

ICS 33.050

M 30

团 体 标 准

T/TAF XXX-2021



网络关键设备安全通用检测方法

General security testing methods for critical network devices

2021-xx-xx 发布

2021-xx-xx 实施

电信终端产业协会 发布

目 次

前言	II
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	1
5 测试环境	2
6 安全功能检测方法	3
6.1 设备标识安全	3
6.2 冗余、备份恢复与异常检测	3
6.3 漏洞和恶意程序防范	6
6.4 预装软件启动及更新安全	7
6.5 用户身份标识与鉴别	10
6.6 访问控制安全	13
6.7 日志审计安全	16
6.8 通信安全	18
6.9 数据安全	20
7 安全保障要求评估方法	21
7.1 设计和开发	21
7.2 生产和交付	24
7.3 运行和维护	26
附录 A（资料性）主要部件清单	31
参考文献	32

前 言

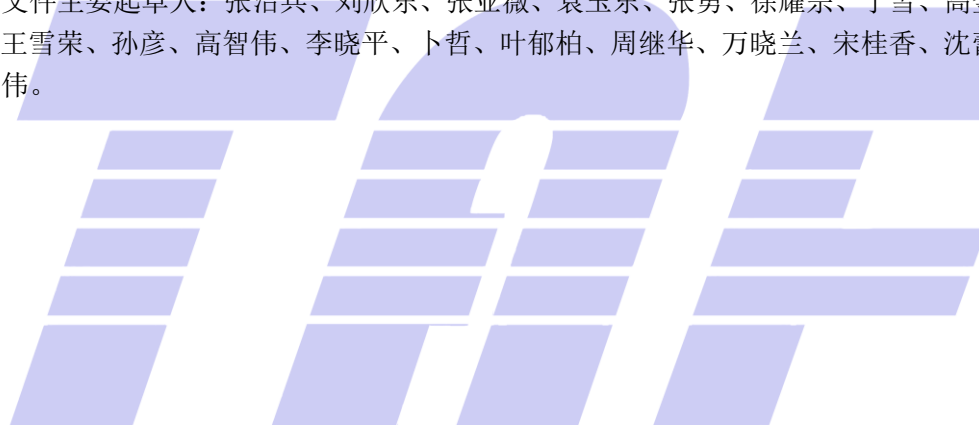
本文件按照 GB/T 1.1-2020《标准化工作导则 第1部分：标准化文件的结构和起草规则》的规定起草。

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。

本文件由电信终端产业协会（TAF）提出并归口。

本文件起草单位：中国信息通信研究院、国家计算机网络与信息安全管理中心、国家工业信息安全发展研究中心、中国电子技术标准化研究院、工业和信息化部电子第五研究所、北京通和实益电信科学技术研究所有限公司、上海泰峰检测认证有限公司、西安通和电信设备检测有限公司、信息产业有线通信产品质量监督检验中心、武汉网锐检测科技有限公司、中国电信股份有限公司研究院（广东）、中汽研软件测评（天津）有限公司、华为技术有限公司、中兴通讯股份有限公司、新华三技术有限公司、浪潮（北京）电子信息有限公司、宁波和利时信息安全研究院有限公司、浙江中控技术股份有限公司、上海诺基亚贝尔股份有限公司、联想（北京）有限公司。

本文件主要起草人：张治兵、刘欣东、张亚薇、袁玉东、张勇、徐耀宗、丁雪、高金君、舒敏、龚志红、王雪荣、孙彦、高智伟、李晓平、卜哲、叶郁柏、周继华、万晓兰、宋桂香、沈蕾、李汝鑫、章维、刘伟。



网络关键设备安全通用检测方法

1 范围

本文件规定了网络关键设备安全通用检测方法。

本文件适用于网络关键设备的检测，还可用于指导网络关键设备的研发、测试等工作。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是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 信息安全技术 术语

GB 40050-2021 网络关键设备安全通用要求

GB/T 39680-2020 信息安全技术 服务器安全技术要求和测评准则

3GPP TS 33.117 通用安全保障要求 (Catalogue of general security assurance requirements)

3 术语和定义

GB/T 25069 和 GB 40050-2021 中界定的以及下列术语和定义适用于本文件。

3.1

网络关键设备 critical network device

支持连网功能，在同类网络设备中具有较高性能的设备，通常应用于重要网络节点、重要部位或重要系统中，一旦遭到破坏，可能引发重大网络安全风险。

注：具有较高性能是指设备的性能指标或规格符合《网络关键设备和网络安全专用产品目录》中规定的范围。

[来源：GB/T 40050-2021，3.7]

4 缩略语

下列缩略语适用于本文件。

ASCII：美国信息交换标准代码 (American Standard Code for Information Interchange)

HTTP：超文本传输协议 (Hyper Text Transfer Protocol)

IP：互联网协议 (Internet Protocol)

IPv4：互联网通信协议第四版 (Internet Protocol Version 4)

IPv6：互联网通信协议第六版 (Internet Protocol Version 6)

MAC：媒体访问控制 (Media Access Control)

MD5：消息摘要算法 (Message Digest Algorithm MD5)

NTP：网络时间协议 (Network Time Protocol)

SNMP：简单网络管理协议 (Simple Network Management Protocol)

SSH：安全壳协议 (Secure Shell)

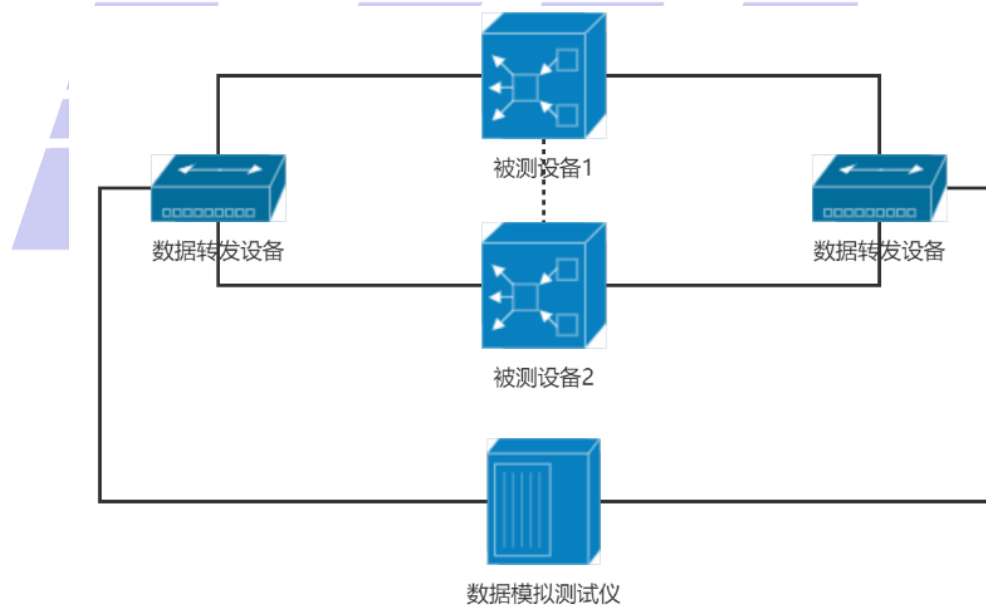
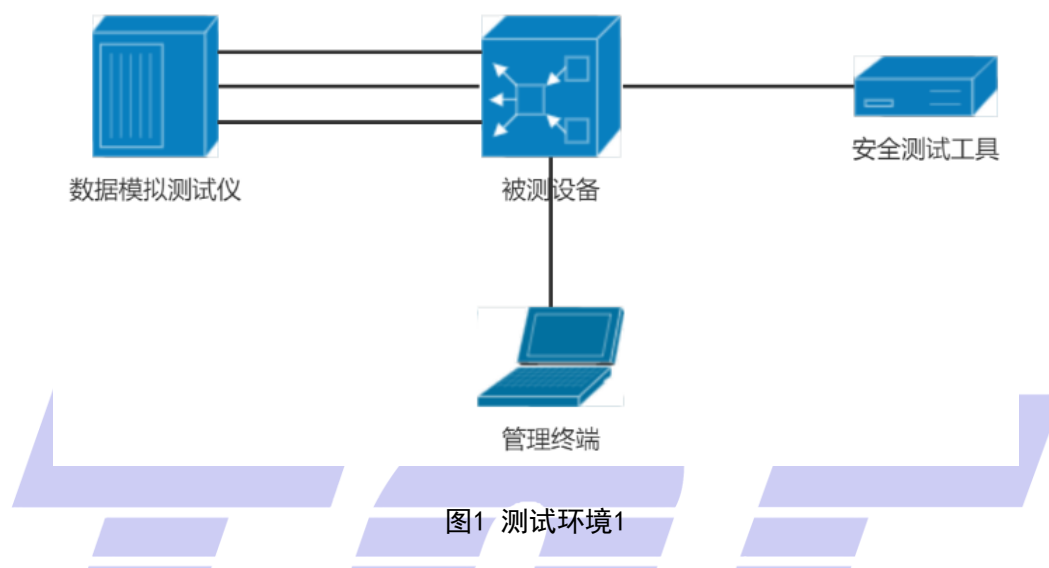
TCP: 传输控制协议(Transmission Control Protocol)

UDP: 用户数据报协议(User Datagram Protocol)

WEB: 全球广域网(World Wide Web)

5 测试环境

测试环境如图所示。



数据模拟测试仪一般连接到被测设备的业务接口，用于模拟发送网络数据包、工业控制数据包等数据。安全测试工具一般连接到设备的业务接口或管理接口，用于进行漏洞扫描、端口扫描等安全测试。管理终端一般连接到被测设备的管理接口，用于对被测设备进行配置管理或状态监控。数据转发用于连接数据模拟测试仪与被测设备，实现二者之间网络数据或工业控制数据的互通。

6 安全功能检测方法

6.1 设备标识安全

6.1.1 硬件标识安全

该检测项包括如下内容：

a) 安全要求：

硬件标识安全要求见 GB40050-2021 5.1 a)。

硬件整机和主要部件应具备唯一性标识。

注：路由器、交换机常见的主要部件：主控板卡、业务板卡、交换网板、风扇模块、电源、存储系统软件的板卡、硬盘或闪存卡等。服务器常见的主要部件：中央处理器、硬盘、内存、风扇模块、电源等。

b) 预置条件：

厂商提供设备硬件配置说明材料。

c) 检测方法：

- 1) 检查硬件整机是否具备唯一性标识；
- 2) 检查设备的主要部件是否具备唯一性标识，主要部件清单参考附录 A。

d) 预期结果：

- 1) 硬件整机具备唯一性标识；
- 2) 主要部件具备唯一性标识。

e) 判定原则：

- 1) 测试结果应与预期结果相符，否则不符合要求。
- 2) 硬件、部件唯一性标识可以是序列号等标识信息。

6.1.2 软件标识安全

该检测项包括如下内容：

a) 安全要求：

软件标识安全要求见 GB40050-2021 5.1 b)。

应对预装软件、补丁包/升级包的不同版本进行唯一性标识。

注：常见的版本唯一性标识方式：版本号等。

b) 预置条件：

厂商提供设备运行所需的预装软件/固件，以及可用的补丁包/升级包。

c) 检测方法：

- 1) 检查预装软件/固件是否具备唯一性标识；
- 2) 检查补丁包/升级包是否具备唯一性标识。

d) 预期结果：

- 1) 预装软件/固件具备唯一性标识；
- 2) 补丁包/升级包具备唯一性标识。

e) 判定原则：

- 1) 测试结果应与预期结果相符，否则不符合要求；
- 2) 软件唯一性标识可以是分配的唯一版本号、软件哈希值等标识信息中的一个或多个。

6.2 冗余、备份恢复与异常检测

6.2.1 设备冗余和自动切换功能

网络关键设备整机应支持主备切换功能或关键部件应支持冗余功能。网络关键设备应至少通过6.2.1.1设备冗余和自动切换功能（整机冗余）和6.2.1.2设备冗余和自动切换功能（部件冗余）中的一项测试。

6.2.1.1 设备冗余和自动切换功能（整机冗余）

该检测项包括如下内容：

a) 安全要求：

设备冗余和自动切换功能（整机冗余）安全要求见GB40050-2021 5.2 a）。

设备整机应支持主备切换功能或关键部件应支持冗余功能，应提供自动切换功能，在设备或关键部件运行状态异常时，切换到冗余设备或冗余部件以降低安全风险。

注：路由器、交换机常见的支持冗余功能的关键部件：主控板卡、交换网板、电源模块、风扇模块等。服务器常见的支持冗余功能的关键部件：硬盘、电源模块、风扇模块等。

b) 预置条件：

- 1) 按测试环境 2 搭建好测试环境；
- 2) 两台设备分别配置为主用设备与备用设备或负载分担模式。

c) 检测方法：

- 1) 测试仪表两对端口之间发送背景流量或与多台设备进行输入输出控制；
- 2) 下线主用设备或负载分担模式下的被测设备 1；
- 3) 查看数据流量或输入输出控制是否自动切换到备用设备或负载分担模式下的被测设备 2；
- 4) 重新上线主用设备或负载分担模式下的被测设备 1；
- 5) 主用设备或负载分担模式下的被测设备 1 恢复正常运行后，查看数据流量状态或输入输出控制状态是否正常。

d) 预期结果：

- 1) 在步骤 3 中，备用设备或负载分担模式下的被测设备 2 能自动启用，数据流量或输入输出控制能切换到备用设备或负载分担模式下的被测设备 2 上；
- 2) 在步骤 5 中，主用设备或负载分担模式下的被测设备 1 能正常运行，且数据流量状态或输入输出控制状态正常。

e) 判定原则：

- 1) 测试结果应与预期结果相符，否则不符合要求；
- 2) 主备模式和负载分担模式支持一种即可。

6.2.1.2 设备冗余和自动切换功能（部件冗余）

该检测项包括如下内容：

a) 安全要求：

设备冗余和自动切换功能（部件冗余）安全要求见 GB40050-2021 5.2 a）。

设备整机应支持主备切换功能或关键部件应支持冗余功能，应提供自动切换功能，在设备或关键部件运行状态异常时，切换到冗余设备或冗余部件以降低安全风险。

注：路由器、交换机常见的支持冗余功能的关键部件：主控板卡、交换网板、电源模块、风扇模块等。服务器常见的支持冗余功能的关键部件：硬盘、电源模块、风扇模块等。

b) 预置条件：

- 1) 厂商提供支持冗余和自动切换的部件清单；
- 2) 按测试环境 1 搭建好测试环境；
- 3) 被测设备关键部件配置冗余。

- c) 检测方法：
服务器安全检测方法参见 GB/T 39680-2020 6.2.5 a) 1) 2)。
其他网络关键设备按照以下步骤进行检测：
- 1) 按照厂商提供的关键冗余部件说明文档，分别拔掉或关闭处于运行状态的关键部件，等待一段时间并观察被测设备的工作状态；
 - 2) 查看被测设备是否能够自动启用备用关键部件。
- d) 预期结果：
服务器安全检测预期结果参见 GB/T 39680-2020 6.2.5 b) 1) 2)。
其他网络关键设备检测预期结果如下：
- 1) 被测设备可以自动启用备用关键部件，工作正常。
- e) 判定原则：
服务器判定原则参见 GB/T 39680-2020 6.2.5 c) 1) 2)。
其他网络关键设备检测判定原则如下：
- 1) 测试结果应与预期结果相符，否则不符合要求。

6.2.2 备份与恢复功能

该检测项包括如下内容：

- a) 安全要求：
备份与恢复功能安全要求见 GB40050-2021 5.2 b)。
应支持对预装软件、配置文件的备份与恢复功能，使用恢复功能时支持对预装软件、配置文件的完整性检查。
- b) 预置条件：
按测试环境 1 搭建好测试环境。
- c) 检测方法：
- 1) 配置被测设备正常工作；
 - 2) 分别针对预装软件、配置文件执行备份操作；
 - 3) 清空或重置设备配置，保存并重启；
 - 4) 恢复预装软件到被测设备并重启，查看设备是否能够以预装软件启动，并恢复到正常工作状态；
 - 5) 恢复配置文件到被测设备，查看设备配置是否恢复到备份前工作状态；
 - 6) 修改备份的预装软件和配置文件，并重复步骤 4-5。
- d) 预期结果：
- 1) 步骤 2 中，软件和配置文件备份成功；
 - 2) 步骤 4 中，恢复的软件工作正常；
 - 3) 步骤 5 中，设备配置与备份前一致；
 - 4) 步骤 6 中，设备能够检测到软件和配置已被修改。
- e) 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.2.3 异常状态识别与提示功能

该检测项包括如下内容：

- a) 安全要求：
异常状态识别与提示功能安全要求见 GB40050-2021 5.2 c)。

应支持识别异常状态，产生相关错误提示信息。

- b) 预置条件：
按测试环境 1 搭建好测试环境。
- c) 检测方法：
服务器安全检测方法参见 GB/T 39680-2020 6.2.5 a) 5)。
其他网络关键设备按照以下步骤进行检测：
1) 根据设备使用说明触发设备处于异常的运行状态并产生错误提示信息。
- d) 预期结果：
服务器安全检测预期结果参见 GB/T 39680-2020 6.2.5 b) 5)。
其他网络关键设备检测预期结果如下：
1) 被测设备支持识别异常状态，产生相应错误提示信息，提供故障的告警、定位等功能。
- e) 判定原则：
1) 测试结果应与预期结果相符，否则不符合要求。

6.3 漏洞和恶意程序防范

6.3.1 漏洞扫描

- a) 安全要求：
漏洞扫描安全要求见 GB40050-2021 5.3 a)。
不应存在已公布的漏洞，或具备补救措施防范漏洞安全风险。
- b) 预置条件：
1) 按测试环境 1 搭建好测试环境；
2) 厂商提供具有管理员权限的账号，用于登录设备；
3) 按照产品说明书进行初始配置，并启用相关的协议和服务；
4) 扫描所使用的工具及其知识库需使用最新版本。
- c) 检测方法：
典型的漏洞扫描方式包括系统漏洞扫描、WEB应用漏洞扫描等，扫描应覆盖具有网络通信功能的各类接口。
1) 系统漏洞扫描：
利用系统漏洞扫描工具通过业务接口和管理接口分别对被测设备系统进行扫描(包含登录扫描和非登录扫描两种方式)，查看扫描结果；
2) WEB应用漏洞扫描(设备不支持WEB功能时不适用)：
利用WEB应用漏洞扫描工具通过业务接口和管理接口分别对WEB应用进行扫描(包含登录扫描和非登录扫描两种方式)，查看扫描结果。
3) 对于以上扫描发现的安全漏洞，检查是否具备补救措施。
- d) 预期结果：
分析扫描结果，没有发现安全漏洞；或者根据扫描结果中，发现了安全漏洞，针对发现的漏洞具备相应的补救措施。
- e) 判定原则：
1) 测试结果应与预期结果相符，否则不符合要求；
2) 常见的补救措施包括修复、规避等措施，如直接修复(打补丁等)、通过相关配置来规避风险(如关闭相关功能或者协议等)。

6.3.2 恶意程序扫描

该检测项包括如下内容：

- a) 安全要求：
 - 恶意程序扫描安全要求见 GB40050-2021 5.3 b)。
 - 预装软件、补丁包/升级包不应存在恶意程序。
- b) 预置条件：
 - 1) 按测试环境 1 搭建好测试环境；
 - 2) 厂商提供具有管理员权限的账号，用于登录设备操作系统；
 - 3) 按照产品说明书进行初始配置，并启用相关的协议和服务，准备开始扫描；
 - 4) 扫描所使用的工具需使用最新版本。
- c) 检测方法：
 - 使用两个不同的恶意程序扫描工具对被测设备预装软件、补丁包/升级包进行扫描，查看是否存在恶意程序。
- d) 预期结果：
 - 未发现设备预装软件、补丁包/升级包存在恶意程序。
- e) 判定原则：
 - 测试结果应与预期结果相符，否则不符合要求。

6.3.3 设备功能和访问接口声明

该检测项包括如下内容：

- a) 安全要求：
 - 设备功能和访问接口声明安全要求见 GB40050-2021 5.3 c)。
 - 不应存在未声明的功能和访问接口（含远程调试接口）。
- b) 预置条件：
 - 1) 厂商提供设备所支持的功能和访问接口清单；
 - 2) 厂商提供管理员权限账号；
 - 3) 厂商说明不存在未声明的功能和访问接口。
- c) 检测方法：
 - 服务器安全检测方法参见 GB/T 39680-2020 6.2.6.2 a) 3)。
 - 其他网络关键设备按照以下步骤进行检测：
 - 1) 使用管理员权限账号登录设备，检查设备所支持的功能是否与文档一致；
 - 2) 查看系统访问接口（含远程调试接口）是否与文档一致。
- d) 预期结果：
 - 服务器安全检测预期结果参见 GB/T 39680-2020 6.2.6.2 b) 3)。
 - 其他网络关键设备检测预期结果如下：
 - 1) 设备支持的功能和访问接口（含远程调试接口）与文档一致；
 - 2) 不存在未声明的功能和访问接口（含远程调试接口）。
- e) 判定原则：
 - 测试结果应与预期结果相符，否则不符合要求。

6.4 预装软件启动及更新安全

6.4.1 预装软件启动完整性校验功能

该检测项包括如下内容：

- a) 安全要求：

预装软件启动完整性校验功能安全要求见 GB40050-2021 5.4 a)。
应支持启动时完整性校验功能，确保系统软件不被篡改。

- b) 预置条件：
 - 1) 测试环境 1 搭建好测试环境；
 - 2) 厂商在设备中预先安装系统软件包。
- c) 检测方法：
 - 1) 破坏预装系统软件的完整性，重启设备。
- d) 预期结果：
 - 步骤 1 和步骤 2 中，设备应有告警提示信息且无法正常启动。
- e) 判定原则：
 - 测试结果应与预期结果相符，否则不符合要求。

6.4.2 更新功能

该检测项包括如下内容：

- a) 安全要求：
 - 更新功能安全要求见 GB40050-2021 5.4 b)。
 - 应支持设备预装软件更新功能。
- b) 预置条件：
 - 1) 按测试环境 1 搭建好测试环境；
 - 2) 厂商提供被测设备预装软件；
 - 3) 厂商提供用于更新的软件包。
- c) 检测方法：
 - 1) 检查预装软件是否可进行更新。
- d) 预期结果：
 - 1) 预装软件可成功更新。
- e) 判定原则：
 - 测试结果应与预期结果相符，否则不符合要求。

6.4.3 更新操作安全功能

该检测项包括如下内容：

- a) 安全要求：
 - 更新操作安全功能安全要求见 GB40050-2021 5.4 c)。
 - 应具备保障软件更新操作安全的功能。

注：保障软件更新操作安全的功能包括用户授权、更新操作确认、更新过程控制等。例如，仅指定授权用户可实施更新操作，实施更新操作的用户需经过二次鉴别，支持用户选择是否进行更新，对更新操作进行二次确认或延时生效等。

- b) 预置条件：
 - 1) 按测试环境 1 搭建好测试环境；
 - 2) 厂商提供用户手册。
- c) 检测方法：
 - 服务器安全检测方法参见 GB/T 39680-2020 6.2.3.2 a) 1)。
 - 其他网络关键设备按照以下步骤进行检测：

- 1) 检查设备是否支持通过用户授权的方式保障软件更新安全,只有授权用户能够执行更新操作,非授权用户不能执行更新操作;
 - 2) 检查设备是否支持更新操作确认功能,确认的方式可包括:选择更新或不更新;通过二次鉴别的方式进行确认;对授权用户提示更新操作在特定时间段或特定操作之后才能生效,生效之前可撤销。
- d) 预期结果:
服务器安全检测预期结果参见 GB/T 39680-2020 6.2.3.2 b) 1)。
其他网络关键设备检测预期结果如下:
- 1) 只有授权用户能够执行更新操作,非授权用户不能执行更新操作;
 - 2) 设备支持检测方法 2) 中的至少一种更新操作确认方式。
- e) 判定原则:
测试结果应与预期结果相符,否则不符合要求。

6.4.4 软件更新防篡改功能

该检测项包括如下内容:

- a) 安全要求:
软件更新防篡改功能安全要求见 GB40050-2021 5.4 d)。
应具备防范软件在更新过程中被篡改的安全功能。
- 注:防范软件在更新过程中被篡改安全功能包括采用非明文的信道传输更新数据、支持软件包完整性校验等。
- b) 预置条件:
- 1) 按测试环境 1 搭建好测试环境;
 - 2) 厂商提供预装软件的更新包、说明材料;
 - 3) 厂商提供签名验证的工具或指令。
- c) 检测方法:
- 1) 被测设备支持网络更新方式时,配置被测设备开启更新,并尝试获得更新包,在更新过程中,抓取数据包,查看是否为非明文数据;
 - 2) 修改厂商提供的预装软件更新包并尝试更新,检查是否可以完成更新过程。
- d) 预期结果:
- 1) 被测设备支持网络更新方式时,设备可获取到所需要的更新包,更新数据传输通道支持加密传输,数据包被加密,非明文传输;
 - 2) 修改后的预装软件更新包无法完成更新过程。
- e) 判定原则:
测试结果应与预期结果相符,否则不符合要求。

6.4.5 更新过程告知功能

该检测项包括如下内容:

- a) 安全要求:
更新过程告知功能安全要求见 GB40050-2021 5.4 e)。
应有明确的信息告知用户软件更新过程的开始、结束以及更新的内容。
- b) 预置条件:
- 1) 按测试环境 1 搭建好测试环境;
 - 2) 厂商提供的被测设备有预装软件更新的能力。
- c) 检测方法:

- 1) 检查是否对此次更新的内容进行说明，可以通过文档或软件提示信息等方式进行说明；
 - 2) 检查更新过程中有无提示开始和结束的信息；
 - 3) 检查更新过程中有无更新步骤信息或更新进度信息显示。
- d) 预期结果：
- 1) 具备更新的内容说明；
 - 2) 具备更新开始提示信息和结束提示信息；
 - 3) 更新过程中显示更新步骤或更新进度信息。
- e) 判定原则：
- 测试结果应与预期结果相符，否则不符合要求。

6.5 用户身份标识与鉴别

6.5.1 身份标识和鉴别功能

该检测项包括如下内容：

- a) 安全要求：
- 身份标识和鉴别功能安全要求见 GB40050-2021 5.5 a)。
应对用户进行身份标识和鉴别，身份标识应具有唯一性。
- b) 预置条件：
- 1) 按测试环境 1 搭建好测试环境；
 - 2) 厂商提供被测设备的管理账号和口令。
- c) 检测方法：
- 服务器安全检测方法参见 GB/T 39680-2020 6.2.6.1 a) 1)。
其他网络关键设备按照以下步骤进行检测：
- 1) 使用管理账号和正确口令以及错误口令分别登录设备，检查是否登录成功；
 - 2) 登录被测设备，创建新的账号和口令，并使用新账号和口令以及新账号和空口令尝试登录设备，检查是否登录成功；
 - 3) 尝试创建与步骤 2 中具有相同用户身份标识的账号，检查是否能够成功创建。
- d) 预期结果：
- 服务器安全检测预期结果参见 GB/T 39680-2020 6.2.6.1 b) 1)。
其他网络关键设备检测预期结果如下：
- 1) 步骤 1，正确的口令登录成功，错误的口令登录失败；
 - 2) 步骤 2，使用新账号和口令登录成功，使用新账号和空口令登录失败；
 - 3) 步骤 3，创建失败。
- e) 判定原则：
- 测试结果应与预期结果相符，否则不符合要求。

6.5.2 口令安全——默认口令、口令生存周期

该检测项包括如下内容：

- a) 安全要求：
- 口令安全——默认口令、口令生存周期安全要求见 GB40050-2021 5.5 b)。
使用口令鉴别方式时，应支持首次管理设备时强制修改默认口令或设置口令，或支持随机的初始口令，支持设置口令生存周期。
- b) 预置条件：
- 1) 按测试环境 1 搭建好测试环境；

- 2) 厂商提供口令鉴别方式相关的说明文档，包括不限于默认设备管理方式、默认口令、口令生存周期等内容；
 - 3) 被测设备处于出厂默认配置状态。
- c) 检测方法：
- 1) i: 若被测设备存在默认口令，则使用默认账号登录被测设备，检查被测设备是否强制修改默认口令，或使用随机的初始口令；
ii: 若被测设备不存在默认口令，则检查是否强制设置口令；
 - 2) 检查被测设备是否支持设置口令生存周期。
- d) 预期结果：
- 首次管理关键设备时，系统提示强制修改默认口令或者设置口令，或支持随机的初始口令，支持设置口令生存周期。
- e) 判定原则：
- 测试结果应与预期结果相符，否则不符合要求。

6.5.3 口令安全——口令复杂度、口令显示

该检测项包括如下内容：

- a) 安全要求：
- 口令安全——口令复杂度、口令显示安全要求见 GB40050-2021 5.5 b) c) 。
- 1) 支持口令复杂度检查功能，口令复杂度检查包括口令长度检查、口令字符类型检查、口令与账号无关性检查中的至少一项；
- 注：不同类型的网络关键设备口令复杂度要求和实现方式不同。常见的口令长度要求示例：口令长度不小于8位；常见的口令字符类型示例：包含数字、小写字母、大写字母、标点符号、特殊符号中的至少两类；常见的口令与账号无关性要求示例：口令不包含账号等。
- 2) 用户输入口令时，不应明文回显口令。
- b) 前置条件：
- 1) 按测试环境 1 搭建好测试环境；
 - 2) 厂商提供口令鉴别方式相关的说明文档，包括不限于口令复杂度、口令保护、设备管理方式等内容。
- c) 检测方法：
- 服务器安全检测方法参见 GB/T 39680-2020 6.2.6.1 a) 4。
- 其他网络关键设备按照以下步骤进行检测：
- 1) 开启口令复杂度检查功能时，配置或确认口令复杂度要求；
 - 2) 按照厂商提供的设备管理方式信息，创建不同管理方式的新账号，配置符合口令复杂度要求的账号，并使用新创建的账号以不同的管理方式登录设备，检查在登录过程中是否明文回显输入的口令信息以及是否能够成功登录；
 - 3) 按照厂商提供的设备管理方式信息，创建不同管理方式的新账号，配置不符合口令复杂度要求的账号，检查配置结果。
- d) 预期结果：
- 服务器安全检测预期结果参见 GB/T 39680-2020 6.2.6.1 b) 4。
- 其他网络关键设备检测预期结果如下：
- 1) 步骤 1 中，口令复杂度检查包括口令长度检查、口令字符类型检查、口令与账号无关性检查中的至少一项。口令复杂度要求长度不少于 8 位，口令字符类型检查要求至少包含 2 种不同类型字符，常见的字符类型包括数字、大小写字母、特殊字符等；

- 2) 步骤 2 中, 创建新账号成功, 以各种管理方式登录过程中没有明文回显输入的口令信息, 且登录成功;
 - 3) 步骤 3 中, 创建失败, 无法创建口令不满足复杂度要求的账号。
- e) 判定原则:
测试结果应与预期结果相符, 否则不符合要求。

6.5.4 用户鉴别信息猜解攻击防范功能

该检测项包括如下内容:

- a) 安全要求:
用户鉴别信息猜解攻击防范功能硬件标识安全要求见GB40050-2021 5.5 d)。
应支持启用安全策略或具备安全功能, 以防范用户鉴别信息猜解攻击。
- 注: 常见的防范用户鉴别信息猜解攻击的安全策略或安全功能包括默认开启口令复杂度检查功能、限制连续的非法登录尝试次数或支持限制管理访问连接的数量、双因素鉴别(例如口令+证书、口令+生物鉴别等)等措施, 当出现鉴别失败时, 设备提供无差别反馈, 避免提示“用户名错误”、“口令错误”等类型的具体信息。
- b) 预置条件:
1) 按测试环境 1 搭建好测试环境;
2) 厂商提供防范用户鉴别信息猜解攻击功能说明。
- c) 检测方法:
服务器安全检测方法参见 GB/T 39680-2020 6.2.6.1 a) 5)。
其他网络关键设备按照以下步骤进行检测:
1) 配置用户鉴别信息猜解攻击防范功能, 常见的防范用户鉴别信息猜解攻击的安全策略或安全功能包括默认开启口令复杂度检查功能、限制连续的非法登录尝试次数或支持限制管理访问连接的数量、双因素鉴别(例如口令+证书、口令+生物鉴别等)等措施, 当出现鉴别失败时, 设备提供无差别反馈, 避免提示“用户名错误”、“口令错误”等类型的具体信息;
2) 模拟用户鉴别信息猜解攻击, 验证设备的安全功能是否生效。
- d) 预期结果:
服务器安全检测预期结果参见 GB/T 39680-2020 6.2.6.1 b) 5)。
其他网络关键设备检测预期结果如下:
1) 配置成功;
2) 设备能够防范用户鉴别信息猜解攻击。
- e) 判定原则:
测试结果应与预期结果相符, 否则不符合要求。

6.5.5 会话空闲时间过长防范功能

该检测项包括如下内容:

- b) 安全要求:
会话空闲时间过长防范功能安全要求见GB40050-2021 5.5 e)。
应支持启用安全策略或具备安全功能, 以防止用户登录后会话空闲时间过长。
- 注: 常见的防止用户登录后会话空闲时间过长的安全策略或安全功能包括登录用户空闲超时后自动退出等。
- c) 预置条件:
3) 按测试环境 1 搭建好测试环境;
4) 厂商提供会话空闲超时控制策略、相关的配置以及设备管理方式说明。

- d) 检测方法：
服务器安全检测方法参见 GB/T 39680-2020 6.2.6.1 a) 6)。
其他网络关键设备按照以下步骤进行检测：
- 1) 配置或确认会话空闲时长；
 - 2) 按照厂商提供的设备管理方式信息，以不同的管理方式登录被测设备，检查登录后空闲时间达到设定值或默认值时是否会锁定或者自动退出。
- e) 预期结果：
服务器安全检测预期结果参见 GB/T 39680-2020 6.2.6.1 b) 6)。
其他网络关键设备检测预期结果如下：
- 1) 配置成功，或者已存在默认的会话空闲时长，并记录会话空闲时长值；
 - 2) 登录后空闲时间达到设定值或默认值时会锁定或者自动退出。
- f) 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.5.6 身份鉴别信息安全保护功能

该检测项包括如下内容：

- a) 安全要求：
身份鉴别信息安全保护功能安全要求见 GB40050-2021 5.5 f)。
应对用户身份鉴别信息进行安全保护，保障用户鉴别信息存储的保密性，以及传输过程中的保密性和完整性。
- b) 预置条件：
- 1) 按测试环境 1 搭建好测试环境；
 - 2) 厂商提供所有身份鉴别信息安全存储、安全传输操作说明；
- c) 检测方法：
服务器安全检测方法参见 GB/T 39680-2020 6.2.6.1 a) 7)。
其他网络关键设备按照以下步骤进行检测：
- 1) 按照厂商提供的说明材料生成用户身份鉴别信息，查看是否以加密方式存储；
 - 2) 按照厂商提供的说明材料生成并传输用户身份鉴别信息，通过抓包或其他有效的方式查看是否具备保密性和完整性保护能力。
- d) 预期结果：
服务器安全检测预期结果参见 GB/T 39680-2020 6.2.6.1 b) 7)。
其他网络关键设备检测预期结果如下：
- 1) 用户身份鉴别信息能以加密方式存储；
 - 2) 具备保障用户身份鉴别信息保密性和完整性能力。
- e) 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.6 访问控制安全

6.6.1 默认开放服务和端口

该检测项包括如下内容：

- a) 安全要求：
默认开放服务和端口安全要求见 GB40050-2021 5.6 a)。

默认状态下应仅开启必要的服务和对应的端口，应明示所有默认开启的服务、对应的端口及用途，应支持用户关闭默认开启的服务和对应的端口；

b) 前置条件：

- 1) 按测试环境 1 搭建好测试环境；
- 2) 设备运行于默认状态，默认状态为设备出厂设置时的配置状态；
- 3) 厂商提供所有默认开启的服务、对应的端口及用途、管理员权限账号的说明材料。

c) 检测方法：

服务器安全检测方法参见 GB/T 39680-2020 6.2.6.4 a) 1) 2)。

其他网络关键设备按照以下步骤进行检测：

- 1) 使用扫描工具对设备进行全端口扫描，查看默认状态开启的服务和对应的端口，是否与厂商提供的说明材料内容一致、是否仅开启必要的服务和对应的端口；
- 2) 配置设备，关闭默认开启的端口和服务，使用扫描工具对设备再次进行扫描，查看扫描结果，检查默认开启的端口和服务是否被关闭。

d) 预期结果：

服务器安全检测预期结果参见 GB/T 39680-2020 6.2.6.3 b) 1) 2)。

其他网络关键设备检测预期结果如下：

- 1) 步骤 1 中，默认状态下，设备仅开启必要的服务和对应的端口，默认开启的服务和端口与厂商提供的说明材料内容一致；
- 2) 步骤 2 中，用户可以自行关闭默认开启的服务和对应的端口。

e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.6.2 开启非默认开放服务和端口

该检测项包括如下内容：

a) 安全要求：

开启非默认开放服务和端口安全要求见 GB40050-2021 5.6 b)。
非默认开放的端口和服务，应在用户知晓且同意后才可启用。

b) 前置条件：

- 1) 按测试环境 1 搭建好测试环境；
- 2) 设备运行于默认状态，默认状态为设备出厂设置时的配置状态；
- 3) 厂商提供设备非默认开放端口和服务对应关系的说明材料；
- 4) 厂商提供说明材料，说明开启非默认开放端口和服务的配置方式，以及如何让用户知晓和同意开启非默认开放端口和服务。

c) 检测方法：

按照厂商提供的说明材料，配置设备，开启非默认开放的端口和服务，确认是否经过用户知晓且同意才可启用。

d) 预期结果：

非默认开放的端口和服务，应在用户知晓且同意后才可启用。

e) 判定原则：

- 1) 测试结果应与预期结果相符，否则不符合要求；
- 2) 用户知晓且同意开启非默认端口和服务的方式通常可包括用户授权、二次确认等。

6.6.3 受控资源访问控制功能

该检测项包括如下内容：

a) 安全要求

受控资源访问控制功能安全要求见GB40050-2021 5.6 c)。

在用户访问受控资源时，支持设置访问控制策略并依据设置的控制策略进行授权和访问控制，确保访问和操作安全。

注1：受控资源指需要授予相应权限才可访问的资源。

注2：常见的访问控制策略包括通过IP地址绑定、MAC地址绑定等安全策略限制可访问的用户等。

b) 预置条件

- 1) 按测试环境1搭建好测试环境；
- 2) 厂商提供受控资源访问控制功能的相关配置说明。

c) 检测方法

- 1) 按照厂商提供的配置说明对设备进行配置，对受控资源仅授权用户可访问，非授权用户不能访问；
- 2) 使用配置的用户对受控资源进行访问，确认仅授权用户可访问，非授权用户不能访问。

d) 预期结果

- 1) 配置成功；
- 2) 仅授权用户可访问受控资源，非授权用户不能访问。

e) 判定原则

测试结果应与预期结果相符，否则不符合要求。

6.6.4 用户权限管理功能

该检测项包括如下内容：

a) 安全要求

用户权限管理功能硬件标识安全要求见GB40050-2021 5.6 d)。

应提供用户分级分权控制机制。对涉及设备安全的重要功能，仅授权的高权限等级用户使用。

注：常见的涉及设备安全的重要功能包括补丁管理、固件管理、日志审计、时间同步等。

b) 预置条件

- 1) 按测试环境1搭建好测试环境；
- 2) 厂商提供所有默认账号信息以及设备管理方式说明。

c) 检测方法

- 1) 分别添加或使用不同权限等级的两个用户 user1、user2；
- 2) 为 user1 配置低等级权限，仅具有修改自己的口令、状态查询等权限，不支持配置系统信息，不支持涉及设备安全的重要功能如补丁管理、固件管理、日志审计、时间同步等权限；
- 3) 为 user2 配置高等级权限，具有涉及设备安全的重要功能如补丁管理、固件管理、日志审计、时间同步等权限；
- 4) 分别使用 user1、user2 登录设备，对设备进行修改自己的口令、状态查询、补丁管理、固件管理、日志审计、时间同步等配置或操作。

d) 预期结果

- 1) 步骤1中成功添加两个用户；
- 2) 步骤4中，user1 仅可修改自己的口令、进行状态查询等基本操作，不支持配置系统信息，不支持涉及设备安全的重要功能如补丁管理、固件管理、日志审计、时间同步等配置或操作；user2 支持涉及设备安全的重要功能如补丁管理、固件管理、日志审计、时间同步等配置或操作。

e) 判定原则

测试结果应与预期结果相符，否则不符合要求。

6.7 日志审计安全

6.7.1 日志记录和要素

该检测项包括如下内容：

a) 安全要求

日志记录和要素安全要求见 GB40050-2021 5.7 a) c) f)。

- 1) 应提供日志审计功能，对用户关键操作行为和重要安全事件进行记录，应支持对影响设备运行安全的事件进行告警提示；

注：常见的用户关键操作包括增/删账户、修改鉴别信息、修改关键配置、文件上传/下载、用户登录/注销、用户权限修改、重启/关闭设备、编程逻辑下载、运行参数修改等。

- 2) 日志审计功能应记录必要的日志要素，为查阅和分析提供足够的信息；

注：常见的日志要素包括事件发生的日期和时间、主体、类型、结果、源IP地址等。

- 3) 不应在日志中明文或弱加密记录敏感数据。

注：常见的弱加密方式包括信息摘要算法（MD5）、Base64等。

b) 预置条件

- 1) 按测试环境 1 搭建好测试环境；
- 2) 厂商提供包括管理员等所有账号信息；
- 3) 厂商提供日志记录功能的相关说明，包括记录的事件类型、要素等。

c) 检测方法

服务器安全检测方法参见 GB/T 39680-2020 6.2.6.3 a) 1) 4)。

其他网络关键设备按照以下步骤进行检测：

- 1) 使用管理员权限账号通过远程管理方式登录被测设备，进行增加、删除账户、修改鉴别信息、修改用户权限等操作；
- 2) 使用系统默认或新增账号登录设备，查看日志，日志应记录相应操作；
- 3) 使用管理员账号进行设备配置、重启，关闭，软件更新，修改 IP 地址等操作；
- 4) 使用管理员权限账号登录，进行关于配置用户口令、SNMP 团体名、WEB 登录或配置私钥等敏感数据操作；
- 5) 查看日志，应该记录以上操作行为；
- 6) 检查日志审计记录中是否包含必要的日志要素，至少包括事件发生日期和时间、主体（如登录账号等）、事件描述（如类型、操作结果等）、源 IP 地址（采用远程管理方式时）等；
- 7) 查看日志的记录内容中是否包含明文或弱加密记录敏感数据等。

d) 预期结果

服务器安全检测预期结果参见 GB/T 39680-2020 6.2.6.3 b) 1) 4)。

其他网络关键设备检测预期结果如下：

- 1) 针对设备的配置、系统安全相关操作等事件均被记录在日志中；
- 2) 日志记录格式符合文档要求，日志审计记录中包含必要的日志要素，例如事件发生日期和时间、主体（如登录账号等）、事件描述（如类型、操作结果等）、源 IP 地址（采用远程管理方式时）等；
- 3) 日志中不存在明文或弱加密（如 MD5、BASE64、ASCII 码转换等）记录敏感数据，如用户口令、SNMP 团体名、WEB 会话 ID 以及私钥等。

- e) 判定原则
测试结果应与预期结果相符，否则不符合要求。

6.7.2 日志信息本地存储安全

该检测项包括如下内容：

- a) 安全要求
日志信息本地存储安全要求见GB40050-2021 5.7 b) e)。
应提供日志信息本地存储功能。应提供本地日志存储空间耗尽处理功能。
注：本地日志存储空间耗尽时常见的处理功能包括剩余存储空间低于阈值时进行告警、循环覆盖等。
- b) 预置条件
- 1) 按测试环境 1 搭建好测试环境；
 - 2) 厂商提供包括管理员等所有账号信息；
 - 3) 厂商提供日志存储空间告警阈值设置信息、触发日志循环覆盖的条件（如日志记录数量的最大值、日志文件存储最大值等）说明。
- c) 检测方法
- 1) 使用管理员账号登录；
 - 2) 反复进行触发日志记录行为的操作（例如登录、登出等），直到日志记录剩余存储空间低于阈值，或达到触发日志循环覆盖的条件（例如日志记录条目数达到最大值或日志文件存储达到最大值）；
 - 3) 查看日志是否进行了本地存储；
 - 4) 如设备支持剩余日志存储空间低于阈值时进行告警的功能，查看步骤 2) 是否产生了日志记录剩余存储空间低于阈值的告警；如设备支持循环覆盖，查看步骤 2) 中的操作是否产生了日志覆盖，且应是最新产生的日志对最早产生的日志进行覆盖。
- d) 预期结果
- 1) 步骤 3 中，能够看到设备本地存储的日志信息；
 - 2) 步骤 4 中，产生了日志记录剩余存储空间低于阈值的告警，或实现了日志的循环覆盖。
- e) 判定原则
测试结果应与预期结果相符，否则不符合要求。

6.7.3 日志信息输出功能

该检测项包括如下内容：

- a) 安全要求
日志信息输出功能安全要求见 GB40050-2021 5.7 b)。
支持日志信息输出。
- b) 预置条件
- 1) 按测试环境 1 搭建好测试环境；
 - 2) 厂商提供包括管理员等所有账号信息；
 - 3) 厂商提供日志输出功能的说明，包括输出形式、方式、配置方法等。
- c) 检测方法
- 1) 使用管理员账号登录被测设备；
 - 2) 配置被测设备，触发日志数据输出操作，如将日志数据传输到远端服务器或手动导出等；
 - 3) 查看日志数据输出操作是否成功，日志数据接收端是否有相关日志信息。
- d) 预期结果

- 1) 步骤 2 中, 支持日志输出功能;
- 2) 步骤 3 中, 日志数据输出操作成功, 日志数据接收端有相关日志信息。
- e) 判定原则
测试结果应与预期结果相符, 否则不符合要求。

6.7.4 日志信息安全保护

该检测项包括如下内容:

- a) 安全要求
日志信息安全保护安全要求见 GB40050-2021 5.7 d)。
应具备对日志在本地存储和输出过程进行保护的安全功能, 防止日志内容被未经授权的查看、输出或删除。
注: 常见的日志保护安全功能包括用户授权访问控制等。
- b) 预置条件
 - 1) 按测试环境 1 搭建好测试环境;
 - 2) 厂商提供具备对日志不同操作权限的账号, 并说明不同权限账号所具备的日志操作权限。
- c) 检测方法
服务器安全检测方法参见 GB/T 39680-2020 6.2.6.3 a) 5) 6)。
其他网络关键设备按照以下步骤进行检测:
 - 1) 使用授权账号登录, 检查该用户是否可以查看/输出/删除本地日志信息;
 - 2) 使用非授权账号登录, 检查该用户是否可以查看/输出/删除日志信息。
- d) 预期结果
服务器安全检测预期结果参见 GB/T 39680-2020 6.2.6.3 b) 5) 6)。
其他网络关键设备检测预期结果如下:
只有获得授权的用户才能对日志内容进行查看、输出或删除。
- e) 判定原则
测试结果应与预期结果相符, 否则不符合要求。

6.8 通信安全

6.8.1 管理协议安全

该检测项包括如下内容:

- a) 安全要求:
管理协议安全要求见 GB40050-2021 5.8 a)。
应支持与管理系统(管理用户)建立安全的通信信道/路径, 保障通信数据的保密性、完整性;
- b) 预置条件:
 - 1) 按测试环境 1 搭建好测试环境;
 - 2) 厂商提供设备支持的安全协议说明材料。
- c) 检测方法:
尝试使用安全协议对设备进行操作;
- d) 预期结果
 - 1) 步骤 1 中, 设备应支持使用至少一种安全协议对设备进行管理, 保障通信数据的保密性、完整性。
- e) 判定原则:
测试结果应与预期结果相符, 否则不符合要求。

6.8.2 协议健壮性安全

该检测项包括如下内容：

a) 安全要求：

协议健壮性安全要求见 GB40050-2021 5.8 b) 。

应满足通信协议健壮性要求，防范异常报文攻击。

注：网络关键设备使用的常见的通信协议包括IPv4/IPv6、TCP、UDP等基础通信协议，SNMP、SSH、HTTP等网络管理协议，路由协议、工业控制协议等专用通信协议，以及其他网络应用场景中的专用通信协议。

b) 预置条件：

厂商提供有关通信协议健壮性测试材料。

c) 检测方法：

检查有关通信协议健壮性测试材料。

d) 预期结果：

步骤 1 中，厂商提供的基础通信协议健壮性测试证明材料，保障信息可信。

e) 判定原则：

1) 测试结果应与预期结果相符，否则不符合要求；

2) 测试材料应由独立于设备提供方和设备使用方的第三方机构出具，测试材料中的测试过程应与《3GPP TS 33.117 Catalogue of general security assurance requirements》中“4.4.4 Robustness and fuzz testing”的要求相一致；

3) 厂商应提供被测对象一致性说明材料，如被测设备与提供的测试材料中被测对象的软件仅有少量差异（例如：小版本号不同、补丁版本号不同等）时，厂商补充提供差异部分的测试材料。

6.8.3 时间同步功能

该检测项包括如下内容：

a) 安全要求：

时间同步功能安全要求见GB40050-2021 5.8 c) 。

应支持时间同步功能。

b) 预置条件：

1) 按测试环境 1 搭建好测试环境；

2) 厂商提供设备 NTP 协议等时间同步的说明材料；

3) 设备开机正常运行。

c) 检测方法：

配置被测设备，开启NTP时间同步功能，并测试其是否能够进行时间同步。

d) 预期结果：

设备支持使用NTP等实现时间同步功能。

e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

6.8.4 协议声明

该检测项包括如下内容：

a) 安全要求：

协议声明安全要求见 GB40050-2021 5.8 d) 。

应不存在未声明的私有协议。

- b) 预置条件：
厂商提供被测设备支持的所有协议以及不存在未声明的私有协议的说明材料。
- c) 检测方法：
检查厂商提供的材料，确认是否提供了被测设备支持的所有协议以及不存在未声明的私有协议的说明材料。
- d) 预期结果：
厂商提供了被测设备支持的所有协议以及不存在未声明的私有协议的说明材料。
- e) 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.8.5 重放攻击防范能力

该检测项包括如下内容：

- a) 安全要求：
重放攻击防范能力安全要求见 GB40050-2021 5.8 e)。
应具备抵御常见重放类攻击的能力。
注：常见的重放类攻击包括各类网络管理协议的身份鉴别信息重放攻击、设备控制数据重放攻击等。

- b) 预置条件：
按测试环境 1 搭建好测试环境。
- c) 检测方法：
 - 1) 配置被测设备，开启相关协议功能；
 - 2) 建立连接关系，抓取并保存认证凭据，通过退出或更改等手段解除连接关系，重新发送保存的认证凭据，查看连接情况。
- d) 预期结果：
步骤 2 中，连接失败。
- e) 判定原则：
测试结果应与预期结果相符，否则不符合要求。

6.9 数据安全

6.9.1 敏感数据保护功能

- a) 安全要求：
敏感数据保护功能安全要求见 GB40050-2021 5.9 a)。
应具备防止数据泄露、数据非授权读取和修改的安全功能，对存储在设备中的敏感数据进行保护。
- b) 预置条件：
 - 1) 按测试环境 1 搭建好测试环境；
 - 2) 厂商提供说明材料，说明存储在设备上的敏感数据类型及查看方式。
- c) 检测方法：
 - 1) 查看被测设备中的用户口令和协议加密口令，检查是否以密文形式存储或不显示；
 - 2) 在运行系统中查看各类口令，检查是否以密文形式存储或不显示；
 - 3) 查看配置文件中的各类口令，检查是否以密文形式存储或不显示。
- d) 预期结果：
 - 1) 设备中的用户口令和协议加密口令均以密文形式存储或不显示；
 - 2) 运行系统的各类口令均显示为密文或不显示；

3) 配置文件中存储的口令均显示为密文或不显示。

e) 判定原则:

测试结果应与预期结果相符, 否则不符合要求。

6.9.2 数据删除功能

a) 安全要求:

数据删除功能安全要求见GB40050-2021 5.9 b)。

应具备对用户产生且存储在设备中的数据进行授权删除的功能, 支持在删除前对该操作进行确认。

注: 用户产生且存储在设备中的数据通常包括日志、配置文件等。

b) 预置条件:

1) 按测试环境 1 搭建好测试环境。

2) 根据设备登录方式说明材料, 使用管理员权限用户登录设备。

3) 设备应支持包括并不限于如下权限用户: 查询权限, 配置权限, 管理员权限, 系统维护权限等。

4) 管理员权限, 系统维护权限账户为授权账户可以删除日志信息。

c) 检测方法:

1) 分别用授权账户和非授权账户对系统运行中生成的日志信息进行删除;

2) 分别用授权账户和非授权账户对系统中存储的日志信息进行删除;

3) 分别用授权账户和非授权账户对系统中存储的配置文件进行删除。

d) 预期结果:

1) 授权账户可以成功删除系统运行过程中生成的日志信息;

2) 非授权账户无法删除系统运行过程中生成的日志信息;

3) 授权账户可以成功删除系统中存储的日志信息;

4) 非授权账户无法删除系统中存储的日志信息;

5) 授权账户可以成功删除系统中存储的配置文件, 删除前应支持对删除操作进行确认;

6) 非授权账户无法删除系统中存储的配置文件。

e) 判定原则:

测试结果应与预期结果相符, 否则不符合要求。

7 安全保障要求评估方法

7.1 设计和开发

7.1.1 设计和开发环节风险识别

a) 安全要求:

设计和开发环节风险识别安全要求见 GB40050-2021 6.1 a)。

应在设备设计和开发环节识别安全风险, 制定安全策略。

注: 设备设计和开发环节的常见安全风险包括开发环境的安全风险、第三方组件引入的安全风险、开发人员导致的安全风险等。

b) 预置条件:

1) 厂商提供说明材料, 说明在设备设计和开发环节识别的安全风险及相应的安全策略。

c) 检测方法:

- 1) 查看厂商提供的说明材料，确认是否对设备在设计和开发环节的主要安全风险进行识别，确认是否明确相应的安全策略。
- d) 预期结果：
 - 1) 说明材料中明确体现了设备在设计和开发环节的主要安全风险，如开发环境的安全风险、第三方组件引入的安全风险、开发人员导致的安全风险等，并且明确相应的安全策略。
- e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

7.1.2 设备安全设计和开发操作规程

- a) 安全要求：

设备安全设计和开发操作规程安全要求见 GB40050-2021 6.1 b)。

应建立设备安全设计和开发操作规程，保障安全策略落实到设计和开发的整个过程。
- b) 预置条件：
 - 1) 厂商提供说明材料，说明设备安全设计和开发操作规程。
- c) 检测方法：
 - 1) 查看厂商提供的说明材料，确认是否有设备安全设计和开发操作规程。
- d) 预期结果：
 - 1) 说明材料中明确体现了设备安全设计和开发操作规程。
- e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

7.1.3 配置管理及变更

- a) 安全要求：

配置管理及变更安全要求见 GB40050-2021 6.1 c)。

应建立配置管理程序及相应配置项清单，配置管理系统应能跟踪内容变更，并对变更进行授权和控制。
- b) 预置条件：
 - 1) 厂商提供配置管理程序及相应配置项清单，以及变更控制记录。
- c) 检测方法：
 - 1) 查看厂商提供的配置管理程序及相应配置项清单；
 - 2) 确认已发生的变更情况，查看厂商提供的变更控制记录。
- d) 预期结果：
 - 1) 厂商应具备配置管理程序及相应配置项清单；
 - 2) 厂商应能提供准确一致的变更控制记录。
- e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

7.1.4 恶意程序防范

- a) 安全要求：

恶意程序防范安全要求见 GB40050-2021 6.1 d) e) f)。

 - 1) 应采取措施防范设备被植入恶意程序。
 - 2) 应采取措施防范设备被设置隐蔽的接口或功能模块。
 - 3) 应采取措施防范第三方关键部件、固件或软件可能引入的安全风险。

- b) 预置条件:
 - 1) 厂商提供防范设备被植入恶意程序的说明材料。
 - 2) 厂商提供防范设备被设置隐蔽的接口或功能模块的说明材料。
 - 3) 厂商提供防范第三方关键部件、固件或软件可能引入的安全风险的说明材料。
- c) 检测方法:
 - 1) 检查厂商提供防范设备被植入恶意程序的说明材料, 确认是否验证防范措施的有效性, 确认措施的实施记录。
 - 2) 检查厂商提供防范设备被设置隐蔽的接口或功能模块的说明材料, 确认是否验证防范措施的有效性, 确认措施的实施记录。
 - 3) 厂商提供防范第三方关键部件、固件或软件可能引入的安全风险的说明材料, 确认是否验证防范措施的有效性, 确认措施的实施记录。
- d) 预期结果:
 - 1) 厂商能够提供防范设备被植入恶意程序的说明材料, 验证了防范措施的有效性, 留存了措施的实施记录。
 - 2) 厂商能够提供防范设备被设置隐蔽的接口或功能模块的说明材料, 验证了防范措施的有效性, 留存了措施的实施记录。
 - 3) 厂商能够提供防范第三方关键部件、固件或软件可能引入的安全风险的说明材料, 验证了防范措施的有效性, 留存了措施的实施记录。
- e) 判定原则:

测试结果应与预期结果相符, 否则不符合要求。

7.1.5 设备安全测试

- a) 安全要求:

设备安全测试安全要求见 GB40050-2021 6.1 g)。

应采用漏洞扫描、病毒扫描、代码审计、健壮性测试、渗透测试和安全功能验证的方式对设备进行安全性测试。
- b) 预置条件:
 - 1) 厂商提供设备安全测试说明材料。
- c) 检测方法:
 - 1) 查看厂商提供的说明材料, 确认是否包含漏洞扫描、病毒扫描、代码审计、健壮性测试、渗透测试和安全功能验证等内容。
- d) 预期结果:
 - 1) 说明材料中明确体现了含漏洞扫描、病毒扫描、代码审计、健壮性测试、渗透测试和安全功能验证等内容。
- e) 判定原则:

测试结果应与预期结果相符, 否则不符合要求。

7.1.6 安全缺陷与漏洞的修复和补救

- a) 安全要求:

安全缺陷与漏洞的修复和补救安全要求见 GB40050-2021 6.1 h)。

应对已发现的安全缺陷、漏洞等安全问题进行修复, 或提供补救措施。
- b) 预置条件:
 - 1) 厂商提供设备安全缺陷、漏洞等的修复说明材料或补救措施说明材料。

- c) 检测方法：
 - 1) 选取厂商已公布的漏洞，查看厂商提供的说明材料，确认是否包含漏洞的修复说明或补救措施说明，如存在补救措施，确认是否对补救措施的有效性进行验证。
- d) 预期结果：
 - 1) 说明材料中明确体现了漏洞的修复说明或补救措施说明，如存在补救措施，存在对补救措施的有效性进行验证的记录。
- e) 判定原则：
 - 测试结果应与预期结果相符，否则不符合要求。

7.2 生产和交付

7.2.1 生产和交付环节风险识别

- a) 安全要求：
 - 生产和交付环节风险识别安全要求见 GB40050-2021 6.2 a)。
 - 应在设备生产和交付环节识别安全风险，制定安全策略。
- 注：生产和交付环节的常见安全风险包括自制或采购的组件被篡改、伪造等风险，生产环境存在的安全风险、设备被植入的安全风险、设备存在漏洞的安全风险、物流运输的风险等。
- b) 预置条件：
 - 1) 厂商提供说明材料，说明在设备生产和交付环节识别的安全风险及相应的安全策略。
- c) 检测方法：
 - 1) 查看厂商提供的说明材料，确认是否识别出设备在生产和交付环节的主要安全风险，确认是否明确相应的安全策略。
- d) 预期结果：
 - 1) 说明材料中明确体现了设备在生产和交付环节的主要安全风险，自制或采购的组件被篡改、伪造等风险，生产环境存在的安全风险、设备被植入的安全风险、设备存在漏洞的安全风险、物流运输的风险等，并且明确相应的安全策略。
- e) 判定原则：
 - 测试结果应与预期结果相符，否则不符合要求。

7.2.2 完整性检测

- a) 安全要求：
 - 完整性检测安全要求见 GB40050-2021 6.2 b) c) d) e)。
 - 1) 应建立并实施规范的设备生产流程，在关键环节实施安全检查和完整性验证。
 - 2) 应建立和执行规范的设备完整性检测流程，采取措施防范自制或采购的组件被篡改、伪造等风险。
 - 3) 应对预装软件在安装前进行完整性校验。
 - 4) 应为用户提供验证所交付设备完整性的工具或方法，防范设备交付过程中完整性被破坏的风险。
- 注：验证所交付设备完整性的常见工具或方法包括防拆标签、数字签名/证书等。
- b) 预置条件：
 - 1) 厂商提供说明材料，说明已建立和执行规范的设备完整性检测流程。
 - 2) 厂商提供说明材料，说明已采取措施防范自制或采购的组件被篡改、伪造等风险。
 - 3) 厂商提供预装软件安装前的完整性校验记录。
 - 4) 厂商提供为用户提供验证所交付设备完整性的工具或方法。

- c) 检测方法:
- 1) 查看厂商提供的说明材料, 确认是否已建立和执行规范的设备完整性检测流程。
 - 2) 查看厂商提供的说明材料, 确认是否采取措施防范自制或采购的组件被篡改、伪造等风险, 确认是否验证措施的有效性。
 - 3) 查看预装软件安装前的完整性校验记录。
 - 4) 查看厂商提供的为用户提供验证所交付设备完整性的工具或方法, 验证工具的有效性。
- d) 预期结果:
- 1) 厂商提供的说明材料明确说明已建立和执行规范的设备完整性检测流程。
 - 2) 厂商提供的说明材料明确说明已采取措施防范自制或采购的组件被篡改、伪造等风险, 已验证措施的有效性。
 - 3) 厂商留存了准确一致的预装软件安装前的完整性校验记录。
 - 4) 厂商能够为用户提供验证所交付设备完整性的工具或方法, 使用提供的工具或方法能够验证设备的完整性。
- e) 判定原则:
- 测试结果应与预期结果相符, 否则不符合要求。

7.2.3 指导性文档

- a) 安全要求:
- 指导性文档安全要求见 GB40050-2021 6.2 f)。
- 应为用户提供操作指南和安全配置指南等指导性文档, 以说明设备的安装、生成和启动的过程, 并对设备功能的现场调试运行提供详细的描述。
- b) 预置条件:
- 1) 厂商提供用户指导性文档材料。
- c) 检测方法:
- 1) 查看厂商提供的用户指导性文档材料, 确认是否包括操作指南和安全配置指南等内容, 确认是否说明设备的安装、生成和启动的过程, 确认是否对设备功能的现场调试运行提供详细的描述。
- d) 预期结果:
- 1) 厂商提供的用户指导性文档材料包括操作指南和安全配置指南等内容, 说明设备的安装、生成和启动的过程, 对设备功能的现场调试运行提供详细的描述。
- e) 判定原则:
- 测试结果应与预期结果相符, 否则不符合要求。

7.2.4 默认端口号与网络服务映射关系

- a) 安全要求:
- 默认端口号与网络服务映射关系安全要求见 GB40050-2021 6.2 g)。
- 应提供设备服务与默认端口号的映射关系说明。
- b) 预置条件:
- 1) 厂商提供设备服务与默认端口号的映射关系说明。
- c) 检测方法:
- 1) 查看厂商提供的设备服务与默认端口号的映射关系说明材料, 确认是否明确描述默认开放的端口信息及对应的网络服务。
- d) 预期结果:

1) 厂商提供的设备服务与默认端口号的映射关系说明材料明确描述默认开放的端口信息及对应的网络服务。

- e) 判定原则：
测试结果应与预期结果相符，否则不符合要求。

7.2.5 私有协议

- a) 安全要求：

私有协议安全要求见 GB40050-2021 6.2 h)。

应声明设备中存在的通过设备外部接口进行通信的私有协议并说明其用途，私有协议不应存在所声明范围之外的用途。

- b) 预置条件：

1) 厂商提供设备私有协议说明材料。

- c) 检测方法：

1) 查看厂商提供的私有协议说明材料，确认是否声明设备中存在的通过设备外部接口进行通信的私有协议并说明其用途，确认是否说明私有协议不存在所声明范围之外的用途。

- d) 预期结果：

1) 厂商能够提供正式的私有协议说明材料，声明设备中存在的通过设备外部接口进行通信的私有协议并说明其用途，说明私有协议不存在所声明范围之外的用途。

- e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

7.2.6 交付前的安全漏洞补救措施

- a) 安全要求：

交付前的安全漏洞补救措施安全要求见 GB40050-2021 6.2 i)。

交付设备前，发现设备存在已知漏洞应当立即采取补救措施。

- b) 预置条件：

1) 厂商提供设备交付前的安全漏洞处置流程说明材料。

- c) 检测方法：

1) 检查厂商提供的设备交付前的安全漏洞处置流程说明材料，确认是否包括采取补救措施的内容。

2) 选取厂商在交付前发现的漏洞实例，查看厂商的补救措施和验证材料。

- d) 预期结果：

1) 说明材料中明确包括采取补救措施的内容。

2) 厂商在交付前发现的漏洞具备补救措施及处置记录。

- e) 判定原则：

测试结果应与预期结果相符，否则不符合要求。

漏洞补救措施可以是漏洞修复补丁、升级包、技术方案等。

7.3 运行和维护

7.3.1 运行和维护环节风险识别

- a) 安全要求：

运行和维护环节风险识别硬件标识安全要求见 GB40050-2021 6.3 a)。

应识别在运行环节存在的设备自身安全风险（不包括网络环境安全风险），以及对设备进行维护时引入的安全风险，制定安全策略。

b) 前置条件:

- 1) 厂商提供说明材料，说明在运行环节存在的设备自身安全风险及相应的安全策略。
- 2) 厂商提供说明材料，说明对设备进行维护时引入的安全风险及相应的安全策略。

c) 检测方法:

- 1) 查看厂商提供的说明材料，确认是否识别出设备运行环节存在的设备自身安全风险，确认是否明确相应的安全策略。
- 2) 查看厂商提供的说明材料，确认是否识别出对设备进行维护时引入的安全风险，确认是否明确相应的安全策略。

d) 预期结果:

- 1) 说明材料中明确体现了设备在运行环节的主要安全风险，并且明确相应的安全策略。
- 2) 说明材料中明确体现了对设备进行维护时引入的主要安全风险，并且明确相应的安全策略。

e) 判定原则:

测试结果应与预期结果相符，否则不符合要求。

7.3.2 安全事件的应急响应

a) 安全要求:

安全事件的应急响应安全要求见 GB40050-2021 6.3 b)。应建立并执行针对设备安全事件的应急响应机制和流程，并为应急处置配备相应的资源。

b) 前置条件:

- 1) 厂商提供说明材料，说明针对设备安全事件的应急响应机制和流程，以及为应急处置配备的资源。

c) 检测方法:

- 1) 查看厂商提供的说明材料，确认是否建立针对设备安全事件的应急响应机制和流程。
- 2) 查看厂商提供的说明材料，确认是否执行针对设备安全事件的应急响应机制和流程，检查执行记录。
- 3) 查看厂商提供的说明材料，确认是否为应急处置配备相应的资源，包括管理人员、技术人员等。

d) 预期结果:

- 1) 说明材料中明确体现了已建立针对设备安全事件的应急响应机制和流程。
- 2) 说明材料中明确体现了已执行针对设备安全事件的应急响应机制和流程，并留存了相应的执行记录。
- 3) 说明材料明确体现了为应急处置配备的资源，包括管理人员、技术人员等。

e) 判定原则:

测试结果应与预期结果相符，否则不符合要求。

7.3.3 交付后的安全漏洞补救措施

a) 安全要求:

交付后的安全漏洞补救措施安全要求见 GB40050-2021 6.3 c)。

在发现设备存在安全缺陷、漏洞等安全风险时，应采取修复或替代方案等补救措施，按照有关规定及时告知用户并向有关主管部门报告。

- b) 预置条件:
 - 1) 厂商提供设备交付后的安全漏洞处置流程说明材料。
- c) 检测方法:
 - 1) 检查厂商提供的设备交付后的安全漏洞处置流程说明材料,确认是否在发现设备存在安全缺陷、漏洞等安全风险时采取修复或替代方案等补救措施,按照有关规定及时告知用户并向有关主管部门报告。
- d) 预期结果:
 - 1) 说明材料中明确包括设备交付后的安全漏洞处置流程,在发现设备存在安全缺陷、漏洞等安全风险时采取修复或替代方案等补救措施,按照有关规定及时告知用户并向有关主管部门报告,留存了补救措施记录、验证材料和报告记录。
- e) 判定原则:

测试结果应与预期结果相符,否则不符合要求。

漏洞补救措施可以是漏洞修复补丁、升级包、技术方案等。

7.3.4 远程维护

- a) 安全要求:

远程维护安全要求见 GB40050-2021 6.3 d) e)。

 - 1) 在对设备进行远程维护时,应明示维护内容、风险以及应对措施,应留存不可更改的远程维护日志记录,记录内容应至少包括维护时间、维护内容、维护人员、远程维护方式及工具。

注:常见的远程维护包括对设备的远程升级、配置修改、数据读取、远程诊断等操作。

 - 2) 在对设备进行远程维护时,应获得用户授权,并支持用户中止远程维护,应留存授权记录。
- b) 预置条件:
 - 1) 厂商提供设备远程维护的操作规程和实施记录。
- c) 检测方法:
 - 1) 检查厂商提供的远程维护的操作规程和实施记录,确认是否明示维护内容、风险以及应对措施,是否留存不可更改的远程维护日志记录,记录内容是否包括维护时间、维护内容、维护人员、远程维护方式及工具。
 - 2) 检查厂商提供的远程维护的操作规程和实施记录,确认是否留存用户授权记录,确认是否支持用户中止远程维护。
- d) 预期结果:
 - 1) 远程维护的操作规程和实施记录中明示维护内容、风险以及应对措施,留存不可更改的远程维护日志记录,记录内容包括维护时间、维护内容、维护人员、远程维护方式及工具。
 - 2) 远程维护的操作规程和实施记录中留存用户授权记录,授权方式可以是鉴别信息授权、书面授权等其中的至少一种,能够支持用户中止远程维护。
- e) 判定原则:

测试结果应与预期结果相符,否则不符合要求。

7.3.5 补丁包/升级包的完整性、来源真实性进行验证

- a) 安全要求:

补丁包/升级包的完整性、来源真实性进行验证安全要求见 GB40050-2021 6.3 f)。

应为用户提供对补丁包/升级包的完整性、来源真实性进行验证的方法。
- b) 预置条件:

- 1) 厂商提供说明材料, 说明为用户提供的对补丁包/升级包的完整性、来源真实性进行验证的方法。
- c) 检测方法:
 - 1) 检查厂商提供的说明材料, 确认是否包含为用户提供的对补丁包/升级包的完整性、来源真实性进行验证的方法, 确认是否验证方法的有效性。
- d) 预期结果:
 - 1) 说明材料中明确包含为用户提供的对补丁包/升级包的完整性、来源真实性进行验证的方法, 包含对验证方法的有效性验证。
- e) 判定原则:

测试结果应与预期结果相符, 否则不符合要求。

7.3.6 销毁处理

- a) 安全要求:

销毁处理安全要求见 GB40050-2021 6.3 g) h) i) 。

 - 1) 应为用户提供对废弃(或退役)设备中关键部件或数据进行不可逆销毁处理的方法。
 - 2) 应为用户提供废弃(或退役)设备回收或再利用前的关于数据泄漏等安全风险控制方面的注意事项。
 - 3) 对于维修后再销售或提供的设备或部件, 应对设备或部件中的用户数据进行不可逆销毁。
- b) 前置条件:
 - 1) 厂商提供说明材料, 说明为用户提供的对废弃(或退役)设备中关键部件或数据进行不可逆销毁处理的方法和实施记录。
 - 2) 厂商提供说明材料, 说明为用户提供的废弃(或退役)设备回收或再利用前的关于数据泄漏等安全风险控制方面的注意事项及实施记录。
 - 3) 厂商提供说明材料, 说明对于维修后再销售或提供的设备或部件中的用户数据进行不可逆销毁的方法和实施记录。
- c) 检测方法:
 - 1) 检查厂商提供的说明材料, 确认是否包括为用户提供对废弃(或退役)设备中关键部件或数据进行不可逆销毁处理的方法, 确认是否包含对销毁方法的有效性验证, 检查实施记录, 确认是否按照标准要求对数据进行不可逆销毁。
 - 2) 检查厂商提供的说明材料, 确认是否包括为用户提供的废弃(或退役)设备回收或再利用前的关于数据泄漏等安全风险控制方面的注意事项, 检查实施记录, 确认是否按照标准要求为用户提供材料。
 - 3) 检查厂商提供的说明材料, 确认是否包括对于维修后再销售或提供的设备或部件中的用户数据进行不可逆销毁的方法, 确认是否包含对销毁方法的有效性验证, 检查实施记录, 确认是否按照标准要求对数据进行不可逆销毁。
- d) 预期结果:
 - 1) 说明材料中明确包括为用户提供对废弃(或退役)设备中关键部件或数据进行不可逆销毁处理的方法, 包含对销毁方法的有效性验证, 存在对应的实施记录, 且记录应是按照标准要求对数据进行不可逆销毁。
 - 2) 说明材料中明确包括为用户提供的废弃(或退役)设备回收或再利用前的关于数据泄漏等安全风险控制方面的注意事项, 存在对应的实施记录, 且记录应是按照标准要求为用户提供材料。

- 3) 说明材料中明确包括对于维修后再销售或提供的设备或部件中的用户数据进行不可逆销毁的方法, 包含对销毁方法的有效性验证, 存在对应的实施记录, 且记录应是按照标准要求对数据进行不可逆销毁。
- e) 判定原则:
测试结果应与预期结果相符, 否则不符合要求。

7.3.7 安全维护要求

- a) 安全要求:
安全维护要求见 GB40050-2021 6.3 j)。
应在约定的期限内, 为设备提供持续的安全维护, 不应以业务变更、产权变更等原因单方面中断或终止安全维护。
- b) 预置条件:
 - 1) 厂商提供说明材料, 说明与客户约定的安全维护要求。
- c) 检测方法:
 - 1) 检查厂商提供的说明材料, 确认是否包括在约定的期限内, 为设备提供持续的安全维护, 不应以业务变更、产权变更等原因单方面中断或终止安全维护。
- d) 预期结果:
 - 1) 说明材料中明确包括在约定的期限内, 为设备提供持续的安全维护, 不应以业务变更、产权变更等原因单方面中断或终止安全维护。
- e) 判定原则:
测试结果应与预期结果相符, 否则不符合要求。

7.3.8 生命周期终止要求

- a) 安全要求:
生命周期终止要求见 GB40050-2021 6.3 k)。
应向用户告知设备生命周期终止时间。
- b) 预置条件:
 - 1) 厂商提供说明材料, 说明向用户告知设备生命周期终止时间。
- c) 检测方法:
 - 1) 检查厂商提供的说明材料, 确认是否明确要求网络关键设备应通过合适的方式(例如: 网站公告等)向用户提前告知设备生命周期终止时间, 检查实施记录, 确认对停止生命周期的设备进行了提前告知。
- d) 预期结果:
 - 1) 说明材料中明确了厂商通过合适的方式(例如: 网站公告等)向用户提前告知设备生命周期终止时间。存在对停止生命周期的设备进行提前告知的实施记录。
- e) 判定原则:
测试结果应与预期结果相符, 否则不符合要求。

附 录 A
(资料性)
主要部件清单

路由器、交换机常见的主要部件：主控板卡、业务板卡、交换网板、风扇模块、电源、存储系统软件的板卡、硬盘或闪存卡等。

服务器常见的主要部件：中央处理器、硬盘、内存、风扇模块、电源等。


PLC 设备常见的主要部件：PLC 的主要部件可包括电源模块、CPU 模块、网络通信信息模块、输入输出模块等。



参 考 文 献

- [1] GB 40050-2021 网络关键设备安全通用要求
- [2] GB/T 39680-2020 信息安全技术 服务器安全技术要求和测评准则
- [3] GB/T 36470-2018 信息安全技术 工业控制系统现场测控设备通用安全功能要求
- [4] YD/T 1439-2006 路由器设备安全测试方法——高端路由器（基于 IPv4）
- [5] 3GPP TS 33.117 Catalogue of general security assurance requirements





电信终端产业协会团体标准
网络关键设备安全通用检测方法

T/TAF 088—2021

*

版权所有 侵权必究

电信终端产业协会印发

地址：北京市西城区新街口外大街 28 号

电话：010-82052809

电子版发行网址：www.taf.org.cn