ICS 35.040
CCS R85

团　体　标　准

T/CITSA 15-2021

智能交通摄像机安全技术要求

Technique requirements for intelligent traffic camera security

2021-07-26 发布　　2021-07-26 实施

中国智能交通协会　发布

目　　次

前　言

本文件按照GB/T 1.1-2020 《标准化工作原则 第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国智能交通协会提出并归口。

本文件起草单位：公安部交通安全产品质量监督检测中心、北京全路通信信号研究设计院集团有限公司、华为技术有限公司、浙江大华技术股份有限公司、上海安讯士网络通讯设备贸易有限公司、重庆紫光华山智安科技有限公司、云从科技集团股份有限公司、青岛以萨数据技术有限公司。

本文件主要起草人：张昊、华莎、程晨、严敏瑞、许辉、陈希韬、封正、葛小宇、潘宇恒、孔鲁、徐晨辉、盛利勇、李军、孙亚妮、罗浩。

智能交通摄像机安全技术要求

1 范围

本文件规定了智能交通摄像机安全功能要求、安全保障要求和安全等级划分。

本文件主要适用于公安交通系统视频监控工程摄像机的产品研制、维护和测评，铁路、城轨、公路等其他交通领域也可参考。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069-2010 信息安全技术 术语

GB 35114-2017 公共安全视频监控联网信息安全技术要求

GA/T 1127-2013 安全防范视频监控摄像机通用技术要求

GM/T 0054-2018 信息系统密码应用基本要求

3 术语和定义

3.1

智能交通摄像机 intelligent traffic camera

应用于交通领域，具备对采集到的交通视频、图片进行检测、识别、比对等智能化操作的摄像机。

3.2

智能交通摄像机应用软件 intelligent traffic camera application software

安装在智能交通摄像机中除操作系统、数据库之外的，用于对智能交通摄像机采集到的交通视频、图片进行检测、识别、比对等操作的应用软件。典型的智能交通摄像机应用软件功能有车牌识别、行人闯红灯识别等。

注：后文将“智能交通摄像机应用软件”简称为“智能交通应用软件”。

3.3

密码管理 password management

对加密保护、安全认证的算法、技术、产品和服务进行管理维护。

3.4

密钥管理 key management

根据安全策略，对密钥的产生、分发、存储、更新、归档、撤销、备份、恢复和销毁等密钥全生命周期的管理。

[来源：GM/T 0054-2018 3.8]

4 缩略语

下列符合和缩略语适用于本文件。

ICMP　互联网控制消息协议（Internet Control Message Protocol）
SYN　同步字符（Synchronousidle）
ARP　地址解析协议（Address Resolution Protocol）
SFTP　安全文件传输协议（Security File Transfer Protocol）
CVE　通用漏洞披露（Common Vulnerabilities & Exposures）
SSH　安全外壳协议（Secure Shell Protocol）
SNMP　简单网络管理协议（Simple Network Management Protocol）
CNNVD　中国国家信息安全漏洞库（China National Vulnerability Database of Information Security）
XML　可扩展标记语言（Extensible Markup Languge）
HTTPS　超文本传输协议（HyperText Transfer Protocol Secure）
XSS　跨站脚本（Cross Site Scripting）

5　一般要求

5.1　安全要求

5.1.1　安全功能框架

本文件依据智能交通摄像机（以下简称摄像机）可能面临的安全威胁（参考附录A），规范可以缓解安全威胁的安全功能，所有安全功能组成的安全框架如图1所示。

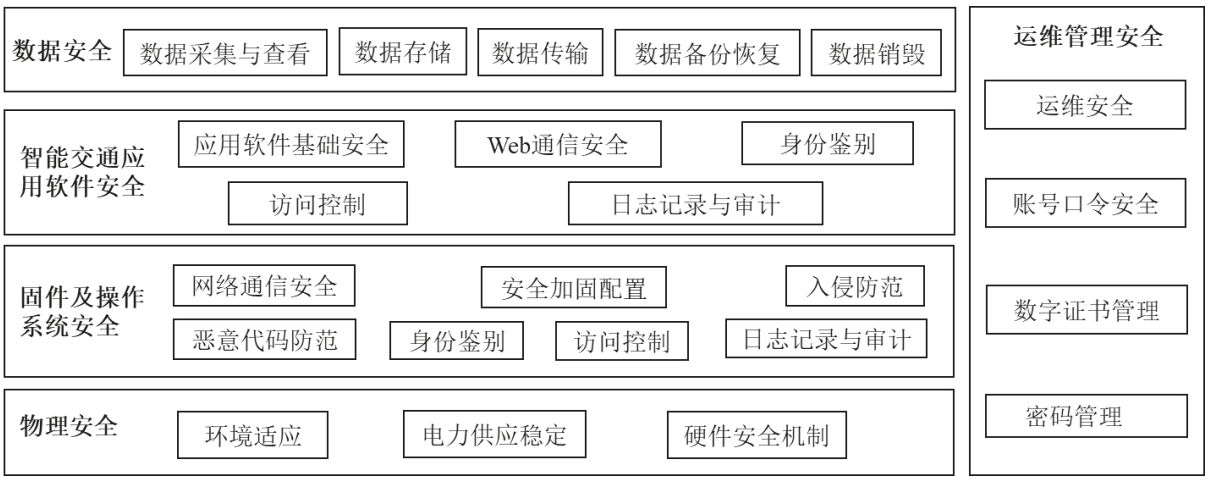

图 1 摄像机安全功能框架图

摄像机安全功能框架分为物理安全、固件及操作系统安全、智能交通应用软件安全、数据安全、运维管理安全五个层次，各个层次主要涵盖以下内容：

a)　物理安全：摄像机在物理层面应具备的环境适应性、电力供应稳定、硬件安全机制方面的安全功能；
b)　固件及操作系统安全：摄像机在固件及操作系统层面应具备的网络通信安全、安全加固配置、入侵防范、恶意代码防范、身份鉴别、访问控制、日志记录与审计方面的安全功能；
c)　智能交通应用软件安全：摄像机在应用层面应具备的应用软件基础安全、Web 通信安全、身份鉴别、访问控制、日志记录与审计方面的安全功能；

d) 数据安全：摄像机在数据层面应具备的数据采集与查看安全、数据存储安全、数据传输安全、数据备份与恢复、数据销毁安全方面的安全功能；
e) 运维管理安全：摄像机在运维管理层面应具备的运维安全、账号口令安全、数字证书管理、密码管理方面的安全功能。

5.1.2 安全保障内容

安全保障要求主要规范了摄像机应满足的研发及维护过程安全，主要包括以下几个方面：
a) 产品研发安全：保障产品研发过程安全，包括产品安全设计、安全编码、安全测试、开源及第三方软件管理等；
b) 配置管理安全：保障对产品研发过程涉及的关键代码、文档、数据等进行规范化安全管控；
c) 产品发布安全：保障产品发布能够提供配套文档，向用户说明产品功能、升级指南、安全问题应急响应方案等；
d) 漏洞管理：保障产品有效生命周期内，出现安全漏洞，能够有序排查受影响的产品版本、部署的系统，帮助用户修复漏洞。

5.2 安全等级划分

安全要求划分为三个等级，第一至第三级要求逐级增强，在实现高级别要求时，低级别要求应得到满足。具体的安全要求等级划分方法见表 1 所示：

表 1 安全要求等级划分方法

安全等级	安全效果	安全功能要求	安全保障要求
第一级	● 产品具备完备的基础防护措施，攻击者难以入侵摄像机； ● 依赖研发人员个人能力，保障产品研发与维护过程基本安全。	涵盖网络通信安全、安全加固配置、日志记录与审计、身份鉴别、访问控制、Web通信安全等基础安全功能要求。	涵盖安全设计、测试、产品配套文档提供、漏洞修复响应等基本的安全保障要求。
第二级	● 提升入侵摄像机的难度，并且增加其他措施保障攻击者即使入侵摄像机，也能被及时检测和发现，难以窃取数据； ● 产品研发及维护关键环节规范化秩序化，保障产品研发及维护过程较为安全。	在第一级安全功能要求的基础上增加安全要求，包括在固件与操作系统安全部分增加入侵防范、恶意代码防范；数据安全部分增加数据存储加密；密码管理部分增加密钥管理等要求。	在第一级安全保障要求的基础上，在设计、开发、测试环节增加一些制度规范相关安全保障要求。
第三级	● 进一步提升入侵摄像机、窃取数据的难度，同时增加其他安全机制保障即使数据被窃取、伪造，也能够追溯和鉴别； ● 保障产品研发及维护过程能够达成可追溯等安全效果，产品研发及维护过程高度安全且可持续改进。	在第二级安全功能要求的基础上增加安全要求，包括在数据安全部分增加隐私保护、防伪鉴别、数据溯源等要求。	在第二级安全保障要求的基础上，增加研发过程安全应达到的效果方面的安全保障要求。

6 第一级安全要求

6.1 第一级安全功能要求

6.1.1 物理安全

本项要求包括：

a) 设备的低温、高温、恒定湿热环境适应性应满足 GA/T 1127-2013 5.1.4 章节的类别 IV 要求；
b) 设备供电应满足 GA/T 1127-2013 5.1.3 章节要求；
c) 设备应满足 GA/T 1127-2013 5.1.5.2 章节射频电磁场辐射抗扰度要求；
d) 应仅提供 RJ45 网口、RS232/485 接口、USB 接口、SD 卡接口等业务必须的物理接口，防范攻击者通过未认证接口非法访问系统内部资源。

6.1.2 固件及操作系统安全

6.1.2.1 网络通信安全

应能够防范 ICMP、SYN 泛洪与畸形报文、ARP 欺骗等常见的网络通信攻击。

6.1.2.2 安全加固配置

本项要求包括：

a) 应保障固件、操作系统及可能使用到的数据库中不存在 CVE、CNNVD 等权威漏洞库 6 个月前已公布的高危及高危以上级别漏洞；
b) 应默认安装最小必要的系统软件包，不存在开发和编译工具、网络嗅探类工具等；
c) 应默认关闭不必要的系统服务（例如，FTP 等）、通信端口；
d) 应默认对操作系统进行安全加固配置，包括但不限于对 SNMP、SSH 等系统服务加固配置；
e) 应默认禁止 ROOT 账号直接登录，且限制用户将账号权限提升至 ROOT。

6.1.2.3 身份鉴别

本项要求包括：

a) 应对登录摄像机的用户进行身份标识和鉴别，身份标识具有唯一性；
b) 应保障身份鉴别机制不可被绕过，不存在无需鉴别的特殊命令、无口令账号、特殊组合键等登录机制；
c) 如采用账号口令机制进行用户身份鉴别，应遵循 6.1.5.2 a)、b)、c)账号口令安全要求；
d) 应具备限制登录失败次数等防范暴力破解机制；
e) 应具备登录连接超时相关功能，如需继续操作则要求重新进行身份鉴别；
f) 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。

6.1.2.4 访问控制

本项要求包括：

a) 应支持用户配置 IP 地址、协议类型等访问控制策略，控制摄像机请求或响应的通信方；
b) 应对访问摄像机的主体实施最小化授权，区分普通用户、管理员用户；
c) 应仅允许经过身份鉴别的用户主体执行权限范围内的操作。

6.1.2.5 日志记录与审计

本项要求包括：

a) 应支持日志记录功能，日志记录覆盖到每个用户，支持对重要的用户行为和重要安全事件进行审计；
b) 应支持对系统启动、关闭、系统升级等记录日志；
c) 审计日志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；

d) 应对日志记录进行保护，避免受到非预期的删除、修改或覆盖等；
e) 应对日志进程进行保护，防止未经授权的中断；
f) 应支持将审计日志上传至管理平台/日志服务器，确保审计日志能够保存不少于 6 个月；
g) 应保障摄像机的日志、诊断调试信息、告警信息中不包含未经加密或脱敏处理的账号口令、个人身份证号码、姓名、电话等敏感数据。

6.1.3 智能交通应用软件安全

6.1.3.1 应用软件基础安全

本项要求包括：
a) 应支持用户根据业务需求安装、升级智能交通应用软件；
b) 应对智能交通应用软件进行完整性、真实性校验，校验通过才允许安装；
c) 应用软件应不存在 CVE、CNNVD 等权威漏洞 6 个月前已公布的高危及高危以上级别漏洞。

6.1.3.2 Web 通信安全

本项要求包括：
a) 应默认启用 SFTP、HTTPS、SSH 等安全协议进行上传、下载、请求与响应等，保障 Web 通信安全，用户如主动启用非安全协议（如 FTP）应提示安全风险；
b) 应对来自自身可控组件以外的数据进行检验，拒绝任何没有通过校验的数据，以防范 SQL/XML 注入、XSS 等攻击；
c) 应支持使用 Web 验证码等机制防范 Web 攻击；
d) 应支持设置会话超时机制，会话超时后，用户如需继续操作，应再次经过身份鉴别；
e) Web 通信过程中，当检测到用户的 IP、UserAgent 等信息发生了变化，应该强制销毁当前的会话，并要求用户重新登录。

6.1.3.3 身份鉴别

本项要求包括：
a) 应对登录用户进行身份标识和鉴别，身份标识具有唯一性；
b) 应保障身份鉴别机制不可被绕过，不存在无需鉴别的特殊命令、无口令账号、特殊组合键等跳过登录机制；
c) 应保障身份鉴别机制能够抵抗重放攻击；
d) 应支持基于账号口令进行用户身份鉴别，并遵循 6.1.5.2 账号口令安全要求；
e) 应至少支持设置人机通信账号口令有效期，口令到期时，在用户登录后提醒其修改口令；
f) 应具备登录失败处理功能，例如，限制非法登录次数、要求输入验证码等机制；
g) 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。

6.1.3.4 访问控制

本项要求包括：
a) 应对访问应用软件的主体实施最小化授权，区分普通用户、管理员用户；
b) 应仅允许经过身份鉴别的用户主体执行权限范围内的操作。

6.1.3.5 日志记录

本项要求包括：

a) 应启用应用软件安全审计功能，审计覆盖到摄像机的每个用户，对重要的用户行为和重要安全事件进行审计；
b) 应支持对应用软件安装、升级、卸载等记录日志；
c) 应保障应用软件的日志、诊断调试信息、告警信息中不应包含用户口令、个人身份证号码、姓名、电话号码等敏感数据；
d) 应对日志记录进行保护，避免受到非预期的删除、修改或覆盖等；
e) 应支持将审计日志上传至管理平台/日志服务器，确保审计日志能够保存不少于 6 个月；
f) 审计日志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；
g) 应对日志进程进行保护，防止未经授权的中断；
h) 应将设备异常告警信息记录日志。

6.1.4 数据安全

6.1.4.1 数据传输安全

本项要求包括：
a) 应采用校验技术或密码技术保证数据在传输过程中的完整性；
b) 应采用校验技术或密码技术保证数据在传输过程中的保密性。

6.1.4.2 数据备份恢复

本项要求包括：
a) 应支持对摄像机关键数据(包括但不限于：Boot 文件、配置文件、密钥文件等)，进行备份与恢复处理；
b) 应支持缓存补录，保障视频平台可从摄像机中补录断网期间的视频图片数据。

6.1.4.3 数据销毁安全

应支持数据彻底删除。

6.1.5 运维管理安全

6.1.5.1 运维安全

本项要求包括：
a) 应能够对镜头遮挡、镜头偏移等异常情况产生告警信息；
b) 应只允许管理员用户进行系统复位、数据删除、更改参数配置等运维操作；
c) 应保障漏洞修复或软件升级过程可靠，支持管理员授权后自动执行，升级时摄像机功能中断时间不应超过 10 分钟；
d) 运维操作过程中应保留不可更改、删除的审计日志。

6.1.5.2 账号口令安全

本项要求包括：
a) 应及时删除或停用多余的、过期的账户；
b) 应使用至少包括数字、大小写字母、特殊字符中的两类，长度不少于 8 位的强复杂度口令或向用户提示风险；
c) 所有口令都应支持用户自主修改，不应使用硬编码口令；
d) 用户首次登录时，应强制用户修改出厂默认口令；
e) 应保障人机账号、机机账号分离，用于程序间通信的机机账号不可作为系统维护的人机账号。

注：有关用户安全管理内容，可参考GB/T 38626-2020 8 用户安全章节内容。

6.1.5.3 密码管理

6.1.5.3.1 密码算法合规

应默认禁止使用业界已知的不安全密码算法参与密钥协商、数字签名、数据加密等高敏感场景，例如，SHA1、MD5、DES、RC4 等。

6.2 第一级安全保障要求

6.2.1 产品研发安全

本项要求包括：

a) 应进行产品安全设计并文档化管理，文档内容包括但不限于产品安全功能的工作流程、外部交互等；
b) 应制定产品代码编写规范，内容包括但不限于代码安全编写规则、命名规则、注释规则等；
c) 应保障产品发布之前经过安全测试并形成测试报告，报告内容包括但不限于已完成的安全测试用例数、用例执行情况、用例执行责任人等；
d) 产品研发过程中凡涉及使用密码技术解决保密性、完整性、真实性、不可否认性等需求的，应遵循密码相关国家标准、行业标准。

6.2.2 产品发布安全

应向用户提供本产品的配套文档，内容包括但不限于产品功能说明、产品所有初始账号口令、升级指南、安全问题应急响应方案等。

6.2.3 漏洞管理

应向用户说明产品漏洞反馈渠道、漏洞修复机制、漏洞修复期间是否需要暂停摄像机工作、漏洞修复过渡期的风险降低方案等。

7 第二级安全要求

7.1 第二级安全功能要求

7.1.1 物理安全

应满足第一级安全功能要求。

7.1.2 固件及操作系统安全

7.1.2.1 网络通信安全

在满足第一级安全功能要求的基础上，应保障摄像机接入网络获得 IP 之前，应至少经过口令机制验证设备身份，防范设备仿冒、网络私接，例如，通过 802.1X 协议实现安全接入认证。

7.1.2.2 安全加固配置

应满足第一级安全功能要求。

7.1.2.3 入侵防范

本项要求包括：

a) 应支持安全启动功能，在设备启动过程中，验证固件、操作系统等的完整性，检测到设备固件、操作系统等遭受篡改，则立即停止启动；

b) 应能够检测和识别异常超级账号、系统敏感文件篡改、进程提权等入侵行为，并提供告警。

7.1.2.4 恶意代码防范

本项要求包括：

a) 应能够对僵尸网络、挖矿程序、恶意 Rootkit 等恶意代码进行检测和识别；

b) 应使用经过数字签名校验的补丁包、升级包进行漏洞修复、系统升级。

7.1.2.5 身份鉴别

应满足第一级安全功能要求。

7.1.2.6 访问控制

应满足第一级安全功能要求。

7.1.2.7 日志记录与审计

应满足第一级安全功能要求。

7.1.3 智能交通应用软件安全

7.1.3.1 应用软件基础安全

在满足第一级安全功能要求的基础上，本项要求还包括：

a) 对于存在多个智能交通应用软件的，应对用户安装的应用软件提供沙箱隔离机制，防范不同应用软件之间相互干扰等风险；

b) 与违法行为取证等相关的应用软件在启动时应执行自检机制。

7.1.3.2 Web 通信安全

应满足第一级安全功能要求。

7.1.3.3 身份鉴别

在满足第一级安全功能要求的基础上，还应满足 GB 35114-2017 6.3.2 要求，支持基于数字证书与管理平台双向身份认证，数字证书格式应符合 GB 35114-2017 附录 A 的规定。

7.1.3.4 访问控制

应满足第一级安全功能要求。

7.1.3.5 日志记录与审计

应满足第一级安全功能要求。

7.1.4 数据安全

7.1.4.1 数据存储安全

本项要求包括：

a) 应支持对密钥文件等敏感数据进行完整性校验；

b） 应支持采用密码技术保证数据在存储过程中的保密性等。

7.1.4.2 数据传输安全

应满足第一级安全功能要求。

7.1.4.3 数据备份恢复

应满足第一级安全功能要求。

7.1.4.4 数据销毁安全

应满足第一级安全功能要求。

7.1.5 运维管理安全

7.1.5.1 运维安全

应满足第一级安全功能要求。

7.1.5.2 账号口令安全

应满足第一级安全功能要求。

7.1.5.3 数字证书管理

本项要求包括：

a） 证书私钥应加密保存，私钥保护口令应满足安全强度要求并以非明文形式存储，同时控制私钥文件和证书文件的访问权限；

b） 应支持周期性检查设备中各类型的证书是否过期或即将过期，并提供告警。

7.1.5.4 密码管理

7.1.5.4.1 密码算法合规

应满足第一级安全功能要求。

7.1.5.4.2 密钥管理

本项要求包括：

a） 至少应支持对数据加密密钥进行更新，并支持用户设定更新周期；

b） 应具备密钥分层机制，至少分为数据加密密钥、密钥加密密钥两个层级，并使用密钥加密密钥对数据加密密钥进行加密存储；

c） 应对密钥调用情况进行日志记录；

d） 用于数据加解密的密钥不应被硬编码在代码中。

7.2 第二级安全保障要求

7.2.1 产品研发安全

在满足第一级安全保障要求的基础上，本项要求还包括：

a） 应进行威胁建模分析并文档化管理，文档内容包括但不限于产品中存在的安全威胁、威胁带来的影响、建议削减措施等；

b) 应制定安全和隐私保护基线要求，内容包括但不限于身份认证、权限管理、账户口令安全、证书及密钥安全管理等通用安全规则；
c) 应依据产品安全威胁建模分析、安全基线要求等，对产品进行安全测试；
d) 应维护产品开发使用到的开源及第三方软件列表，内容包括但不限于开源及第三方软件的版本、来源、许可证或 License 类型等。

7.2.2 配置管理安全

应进行产品版本管理工作，形成各版本产品的版本命名规则、产品功能清单等文档。

7.2.3 产品发布安全

应满足第一级安全保障要求。

7.2.4 漏洞管理

在满足第一级安全保障要求的基础上，还应建立漏洞管理规范，内容包括漏洞分级规则、受漏洞影响的产品版本排查流程、漏洞修复流程等。

8 第三级安全要求

8.1 第三级安全功能要求

8.1.1 物理安全

应满足第二级安全功能要求。

8.1.2 固件及操作系统安全

8.1.2.1 网络通信安全

在满足第二级安全功能要求的基础上，应保障摄像机接入网络获得 IP 之前，经过遵循 X.509 等通用格式的数字证书认证，防范设备仿冒、网络私接。

8.1.2.2 安全加固配置

应满足第二级安全功能要求。

8.1.2.3 入侵防范

应满足第二级安全功能要求。

8.1.2.4 恶意代码防范

应满足第二级安全功能要求。

8.1.2.5 身份鉴别

应满足第二级安全功能要求。

8.1.2.6 访问控制

应满足第二级安全功能要求。

8.1.2.7 日志记录与审计

应满足第二级安全功能要求。

8.1.3 智能交通应用软件安全

8.1.3.1 应用软件基础安全

应满足第二级安全功能要求。

8.1.3.2 Web 通信安全

应满足第二级安全功能要求。

8.1.3.3 身份鉴别

应满足第二级安全功能要求。

8.1.3.4 访问控制

应满足第二级安全功能要求。

8.1.3.5 日志记录与审计

应满足第二级安全功能要求。

8.1.4 数据安全

8.1.4.1 数据采集与查看安全

本项要求包括：

a) 应支持对视频图像数据添加鉴别信息，用于鉴别某视频图像数据是否遭篡改；
b) 应支持在用户查看视频图像数据时，添加含有用户唯一标识的溯源信息；
c) 数据查看时应支持对人脸等隐私信息进行遮挡。

8.1.4.2 数据存储安全

应满足第二级安全功能要求。

8.1.4.3 数据传输安全

应满足第二级安全功能要求。

8.1.4.4 数据备份恢复

应满足第二级安全功能要求。

8.1.4.5 数据销毁安全

应满足第二级安全功能要求。

8.1.5 运维管理安全

8.1.5.1 运维安全

应满足第二级安全功能要求。

8.1.5.2 账号口令安全

应满足第二级安全功能要求。

8.1.5.3 数字证书管理

在满足第二级安全功能要求的基础上，本项要求还包括：

a) 应支持对证书的吊销状态进行验证；

b) 当检测到证书过期或被吊销时，应支持在线更新证书。

8.1.5.4 密码管理

8.1.5.4.1 密码算法合规

在满足第二级安全功能要求的基础上，还应优先采用国家商用密码算法。

8.1.5.4.2 密钥管理

在满足第二级安全功能要求的基础上，密钥管理应分为数据加密密钥、密钥加密密钥、根密钥三个层级。

8.2 第三级安全保障要求

8.2.1 产品研发安全

在满足第二级安全保障要求的基础上，还应保障产品研发中使用到的开源或第三方软件不存在已明确停止服务（EOS）或含有 CNNVD 权威漏洞库 6 个月前披露的高危及高危以上漏洞等情况。

8.2.2 配置管理安全

在满足第二级安全保障要求的基础上，本项要求还包括：

a) 应进行产品配置管理工作，包括对配置项的定义、对配置项的修改、删除等进行权限管控；

b) 应保障产品运行过程中遇到问题，可以追溯到对应的二进制包、源代码包，以辅助定位、解决问题。

8.2.3 产品发布安全

应满足第二级安全保障要求。

8.2.4 漏洞管理

在满足第二级安全保障要求的基础上，还应能够在漏洞处置过程中（包括自研软件及使用到的开源或第三方软件漏洞），判断该漏洞是否影响现网已部署的同类产品。

附 录 A
（资料性）
摄像机安全威胁分析

摄像机常见安全威胁见表 A.1。

表 A.1 摄像机常见安全威胁

威胁来源	关键威胁	削减措施
物理层面	物理遮挡镜头	系统识别异常，并产生告警信息
	镜头偏移	系统告警
	物理接口私接	物理接口最少化
	物理插拔SD卡	本地数据加密
	私自插拔、网络私接	告警，接入认证（如，802.1x认证协议）
固件及操作系统层面	泛洪、畸形报文等网络攻击	流量控制、黑白名单等网络访问控制策略配置
	漏洞利用	系统最小化安装、出厂漏洞修复、默认启用安全通信协议、协议加固配置、Web通信安全
	端口扫描	端口最少化开启
	固件篡改、刷机	安全启动
	系统入侵	入侵检测
	恶意代码植入	恶意代码检测
应用层面	身份仿冒	身份鉴别（登录口令、证书验证）
	命令注入	请求参数检测
	XSS攻击	请求参数检测
	会话劫持	Web登录验证码、登录超时
	恶意软件	软件包签名校验
	非法访问	身份鉴别、访问控制、沙箱隔离机制
	权限滥用	最小化授权
数据层面	数据篡改	完整性校验
	数据泄露	安全通信协议、数据加密及密钥管理机制、日志审计
	隐私泄露	隐私遮挡
	视频图像伪造	防伪鉴别
运维管理层面	口令暴力破解	设置口令复杂度检测、初次登录强制修改厂商默认口令、口令过期检测、定期修改等机制
	操作抵赖	日志记录与审计
	不安全算法破解	默认关闭已知的不安全协议、密码算法
	密钥破解/泄漏	密钥管理

参 考 文 献

[1] 中华人民共和国密码法
[2] GB/T 15532 计算机软件测试规范
[3] GB/T 18336.3-2015 信息技术 安全技术 信息技术安全评估准则 第3部分安全保障组件
[4] GB/T 22081-2016 信息技术 安全技术 信息安全控制实践指南
[5] GB/T 30276 网络安全漏洞管理规范
[6] GB/T 30279-2020 信息安全技术 网络安全漏洞分类分级指南
[7] GB/T 37970-2019 软件过程及制品可信度评估
[8] GB/T 37939-2019 信息安全技术 网络存储安全功能要求
[9] GB/T 38626-2020 信息安全技术 智能联网设备口令保护指南
[10]GA/T XXX 公安视频图像信息系统安全功能要求 第2部分：前端设备安全功能要求
[11] NCSC install the latest software and app updates
[12] NCSC Secure development and deployment
[13] NIST SP 800-57 part2 - 2.3.8 Hierarchies and Meshes
[14] SAFE Code --- managing security risks inherent in the use of third-party components
[15] 白帽汇——2018年摄像头安全报告：网络空间测绘系列