ICS 33.050
CCS M 30

团　体　标　准

T/TAF 230—2024

光传送网设备安全技术要求

Security technical requirements for optical transport network equipment

2024-05-13 发布　　2024-05-13 实施

电信终端产业协会　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。

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提出并归口。

本文件起草单位：中国信息通信研究院、华为技术有限公司、成都泰瑞通信设备检测有限公司、武汉网锐检测科技有限公司、中兴通讯股份有限公司、上海泰峰检测认证有限公司、北京通和实益电信科学技术研究所有限公司、博鼎实华（北京）技术有限公司、郑州信大捷安信息技术股份有限公司、深圳信息通信研究院、北京邮电大学。

本文件主要起草人：路晔绵、张治兵、吴荣春、刘欣东、刁汝楠、吴翔宇、龚志红、陈玺、周继华、任华、宋祥烈、张大超、刘刚、刘向东、刘为华、刘献伦、唐伟生、李冠伟、邓科、张杰、王伟、吴文旭。

光传送网设备安全技术要求

1 范围

本文件规定了针对光传送网（OTN）设备的安全技术要求，包括安全功能要求和安全保障要求。其中安全功能要求主要关注于光传送网设备应具备的安全功能，以及需要网络管理系统或模块配合完成的安全功能。安全保障要求主要关注于光传送网设备的安全管理的要求。

本文件适用于光传送网设备的研制、生产、测试、评估与认证。

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 40050—2021 网络关键设备安全通用要求

ISO/IEC 9899:2018 C语言规范（Programming languages—C）

3 术语和定义

GB/T 25069—2022界定的以及下列术语和定义适用于本文件。

3.1

信任根 root of trust

处于信任链初始位置，用于验证信任链上后续实体完整性和真实性的实体。

4 缩略语

下列缩略语适用于本文件。

ARP：地址解析协议（Address Resolution Protocol）

ASLR：地址空间布局随机化（Address Space Layout Randomization）

DoS：拒绝服务（Denial of Service）

DTLS：数据包传输层安全性协议（Datagram Transport Layer Security）

ICMP：因特网控制报文协议（Internet Control Message Protocol）

LTS：长期支持（Long Term Support）

NX：不可执行（No-eXecute）

OTN：光传送网（Optical Transport Network）

PIE：地址无关可执行（Position-Independent Executable）

RADIUS：远程用户拨号认证服务（Remote Authentication Dial In User Service）

SFTP：安全文件传输协议（Secret File Transfer Protocol）

SNMP：简单网络管理协议（Simple Network Management Protocol）
SSH：安全外壳协议（Secure Shell）
SYN：同步序列编号（Synchronize Sequence Numbers）
TACACS：终端访问控制器访问控制系统（Terminal Access Controller Access-Control System）
TCP：传输控制协议（Transmission Control Protocol）
TLS：传输层安全协议（Transport Layer Security）
UDP：用户数据报协议（User Datagram Protocol）
USB：通用串行总线（Universal Serial Bus）

5 安全要求

5.1 概述

光传送网设备的安全威胁和安全目的分析可见附录B。

光传送网设备的安全要求可分为安全功能要求和安全保障要求，可根据不同安全要求提供的安全防护能力强弱将安全要求分为三个等级，不同级别的安全防护能力如下。

——一级安全要求（基本级）：能够防护拥有很少资源的威胁源发起的恶意攻击所造成的关键资源损害，能够对抗来自于应用层面和网络层面的基础攻击，能够妥善应对产品中的安全漏洞、具备漏洞修复或缓解措施，能够记录安全事件以供审计和处置。

——二级安全要求（增强级）：能够防护拥有较为丰富资源的威胁源发起的恶意攻击造成的重要资源损害，在满足一级安全要求的基础上，能够提供操作系统层的安全防护能力，能够提供软件供应链安全检查，能够提供数据加密存储，能够及时发现、监测攻击行为，能够在自身遭到损害后进行一定的恢复。

——三级安全要求（卓越级）：能够防护拥有丰富资源的威胁源发起的恶意攻击造成的主要资源损害，在满足二级安全要求的基础上，能够从多个层面限制攻击者的访问能力，能够提供合适的加密能力和安全协议，能够提供更灵活的恢复能力。

各等级对应的条款见附录A。

5.2 安全功能要求

5.2.1 操作系统安全

光传送网设备使用的操作系统满足以下要求：

a） 应使用具备用户态进程与操作系统内核隔离能力的操作系统；
b） 若支持多用户机制，应禁止操作系统特权用户远程访问设备；
c） 应限制或去除操作系统中的调试能力或工具；
d） 若存在文件系统，应限定操作系统可执行文件及其所属文件夹的写权限仅创建当前文件的主体可拥有；
e） 操作系统应默认开启ASLR配置以加强系统安全性；
f） 若支持多用户和用户组机制，应为不同风险等级的进程分配不同的用户和用户组；
g） 设备上运行的进程应根据业务诉求最小化使用系统特权（如capability特权）；
h） 操作系统应使用强制访问控制机制（例如SELinux），控制关键资源（例如加密密钥）的访问权限。

5.2.2 软件安全

光传送网设备软件满足以下要求：

a） 满足本文件一级要求的设备中不应存在已公布的中危及以上级别安全漏洞，或具备补救措施防范漏洞风险；满足本文件二级及三级要求的设备中不应存在已公布的所有级别安全漏洞，或具备补救措施防范漏洞风险；

b） 设备软件包中不应存在病毒等恶意代码；

c） 设备应支持安全启动，在设备启动时逐级校验软件完整性；

d） 设备加载软件升级包、补丁等文件时，应验证文件的完整性，拒绝加载被篡改的文件；

e） 应使用数字签名技术验证软件升级包、补丁等文件的完整性和来源；

f） 应基于硬件机制保护安全启动使用的信任根不被篡改。

5.2.3 身份鉴别与访问控制

光传送网设备支持以下身份鉴别与访问控制要求：

a） 应对设备用户进行身份标识和鉴别，身份标识应具有唯一性；

b） 若支持多用户，应具备创建、禁用（或主动锁定）、删除账号的能力，且相应操作应仅由具备安全管理员组权限的管理员账号方可实施；

c） 应支持自动禁用长期未使用的账号；

d） 应支持账号角色管理，对每个账号分配合适的角色，不同的角色具备不同的权限，应仅允许经过身份鉴别的账号执行权限范围内的操作；

e） 使用口令鉴别方式时，应满足以下要求：

1） 应支持首次登录设备时强制修改默认口令或设置口令；

2） 应支持设置口令生存周期；

3） 应支持口令复杂度检查及长度检查，其中满足本文件一级要求的设备，口令应至少包含如下字符中的三种：大写字母、小写字母、数字、特殊字符，长度至少为8个字符；满足本文件二级及三级要求的设备，口令应至少包含如下字符中的四种：大写字母、小写字母、数字、特殊字符，长度至少为12个字符；

4） 应提供口令防暴力破解机制；

注：常见的口令防暴力破解机制包括限制连续的非法登录尝试次数、登录延迟、使用验证码等。

5） 用户修改口令应重新进行身份鉴别；

f） 当出现鉴别失败时，设备应提供无差别反馈，避免提示“用户名错误”“口令错误”等类型的具体信息；

g） 应支持远程认证管理方式；

h） 远程认证管理应支持使用安全的传输通道进行交互，如基于DTLS、TLS保护的RADIUS、TACACS认证等；

i） 应具备用户弱口令字典管理功能，并支持用户自行配置弱口令字典内容。

5.2.4 通信安全

5.2.4.1 通信主体身份认证

光传送网设备应对连接至管理接口的设备或系统（如网管系统）进行身份认证，仅允许合法主体接入管理接口。

5.2.4.2 通信协议安全

光传送网设备使用通信协议满足以下要求：

a） 应支持安全的TLS/SSH协议版本，并使用安全的加密算法套件；
b） 应支持安全的SNMP协议版本，并使用安全的加密算法套件；
c） 应支持安全的SFTP协议，并使用安全的加密算法套件。

5.2.4.3 证书使用

光传送网设备支持以下证书使用要求：
a） 设备应支持基于数字证书的身份认证机制；
b） 设备导入数字证书时，应对证书正确性进行校验；
c） 设备应支持数字证书的更新或替换；
d） 设备应支持吊销证书的处理；
e） 应支持设备证书过期告警；
f） 应支持查询证书状态、证书有效期、证书应用场景等信息。

5.2.5 数据安全

光传送网设备提供的数据保护机制满足以下要求：
a） 设备上的敏感数据（如口令、私钥等）不应在操作时进行明文显示；
b） 设备上的敏感数据（如口令、私钥等）应进行加密存储；
c） 设备应支持传输加密（如OTNSec）能力，保护传输数据的机密性；
d） 传输数据的加密，应使用安全强度不弱于128bit的密码算法；
注1：密码算法安全强度是指与破坏密码算法或系统所需的工作量相关联的数字，单位为bit。一个算法安全强度为128 bit，则意味着攻破它所需的计算量为2的128次方。该定义来源于NIST Special Publication 800-57 Part 1, Revision 5, Recommendation for Key Management: Part 1 - General。
e） 应采用多级密钥管理机制，保护密钥的机密性。
注2：密钥管理机制通常包含密钥派生、密钥更新、密钥销毁等一个或多个环节的内容。

5.2.6 防护能力

5.2.6.1 管理端口防攻击

光传送网设备管理端口满足以下防攻击要求：
a） 应具备防ARP攻击能力；
注：常见ARP攻击如：ARP泛洪、ARP欺骗等。
b） 应具备防ICMP/UDP/TCP SYN报文DoS攻击能力；
c） 应具备流量控制功能，在设备遭受DoS攻击时，保证设备正常运行。

5.2.6.2 暴露面最小化

光传送网设备应尽可能减少暴露的攻击面，满足以下要求：
a） 默认状态下开启的端口和服务应满足GB 40050—2021中5.6 a)的要求；
b） 非默认开放的端口和服务应满足GB 40050—2021中5.6 b)的要求；
c） 设备主控板上不应存在调试接口或调试接口不可用；
注：常见调试接口如JTAG，调试串口，调试网口，调试USB等。
d） 设备主控板上不应存在调试接口的标识丝印。

5.2.6.3 备份恢复与冗余

光传送网设备备份恢复与冗余设计满足以下要求：

a） 应支持设备本地备份及备份导出功能，实现异常场景业务恢复；

b） 应提供对备份文件进行完整性保护的措施；

c） 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，应满足GB 40050—2021中5.2 a）的要求；

d） 应支持定时备份和手动备份两种模式。

5.2.6.4 异常检测能力

光传送网设备应提供安全防护能力，满足以下要求：

a） 应具备账号暴力破解入侵行为的检测和告警能力；

注1：告警形式可包括日志中记录、邮件通知、风险提示等形式。

b） 应具备常见操作系统入侵行为的检测和告警能力；

注2：常见操作系统入侵行为包括但不限于文件权限提升操作、超级用户创建等。

c） 应支持对异常账号操作行为的检测和告警。

注3：异常账号如被暴力破解的账号、被异常账号创建的账号等。

5.2.6.5 安全配置管理

光传送网设备应支持安全配置管理能力，应提供安全配置基线管理、安全配置核查功能。

注：安全配置包括但不限于安全协议版本配置、安全算法配置等。

5.2.7 日志审计和管理

光传送网设备满足以下日志审计和管理要求：

a） 应支持对管理员用户活动、操作指令等操作记录日志，记录应包括用户ID、时间、事件类型等；

b） 应仅允许管理员用户访问和查看日志信息；

c） 应禁止对安全操作相关日志的删除和修改；

d） 应支持基于安全传输协议的日志备份机制，例如基于TLS的Syslog协议，并将日志记录实时传输到服务器；

e） 应对日志文件进行访问控制，应仅限创建文件的主体进行读写操作，其所属用户组仅可进行读操作，其他用户不可进行读写操作。

5.3 安全保障要求

5.3.1 设计和开发

光传送网设备提供者应在光传送网设备的设计和开发环节满足以下要求：

a） 设备使用的开源软件应经过主流杀毒软件扫描，以确保无恶意程序植入；

b） 应对已发现的开源软件的安全漏洞进行及时修复，或提供补救措施；

c） 使用开源软件应提供对外开源使用声明，并保证用户在获取产品软件包时可获取该内容；

d） 应确保提供所有使用的开源软件的许可证，且履行许可证要求；

e） 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；

f） 应对设备使用的开源软件进行管理，保证设备使用的开源软件为开源社区官网或官方托管网站的正式发布版本，核心软件所用开源软件应优先选择开源社区官网或官方托管网站LTS版本或稳定版本，不应使用已停止维护的开源软件版本；

注1：核心软件一般可包括驱动引导、操作系统类软件、编译类软件、算法类软件、核心应用软件等。

g） 应提供措施确保设备使用的开源软件源码可追溯到来源社区；
h） 应对设备使用的开源软件版本进行管理，确保设备使用的开源软件版本归一，不应在产品中使用同一开源软件的不同版本；
i） 应维护设备所用开源软件清单，并确保设备实际所用开源软件及其版本与开源软件清单一致；
j） 应针对所用开源软件的生命周期制定管理机制，明确开源软件生命周期关键节点（如停止维护、停止服务等），并根据关键节点对开源软件进行维护（如升级、更换其他软件等）；
k） 应建立完善的开源软件漏洞管理机制，包括以下内容：
1） 应实现漏洞感知可追溯，将所有已发现漏洞进行记录并入库；
2） 应实现漏洞影响范围可追溯，可根据漏洞信息查询到受漏洞影响的产品；
3） 应实现漏洞修改发布过程可追溯，对技术方案修补、结果验证、公告发布等环节进行流程跟踪；
l） 设备所用软件编译时应开启安全编译选项，包括但不限于PIE、NX等；
m） 设备软件应在代码中使用安全的字符串操作函数，其中安全字符串操作函数所占比例不低于20%时满足本文件二级要求，安全字符串操作函数所占比例不低于40%时满足本文件三级要求；

注2：安全字符串操作函数范围见ISO/IEC 9899:2018标准的K3.7章节，包括memcpy_s、memmove_s、strcpy_s、strncpy_s、strcat_s、strncat_s、strtok_s、memset_s、strerror_s、strerrorlen_s、strnlen_s；对应的非安全字符串操作函数为memcpy、memmove、strcpy、strncpy、strcat、strncat、strtok、memset、strerror、strerrorlen、strnlen。

注3：安全字符串操作函数的占比计算如下：安全字符串操作函数百分比 = 安全字符串操作函数调用次数 /（非安全字符串操作函数调用次数 + 安全字符串操作函数调用次数）* 100%。

n） 应保证设备证书一机一证；
o） 应实现开源软件漏洞修复过程的信息化管理（使用IT系统），包含开源软件漏洞感知、影响分析和修复记录等内容的管理。

5.3.2 生产和交付

光传送网设备提供者应在光传送网设备的生产和交付环节满足以下要求：
a） 应为用户提供安全配置加固指导文档，列出设备安全风险项及对应的手工加固指导；
b） 应提供设备开放端口使用说明，并提供设备服务与设备默认端口的映射关系说明；
c） 交付设备前，应对设备进行漏洞扫描，发现设备存在已知漏洞应当立即采取补救措施；
d） 应在交付前对设备软件包进行病毒扫描，确保其中不存在病毒等恶意代码。

5.3.3 运行和维护

光传送网设备提供者应在光传送网设备的运行和维护环节满足以下要求：
a） 应向用户提供漏洞反馈渠道、漏洞处理流程和设备漏洞安全公告查看途径；
b） 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；
c） 应向用户告知设备生命周期终止时间。

附 录 A
（规范性）
安全等级划分

本文件中三个安全等级对应的条款如表 A.1 所示。

表 A.1 光传送网设备安全技术要求条款等级划分表

安全要求			一级（基本级）	二级（增强级）	三级（卓越级）
安全功能要求	操作系统安全		-	5.2.1 a)~e)	5.2.1
	软件安全		5.2.2 a)b)	5.2.2 a)~d)	5.2.2
	身份鉴别与访问控制		5.2.3 a)~e)	5.2.3 a)~g)	5.2.3
	通信安全	通信主体身份认证	5.2.4.1	5.2.4.1	5.2.4.1
		通信协议安全	5.2.4.2	5.2.4.2	5.2.4.2
		证书使用	-	-	5.2.4.3
	数据安全		5.2.5 a)	5.2.5 a)~c)	5.2.5
	防护能力	管理端口防攻击	5.2.6.1	5.2.6.1	5.2.6.1
		暴露面最小化	5.2.6.2 a)b)	5.2.6.2	5.2.6.2
		备份恢复与冗余	-	5.2.6.3 a)~c)	5.2.6.3
		异常检测能力	-	5.2.6.4 a)b)	5.2.6.4
		安全配置管理	-	5.2.6.5	5.2.6.5
	日志审计和管理		5.2.7 a)~c)	5.2.7	5.2.7
安全保障要求	设计和开发		5.3.1 a)~e)	5.3.1 a)~n)	5.3.1
	生产和交付		5.3.2	5.3.2	5.3.2
	运行和维护		5.3.3	5.3.3	5.3.3

附 录 B
（资料性）
安全威胁与安全目的分析

B.1 安全资产

光传送网设备的核心资产如下：

a) 传输的业务数据；
b) 设备上存储的用户数据、配置信息、审计记录等；
c) 设备备份数据；
d) 设备系统代码、系统升级包、软件包等。

光传送网设备在设计和实现过程中应采取措施保护上述资产的机密性、完整性和可用性。

B.2 安全威胁

光传送网设备可能面临以下安全威胁：

a) 系统完整性破坏：
   1) 攻击者通过替换或篡改设备软件包或升级包，注入恶意代码加载运行，
   2) 攻击者通过利用系统漏洞或缺陷，破坏系统内核代码的运行；
b) 非授权访问：
   1) 攻击者伪装成合法用户或破解用户口令登录设备，以在设备中创建后门账号等方式实现对设备的持续控制，
   2) 攻击者伪装成合法设备接入传输网络，获取网络中传输的数据，
   3) 攻击者通过利用代码中的漏洞或缺陷，提升自身进程权限，绕过访问控制机制，访问或篡改系统中存储的敏感数据；
c) 数据泄露：
   1) 攻击者通过侦听设备的通信，截获不安全通信协议中明文传输的机密数据，
   2) 攻击者通过开放的端口、系统调试接口、软件漏洞等方式，侵入设备内部，获取设备上存储的用户数据、配置信息、审计记录、备份数据等敏感数据；
d) 攻击面暴露：
   1) 用户进行错误的配置，导致可被攻击者利用的攻击路径扩大，例如将通信协议配置为不安全的版本，从而导致敏感数据明文传输，
   2) 设备开启不安全的服务，导致可被攻击者利用获取传输数据或侵入系统内部。
e) 设备可用性破坏：
   1) 攻击者通过泛洪攻击设备管理端口，导致设备脱管，
   2) 外部攻击、核心配置数据丢失等导致产品当前运行部件或系统功能失效，造成业务中断。

B.3 安全目的

为了应对可能的安全威胁，光传送网设备应实现以下安全目的。

a) 操作系统安全防护。光传送网设备操作系统应通过隔离技术、权限最小化等措施，限制应用进程的能力，保护系统内核代码的运行，从而保护系统的完整性，同时避免应用进程进行非授权访问。光传送网设备操作系统应通过限制调试能力、开启安全配置等措施，减少暴露的攻击面，减少可被恶意应用程序利用的缺陷，从而保护系统运行的完整性。

b) 软件安全防护。光传送网设备应通过安全启动、安全更新等措施，对设备的软件包和升级包进行完整性校验，从而保护系统运行代码的完整性。光传送网设备应采取开启安全编译选项、使用安全操作函数等措施尽量减少软件包中可被利用的漏洞和缺陷，从而避免被攻击者利用破坏系统的完整性。

c) 身份鉴别与访问控制。光传送网设备应提供身份鉴别与访问控制机制，对访问者的身份及权限进行限制，以尽可能防止非授权访问的发生。

d) 通信协议安全防护。光传送网设备应使用安全的通信协议及安全的密码算法套件，从而保护传输中的业务数据的安全，避免数据泄露。

e) 证书安全使用。应通过设备证书对光传送网设备身份进行识别和管理，并保证证书使用的安全，以避免攻击者伪装成合法设备进行非授权访问。

f) 数据机密性保护。光传送网设备应使用合适的密码算法和密钥管理机制，对设备上存储和传输的敏感数据进行机密性保护，避免数据泄露。

g) 管理端口安全保护。光传送网设备应提高管理端口的防攻击能力，避免设备因外部攻击脱管，影响设备的可用性。

h) 暴露面最小化。光传送网设备应尽可能减少暴露的接口和端口，减少可被攻击者利用的攻击路径。

i) 可靠性设计。光传送网设备应采取备份、资源冗余设计等措施，以便在设备遭受攻击时仍可保证一定的可用性。

j) 系统入侵检测。光传送网设备应提供入侵检测能力，及时感知设备安全状态，减缓或阻断攻击，增强纵深防御能力。

k) 安全配置核查。光传送网设备应提供安全配置核查能力，避免因用户的错误配置或不安全服务的开启导致可被攻击者利用的攻击路径扩大。

l) 日志审计和管理。光传送网设备应提供日志审计能力，记录安全相关操作和事件，以便进行安全事件的分析和溯源；光传送网设备应对审计日志进行保护，以保证其完整性和可用性。

参 考 文 献

[1] NIST SP 800-57 Part 1, Revision 5, Recommendation for Key Management: Part 1 – General

电信终端产业协会团体标准

光传送网设备安全技术要求

T/TAF 230—2024

*

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