ICS 33.050
CCS M 30

# 团　体　标　准

T/TAF 143—2023

# 面向实时操作系统智能应用开发的通用技术要求

General requirements for smart application development based on real time operation system

2023-02-08 发布　　2023-02-08 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：蚂蚁科技集团股份有限公司、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、阿里巴巴(中国)有限公司。

本文件主要起草人：孟飞、林冠辰、曾晨曦、沈军强、彭晋、李军汲、戈志勇、马霁阳、刘献伦、刘为华、崔晓夏、黄天宁。

# 面向实时操作系统智能应用开发的通用技术要求

## 1 范围

本文件规定了面向实时操作系统智能应用开发的通用技术框架、功能要求、技术要求和安全要求。

本文件适用于面向实时操作系统的通用应用开发活动。

## 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 062-2020 物联网设备安全平台技术要求和分级方法

## 3 术语和定义

下列术语和定义适用于本文件。

3.1

**轻应用 light applications**

一种在实时操作系统上运行的，通过实时操作系统提供的接口，实现某项或某几项特定功能的免安装的应用软件。

3.2

**小程序 mini application**

一种在应用软件上运行的，通过应用软件提供的接口，实现某项或某几项特定功能的免安装的应用软件。

**示例：**用户通过扫一扫或者搜索即可打开应用。

## 4 缩略语

下列缩略语适用于本文件。

API：应用程序接口（Application Interface）

POSIX：可移植操作系统接口（Portable Operating System Interface）

RTOS：实时操作系统（Real Time Operation System）

## 5 通用技术架构

通用技术架构见图1。本架构图主要从应用视角出发，屏蔽不同类型的硬件、不同系统带来的碎片化适配问题，并抽象出常用的系统模块作为中间层，方便应用开发者在不必感知底层硬件和系统差异，进行应用开发。

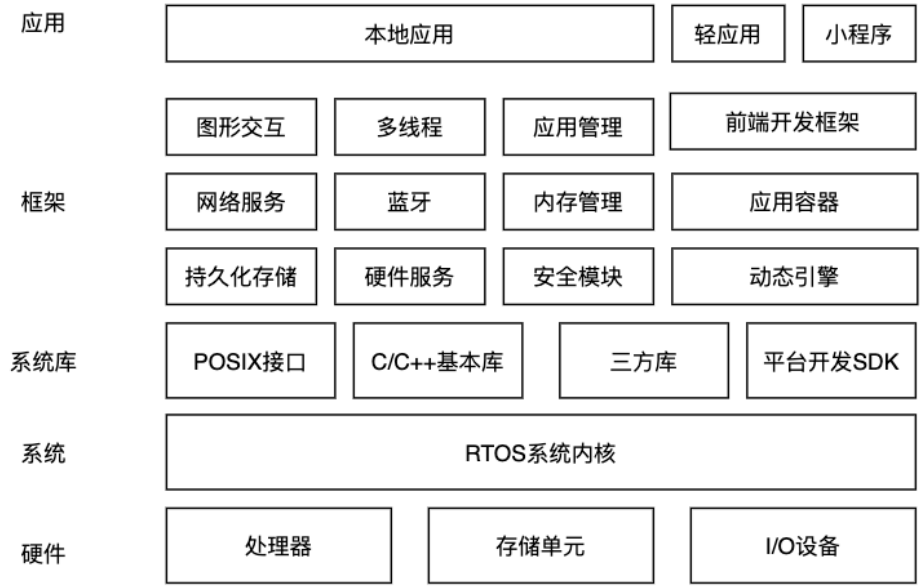


图1　通用技术架构

通用技术架构自上而下可以划分为如下几个层次：

a) 应用，主要为基于 RTOS 系统和框架开发的应用程序，包括本地应用、轻应用和小程序等；
b) 框架，框架层由各种通用的功能单元组成，提供各种应用所需的能力，包括图形交互、多线程编程、应用管理、前端开发框架、网络服务、蓝牙、内存管理、应用容器、持久化存储、硬件服务、安全模块、动态引擎等；
c) 系统库，系统库主要通过标准接口形式提供应用开发者所需的各类能力，包括 C/C++基础库、三方库、平台开发 SDK 等；
d) 系统，为 RTOS 操作系统层，主要为 RTOS 系统内核；
e) 硬件，包括处理器、存储单元，I/O 设备等。

## 6　功能要求

### 6.1　系统库功能

为屏蔽平台相关的差异性，增加上层模块的可移植性，宜引入业界广泛应用的接口标准，如POSIX和C/C++的基本库，对于上述标准无法覆盖的设备特有的能力，再以平台SDK的方式进行扩展。

### 6.2　框架功能

在系统库基础上，应进一步封装平台无关和平台相关的底层能力，以对开发者更友好的方式进行提供相关能力，具体框架功能应包括如下：

a) 图形交互，主要为完成图形接口编程的功能；
b) 多线程，支持平台无关的多任务开发模型；

c) 应用管理，主要针对应用安装、更新、删除以及授权和访问控制等机制；
d) 前端开发框架，提供便捷的前端开发环境；
e) 网络服务，主要解决设备通过 wifi/蜂窝网络以及设备代理网络等基础联网能力；
f) 蓝牙，提供统一的蓝牙服务功能；
g) 内存管理，提供高效安全的内存申请、释放以及监控利用等功能；
h) 应用容器，为动态应用(javascript 快应用、小程序等)提供运行时环境；
i) 持久化存储，主要解决应用在设备上永久存储数据的需求，可分为安全存储和普通存储；
j) 硬件服务，针对设备硬件(如相机、传感器等)外设做操作的统一服务；
k) 安全模块，提供包括加解密、设备认证(本地认证、远程认证)、可信根管理等基础能力；
l) 动态引擎，保障应用运行的性能。

## 7 技术要求

### 7.1 图形开发框架

要求如下：
a) 应具备较好的可移植性，可满足在不同硬件平台和底层系统上快速移植适配；
b) 应具备完备的多窗口机制和消息传递机制；
c) 可升缩性强，轻量，占用资源少，可支持在低端设备上运行；
d) 框架应高性能，高可靠；
e) 框架可灵活嫁接到现有较流行的 GUI 开发框架之上。

### 7.2 多线程

应提供平台无关的多线程开发模型，包括线程生命周期管理，信号量、互斥锁等原语，以及任务间通信机制。

### 7.3 应用管理

提供对系统中本地应用、轻应用、小程序等各类型应用程序管理功能，包括安装、升级、卸载、授权、访问控制等。

可支持应用的三方开发者自助开发、发布应用，并且由用户进行安装和增量升级。

### 7.4 网络服务

#### 7.4.1 概述

提供设备对远程服务访问的统一通道，屏蔽掉底层wifi、蜂窝以及ip over bluetooth等代理联网方案的底层差异性，应用开发者可以使用统一编程接口进行网络访问。

#### 7.4.2 sockets API

应兼容sockets API，API字段及描述示例见表1。

表1 sockets API示例

| 字段 | 描述 |
| --- | --- |
| socket | 分配一个套接字，用于后续的读取和写入数据。 |

表1　sockets API 示例（续）

| 字段 | 描述 |
| --- | --- |
| setsockopt | 设置套接字的属性。 |
| bind | 将套接字绑定到一个特定的端口上。 |
| listen | 向 TCP 注册一个在套接字上的的连接等待。 |
| connect | 客户端建立一个与服务端口的连接。 |
| accept | 服务端接受来自客户端的连接请求。 |
| send/sendto | 向连接的另一端发送数据。 |
| recv/recvfrom | 接受发送自另一端的数据。 |

### 7.4.3　网络服务要求

应符合如下要求：

a)　可重入和线程安全；

b)　支持 ARP、DHCP、DNS、 LLMNR、NBNS 等协议栈；

c)　支持 SSL、TLS 或 TLCP 通信模式。

## 7.5　蓝牙

蓝牙功能框架图如图2所示。

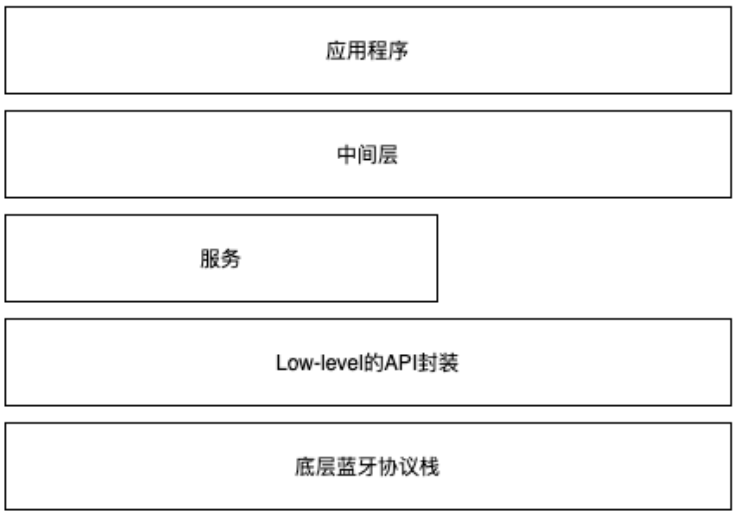


图2　蓝牙功能框架图

蓝牙功能主要要求如下：

a)　中间层：对底层 API 和服务的抽象，为上层应用提供更为友好访问底层蓝牙协议栈的接口。可以通过注册回调的方式来启用底层服务、广播等；

b)　服务层：提供 GAP/GATT 等基础配置服务。

## 7.6　持久化存储

应提供持久化存储能力，包括键值对存储和数据块存储，要求如下：

a)　应具备键值对存储：

1) 为应用提供快捷的数据访问接口，适合存储体积较小的内容；
2) 提供按应用隔离访问的机制；
3) 按应用和设备维度做透明加解密；
4) 可提供类似安卓 keystore 或 iOS keychain 的密钥数据生成、导入、导出和常用加解密算法操作；

b) 数据块存储：

应提供适合体积较大的普通数据的文件系统存储标准接口。

## 7.7 硬件服务

硬件服务框架如图3所示。现有的SoC中通常有较为丰富的传感器外设，而针对这类设备的驱动API则往往与特定平台相关，应用在调用这些外设时非常不便。应基于图2的蓝牙功能框架，通过搭建硬件服务接口层，为应用层提供统一编程接口。

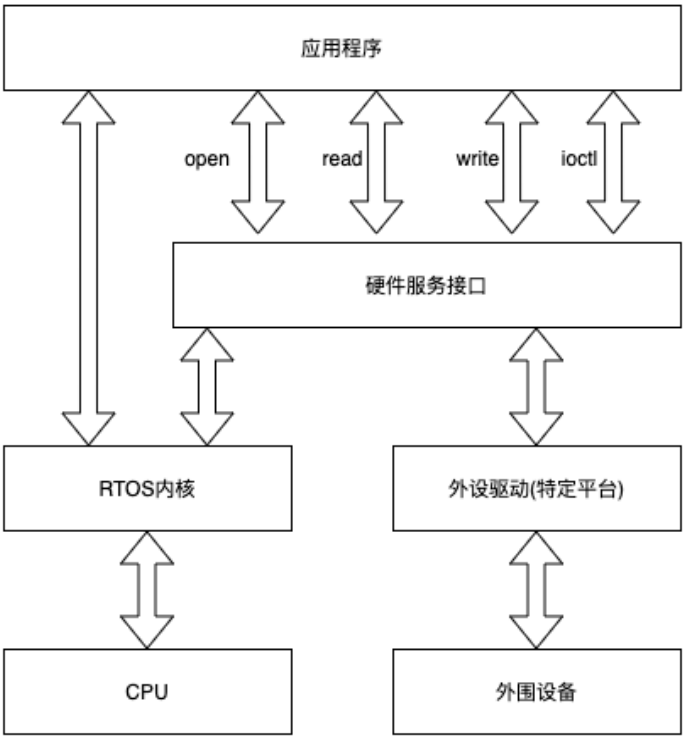


图3 硬件服务框架

# 8 安全要求

涉及到物联网设备相关的安全平台的安全功能要求，参照T/TAF 062-2020的安全隔离、安全启动、安全存储、密码算法和密钥、固件版本控制、安全生命周期、绑定、远程验证相关要求。针对高安全性要求的应用类，设备和系统侧还需要提供更高级别的安全机制，包括具备可信执行环境等。

**示例：**业界常见的可信执行环境方案如安全单元(SE)、TEE(arm-trustzone, intel SGX 等)以及其他基于虚拟化和内存隔离的应用执行环境等。

# 电信终端产业协会团体标准

# 面向实时操作系统智能应用开发的通用技术要求

T/TAF 143—2023

*



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