需要的程序和组件，但未根据实际应用关闭不必要的服务和端口，如 rpcbind 111(TCP)、cupsd 631(UDP),未启用 iptables 防火墙。未及时更新系统安全补丁。	应禁用不必要的服务和端口，并及时更新系统补丁。

（六） 恶意代码防范

具体要求	现状	差异
a) 应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库；	操作系统未安装防恶意代码软件。	应安装支持统一管理的的防病毒产品。
b)主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库；	操作系统未安装防恶意代码软件。	应安装支持统一管理的的防病毒产品。
c) 应支持恶意代码防范的统一管理。	操作系统未安装防恶意代码软件。	应安装支持统一管理的的防病毒产品。

（七） 资源控制

具体要求	现状	差异
a)应通过设定终端接入方式、网络地址范围等条件限制终端登录；	未在/etc/hosts.allow、/etc/hosts.deny、iptables、/etc/sshd_config 中对 SSH 的远程登录地址进行限制。	应限制远程登录服务器的客户端 IP 地址。

b)应根据安全策略设置登录终端的操作超时锁定；	未在/etc/profile 中设置 TMOUT 值。	未配置登录超时。
c)应对重要服务器进行监视，包括监视服务器的 CPU、硬盘、内存、网络等资源的使用情况；	未定期对重要服务器的 CPU、硬盘、内存等使用情况进行监视。	应定期对重要服务器的 CPU、硬盘、内存等使用情况进行监视。
d)应限制单个用户对系统资源的最大或最小使用限度；	未限制单个用户对系统资源的使用。	应限制单个账户的资源使用限度。
e)应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。	未采取措施对系统服务水平进行检测和报警。	应采取措施对系统服务水平进行检测和报警。

5.3.3 大华视频转码服务器

（一） 身份鉴别

具体要求	现状	差异
a） 应对登录操作系统的用户进行身份标识和鉴别；	通过用户名和口令对操作系统用户进行身份标识和鉴别。	无差异。
b） 操作系统管理用户身份标识应具有不易被冒用的特点，口令应有复杂度要求并定期更换；	Linux 复杂性策略： 未在/etc/pam.d/password-auth 中配置操作系统密码复杂性策略，目前 root 实际口令为 8 位以上由数字和大小写字母组成，未定期更换操作系统用户口令。	应定期更换系统登录口令。

c）应启用登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；	未在/etc/pam.d/system-auth 中配置操作系统账户锁定策略。	应配置账户锁定次数、锁定时间。
d）当对服务器进行远程管理时，应采取必要措施，防止鉴别信息在网络传输过程中被窃听；	采用 ssh 对服务器进行远程管理。	无差异。
e）应为操作系统的不同用户分配不同的用户名，确保用户名具有唯一性；	不存在 UID 相同的账户，用户标识具有唯一性。	无差异。
f）应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。	仅使用用户名和口令一种鉴别技术对登录服务器的管理用户进行鉴别。	应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。

（二） 访问控制

具体要求	现状	差异
a)应启用访问控制功能，依据安全策略控制用户对资源的访问；	启用了操作系统访问控制功能，根据岗位设置账户权限。已合理设置配置文件的权限：/etc/shadow -r--------、/etc/passwd-rw-r--r--。但未合理设置 Umask 值 ，umask=022。	应合理设置 Umask 值。
b)应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限；	管理员均使用 root 账户进行管理，未实现操作系统特权用户的权限分离。	应实现操作系统特权用户的权限分离。

c)应实现操作系统和数据库系统特权用户的权限分离；	未实现操作系统特权用户的权限分离。	应实现操作系统特权用户的权限分离。
d)应严格限制默认帐户的访问权限，重命名系统默认帐户，修改这些帐户的默认口令；	已禁用系统默认账户，已修改 root 默认口令。	无差异。
e)应及时删除多余的、过期的帐户，避免共享帐户的存在；	目前操作系统中启用的账户有 root 和 admin 户，admin 为应用账户，不存在多余、过期账户。目前仅有一位管理员，不存在共用账户的现象。	无差异。
f)应对重要信息资源设置敏感标记；	未对重要信息资源设置敏感标记。	应对重要信息资源设置敏感标记。
g)应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。	未依据安全策略严格控制用户对有敏感标记重要信息资源的操作。	应对重要信息资源设置敏感标记。

（三） 安全审计

具体要求	现状	差异
a） 审计范围应覆盖到服务器和重要客户端上的每个操作系统用户；	操作系统未开启审计服务。	建议开启操作系统安全审计策略，并对重要系统安全事件及用户操作行为进行日志审计。
b） 审计内容应包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；	操作系统未开启审计服务。	合理配置系统审计策略，对系统关键事件、重要用户行为等进行审计。

c）审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；	操作系统未开启审计服务。	审计记录应包括事件的日期、时间、事件类型、用户（账户、IP 等）、操作内容和结果等。
d）应能够根据记录数据进行分析，并生成审计报表；	操作系统未开启审计服务。	建议通过第三方日志审计管理软件对操作系统日志进行定期分析汇总，并生成报表。
e）应保护审计进程，避免受到未预期的中断；	操作系统未开启审计服务。	建议配置日志服务器或第三方审计系统，对审计记录进行收集和保存。
f）应保护审计记录，避免受到未预期的删除、修改或覆盖等。	操作系统未开启审计服务。	建议合理配置日志文件的访问权限，禁止普通用户访问、修改或删除审计日志。并配置日志服务器或第三方审计系统，对审计记录进行分析和保存，保存时间最好不小于 6 个月。

（四） 剩余信息包含

具体要求	现状	差异
a)应保证操作系统和数据库管理系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；	Linux 满足 TCSEC C2 级	无差异。
b)应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除。	Linux 满足 TCSEC C2 级	无差异。

（五） 入侵防范

具体要求	现状	差异

a)应能够检测到对重要服务器进行入侵的行为，能够记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警；	主机层面未采取入侵检测措施。	应采取入侵检测措施。
b)应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施；	未对重要程序的完整性进行检测。	应对重要程序的完整性进行检测。
c)操作系统应遵循最小安装的原则，仅安装需要的组件和应用程序，并通过设置升级服务器等方式保持系统补丁及时得到更新。	操作系统仅安装需要的程序和组件，但未根据实际应用关闭不必要的服务和端口，如 rpcbind 111(TCP)、cupsd 631(UDP),未启用 iptables 防火墙。未及时更新系统安全补丁。	应禁用不必要的服务和端口，及时更新系统补丁。

（六） 恶意代码防范

具体要求	现状	差异
a) 应安装防恶意代码软件，并及时更新防恶意代码软件版本和恶意代码库；	未采取防恶意代码措施。	应安装支持统一管理的的防病毒产品。
b)主机防恶意代码产品应具有与网络防恶意代码产品不同的恶意代码库；	未采取防恶意代码措施。	应安装支持统一管理的的防病毒产品。
c) 应支持恶意代码防范的统一管理。	未采取防恶意代码措施。	应安装支持统一管理的的防病毒产品。

（七） 资源控制

具体要求	现状	差异
a)应通过设定终端接入方式、网络地址范围等条件限制终端登录；	未在/etc/hosts.allow、/etc/hosts.deny、iptables、/etc/sshd_config 中对 SSH 的远程登录地址进行限制。	应限制远程登录服务器的客户端 IP 地址。
b)应根据安全策略设置登录终端的操作超时锁定；	未在/etc/profile 中设置 TMOUT 值。	未配置登录超时。
c)应对重要服务器进行监视，包括监视服务器的 CPU、硬盘、内存、网络等资源的使用情况；	未定期对重要服务器的 CPU、硬盘、内存等使用情况进行监视。	应定期对重要服务器的 CPU、硬盘、内存等使用情况进行监视。
d)应限制单个用户对系统资源的最大或最小使用限度；	未限制单个用户对系统资源的使用。	应限制单个账户的资源使用限度。
e)应能够对系统的服务水平降低到预先规定的最小值进行检测和报警。	未采取措施对系统服务水平进行检测和报警。	应采取措施对系统服务水平进行检测和报警。

5.3.4 主机差距分析小结

经过对服务器的检测、访谈，对服务器需实现的等级保护 3 级技术要求项共计 32 项，检测结果无差异的占 2 项，检测结果部分差异的占 15 项。检测结果为有差异的占 15 项。检测结果为不适用的占 0 项。

5.4 应用安全

5.4.1 DIGITAL SURVEILLANCE SYSTEM

(一) 身份鉴别

具体要求	现状	差异
a)应提供专用的登录控制模块对登录用户进行身份标识和鉴别；	通过用户和口令方式对用户进行身份标识和鉴别。	无差异。
b)应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别；	未使用两种或两种以上组合的鉴别技术。	应使用两种或两种以上组合的鉴别技术。
c)应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；	已提供用户身份标识唯一性检查功能，不能新建用户名相同的账户。已提供鉴别信息复杂度检查功能，密码需满足以下要求：同时字母和数字，密码长度至少为 8 个字符。	无差异。
d)应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；	未提供登录失败处理功能，经测试输错密码超过 10 次后仍未锁定账户。	应提供账户锁定次数和锁定时间。
e)应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。	已提供用户身份标识唯一性检查、鉴别信息复杂度检查的功能并进行合理配置，但未提供登录失败处理功能。	应提供登陆失败处理功能。

（二） 访问控制

具体要求	现状	差异
a)应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；	已提供访问控制功能，通过角色合理分配账户的权限，角色分为省结算中心和 admin，管理员根据视频通道权限、报警输入通道权限、报警输出通道权限、电视墙权限、门禁权限、卡口设备图片通道权限和设备树展示权限设置不同的管理权限。已根据人同岗位分配合适的角色，如系统管理员为 admin、推送人员为省结算中心。	无差异。
b)访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作；	访问控制的覆盖范围包括不同角色（admin、省结算中心）对实时预览、录像回放、电子地图、报警管理、视频上墙、语音对讲、车辆查询和行为分析等功能的访问。	无差异。
c)应由授权主体配置访问控制策略，并严格限制默认帐户的访问权限；	已授权系统管理员负责分配系统用户的权限，已禁用无用的默认账户。	无差异。
d)应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系；	仅授予推送账户账户实时预览、录像回放和录像下载的权限，满足最小授权原则。但未形成相互制约的关系,如 admin 拥有最高权限。	角色权限应形成制约关系。

e)应具有对重要信息资源设置敏感标记的功能；	未提供对重要信息资源设置敏感标记的功能。	应提供对重要信息资源设置敏感标记的功能。
f)应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。	未提供对重要信息资源设置敏感标记的功能。	应提供对重要信息资源设置敏感标记的功能。

（三） 安全审计

具体要求	现状	差异
a)应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计；	应用系统具有安全审计功能，已覆盖系统中的所有角色（省结算中心、admin），并对登录、登出、实时视频、云台控制、录像回放和下载等事件进行记录。	无差异。
b)应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录；	所有用户均无法中断审计进程，应用系统未提供删除审计记录的功能。	无差异。
c)审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等；	审计记录的内容包括时间、操作用户、IP 地址、设备名称、通道名称、操作、操作内容等。	无差异。
d)应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。	未能根据审计记录生成审计报表。	应提供日志分析功能。

（四） 剩余信息保护

具体要求	现状	差异
a)应保证用户鉴别信息所在的存储空间被释放或再分配	未保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前能得到完全清除，无论这些信息是否存放在硬	应采取技术措施保证用户鉴别信息所在的存储空间在释放或再分配前完全清除。

给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；	盘上还是在内存中。	
b)应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。	未保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。	应采取技术措施保证系统重要信息资源所在的存储空间在释放或再分配前完全清除。

（五） 通信完整性

具体要求	现状	差异
a)应采用密码技术保证通信过程中数据的完整性。	使用 http 进行访问，未采用密码技术对通信过程的数据完整性进行传输。	应采用 HTTPS 协议传输。

（六） 通信保密性

具体要求	现状	差异
a)在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证；	使用 http 进行访问，未对通信双方进行会话初始化验证。	应采用 HTTPS 协议传输。
b)应对通信过程中的整个报文或会话过程进行加密。	使用 http 进行访问，未对通信过程的整改会话或报文进行加密传输。	应采用 HTTPS 协议传输。

（七） 抗抵赖

具体要求	现状	差异
a)应具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能；	未采用数字签名等技术实现抗抵赖功能。	应采用数字签名等技术实现抗抵赖功能。
b)应具有在请求的情况下为数据原发者或接收者提供数	未采用数字签名等技术实现抗抵赖功能。	应采用数字签名等技术实现抗抵赖功能。

据接收证据的功能。		

（八） 软件容错

具体要求	现状	差异
a)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数据格式或长度符合系统设定要求；	已对用户输入数据的长度、格式进行检查，如用户名格式、时间段格式。	无差异。
b)应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。	系统无法保证发生故障时，能够继续提供一部分功能。	建议系统采用集群、热备等方式部署。

（九） 资源控制

具体要求	现状	差异
a)当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；	系统未提供登录超时自动结束会话的功能。	应根据业务需要对系统空闲会话超时时间进行设置。
b)应能够对系统的最大并发会话连接数进行限制；	未对系统的最大并发会话连接数进行限制。	应业务需要对系统允许的最大并发会话数进行限制。
c)应能够对单个帐户的多重并发会话进行限制；	未限制单个账户的多重并发会话登录。	应对单个用户的多重并发会话进行限制。
d)应能够对一个时间段内可能的并发会话连接数进行限制；	未限制系统一段时间内的最大并发连接数。	应根据需要对系统允许的一个时间段内系统最大并发会话数以及一个帐户或进程占用的资源分配阈值进行限制。
e)应能够对一个访问帐户或一个请求进程占用的资源分配最大限额和最小限额；	无法对一个访问帐户或一个请求进程占用的资源分配最大限额和最小限额。	应根据业务需要对一个帐户或进程占用的资源进行最大/最小额度限制。

f)应能够对系统服务水平降低到预先规定的最小值进行检测和报警；	无法对系统服务水平降低到预先规定的最小值进行检测和报警。	建议对系统服务水平进行有效监控，当服务降低到预先规定的最小值时能进行报警。
g)应提供服务优先级设定功能，并在安装后根据安全策略设定访问帐户或请求进程的优先级，根据优先级分配系统资源。	未提供服务优先级设定功能。	建议对访问用户或请求进行的优先级进行划分，并根据优先级合理分配系统资源。

5.4.2 VAM 视频监控系统

(一) 身份鉴别

具体要求	现状	差异
a)应提供专用的登录控制模块对登录用户进行身份标识和鉴别；	通过用户和口令方式对用户进行身份标识和鉴别。	无差异。
b)应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别；	未使用两种或两种以上组合的鉴别技术。	应使用两种或两种以上组合的鉴别技术。
c)应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；	该系统无新建账户的模块，仅一个系统管理员角色。已提供鉴别信息复杂度检查功能，密码需满足以下要求：密码由字母、数字组成，长度 1-16 个字符，字母区分大小写。	无差异。
d)应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；	未提供登录失败处理功能，经测试输错密码超过 10 次后仍未锁定账户。	应提供账户锁定次数和锁定时间。

e)应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。	该系统无新建账户的模块，仅一个系统管理员角色。已提供鉴别信息复杂度检查功能，但未提供登录失败处理功能。	应提供账户锁定次数和锁定时间。

(二) 访问控制

具体要求	现状	差异
a)应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；	该系统无新建账户的模块，仅一个系统管理员角色，无访问控制功能。	应根据安全设计需求，对用户访问系统及相关资源进行控制。
b)访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作；	该系统无新建账户的模块，仅一个系统管理员角色，无访问控制功能。	应根据安全设计需求，对用户访问系统及相关资源进行控制。
c)应由授权主体配置访问控制策略，并严格限制默认帐户的访问权限；	该系统无新建账户的模块，仅一个系统管理员角色，无访问控制功能。	应严格限制默认帐户的访问权限，关闭不必要的默认帐号。
d)应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系；	该系统无新建账户的模块，仅一个系统管理员角色，无访问控制功能。	应根据安全设计需求，对用户访问系统及相关资源进行控制。
e)应具有对重要信息资源设置敏感标记的功能；	未提供对重要信息资源设置敏感标记的功能。	未提供对重要信息资源设置敏感标记的功能。
f)应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。	未提供对重要信息资源设置敏感标记的功能。	未提供对重要信息资源设置敏感标记的功能。

(三)　安全审计

具体要求	现状	差异
a)应提供覆盖到每个用户的安全审计功能,对应用系统重要安全事件进行审计;	应用系统具有安全审计功能，对调度情况和告警事件进行记录，但无操作日志，审计内容不全面。	应对应用系统操作事件进行审计。
b)应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录;	所有用户均无法中断审计进程，应用系统未提供删除审计记录的功能。	无差异。
c)审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等;	审计记录的内容包括调度情况（调度时间、调度员、调度对象、调度内容、调度结果）和告警事件（告警时间、告警节点、告警名称、告警级别、确认状态、确认时间、确认用户）等内容。	无差异。
d)应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。	未能根据审计记录生成审计报表。	应供日志分析功能。

(四)　剩余信息保护

具体要求	现状	差异
a)应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中;	未保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前能得到完全清除，无论这些信息是否存放在硬盘上还是在内存中。	应采取技术措施保证用户鉴别信息所在的存储空间在释放或再分配前完全清除。
b)应保证系统内的文件、目录和数据库记录等资源所在的	未保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给	应采取技术措施保证系统重要信息资源所在的存储空间在释放或再分配前完全清

存储空间被释放或重新分配给其他用户前得到完全清除。	其他用户前得到完全清除。	除。

（五） 通信完整性

具体要求	现状	差异
a)应采用密码技术保证通信过程中数据的完整性。	使用 http 进行访问，未采用密码技术对通信过程的数据完整性进行传输。	应采用 HTTPS 协议传输。

（六） 通信保密性

具体要求	现状	差异
a)在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证；	使用 http 进行访问，未对通信双方进行会话初始化验证。	应采用 HTTPS 协议传输。
b)应对通信过程中的整个报文或会话过程进行加密。	使用 http 进行访问，未对通信过程的整改会话或报文进行加密传输。	应采用 HTTPS 协议传输。

（七） 抗抵赖

具体要求	现状	差异
a)应具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能；	未采用数字签名等技术实现抗抵赖功能。	应采用数字签名等技术实现抗抵赖功能。
b)应具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能。	未采用数字签名等技术实现抗抵赖功能。	应采用数字签名等技术实现抗抵赖功能。

（八） 软件容错

具体要求	现状	差异
a)应提供数据有效性检验功	已对用户输入数据的长度、	无差异。

能，保证通过人机接口输入或通过通信接口输入的数据格式或长度符合系统设定要求；	格式进行检查，如用户名格式、时间段格式。	
b)应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。	系统无法保证发生故障时，能够继续提供一部分功能。	建议系统采用集群、热备等方式部署。

（九） 资源控制

具体要求	现状	差异
a)当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；	系统未提供登录超时自动结束会话的功能。	应根据业务需要对系统空闲会话超时时间进行设置。
b)应能够对系统的最大并发会话连接数进行限制；	未对系统的最大并发会话连接数进行限制。	应业务需要对系统允许的最大并发会话数进行限制。
c)应能够对单个帐户的多重并发会话进行限制；	未限制单个账户的多重并发会话登录。	应对单个用户的多重并发会话进行限制。
d)应能够对一个时间段内可能的并发会话连接数进行限制；	未限制系统一段时间内的最大并发连接数。	应根据需要对系统允许的一个时间段内系统最大并发会话数以及一个帐户或进程占用的资源分配阈值进行限制。
e)应能够对一个访问帐户或一个请求进程占用的资源分配最大限额和最小限额；	无法对一个访问帐户或一个请求进程占用的资源分配最大限额和最小限额。	应根据业务需要对一个帐户或进程占用的资源进行最大/最小额度限制。
f)应能够对系统服务水平降低到预先规定的最小值进行检测和报警；	无法对系统服务水平降低到预先规定的最小值进行检测和报警。	建议对系统服务水平进行有效监控，当服务降低到预先规定的最小值时能进行报警。
g)应提供服务优先级设定功能，并在安装后根据安全策略	未提供服务优先级设定功能。	建议对访问用户或请求进行的优先级进行划分，并根据优先级合理分配系统资源。

设定访问帐户或请求进程的优先级，根据优先级分配系统资源。		

5.4.3 诸永高速温州延伸段监控系统

(一) 身份鉴别

具体要求	现状	差异
a)应提供专用的登录控制模块对登录用户进行身份标识和鉴别；	通过用户和口令方式对用户进行身份标识和鉴别。	无差异。
b)应对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别；	未使用两种或两种以上组合的鉴别技术。	应使用两种或两种以上组合的鉴别技术。
c)应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；	已提供用户身份标识唯一性检查功能，不能新建用户名相同的账户。未提供鉴别信息复杂度检查功能。	应提供鉴别信息复杂度检查功能。
d)应提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；	未提供登录失败处理功能，经测试输错密码超过 10 次后仍未锁定账户。	应提供账户锁定次数和锁定时间。
e)应启用身份鉴别、用户身份标识唯一性检查、用户身份鉴别信息复杂度检查以及登录失败处理功能，并根据安全策略配置相关参数。	已提供用户身份标识唯一性检查功能并进行合理配置，但未提供鉴别信息复杂度检查、登录失败处理功能。	应提供鉴别信息复杂度检查功能和登录失败处理功能，并合理配置。

（二） 访问控制

具体要求	现状	差异
a)应提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；	已提供访问控制功能，通过角色合理分配账户的权限，角色分为超级用户、监控中心-监控班长、监控中心-监控员、省中心-系统管理员、省中心-信息发布员，超级用户根据运行管理、资源管理、智能分析、业务通讯、大屏管理、事件管理预案管理等模块设置不同的管理权限。已根据人员岗位分配合适的角色，如管理员为超级用户，普通监控员为监控中心-监控员。	无差异。
b)访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作；	访问控制的覆盖范围包括不同角色（超级用户、监控中心-监控班长、监控中心-监控员等）对资源管理、智能分析、业务通讯、大屏管理、事件管理预案管理等功能的访问。	无差异。
c)应由授权主体配置访问控制策略，并严格限制默认帐户的访问权限；	已授权管理员负责分配系统用户的权限，已禁用无用的默认账户。	无差异。
d)应授予不同帐户为完成各自承担任务所需的最小权限，	仅授予事件管理-角色权限查看日志和管理用户的权限，	超级管理员账号具有所有权限，未形成制约关系。

并在它们之间形成相互制约的关系；	监控中心系统管理员无业务通讯中 的模板管理等权限，满足最小授权原则。但未形成相互制约的关系,如超级用户拥有最高权限。	
e)应具有对重要信息资源设置敏感标记的功能；	未提供对重要信息资源设置敏感标记的功能。	应提供对重要信息资源设置敏感标记的功能。
f)应依据安全策略严格控制用户对有敏感标记重要信息资源的操作。	未提供对重要信息资源设置敏感标记的功能。	应提供对重要信息资源设置敏感标记的功能。

(三) 安全审计

具体要求	现状	差异
a)应提供覆盖到每个用户的安全审计功能,对应用系统重要安全事件进行审计；	应用系统具有安全审计功能，已覆盖系统中的所有角色(超级用户、监控中心-监控班长、监控中心-监控员等)，并对定交通管制措施、现场情况等进行记录，但无操作日志，审计内容不全面。	应对操作行为进行记录。
b)应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录；	所有用户均无法中断审计进程,应用系统未提供删除审计记录的功能。	无差异。
c)审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等；	审计记录的内容包括事件类型、所属高速、具体位置、发生时间、持续时间、现场情况、交通管制措施、处理人和事件状态等。	无差异。
d)应提供对审计记录数据进	未能根据审计记录生成审计	应提供日志分析功能。

行统计、查询、分析及生成审计报表的功能。	报表。	

（四） 剩余信息保护

具体要求	现状	差异
a)应保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；	未保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前能得到完全清除，无论这些信息是否存放在硬盘上还是在内存中。	应采取技术措施保证用户鉴别信息所在的存储空间在释放或再分配前完全清除。
b)应保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。	未保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。	应采取技术措施保证系统重要信息资源所在的存储空间在释放或再分配前完全清除。

（五） 通信完整性

具体要求	现状	差异
a)应采用密码技术保证通信过程中数据的完整性。	使用 http 进行访问，未采用密码技术对通信过程的数据完整性进行传输。	应采用 HTTPS 协议传输。

（六） 通信保密性

具体要求	现状	差异
a)在通信双方建立连接之前，应用系统应利用密码技术进行会话初始化验证；	使用 http 进行访问，未对通信双方进行会话初始化验证。	应采用 HTTPS 协议传输。
b)应对通信过程中的整个报文或会话过程进行加密。	使用 http 进行访问，未对通信过程的整改会话或报文进行加密传输。	应采用 HTTPS 协议传输。

（七） 抗抵赖

具体要求	现状	差异
a)应具有在请求的情况下为数据原发者或接收者提供数据原发证据的功能；	未采用数字签名等技术实现抗抵赖功能。	应采用数字签名等技术实现抗抵赖功能。
b)应具有在请求的情况下为数据原发者或接收者提供数据接收证据的功能。	未采用数字签名等技术实现抗抵赖功能。	应采用数字签名等技术实现抗抵赖功能。

（八） 软件容错

具体要求	现状	差异
a)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数据格式或长度符合系统设定要求；	已对用户输入数据的长度、格式进行检查，如用户名格式、时间段格式。	无差异。
b)应提供自动保护功能，当故障发生时自动保护当前所有状态，保证系统能够进行恢复。	系统无法保证发生故障时，能够继续提供一部分功能。	建议系统采用集群、热备等方式部署。

（九） 资源控制

具体要求	现状	差异
a)当应用系统的通信双方中的一方在一段时间内未作任何响应，另一方应能够自动结束会话；	仅允许 Windows 远程桌面服务进行管理，但未限制远程登录的地址范围。未限制能够远程登录数据库的地址范围。	应限制远程登录服务器的客户端 IP 地址。
b)应能够对系统的最大并发会话连接数进行限制；	已设置活动但空间的远程桌面服务会话的时间限制为 15	无差异。

	分钟。已设置 Microsoft SQL Server 数据库连接超时值十五分钟。	
c)应能够对单个帐户的多重并发会话进行限制；	未定期对重要服务器的 CPU、硬盘、内存等使用情况进行监视。	应对重要服务器的 CPU、硬盘、内存等使用情况进行监视。
d)应能够对一个时间段内可能的并发会话连接数进行限制；	未限制单个账户的资源使用限度。	应限制单个账户的资源使用限度。
e)应能够对一个访问帐户或一个请求进程占用的资源分配最大限额和最小限额；	未采取措施对系统服务水平进行检测和报警。	应对系统服务水平进行检测和报警。
f)应能够对系统服务水平降低到预先规定的最小值进行检测和报警；	仅允许 Windows 远程桌面服务进行管理，但未限制远程登录的地址范围。未限制能够远程登录数据库的地址范围。	应限制远程登录服务器的客户端 IP 地址。
g)应提供服务优先级设定功能，并在安装后根据安全策略设定访问帐户或请求进程的优先级，根据优先级分配系统资源。	已设置活动但空间的远程桌面服务会话的时间限制为 15 分钟。已设置 Microsoft SQL Server 数据库连接超时值十五分钟。	无差异。

5.4.4 应用安全差距分析总结

经过对应用安全的安全访谈、检测，应用安全需实现的等级保护 3 级技术要求项共有 31 项，检测结果无差异的占 5 项。检测结果部分差异的占 6 项。检测结果均为有差异的占 20 项。

5.5 数据安全及备份恢复

5.5.1 监控系统

（一） 数据完整性

具体要求	现状	差异
a)应能够检测到系统管理数据、鉴别信息和重要业务数据在传输过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施；	采用 http 协议，无法保证通信过程中数据的完整性。	应采用 https 协议来保证数据存储的完整性。
b)应能够检测到系统管理数据、鉴别信息和重要业务数据在存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。	服务器未采用技术来保证数据存储的完整性。	服务器应采用 RAID 技术来保证数据存储的完整性。

（二） 数据保密性

具体要求	现状	差异
a)应采用加密或其他有效措施实现系统管理数据、鉴别信息和重要业务数据传输保密性；	未对操作系统、应用系统及部分网络设备和安全设备的系统管理数据、鉴别信息进行加密传输，未对重要业务数据进行加密传输。	通信过程中应使用 https 协议保证通信保密性。
b)应采用加密或其他保护措施实现系统管理数据、鉴别信息和重要业务数据存储保密性。	系统用户鉴别信息通过 MD5 转换后进行存储，但未对业务数据进行加密存储。	应对重要信息进行加密存储。

（三） 备份与恢复

具体要求	现状	差异
a)应提供本地数据备份与恢复功能，完全数据备份至少每天一次，备份介质场外存放；	未对系统中的重要数据进行数据备份。	应对重要数据进行数据备份。
b)应提供异地数据备份功能，利用通信网络将关键数据定时批量传送至备用场地；	未对系统中的重要数据进行异地数据备份。	应对重要数据进行异地数据备份。
c)应采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障；	未采用冗余技术设计网络拓扑结构，存在单点故障。	应采用冗余技术。
d)应提供主要网络设备、通信线路和数据处理系统的硬件冗余，保证系统的高可用性。	网络设备、通信线路和服务器未进行冗余部署。	应对网络设备、通信线路和服务器进行冗余部署。

5.5.2 数据安全及备份差距分析总结

经过对数据安全及备份的安全访谈、检测，该数据安全及备份需实现的等级保护 3 级技术要求项共有 8 项，检测结果无差异的占 0 项。检测结果部分差异的占 1 项。检测结果均为有差异的占 7 项。

6 差距分析汇总：

基本要求控制点		差异性评价	备注
物理安全			
7.1.1.1	物理位置的选择（G3）	无差异	
7.1.1.2	物理访问控制（G3）	部分差异	
7.1.1.3	防盗窃和防破坏（G3）	部分差异	
7.1.1.4	防雷击（G3）	部分差异	

7.1.1.5	防火（G3）	有差异	
7.1.1.6	防水和防潮	部分差异	
7.1.1.7	防静电（G3）	无差异	
7.1.1.8	温湿度控制（G3）	有差异	
7.1.1.9	电力供应（A3）	部分差异	
7.1.1.10	电磁防护（S3）	部分差异	
网络安全			
7.1.2.2	访问控制（G3）	部分差异	
7.1.2.3	安全审计（G3）	部分差异	
7.1.2.4	边界完整性检查（S3）	有差异	
7.1.2.5	入侵防范（G3）	有差异	
7.1.2.6	恶意代码防范（G3）	有差异	
7.1.2.7	网络设备防护（G3）	部分差异	
主机安全			
7.1.3.1	身份鉴别（S3）	部分差异	
7.1.3.2	访问控制（S3）	部分差异	
7.1.3.3	安全审计（G3）	部分差异	
7.1.3.4	剩余信息包含（G3）	部分差异	
7.1.3.5	入侵防范（G3）	有差异	
7.1.3.6	恶意代码防范（G3）	部分差异	
7.1.3.7	资源控制（A3）	部分差异	
应用安全			
7.1.4.1	身份鉴别	部分差异	
7.1.4.2	访问控制	部分差异	
7.1.4.3	安全审计	部分差异	
7.1.4.4	剩余信息保护	有差异	
7.1.4.5	通信完整性	有差异	
7.1.4.6	通信保密性	有差异	

7.1.4.7	抗抵赖	有差异	
7.1.4.8	软件容错	部分差异	
7.1.4.9	资源控制	有差异	
数据安全及备份恢复			
7.1.5.1	数据完整性（S3）	有差异	
7.1.5.2	数据保密性（S3）	部分差异	
7.1.5.3	备份和恢复（A3）	有差异	
安全管理制度			
7.2.1.1	管理制度（G3）	\	
7.2.1.2	制定和发布（G3）	\	
7.2.1.3	评审和修订（G3）	\	
安全管理机构			
7.2.2.1	岗位设置（G3）	\	
7.2.2.2	人员配备（G3）	\	
7.2.2.3	授权和审批（G3）	\	
7.2.2.4	沟通和合作（G3）	\	
7.2.2.5	审核和检查（G3）	\	
人员安全管理			
7.2.3.1	人员录用（G3）	\	
7.2.3.2	人员离岗（G3）	\	
7.2.3.3	人员考核（G3）（G3）	\	
7.2.3.4	安全意识教育和培训（G3）	\	
7.2.3.5	外部人员访问管理（G3）	\	
系统建设管理			
7.2.4.1	系统定级（G3）	\	
7.2.4.2	安全方案设计（G3）	\	
7.2.4.3	产品采购和使用（G3）	\	
7.2.4.4	自行软件开发（G3）	\	

7.2.4.5	外包软件开发（G3）	\	
7.2.4.6	工程实施（G3）	\	
7.2.4.7	测试验收（G3）	\	
7.2.4.8	系统交付（G3）	\	
7.2.4.9	系统备案（G3）	\	
7.2.4.10	等级测评（G3）	\	
7.2.4.11	安全服务商选择（G3）	\	
系统运维管理			
7.2.5.1	环境管理（G3）	\	
7.2.5.2	资产管理（G3）	\	
7.2.5.3	介质管理（G3）	\	
7.2.5.4	设备管理（G3）	\	
7.2.5.5	监控管理和安全管理中心（G3）	\	
7.2.5.6	网络安全管理（G3）	\	
7.2.5.7	系统安全管理（G3）	\	
7.2.5.8	恶意代码防范管理（G3）	\	
7.2.5.9	密码管理（G3）	\	
7.2.5.10	变更管理（G3）	\	
7.2.5.11	备份与恢复管理（G3）	\	
7.2.5.12	安全事件处置（G3）	\	
7.2.5.13	应急预案管理（G3）	\	

6.1 差距分析风险：

序号	安全层面	差距描述	关联资产[1]	关联威胁[2]	危害分析结果	风险等级
1	物理安全	来访人员进入机房无审批流程。	视频监控中心	非授权访问	未对外部人员进入机房执行申请和审批手续，存在非授权访问机房的风险。可能导致非授权人员进入机房进行物理破坏或盗窃。	低
2	物理安全	未对机房划分区域进行管理。	视频监控中心	越权或滥用	可能导致授权的来访人员越权访问本来无权访问的资源，做出破坏信息系统的行为。	低
3	物理安全	无防盗报警系统。	视频监控中心	盗窃	无法对盗窃破坏行为进行及时侦测并报警。	中
4	物理安全	未设置监控报警系统。	视频监控中心	物理攻击	无法对机房内的人员活动及操作施工进行监控记录，无法在发生安全事件后对之前机房内的活动进行追溯查询。	中
5	物理安全	机房未设置防雷保安器。	视频监控中心	电力故障	可能因电力波动或感应雷引发电力故障（如尖峰或浪涌），造成设备损毁。	中

[1] 如风险值和评价相同，可填写多个关联资产。

[2]对于多个威胁关联同一个问题的情况，应分别填写。

序号	安全层面	差距描述	关联资产[1]	关联威胁[2]	危害分析结果	风险等级
6	物理安全	机房存在二氧化碳灭火器，但无自动灭火设施。	视频监控中心	火灾	在发生火情后无法及时自动检测报警，并自动进行灭火，可能导致机房损毁。	中
7	物理安全	机房未采用具有耐火等级的建筑材料。	视频监控中心	火灾	机房未采用具有耐火等级的建筑材料进行装修装饰，增加了在发生火情时助燃火灾概率。	低
8	物理安全	机房未采用区域隔离。	视频监控中心	火灾	机房未采取区域隔离防火措施，在发生火灾时无法有效进行区域阻隔，造成损失范围扩大。	低
9	物理安全	机房未配备精密空调。	视频监控中心	漏水	机房环境湿度过高，可能因为水蒸气结露和地下积水腐蚀通信线缆、供电线缆、设备，甚至导致短路。	中
10	物理安全	机房无自动调节湿度的功能。	视频监控中心	湿度异常	因湿度达不到机房安全运行的环境条件，增加了设备故障几率。	中
11	物理安全	机房未配备过电压防护设备。	视频监控中心	电力故障	可能因电力波动影响设备正常运行（由于电压过低或衰变）或损毁设备（由于电压过高，如尖峰或浪涌）。	中

序号	安全层面	差距描述	关联资产[1]	关联威胁[2]	危害分析结果	风险等级
12	物理安全	机房未采用双路市供电。	视频监控中心	电力故障	一旦单个电路发生供电线路故障，系统将不能继续提供服务，系统可用性将受到严重影响。	低
13	物理安全	机房无备用供电系统。	视频监控中心	电力故障	机房未配备后备发电设备，在外部电力供应中断的情况下，系统不能继续提供服务，系统可用性将受到严重影响，可能因断电（长时间停电）导致信息系统无法提供服务。	低
14	物理安全	机房通信线缆未隔离敷设。	视频监控中心	电磁干扰	机房内电源线和通信未隔离铺设，可能造成设备通信干扰，从而导致系统运行故障。	低
15	物理安全	机房无电磁屏蔽措施。	视频监控中心	电磁干扰	未对关键设备和磁介质实施电磁屏蔽，可能因电磁泄漏造成秘密信息泄漏，也可能因电磁干扰导致数据被破坏。	低

序号	安全层面	差距描述	关联资产[1]	关联威胁[2]	危害分析结果	风险等级
16	网络安全	该系统服务器与其他系统服务器同一VLAN。	网络拓扑结构	非授权访问	系统之间可以互访，或网络用户可以超越自己的权限访问本来无权访问的资源，造成资源被非授权访问。	中
17	网络安全	在省高速结算中心边界部署了防火墙，但服务器网段与其他网段未隔离。	网络拓扑结构	网络攻击	将重要网段部署在网络边界处，系统容易被病毒入侵、网络攻击等，造成系统服务中断或瘫痪。	中
18	网络安全	未按业务服务的重要次序分配带宽优先级。	网络拓扑结构	网络攻击	在网络发生拥堵时，重要业务数据可能会受到延迟或丢弃，不能保障重要业务的正常运行。	中
19	网络安全	已在省高速结算中心边界部署了防火墙，但未启用访问控制功能。	网络拓扑结构	非授权访问	导致网络用户可以超越自己的权限访问本来无权访问的资源，造成资源被非授权访问。	中
20	网络安全	未按照业务会话配置明确的访问控制策略。	网络拓扑结构	非授权访问	导致网络用户可以超越自己的权限访问本来无权访问的资源，造成资源被非授权访问。	中
21	网络安全	未对进出网络的信息进行过滤。	网络拓扑结构	恶意代码	未对进出网络的内容进行过滤，可能引起信息系统遭受恶意代码攻击。	中

序号	安全层面	差距描述	关联资产[1]	关联威胁[2]	危害分析结果	风险等级
22	网络安全	未限制会话老化时间。	网络拓扑结构	拒绝服务	未及时断开会话，占用大量网络资源，可能导致系统由于资源耗尽而无法提供服务。	低
23	网络安全	未限制网络最大流量数和连接数。	网络拓扑结构	拒绝服务	一旦发生网络攻击事件，可能导致网络资源被耗尽，业务系统不能正常提供服务。	中
24	网络安全	服务器网段未采取IP-MAC地址绑定防止地址欺骗。	网络拓扑结构	网络攻击	1、网关欺骗，交换机、路由器等网关设备遭到ARP攻击，导致网关设备的ARP表被篡改，导致网关设备不能正常向下面主机发送信息。2、主机欺骗，主机ARP缓存表中的网关MAC地址被篡改，导致主机无法正常上网或与外部系统进行通信。3、主机欺骗，导致中间人攻击、嗅探，导致被攻击者信息泄露。	中
25	网络安全	未完善非法内联技术。	网络拓扑结构	非授权访问	无法有效防止非授权设备接入内部网络，可能导致重要信息泄漏或系统遭到入侵。	中

序号	安全层面	差距描述	关联资产[1]	关联威胁[2]	危害分析结果	风险等级
26	网络安全	未完善非法外联技术。	网络拓扑结构	非授权访问	无法有效防止“非法外联”行为发生，内部用户能够绕过安全措施访问外部网络，可能导致重要信息泄漏或系统遭到入侵。	中
27	网络安全	未完善入侵检测技术。	网络拓扑结构	网络攻击	不能对来自网络外部的攻击事件进行检测和记录，难以及时对攻击事件进行响应和事后追溯。	中
28	网络安全	未完善入侵检测技术。	网络拓扑结构	网络攻击	无法及时发现严重入侵行为，不能及时对严重入侵行为进行响应和处理。	中
29	网络安全	未完善防恶意代码技术。	网络拓扑结构	恶意代码	无法对来自外部网络的恶意代码进行有效的检测和清除。	中
30	网络安全	未完善防恶意代码技术。	网络拓扑结构	恶意代码	无法对新型的恶意代码进行有效的检测和清除。	中
31	网络安全	未能对日志记录进行分析并生成审计报表。	核心防火墙、路由器、防火墙、接入交换机	无作为	无法及时了解设备实际运行状况以及存在的安全隐患。	中
32	网络安全	日志本地保存，未能避免未预期的删除、覆盖或修改等。	核心防火墙、路由器、防火墙、接入交换机	篡改	日志可能被删除或篡改，导致发生安全事件后无法对事件过程进行追溯。	中

序号	安全层面	差距描述	关联资产[1]	关联威胁[2]	危害分析结果	风险等级
33	网络安全	未对登录设备的用户进行身份鉴别。	核心防火墙	非授权访问	未配置用户名和口令，存在设备被非授权访问进行攻击或破坏的风险。	高
34	网络安全	未对网络设备的管理员登录地址进行限制。	路由器、防火墙、接入交换机	非授权访问	在所有可以发起远程连接的地方，终端都可以尝试登录设备。	中
35	网络安全	未设置 console 口登录的用户名和口令。用户身份标识唯一，但未设置 console 口登录的用户名和口令。	核心防火墙、路由器、防火墙、接入交换机	抵赖	存在管理帐户滥用权限和恶意破坏的风险，无法准确通过审计日志对操作人员进行分析审计。	高
36	网络安全	未对登录设备的用户进行身份鉴别。仅采用用户名口令对同一用户进行身份鉴别。	核心防火墙、路由器、防火墙、接入交换机	口令破解	仅采取用户名口令进行身份鉴别，一旦用户口令遭到窃取，将无其它鉴别机制来防止未授权登录设备等风险。	中
37	网络安全	口令未定期更改。	核心防火墙、路由器、防火墙、接入交换机	口令破解	攻击者可能通过暴力口令猜测等手段破解用户口令。	中
38	网络安全	未配置设备的登录失败处理功能。	核心防火墙、路由器、防火墙、接入交换机	口令破解	未配置登录失败处理策略，增加了用户口令被暴力破解的风险。	低

序号	安全层面	差距描述	关联资产[1]	关联威胁[2]	危害分析结果	风险等级
39	网络安全	采用 telnet 和 http 的方式对安全设备进行管理。	路由器、防火墙、接入交换机	窃听	使用 HTTP 或 Telnet 等明文的传输协议进行网络管理，增加了鉴别信息或管理信息被网络截取的风险。	中
40	网络安全	未实现特权账户的权限分离。	核心防火墙、路由器、防火墙、接入交换机	越权或滥用	无法实现不同权限角色间的监督，存在管理帐户越权管理或滥用权限的风险。	低
41	主机安全	服务器和运维终端均存在弱口令，且均未定期更换口令。	情报板服务器、微创视频转码服务器、大华视频转码服务器、运维终端	口令破解	口令可能被恶意用户猜测获得，合法用户身份被仿冒，导致系统被非授权访问。	高
42	主机安全	未设置登陆失败处理功能。	情报板服务器、微创视频转码服务器、大华视频转码服务器、运维终端	口令破解	增加了用户口令被暴力破解的风险。	中
43	主机安全	未使用安全的远程连接方式。	情报板服务器	嗅探	默认 RDP 协议存在安全隐患，可能在通信过程中被攻击者破解获得口令。	低
44	主机安全	未采用两种或两种以上组合的鉴别技术。	情报板服务器、微创视频转码服务器、大华视频转码服务器、运维终端	口令破解	仅采取用户名口令进行身份鉴别，一旦用户口令遭到窃取，将无其它鉴别机制来防止未授权登录设备等风险。	中

序号	安全层面	差距描述	关联资产[1]	关联威胁[2]	危害分析结果	风险等级
45	主机安全	未合理设置 UMASK 值。	微创视频转码服务器、大华视频转码服务器	越权或滥用	用户权限过高，可能访问未授权访问的资源，造成信息泄露、数据被破坏等。	低
46	主机安全	未实现管理用户的权限分离。	情报板服务器、微创视频转码服务器、大华视频转码服务器、运维终端	越权或滥用	存在多个管理员共用同一帐户导致安全事件发生后难以对责任进行界定。此外，单个帐户授予过高权限易引起越权、滥用风险。	低
47	主机安全	未实现系统特权用户的权限分离。	情报板服务器、微创视频转码服务器、大华视频转码服务器、运维终端	越权或滥用	由于单个管理员用户权限过大，可能存在权限滥用的风险。	低
48	主机安全	数据库未禁用默认无用账户。	情报板服务器	非授权访问	未限制的默认账户可能被攻击者利用，未授权访问重要数据。	中
49	主机安全	数据库存在多余账户。	情报板服务器	非授权访问	多余、过期账户的往往缺少监管，现有的安全措施未得到有效落实，可能被攻击者利用入侵系统。	中
50	主机安全	未对重要信息资源设置敏感标记。	情报板服务器、微创视频转码服务器、大华视频转码服务器、运维终端	越权或滥用	存在恶意用户通过修改用户权限等方法，非授权访问重要信息资源的可能。	中

序号	安全层面	差距描述	关联资产[1]	关联威胁[2]	危害分析结果	风险等级
51	主机安全	未开启安全审计服务。	大华视频转码服务器	抵赖	操作系统无法对重要用户行为进行审计记录，不便于安全事件的追溯，不易发现系统安全隐患	中
52	主机安全	审计内容不全面。	情报板服务器	抵赖	导致重要系统事件、用户操作日志记录的信息不全面，发生安全事件后无法还原安全事件的全过程。	中
53	主机安全	未开启安全审计服务。	大华视频转码服务器	抵赖	导致日志记录中重要属性缺失，在分析过程中缺少必要的内容，不利于发生风险之后的事件追溯。	中
54	主机安全	无生成审计报表的功能。	情报板服务器、微创视频转码服务器、大华视频转码服务器、运维终端	抵赖	无法及时发现系统安全隐患，并对可能发生的事件进行预判。	中
55	主机安全	审计记录本地保存，不能避免受到未预期的删除、修改或覆盖，且存储空间过小。	情报板服务器、微创视频转码服务器、大华视频转码服务器、运维终端	越权或滥用	未授权用户可能利用获得的权限访问、修改或删除审计日志。	中
56	主机安全	未能保证鉴别信息所在的存储空间，在被释放或再分配给其他用户前得到完全清除。	情报板服务器、运维终端	信息泄漏	残留在系统中的敏感信息可能被攻击者获取。	中

序号	安全层面	差距描述	关联资产[1]	关联威胁[2]	危害分析结果	风险等级
57	主机安全	未能保证系统内的文件、目录和数据库记录等资源所在的存储空间，在被释放或再分配给其他用户前得到完全清除。	情报板服务器、运维终端	信息泄漏	残留在系统中的敏感信息可能被攻击者获取。	中
58	主机安全	未采取主机入侵检测措施。	情报板服务器、微创视频转码服务器、大华视频转码服务器、运维终端	网络攻击	不能对攻击事件进行检测和记录，难以及时对攻击事件进行响应和事后追溯。	中
59	主机安全	未对重要程序完整性进行检测。	情报板服务器、微创视频转码服务器、大华视频转码服务器、运维终端	篡改	无法及时发现系统内重要程序被恶意篡改，完整性被破坏后无法及时恢复，可能造成业务中断。	低
60	主机安全	系统存在不必要的服务和端口，且未及时更新系统安全补丁。	情报板服务器、微创视频转码服务器、大华视频转码服务器、运维终端	网络攻击	已存在的安全漏洞可能被攻击者利用入侵系统。多余的组件和服务可能存在安全漏洞，额外增加了系统面临的风险。	中
61	主机安全	未安装防恶意代码软件。	微创视频转码服务器、大华视频转码服务器、运维终端	恶意代码	无法对病毒、木马等恶意代码进行检测和清除。	中
62	主机安全	网络层面未安装防恶意代码软件。	微创视频转码服务器、大华视频转码服务器、运维终端	恶意代码	恶意代码防护能力不够全面，存在发生恶意代码在系统内部网络传播的可能性。	中

序号	安全层面	差距描述	关联资产[1]	关联威胁[2]	危害分析结果	风险等级
63	主机安全	未安装防恶意代码软件。	微创视频转码服务器、大华视频转码服务器、运维终端	管理不到位	缺少有效手段对防病毒情况进行统一升级与管理，无法及时发现存在的防病毒隐患，形成全面的恶意代码防护能力。	中
64	主机安全	未限制终端登录接入方式。	情报板服务器、微创视频转码服务器、大华视频转码服务器、运维终端	非授权访问	未授权用户可能通过开放的远程管理服务登录服务器系统。	中
65	主机安全	未设置终端登录超时锁定。	微创视频转码服务器、大华视频转码服务器	非授权访问	用户登录后，离开时未及时退出或锁定计算机，可能被未授权人员利用。	中
66	主机安全	未定期对重要服务器的 CPU、硬盘、内存等使用情况进行监视。	情报板服务器、微创视频转码服务器、大华视频转码服务器、运维终端	软硬件故障	服务器运行情况发生异常时管理人员无法及时发现，无法及时进行响应。	低
67	主机安全	未限制单个用户对系统资源的使用。	情报板服务器、微创视频转码服务器、大华视频转码服务器、运维终端	拒绝服务	可能由于某个用户占用过多系统资源，导致响应缓慢、卡顿甚至服务器宕机。	低
68	主机安全	未采取措施对系统服务水平进行检测和报警。	情报板服务器、微创视频转码服务器、大华视频转码服务器、运维终端	软硬件故障	缺少针对服务器运行情况的监控报警机制，出现服务水平降低时，管理人员无法及时发现和进行响应。	低

序号	安全层面	差距描述	关联资产[1]	关联威胁[2]	危害分析结果	风险等级
69	应用安全	未采用两种或两种以上的组合鉴别方式。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	口令破解	仅采取用户名口令进行身份鉴别，一旦用户名和口令遭到窃取，将无其它鉴别机制来防止未授权登录设备等风险。	中
70	应用安全	未提供鉴别信息复杂度检查功能。	诸永高速温州延伸段监控系统	口令破解	用户可以设置弱口令，存在被恶意用户暴力破解的可能。	中
71	应用安全	未提供登陆失败处理功能。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	口令破解	登录口令可能被恶意用户使用暴力猜解方式获得，导致系统被非授权访问。	中
72	应用安全	该系统未提供访问控制功能。	VAM 视频监控系统	非授权访问	信息系统重要资源被未授权访问的可能性增大，对信息系统的正常运行带来影响。	中
73	应用安全	该系统未提供访问控制功能。	VAM 视频监控系统	非授权访问	访问控制覆盖范围不完善，使攻击者对相关系统未授权访问成功的可能性增大。	中
74	应用安全	该系统未提供访问控制功能。	VAM 视频监控系统	越权或滥用	存在默认用户，且权限过大，攻击者可能利用该帐户访问系统。	中

序号	安全层面	差距描述	关联资产[1]	关联威胁[2]	危害分析结果	风险等级
75	应用安全	Digital Surveillance System 和诸永高速温州延伸段监控系统权限设置不合理，VAM 视频监控系统未提供访问控制功能。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	越权或滥用	管理员权限过大，可能无法对管理员的行为进行监管、制约。	低
76	应用安全	未对重要信息资源设置敏感标记。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	非授权访问	存在恶意用户通过修改用户权限等方法，非授权访问重要信息资源的可能。	低
77	应用安全	审计内容不全面。	VAM 视频监控系统、诸永高速温州延伸段监控系统	抵赖	不能对重要用户、重要事件进行日志记录，不便于安全事件的追溯，不利于系统日常的安全运维。	中
78	应用安全	无生成审计报表的功能。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	管理不到位	不利于管理员定期分析系统日志信息，从而无法及时发现系统可能存在的侵害。	低
79	应用安全	未保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前能得到完全清除，无论这些信息是否存放在硬盘上还是在内存中。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	越权或滥用	恶意人员可能获取到合法用户的鉴别信息，并利用这些鉴别信息仿冒他人身份访问目标系统。	低

序号	安全层面	差距描述	关联资产[1]	关联威胁[2]	危害分析结果	风险等级
80	应用安全	未保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	越权或滥用	由于上述问题，恶意人员可能获取到合法用户的敏感/重要数据，造成敏感/重要数据的泄露，从而侵害了其他合法用户的利益，影响了信息系统的正常运行。	低
81	应用安全	采用 http 协议，无法保证通信过程中数据的完整性。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	篡改	可能导致重要数据在传输过程中被攻击者劫持、篡改，使传输数据的完整性遭到破坏，可能影响到用户和企业的声誉和经济利益。	中
82	应用安全	已采用 http 协议，未采用密码技术进行会话初始化验证。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	泄密	用户重要数据在不安全的会话中传递，可能导致数据被嗅探、劫持。	中
83	应用安全	已采用 http 协议，未对传输过程中的数据进行加密。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	嗅探	通信过程中存在用户鉴别信息和重要业务数据被嗅探并盗用的可能性。	中
84	应用安全	未采用数字签名等密码技术实现通信过程中数据原发行为的抗抵赖。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	抵赖	在需要获取历史的数据接收证据时，若无法有效获取相关证明，可能损害系统中收发双方用户对此系统的信赖。	低

序号	安全层面	差距描述	关联资产[1]	关联威胁[2]	危害分析结果	风险等级
85	应用安全	未采用数字签名等密码技术实现通信过程中数据接收行为的抗抵赖。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	抵赖	存在操作抵赖事件发生的可能性。	低
86	应用安全	未提供自动保护功能，故障发生时不能自动保护当前所有状态。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	软硬件故障	系统发生故障，无法及时自动恢复，可能导致系统无法提供服务。	低
87	应用安全	不能自动结束会话。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	非授权访问	存在恶意用户非授权访问系统，造成系统业务信息被非法获取的可能性。	中
88	应用安全	未能对系统的最大并发会话连接数进行限制。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	拒绝服务	访问量大或遭受拒绝服务攻击时，由于系统资源占用率过高，可能导致系统运行缓慢，甚至系统中断。	低
89	应用安全	未对单个账户的多重并发会话进行限制。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	拒绝服务	无法有效的防护拒绝服务攻击，增加了遭到拒绝服务攻击的风险。	低
90	应用安全	未能对一个时间段内可能的并发会话连接数进行限制	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	软硬件故障	可能导致系统资源占用率过高，影响业务稳定运行。	低
91	应用安全	未能对访问账户或请求进程占用的资源分配最大和最小值的限额。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	软硬件故障	可能导致系统资源占用率过高，影响业务稳定运行。	低

序号	安全层面	差距描述	关联资产[1]	关联威胁[2]	危害分析结果	风险等级
92	应用安全	未能对服务水平降到最小值进行检测和报警。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	软硬件故障	无法及时发现系统出现的异常情况，无法及时进行响应。	低
93	应用安全	未提供服务优先级的功能。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	软硬件故障	一旦发生系统资源紧张，无法保证重要的服务正常运行。	低
94	数据安全及备份恢复	系统采用 HTTP 协议无法保证通信过程中数据的完整性。	监控系统	篡改	数据在通信过程中可能被篡改，导致业务运营、声誉、经济利益受损。	中
95	数据安全及备份恢复	系统未采用任何技术来保证数据存储的完整性。	监控系统	篡改	无法保证数据在存储过程中的完整性，可能被攻击者篡改。	中
96	数据安全及备份恢复	系统采用 HTTP 协议无法保证数据在传输过程中的保密性。	监控系统	嗅探	重要数据在传输过程中被攻击者嗅探并盗用成功的可能性增大。	中
97	数据安全及备份恢复	未对业务数据进行加密存储。	监控系统	泄密	重要数据在存储过程中被攻击者直接盗用成功的可能性增大。	中
98	数据安全及备份恢复	未对系统中的重要数据进行数据备份。	监控系统	数据丢失	系统如出现故障，可能无法及时恢复，或造成重要数据丢失。	中

序号	安全层面	差距描述	关联资产[1]	关联威胁[2]	危害分析结果	风险等级
99	数据安全及备份恢复	未提供异地备份功能	监控系统	数据丢失	如机房遭受严重破坏,可能导致数据完全丢失。	中
00	数据安全及备份恢复	未采采用冗余技术设计网络拓扑结构。	监控系统	软硬件故障	如网络关键节点故障,可能导致网络不可用。	中
01	数据安全及备份恢复	主要网络设备、通信线路和服务器均未采用硬件冗余	监控系统	硬件故障	数据处理系统未配置硬件冗余,无法保证系统的高可用性。	中

7 差距整改建议：

序号	问题描述	涉及对象	整改建议
1	来访人员进入机房无审批流程。	视频监控中心	建立机房访问审批流程，来访人员提交书面申请，说明来访人员的包括姓名、单位、联系方式、事由、时间、人数等内容，在获得授权后，方可访问机房。
2	未对机房划分区域进行管理。	视频监控中心	按功能不同对机房进行区域划分，如分为主机房（服务器室、网路设备室、数据存储室等），辅助房（不间断电源室、空调机室、气体钢瓶室、监控室等），并设置有效的物理隔离措施（如玻璃幕墙、物理实墙等）。
3	无防盗报警系统。	视频监控中心	在机房出入口处设置安全报警设施，如红外线防盗报警器。
4	未设置监控报警系统。	视频监控中心	在机房设置视频监控系统，监控范围覆盖整个机房，确保视频监控系统正常启用。监控记录应保存 6 个月。
5	机房未设置防雷保安器。	视频监控中心	在大楼进线端、机房进线端等处设置防雷保安器（SPD、电源避雷器），防止感应雷。
6	机房存在二氧化碳灭火器，但无自动灭火设施。	视频监控中心	对机房设置火灾自动消防系统，具有自动检测火情、自动报警，并自动灭火的功能。采用洁净气体灭火系统，如七氟丙烷（FM-200）、烟烙尽（IG541）、FE-13 等。
7	机房未采用具有耐火等级的建筑材料。	视频监控中心	1.机房耐火等级不应低于二级。 2.主机房的顶棚、壁板（包括夹芯材料）和隔断采用不燃烧体。地面及其他装修采用不低于 B1 级（难燃材料）的装修材料。

序号	问题描述	涉及对象	整改建议
8	机房未采用区域隔离。	视频监控中心	1.机房与其它功能用房之间采用耐火极限不低于 2.0h 的防火隔墙和1.5h的楼板隔开。隔墙上有开门时，采用甲级防火门。 2.主机房采取区域隔离防火措施，将重要设备与其他设备隔离开。区域间采用耐火玻璃幕墙或物理实墙进行隔断。
9	机房未配备精密空调。	视频监控中心	1.采取措施对机房湿度进行控制，相对湿度不大于 60%。 2.采取防结露除积水措施。如采取下送风、在防静电地板下铺设防潮海绵、设置洁净室专用地漏或自闭式地漏。
10	机房无自动调节湿度的功能。	视频监控中心	购买精密空调，并使其正常启用，加强日常人工巡检，确保机房湿度正常。
11	机房未配备过电压防护设备。	视频监控中心	在机房进线端配置瞬态电压浪涌保护器，可配备在配电柜或配电列头柜内。
12	机房未采用双路市供电。	视频监控中心	配备双路电源为主机房供电。
13	机房无备用供电系统。	视频监控中心	配备备用供电系统，如应急供电车，或者柴油发电机组。发电机组的输出功率应满足机房最大平均负荷的需要。设置现场储油装置，储存柴油的供应时间，A 级满足 12h 用油。当外部供油时间有保障时，燃料存储量仅需大于外部供油时间。
14	机房通信线缆未隔离敷设。	视频监控中心	1.对现有线路进行梳理，将电源线和通信线缆隔离。 2.进行网络改造时，重新对布线进行梳理，当电缆线槽与通信线槽并列或交叉敷设时，配电电缆线槽敷设在通信线槽的下方。 3.采用屏蔽布线系统、光缆布线系统以避免电磁干扰。

序号	问题描述	涉及对象	整改建议
15	机房无电磁屏蔽措施。	视频监控中心	1.设置电磁屏蔽室，将关键设备与磁介质放置在电磁屏蔽室内。电场屏蔽衰减指标大于60dB 的屏我蔽室，屏蔽材料可选择镀锌钢板。电场屏蔽衰减指标大于 25dB 的屏蔽室，屏蔽材料可选择金属丝网。 2.设置电磁屏蔽机柜，将关键设备与磁介质放置在电磁屏蔽机柜内。
16	该系统服务器与其他系统服务器同一 VLAN。	网络拓扑结构	根据各部门的工作职能、重要性和所涉及信息的重要程度等因素，划分不同的子网或网段，并按照方便管理和控制的原则为各子网、网段分配地址段；
17	在省高速结算中心边界部署了防火墙，但服务器网段与其他网段未隔离。	网络拓扑结构	避免将重要网段部署在网络边界处，重要网段与其他网段之间采取可靠的技术隔离手段，如 vlan 划分。
18	未按业务服务的重要次序分配带宽优先级。	网络拓扑结构	按照对业务服务的重要次序来指定带宽分配优先级别，保证在网络发生拥堵的时候优先保护重要主机。
19	已在省高速结算中心边界部署了防火墙，但未启用访问控制功能。	网络拓扑结构	建议在网络边界处部署网络控制设备，并根据系统业务需求最小化原则设置访问控制策略，控制粒度应达到端口级。
20	未按照业务会话配置明确的访问控制策略。	网络拓扑结构	根据业务需求在访问控制设备中配置端口级别的访问控制策略。
21	未对进出网络的信息进行过滤。	网络拓扑结构	通过部署访问控制设备，配置访问控制策略对进出网络的信息内容进行过滤，实现对应用层协议命令级的控制。
22	未限制会话老化时间。	网络拓扑结构	在防火墙中明确定义会话非活跃终止时间，超过此时间自动结束会话。

序号	问题描述	涉及对象	整改建议
23	未限制网络最大流量数和连接数。	网络拓扑结构	在具备网络流量限制功能设备中限制网络最大流量及网络连接数。网络的最大流量数与连接数应与业务实际情况相结合，再做限制。
24	服务器网段未采取 IP-MAC 地址绑定防止地址欺骗。	网络拓扑结构	1、在网关设备上对同网段下的主机进行静态 ARP 绑定。2、在主机 ARP 表上绑定网关的 IP 和 MAC（PC ip/mac 绑定）。3、在主机 ARP 表上绑定自身的 IP 和 MAC。
25	未完善非法内联技术。	网络拓扑结构	建议部署能够对“非法内联”行为进行检查和阻断的产品，如准入系统。
26	未完善非法外联技术。	网络拓扑结构	建议部署能够对“非法外联”行为进行检查和阻断的产品，如桌面管理系统。
27	未完善入侵检测技术。	网络拓扑结构	部署入侵检测设备，对端口扫描、强力攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、IP 碎片攻击和网络蠕虫攻击等，并及时更新设备攻击检测库，启用设备报警功能并保证功能有效。
28	未完善防恶意代码技术。	网络拓扑结构	在网络边界部署恶意代码检测设备，如防毒墙，并及时更新检测库。
29	未能对日志记录进行分析并生成审计报表。	核心防火墙、路由器、防火墙、接入交换机	建议部署第三方日志管理系统，以便于管理员对该设备的日常管理和安全分析。
30	日志本地保存，未能避免未预期的删除、覆盖或修改等。	核心防火墙、路由器、防火墙、接入交换机	建议配置日志服务器，将日志信息传输到服务器进行保存，至少保存 6 个月。
31	未对登录设备的用户进行身份鉴别。	核心防火墙	设置用户名和口令。
32	未对网络设备的管理员登录地址进行限制。	路由器、防火墙、接入交换机	建议限制设备的远程管理地址，仅允许管理员终端远程登录设备。
33	未设置 console 口登录的用户名和口令。	核心防火墙、路由器、防火墙、接入交换机	设置 consloe 登录的用户名和口令。

序号	问题描述	涉及对象	整改建议
34	仅采用用户名口令对同一用户进行身份鉴别。	核心防火墙、路由器、防火墙、接入交换机	建议采用两种或两种以上的鉴别技术进行身份鉴别。除用户名和口令外再选用第二种身份鉴别手段，如 USB KEY、IC 卡、数字证书、动态令牌等。
35	未配置设备的登录失败处理功能。	核心防火墙、路由器、防火墙、接入交换机	建议增加（或设置）登录失败处理功能和登录超时功能，并设置合理的参数。
36	采用 telnet 和 http 的方式对安全设备进行管理。	路由器、防火墙、接入交换机	建议采用安全的方式（如：SSH、HTTPS 等）进行设备的远程管理。
37	未实现特权账户的权限分离。	核心防火墙、路由器、防火墙、接入交换机	为不同用户分别设置相应权限的帐户，实现不同权限角色间的监督和制约。
38	服务器和运维终端均存在弱口令，且均未定期更换口令。	情报板服务器、微创视频转码服务器、大华视频转码服务器、运维终端、核心防火墙、路由器、防火墙、接入交换机	建议合理配置操作系统和数据库系统的密码策略，加强用户口令长度与复杂度要求，口令应由 8 位以上数字、字母和字符组成，并定期更换，建议每三个月更改一次。尽快更改运维终端简单口令，口令应满足复杂度要求。
39	未设置登陆失败处理功能。	情报板服务器、微创视频转码服务器、大华视频转码服务器、运维终端	建议开启失败登录处理功能，如限制非法登录次数（10 次以下）、锁定时间等。
40	未使用安全的远程连接方式。	情报板服务器	建议 Windows 操作系统配置 ssl 方式进行远程管理。（设置方法："管理工具-远程桌面会话主机配置-RDP-Tcp 属性-常规-安全性，将安全层修改为 SSL(TLS1.0)",加密级别设置为"高或符合 FIPS 标准"，并勾选"仅允许运行使用网络级别身份验证的远程桌面的计算机连接"。

序号	问题描述	涉及对象	整改建议
41	未采用两种或两种以上组合的鉴别技术。	情报板服务器、微创视频转码服务器、大华视频转码服务器、运维终端	建议采用两种或两种以上的鉴别技术进行身份鉴别。除用户名和口令外再选用第二种身份鉴别手段，如指纹、USB KEY、短信验证码、数字证书、动态令牌等。
42	未合理设置 UMASK 值。	微创视频转码服务器、大华视频转码服务器	根据业务需要合理设置 umask 值。
43	未实现管理用户的权限分离。	情报板服务器、微创视频转码服务器、大华视频转码服务器、运维终端	建议实现特权用户的权限分离，如分设系统管理员、安全管理员、审计管理员。
44	未实现系统特权用户的权限分离。	情报板服务器、微创视频转码服务器、大华视频转码服务器、运维终端	建议实现特权用户的权限分离，如服务器分设系统管理员、安全管理员、审计管理员，同时数据库也分设系统管理员、安全管理员、审计管理员。
45	数据库未禁用默认无用账户。	情报板服务器	建议禁用无用的数据库默认账户，如 SA。
46	数据库存在多余账户。	情报板服务器	建议删除或禁用数据库无用账户。
47	未对重要信息资源设置敏感标记。	情报板服务器、微创视频转码服务器、大华视频转码服务器、运维终端	建议对系统重要资源增加敏感标记的功能，并控制用户对已标记的敏感信息的操作。
48	未开启安全审计服务。	大华视频转码服务器	建议开启操作系统安全审计策略，并对重要系统安全事件及用户操作行为进行日志审计。
49	审计内容不全面。	情报板服务器	情报板服务器应合理配置系统审计策略，对系统关键事件、重要用户行为等进行审计。大华视频转码服务器应开启审计功能，并合理配置审计策略。

序号	问题描述	涉及对象	整改建议
50	无生成审计报表的功能。	情报板服务器、微创视频转码服务器、大华视频转码服务器、运维终端	建议通过第三方日志审计管理软件对操作系统日志进行定期分析汇总，并生成报表。
51	审计记录本地保存，不能避免受到未预期的删除、修改或覆盖，且存储空间过小。	情报板服务器、微创视频转码服务器、大华视频转码服务器、运维终端	建议合理配置日志文件的访问权限，禁止普通用户访问、修改或删除审计日志。并配置日志服务器或第三方审计系统，对审计记录进行分析和保存，保存时间最好不小于 6 个月。
52	未能保证鉴别信息所在的存储空间，在被释放或再分配给其他用户前得到完全清除。	情报板服务器、运维终端	本地安全选项启用“不显示最后登录的用户名”。
53	未能保证系统内的文件、目录和数据库记录等资源所在的存储空间，在被释放或再分配给其他用户前得到完全清除。	情报板服务器、运维终端	本地安全选项启用“关机前清除虚拟内存页面”。
54	未采取主机入侵检测措施。	情报板服务器、微创视频转码服务器、大华视频转码服务器、运维终端	建议采取入侵检测措施，根据需要安装第三方入侵检测软件，对服务器进行防护，记录攻击的具体日志，并提供告警功能。
55	未对重要程序完整性进行检测。	情报板服务器、微创视频转码服务器、大华视频转码服务器、运维终端	建议安装第三方的完整性保护软件。
56	操作系统存在多余的服务和端口，且未及时更新系统安全补丁。	情报板服务器、微创视频转码服务器、大华视频转码服务器、运维终端	1、建议关注厂商补丁发布情况，及时更新系统安全补丁。在更新前对补丁进行测试，避免影响系统运行。2、建议根据最小化原则卸载多余的系统组件，关闭不必要的服务和端口。

序号	问题描述	涉及对象	整改建议
57	未安装防恶意代码软件。	微创视频转码服务器、大华视频转码服务器、运维终端	建议选择并安装支持统一管理的主机防病毒产品，如企业版防病毒软件，并及时更新防病毒特征库。
58	未限制终端登录接入方式。	微创视频转码服务器、大华视频转码服务器	建议限制可远程登录服务器的管理终端 IP 地址，仅允许特定终端登录。
59	未设置终端登录超时锁定。	微创视频转码服务器、大华视频转码服务器	建议在 /etc/profile 中设置 TMOUT 值。
60	未定期对重要服务器的 CPU、硬盘、内存等使用情况进行监视。	情报板服务器、微创视频转码服务器、大华视频转码服务器、运维终端	建议通过第三方软件对服务器的资源使用情况进行监控。
61	未限制单个用户对系统资源的使用。	情报板服务器、微创视频转码服务器、大华视频转码服务器、运维终端	建议限制单个用户对系统资源的最大使用，如 CPU、内存。
62	未采取措施对系统服务水平进行检测和报警。	情报板服务器、微创视频转码服务器、大华视频转码服务器、运维终端	建议通过第三方软件对系统的服务水平进行检测和报警。对操作系统运行过程中可能出现的资源瓶颈或异常事件设置相应的报警阈值，并能通过界面或短信等方式提供告警功能。
63	未采用两种或两种以上的组合鉴别方式。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	建议采用两种或两种以上的鉴别技术进行身份鉴别。除用户名和口令外再选用第二种身份鉴别手段，如指纹、USB KEY、短信验证码、数字证书、动态令牌等。
64	未提供鉴别信息复杂度检查功能。	诸永高速温州延伸段监控系统	建议根据需要对系统用户口令设置复杂度限制。
65	未提供登陆失败处理功能。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	建议系统提供专用的登录失败处理功能并合理配置。

序号	问题描述	涉及对象	整改建议
66	该系统未提供访问控制功能。	VAM 视频监控系统	建议根据安全设计需求，对用户访问系统及相关资源进行控制。对系统各个模块进行访问控制，防止用户进行非授权访问，严格限制默认帐户的访问权限，关闭不必要的默认帐号。
67	Digital Surveillance System 和诸永高速温州延伸段监控系统权限设置不合理，VAM 视频监控系统未提供访问控制功能。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	建议系统授予不同用户为完成各自承担的任务所需的最小权限，将系统管理员和业务操作员权限分离，并设置独立的安全审计员角色，对各类用户的操作行为进行审计监督。
68	未对重要信息资源设置敏感标记。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	建议对系统重要资源增加敏感标记的功能，并控制用户对已标记的敏感信息的操作。
69	审计内容不全面。	VAM 视频监控系统、诸永高速温州延伸段监控系统	建议对系统后台重要操作（如用户新增、删除等）、系统管理员和运维管理员的登录、登出、鉴别失败等事件进行记录。
70	无生成审计报表的功能。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	建议为系统增加对审计日志统计、查询、分析及生成审计报表的功能。
71	未保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前能得到完全清除，无论这些信息是否存放在硬盘上还是在内存中。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	采取技术措施保证用户鉴别信息所在的存储空间在释放或再分配前完全清除。

序号	问题描述	涉及对象	整改建议
72	未保证系统内的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	采取技术措施保证系统重要信息资源所在的存储空间在释放或再分配前完全清除。
73	采用 http 协议，无法保证通信过程中数据的完整性。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	建议采用 HTTPS 协议传输。
74	已采用 http 协议，未采用密码技术进行会话初始化验证。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	建议采用 HTTPS 协议传输。
75	已采用 http 协议，未对传输过程中的数据进行加密。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	建议采用 HTTPS 协议传输。
76	未采用数字签名等密码技术实现通信过程中数据原发行为的抗抵赖。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	采用数字签名方式对用户的重要业务操作进行抗抵赖验证。
77	未采用数字签名等密码技术实现通信过程中数据接收行为的抗抵赖。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	采用数字签名方式对用户的重要业务操作进行抗抵赖验证。
78	未提供自动保护功能，故障发生时不能自动保护当前所有状态。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	建议系统采用集群、热备等方式部署。
79	不能自动结束会话。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	建议根据业务需要对系统空闲会话超时时间进行设置。

序号	问题描述	涉及对象	整改建议
80	未能对系统的最大并发会话连接数进行限制。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	根据业务需要对系统允许的最大并发会话数进行限制。
81	未对单个账户的多重并发会话进行限制。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	建议对单个用户的多重并发会话进行限制。
82	未能对一个时间段内可能的并发会话连接数进行限制	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	建议根据需要对系统允许的一个时间段内系统最大并发会话数以及一个帐户或进程占用的资源分配阈值进行限制。
83	未能对访问账户或请求进程占用的资源分配最大和最小值的限额。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	建议根据业务需要对一个帐户或进程占用的资源进行最大/最小额度限制。
84	未能对服务水平降到最小值进行检测和报警。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	建议对系统服务水平进行有效监控，当服务降低到预先规定的最小值时能进行报警。
85	未提供服务优先级的功能。	Digital Surveillance System、VAM 视频监控系统、诸永高速温州延伸段监控系统	建议对访问用户或请求进行的优先级进行划分，并根据优先级合理分配系统资源。
86	系统采用 HTTP 协议无法保证通信过程中数据的完整性。	监控系统	建议系统采用 HTTPS 协议传输
87	系统未采用任何技术来保证数据存储的完整性。	监控系统	建议服务器采用 RAID1 或 RAID5 或 RAID10 技术来保证数据存储的完整性。
88	系统采用 HTTP 协议无法保证数据在传输过程中的保密性。	监控系统	建议系统采用 HTTPS 协议传输

序号	问题描述	涉及对象	整改建议
89	未对业务数据进行加密存储。	监控系统	建议对重要信息进行加密存储。
90	未对系统中的重要数据进行数据备份。	监控系统	建议对数据每天至少完全备份一次，并将备份介质场外存放。
91	未提供异地备份功能	监控系统	建议利用通信网络将关键数据定时批量传送至备用场地（起码在不同区），实现数据异地备份。
92	未采采用冗余技术设计网络拓扑结构。	监控系统	建议采用冗余技术设计网络拓扑结构，避免关键节点存在单点故障。
93	主要网络设备、通信线路和服务器均未采用硬件冗余	监控系统	建议主要网络设备、通信线路和服务器均采用冗余部署。

（全文完）