ICS 33.050
CCS M 30

团　体　标　准

T/TAF 102-2021

面向工业互联网的物联网智能终端安全技术要求

Security technical requirements of Internet of Things intelligent terminal for industrial Internet

2021-12-13 发布　　2021-12-13 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：百度在线网络技术（北京）有限公司、中国信息通信研究院、郑州信大捷安信息技术股份有限公司、联想（北京）有限公司、高通无线通信技术(中国)有限公司、四川长虹电子控股集团有限公司、北京豆荚科技有限公司。

本文件主要起草人：王海棠、唐佳伟、郭建领、国炜、袁琦、徐晓娜、刘献伦、刘为华、康亮、李汝鑫、林巍巍、王江胜、唐博、谭源泉、黄德俊、杨子光、刘涛、窦丽娟。

引　　言

物联网飞速发展，安全作为一个进阶需求在物联网初期并没有被各大平台所重视，随着物联网的发展以及物联网 DDOS 等安全问题的爆发，用户、设备厂商、物联网平台也越来越重视物联网的安全。物联网场景比较复杂，在整个物联网生态中，大概分为设备端、云端、移动端三个部分，每个部分的对安全的侧重都不相同。设备端情况更加复杂，物理网的设备多种多样，设备的硬件、系统、应用、协议以及使用的库也碎片化严重，很难说有一个方案能够解决所有问题。

工业物联网智能终端是物联网信息系统的重要组成部分,其在应用中安全防护水平参差不齐,直接影响了物联网信息系统的整体安全。与一般信息系统相比,物联网信息系统中使用的智能终端具有数量众多、种类繁杂、分布区域广、部署环境多样、安全功能受限等特点,这些特点使得智能终端应用面临软硬件故障、物理攻击、通信不正常、信息泄露或篡改、非授权访问或恶意控制等安全风险。为了提高物联网信息系统中智能终端应用的安全防护水平,建议开展工业物联网智能终端安全技术要求立项。

面向工业互联网的物联网智能终端安全技术要求

1 范围

本文件规定了面向工业互联网的物联网智能终端设备安全技术要求，包括系统安全、硬件安全、固件安全、通信安全、数据安全等。

本文件适用于工业互联网物联网智能终端设备，个别条款不适用于特殊行业、专业应用，其他类似设备也可参考使用。

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 35273-2020 信息安全技术 个人信息安全规范

T/TAF 062-2020 物联网设备安全平台技术要求和分级方法

T/TAF 072-2020 物联网设备统一编码方法

3 术语和定义

GB/T 35273-2020、T/TAF 062-2020、T/TAF 072-2020界定的以及下列术语和定义适用于本文件。

3.1

物联网智能终端 Internet of Things smart terminals

具有数据采集，存储能力、计算能力等，可通过接口与平台建立通信连接，应用于物联网的嵌入式计算机系统设备。

3.2

算法模型 algorithm model

采用机器学习技术理论求解问题，明确界定的有限且有序的规则集合，并基于输入数据生成分类、推理、预测等的算法。

3.3

鲁棒性 Robustness

计算机控制系统正确执行以及处理意外终止和意外操作的能力。

4 缩略语

下列缩略语适用于本文件：

API：应用程序接口（Application Programming Interface）

TEE：可信执行环境（Trusted Execution Environment）
URL：统一资源定位系统（Uniform Resource Locator）

5 工业互联网物联网智能终端安全要求

5.1 通用安全要求

智能终端设备依据自身在身份标识与鉴别、硬件、操作系统、固件、通信、模型算法、数据等安全能力提出要求，涉及物联网设备安全平台相关要求应符合 T/TAF 062-2020 的相关规定。

a) 具备与平台双向认证能力，实现基于硬件的数字证书机制，宜采用国产商用密码算法；
b) 应支持安全芯片或同等安全能力的安全单元，为系统提供独立的安全服务。对采用安全芯片的，应满足 GM/T 0008 安全等级 2 级及以上要求，且应具备商用密码产品认证证书；
c) 具备操作系统安全，应采用可信计算等技术，保证系统安全，内部程序采用白名单机制；
d) 智能终端应可支持物理隔离安全性、芯片级防篡改保护机制并具备可抵御芯片级攻击能力，可在物理设备层被攻破的情况下仍然保障密钥的安全性。

5.2 硬件安全要求

硬件安全应符合下列要求：

a) 对于具有控制台接口的设备，需配置用户名、口令等方式进行认证授权，禁止未授权访问；
b) 对具备USB接口的设备，应默认关闭USB调试接口功能，或者增加调试接口验证功能；
c) 应禁用不再使用的物理接口，宜移除相关物理接口；
d) 智能终端设备应支持硬件安全隔离功能。

5.3 固件安全要求

固件安全应符合下列要求：

a) 智能终端固件及对固件的任何改动都应经过严格的流程控制和验证，以保证固件中不含隐藏的非法功能；
b) 智能终端上电时应对固件做真实性、完整性校验，确保固件未被非法篡改。
c) 固件升级时，应对新版固件进行签名验签，保证新版固件的合法性；
d) 应具备固件芯片的物理写入保护的功能，防止固件被恶意篡改。

5.4 操作系统安全要求

操作系统安全应符合下列要求：

a) 应提供安全启动机制进行系统的完整性保护，当安全验证通过后，系统方能正常启动，并进行定期的检查校验；
b) 系统应具备对远程控制的请求身份验证和接入认证的能力，避免非法用户或应用控制系统；
c) 系统应具有有防回滚策略，防止系统被恶意降级；
d) 系统应最小化开放网络服务，如端口23的telnet，端口80的http等；
e) 应禁止预留任何的未公开帐号，所有帐号应可被系统管理，并在资料中提供所有帐号及管理操作说明；
f) 对于任何的外界输入，系统应做充分的参数检查，防止非法输入或非法报文攻击；
g) 系统在应用安装时应获得授权同意，禁止安装未知来源或未授权应用。应用安装时，权限分配采取授权最小化原则，系统应能禁止所有未被允许权限的使用；

h) 应禁止存在绕过正常认证机制直接进入到系统的隐秘通道，包括不限于：组合键、特殊敲击、连接特定接口、使用特殊URL等；
i) 对于支持多个用户账号的系统，用户权限分配应遵循最小权限原则，普通用户只拥有系统赋予的最小权限，禁止越权操作，禁止使用弱密码进行登录；
j) 智能终端设备的操作系统宜能够实现用户、进程空间和数据安全隔离；
k) 对具备调试功能的设备，应限制调试进程在操作系统中的访问权限和操作权限，防止权限设置过高导致权限滥用。

5.5 通信安全要求

智能终端设备与业务平台之间通信连接安全包括网络接入安全，接口安全，数据传输安全等应符合以下要求：

a) 通信会话建立前应有安全的接入认证机制；
b) 传输敏感数据时的加密密钥禁止硬编码在代码中；
c) 通信会话应支持加密、完整性保护及防重放攻击，建议使用TLS/DTLS/TLCP等安全通信协议；
d) 会话服务端应对客户端的请求进行合法性校验，应校验会话标识、及会话标识是否与用户IP匹配；
e) 通信会话标识应使用安全随机数算法生成；
f) 禁止在URL、错误信息或日志中暴露会话标识符；
g) 所有登录后才能访问的界面都应提供主动退出选项，当用户退出时，设备端应断开会话连接；
h) 应设置会话超时机制，在超时过后需断开会话连接。

5.6 加密安全要求

加密安全应符合下列要求：

a) 智能终端应支持密钥的生成、分发、存储、更新等密钥管理功能。根密钥应采用安全的密码算法；
b) 应保证每个设备具有唯一的设备根密钥，且设备根密钥与智能终端身份识别信息一一绑定。智能终端认证过程中禁止明文传递密钥或以弱算法等变换后传递，防止反向推出密钥，保证认证安全。

5.7 身份标识与鉴别安全要求

身份标识与鉴别安全应符合下列要求：

a) 智能终端应具有唯一的终端身份识别信息，身份识别信息应不可篡改、不可伪造、具备全球唯一性且由平台进行统一管理；
b) 智能终端身份识别信息应与终端设备信息进行关联，如设备厂商代码、设备型号代码、唯一标识代码、身份识别服务规范版本号等，具体身份识别信息格式应符合T/TAF 072-2020的相关规定。

5.8 模型算法安全要求

对于具备算法模型的智能终端应符合以下安全要求：

a) 模型算法宜具备抵抗对抗性攻击的能力，如对抗样本攻击等；
b) 应对算法模型进行安全保护，以保护模型不被非法窃取，如为模型参数或预测API接口设置一定的访问控制机制，使之不可被公开获取。算法模型可被限制在TEE加载和运行，保护隐私数据不被非法获取。

5.9 数据安全要求

5.9.1 数据生命周期安全

数据生命周期分为数据采集、数据存储、数据传输、数据使用和数据销毁。在每个阶段都需要特定的安全措施来保护数据安全。

涉及个人信息相关活动应符合GB/T 35273-2020的相关规定。

5.9.2 数据采集安全要求

a) 应保证信息收集主体的所有行为的合法要求，包括信息主体的授权和法律责任的明确；
b) 数据采集应遵循最小化原则，禁止过度收集与业务无关的数据；
c) 应保证用户拥有充分的知情权；
d) 应通过技术手段保障用户的数据访问权、删除权、纠正权和迁移权。

5.9.3 数据存储安全要求

a) 应对文件数据采用加密技术实现文件的存储保密性；
b) 应对敏感信息，如隐私信息，除了保证存储保密性，还需要在此之前完成脱敏。

5.9.4 数据传输安全要求

a) 应保证使用安全的加密保护用户数据；
b) 应保证用户数据在不影响业务使用的情况下脱敏后传输；
c) 应保证安全可靠的密钥管理方式，采取完整的密钥全生命周期的管理，包括创建、激活、禁用、转换、分发、备份、销毁等，同时基于密钥的数据加密存储；
d) 应保证使用动态密钥或设备唯一密钥，保障设备安全；
e) 应保证数据完整性校验，对数据包的所有内容进行签名。

5.9.5 数据使用安全要求

a) 应禁止未授权访问和非法使用用户个人信息；
b) 应保证权限控制，数据上传下载时，限制用户向上跨目录访问，只能访问指定目录下的文件。

5.9.6 数据销毁安全要求

a) 应能够提供手段协助清除因数据在不同存储设备间迁移、业务终止、自然灾害、合同终止等遗留的数据，对日志的留存期限应符合国家有关规定；
b) 应提供手段清除数据的所有副本。

附 录 A
（资料性）
工业互联网物联网智能终端安全能力分级

根据工业互联网物联网智能终端支持的安全能力程度，将工业互联网物联网智能终端的安全能力自高到低划分为5个等级。在每一等级定义了对应的安全能力的最小集合，也就是工业互联网物联网智能终端必须支持该集合中的所有安全能力才能标识为该级别，例如达到第五级的智能终端应支持本文件第5章所定义的所有安全能力。具体的等级划分详见表A.1.

表 A.1 工业互联网物联网智能终端安全能力分级

安全能力		安全能力等级				
		一级	二级	三级	四级	五级
智能终端设备安全要求	a）	√	√	√	√	√
	b）	-	√	√	√	√
	c）	-	-	√	√	√
	d）	-	-	-	-	√
身份认证安全要求	a）	√	√	√	√	√
	b）	-	√	√	√	√
	c）	-	-	√	√	√
	d）	-	-	-	-	√
硬件安全要求	a）	√	√	√	√	√
	b）	-	√	√	√	√
	c）	-	-	√	√	√
	d）	-	-	-	√	√
	e）	-	-	-		√
智能终端设备操作系统安全要求	a）	√	√	√	√	√
	b）	√	√	√	√	√
	c）	-	√	√	√	√
	d）	-	√	√	√	√
	e）	-	-	√	√	√
	f）	-	-	√	√	√
	g）	-	-	-	√	√
	h）	-	-	-	√	√
	i）	-	-	-	-	√
	j）	-	-	-	-	√
	k）	-	-	-	-	√
固件安全要求	a）	√	√	√	√	√
	b）	-	-	√	√	√
	c）	-	-	-	-	√

表 A.1　工业互联网物联网智能终端安全能力分级（续）

安全能力		安全能力等级				
		一级	二级	三级	四级	五级
通信安全要求	a）	√	√	√	√	√
	b）	√	√	√	√	√
	c）	–	√	√	√	√
	d）	–	–	√	√	√
	c）	–	–	–	√	√
	d）	–	–	–	√	√
	e)	–	–	–	–	√
	h）	–	–	–	–	√
模型算法安全要求	a）	√	√	√	√	√
	b）			√	√	√
数据采集安全要求	a）	√	√	√	√	√
	b）	–	√	√	√	√
	c）	–	–	√	√	√
	d）	–	–	–	√	√
	e）	–	–	–	–	√
数据传输安全要求	a）	√	√	√	√	√
	b）	–	√	√	√	√
	c）	–	–	√	√	√
	d）	–	–	–	√	√
	e）	–	–	–	–	√
数据使用安全要求	a）	√	√	√	√	√
	b）	–	–	√	√	√
数据存储安全要求	a）	–	√	√	√	√
	b）	–	–	√	√	√
数据销毁安全要求	a）	–	√	√	√	√
	b）	–	–	√	√	√

附 录 B
（资料性）
安全能力等级建议

工业互联网通用型典型场景有协同研发设计、远程设备操控、协同作业、辅助装配、智能质检、设备故障诊断、智能物流、智能巡检、智能监测等。相关领先行业应用实践包括电子设备制造业、装备制造业、钢铁行业、采矿行业、电力行业、农业。附表 B.1 提供了分场景的安全级别建议。

表 B.1 工业互联网物联网智能终端分场景安全级别建议

工业互联网行业	应用场景	建议级别
电子设备制造业	远程设备操控	三级及以上
	协同研发设计	三级及以上
	现场辅助装配	四级
	机器视觉质检	四级
	设备故障诊断	三级
装备制造业	远程设备操控	三级及以上
	现场辅助装配	四级
	机器视觉质检	四级
	设备故障诊断	三级
钢铁行业	智能废钢判定系统	三级及以上
	智能点检	三级
	智慧天车	四级
	安全生产	五级
采矿行业	远程设备操控	四级及以上
	安全生产	五级
电力行业	智能巡检	五级
	智能检测	四级
农业	远程设备操控	三级
	农作物监测	三级
	智慧分拣	三级
交通	自动驾驶	五级

电信终端产业协会团体标准

面向工业互联网的物联网智能终端安全技术要求

T/TAF 102-2021

*

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