

---

# **ESC0830EVBT0.1 开发板使用手册**

**V0.2**

**紫金山实验室**

## 修订记录

[illegible]

---

# 目录

1. 目的与范围 .....	4
2. 芯片简介 .....	4
2.1. 开发板功能框图 .....	5
2.2. 开发板实物图 .....	5
3. 技术方案 .....	6
3.1. 拟态 MCU 开发板启动 .....	6
3.2. 拟态 MCU 芯片工作模式 .....	7
3.3. 烧录方法 .....	7
3.4. 三模启动 .....	8

---

## 图目录

图 2-1 拟态 MCU 芯片 .....	4
图 2-2 开发板系统框图 .....	5
图 2-3 拟态 MCU 开发板 .....	6
图 3-1 烧写软件图 .....	8
图 3-2 烧写软件图 .....	8

---

## 表目录

表 3-1 拟态 MCU 芯片功能切换引脚 .....	6
-----------------------------	---

---

## 1. 目的与范围

本文档规定了拟态 MCU 芯片的测试计划，规定了开发板的使用说明以及相应操作步骤。本文档适用 ESC0830EVBT0.1 开发板。

## 2. 芯片简介

嵌入式内生安全控制器芯片引入异构多核 CPU 架构，紧贴嵌入式控制与物联网场景。相关理论研究表明，在异构多核 CPU 架构下能够大大降低 MCU 被攻破概率，在很多场景下很大程度提升安全等级。主要实现外部环境与控制芯片之间的安全防护功能。通过内置 3 个异构执行体（CPU）实现 MCU 的拟态化（外界看到的是 1 个 CPU，而内部是由最多 3 个异构 CPU 共同执行），使得攻击者无法有效攻击 MCU，进而保证 MCU 的安全性。



图 2-1 拟态 MCU 芯片

嵌入式内生安全控制器芯片具备兼容市面主流 MCU 的 IO 及功能特性，具备多个异构微处理器内核及拟态负反馈控制器，可以实现多冗余度的拟态判决。具备适用于工业控制网络及边缘计算的外设子系统：集成 UART，I2C，SPI 等

MCU 的常用外部接口，集成 CAN 总线控制器；具备内嵌 EFlash、PLL、IO 等模拟 IP，支持传感器网络等应用场景。

系统采用异构 CPU 系统架构，包含三个相互独立的 CPU 子系统，每个 CPU

子系统包含 CPU 核、FlashMemoryinterfacemodule(FLITF) 及 Flashmemory(NORFlash)。三个异构 CPU 子系统分别采用 ARMCortex-M3、MIPSMicroAptivUC 及 RISC-VE906 等三种不同指令集架构的 CPU，搭配各自独立的内存(NORFLASH)，三套 CPU 子系统相互独立，保证物理隔绝，最大程度的实现安全。

## 2.1. 开发板功能框图

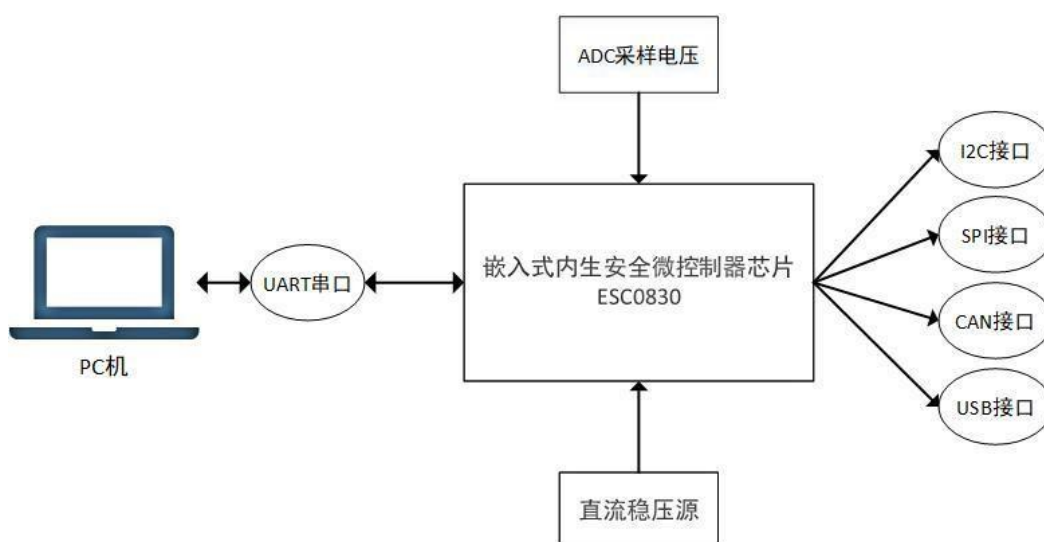


图 2-2 开发板系统框图

## 2.2. 开发板实物图

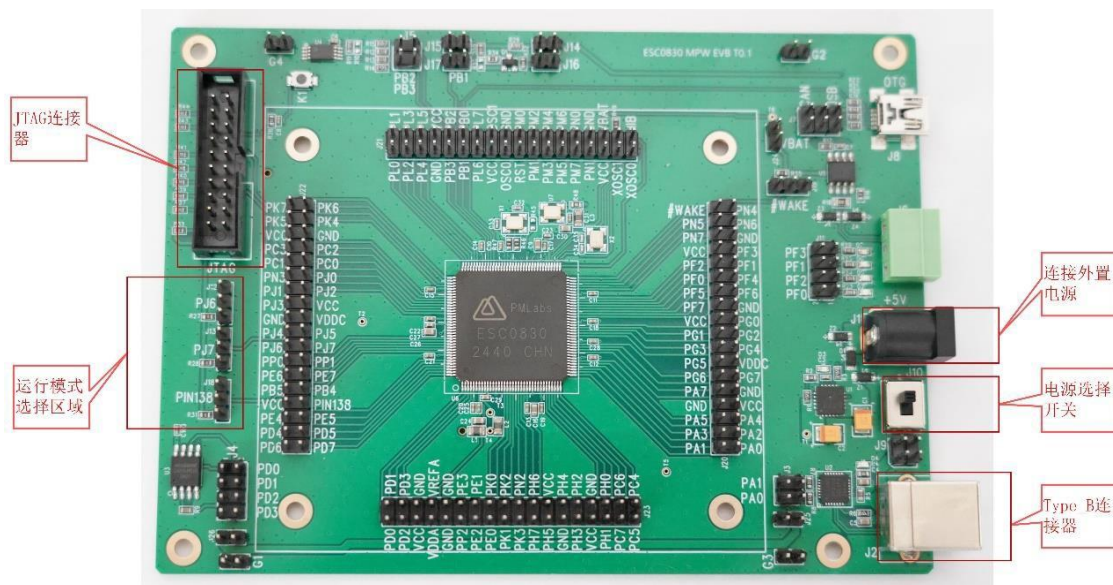


图 2-3 拟态 MCU 开发板

### 3. 技术方案

拟态 MCU 开发板为实现拟态 MCU 芯片而进行开发的测试板卡，开发板为拟态 MCU 芯片提供电源、串口外设和相应的控制电路。在烧写相应的程序之后，开发板可以实现拟态防御的相关功能，并实现与拟态 MCU 芯片的交互应用。

表 3-1 拟态 MCU 芯片功能切换引脚

信号	芯片复用 IO	开发板位置
test mode	管脚 138	J18
test sel0	管脚 129	J12
test sel1	管脚 130	J13

#### 3.1. 拟态 MCU 开发板启动

开发板兼容两种不同供电方式，分别为外置电源供电和 USB 供电。将板上开关 J10 至 USB 方向即为 USB 供电，此场景下只需连接 USB 串口线即可。将开关 J10 拨至电源连接器方向即为外置电源供电，此场景下需要连接外部电源，USB 串口线仅传输数据。开发板支持 CAN、USB、I2C、JTAG 等多种外设，相关接口通过插针连接。通过 J2 位置 Type\_B 类连接 PC 进行串口通信。



---

### 3.2. 拟态 MCU 芯片工作模式

开发板提供插针进行选择不同的启动模式，通过 J18、J12 和 J13 这三处插针，通过跳线帽将芯片配置引脚进行电平切换，共有三种工作模式。

#### ➤Flash 烧写模式

将芯片 Pin138（对应板子上 J18）接高电平（3.3V），Pin129（对应板子上 J12 的 PJ6）接高电平（3.3V），Pin130（对应板子上 J13 的 PJ7）接高电平（3.3V），PM4 接高电平（3.3V），配置芯片为 Flash 烧写模式，插入 USB\_UART 串口线，并将 PA0,PA1 接 U0Rx, U0Tx。上电或者复位芯片，使用芯片烧写工具烧录 bin 程序。

#### ➤ 正常运行模式

将芯片 Pin138（对应板子上 J18）接低电平（GND），配置为正常工作模式，插入 USB\_UART 串口线，并将 PA0,PA1 接 U0Rx, U0Tx。上电或者复位芯片，运行芯片内部程序。

#### ➤IP-TEST 模式

将芯片 Pin138（对应板子上 J18）接高电平（3.3V），Pin129 对应板子上 J12 的 PJ6)接低电平(GND),Pin130(对应板子上 J13 的 PJ7)接高电平(3.3V)，配置芯片进入测试模式，对内部时钟状态进行引脚检测。

### 3.3. 烧录方法

使用 ESC08x0 芯片烧写工具进行烧录，烧录比特率为 230400，首次烧录需要点击“Flash 配置”按钮，后续烧录只需勾选待烧写的核、指定拟烧录的 bin 文件、点击“一键烧写”。



图 3-1 烧写软件图

### 3.4. 三模启动

调度器应用程序置于默认的三模启动状态；使 ARM、MIPS 及 RISC-V 三个不同类型 CPU 在应用程序代码中通过 UART 输出信息；编译生成调度 CPU 的 bin 文件,并分别编译 ARM、MIPS 及 RISC-V 三个 CPU 输出“Hello,ESC0830.Welcometothemimicworld!”的 bin 文件，测试板置于烧录模式，依次烧录调度 CPU 和 ARM、MIPS 及 RISC-V 三个不同类型 CPU 的 bin 文件到 flash，测试板置于运行模式，复位运行，串口波特率设置为 115200，串口即可打印相关信息。



图 3-2 烧写软件图