

团 标 准

T/ZSA XXXX—XXXX

移动终端快速充电适配器安全技术要求和 测试方法

Security Technical Requirements and Test Methods for Fast Charging Adapters of
Mobile Terminals

征求意见稿

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX - XX - XX 发布

XXXX - XX - XX 实施

中关村标准化协会 发布

目 次

前 言	II
引 言	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	2
5 快速充电适配器架构	2
6 技术要求	3
6.1 线缆安全	3
6.2 硬件芯片安全	3
6.3 固件安全	3
6.4 快速充电协议安全	4
6.5 异常处理	4
7 安全保障要求	4
8 技术测试试验方法	4
8.1 试验要求	4
8.2 线缆安全测试	4
8.3 硬件芯片安全测试	5
8.4 固件安全测试	5
8.5 快速充电协议安全测试	6
8.6 异常处理测试	7
9 安全保障要求测试	7
9.1 测试方法	7
9.2 预期效果	7
9.3 结果判定	7
附录 A	8

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。

本文件由中关村标准化协会技术委员会提出并归口。

本文件起草单位：联想（北京）有限公司、北京市闪联信息产业协会、深圳市航嘉驰源电气股份有限公司、康舒电子（东莞）有限公司、台达电子企业管理（上海）有限公司、北京百度网讯科技有限公司、群光电能科技股份有限公司、立讯精密工业股份有限公司、英集芯科技股份有限公司、深圳慧能泰半导体科技有限公司、南京博兰得（Powerland）电子科技有限公司。

本文件主要起草人：尘兴灿、李汝鑫、曹坤鹏、娄长永、耿晶鑫、蒋青喆、何丙阳、李捷、彭峰、欧应阳、关明、赵如、孙志勇、陶宏芝、林巍巍、谢军、罗斌、张海涛、黄硕国、侯晶晶、王志强、伍金铨、谢仁践、陈伟、黄镇华、王薇、邱阳、丁帮杰、胡冰涛、刘耀武。

引　　言

在移动终端的普及和广泛运用的背景下，各种新型应用程序的出现并伴随其使用频率的增长，使得移动终端的耗电量陡增。因此，为了缓解消费者对于移动终端的电量焦虑，快速充电技术应运而生。

由于快速充电技术发展迅速，市场前景广阔，所以生产制造快速充电适配器的厂商数量众多，快速充电适配器的市场占有率也大幅提升。同时，在行业内部，也制定了与快速充电技术相关的部分标准。但快速充电适配器作为一种高功率、大电压的供电设备，本身的安全问题常常被忽略，而且目前没有统一的安全技术要求和规范去保障其安全。

本标准聚焦快速充电适配器的安全问题，从产品安全角度出发，深度挖掘快速充电适配器面临的安全风险，将风险消减措施转换为安全技术要求，提出适用于快速充电适配器安全发展和应用的标准化方案，以起到引导行业安全发展的目的。

移动终端快速充电适配器安全技术要求和测试方法

1 范围

本文件规定了移动终端快速充电适配器（以下简称“适配器”）的安全技术要求和测试方法，包括线缆安全、硬件芯片安全、固件安全、快充协议安全、异常处理和安全保障要求的技术要求和测试方法。

本文件适用于研发、生产、制造移动终端快速充电适配器的厂商和研究机构。

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。

YD/T 1591 移动通信终端电源适配器及充电/数据接口技术要求和测试方法

YD/T 3815—2021 移动通信终端快速充电技术要求和测试方法

T/TAF 083—2021 移动终端融合快速充电技术规范

3 术语和定义

下列术语和定义适用于本文件。

3.1 快速充电模式 fast charging mode

在常温（ $23\pm2^{\circ}\text{C}$ ）条件下，一个由快速充电适配器、线缆和快速充电终端（以下简称“终端”）组成的充电系统，从初始充电状态开始，至充电30min，通过提高适配器的输出电压或输出电流，实现进入电池的平均电流大于等于3A或总充电量大于等于电池额定容量的60%的充电方式。

3.2 初始充电状态 initial charging status

在常温（ $23\pm2^{\circ}\text{C}$ ）条件下，终端耗电至自动关机，静置30min，再次接入充电回路的瞬间状态。

3.3 普通充电模式 normal charging mode

在常温（ $23\pm2^{\circ}\text{C}$ ）条件下，适配器额定输出电压为5V，额定输出电流小于等于3A的充电模式，在此模式下适配器输出端口D+和D-短路。

3.4 快速充电适配器 fast charging adapter

能够兼容普通充电模式和快速充电模式的电源适配器。
3.5 快速充电终端 fast charging terminal
具有快速充电管理功能，能够兼容普通充电模式和快速充电模式的终端。

3.6 快速充电系统 fast charging system

包含快速充电适配器、线缆及快速充电终端（含快充电池），并能够在快速充电模式下进行充电的系统。
3.7 线缆 cable

用于连接快速充电适配器和快速充电终端。线缆的两端接口，可以都是USB Type-C接口，可以一端是USB Type-A接口，另一端是USB Type-C接口；也可以是其它的标准USB接口组合。线缆至少要支持VBUS、D+、D-、GND四根信号线。如果线缆要支持大功率充电模式，还需集成线缆电子标签。

3.8

线缆电子标签 cable electronic marker

可以读取该线缆的属性：电源传输能力、数据传输能力、ID等信息的芯片。

3.9

快速充电协议 fast charging protocol

用于快速充电适配器与快速充电终端之间进行充电电压、充电电流协商的协议。常见的快速充电协议有USB PD协议、QC协议、VOOC协议、SCP协议等。

3.10

安全漏洞 security vulnerability

硬件、软件、协议的具体实现或系统安全策略上存在的缺陷，从而可以使攻击者能够在未授权的情况下访问或破坏系统。

4 缩略语

下列缩略语适用于本文件。

CRC	循环冗余校验	Cyclic Redundancy Check
D+	高电平数据线	Data+
D-	低电平数据线	Data-
E-Marker	线缆电子标签	Cable Electronic Marker
GND	地（电源负极）	Ground
JTAG	联合测试工作组	Joint Test Action Group
PD	供电协议	Power Delivery
QC	快速充电	Quick Charge
SCP	超级充电协议	Super Charge Protocol
SHA128	安全哈希标准128	Secure Hash Standard 128
SHA256	安全哈希标准256	Secure Hash Standard 256
SWD	串行调试	Serial Wire Debug
UART	通用异步收发传输器	Universal Asynchronous Receiver/Transmitter
USB	通用串行总线	Universal Serial Bus
USB Type-A	通用串行总线A型	Universal Serial Type-A
USB Type-C	通用串行总线C型	Universal Serial Bus Type-C
VBUS	总线电压（电源正极）	Voltage Bus
VOOC	开电压环，分段恒流充电	Voltage Open-Looped, Multi-Step Constant-Current Charging

5 快速充电适配器架构

快速充电系统由快速充电适配器、线缆和快速充电终端组成，快速充电适配器主要包括快充协议芯片、主控芯片和功率电路。适配器通过线缆与终端进行通信，适配器基于快充协议判断终端是否支持快速充电并确定其快速充电模式，由适配器的主控芯片控制功率电路产生相应的电压、电流对终端进行充电。

具体的组成框图如图1所示。

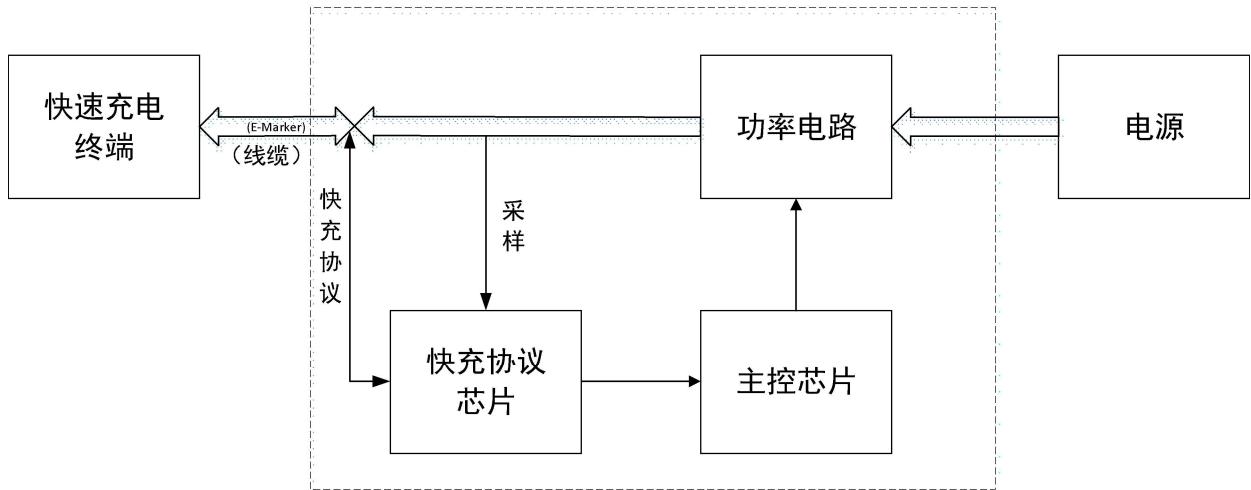


图1 快速充电适配器架构图

6 技术要求

6.1 线缆安全

普通线缆可不包含芯片，若包含，除线缆电子标签等必要芯片外，不应存在其他芯片。

6.2 硬件芯片安全

6.2.1 调试接口

适配器调试接口的要求如下：

- 宜默认关闭和移除，如：UART、JTAG、SWD、USB等调试接口。
- 若需保留必要调试接口，调试接口应具备访问控制功能。

6.2.2 访问控制

- 适配器应对一切访问行为进行权限控制，并合理分配权限。

b) 调试接口应具备防止暴力破解的安全访问控制措施，如密码连续输入错误5次及以上，应拒绝访问请求。

6.2.3 芯片安全

适配器芯片应具备安全的设计实现，应能抵抗常见故障注入攻击方式，如电磁故障注入、电压故障注入、激光故障注入等。

6.3 固件安全

6.3.1 读写保护

适配器的主控芯片、快充协议芯片等含有固件的芯片应开启读/写保护，防止非法修改固件。

6.3.2 固件升级安全

对于支持固件升级的适配器，在固件升级时，应符合以下要求：

- 在适配器固件升级的过程中，应停止给终端充电，以确保充电安全，升级成功后重新协商充电状态。
- 应校验升级包的完整性和保密性，如：签名证书校验、SHA128/256校验、CRC校验等，并拒绝非法的固件升级包。
- 固件传输通道应具有安全的实现，包括但不限于加密数据传输通道，双向鉴权等。

6.3.3 安全漏洞

适配器的固件中不应存在已知漏洞，不应存在后门逻辑和未激活代码。

6.4 快速充电协议安全

使用快充协议的适配器符合以下要求来保障协议的安全性：

- a) 使用PD、QC等行业协议，应遵守该协议的协议栈，应符合行业协议认证要求。
- b) 使用VOOC、SCP等厂商协议，应遵守该协议的协议栈，应符合厂商协议认证要求。

6.5 异常处理

具有电压、电流、功率、数据等异常监测和处理能力的适配器要求如下：

- a) 适配器异常状态包括但不限于，适配器工作在快速充电模式时，实际输出的电压、电流、功率与通过快速充电协议协商的额定值的差值超过 $\pm 5\%$ ；适配器与终端通信失败等。
- b) 适配器处于异常状态时应停止快速充电，并重新发起快速充电协议协商过程。

7 安全保障要求

适配器提供者应满足以下安全保障要求：

- a) 建立产品开发安全管理流程，包括但不限于威胁建模、源代码扫描、黑/白盒测试、开源安全等。
- b) 授权使用开发、测试、维修工具，并将其纳入资产安全管理体系。
- c) 具备安全应急响应能力，在产品生命周期内为用户提供安全补丁。

8 技术测试试验方法

8.1 试验要求

8.1.1 试验环境条件

除特殊规定外，所有测试应在下列正常条件下进行：

环境温度：15°C~35°C

相对湿度：25%~75%

对适配器测试时，应将线缆可靠连接在终端上。对于任何可能会引起燃烧、爆炸的实验环节，应在防爆环境下进行。

8.1.2 试验设备条件

试验设备条件如图2所示。

安全测试工具串联在适配器和终端之间，用于监控适配器与终端之间快充协议、电压、电流等数据。

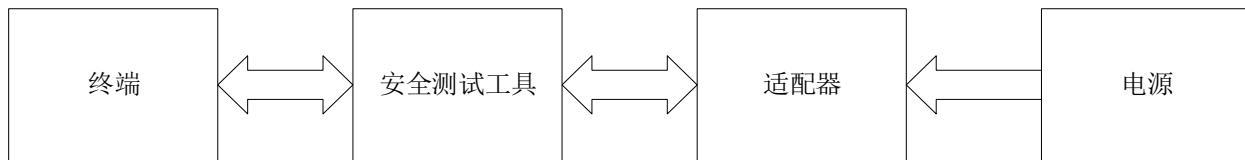


图2 试验设备条件

8.2 线缆安全测试

8.2.1 测试方法

首先测试线缆是否可以正常使用，使用安全测试工具（如USB测试仪、逻辑分析仪等）测试线缆中是否存在芯片，若存在，确实是否为线缆电子标签等必要芯片，必要时可以拆解线缆。

8.2.2 预期效果及判定

线缆中不含有芯片或只含有线缆电子标签等必要芯片。

8.2.3 结果判定

满足上述预期效果则判定为符合，否则为不符合。

8.3 硬件芯片安全测试

8.3.1 调试接口测试

8.3.1.1 测试方法

拆解适配器，检测设备硬件电路上是否存在暴露的调试接口，如UART、SWD、JTAG等，如果存在调试接口，测试是否可以未授权访问。

8.3.1.2 预期效果

设备上不存在暴露的调试接口，或存在需要厂商提供口令才可以访问的调试接口。

8.3.1.3 结果判定

满足上述预期效果则判定为符合，否则为不符合。

8.3.2 访问控制测试

8.3.2.1 测试方法

如果适配器存在暴露的调试接口，使用测试工具，如串口调试工具，JTAG调试器、烧录器等，连接调试接口，测试是否可以直接进行调试，是否需要权限认证，对于需要权限认证的，尝试暴力破解其口令。

8.3.2.2 预期效果

设备上的调试接口无法直接调试，对于访问时需要权限验证的，在连续输入错误口令5次及以上，设备直接拒绝访问请求。

8.3.2.3 结果判定

满足上述预期效果则判定为符合，否则为不符合。

8.3.3 芯片安全测试

8.3.3.1 测试方法

在适配器正常工作时，使用电磁故障注入工具、电压故障注入工具、激光故障注入工具对适配器中的功能芯片进行测试，监测适配器工作状态，是否能够造成芯片运行异常，扰乱正常运行逻辑等。

8.3.3.2 预期效果

故障注入不影响芯片的正常运行。

8.3.3.3 结果判定

满足上述预期效果则判定为符合，否则为不符合。

8.4 固件安全测试

8.4.1 读写保护测试

8.4.1.1 测试方法

使用烧录器或其他编程工具尝试读取快充协议芯片、主控芯片的固件，检测是否存在固件读写保护。

8.4.1.2 预期效果

无法直接读取芯片中的固件，或需要身份认证才可以读取固件。

8.4.1.3 结果判定

满足上述预期效果则判定为符合，否则为不符合。

8.4.2 固件升级校验测试

8.4.2.1 测试方法

如果适配器支持固件升级功能，在适配器正常充电时，进行固件升级，测试在升级过程中是否对终端终止充电；修改正常升级包，并尝试使用被修改的升级包进行升级，测试适配器是否接受该升级包；如果升级包采用网络传输，检查是否加密传输，是否可以劫持、修改升级包。

8.4.2.2 预期效果

在固件升级过程中，适配器终止对终端充电；设备无法使用被修改的升级包进行升级；升级包采用加密的网络传输。

8.4.2.3 结果判定

满足上述预期效果则判定为符合，否则为不符合。

8.4.3 安全漏洞测试

8.4.3.1 测试方法

根据设备的固件类型进行黑盒测试、源代码审计，检查固件中是否存在已知漏洞，是否存在其他漏洞，如栈溢出、未激活代码、后门功能等。

8.4.3.2 预期效果

固件中不存在已知漏洞，也不存在其他安全漏洞。

8.4.3.3 结果判定

满足上述预期效果则判定为符合，否则为不符合。

8.5 快速充电协议安全测试

8.5.1 行业协议

8.5.1.1 测试方法

按照行业协议的安全测试方法进行安全测试或查看适配器提供商提交的安全认证报告。

8.5.1.2 预期效果

适配器的快充协议实现满足行业协议的安全测试要求。

8.5.1.3 结果判定

满足上述预期效果则判定为符合，否则为不符合。

8.5.2 厂商协议

8.5.2.1 测试方法

按照厂商协议的安全测试方法进行安全测试或查看适配器提供商提交的安全认证报告。

8.5.2.2 预期效果

适配器的快充协议实现满足厂商协议的安全测试要求。

8.5.2.3 结果判定

满足上述预期效果则判定为符合，否则为不符合。

8.6 异常处理测试

8.6.1 测试方法

按照测试环境连接适配器、安全测试工具（逻辑分析仪）和终端，监测适配器实际输出电压、电流与快速充电协议协商结果是否一致；在适配器与终端通过快速充电协议协商时，使用安全测试工具修改两者通信数据包内容，检测适配器是否重新发起协商；适配器与终端建立快速充电关系后，尝试使用修改适配器内部工作逻辑，使适配器输出与已协商的快速充电模式不一致的电压、电流，检测适配器的工作状态是否正常。

8.6.2 预期效果

适配器实际输出电压、电流与快速充电协议协商结果一致；适配器可以监测到快充充电协议协商过程中的数据包异常并重新发起协商；当适配器实际输出电压、电流与快速充电协议协商结果不一致时，适配器停止快速充电并重新发起快速充电协议协商。

8.6.3 结果判定

满足上述预期效果则判定为符合，否则为不符合。

9 安全保障要求测试

9.1 测试方法

厂商提供说明材料，说明适配器开发安全管理流程、资产安全管理体系以及安全应急响应方案。

9.2 预期效果

查看厂商提供的说明材料，确认是否对适配器在设计开发、资产管理和应急响应方面采取有效安全保障措施。

9.3 结果判定

满足上述预期效果则判定为符合，否则为不符合。

附录 A

(规范性附录) 试验用仪器和设备

A. 1 直流数字电压表

量程:0~100V;

精度:0.5级。

A. 2 直流数字电流表

量程:0~10A;

精度:0.5级。

A. 3 螺丝刀套件

A. 4 撬棒套件

A. 5 逻辑分析仪测试前准备

支持分析各种快充协议。

A. 6 固件烧录器

支持快充协议芯片和适配器主控芯片固件烧录。

A. 7 串口调试工具

A. 8 芯片调试器

JTAG, SWD, J-link等。

A. 9 芯片安全测试工具

电磁错误注入工具, 电压错误注入工具。