# OSR-2560开发板

## 基本介绍

OSR-2560开发板采用8位Atmel的AVR单片机 ATmega2560，如图 1所示。为方便测试，ATmega2560芯片数字IO和模拟IO全部引出。该开发板出厂时预置Arduino Bootloader程序，可支持Arduino IDE编程和下载。开发板供电采用USB供电和DC直流供电的双供电模式，DC供电范围在9V-12V。

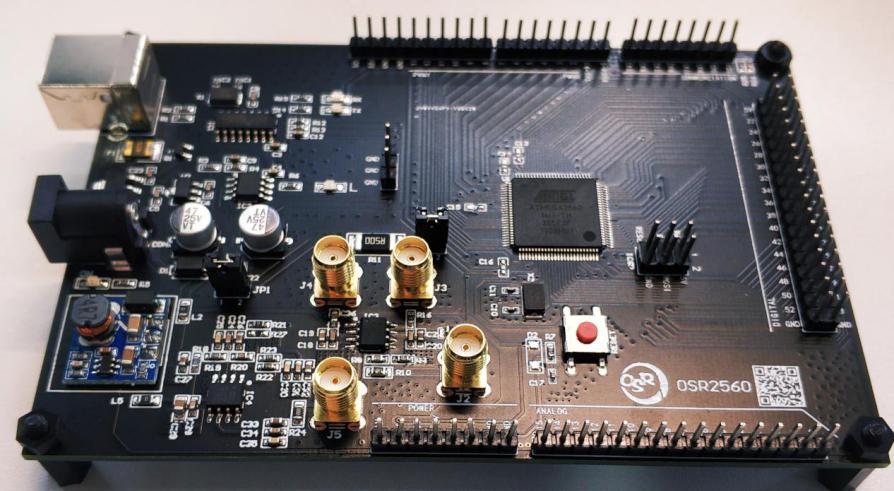
****

图 1 OSR-2560

表格1 OSR-2560性能参数

|  |  |
| --- | --- |
| 微处理器 | ATmega2560 |
| 工作电压 | 5V |
| Flash | 256KB，其中引导程序8KB |
| SRAM | 8KB |
| EEPROM | 4KB |
| 时钟频率 | 16MHz |

## 程序下载

默认测试工程的波特率是115200，如有变化请查看工程确认。

从附赠的软件安装包打开安装arduino-1.8.9-windows，安装Arduino IDE。

使用附赠的USB线将开发板与电脑连接，确保开发板上JP1的1和2脚用跳线帽短接以及JP2的1脚和2脚用跳线帽短接。

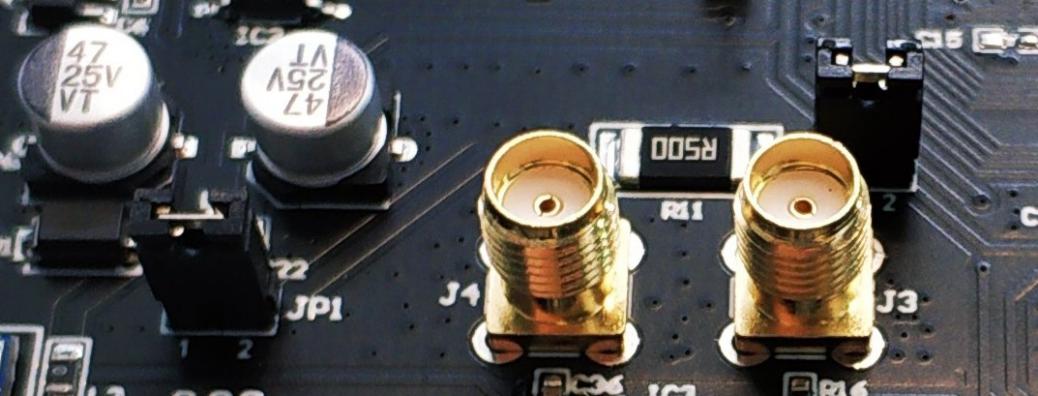


图 2 JP1位置

在菜单工具栏下 开发板中选择 Arduino/Genuion Mega or Mega2560 开发板，在端口中选择对应的串口端口号（端口号可在电脑设备管理器中查看）。



图 3 端口号选择

点击IDE中 图标对代码进行编译验证，如果没有错误最后会显示编译完成以及存储占用情况。编译通过后，点击图标上传代码，即可将代码上传到开发板中。如果上传不成功请查看串口是否正确以及是否被其它应用占用。



图 4 编译显示

文本

描述已自动生成

图 5 上传显示

## 侧信道功耗采集接口

OSR-2560发板上J5、J4、J3、J2四个SMA端子可用于电压功耗曲线采集。电压功耗采集基本原理是在MCU供电的干路上串连一个采样电阻，MCU在运算过程中，电阻中会流过电流，电流在电阻两端将产生压降，采集电阻压降可反映MCU的功耗情况。

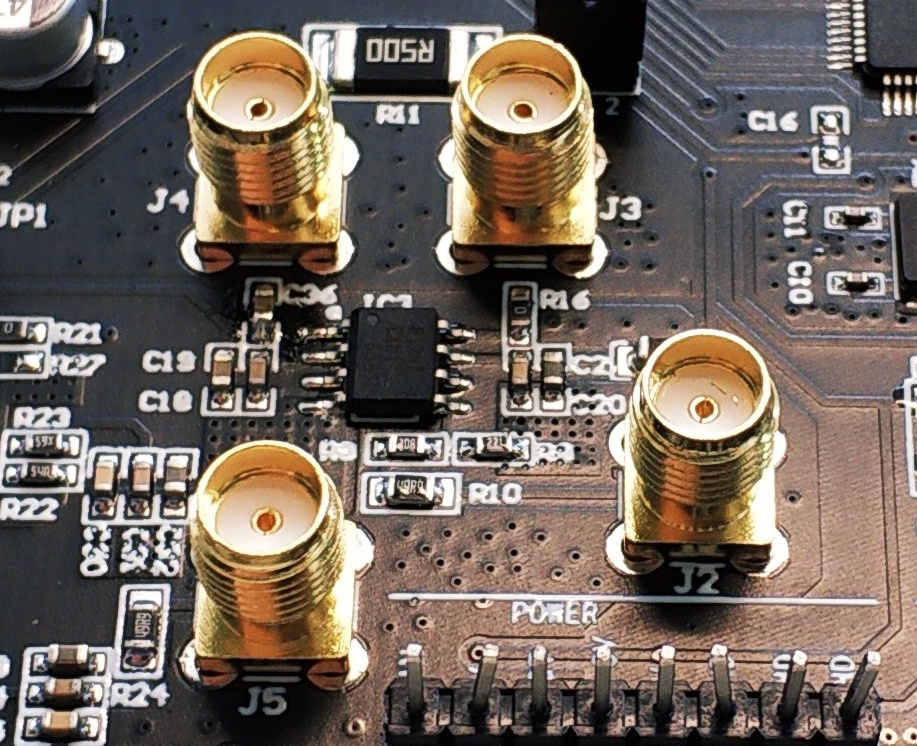


图 6 采集用SMA端子

J4是采样电阻靠近线性稳压源一端，J3是采样电阻靠近MCU芯片一端，J2是J4与J3差分放大后的信号输出端，J5是J3端信号放大后的输出端。实际采集时，可使用J5或者J2。如使用J5进行采集，一般需要外接12V直流电源，防止信号放大后截止。OSR2560进行测信道采集时尽量外接12V电源，可以消除低频纹波。

## 电压故障攻击接口

当进行电压故障攻击时，可拔掉OSR-2560开发板JP2上的跳线帽，将电压故障注入设备的电压正极输出端接到JP2的2脚，电压负极输出端接到板子上任意GND的引脚，即可实现设备对MCU的供电。

当进行电压或电磁故障攻击时，芯片可能受到干扰无法正常工作。此时，可设置JP2的2脚的电压为零，延时0.3s，再设置成正常工作电压，即可完成复位。

# OSR-407开发板

## 基本介绍

OSR-407开发板采用32位的STM32F407IGT6 MCU，该MCU为ARM Cortex-M4架构。开发板如图 7所示。

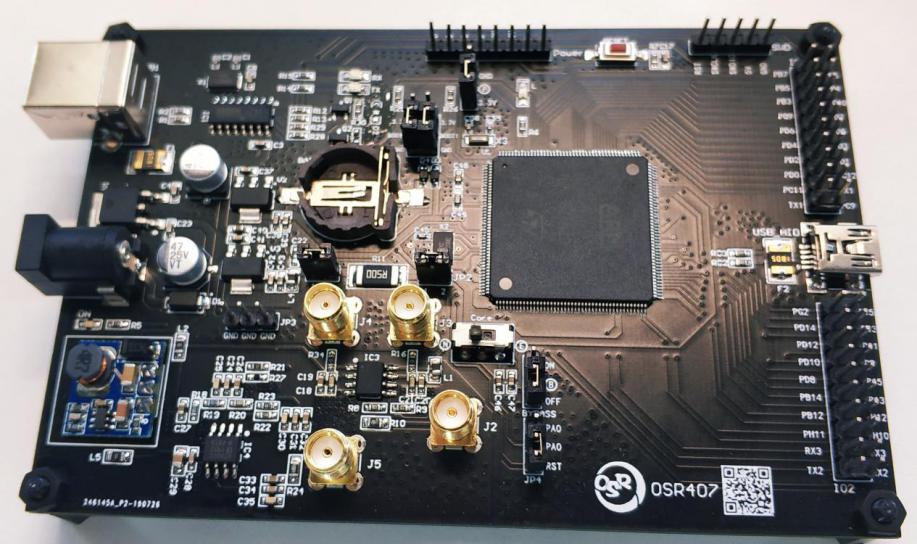
****

图 7 OSR-407开发板

OSR-407开发板引出40个GPIO供测试使用，供电采用USB供电和DC直流供电的双供电模式，DC供电范围在9V-12V。

表格 2 OSR-407开发板性能参数

|  |  |
| --- | --- |
| 微处理器 | STM32F407IG |
| 工作电压 | 3.3 V |
| Flash | 1024 KB |
| SRAM | 192 KB |
| 时钟频率 | 53.76Mhz |

为进行侧信道和故障注入攻击实验，OSR-407开发板将STM32F407核心供电引脚引出，采用外部供电。STM32F407芯片内部分为外设与核心，核心负责运算，外设为GPIO、串口、flash存储等。核心供电与外设供电电压不同：核心供电是1.2V，外设供电为3.3V。当芯片核心供电由外部输入时，芯片的运行频率需要调低到53.76Mhz以下，否则芯片不能正常工作。我们已经将芯片进行调整(使用我们提供的Arduino15.rar包才可以)，调用delay函数的实际延迟将会比设定值更长。

## 程序下载

### 下载环境配置

安装Arduino IDE 后，将软件安装文件夹中的Arduino15.rar解压缩到，C:\Users\<USERNAME>\AppData\Local，覆盖原有Arduino15文件夹及其下文件。

重新打开Arduino IDE, 在工具开发板选项卡中可以看到已经有了对STM32F4系列的支持。

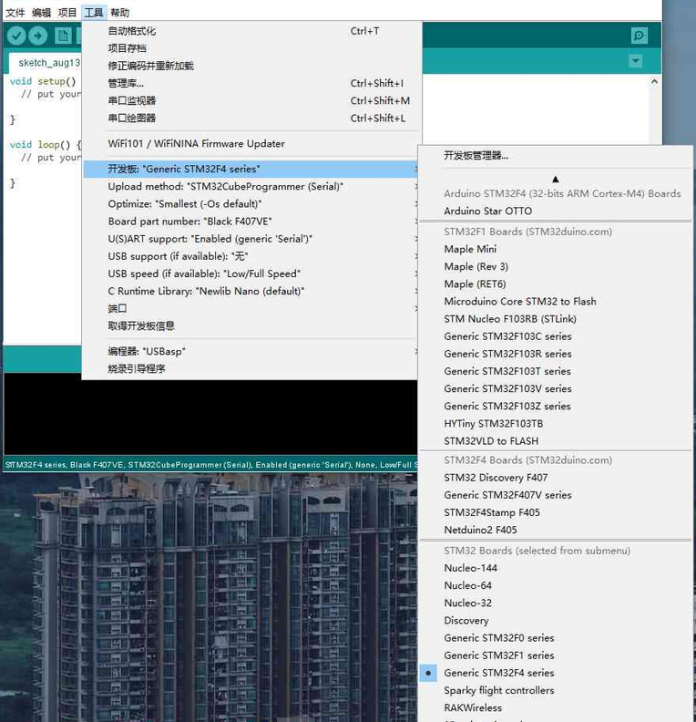


图 8 STM32F4系列支持

解压缩软件安装文件夹中STM32CubeProgrammer\_v1.3.0.rar压缩包到本地，双击解压后的SetupSTM32CubeProgrammer-1.3.0.exe按照默认路径安装不要更改。

### 程序下载

默认测试工程的波特率是115200，如有变化请查看工程确认。

用附赠的USB线将开发板与电脑连接，确保开发板上JP1的1和2脚以及JP2的1脚和2脚用跳线帽短接。将PDR排针的P脚与3.3V短接。将JP4 的PA0与RST短接。将BYPASS的B脚与OFF短接，将拨动开关Core拨向左侧即可将核心供电改变为外部1.2V供电。以上跳线连接方式为出厂默认，用户使用过程中无需进行改变。(如果需要更改为内部核心供电BYPASS的B脚与ON短接,拨动开关拨向右侧)

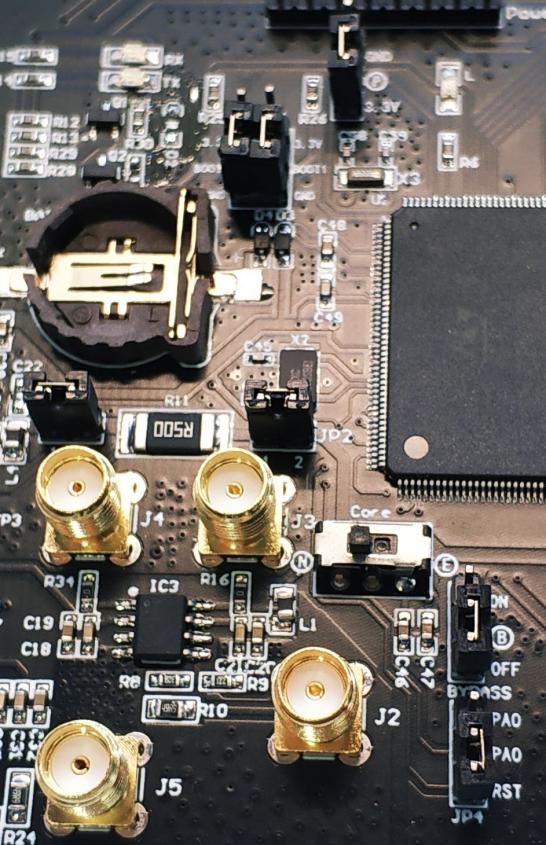


图 9 默认跳线和开关位置

将Boot排针左侧的BOOT0跳线帽连接3.3V，MCU进入等待烧写模式，如图 10所示。

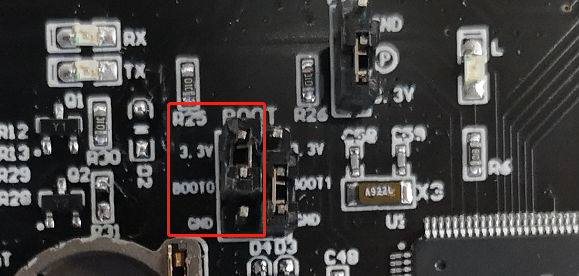
****

图 10 BOOT0跳线烧写模式

在菜单工具栏下开发板中选择 Generic STM32F4 series开发板，在Upload method中选择STM32CubeProgrammer (Serial)，在端口中选择已经查看好的端口号，其余默认不变。

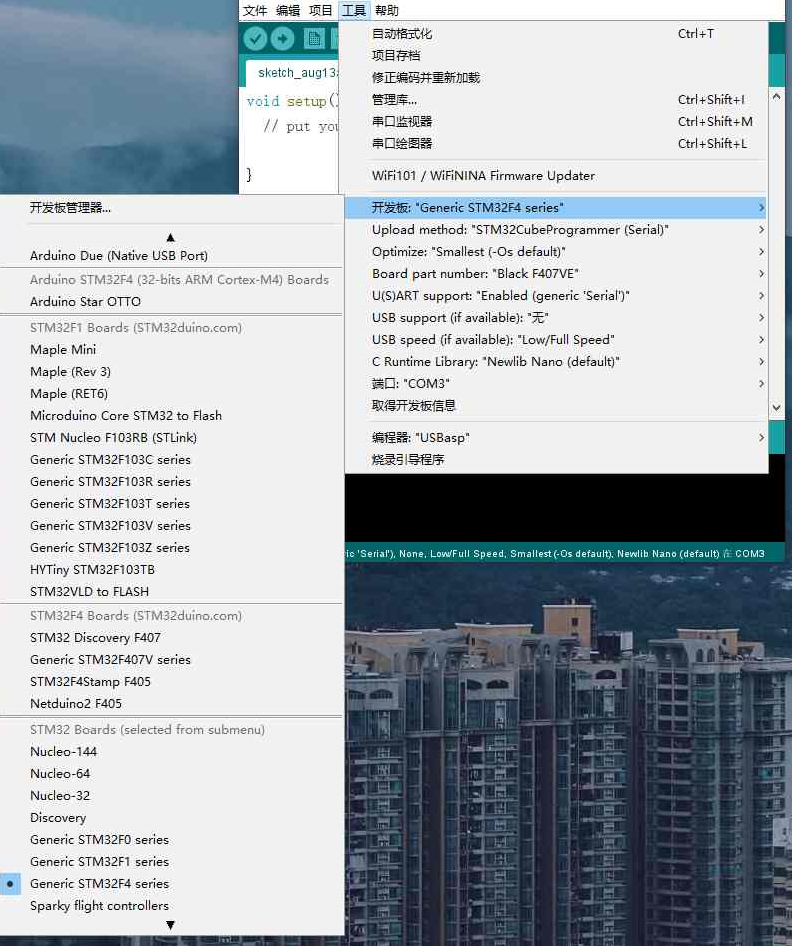


图 11 Arduino IDE开发板选择

点击IDE中 图标对代码进行编译验证，如果没有错误最后会显示编译完成以及存储占用情况。编译通过后，点击图标上传代码，即可将代码上传到开发板中。下载完毕后把Boot0跳线连接GND，然后按下复位按键程序即可正常运行。

如果下载提示失败，则请再次将BOOT0跳线帽连接3.3V，并按一下复位按键，(每次下载失败必须按一下复位按键)如果持续下载失败，可以将核心供电切回到内部再次尝试。或者在开始菜单打开安装完毕的STM32CubeProgrammer选择Arduino编译后的固件使用串口下载。

## 侧信道功耗采集接口

OSR-407开发板上J5、J4、J3、J2四个SMA端子可用于电压功耗曲线采集。电压功耗采集基本原理是在MCU供电的干路上串连一个采样电阻，MCU在运算过程中，电阻中会流过电流，电流在电阻两端将产生压降，采集电阻压降可反映MCU的功耗情况。

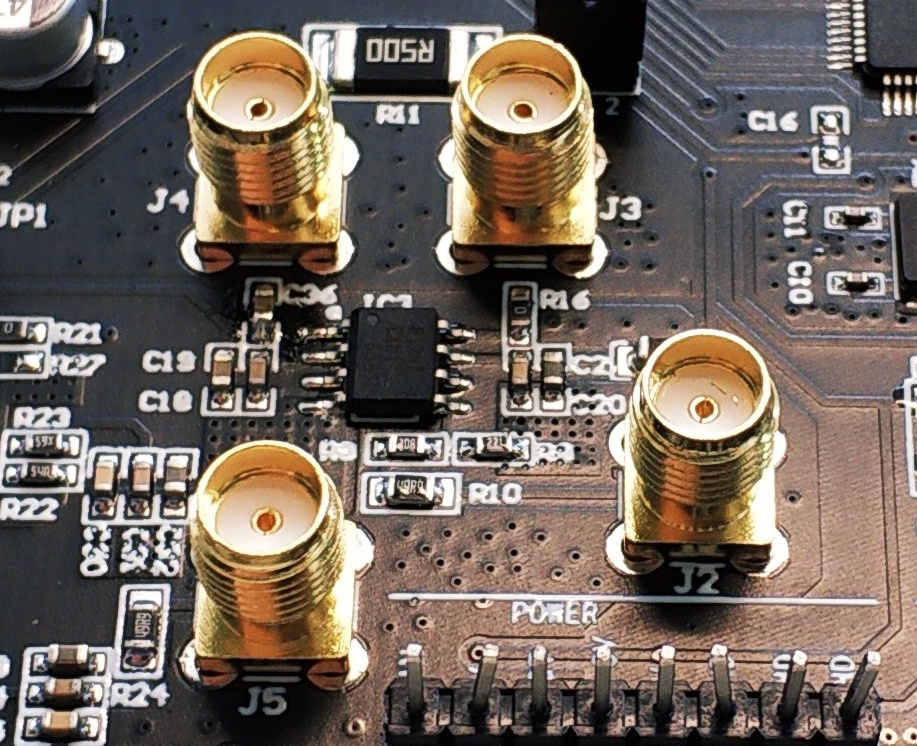


图 12 采集用SMA端子

J4是采样电阻靠近线性稳压源一端，J3是采样电阻靠近MCU芯片一端，J2是J4与J3差分放大后的信号输出端，J5是J3端信号放大后的输出端。实际采集时，可使用J5或者J2。

## 电压故障攻击接口

注意：芯片核心供电时有严格的上电顺序。

电压故障注入时，一定要保证USB口或者DC口先上电，然后才能用电压故障注入设备向核心供电。

断电时，先断核心供电，然后断USB或DC供电。

USB或者DC供电要一直存在，不能在USB和DC不供电的情况下单独给核心供电，否则芯片会烧毁。

进行电压故障攻击时，核心供电需由外部提供。移除JP2上的短接帽，将电压故障注入设备的电压正极输出端接到JP2的2脚，提供核心电压输入，电压负极输出端接到板子上任意GND的引脚。正常核心电压输入为1.2V。

当进行电压或电磁故障攻击时，芯片可能受到干扰无法正常工作。此时，可按照以下流程，完成复位：

1. 切断核心电压，延迟50ms
2. 拉低JP4的PA0引脚，延迟50ms
3. 接通核心电压，延迟50ms
4. 拉高PA0引脚为3.3V，延迟50ms

对PA0引脚的操作可通过故障注入设备的GPIO输出进行控制，具体可参见故障注入设备手册。