ICS 33.050
CCS M 30

团　体　标　准

T/TAF 133—2022

网络产品供应链安全要求　制造要求

Security requirements for network product supply chain—
Manufacture requirements

2022-09-15 发布　　2022-09-15 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。

本文件是网络产品供应链安全要求系列标准之一，该系列标准结构如下：

——《网络产品供应链安全要求》

——《网络产品供应链安全要求　采购要求》

——《网络产品供应链安全要求　物流要求》

——《网络产品供应链安全要求　制造要求》

请注意本文件中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、联想（北京）有限公司、中兴通讯股份有限公司、新华三技术有限公司、成都泰瑞通信设备检测有限公司、杭州迪普科技股份有限公司、浪潮电子信息产业股份有限公司、深圳市腾讯计算机系统有限公司。

本文件主要起草人：张治兵、郭春颖、薄菁、薛勇波、杨春阳、陈鹏、李汝鑫、柯妍、施辰琛、汪剑、周继华、吴萍、童天予、万晓兰、仇俊杰、宋桂香、倪平。

网络产品供应链安全要求　制造要求

1　范围

本文件提出了网络产品在制造环节的安全管理、组织机构和人员、信息系统等不同等级的安全要求，包括产品导入、生产、生产外包、维修、追溯等过程的安全要求。

本文件适用于网络产品的提供者对供应链制造过程进行安全管理，也可为网络产品的采购者和第三方机构对网络产品制造过程进行安全性评价时提供参考。

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。

T/TAF 073—2020　网络产品供应链安全要求

3　术语和定义

下列术语和定义适用于本文件。

3.1

网络　network

是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

[来源：T/TAF 073—2020，3.1]

3.2

网络产品　network product

是指作为网络组成部分以及维持网络功能的设备、软件等。

[来源：T/TAF 073—2020，3.2]

3.3

供应链　supply chain

通过多个资源和过程联系在一起的一系列组织，根据由服务协议或其他采购协议建立连续的供应关系，每个组织充当一个需求方、提供方或双重角色。

[来源：T/TAF 073—2020，3.3]

3.4

采购　purchase

指组织在一定的条件下从供应市场获取产品或服务作为组织资源，以保证组织生产及经营活动正常开展的一项经营活动。

[来源：T/TAF 073—2020，3.8]

3.5

关键部件　critical component

存储软件、数据的介质以及具备数据处理能力的部件。如芯片、存储介质、可编程控制器件等。

[来源：T/TAF 073—2020，3.10]

3.6

职责分离 separation of duty

一项控制措施，用来确保同一个员工没有以下情况中的一种或两种，包括：

——某个流程的多个职责；

——应用系统的多个权限。

从而防止员工在不被察觉的情况下滥用、破坏或转移公司资产。

4 缩略语

下列缩略语适用于本文件。

DFM：可制造性设计（Design for Manufacturability）

MAC：媒体访问控制（Media Access Control）

5 制造要求概述

网络产品供应链安全要求中的制造安全包括以下三个目标：

a) 完整性：保障产品及其所包含的软件、关键部件、数据等以及所使用的工具在制造过程不被植入或篡改；

b) 真实性：防止部件在制造过程中被伪造或替换，保障生产过程及交付给客户产品的真实性；

c) 可追溯性：对产品和主要部件建立唯一性标识，可识别其来源，并确保这些信息有效，支撑产品和部件在制造过程中的可追溯性。芯片、存储介质、可编程控制器件、软件等部件可以使用来料批次信息或软件版本号进行标识。

制造要求管理框架见图1。

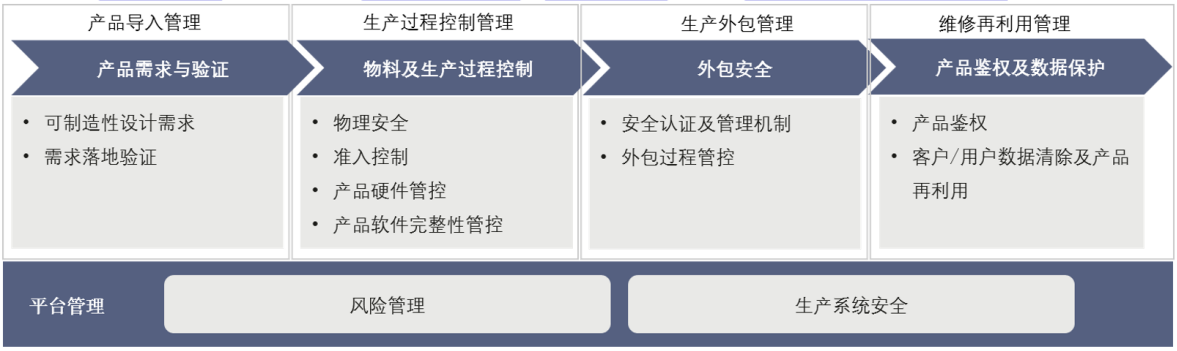

图 1 制造要求管理框架

由于网络产品供应链在不同产品业务场景下，其制造环节安全管理要求存在差异。本文件将制造安全要求分为三个等级，即一级、二级和三级，安全等级由低到高，安全要求逐级增强。一级提出了保障供应链制造安全管理的基本要求。二级在基本要求的基础上，增加了安全培训、过程可追溯、数据保护、网络隔离等要求，以增强供应链制造环节安全保障。三级在二级要求的基础上增加了应急演练、异常监控等要求，并通过增加使用自动化工具和技术要求，对供应链制造环节提供较强的安全保障。每一等级定义了网络产品供应链满足相应等级要求的最小集合，满足该等级标识的所有项目才能标识为该级别。制造安全要求等级划分见表 1。安全要求条目中的“ALL”表示一级、二级和三级均具有该要求，“L2，L3”表示二级和三级具有该要求，“L3”表示三级具有该要求。

表 1　制造安全要求等级划分表

制造安全要求				一级	二级	三级
6 总体要求			(a)	✓	✓	✓
			(b)	—	✓	✓
			(c)	✓	✓	✓
			(d)	—	—	✓
			(e)	—	✓	✓
			(f)	—	✓	✓
7 网络产品制造环节安全要求	7.1 产品导入		(a)	✓	✓	✓
			(b)	✓	✓	✓
			(c)	✓	✓	✓
	7.2 生产过程控制	7.2.1 物理安全	(a)	✓	✓	✓
			(b)	✓	✓	✓
		7.2.2 准入控制	(a)	✓	✓	✓
			(b)	✓	✓	✓
		7.2.3 产品硬件管控	(a)	✓	✓	✓
			(b)	✓	✓	✓
			(c)	✓	✓	✓
			(d)	✓	✓	✓
			(e)	✓	✓	✓
			(f)	—	✓	✓
		7.2.4 产品软件完整性管控	(a)	✓	✓	✓
			(b)	✓	✓	✓
			(c)	✓	✓	✓
			(d)	✓	✓	✓
			(e)	✓	✓	✓
			(f)	—	—	✓
	7.3 生产外包管理		(a)	✓	✓	✓
			(b)	✓	✓	✓
			(c)	✓	✓	✓
			(d)	✓	✓	✓
			(e)	—	✓	✓
			(f)	—	—	✓
	7.4 维修		(a)	✓	✓	✓
			(b)	—	✓	✓
			(c)	✓	✓	✓
	7.5 生产系统安全		(a)	✓	✓	✓
			(b)	✓	✓	✓
			(c)	✓	✓	✓
			(d)	—	✓	✓
			(e)	✓	✓	✓
			(f)	—	✓	✓
			(g)	—	✓	✓
			(h)	—	—	✓

注 1：“—”表示不具有该要求；“✓”表示具有该要求。
注 2：表中制造安全要求对应本文件第 6 章至第 7 章。

6 总体要求

网络产品提供者应：

a) （ALL）建立制造环境的网络安全与数据保护管理要求，并形成基线；

b) （L2，L3）制造环境的网络安全与数据保护管理要求应融入生产流程和业务过程，按照基线定期进行网络安全评估并留存评估记录；

c) （ALL）定期识别制造所有流程中各种可能存在的安全风险，进行评估、制定处置方案及预防措施，并对处置方案及预防措施进行评估和度量；

d) （L3）针对网络安全高风险场景（如 IT 系统被攻击、软件服务器宕机、加载的软件被植入、篡改等）制定应急演练计划，定期开展应急演练；

e) （L2，L3）制定安全培训计划，对员工进行网络安全意识和技能培训；

f) （L2，L3）识别制造环节的网络安全关键岗位人员，建立并维护网络安全关键岗位人员名单，并在招聘前落实背景调查，在上岗、内部调配、离岗等环节通过培训、权限管控等措施进行管理。

7 网络产品制造环节安全要求

7.1 产品导入

网络产品提供者应：

a) （ALL）将对产品的制造网络安全要求(包括但不限于：生产环节软件完整性校验，生产环节硬件防护，禁止未公开接口，产品中的数据储存范围、清除及验证方法等)纳入 DFM 并传递给研发；

b) （ALL）在产品量产前验证 DFM 需求得到实现；

c) （ALL）与研发协同，建立和维护关键物料清单。

7.2 生产过程控制

7.2.1 物理安全

网络产品提供者应：

a) （ALL）对制造中的产品安全以及与产品安全防护相关的基础设施（如：摄像头、门禁、安检等硬件设施）进行管理；生产区域的主要出入口、主通道、货台等关键物流路径及网络安全关键区域（如：网络安全关键物料存放区域、库房、软件灌装、生产软件服务器存放区域等），须确保监控录像有效覆盖；

b) （ALL）采取措施重点对网络安全关键区域的物理设施进行管理(如设立区域责任人，定期巡查、检测、维护等)，防止其被破坏，保证这些设施的正常运行。

7.2.2 访问控制

网络产品提供者应：

a) （ALL）对生产场所、仓储区域的门禁、安保等进行有效管理，防止非授权进入、非授权接触产品；生产现场外来人员需由内部人员陪同管理，降低产品在制造环节被破坏和被伪造的风险；

b) （ALL）对涉及生产和交付的 IT 系统，明确用户权限设置策略及口令管理要求，保护产品软件的完整性及客户信息的安全。

7.2.3 产品硬件管控

网络产品提供者应：

a) （ALL）识别第三方来料信息与采购要求的一致性，保证来源清晰可靠；
b) （ALL）应采取有效的技术手段对关键部件来料进行安全检验；
c) （ALL）在仓储及内部物流过程中对部件落实定期检查及盘点，确保账务与实物信息保持一致，在物料交接时，双方人员须核对账务与实物信息保持一致、记录完整；
d) （ALL）在生产使用前对存储器件进行格式化，确保产品硬件在生产、内部仓储及物流过程中的安全；
e) （ALL）存储生产过程中的物料配送、交接、制造、测试过程中的记录和数据，确保生产过程可追溯；
f) （L2，L3）对部件基于唯一标识(条码、标签、电子 ID 等)建立追溯体系，追溯能力应包含：产品或物料条码、日期、软件版本、产品或物料编码、合同号、对应关系等信息并被有效记录。

7.2.4 产品软件完整性管控

网络产品提供者应：

a) （ALL）制定安全的软件发布与部署流程获取软件（包括第三方软件），并依据职责分离原则对下载的软件进行完整性校验；
b) （ALL）在软件灌装环节进行软件完整性(如：数字签名) 校验，确保加载到产品中的软件与研发发布的一致；
c) （ALL）在产品测试时对配置参数(如：MAC 地址)进行检查，确保加载到产品中的配置参数的准确性；
d) （ALL）在完成产品最后测试步骤后验证接口状态，确保与发布状态一致；
e) （ALL）具备生产加载软件数字签名校验的能力，若涉及多级加工或者多地制造需要对软件进行分拆的，分拆的软件也应具备数字签名校验能力，在软件灌装前按加载软件的形态进行完整性校验；
f) （L3）通过 IT 实现软件发布、下载、灌装、加载、校验等全流程自动化管控，减少人工干预导致软件被植入或篡改。

7.3 生产外包管理

制造由生产外包合作商完成时，网络产品的提供者应：

a) （ALL）制定生产环境的网络安全与数据保护要求并融入到生产外包合作商的认证和管理流程中；
b) （ALL）确保所选择的生产外包合作商是认证通过并签署网络安全和数据保护协议的合格供应商，确保生产外包合作商生产与交付的产品及网络安全保障体系不低于组织的安全要求；
c) （ALL）应对生产外包合作商进行检查和考核等日常管理；
d) （ALL）采用安全的方法和传递途径(如 HTTPS 等)保证传递到生产外包合作商的软件安全；
e) （L2，L3）对生产外包生产过程进行监控，包括但不限于外包过程中安全规范的落实情况，人员的安全意识等；
f) （L3）通过 IT 自动获取生产外包合作商加载的软件信息，实现组织与生产外包合作商之间软件实体及加工信息同源传递。

7.4 维修

网络产品提供者应：

a) （ALL）对返回的物料或产品（包括未使用但已拆箱的退货物料或产品）进行鉴权，进行真实性、完整性检查，检查物料的外观、条码、编码、电子标签等，并进行功能检测，确保这些物料没有被篡改、植入；

b) （L2，L3）对返回物料中的个人信息及客户数据进行不可逆销毁，测试合格后方可再利用。可对存储介质采取低级格式化、放电、装备清除等方式无损不可逆销毁其中的数据；如无法进行无损不可逆销毁，可拆除并报废存储介质；

c) （ALL）对维修合格的产品重新加载软件并测试，测试合格后方可再进入供应环节。

7.5 生产系统安全

网络产品提供者应：

a) （ALL）建立与产品安全相关的生产系统清单（包括：制造执行系统、生产服务器、生产设备、IoT 设备、自动化装备、测试终端、可移动存储器件等），并定期维护生产系统所必需的信息（包括：软件许可信息、软件版本号、制造商、设备类型、型号、序列号、物理位置、网络地址等）；

b) （ALL）对产品安全相关的 IT 系统、软件和设备进入生产、测试网络进行安全检测和安全措施配置。安全检测需覆盖新采购设备、调拨设备、返厂维修设备、外部人员携带的设备等；安全控制措施包括安装杀毒软件、及时升级操作系统及防病毒补丁，设置设备定期病毒扫描等；

c) （ALL）评估生产过程中使用的工具和设备的安全风险，并制定相应的消减措施；

d) （L2，L3）建立与办公网络隔离且独立的生产网络及测试网络，建立不同业务属性之间的网络隔离措施。不同业务属性之间的防火墙应建立访问控制策略，不应对外暴露非业务需要端口；

e) （ALL）对生产系统的规划、设计、开发、验收及运维全生命周期进行安全管理，生产系统开发应遵从 IT 安全标准、法律法规等要求，在生产系统上线发布前应进行安全测试和安全验收，测试和验收合格方可使用；

f) （L2，L3）对生产业务数据进行分级管理，采取业务隔离、访问控制、数据加密、容灾备份、离线备份等防护措施，保障业务数据安全；

g) （L2，L3）建立应急响应程序，对生产过程中基础设施（如 IT 系统、测试装备等）的故障、产品安全（如漏洞）等进行管理；

h) （L3）建立网络异常监控能力，及时识别针对制造生产系统的内外部网络攻击行为，及时预警、响应及恢复。

参 考 文 献

[1] GB/T 24420—2009 供应链风险管理

[2] GB/T 32921—2016 信息安全技术 信息技术产品供应方行为安全准则

[3] GB/T 36637—2018 信息安全技术 ICT供应链安全风险管理指南

[4] ISO 28001:2007 Security management systems for the supply chain—Best practices for implementing supply chain security, assessments and plans—Requirements and guidance

[5] ISO/IEC 27036-2-2014 Information technology—Security techniques—Information security for supplier relationships—Part2: Requirements

[6] ISO/IEC 27036-3-2013 Information technology—Security techniques—Information security for supplier relationships—Part3: Guidelines for information and communication technology supply chain security

[7] NIST SP800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations

电信终端产业协会团体标准

网络产品供应链安全要求　制造要求

T/TAF 133—2022

*

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：82052809
电子版发行网址：www.taf.org.cn