T/SNISA

深圳市网络与信息安全行业协会团体标准

T/SNISA 001—2024

视频安全防护系统

The video security protection system

草案版次选择

XXXX - XX - XX 发布　　XXXX - XX - XX 实施

深圳市网络与信息安全行业协会　　发 布

目　　次

前　言

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

本文件由深圳市网络与信息安全行业协会提出并归口。

本文件起草单位：深圳市博通智能技术有限公司、中兴通讯股份有限公司、华测检测认证集团股份有限公司、深圳市安络科技有限公司、广东省信息安全测评中心。

本文件主要起草人：林鲁冰、钟焰涛、王智、李虹、肖建林、张建华、齐文辉、朱永进、种秋东、俞婷、甄茁、李科高、张永毅、汤明。

视频安全防护系统

1 范围

本标准规定了视频安全防护系统的系统结构、接口要求、功能要求、性能要求、安全要求、实验方法。

本标准适用于视频安全防护系统的研制、生产、销售。

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 25069-2022 信息安全技术 术语

GB/T 28181-2022 公共安全视频监控联网系统信息传输、交换、控制技术要求

3 术语和定义

GB/T 25069-2022界定的术语和定义、下列术语和定义适用于本文件。

3.1

数字水印 digital watermarking

一种将水印信息通过一定的规则与算法隐藏在数字载体（比如数字图像、数字视频和结构化数据集）中的技术。

3.2

显式水印 explicit watermark

在视频内容中明显可见的水印，通常通过对视频帧的像素值进行微调，或者通过叠加图层的方式将水印信息添加到视频上。

3.3

隐式水印 implicit watermark

通过不易被肉眼察觉的方式嵌入的视频数字水印。其特点是视频内容本身的可读性或观瞻性干扰较小。

3.4

视频监控 video surveillance

使用摄像头和相关设备来实时监视和记录特定区域或场所活动的技术和系统，能够实时查看视频录像、调阅历史数据、进行红外夜视以及远程操控，被广泛用于安全监控、防盗、交通监管、员工监管、公共安全等领域。

3.5

视频终端 video terminal

视频监控系统中，用于采集本地（现场）视频和音频等信号，并通过协议或其他系统接口将这些信号上传的终端设备。

3.6

视频防泄密客户端 video leakage prevention client

基于Windows、安卓的软件，安装在客户端上，和屏幕数据保护服务器、视频数据安全传输服务器、视频数据管控服务器等服务器配合使用，实现视频防泄密功能。

3.7

截屏 screenshot

将当前屏幕上的可视内容（包括图像、文字、图标等）捕获并保存为图像文件的过程。

3.8

录屏 screen recording

即屏幕录制，是指将终端屏幕上的内容，包括画面的变化等，实时捕捉并保存为视频文件的过程。

3.9

视频还原 video restoration

将视频安全防护系统中受保护的视频进行解密、去水印等操作，还原为原始视频的过程。

3.10

网桥模式 bridge mode

终端安全控制网关设备的部署模式之一，将设备视为一条带过滤功能的网线使用，将设备接在原有网关及内网用户之间，不用更改网络拓扑结构和配置。

3.11

路由模式 router mode

终端安全控制网关设备的部署模式之一，将设备作为网络出口，可进行NAT、端口映射等配置。

3.12

旁路模式 bypass mode

终端安全控制网关设备的部署模式之一，设备旁接在交换机上面，只对网络中的数据进行记录和监控，不对网络中的数据进行过滤和控制。

3.13

多功能视频数据保护矩阵 multi-functional video data protection matrix

保护大屏显示监控视频数据泄露的设备，包括用户端和服务器端两部分。用户端连接各类外接显示屏、拼接大屏，服务器端对各个客户端下发水印策略，从视觉安全维度实现对视频数据的安全防护。

3.14

屏幕数据保护服务器 screen data protection server

在视频安全防护系统中，用于实现对受控PC客户端进行准入和认证管理，对PC、智慧屏、大屏显示器显示画面进行屏幕防泄密水印加载等功能的软硬件集成一体化服务器。

3.15

视频网络安全态势感知平台 video network security situation awareness platform

与前端视频终端安全控制服务器进行对接，基于数据汇聚和统计，对视频网络进行安全检测的可视化预警的平台。该平台能够将复杂的视频网络安全信息转化为直观、可视化的形式，帮助决策者实时掌控安全态势，对安全隐患和安全事件进行快速反应处置。

3.16

视频数据安全传输服务器 video data secure transmission server

在针对视频数据跨域调阅传输中，实现高速视频流逐帧水印加载功能的软硬件集成一体化服务器。

3.17

视频数据管控服务器 video data control server

在视频安全防护系统中，通过视频调阅客户端的准入和认证管理、视频调阅的防泄密水印加载、视频文件的自动加密、视频文件还原和外发审批等功能对视频数据安全进行有效管控的软硬件集成一体化服务器，需要和视频防泄密客户端配合使用。

3.18

视频终端安全控制服务器 video terminal security control server

在视频安全防护系统中，实现视频终端的管理、准入控制、安全防护以及风险检测评估的软硬件集成一体化服务器。

4 系统结构

4.1 外观要求

硬件设备的外观应符合以下的要求：

a）产品表面不应有明显的凹痕、划伤、裂缝、变形和污渍；

b）表面不应有起泡、龟裂、脱落和磨损现象，金属部件不应有锈蚀；

c）表面的文字标志应清晰、端正、完整。

4.2 整体结构

视频安全防护系统由多功能视频数据保护矩阵（服务器、客户端）、屏幕数据保护服务器、视频数据安全传输服务器、视频数据管控服务器、视频终端安全控制服务器等硬件设备以及配套的服务器端、客户端软件组成，应支持以网桥模式、网关模式、旁路模式部署。视频安全防护系统的各组成部分之间的连接关系见图1。

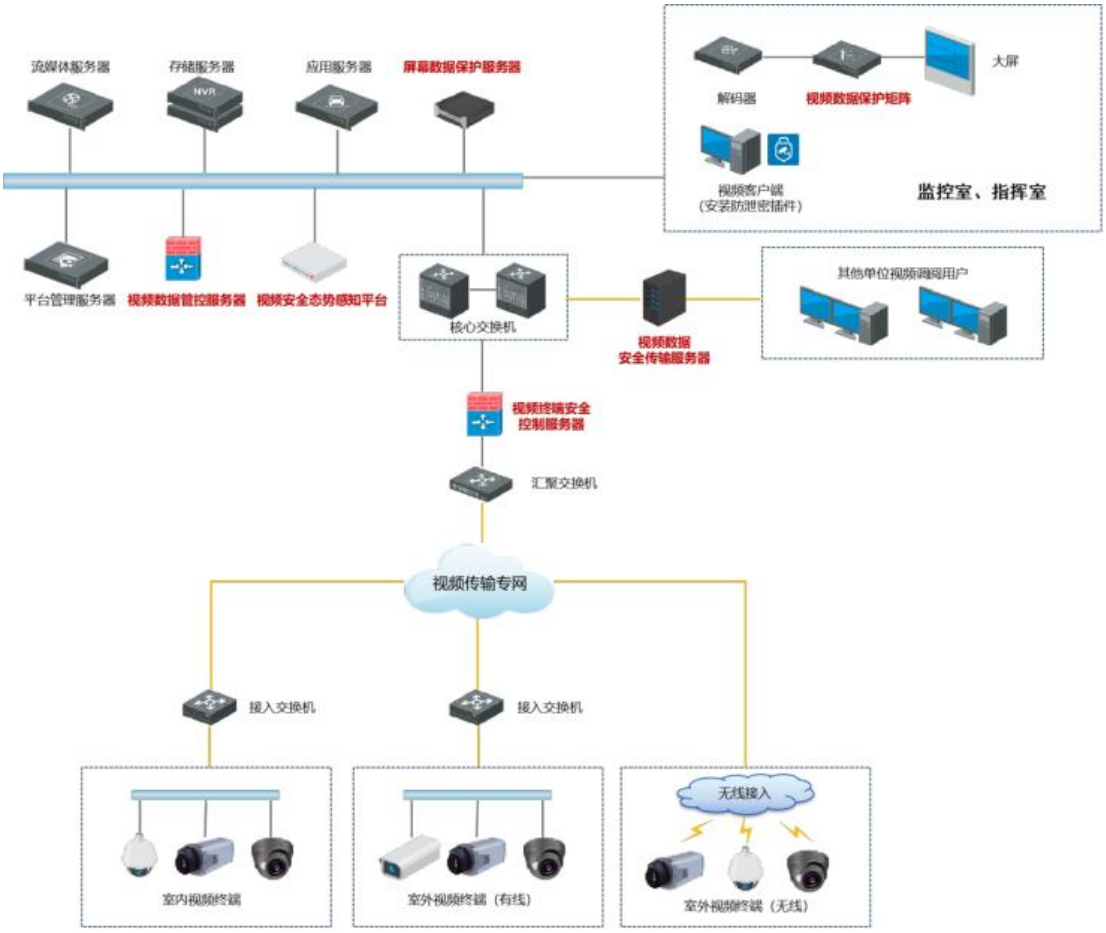

图1 视频安全防护系统各组成部分连接

5 接口要求

视频安全防护系统的设备接口满足以下要求：

a） 应支持网络接口类型为10/100/1000Mbps以太网接口，应符合IEEE802.3标准，采用RJ45连接，宜支持光纤接口、支持多路HDMI输入\输出；

b） 应支持带外管理接口；

c） 宜支持数据接口，宜采用USB接口，具有1个及以上USB2.0/3.0规范规定的USB接口。

6 功能要求

6.1 视频终端安全防护

视频安全防护系统通过视频终端安全控制服务器提供视频终端安全防护功能，应包括但不限于：

a） 通过防火墙防护网络攻击，控制视频单向传输；

b） 防止视频终端遭受DoS/DDoS攻击；

c） 建立安全漏洞库，对视频终端的安全漏洞进行防护，漏洞库的更新频率宜不低于每周更新一次；

d） 对终端进行信息安全风险评估，支持漏洞扫描和弱口令扫描功能。其中漏洞扫描基于针对视频终端的漏洞库，能够扫描出大华、海康威视等主流品牌的安全漏洞；弱口令扫描面向FTP、TELNET、SSH、RTP等主流协议。

6.2 视频水印

视频安全防护系统应实现对屏幕显示的视频加载水印的功能，且应满足：

a）支持加载显式水印、隐式水印；

b）水印内容信息可以定制；

c）能够在多种电子屏幕上实现水印功能，包括但不限于：PC电脑屏幕、电视屏幕、拼接屏、智慧屏。

6.3 视频跨域调阅控制

视频安全防护系统应对视频跨域传播进行管理和控制，实现对跨域调阅的视频数据逐帧加载水印。

6.4 防截屏和录屏

视频安全防护系统应实现客户端视频播放的防截屏/录屏功能,并对客户端视频的记录截屏/录屏操作进行记录。

6.5 客户端管理和控制

视频安全防护系统应对客户端进行管理和控制，实现以下功能：

a）客户端准入：根据IP地址、MAC地址、是否强制安装视频防泄密客户端等参数制定准入策略；

b）客户端认证：使用用户名+密码进行客户端身份认证，支持对客户端进行用户管理。

6.6 视频终端管理和控制

视频安全防护系统应对视频终端进行管理和控制，实现以下功能：

a）终端类型识别：支持识别包括大华、海康威视、宇视、科达、天地伟业、汉邦等主流视频终端，以及具体的视频终端的品牌、型号、条码；

b）终端列举：支持列出在线已准入终端列表，并支持查询；

c）自动化准入策略：支持根据设备MAC、IP、终端类型、品牌，对终端进行自动准入，并分配到不同的分组；

d）应用准入策略：支持根据应用进行允许和阻断，识别超过100种视频应用；

e）阻断策略：对私接终端，仿冒终端可以选择阻断或者是仅记录日志；

f）终端黑/白名单：支持根据VLAN，IP网段，MAC地址对流量设置黑/白名单；

g）交换机联动：支持通过SNMP协议到三层交换机上获取到终端的真实MAC地址，同时也支持通过SNMP到锐捷、华为、华三等品牌三层交换机上设置MAC地址黑名单，进行交换机联动阻断；

h）支持列出已阻断终端，并支持查询；

i）终端建档：支持国标 GB/T 28181-2022 中要求的视频终端建档信息的录入采集、传输要求；

j）IP地址池查询：对网络中的IP地址池进行管理，支持扫描IP地址池的使用状态；

k）存在安全风险终端的列举：支持列出存在安全风险的终端，并支持查询。

6.7 态势感知

视频安全防护系统应能够统计、汇聚视频系统的安全态势，应支持通过可视化屏幕，实时展示和更新视频安全统计数据。系统统计数据应包括但不限于：

a）视频终端数量、准入终端数、待准入终端数；

b）视频终端在线数量和在线率；

c）安全告警数据，包括普通、紧急、严重不同级别告警统计，最新安全告警详情滚动展示；

d）安全事件数量和分类；

e）弱口令资产数量和分布；

f）漏洞资产数量和分布；

g）安全事件数量时间趋势；

h）异常流量时间趋势展示。

6.8 日志

视频安全防护系统应对操作日志进行完整记录。以下事件应该记入日志：

a）管理员操作行为，包括登录、身份认证、系统配置、数据统计等；

b）网络攻击事件，包括针对视频终端、服务器、客户端的各类网络攻击；

c）客户端操作事件，包括客户端接入、视频调阅、视频外发等；

d）异常操作事件，包括客户端认证失败、视频终端认证失败、服务器非法访问、客户端截屏与录屏等。

7 性能要求

7.1 视频帧率

应符合GB/T 28181-2022 第5.6节的要求。

7.2 支持终端数量

应同时支持终端数量不少于1000个。

7.3 运行稳定性

设备在正常工作条件下，连续工作7×24小时,不应出现电、机械或系统的故障。

7.4 兼容性

视频安全防护系统应兼容大华、海康威视、宇视、科达、天地伟业、汉邦等主流视频终端。视频安全防护系统的客户端软件应兼容win7以上版本桌面操作系统，宜兼容信创操作系统。

8 试验方法

8.1 试验环境

除特别声明环境条件的试验外，试验应在下列环境条件下进行：

- 环境温度：6℃～42℃；
- 相对湿度：RH30%～RH75%；
- 大气压强：86kPa～110kPa。

8.2 硬件外观和结构试验

8.2.1 外观试验

通过目测法对外观进行检查。

8.2.2 结构试验

通过目测法对结构进行检查。

8.3 接口试验

目测并记录设备具有的接口类型和数量，对每个接口进行连接，并测试接口对应功能是否正常，验证接口类型和数量是否符合第5节的要求。

8.4 功能试验

8.4.1 视频终端安全防护试验

视频终端安全防护的试验方法、预期结果和结果判定方法如下。

a）试验方法：

1） 选择若干具有安全漏洞的大华、海康威视等主流品牌的视频终端，接入视频安全防护系统；

2） 为防火墙配置防护网络攻击策略；

3） 模拟发起流量劫持攻击、错误及弱配置攻击、脆弱性利用攻击、拒绝服务攻击等多种不同类型的攻击事件，检查能否防护视频终端免受上述攻击；

4） 查看安全漏洞库的最新更新日期；

5） 对视频终端进行漏洞扫描，检查能否扫描出漏洞。

b）预期结果：

1） 视频安全防护系统能够防护视频终端免受所发起的各种攻击行为；

2） 安全漏洞库的最新更新日期在试验日的一周内；

3） 能够扫描出视频终端的漏洞。

c）结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

8.4.2 视频水印试验

视频水印的试验方法、预期结果和结果判定方法如下。

a）试验方法：

1） 选择功能正常视频终端作为视频数据源接入试验系统；

2） 将PC屏幕、电视屏幕、拼接屏、智慧屏四种不同屏幕接入试验系统；

3） 使用管理员账户登录屏幕数据保护服务器，定制至少两种不同的水印信息，分别将加载显式水印、隐式水印策略下发到多功能视频数据保护矩阵、防泄密客户端；

4） 在PC屏幕、电视屏幕、拼接屏、智慧屏上分别观看水印效果。

b）预期结果：

1） 显示水印、隐式水印功能正常，且不同的定制水印信息均能生效；

2） 四种不同屏幕上水印信息均能有效。

c）结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

8.4.3 视频调阅和外发控制试验

视频调阅和外发控制的试验方法、预期结果和结果判定方法如下。

a） 试验方法：

1） 将跨域调阅客户端接入试验系统；

2） 在视频数据安全传输服务器上配置实现逐帧水印加载；

3） 在跨域调阅客户端上调阅的视频，查看是否有水印；并随机截取20帧以上屏幕截图，查看这些截取的帧是否都有水印。

b） 预期结果：在跨域调阅客户端上调阅的视频均加载水印；所有截取帧均有水印。

c） 结果判定：

满足上述预期结果判定为符合，否则判定为不符合。

8.4.4 防截屏和录屏试验

防截屏和录屏的试验方法、预期结果和结果判定方法如下。

a） 试验方法：

1） 将安装有视频防泄密客户端软件的客户端接入试验系统，确认视频数据管控服务器已接入系统并工作正常；

2） 通过该客户端调阅视频平台的视频资源，并在客户端上进行录屏和截屏操作；

3） 查看系统日志。

b） 预期结果：

1） 视频画面转变为黑屏状态；

2） 系统日志中记录上述录屏和截屏操作。

c） 结果判定：

上述预期结果均满足判定为符合，否则判定为不符合。

8.4.5 客户端管理和控制试验

客户端管理和控制的试验方法、预期结果和结果判定方法如下。

a） 试验方法：

1） 将安装有视频防泄密客户端软件的客户端接入试验系统，确认视频数据管控服务器已接入系统并工作正常；

2） 查看客户端的IP地址、MAC地址参数；

3） 通过视频数据管控服务器分别根据IP地址、MAC地址、是否强制安装视频防泄密客户端等参数分别制定不同的准入策略，并查看在不同策略配置下客户端能否接入系统；

4） 在客户端使用管理员用户名+密码进行登录，并查看能否对客户端的用户进行管理。

b） 预期结果：

1） 通过视频数据管控服务器配置的不同准入策略能够生效；

2） 在客户端使用管理员的用户名+密码能够登录成功，并且能够对客户端用户进行管理。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

8.4.6 视频终端管理和控制试验

视频终端管理和控制的试验方法、预期结果和结果判定方法如下。

a） 试验方法：

1） 将包括大华、海康威视、宇视、科达、天地伟业、汉邦品牌的不同型号视频终端接入试验系统，且其中至少一个终端使用存在安全风险的型号；

2） 通过视频终端安全控制服务器，查看列出所有接入终端，以及终端的品牌、型号、IP地址、MAC地址信息；

3） 通过视频终端安全控制服务器配置不同的准入策略、终端黑/白名单、阻断策略，查看准入策略、终端黑/白名单、阻断策略是否生效；

4） 查看是否能够列出已阻断终端；

5） 查看终端是否存在建档信息；

6） 扫描IP地址池，查看是否列出各IP地址的使用状态；

7） 查看是否列出存在安全风险的终端。

b） 预期结果：

1） 能够正确列举视频终端的品牌、型号、IP地址、MAC地址信息；

2） 配置不同的准入策略、终端黑/白名单、阻断策略均能生效；

3） 能够列出已阻断终端；

4） 终端均存在建档信息；

5） 能够列出IP地址池中各IP地址的使用状态；

6） 能够列出存在安全风险的终端。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

8.4.7 态势感知试验

态势感知的试验方法、预期结果和结果判定方法如下。

a） 试验方法：

1）将可视化大屏接入试验系统并配置为态势感知客户端，确认前端视频终端安全控制服务器接入试验系统并能够正常工作；

2）在可视化大屏上查看统计数据和图表是否包含以下数据：视频终端数量、准入终端数、待准入终端数；视频终端在线数量和在线率；安全告警数据，包括普通、紧急、严重不同级别告警统计，最新安全告警详情滚动展示；安全事件数量和分类；漏洞资产数量和分布；安全事件数量时间趋势；异常流量时间趋势。

b） 预期结果：

可视化大屏上显示的统计数据和图表包含上述数据。

c） 结果判定：

满足预期结果判定为符合，否则判定为不符合。

8.4.8 日志试验

日志的试验方法、预期结果和结果判定方法如下。

a） 试验方法：

1） 使用管理员账户进行多次不同的操作，包括登录、身份认证、系统配置、数据统计，并查看系统日志记录信息是否正确；

2） 针对视频终端、服务器，模拟发起多次不同类型的网络攻击，查看系统日志记录信息是否正确；

3） 在客户端上，使用“用户名+密码”登录后，进行多次不同的操作，包括客户端接入、视频调阅、视频外发，查看系统日志记录信息是否正确；

4） 通过配置服务器策略，并在客户端进行操作，实现异常操作状况，包括客户端认证失败、视频终端认证失败、服务器非法访问、客户端截屏与录屏，查看系统日志记录信息是否正确。

b） 预期结果：

1） 系统日志能够记录管理员账户的各类操作行为，包括登录、身份认证、系统配置、数据统计；

2） 系统日志能够记录各类的网络攻击事件；

3） 系统日志能够记录各类的客户端操作事件，包括客户端接入、视频调阅、视频外发；

4） 系统日志能够记录各类异常操作事件。

c） 结果判定：

上述预期结果均满足判定为符合，其他情况判定为不符合。

8.5 性能试验

8.5.1 视频帧率试验

视频帧率的试验方法、预期结果和结果判定方法如下。

a） 试验方法：

设置视频传播速率为25帧/秒，进行8.4的各项功能试验。

b） 预期结果：

各项功能试验均判定为符合。

c） 结果判定：

满足预期结果时判定为符合，否则判定为不符合。

8.5.2 支持终端数量试验

终端数量的试验方法、预期结果和结果判定方法如下。

a） 试验方法：

接入1000个视频终端，进行8.4的各项功能试验。

b） 预期结果：

各项功能试验均判定为符合。

c） 结果判定：

满足预期结果时判定为符合，否则判定为不符合。

8.5.3 运行稳定性试验

在正常工作条件下运行系统，连续工作7×24小时，应满足7.3的要求。

9 检验规则

9.1 检验分类

系统的检验分为型式检验、出厂检验两种。通过型式检验合格后，才能批量生产。检验项目如下表所示。

表1 型式检验和出厂检验项目

序号	检验项目	技术要求	试验方法	型式检验	出厂检验
1	外观要求	4.1	8.2.1	√	√
2	整体结构	4.2	8.2.2	√	√
3	接口要求	5	8.3	√	√
4	视频终端安全防护	6.1	8.4.1	√	-
5	视频水印	6.2	8.4.2	√	-
6	视频跨域调阅控制	6.3	8.4.3	√	-
7	防截屏和录屏	6.4	8.4.4	√	-
8	客户端管理和控制	6.5	8.4.5	√	-
9	视频终端管理和控制	6.6	8.4.6	√	-
10	态势感知	6.7	8.4.7	√	-

11	日志	6.8	8.4.8	√	-
12	视频帧率	7.1	8.5.1	√	-
13	支持终端数量	7.2	8.5.2	√	-
14	运行稳定性	7.3	8.5.3	√	-
注：√表示必检项目；- 表示选检项目。					

9.2 型式检验

凡有下列情况之一时，应进行型式检验：

a) 新产品投产或老产品转产生产的试制定型鉴定；

b) 正式生产后，如果结构、材料有较大改变，可能影响产品性能；

c) 正式生产后，周期性进行检验；

d) 产品长期停产后，恢复生产；

e) 国家质量监督机构提出型式检验要求；

f) 项目招标要求；

g) 合同规定；

h) 其他法律法规要求。

型式检验的样品应从出厂检验合格的产品中随机抽取，检验结果按照如下规则给出：

a) 检测数据全部符合要求，则判定该批产品合格；

b) 检测数据有一项不符合要求，则抽取双倍数量产品对该项指标进行复检。若复检合格，则判定该批产品合格；否则判定该批产品不合格。

9.3 出厂检验

出厂检验由公司的质量检验部门按照表1进行检验，合格后签发合格证，方可出厂。若在出厂检验过程中发现不合格，则应返修；返修后应重新对不合格项进行检验。

10 标志、包装、运输、贮存

10.1 标志

10.1.1 产品

硬件设备产品上应有标志，标志的文字、符号、图形等应清晰，内容包括：

a) 企业标志；

b) 产品名称及型号；

c) 产品编号。

10.1.2 合格证

合格证上应有以下标志：

a) 产品名称及型号；

b) 产品标号；

c) 检验员印章；

d) 出厂日期；

e) 厂址。

10.2 包装

包装箱应设置防潮、防震的要求。包装箱内应附带下列文件：

a）产品合格证；

b）产品使用说明书；

c）保修卡。

10.3 运输

硬件设备产品在运输过程中应防碰撞、防雨淋。

10.4 贮存

包装后的设备应存放在温度为0℃～42℃，相对湿度不超过80%，无腐蚀性气体、通风良好的室内。