

# RMP轻量级实时操作系统 技术参考手册



## 演进·远古·原核（五阶）

## Mutatus·Protero·Prokaron(R.V)

## M5P1(Prokaron) R4T5

# 轻量级实时操作系统（四版五型）

## 技术参考手册

### 系统特性

#### 高易用性

- 以轻量易用为第一准绳构建的实时操作系统
- 容易配置开发环境及工程路径
- 提供最常见的线程通信接口

#### 高实时性

- 强实时策略的全抢占式内核
- 相同优先级的线程之间时间片轮转式调度
- 所有关键操作时间复杂度  $O(1)$

#### 高可移植性

- 在所有实时系统中底层汇编语言数量最少
- 严格按照 ANSI C89 和 MISRA C 要求进行编写，保证对编译器的兼容性
- 最小系统对资源的要求极低
- 可作为客户操作系统运行在其他操作系统上

#### 高执行效率

- 对代码关键性能部分进行调优
- 极短的线程切换时间和中断响应时间

#### 高可靠性

- 提供参数检查(Assert)功能，进行广泛存在的接口参数检查
- 经形式化验证，相当于 IEC61508 SIL4、橙书 A1 级别或 EAL 7+
  - \*暂时未完成，目前相当于 SIL2 预认证级别

# 目录

系统特性	2
目录	3
表目录	7
图目录	10
版本历史	11
第 1 章 概述	12
1.1 简介	12
1.1.1 设计目的和指标	12
1.1.2 软件版权与许可证	12
1.1.3 易混术语表	12
1.1.4 主要参考系统	13
1.2 前言	13
1.3 实时操作系统及其组件的性能指标	14
1.3.1 内核大小	14
1.3.2 执行时间、最坏执行时间及其抖动	15
1.3.3 中断响应时间、最坏中断响应时间及其抖动	16
1.3.4 实际中断响应时间、最坏实际中断响应时间及其抖动	17
1.4 RMP 系统调用格式	18
1.5 本章参考文献	19
第 2 章 系统内核	20
2.1 系统内核简介	20
2.1.1 内核调度器	20
2.1.2 内存管理与内存保护	20
2.1.3 应用升级与应用模块	20
2.1.4 系统启动流程	20
2.2 线程相关接口	21
2.2.1 出让处理器	22
2.2.2 线程创建	22
2.2.3 线程删除	23
2.2.4 设置线程属性	24

2.2.5 悬起线程	24
2.2.6 解除线程悬起	25
2.2.7 线程延时	25
2.2.8 解除线程延时	26
2.3 线程间通信相关接口	26
2.3.1 向线程邮箱发送	26
2.3.2 在中断中向线程邮箱发送	27
2.3.3 从线程邮箱接收	27
2.3.4 创建信号量	28
2.3.5 删除信号量	28
2.3.6 等待信号量	29
2.3.7 解除信号量等待	29
2.3.8 发布信号量	30
2.3.9 从中断发布信号量	30
2.4 内存管理接口	30
2.4.1 初始化内存池	31
2.4.2 从内存池分配内存	31
2.4.3 向内存池归还内存	32
2.4.4 重新配置某内存块的大小	32
2.5 其他系统接口	33
2.5.1 中断系统和调度器系统接口	33
2.5.2 辅助库函数接口	34
2.5.3 钩子函数接口	38
2.6 本章参考文献	40
第3章 轻量级图形界面库	42
3.1 嵌入式图形界面简介	42
3.1.1 简单性	42
3.1.2 多样性	42
3.1.3 平面性	42
3.1.4 受限性	42
3.2 RMP 的嵌入式图形界面支持	42
3.2.1 画直线	43
3.2.2 画间断直线	44
3.2.3 画矩形	44
3.2.4 画圆角矩形	45

3.2.5 画圆	46
3.2.6 绘制单色位图	46
3.2.7 以抗锯齿方式绘制单色位图	47
3.2.8 绘制光标	48
3.2.9 绘制复选框	49
3.2.10 选中复选框	49
3.2.11 清除复选框	50
3.2.12 绘制按钮	50
3.2.13 按下按钮	51
3.2.14 弹起按钮	51
3.2.15 绘制文字编辑框	52
3.2.16 清除文字编辑框的一部分	52
3.2.17 绘制单选按钮	53
3.2.18 选中单选按钮	53
3.2.19 清除单选按钮	54
3.2.20 绘制进度条	54
3.2.21 改变进度条进度	55
3.3 图形界面设计指南	56
3.3.1 扁平化设计	56
3.3.2 使用简单的背景和单色位图	56
3.3.3 字库的设计和实现	56
3.3.4 复杂控件的设计和实现	56
3.4 本章参考文献	57
<b>第 4 章 形式化验证</b>	<b>58</b>
4.1 形式化验证简介	58
4.2 系统的形式化规范	60
4.3 形式化证明	60
4.4 其他文档	60
4.5 本章参考文献	60
<b>第 5 章 移植 RMP 到新架构</b>	<b>61</b>
5.1 移植概述	61
5.2 移植前的检查工作	61
5.2.1 处理器	61
5.2.2 编译器	61
5.2.3 汇编器	61

5.2.4 调试器	62
5.3 RMP 架构相关部分介绍	62
5.3.1 类型定义	62
5.3.2 宏定义	63
5.3.3 底层汇编函数	65
5.3.4 系统中断向量	65
5.3.5 其他底层函数	65
5.4 底层汇编函数的移植	66
5.4.1 RMP_Disable_Int 的实现	66
5.4.2 RMP_Enable_Int 的实现	66
5.4.3 _RMP_Yield 的实现	66
5.4.4 _RMP_Start 的实现	67
5.5 系统中断向量的移植	67
5.5.1 定时器中断向量	67
5.5.2 线程上下文切换中断向量	68
5.6 其他底层函数的移植	68
5.6.1 底层硬件初始化	68
5.6.2 初始化某线程的线程栈	69
5.7 本章参考文献	69
第 6 章 附录	70
6.1 特殊内核功能的实现	70
6.1.1 无节拍内核的实现	70
6.1.2 浮点处理器上下文的保存和恢复	70
6.1.3 线程内存保护的实现	70
6.1.4 低功耗设计注意事项	71
6.2 RMP 中已知的影响实时性的因素	71
6.2.1 延时队列	71
6.2.2 锁调度器和关中断	71
6.3 缩减 RMP 的存储器占用	71
6.3.1 降低系统支持的优先级的数量	71
6.3.2 调整厂商提供的库	72
6.3.3 调整编译器选项	72
6.3.4 不使用动态内存管理	72
6.4 本章参考文献	72

## 表目录

表 1-1	线程切换的第一种情况	15
表 1-2	线程切换的第二种情况	16
表 1-3	线程间异步通信	16
表 1-4	中断响应时间	17
表 1-5	实际中断响应时间	18
表 1-6	RMP 系统调用一览	18
表 2-1	线程状态转移图中各标号的含义	21
表 2-2	线程相关接口的可能返回值	22
表 2-3	出让处理器	22
表 2-4	线程创建	23
表 2-5	线程删除	24
表 2-6	设置线程属性	24
表 2-7	悬起线程	25
表 2-8	解除线程悬起	25
表 2-9	线程延时	25
表 2-10	解除线程延时	26
表 2-11	向线程邮箱发送	26
表 2-12	在中断中向线程邮箱发送	27
表 2-13	从线程邮箱接收	27
表 2-14	创建信号量	28
表 2-15	删除信号量	28
表 2-16	等待信号量	29
表 2-17	解除信号量等待	29
表 2-18	发布信号量	30
表 2-19	从中断发布信号量	30
表 2-20	初始化内存池	31
表 2-21	从内存池分配内存	32
表 2-22	向内存池归还内存	32
表 2-23	重新配置某内存块的大小	32
表 2-24	除能中断	33
表 2-25	使能中断	34
表 2-26	锁定调度器	34
表 2-27	解锁调度器	34

表 2-28	清零内存	34
表 2-29	打印一个字符	35
表 2-30	打印整形数字	35
表 2-31	打印无符号整形数字	35
表 2-32	打印字符串	36
表 2-33	得到一个字的最高位	36
表 2-34	得到一个字的最低位	36
表 2-35	翻转一个字的高低位	37
表 2-36	创建双向循环链表	37
表 2-37	在双向链表中删除节点	37
表 2-38	在双向循环链表中插入节点	37
表 2-39	计算 CRC16	38
表 2-40	系统启动钩子	38
表 2-41	系统上下文保存钩子	39
表 2-42	系统上下文恢复钩子	39
表 2-43	调度器钩子	39
表 2-44	系统嘀嗒钩子	40
表 2-45	空闲线程首次运行钩子	40
表 2-46	空闲线程反复运行钩子	40
表 3-1	使用内建嵌入式图形界面所需的宏定义	43
表 3-2	画直线	43
表 3-3	画间断直线	44
表 3-4	画矩形	44
表 3-5	画圆角矩形	45
表 3-6	画圆	46
表 3-7	绘制单色位图	46
表 3-8	以抗锯齿方式绘制单色位图	47
表 3-9	绘制光标	48
表 3-10	绘制复选框	49
表 3-11	选中复选框	49
表 3-12	清除复选框	50
表 3-13	绘制按钮	50
表 3-14	按下按钮	51
表 3-15	弹起按钮	51
表 3-16	绘制文字编辑框	52
表 3-17	清除文字编辑框的一部分内容	52



表 3-18	绘制单选按钮	53
表 3-19	选中单选按钮	53
表 3-20	清除单选按钮	54
表 3-21	绘制进度条	54
表 3-22	改变进度条进度	55
表 4-1	EAL 等级及其描述	58
表 5-1	类型定义一览	62
表 5-2	必要类型定义一览	63
表 5-3	宏定义一览	63
表 5-4	底层汇编函数一览	65
表 5-5	系统中断向量一览	65
表 5-6	其他底层函数一览	66
表 5-7	RMP_Disable_Int 的实现	66
表 5-8	RMP_Enable_Int 的实现	66
表 5-9	_RMP_Yield 的实现	67
表 5-10	_RMP_Start 的实现	67
表 5-11	定时器中断处理函数	67
表 5-12	线程上下文切换中断处理函数	68
表 5-13	_RMP_Low_Level_Init 的实现	69
表 5-14	_RMP_Stack_Init 的实现	69
表 6-1	得到最近超时嘀嗒数	70

## 图目录

图 2-1 线程状态转移图	21
---------------	----

## 版本历史

版本	日期（年-月-日）	说明
R1T1	2018-02-15	初始发布
R2T1	2018-03-12	增加了移植说明和附录
R4T3	2018-07-31	修正手册的错误
R4T3	2018-09-01	更新手册到新版本
R4T4	2018-10-10	解除内存管理单元的 128MB 限制，使用更优化的圆角矩形绘制算法
R4T5	2018-11-25	解除最大优先级个数的限制，允许更激进的内存用量优化策略

## 第 1 章 概述

### 1.1 简介

在小型物联网系统中，16 到 32 位的单片机的使用越发普遍。同时，对于开发周期和可靠性的要求也在增长。因此，有必要开发轻量级的小型系统以实现简单高效的物联网应用。同时，在现代系统中，轻量级虚拟化功能的重要性逐渐增加，因此我们也需要一个轻型操作系统来作为其他操作系统的客户机使用。此外，对于此类操作系统，由于缺乏内存保护单元的介入，因此需要进行形式化验证来保证其可靠性。

**RMP** 实时操作系统是一种简单高效易用的全抢占式实时操作系统（Real-Time Operating System, RTOS）。它提供了典型 RTOS 内核所提供的所有特性：全抢占静态优先级时间片轮转调度器，简单的存储管理功能，简明的通信机制以及针对硬件的特殊优化能力。**RMP** 操作系统被设计为可以在仅具 2kB ROM、1kB RAM 的微控制器上高效地运行。

本手册从用户的角度提供了 **RMP** 的内核 API 的描述。在本手册中，我们先简要回顾关于小型实时操作系统的若干概念，然后分章节介绍 **RMP** 的特性和 API。

#### 1.1.1 设计目的和指标

**RMP** 操作系统的设计目的是创建一个简单易用的开源 RTOS 内核。这个内核要具有同级别中最好的实时性和可靠性，并且在平均执行效率上和主流内核相近。

#### 1.1.2 软件版权与许可证

综合考虑到不同应用对开源系统的不同要求，**RMP** 内核本身所采用的许可证为 **LGPL v3**，但是对一些特殊情况<sup>[1]</sup>使用特殊的规定。这些特殊规定是就事论事的，对于每一种可能情况的具体条款都会有不同。

#### 1.1.3 易混术语表

在本手册中，容易混淆的基本术语规定如下：

##### 1.1.3.1 操作系统

指运行在设备上的执行最底层处理器、内存等硬件资源管理的基本软件。

##### 1.1.3.2 线程

线程指操作系统中拥有一个独立执行栈和一个独立指令流的可被调度的实体。一个进程内部可以拥有多个线程，它们共享一个进程地址空间。

---

<sup>[1]</sup> 比如安防器材和医疗器材等

### 1.1.3.3 静态分配

指在系统编译时就决定好资源分配方式的情形。

### 1.1.3.4 动态分配

指在系统运行过程中，可以更改资源分配的情形。

### 1.1.3.5 软实时

指绝大多数情况下操作应该在时限之内完成，但也允许小部分操作偶尔在时限之外完成的实时性保证。

### 1.1.3.6 硬实时

指所有操作都必须在时限之内完成的实时性保证。

### 1.1.3.7 常数实时

指所有操作对用户输入和系统配置都是  $O(1)$  的，而且执行都能在某个有实际意义的常数时限之内完成的实时性保证。这是所有实时保证中最强的一种。

### 1.1.3.8 对某值常数实时

指所有操作和响应在某值不变的时候都是  $O(1)$  的，而且执行都能在某个有实际意义的常数时限之内完成的实时性保证。

## 1.1.4 主要参考系统

调度器部分参考了 [FreeRTOS \(@RT Engineering LTD/Amazon\)](#)。

形式化证明参考了 [seL4 \(@2016 Data61/CSIRO\)](#)。

API 接口的实现参考了 [RMProkaron \(@EDI\)](#)。

其他各章的参考文献和参考资料在该章列出。

## 1.2 前言

操作系统是一种运行在设备上的执行最底层处理器、内存等硬件资源管理的基本软件。对于实时操作系统而言，系统的每个操作都必须是正确的和及时的，其执行时间必须是可预测的。总的而言，有两类实时操作系统：第一类是软实时系统，第二类是硬实时系统。对于软实时系统，只要在大多数时间之内，程序的响应在时限之内即可；对于硬实时系统，系统的相应在任何时候都必须在时限之内。实际上，很少有实时应用或操作系统完全是软实时的或者完全是硬实时的；他们往往是软实时部分和硬实时部分的有机结合。一个最常见的例子是 LCD 显示屏人机界面部分是软实时的，而电机控制部分是硬实时的。

**RMP** 系统是一种基本实时系统。此类系统是初步展现了实时系统的基本特性的最小系统。它们一般运行在高档 8/16 位机以及低档 32 位机上面，需要一个系统定时器。此类系统没有用户态和内核态的区

别，但是可以将 MMU 和 MPU 配置为保护某段内存。此类系统需要简单的架构相关汇编代码来进行上下文堆栈切换。若要使得其在多种架构上可运行，修改这段汇编代码是必须的。移植往往还涉及系统定时器，堆栈切换，中断管理和协处理器管理。此类系统可以使用定制的连接器脚本也可以不使用，通常而言在涉及到内存保护的时候必须使用定制的连接器脚本。

在此类系统中任务表现为线程。任务函数有可能是可重入的。每个任务会使用单独的执行栈。任务代码和内核代码可以编译在一起也可以不编译在一起。任务调用系统函数往往使用直接的普通函数调用，没有经由软中断进行系统调用的概念。

此类系统具备优先级的概念，并且一般实现了不同优先级之间的抢占和相同优先级之间的时间片轮转调度。此类系统具备初级的内存管理方案，并且这种内存管理方案一般基于 SLAB 和伙伴系统。

中断对操作系统可以是完全透明的，此时操作系统并不需要知道中断是否已经到来；如果需要在中断中进行上下文切换，那么就必须将堆栈切换汇编插入该中断函数中，此时需要用汇编代码编写中断的进入和退出。

典型的此类操作系统包括 RMPProkaron、RT-Thread、FreeRTOS、uC/OS、Salvo 和 ChibiOS。对于此类实时系统，要进行完全的形式化验证通常是容易的，因为内核代码的数量非常少。传统的软件工程最多只能系统性地对软件的功能进行测试，最多能说明软件存在缺陷的可能性很小；而形式化验证可以根据某种规范或者逻辑推演规则，证明系统符合一定的属性，也即相当于证明了在给定条件下系统不可能有缺陷。

## 1.3 实时操作系统及其组件的性能指标

当前市场上有几百种不同种类的 RTOS 存在，而爱好者和个人开发的内核更是数不胜数。这些系统的性能往往是良莠不齐的。我们需要一些指标来衡量这些 RTOS 的性能。下面所列的指标都只能在处理器架构相同，编译器、编译选项相同的情况下进行直接比较。如果采用了不同的架构、编译器或编译选项，得到的数据没有直接意义，只具有参考性而不具有可比性。一个推荐的方法是使用工业实际标准的 ARM 或 MIPS 系列处理器配合 GCC -O2 选项进行评估。此外，也可以使用 Chronos 模拟器来进行评估。在评估时还要注意，系统的负载水平可能会对这些值有影响，因此只有在系统的负载水平一致的情况下，这些值才能够被比较。

### 1.3.1 内核大小

内核的尺寸是衡量 RTOS 的一个重要指标。由于 RTOS 通常被部署在内存极度受限的设备中，因此内核的小体积是非常关键的。内核的尺寸主要从两个方面衡量，一是只读段大小，二是数据段大小。只读段包括了内核的代码段和只读数据段，数据段包括了内核的可读写数据段大小。在基于 Flash 的微控制器系统中，只读段会消耗 Flash，而数据段则会消耗 SRAM[1]。

由于 RTOS 是高度可配置的，其内核大小往往不是固定的，而是和所选用的配置紧密相关的。因此，衡量此项性能，应该查看衡量最小内核配置、常见内核配置和最大内核配置下的内核大小[1]。

内核大小数据的获得非常简单，只要用编译器编译该内核，然后使用专门的二进制查看器<sup>[1]</sup>查看目标文件各段的大小即可。

### 1.3.2 执行时间、最坏执行时间及其抖动

执行时间指 RTOS 系统调用的用时大小。最坏执行时间指执行时间在最不利条件下能达到的最大长度。RTOS 的最坏执行时间通常会在如下情况下达到：执行最长的系统调用，并在此过程中产生了大量的缓存未命中。RTOS 在执行系统调用时一般都会关中断；最坏执行时间通常是系统关中断最长的时间，因此对系统的实时性的影响是非常巨大的。

最坏执行时间可以分成两类：第一类是内核系统调用的最坏执行时间，另一类是线程间同步的最坏执行时间。

要获得第一类最坏执行时间，可以在调用某个系统调用之前，计时器记下此时的时间戳  $T_s$ ，然后在系统调用结束之后，再调用计时器记下此时的时间戳  $T_e$ 。然后，连续调用两次计时器，记下两个时间戳  $T_{ts}$  和  $T_{te}$ ，得到调用计时器的额外代价为  $T_{te} - T_{ts}$ 。此时，执行时间就是  $T_e - T_s - (T_{te} - T_{ts})$ 。最坏执行时间就是所有的系统调用测试之中执行时间最大的那一个。

要获得第二类最坏执行时间，可以在通信机制的发送端调用一次计时器，记下此时的时间戳  $T_s$ ，在通信机制的接收端调用一次计时器，记下此时的时间戳  $T_e$ 。对于调用计时器的代价测量是类似第一类最坏执行时间的。最终得到的  $T_e - T_s - (T_{te} - T_{ts})$  就是执行时间。最坏执行时间，就是所有的通信测试之中，执行时间最大的那一个。

执行时间的抖动也是非常重要的。在多次测量同一个系统的执行、通信时间时，我们往往会得到一个分布。这个分布的平均值是平均执行时间，简称执行时间；其标准差<sup>[2]</sup>被称为执行时间抖动。

对于一个 RTOS，我们通常认为执行时间、最坏执行时间和抖动都是越小越好。执行时间又可以详细分成以下几类<sup>[1]</sup>：

#### 1.3.2.1 线程切换时间

线程切换时间指从一个线程切换到另外一个线程所消耗的时间。我们用下图的方法进行测量。在测量时，除了使用  $T_e - T_s$  的方法，也可以使用两次  $T_s$  之间的差值除以 2。线程切换包括两种情况，一种情况是同优先级线程之间互相切换，另外一种是由低优先级线程唤醒高优先级线程<sup>[2]</sup>。

在第一种情况下，我们假设图中的两个线程是相同优先级的，而且在测量开始时，我们正执行的是刚刚由线程 B 切换过来的线程 A。

表 1-1 线程切换的第一种情况

线程 A	线程 B
永久循环	永久循环

<sup>[1]</sup> 如 Objdump

<sup>[2]</sup> 有时我们也使用极差

线程 A	线程 B
{	{
>> 计时 $T_s$ ;	计时 $T_e$ ;
切换到线程 B;	>> 切换到线程 A;
}	}

在第二种情况下，我们假设图中的线程 B 优先级较高，而且在测量开始时，我们正执行的是刚刚由线程 B 切换过来的线程 A。

表 1-2 线程切换的第二种情况

线程 A	线程 B
永久循环	永久循环
{	{
>> 计时 $T_s$ ;	计时 $T_e$ ;
唤醒 B;	>> 睡眠;
}	}

### 1.3.2.2 异步通信时间

异步通信时间指不同线程之间发送和接收异步信号所用的时间。我们用下图的方法进行测量。我们假设线程 B 已经在接收端阻塞，线程 A 进行发送，而且线程 B 的优先级比线程 A 高[2]。

表 1-3 线程间异步通信

线程 A	线程 B
永久循环	永久循环
{	{
>> 计时 $T_s$ ;	计时 $T_e$ ;
向 B 线程发送;	>> 从自己的邮箱接收;
}	}

### 1.3.3 中断响应时间、最坏中断响应时间及其抖动

中断响应时间指从中断发生到 RTOS 调用中断对应的处理线程之间的时间。最坏中断响应时间指中断响应时间在最不利条件下能达到的最大长度。最坏中断响应时间通常会在如下情况下达到：在中断处理过程中发生了大量的缓存未命中和快表（Trans Look-aside Buffer, TLB）未命中。中断响应时间是 RTOS 最重要的指标，甚至可以说，RTOS 的一切设计都是围绕着该指标进行的。该指标是 RTOS 对外界刺激响应时间的最直接的标准。



要获得最坏中断响应时间，可以在中断向量的第一行汇编代码<sup>[1]</sup>中调用计时器，得到一个时间戳  $T_s$ ；在中断处理线程的第一行代码处调用计时器，得到一个时间戳  $T_e$ 。对于计时器代价的测量同上。最终得到的  $T_e - T_s - (T_{te} - T_{ts})$  就是中断响应时间。最坏中断响应时间，就是所有的中断响应测试之中，响应时间最大的那一个。

中断响应时间的抖动也是非常重要的。在多次测量同一个系统的中断响应时间时，我们往往会得到一个分布。这个分布的平均值是平均中断响应时间，其标准差<sup>[2]</sup>被称为中断响应时间抖动。

对于一个 RTOS，我们通常认为中断响应时间、最坏中断响应时间和抖动都是越小越好。中断响应时间的测量通常如下所示<sup>[1][3]</sup>：

表 1-4 中断响应时间

内核	线程 A
硬件中断向量	永久循环
{	{
>> 计时 $T_s$ ;	计时 $T_e$ ;
从内核向异步端点 P 发送信号;	>> 从异步端点 P 接收信号;
}	}

### 1.3.4 实际中断响应时间、最坏实际中断响应时间及其抖动

实际中断响应时间指软硬件系统中断外部信号输入到发出 IO 操作响应之间的时间。最坏实际中断响应时间指实际中断响应时间在最不利条件下能达到的最大长度。影响实际最坏中断响应时间的因素中，除了那些能影响最坏中断响应时间的因素之外，还有对应的 CPU 及 IO 硬件本身的因素。

要获得实际中断响应时间，我们需要一些外部硬件来支持该种测量。比如，我们需要测量某系统的 I/O 的实际中断响应时间，我们可以将一个 FPGA 的管脚连接到某 CPU 或主板的输入管脚，然后将另一个管脚连接到某 CPU 或者主板上的输出管脚。首先，FPGA 向输入管脚发出一个信号，此时 FPGA 内部的高精度计时器开始工作；在 FPGA 接收到输出管脚上的信号的时候，FPGA 内部的高精度计时器停止工作。最终得到的 FPGA 内部计时器的时间就是系统的实际中断响应时间。最坏实际中断响应时间，就是所有测试之中，响应时间最大的那一个。

对于一个软硬件系统，我们通常认为实际中断响应时间、最坏实际中断响应时间和抖动都是越小越好。值得注意的是，实际最坏中断响应时间一般会大约等于最坏执行时间加上最坏中断响应时间加上系统 CPU/IO 的固有延迟。比如，某系统在 IO 输入来临时刚刚开始执行某系统调用，此时硬件中断向量无法立刻得到执行，必须等到该系统调用执行完毕才可以。等到该系统调用执行完毕时，实际的硬件中断向量才开始执行，切换到处理线程进行处理并产生输出。实际中断响应时间的测量通常如下所示<sup>[1]</sup>：

<sup>[1]</sup> 不能等到 C 函数中再去调用，因为寄存器和堆栈维护也是中断响应时间的一部分

<sup>[2]</sup> 有时我们也使用极差

表 1-5 实际中断响应时间

FPGA（或者示波器）	被测系统
永久循环	永久循环
{	{
>> 发出信号并启动计时器；	从 I/O 上接收信号；
接收信号；	最简化的内部处理流程；
停止计时器；	从 I/O 上输出信号；
}	}

## 1.4 RMP 系统调用格式

系统调用是使用系统提供的功能的唯一方法。对于 RMP 而言，系统调用和通常的函数调用是一样的。下面是 RMP 中所有的系统调用接口的列表。

表 1-6 RMP 系统调用一览

系统调用名称	序号	意义
RMP_Yield	0	出让当前线程的处理器
RMP_Thd_Crt	1	创建一个线程
RMP_Thd_Del	2	删除一个线程
RMP_Thd_Set	3	设置一个线程的优先级和时间片
RMP_Thd_Suspend	4	悬起一个线程
RMP_Thd_Resume	5	解除一个线程的悬起
RMP_Thd_Delay	6	延时一段时间
RMP_Thd_Cancel	7	解除一个线程的延时
RMP_Thd_Snd	8	向某线程的邮箱发送数值
RMP_Thd_Snd_ISR	9	从中断向某线程的邮箱发送数值
RMP_Thd_Rcv	10	接收本线程邮箱值
RMP_Sem_Crt	11	创建一个计数信号量
RMP_Sem_Del	12	删除一个计数信号量
RMP_Sem_Pend	13	试图获取一个信号量
RMP_Sem_Abort	14	解除某线程对信号量的获取
RMP_Sem_Post	15	释放信号到某信号量
RMP_Sem_Post_ISR	16	从中断释放信号到某信号量

## 1.5 本章参考文献

- [1] T. N. B. Anh and S.-L. Tan, "Real-time operating systems for small microcontrollers," IEEE micro, vol. 29, 2009.
- [2] R. P. Kar, "Implementing the Rhealstone real-time benchmark," Dr. Dobb's Journal, vol. 15, pp. 46-55, 1990.
- [3] T. J. Boger, Rhealstone benchmarking of FreeRTOS and the Xilinx Zynq extensible processing platform: Temple University, 2013.

## 第 2 章 系统内核

### 2.1 系统内核简介

RMP 的内核提供了一个可使用的实时操作系统应具有的最简单的功能，主要包括线程、线程延时、邮箱机制和信号量机制。如果用户需要更复杂的机制，那么可以从 RMP 提供的几种基本机制出发实现其他的机制。本系统还额外提供了一个轻量级图形界面库，它在不使用<sup>[1]</sup>的时候完全不消耗内存。

本系统推荐用于 32 个优先级以下，64 个线程以下的系统。本系统理论上最多支持的线程数量和优先级数量都是无限的，但为了系统效率和易用性，不推荐使用本系统实现超过这个复杂度的嵌入式应用。如果需要进行更复杂的嵌入式应用，推荐使用 RMEukaryon (M7M1) 等更高级的系统。

#### 2.1.1 内核调度器

RMP 内核的调度器是一个全抢占式的固定优先级时间片轮转的调度器。该类调度器在同一个优先级内部使用时间片轮转法则进行线程调度，在不同的优先级之间则采取抢占式调度策略。和某些 RTOS 不同，RMP 的调度器在某些架构上永远不会关闭中断，从而保证了系统的实时性。为了提高内核的实时性，当处理器具备 CLZ 等指令时，RMP 还可以使用这些指令加速最高优先级查找。

RMP 没有<sup>[2]</sup>内建对多核系统的直接支持。如果要支持多核处理器也是可能的，这需要编译多个 RMP 副本并且在每个处理器上运行一个副本，以分区操作系统的方式存在，类似于 Barrelfish<sup>[1]</sup>。

#### 2.1.2 内存管理与内存保护

RMP 提供了一个基于二级分割适配算法 (Two-Level Segregated Fit, TLSF) <sup>[2][3]</sup> 机制的内存分配器。这个分配器在所有 O(1) 时间复杂度的内存分配器中具备较高空间效率。然而，在小型嵌入式系统中动态内存分配并不被推荐，因此应该尽量少用该分配器。RMP 不具备真正意义上的内存保护功能，各个线程之间的地址是没有隔离的，因此在编写应用程序时应当遵循编程规范。

#### 2.1.3 应用升级与应用模块

由于本系统相对较为小型，因此不支持应用升级和应用模块。通常而言，使用本系统编译出的完整映像大小不应超过 128kB，因此是可以全部升级的。如果需要应用模块功能，那么需要用户自行实现。

#### 2.1.4 系统启动流程

RMP 内核的第一个线程永远是 RMP\_Init，它位于内核提供的代码中。Init 线程负责系统的初期初始化和低功耗，并且它永远不可能停止运行。Init 线程引出了两个接口 RMP\_Init\_Hook 和 RMP\_Init\_Idle，它们负责将用户代码导入到内核运行的过程中。关于这两个接口的说明请参见 2.5 所述。

---

<sup>[1]</sup> 未检测到相关宏被定义

<sup>[2]</sup> 将来也永远不会

## 2.2 线程相关接口

由于整个 RMP 系统都运行在一个地址空间，因此 RMP 系统仅提供线程抽象。线程可以有就绪、运行、悬起、阻塞<sup>[1]</sup>四种状态，阻塞状态还具有一段时间后接收不到自动返回的功能。悬起状态可以被施加于任何线程，此时该线程总是暂时停止执行，无论其当前处于什么状态。

完整的线程状态转移图如下所示：

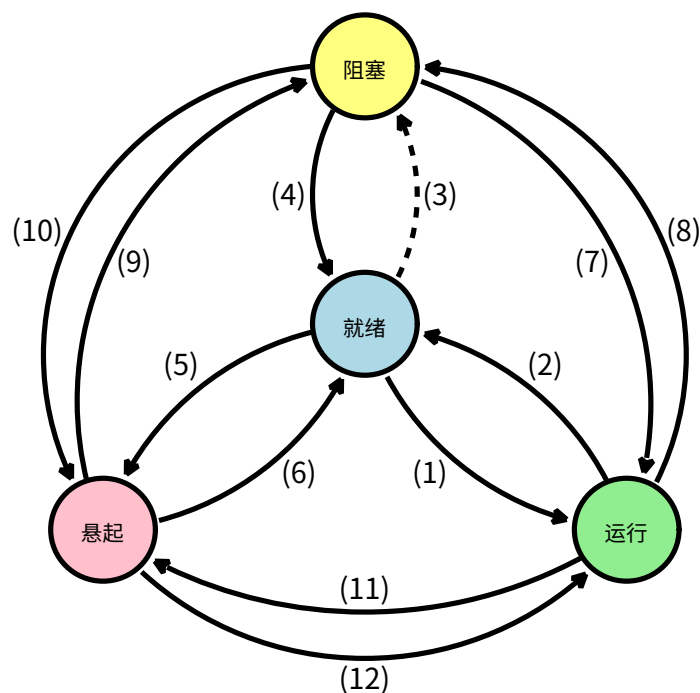


图 2-1 线程状态转移图

图中各个数字标号的意义如下所示：

表 2-1 线程状态转移图中各标号的含义

标号	代表意义
(1)	该线程处于就绪态且优先级最高，因此由就绪态转入运行态。
(2)	该线程处于运行态且优先级非最高，因此由运行态转入就绪态。
(3)	该可能性不存在（图中以虚线表示），线程不可能直接由就绪态进入阻塞态。
(4)	该线程被解除阻塞且未悬起，且优先级非最高，因此由阻塞态进入就绪态。
(5)	该线程在就绪态被悬起，因此由就绪态进入悬起态。
(6)	该线程被解除悬起且未阻塞，且优先级非最高，因此由悬起态进入就绪态。
(7)	该线程被解除阻塞且未悬起，且优先级最高，因此由阻塞态进入运行态。
(8)	该线程在邮箱、信号量或延时功能处阻塞，因此由运行态进入阻塞态。

<sup>[1]</sup> 包括延时、等待信号量、等待邮箱接收、等待邮箱发送四种阻塞方式

标号	代表意义
(9)	该线程在被解除悬起且仍在阻塞，因此由悬起态进入阻塞态。
(10)	该线程在阻塞态被悬起，因此由阻塞态进入悬起态。
(11)	该线程在运行态被悬起，因此由运行态进入悬起态。
(12)	该线程在被解除悬起且未阻塞，且优先级最高，因此由悬起态进入运行态。

下面是所有的线程相关接口。这些函数都只能在普通线程中调用，不能在中断服务程序中调用。它们可能有如下返回值：

表 2-2 线程相关接口的可能返回值

返回值	数值	意义
RMP_ERR_THD	-1	由于线程控制块相关的原因导致操作失败。
RMP_ERR_PRIO	-2	由于优先级相关的原因导致操作失败。
RMP_ERR_SLICE	-3	由于时间片相关的原因导致操作失败。
RMP_ERR_STATE	-4	由于线程状态相关的原因导致操作失败。
RMP_ERR_OPER	-5	由于其他原因导致操作失败。
RMP_ERR_SEM	-6	由于信号量控制块相关的原因导致操作失败。

具体的各个函数中返回值的意义请在相应函数下查找。

### 2.2.1 出让处理器

本操作会使当前线程放弃 CPU，并且调度器会自动选择下一个线程进行调度。如果当前线程是唯一的优先级最高的线程，那么该线程仍然会被选中进行调度。

表 2-3 出让处理器

函数原型	void RMP_Yield(void)
返回值	无。
参数	无。

### 2.2.2 线程创建

本操作会创建一个新的线程并使其处于就绪态。RMP 并不提供内核对象的管理，因此线程控制块所需的内存需要用户自行分配。该函数的 *Stack* 参数是栈的起始地址；对于递增堆栈，该值位于整个堆栈的低端；对于递减堆栈，该值则位于整个堆栈的高端。

需要注意的是，该地址是会被直接赋给线程的当前栈指针的，并且在第一次弹栈恢复上下文进入此线程时弹栈将从该处开始，因此要考虑到在整个栈空间的顶端留出一段位置用来在创建时初始化上下文。如果还需要在栈上存储其他信息，或者留出栈顶的额外安全空间，那么这段空间的大小也要留出。

比如，分配的堆栈区域 `Stack_Array` 数组的大小是 256 个字，已知该种处理器使用递减堆栈而且上下文的大小是 16 字，我们还要额外留出 10 个字的空间作为额外安全空间。那么，传给创建线程函数的 `Stack` 参数就应该是 `&Stack_Array[256-16-10]`。在上例中，如果处理器使用递增堆栈，那么传给创建线程函数的 `Stack` 参数就应该是 `&Stack_Array[16+10]`。

表 2-4 线程创建

函数原型	<code>rpm_ret_t RMP_Thd_Crt(volatile struct RMP_Thd* Thread, rpm_ptr_t Entry, rpm_ptr_t Stack, rpm_ptr_t Arg, rpm_ptr_t Prio, rpm_ptr_t Slices)</code>	
返回值	<code>rpm_ret_t</code>	如果成功，返回 0。如果失败则可能有如下返回值：
	<code>RMP_ERR_PRIO</code>	输入的优先级不小于 <code>RMP_MAX_PREEMPT_PRIO</code> 。
	<code>RMP_ERR_SLICE</code>	输入的时间片为 0 或不小于 <code>RMP_MAX_SLICES</code> 。
	<code>RMP_ERR_THD</code>	线程控制块为 0（NULL）或者正在被使用。
参数	<code>volatile struct RMP_Thd* Thread</code>	指向空的、将被用于该线程的线程控制块的指针。
	<code>rpm_ptr_t Entry</code>	线程的入口地址。
	<code>rpm_ptr_t Stack</code>	线程的运行栈。对于栈向下生长的体系结构，它指向栈空间的高地址端；对于栈向上生长的体系结构，它指向栈空间的低地址端。
	<code>rpm_ptr_t Arg</code>	传递给线程的参数。
	<code>rpm_ptr_t Prio</code>	线程的优先级。
	<code>rpm_ptr_t Slices</code>	线程的时间片数量。时间片数量的单位是时钟嘀嗒。

2.2.3 线程删除

本操作会删除系统中的一个线程。线程被删除后，一切资源将释放，正在向它发送的线程的发送等待将被解除并会返回发送失败。

值得注意的是，RMP 的线程并不允许通过返回来直接退出。如果任何一个线程想要终止自己，就必须显式调用这个函数删除自己。这个设计是有意而为，是为了显式地提醒用户线程正被删除，从而方便用户最大限度地避免“创建 - 运行一次 - 删除”的用法<sup>[1]</sup>。

表 2-5 线程删除

函数原型	rmp_ret_t RMP_Thd_Del(volatile struct RMP_Thd* Thread)	
	rmp_ret_t	
返回值	如果成功，返回 0。如果失败则可能有如下返回值：	
	RMP_ERR_THD	线程控制块为 0（NULL）或者未被使用。
参数	volatile struct RMP_Thd* Thread	
	指向要删除的的线程的线程控制块的指针。	

#### 2.2.4 设置线程属性

本操作会设置某个线程的时间片和优先级。当只需要设置其中一个时，只要保证另一个参数与原来的相同即可。

表 2-6 设置线程属性

函数原型	rmp_ret_t RMP_Thd_Set(volatile struct RMP_Thd* Thread, rmp_ptr_t Prio, rmp_ptr_t Slices)	
	rmp_ret_t	
返回值	如果成功，返回 0。如果失败则可能有如下返回值：	
	RMP_ERR_PRIO	输入的优先级不小于 RMP_MAX_PREEMPT_PRIO。
	RMP_ERR_SLICE	输入的时间片为 0 或不小于 RMP_MAX_SLICES。
	RMP_ERR_THD	线程控制块为 0（NULL）或者未被使用。
参数	volatile struct RMP_Thd* Thread	
	指向要更改优先级和时间片的线程的线程控制块的指针。	
	rmp_ptr_t Prio	
	要设置的优先级。	
	rmp_ptr_t Slices	
	要设置的时间片数量。	

#### 2.2.5 悬起线程

<sup>[1]</sup> 这种用法应该被“阻塞 - 运行一次 - 再次阻塞”代替



本操作会使某线程悬起，使调度器暂时停止对其的调度。无论线程处于哪个状态，它都可以被悬起，但是已经处于的延时、发送、接收等状态仍继续存在，也即线程处于悬起状态和延时、发送、接收等状态之一的叠加。当延时、发送、接收等状态结束后，如果该线程还处于被悬起状态，那么它将被置于纯粹的悬起状态，仍然不参与调度，直到悬起状态被手动解除。

表 2-7 悬起线程

函数原型	rmp_ret_t RMP_Thd_Suspend(volatile struct RMP_Thd* Thread)	
	rmp_ret_t	
返回值	如果成功，返回 0。如果失败则可能有如下返回值：	
	RMP_ERR_THD	线程控制块为 0（NULL）或者未被使用。
	RMP_ERR_STATE	该线程已经被悬起，无法被再次悬起。
参数	struct RMP_Thd* Thread	
	指向要悬起执行的线程的线程控制块的指针。	

### 2.2.6 解除线程悬起

本操作会解除某个线程的悬起状态，使其有重新参与调度的可能。

表 2-8 解除线程悬起

函数原型	rmp_ret_t RMP_Thd_Resume(volatile struct RMP_Thd* Thread)	
	rmp_ret_t	
返回值	如果成功，返回 0。如果失败则可能有如下返回值：	
	RMP_ERR_THD	线程控制块为 0（NULL）或者未被使用。
	RMP_ERR_STATE	该线程未被悬起，无法被解除悬起。
参数	volatile struct RMP_Thd* Thread	
	指向要解除悬起的线程的线程控制块的指针。	

### 2.2.7 线程延时

本操作会使当前线程延时一段时间。

表 2-9 线程延时

函数原型	rmp_ret_t RMP_Thd_Delay(rmp_ptr_t Slices)	
	rmp_ret_t	
返回值	如果成功，返回 0。如果失败则可能有如下返回值：	
	RMP_ERR_SLICE	输入的时间片为 0 或不小于 RMP_MAX_SLICES。

	<code>RMP_ERR_OPER</code>	该延时没有进行完毕就被解除。
参数	<code>rpm_ptr_t Slices</code>	要延时的时间，单位是时间片。

### 2.2.8 解除线程延时

本操作会解除某个线程的延时。

表 2-10 解除线程延时

函数原型	<code>rpm_ret_t RMP_Thd_Cancel(volatile struct RMP_Thd* Thread)</code>	
	<code>rpm_ret_t</code>	
返回值	如果成功，返回 0。如果失败则可能有如下返回值：	
	<code>RMP_ERR_THD</code>	线程控制块为 0（NULL）或者未被使用。
	<code>RMP_ERR_STATE</code>	该线程未处于延时状态，无法被解除延时。
参数	<code>volatile struct RMP_Thd* Thread</code>	
	指向要解除延时的线程的线程控制块的指针。	

## 2.3 线程间通信相关接口

**RMP** 提供了相对简单但高效的线程间通信机制，包括了线程邮箱和信号量。这些机制可以被单独使用，也可以被组合成更复杂的通信接口使用。可以阻塞的通信接口都有三个选项：探知可能阻塞后立即返回、阻塞超时后返回、一直阻塞。这大大提高了接口使用的灵活性。需要注意的是，所有的通信接口在有多个线程阻塞时，服务顺序永远是按照时间先后顺序的，不提供优先级插队功能。如果一个高优先级线程在低优先级线程阻塞后才阻塞，那么第一个被服务的是低优先级线程，然后才是高优先级线程。

### 2.3.1 向线程邮箱发送

本操作会向线程邮箱发送一个处理器字长的信息。

表 2-11 向线程邮箱发送

函数原型	<code>rpm_ret_t RMP_Thd_Snd(volatile struct RMP_Thd* Thread, rpm_ptr_t Data, rpm_ptr_t Slices)</code>	
	<code>rpm_ret_t</code>	
返回值	如果成功，返回 0。如果失败则可能有如下返回值：	
	<code>RMP_ERR_THD</code>	线程控制块为 0（NULL）或者未被使用。
	<code>RMP_ERR_OPER</code>	在不阻塞条件下探测到可能造成阻塞，或者试图发送到自己的邮箱，或者发送因超时、目标线程被删除而失败。

	<code>volatile struct RMP_Thd* Thread</code>
	指向要发送到的线程的线程控制块的指针。
	<code>jmp_ptr_t Data</code>
	要发送的数据。
参数	<code>jmp_ptr_t Slices</code>
	要等待的时间片数量。如果为 0，那么意味着如果探测到阻塞则立即返回；如果为 0 到 <code>RMP_MAX_SLICES</code> 之间的数值（不包括 <code>RMP_MAX_SLICES</code> ），那么将会最多阻塞等待该数量的时间片后返回；如果为超过或等于 <code>RMP_MAX_SLICES</code> 的值，那么意味着将永远阻塞直到被接收或者目标线程被销毁。

2.3.2 在中断中向线程邮箱发送

本操作会从中断向量中向线程邮箱发送一个处理器字长的信息。和上面的普通版本调用不同，该版本总是立即返回而不会阻塞。这个函数不会给调度器加锁，也不关心调度器是否被上锁；因为如果能够进入可调用本函数的中断，那么调度器一定没有被锁定。

表 2-12 在中断中向线程邮箱发送

函数原型	<code>jmp_ret_t RMP_Thd_Snd_ISR(volatile struct RMP_Thd* Thread, jmp_ptr_t Data)</code>
	<code>jmp_ret_t</code>
返回值	如果成功，返回 0。如果失败则可能有如下返回值： <code>RMP_ERR_THD</code> 线程控制块为 0（NULL）或者未被使用。 <code>RMP_ERR_OPER</code> 目标线程的邮箱已满，无法发送。
	<code>volatile struct RMP_Thd* Thread</code>
	指向要发送到的线程的线程控制块的指针。
参数	<code>jmp_ptr_t Data</code>
	要发送的数据。

2.3.3 从线程邮箱接收

本操作会从当前线程的邮箱中接收一个值。

表 2-13 从线程邮箱接收

函数原型	<code>jmp_ret_t RMP_Thd_Rcv(jmp_ptr_t* Data, jmp_ptr_t Slices)</code>
	<code>jmp_ret_t</code>
返回值	如果成功，返回 0。如果失败则可能有如下返回值： <code>RMP_ERR_OPER</code> 在不阻塞条件下探测到可能造成阻塞，或者接收因超时而失败，或者

	传入了空指针。
	<code>rmp_ptr_t* Data</code> 该参数用于输出，输出接收到的数据。
参数	<code>rmp_ptr_t Slices</code> 要等待的时间片数量。如果为 0，那么意味着如果探测到阻塞则立即返回；如果为 0 到 <code>RMP_MAX_SLICES</code> 之间的数值 <sup>[1]</sup> ，那么将会最多阻塞等待该数量的时间片后返回；如果为超过或等于 <code>RMP_MAX_SLICES</code> 的值，那么意味着将永远阻塞直到接收完成。

2.3.4 创建信号量

本操作会创建一个新的信号量。

表 2-14 创建信号量

函数原型	<code>rmp_ret_t RMP_Sem_Crt(volatile struct RMP_Sem* Semaphore, rmp_ptr_t Number)</code>
	<code>rmp_ret_t</code> 如果成功，返回 0。如果失败则可能有如下返回值： <code>RMP_ERR_SEM</code> 信号量控制块为 0（NULL）或者已被使用。 <code>RMP_ERR_OPER</code> 初始信号量值过大，超出或等于 <code>RMP_SEM_MAX_NUM</code> 。
参数	<code>volatile struct RMP_Sem* Semaphore</code> 指向空的、将被用于该信号量的信号量控制块的指针。 <code>rmp_ptr_t Number</code> 该信号量的初始值，应该小于 <code>RMP_SEM_MAX_NUM</code> 。

2.3.5 删除信号量

本操作会删除一个信号量。如果有线程在其上阻塞，那么这些线程的等待信号量函数会直接返回 `RMP_ERR_OPER`。

表 2-15 删除信号量

函数原型	<code>rmp_ret_t RMP_Sem_Del(volatile struct RMP_Sem* Semaphore)</code>
	<code>rmp_ret_t</code> 如果成功，返回 0。如果失败则可能有如下返回值： <code>RMP_ERR_SEM</code> 信号量控制块为 0（NULL）或者未被使用。
参数	<code>volatile struct RMP_Sem* Semaphore</code>

<sup>[1]</sup> 不包括 `RMP_MAX_SLICES`

指向要删除的信号量的信号量控制块的指针。

2.3.6 等待信号量

本操作会使当前线程尝试获取信号量。获取的数量总是为 1。

表 2-16 等待信号量

函数原型		rmp_ret_t RMP_Sem_Pend(volatile struct RMP_Sem* Semaphore, rmp_ptr_t Slices)	
		rmp_ret_t	
		如果成功，返回当前信号量的剩余值。如果失败则可能有如下返回值：	
返回值	RMP_ERR_SEM	信号量控制块为 0（NULL）或者未被使用。	
	RMP_ERR_OPER	在不阻塞条件下探测到可能造成阻塞，或者等待因超时、目标信号量被删除、被中途解除而失败。	
		volatile struct RMP_Sem* Semaphore	
		指向要等待的信号量的信号量控制块的指针。	
		rmp_ptr_t Slices	
参数		要等待的时间片数量。如果为 0，那么意味着如果探测到阻塞则立即返回；如果为 0 到 RMP_MAX_SLICES 之间的数值 <sup>[1]</sup> ，那么将会最多阻塞等待该数量的时间片后返回；如果为超过或等于 RMP_MAX_SLICES 的值，那么意味着将永远阻塞直到获取到信号量或者目标信号量被销毁。	

2.3.7 解除信号量等待

本操作解除某线程的信号量等待。如果等待成功被解除，那么目标线程的等待信号量函数会返回 RMP\_ERR\_OPER。

表 2-17 解除信号量等待

函数原型		rmp_ret_t RMP_Sem_Abort(volatile struct RMP_Thd* Thread)	
		rmp_ret_t	
		如果成功，返回 0。如果失败则可能有如下返回值：	
返回值	RMP_ERR_THD	线程控制块为 0（NULL）或者未被使用。	
	RMP_ERR_STATE	该线程未等待信号量状态，无法被解除等待。	
		volatile struct RMP_Thd* Thread	
参数		指向要取消信号量等待的线程的线程控制块的指针。	

<sup>[1]</sup> 不包括 RMP\_MAX\_SLICES

### 2.3.8 发布信号量

本操作会发布一定数量的信号到某信号量。

表 2-18 发布信号量

函数原型	<code>rmp_ret_t RMP_Sem_Post(volatile struct RMP_Sem* Semaphore, rmp_ptr_t Number)</code>	
	<code>rmp_ret_t</code>	
	如果成功，返回 0。如果失败则可能有如下返回值：	
返回值	<code>RMP_ERR_SEM</code>	信号量控制块为 0（NULL）或者未被使用。
	<code>RMP_ERR_OPER</code>	目标信号量如果接受此数量的信号会溢出，也即超过 <code>RMP_SEM_MAX_NUM</code> 。
参数	<code>volatile struct RMP_Sem* Semaphore</code>	
	指向要发布到的信号量的信号量控制块的指针。	
	<code>rmp_ptr_t Number</code>	要发布的信号数量。

### 2.3.9 从中断发布信号量

本操作会从中断中发布一定数量的信号到某信号量。这个函数不会给调度器加锁，也不关心调度器是否被上锁；因为如果能够进入可调用本函数的中断，那么调度器一定没有被锁定。

表 2-19 从中断发布信号量

函数原型	<code>rmp_ret_t RMP_Sem_Post_ISR(volatile struct RMP_Sem* Semaphore, rmp_ptr_t Number)</code>	
	<code>rmp_ret_t</code>	
	如果成功，返回 0。如果失败则可能有如下返回值：	
返回值	<code>RMP_ERR_SEM</code>	信号量控制块为 0（NULL）或者未被使用。
	<code>RMP_ERR_OPER</code>	目标信号量如果接受此数量的信号会溢出，也即超过 <code>RMP_SEM_MAX_NUM</code> 。
参数	<code>volatile struct RMP_Sem* Semaphore</code>	
	指向要发布到的信号量的信号量控制块的指针。	
	<code>rmp_ptr_t Number</code>	要发布的信号数量。

## 2.4 内存管理接口

RMP 提供了一个基于 TLSF 的内存分配器。它可以有效地管理动态内存。TLSF 分配器是一种二级适配算法，它把内存块先按照 2 的方次放入不同的初级指数区间（First-Level Interval, FLI），如 127-64 Byte，255-128 Byte 等，然后在每个区间之内再将内存块放入各个线性区间，比如在 127-64 Byte 的二级线性区间（Second-Level Interval, SLI）就有[127, 112]，[111, 96]，……，[79, 64]一共 8 个。在分配时，先查找某大小对应的 SLI 的下一级 SLI 有没有可供分配的内存块，如果有则分配；如果没有则向上查找到最近的 SLI，从那里分配内存。当内存被释放时，内存块会被即刻合并并且放入对应的 SLI，准备下次分配。

RMP 的 TLSF 实现中,FLI 的数目会根据内存池的大小决定,SLI 的数目则固定为 8,同时规定当 FLI=0 时对应 127-64Byte 的内存块，并且单个内存池的大小不能低于 1024 个机器字<sup>[1]</sup>。该分配器是为 128MB 以下的内存池特别优化的，不推荐将其用于更大的内存池。此外，内存池和内存池的大小均要求对其到机器字，并且一次分配的最小内存数量为 64Byte。

内存池的初始化和使用均非常灵活<sup>[2]</sup>，因此 RMP 的内存池操作默认是不锁调度器的。如果需要锁调度器，那么可以使用 RMP\_Lock\_Sched 和 RMP\_Unlock\_Sched 自行实现。

最后，要注意 RMP 的内存分配器并不实现内存保护功能，无法在内存结构被破坏时恢复。因此，使用动态分配的内存时一定要注意不要在分配的区域外进行读写。如果进行读写，可能会破坏分配器的数据结构而引起异常。

RMP 的 TLSF 分配器仅仅包括四个调用，如下列出。

2.4.1 初始化内存池

本操作按照传入的内存池大小和地址初始化该内存池。内存池的大小和地址必须对齐到机器字。

表 2-20 初始化内存池

函数原型	rmp_ret_t RMP_Mem_Init(volatile void* Pool, rmp_ptr_t Size)	
	rmp_ret_t	
返回值	如果成功，返回 0。如果失败则可能有如下返回值：	
	RMP_ERR_MEM	内存池为空（NULL）或大小、地址未对齐，或者传入的内存池大小小于 1024 个机器字。
	volatile void* Pool	
参数	指向要初始化为内存池的空白内存的指针。	
	rmp_ptr_t Size	
	该块空白内存的大小。	

2.4.2 从内存池分配内存

<sup>[1]</sup> 对于 16 位机不能少于 2kB，对于 32 位机则不能少于 4kB

<sup>[2]</sup> 可以每个线程使用自己的私有内存池也可以任意共享

本操作会试图从某内存池分配内存。分配的最小数量为 64Byte，如果试图分配的数量小于它而大于 0，那么实际上会分配 64Byte；如果传入的大小为 0 则会直接返回分配失败。

表 2-21 从内存池分配内存

函数原型	<code>void* RMP_Malloc(volatile void* Pool, rmp_ptr_t Size)</code>
返回值	<code>void*</code> 如果成功，指向返回内存的非 0（NULL）指针。如果失败则返回 0（NULL）。
参数	<code>volatile void* Pool</code> 指向要分配内存的内存池的指针。
	<code>rmp_ptr_t Size</code> 要分配的内存大小，单位是 Byte。

### 2.4.3 向内存池归还内存

本操作会向某个内存池归还内存。传入的指针必须是由 `RMP_Malloc` 返回的某个地址，并且必须归还到分配该内存时使用的内存池。

表 2-22 向内存池归还内存

函数原型	<code>void RMP_Free(volatile void* Pool, void* Mem_Ptr)</code>
返回值	无。
参数	<code>volatile void* Pool</code> 指向要归还内存的内存池的指针。
	<code>void* Mem_Ptr</code> 指向要归还的内存块的指针。

### 2.4.4 重新配置某内存块的大小

本操作会试图重新配置某内存块的大小。传入的指针必须是由 `RMP_Malloc` 返回的某个地址，而且传入的内存池必须与调用 `RMP_Malloc` 时的内存池一致。该函数在成功时，会返回原内存块或者一个前 `Size` 字节和原地址内容相同的新内存块；若不成功，则返回 0（NULL）且原内存块不受影响。另外，如果 `Size` 的值为 0，该函数的行为与 `RMP_Free` 相同，会直接释放该内存块；如果 `Mem_Ptr` 为 0，该函数的行为与 `RMP_Malloc` 相同，会直接分配新的内存块。

表 2-23 重新配置某内存块的大小

函数原型	<code>void* RMP_Realloc(volatile void* Pool, void* Mem_Ptr, rmp_ptr_t Size)</code>
返回值	<code>void*</code>



	如果成功，返回指向重新配置大小后的内存块的非 0（NULL）指针。如果失败则返回 0（NULL）。
	<code>volatile void* Pool</code> 指向要重新配置大小的内存块所在的内存池的指针。
参数	<code>void* Mem_Ptr</code> 指向要重新配置大小的内存块的指针。
	<code>rpm_ptr_t Size</code> 要将该内存块重新配置为的大小。该大小可以大于或者小于原内存块大小。

2.5 其他系统接口

RMP 提供的其他接口包括了中断开关、调度器锁定解锁和一些辅助函数。这些函数可以在用户编写应用程序的时候提供一些便利。

2.5.1 中断系统和调度器系统接口

在 RMP 中，中断系统的接口仅包括一对开关中断的函数。这一对函数是提供给用户使用的，因为在某些架构上 RMP 自身在运行过程中不关闭中断。除非硬性需要，否则不建议关闭中断，因为这会大大影响系统的实时性。

调度器系统的接口则包括一对带有嵌套计数功能的使能和除能调度器的函数。这一对函数也提供给用户使用。由于锁调度器也会降低系统的实时性，因此也不建议经常使用。总的方针是，如果不锁调度器能解决问题，那就不锁调度器；如果锁调度器和关中断都能解决，那么锁调度器；只有必须关中断时才关中断，而且关中断的区间应当尽量短。

2.5.1.1 除能中断

本操作关闭处理器对所有中断源的响应，包括系统定时器中断和调度中断。该函数不具备嵌套计数功能；如果需要嵌套计数功能，那么需要用户自行实现。

表 2-24 除能中断

函数原型	<code>void RMP_Disable_Int(void)</code>
返回值	无。
参数	无。

2.5.1.2 使能中断

本操作开启处理器对所有中断源的响应。该函数不具备嵌套计数功能；如果需要嵌套计数功能，那么需要用户自行实现。

表 2-25 使能中断

函数原型	void RMP_Enable_Int(void)
返回值	无。
参数	无。

### 2.5.1.3 锁定调度器

本操作锁定调度器，使调度器无法选择新的线程进行调度。该函数具备嵌套计数功能。

表 2-26 锁定调度器

函数原型	void RMP_Lock_Sched(void)
返回值	无。
参数	无。

### 2.5.1.4 解锁调度器

本操作解锁调度器，使之又可以选择新的线程进行调度。该函数具备嵌套计数功能。

表 2-27 解锁调度器

函数原型	void RMP_Unlock_Sched(void)
返回值	无。
参数	无。

## 2.5.2 辅助库函数接口

为了方便用户应用程序的编写，RMP 提供了一系列库函数供用户使用。这些库函数包括了内存清零、调试信息打印和链表操作等。这些库函数的列表如下：

### 2.5.2.1 清零内存

本操作将一段内存清零。

表 2-28 清零内存

函数原型	void RMP_Clear(volatile void* Addr, rmp_ptr_t Size)
返回值	无。
参数	volatile void* Addr
	要清零的内存段的起始地址。
	rmp_ptr_t Size
	要清零的内存段的大小，单位为字节。

### 2.5.2.2 打印一个字符

本操作打印一个字符到控制台<sup>[1]</sup>。

表 2-29 打印一个字符

函数原型	void RMP_Putchar(char Char)
返回值	无。
参数	char Char 要打印的字符本身。

### 2.5.2.3 打印整形数字

本操作以包含符号的十进制打印一个机器字长的整形数字到调试控制台。

表 2-30 打印整形数字

函数原型	rpm_cnt_t RMP_Print_Int(rpm_cnt_t Int)
返回值	rpm_cnt_t 返回打印的字符数量。
参数	rpm_cnt_t Int 要打印的整形数字。

### 2.5.2.4 打印无符号整形数字

本操作以无前缀十六进制打印一个机器字长的无符号整形数字到调试控制台。

表 2-31 打印无符号整形数字

函数原型	rpm_cnt_t RMP_Print_Uint(rpm_ptr_t Uint)
返回值	rpm_cnt_t 返回打印的字符数量。
参数	rpm_ptr_t Uint 要打印的无符号整形数字。

### 2.5.2.5 打印字符串

本操作打印一个最长不超过 255 字符的字符串到调试控制台。

<sup>[1]</sup> 一般是串口

表 2-32 打印字符串

函数原型	<code>rmp_cnt_t RMP_Print_String(rmp_s8_t* String)</code>
返回值	<code>rmp_cnt_t</code> 返回打印的字符数量。
参数	<code>rmp_s8_t* String</code> 要打印的字符串。

#### 2.5.2.6 得到一个字的最高位

本操作得到一个字的最高位的位号<sup>[1]</sup>。如果该数字为 0，那么需要返回-1<sup>[2]</sup>。

表 2-33 得到一个字的最高位

函数原型	<code>rmp_ptr_t RMP_MSB_Get(rmp_ptr_t Val)</code>
返回值	<code>rmp_ptr_t</code> 返回该字最高位的位号。
参数	<code>rmp_ptr_t Val</code> 要求出最高位位号的无符号整数。

#### 2.5.2.7 得到一个字的最低位

本操作得到一个字的最低位的位号<sup>[3]</sup>。如果该数字为 0，那么返回一个等于处理器字长的值<sup>[4]</sup>。

表 2-34 得到一个字的最低位

函数原型	<code>rmp_ptr_t RMP_LSB_Get(rmp_ptr_t Val)</code>
返回值	<code>rmp_ptr_t</code> 返回该字最低位的位号。
参数	<code>rmp_ptr_t Val</code> 要求出最低位位号的无符号整数。

#### 2.5.2.8 翻转一个字的高低位

本操作会将一个字的比特位翻转，例如在 32 位处理器上会令第 0 位和第 31 位交换，第 1 位和第 30 位交换，第 2 位和第 29 位交换，依此类推。

<sup>[1]</sup> 比如 32 位处理器会返回 0-31

<sup>[2]</sup> 比如 32 位处理器应返回 0xFFFFFFFF

<sup>[3]</sup> 比如 32 位处理器会返回 0-31

<sup>[4]</sup> 比如 32 位处理器会返回 32

表 2-35 翻转一个字的高低位

函数原型	<code>rm_ptr_t RMP_RBIt_Get(rm_ptr_t Val)</code>
返回值	<code>rm_ptr_t</code> 高低位翻转后的该字。
参数	<code>rm_ptr_t Val</code> 要翻转高低位的无符号整数。

#### 2.5.2.9 创建双向循环链表

本操作初始化双向循环链表的链表头。

表 2-36 创建双向循环链表

函数原型	<code>void RMP_List_Crt(volatile struct RMP_List* Head)</code>
返回值	无。
参数	<code>volatile struct RMP_List* Head</code> 指向要初始化的链表头结构体的指针。

#### 2.5.2.10 在双向循环链表中删除节点

本操作从双向链表中删除一个或一系列节点。

表 2-37 在双向链表中删除节点

函数原型	<code>void RMP_List_Del(volatile struct RMP_List* Prev, volatile struct RMP_List* Next)</code>
返回值	无。
参数	<code>volatile struct RMP_List* Prev</code> 指向要删除的节点（组）的前继节点的指针。 <code>volatile struct RMP_List* Next</code> 指向要删除的节点（组）的后继节点的指针。

#### 2.5.2.11 在双向循环链表中插入节点

本操作从双向链表中插入一个节点。

表 2-38 在双向循环链表中插入节点

函数原型	<code>void RMP_List_Ins(volatile struct RMP_List* New, volatile struct RMP_List* Prev, volatile struct RMP_List* Next)</code>
------	---

返回值	无。
参数	<code>volatile struct RMP_List* New</code> 指向要插入的新节点的指针。
	<code>volatile struct RMP_List* Prev</code> 指向要被插入的位置的前继节点的指针。
	<code>volatile struct RMP_List* Next</code> 指向要被插入的位置的后继节点的指针。

### 2.5.2.12 计算 CRC16

本函数会按照多项式 0xA001 来计算一段内存的 CRC16 校验码。只有当 `rpm_u8_t` 和 `rpm_u16_t` 两个类型被定义，并且宏 `__RMP_U8_T__` 和 `__RMP_U16_T__` 被定义时，该函数才参与编译。

表 2-39 计算 CRC16

函数原型	<code>rpm_ptr_t RMP_CRC16(const rpm_u8_t* Data, rpm_ptr_t Length)</code>
返回值	<code>rpm_ptr_t</code> 计算得出的 CRC16 值。
参数	<code>const rpm_u8_t* Data</code> 指向要计算 CRC16 的内存段的指针。
	<code>rpm_ptr_t Length</code> 该内存段的长度，其单位是字节。

### 2.5.3 钩子函数接口

为了方便在系统运行的一些关键点插入用户所需的功能，RMP 系统还提供了钩子函数。要使用这些钩子函数，需要定义宏 `RMP_USE_HOOKS` 为 `RMP_TRUE`。系统中所提供的钩子函数的列表如下：

#### 2.5.3.1 系统启动钩子

该钩子函数会在系统完成处理器初始化后立即被调用。由于每个移植在系统启动时都仅仅会初始化一部分最基本的硬件，因此推荐将硬件的进一步初始化放置在这个钩子内部完成。如果所想要的基本系统配置与该平台中的配置头文件提供的基本初始化冲突<sup>[1]</sup>，那么也可以在该钩子内部重新完成系统基本配置。

表 2-40 系统启动钩子

函数原型	<code>void RMP_Start_Hook(void)</code>
------	--

<sup>[1]</sup> 比如想要配置系统到完全不同的工作频率

返回值	无。
参数	无。

### 2.5.3.2 系统上下文保存钩子

该钩子函数会在系统完成基本上下文保存后被调用。如果有额外的上下文<sup>[1]</sup>需要保存，可以在该函数中将这些上下文压栈。具体的实现方法请参见第四章。

表 2-41 系统上下文保存钩子

函数原型	void RMP_Save_Ctx(void)
返回值	无。
参数	无。

### 2.5.3.3 系统上下文恢复钩子

该钩子函数会在系统完成基本上下文恢复前被调用。如果有额外的上下文<sup>[2]</sup>需要恢复，可以在该函数中将这些上下文弹栈。具体的实现方法请参见第四章。

表 2-42 系统上下文恢复钩子

函数原型	void RMP_Load_Ctx(void)
返回值	无。
参数	无。

### 2.5.3.4 调度器钩子

该钩子函数会在系统完成当前线程选择时被调用。如果需要进行无滴答内核，可以在这个钩子内调用相关函数进行。具体的无滴答系统实现方法请参见 [6.1.1](#)。

表 2-43 调度器钩子

函数原型	void RMP_Sched_Hook(void)
返回值	无。
参数	无。

### 2.5.3.5 系统滴答钩子

该钩子函数会在系统滴答到来时被调用。如果需要进行无滴答内核，可以在这个钩子内调用相关函数进行。具体的无滴答系统实现方法请参见 [6.1.1](#)。

<sup>[1]</sup> FPU 和其他外设寄存器组

<sup>[2]</sup> FPU 和其他外设寄存器组

表 2-44 系统嘀嗒钩子

函数原型	void RMP_Tick_Hook(rmp_ptr_t Ticks)
返回值	无。
参数	<code>rmp_ptr_t Ticks</code> 当前时钟嘀嗒和上一个时钟嘀嗒之间经过的嘀嗒数量。

#### 2.5.3.6 空闲线程首次运行钩子

该钩子函数会在空闲线程首次运行时被调用一次。这个钩子函数总是被使能的，不论宏 `RMP_USE_HOOKS` 的定义情况如何。在这个函数中可以添加更多的线程创建操作以启动其他线程，或者做一些系统初始化工作。

表 2-45 空闲线程首次运行钩子

函数原型	void RMP_Init_Hook(void)
返回值	无。
参数	无。

#### 2.5.3.7 空闲线程反复运行钩子

该钩子函数会在空闲线程被运行时反复被调用。这个钩子函数总是被使能的，不论宏 `RMP_USE_HOOKS` 的定义情况如何。典型的用法是在这个函数中进入低功耗模式以省电，或者做一些性能分析、堆栈检测打印输出。

表 2-46 空闲线程反复运行钩子

函数原型	void RMP_Init_Idle(void)
返回值	无。
参数	无。

## 2.6 本章参考文献

[1] A. Baumann, P. Barham, P.-E. Dagand, T. Harris, R. Isaacs, S. Peter, et al., "The multikernel: a new OS architecture for scalable multicore systems," in Proceedings of the ACM SIGOPS 22nd symposium on Operating systems principles, 2009, pp. 29-44.

[2] M. Masmano, I. Ripoll, A. Crespo, and J. Real, "TLSF: A new dynamic memory allocator for real-time systems," in Real-Time Systems, 2004. ECRTS 2004. Proceedings. 16th Euromicro Conference on, 2004, pp. 79-88.



[3] X. Sun, J. Wang, and X. Chen, "An improvement of TLSF algorithm," in Real-Time Conference, 2007 15th IEEE-NPSS, 2007, pp. 1-5.

## 第 3 章 轻量级图形界面库

### 3.1 嵌入式图形界面简介

嵌入式图形界面（Graphic User Interface, GUI）是用于嵌入式系统的专用图形解决方案。和传统的计算机图形界面相比，嵌入式 GUI 具有简单性、多样性、平面性和受限性的特点。抓住这四点特征是良好完成嵌入式 GUI 设计的关键。

#### 3.1.1 简单性

通常而言，嵌入式 GUI 的组成元素比较单一，一般是几个按钮或者几个显示控件，不像传统 GUI 一样有滚动条、树状列表等诸多组成元素。而且，一旦 UI 界面设计完成，在产品使用过程中就很少改变。

#### 3.1.2 多样性

传统 GUI 的设计在经过多年演化后，基本上达成了一定的共识，形成了如 Windows, MacOS, Gnome 和 Unity 为代表的一大批桌面环境。它们都强调优化键鼠操作的使用体验，并使用近乎相同的使用逻辑，其控件大多标准化。而在嵌入式 GUI 中则正好相反，很少使用标准键鼠输入而较多使用定制键盘和触摸屏，并且有大量的非标准控件和界面。这些控件的界面和逻辑也是趣旨各异的，需要针对具体应用做大量的优化和适配。

#### 3.1.3 平面性

传统 GUI 的技术栈非常强调采用复杂的窗口裁剪，使得窗口具备垂直向的叠加关系，并且需要通过复杂的算法计算出各个窗口的显示区域，并且予以绘制。这在多窗口多任务的极度复杂环境中是必须的。而在嵌入式 GUI 中，由于显示区域本来就很小，再加上输入手段受限，很少用到多个窗口之间的纵向空间关系，而更加强调扁平而人性化的 GUI 设计。这一点从各个手机操作系统的演化上也可以看出端倪。

#### 3.1.4 受限性

传统 GUI 的实现往往有赖于强有力的 CPU 和 GPU 的支持，并且需要很大的内存来做各种复杂的图形学操作。但在嵌入式环境下，很多时候凑出足够的帧缓存都是很困难的，更不要说使用专用硬件进行图形学操作了。因此，用于嵌入式环境中的 GUI 需要有特别优化。

### 3.2 RMP 的嵌入式图形界面支持

RMP 通过提供一系列绘制功能来支持 GUI 界面，它的基本绘图功能包括了画点画线、几何图形绘制和位图抗锯齿渲染，而稍复杂的功能则包括了各类控件的绘制。这些绘制功能都是不记录 GUI 对象的状态的，也不采用面向对象设计，因此在使用时不消耗任何额外的 RAM 而仅仅消耗一定量的 ROM。要使用图形界面，需要额外在配置头文件中定义几个宏，这样相关的部分才参与编译。这些宏的列表如下：

表 3-1 使用内建嵌入式图形界面所需的宏定义

宏名称	作用
RMP_POINT	<p>画点函数的宏定义。定义这个宏对于使用所有的图形绘制函数都是必须的。应该将这个宏定义为画点函数的函数名，而画点函数必须具备如下的原型：</p> <pre>void foo(rmp_cnt_t X, rmp_cnt_t Y, rmp_ptr_t Color);</pre> <p>其作用必须是在屏幕上的某处画一个点。</p> <p>例子：#define RMP_POINT RMP_Point</p>
RMP_COLOR_25P(C1, C2)	颜色混合函数的宏定义。定义这些宏仅仅对于使用抗锯齿位图绘制是必须的。三个宏都携带两个颜色作为参数，并返回一个颜色。
RMP_COLOR_50P(C1, C2)	RMP_COLOR_25P 意味着将 C1 与 C2 做 25%+75%的混合，
RMP_COLOR_75P(C1, C2)	RMP_COLOR_50P 意味着将 C1 与 C2 做对半混合， RMP_COLOR_75P 意味着将 C1 与 C2 做 75%+25%的混合。
RMP_CTL_WHITE	内建控件颜色的宏定义。定义这些宏仅仅对于使用内建控件是必须的。
RMP_CTL_LGREY	RMP_CTL_WHITE 为白色的编码定义，推荐#FFFFFF。
RMP_CTL_GREY	RMP_CTL_LGREY 为淡灰色的编码定义，推荐#B8B8B8。
RMP_CTL_DGREY	RMP_CTL_GREY 为灰色的编码定义，推荐#E0E0E0。
RMP_CTL_DARK	RMP_CTL_DGREY 为深灰色的编码定义，推荐#A0A0A0。
RMP_CTL_DDARK	RMP_CTL_DARK 为暗灰色的编码定义，推荐#787C78。
RMP_CTL_BLACK	RMP_CTL_DDARK 为极暗灰色的编码定义，推荐#686868。 RMP_CTL_BLACK 为黑色的编码定义，推荐#000000。

RMP 提供的绘图函数在绘图时均不检查绘制范围的 X 和 Y 是否超出屏幕边界。这个责任是应用程序开发者负担的。这些绘图函数的列表如下：

### 3.2.1 画直线

该函数在屏幕上绘制一条宽度为 1 的直线。绘制采用 Bresenham 算法进行光栅化。

表 3-2 画直线

函数原型	void RMP_Line(rmp_cnt_t Start_X, rmp_cnt_t Start_Y, rmp_cnt_t End_X, rmp_cnt_t End_Y, rmp_ptr_t Color)
返回值	无。
参数	<p>rmp_cnt_t Start_X 直线的起始点的 X 坐标。</p> <p>rmp_cnt_t Start_Y</p>

	直线的起始点的 Y 坐标。
<code>rmp_cnt_t End_X</code>	
	直线的终止点的 X 坐标。
<code>rmp_cnt_t End_Y</code>	
	直线的终止点的 Y 坐标。
<code>rmp_ptr_t Color</code>	
	直线的颜色。

3.2.2 画间断直线

该函数在屏幕上绘制一条宽度为 1 的间断直线。绘制采用 Bresenham 算法进行光栅化。

表 3-3 画间断直线

函数原型	<code>void RMP_Dot_Line(rmp_cnt_t Start_X, rmp_cnt_t Start_Y, rmp_cnt_t End_X, rmp_cnt_t End_Y, rmp_ptr_t Dot, rmp_ptr_t Space)</code>
返回值	无。
	<code>rmp_cnt_t Start_X</code>
	间断线的起始点的 X 坐标。
	<code>rmp_cnt_t Start_Y</code>
	间断线的起始点的 Y 坐标。
	<code>rmp_cnt_t End_X</code>
	间断线的终止点的 X 坐标。
参数	<code>rmp_cnt_t End_Y</code>
	间断线的终止点的 Y 坐标。
	<code>rmp_ptr_t Dot</code>
	间断线的点的颜色。
	<code>rmp_ptr_t Space</code>
	间断线的空位的颜色。如果填入 <code>RMP_TRANS</code> ，不绘制空位。

3.2.3 画矩形

该函数在屏幕上绘制一个矩形。矩形可以具备一个与填充颜色不同的轮廓颜色，可以填充也可以不填充。

表 3-4 画矩形

函数原型	void RMP_Rectangle(rmp_cnt_t Coord_X, rmp_cnt_t Coord_Y, rmp_cnt_t Length, rmp_cnt_t Width, rmp_ptr_t Border, rmp_ptr_t Fill)
返回值	无。
参数	<a href="#">rmp_cnt_t Coord_X</a> 矩形左上角的 X 坐标。
	<a href="#">rmp_cnt_t Coord_Y</a> 矩形左上角的 Y 坐标。
	<a href="#">rmp_cnt_t Length</a> 矩形的长度。
	<a href="#">rmp_cnt_t Width</a> 矩形的宽度。
	<a href="#">rmp_ptr_t Border</a> 矩形的边界颜色。
	<a href="#">rmp_ptr_t Fill</a> 矩形的填充颜色。如果填入 <a href="#">RMP_TRANS</a> ，不进行填充。

### 3.2.4 画圆角矩形

该函数在屏幕上绘制一个圆角矩形。圆角矩形的轮廓颜色与填充颜色一致，且本身必须被全部填充。

表 3-5 画圆角矩形

函数原型	void RMP_Round_Rect(rmp_cnt_t Coord_X, rmp_cnt_t Coord_Y, rmp_cnt_t Length, rmp_cnt_t Width, rmp_cnt_t Round, rmp_ptr_t Color)
返回值	无。
参数	<a href="#">rmp_cnt_t Coord_X</a> 矩形左上角的 X 坐标。
	<a href="#">rmp_cnt_t Coord_Y</a> 矩形左上角的 Y 坐标。
	<a href="#">rmp_cnt_t Length</a> 矩形的长度。
	<a href="#">rmp_cnt_t Width</a> 矩形的宽度。
	<a href="#">rmp_ptr_t Round</a>

圆角矩形的圆角半径。

`rpm_ptr_t Color`

圆角矩形的颜色。

### 3.2.5 画圆

该函数在屏幕上绘制一个圆。圆可以具备一个与填充颜色不同的轮廓颜色，可以填充也可以不填充。

表 3-6 画圆

函数原型	<code>void RMP_Circle(rpm_cnt_t Center_X, rpm_cnt_t Center_Y, rpm_cnt_t Radius, rpm_ptr_t Border, rpm_ptr_t Fill)</code>
返回值	无。
参数	<code>rpm_cnt_t Center_X</code> 圆心的 X 坐标。
	<code>rpm_cnt_t Center_Y</code> 圆心的 Y 坐标。
	<code>rpm_cnt_t Radius</code> 圆的半径。
	<code>rpm_ptr_t Border</code> 圆的边界颜色。
	<code>rpm_ptr_t Fill</code> 圆的填充颜色。如果填入 <code>RMP_TRANS</code> ，不进行填充。

### 3.2.6 绘制单色位图

该函数绘制一个单色位图到屏幕。位图的长度必须为 8 的整数，位图必须按照行优先从左到右从高到低扫描的方式储存。在绘制时可以选择高位优先模式或者低位优先模式，当选择前者时，一个字节的最高位的点的 X 值在一个字节代表的各个像素中最小，选择后者则反之<sup>[1]</sup>。

表 3-7 绘制单色位图

函数原型	<code>void RMP_Matrix(rpm_cnt_t Coord_X, rpm_cnt_t Coord_Y, const rpm_u8_t* Matrix, rpm_cnt_t Bit_Order, rpm_cnt_t Length, rpm_cnt_t Width, rpm_ptr_t Color)</code>
返回值	无。

<sup>[1]</sup> 这和字节序的概念很相似，不过这里是一个字节内部的各个位的像素顺序

参数	<code>rmc_cnt_t Coord_X</code>
	位图左上角的 X 坐标。
	<code>rmc_cnt_t Coord_Y</code>
	位图左上角的 Y 坐标。
	<code>const rmc_u8_t* Matrix</code>
	指向单色位图数据的指针。
	<code>rmc_cnt_t Bit_Order</code>
	字节内的位序。填入 <code>RMP_MAT_BIG</code> 为高位优先模式，0 为低位优先模式。
	<code>rmc_cnt_t Length</code>
	位图的长度，必须是 8 的倍数，否则绘制不会开始。
	<code>rmc_cnt_t Width</code>
	位图的宽度。
	<code>rmc_ptr_t Color</code>
	绘制位图所用的颜色。

3.2.7 以抗锯齿方式绘制单色位图

该函数以 4 x FXAA 的抗锯齿模式绘制一个单色位图到屏幕。位图的长度必须为 8 的整数，位图必须按照行优先从左到右从高到低扫描的方式储存。在绘制时可以选择高位优先模式或者低位优先模式。在绘制时需要传入位图所在的图层的背景色以进行抗锯齿处理。要使用该函数还要求三个颜色混合宏已经被定义。

表 3-8 以抗锯齿方式绘制单色位图

函数原型	<code>void RMP_Matrix_AA(rmc_cnt_t Coord_X, rmc_cnt_t Coord_Y, const rmc_u8_t* Matrix, rmc_cnt_t Bit_Order, rmc_cnt_t Length, rmc_cnt_t Width, rmc_ptr_t Color, rmc_ptr_t Back)</code>
返回值	无。
参数	<code>rmc_cnt_t Coord_X</code>
	位图左上角的 X 坐标。
	<code>rmc_cnt_t Coord_Y</code>
	位图左上角的 Y 坐标。
	<code>const rmc_u8_t* Matrix</code>
	指向单色位图数据的指针。

<code>rmp_cnt_t Bit_Order</code>
字节内的位序。填入 <code>RMP_MAT_BIG</code> 为高位优先模式，0 为低位优先模式。
<code>rmp_cnt_t Length</code>
位图的长度，必须是 8 的倍数，否则绘制不会开始。
<code>rmp_cnt_t Width</code>
位图的宽度。
<code>rmp_ptr_t Color</code>
绘制位图所用的颜色。
<code>rmp_ptr_t Back</code>
位图所在图层的背景色。

3.2.8 绘制光标

该函数可以绘制各种 16x16 的光标到屏幕。使用该函数及该函数之后所列的所有函数，均需要所有的控件颜色宏被定义。

表 3-9 绘制光标

函数原型	<code>void RMP_Cursor(rmp_cnt_t Coord_X, rmp_cnt_t Coord_Y, rmp_ptr_t Style)</code>	
返回值	无。	
	<code>rmp_cnt_t Coord_X</code>	光标左上角的 X 坐标。
	<code>rmp_cnt_t Coord_Y</code>	光标左上角的 Y 坐标。
	<code>rmp_ptr_t Style</code>	绘制光标的样式。可选择如下项之一：
参数	<code>RMP_CUR_NORM</code>	通常光标。
	<code>RMP_CUR_BUSY</code>	带有沙漏符号的忙光标。
	<code>RMP_CUR_QUESTION</code>	带有问号符号的光标。
	<code>RMP_CUR_HAND</code>	手形光标。
	<code>RMP_CUR_TEXT</code>	文字编辑光标。
	<code>RMP_CUR_STOP</code>	停止光标。
	<code>RMP_CUR_MOVE</code>	移动光标。
	<code>RMP_CUR_LR</code>	左右调整光标。



RMP_CUR_UD	上下调整光标。
RMP_CUR_ULBR	右下-左上调整光标。
RMP_CUR_URBL	左下-右上调整光标。
RMP_CUR_CROSS	十字准心光标。

3.2.9 绘制复选框

该函数在屏幕上绘制一个大小可变的复选框。

表 3-10 绘制复选框

函数原型	void RMP_Checkbox(rmp_cnt_t Coord_X, rmp_cnt_t Coord_Y, rmp_cnt_t Length, rmp_ptr_t Status)
返回值	无。
参数	rmp_cnt_t Coord_X 复选框左上角的 X 坐标。
	rmp_cnt_t Coord_Y 复选框左上角的 Y 坐标。
	rmp_cnt_t Length 复选框的长度 <sup>[1]</sup> 。
	rmp_ptr_t Status 复选框的当前状态。填入 RMP_CBOX_CHECK，复选框被选中，0 则为不选中。

3.2.10 选中复选框

该函数选中一个已经绘制的复选框。

表 3-11 选中复选框

函数原型	void RMP_Checkbox_Set(rmp_cnt_t Coord_X, rmp_cnt_t Coord_Y, rmp_cnt_t Length)
返回值	无。
参数	rmp_cnt_t Coord_X 复选框左上角的 X 坐标。
	rmp_cnt_t Coord_Y 复选框左上角的 Y 坐标。

<sup>[1]</sup> 同时也是宽度

`rpm_cnt_t Length`

复选框的长度<sup>[1]</sup>。

3.2.11 清除复选框

该函数清除一个已经绘制的复选框。

表 3-12 清除复选框

函数原型	<code>void RMP_Checkbox_Clr(rpm_cnt_t Coord_X, rpm_cnt_t Coord_Y, rpm_cnt_t Length)</code>
返回值	无。
参数	<code>rpm_cnt_t Coord_X</code> 复选框左上角的 X 坐标。
	<code>rpm_cnt_t Coord_Y</code> 复选框左上角的 Y 坐标。
	<code>rpm_cnt_t Length</code> 复选框的长度 <sup>[2]</sup> 。

3.2.12 绘制按钮

该函数绘制一个大小可变的按钮。

表 3-13 绘制按钮

函数原型	<code>void RMP_Cmdbtn(rpm_cnt_t Coord_X, rpm_cnt_t Coord_Y, rpm_cnt_t Length, rpm_cnt_t Width, rpm_ptr_t Status)</code>
返回值	无。
参数	<code>rpm_cnt_t Coord_X</code> 按钮左上角的 X 坐标。
	<code>rpm_cnt_t Coord_Y</code> 按钮左上角的 Y 坐标。
	<code>rpm_cnt_t Length</code> 按钮的长度。
	<code>rpm_cnt_t Width</code>

<sup>[1]</sup> 同时也是宽度

<sup>[2]</sup> 同时也是宽度

按钮的宽度。

`tmp_ptr_t Status`

按钮的当前状态。填入 `RMP_CBTN_DOWN`，按钮被按下，0 则为弹起状态。

3.2.13 按下按钮

该函数按下一个已经绘制的按钮。

表 3-14 按下按钮

函数原型	<code>void RMP_Cmdbtn_Down(tmp_cnt_t Coord_X, tmp_cnt_t Coord_Y, tmp_cnt_t Length, tmp_cnt_t Width)</code>
返回值	无。
参数	<code>tmp_cnt_t Coord_X</code> 按钮左上角的 X 坐标。
	<code>tmp_cnt_t Coord_Y</code> 按钮左上角的 Y 坐标。
	<code>tmp_cnt_t Length</code> 按钮的长度。
	<code>tmp_cnt_t Width</code> 按钮的宽度。

3.2.14 弹起按钮

该函数弹起一个已经绘制的按钮。

表 3-15 弹起按钮

函数原型	<code>void RMP_Cmdbtn_Up(tmp_cnt_t Coord_X, tmp_cnt_t Coord_Y, tmp_cnt_t Length, tmp_cnt_t Width)</code>
返回值	无。
参数	<code>tmp_cnt_t Coord_X</code> 按钮左上角的 X 坐标。
	<code>tmp_cnt_t Coord_Y</code> 按钮左上角的 Y 坐标。
	<code>tmp_cnt_t Length</code> 按钮的长度。
	<code>tmp_cnt_t Width</code> 按钮的宽度。

按钮的宽度。

### 3.2.15 绘制文字编辑框

该函数绘制一个大小可变的文字编辑框。

表 3-16 绘制文字编辑框

函数原型	void RMP_Lineedit(rmp_cnt_t Coord_X, rmp_cnt_t Coord_Y, rmp_cnt_t Length, rmp_cnt_t Width)
返回值	无。
参数	<a href="#">rmp_cnt_t Coord_X</a> 文字编辑框左上角的 X 坐标。
	<a href="#">rmp_cnt_t Coord_Y</a> 文字编辑框左上角的 Y 坐标。
	<a href="#">rmp_cnt_t Length</a> 文字编辑框的长度。
	<a href="#">rmp_cnt_t Width</a> 文字编辑框的宽度。

### 3.2.16 清除文字编辑框的一部分

该函数清除文字编辑框的一部分内容。

表 3-17 清除文字编辑框的一部分内容

函数原型	void RMP_Lineedit_Clr(rmp_cnt_t Coord_X, rmp_cnt_t Coord_Y, rmp_cnt_t Length, rmp_cnt_t Width, rmp_cnt_t Clr_X, rmp_cnt_t Clr_Len)
返回值	无。
参数	<a href="#">rmp_cnt_t Coord_X</a> 文字编辑框左上角的 X 坐标。
	<a href="#">rmp_cnt_t Coord_Y</a> 文字编辑框左上角的 Y 坐标。
	<a href="#">rmp_cnt_t Length</a> 文字编辑框的长度。
	<a href="#">rmp_cnt_t Width</a> 文字编辑框的宽度。
	<a href="#">rmp_cnt_t Clr_X</a>

要清除的位置的起始 X 坐标。该坐标值为相对坐标值。

`rmc_cnt_t Clr_Len`

要清除的长度。

3.2.17 绘制单选按钮

该函数绘制一个大小可变的单选按钮。

表 3-18 绘制单选按钮

函数原型	<code>void RMP_Radiobtn(rmc_cnt_t Coord_X, rmc_cnt_t Coord_Y, rmc_cnt_t Length, rmc_ptr_t Status)</code>
返回值	无。
参数	<code>rmc_cnt_t Coord_X</code> 单选按钮左上角的 X 坐标。
	<code>rmc_cnt_t Coord_Y</code> 单选按钮左上角的 Y 坐标。
	<code>rmc_cnt_t Length</code> 单选按钮的长度 <sup>[1]</sup> 。
	<code>rmc_ptr_t Status</code> 单选按钮的当前状态。填入 <code>RMP_RBTN_SEL</code> ，单选按钮被选中，0 为不选中。

3.2.18 选中单选按钮

该函数选中一个已绘制的单选按钮。

表 3-19 选中单选按钮

函数原型	<code>void RMP_Radiobtn_Set(rmc_cnt_t Coord_X, rmc_cnt_t Coord_Y, rmc_cnt_t Length)</code>
返回值	无。
参数	<code>rmc_cnt_t Coord_X</code> 单选按钮左上角的 X 坐标。
	<code>rmc_cnt_t Coord_Y</code> 单选按钮左上角的 Y 坐标。
	<code>rmc_cnt_t Length</code>

<sup>[1]</sup> 同时也是宽度

单选按钮的长度<sup>[1]</sup>。

3.2.19 清除单选按钮

该函数清除一个已绘制的单选按钮。

表 3-20 清除单选按钮

函数原型	void RMP_Radiobtn_Clr(rmp_cnt_t Coord_X, rmp_cnt_t Coord_Y, rmp_cnt_t Length)
返回值	无。
参数	<code>rmp_cnt_t Coord_X</code> 单选按钮左上角的 X 坐标。
	<code>rmp_cnt_t Coord_Y</code> 单选按钮左上角的 Y 坐标。
	<code>rmp_cnt_t Length</code> 单选按钮的长度 <sup>[2]</sup> 。

3.2.20 绘制进度条

该函数绘制一个进度条。

表 3-21 绘制进度条

函数原型	void RMP_Progbar(rmp_cnt_t Coord_X, rmp_cnt_t Coord_Y, rmp_cnt_t Length, rmp_cnt_t Width, rmp_cnt_t Style, rmp_cnt_t Prog, rmp_ptr_t Fore, rmp_ptr_t Back)
返回值	无。
参数	<code>rmp_cnt_t Coord_X</code> 进度条左上角的 X 坐标。
	<code>rmp_cnt_t Coord_Y</code> 进度条左上角的 Y 坐标。
	<code>rmp_cnt_t Length</code> 进度条的长度。
	<code>rmp_cnt_t Width</code> 进度条的宽度。

<sup>[1]</sup> 同时也是宽度

<sup>[2]</sup> 同时也是宽度

<code>rpm_cnt_t Style</code>	
进度条的样式。可以是以下四种之一：	
<code>RMP_PBAR_L2R</code>	从左向右增长的进度条。
<code>RMP_PBAR_D2U</code>	从下向上增长的进度条。
<code>RMP_PBAR_R2L</code>	从右向左增长的进度条。
<code>RMP_PBAR_U2D</code>	从上向下增长的进度条。
<code>rpm_cnt_t Prog</code>	
进度条的进度，必须是一个 0-100 之间的数字。	
<code>rpm_ptr_t Fore</code>	
进度条的前景颜色，也即进度本身的颜色。	
<code>rpm_ptr_t Back</code>	
进度条的背景颜色，也即进度空白部分的颜色。	

3.2.21 改变进度条进度

该函数改变一个已绘制的进度条的进度。

表 3-22 改变进度条进度

函数原型	<code>void RMP_Progbar_Set(rpm_cnt_t Coord_X, rpm_cnt_t Coord_Y,</code>	
	<code>rpm_cnt_t Length, rpm_cnt_t Width, rpm_cnt_t Style,</code>	
	<code>rpm_cnt_t Old_Prog, rpm_cnt_t New_Prog,</code>	
	<code>rpm_ptr_t Fore, rpm_ptr_t Back)</code>	
返回值	无。	
参数	<code>rpm_cnt_t Coord_X</code>	
	进度条左上角的 X 坐标。	
	<code>rpm_cnt_t Coord_Y</code>	
	进度条左上角的 Y 坐标。	
	<code>rpm_cnt_t Length</code>	
	进度条的长度。	
	<code>rpm_cnt_t Width</code>	
	进度条的宽度。	
	<code>rpm_cnt_t Style</code>	
	进度条的样式。可以是以下四种之一：	
	<code>RMP_PBAR_L2R</code>	从左向右增长的进度条。

<code>RMP_PBAR_D2U</code>	从下向上增长的进度条。
<code>RMP_PBAR_R2L</code>	从右向左增长的进度条。
<code>RMP_PBAR_U2D</code>	从上向下增长的进度条。
<code>rmp_cnt_t Old_Prog</code>	进度条的原先进度，必须是一个 0-100 之间的数字。
<code>rmp_cnt_t New_Prog</code>	进度条的新进度，必须是一个 0-100 之间的数字。
<code>rmp_ptr_t Fore</code>	进度条的前景颜色，也即进度本身的颜色。
<code>rmp_ptr_t Back</code>	进度条的后景颜色，也即进度空白部分的颜色。

### 3.3 图形界面设计指南

由于本库的功能相比全功能图形库功能极为受限，因此在设计时需要遵循一些基本原则，也需要一些设计技巧。这些设计技巧将在以下各节详细介绍。

#### 3.3.1 扁平化设计

由于本图形库不支持窗口管理器，因此最好使用扁平化设计。扁平化设计也是目前的设计潮流。关于其具体概念和细节，可以参考相关的网站和文献资料，比如[苹果公司](#)的 UI 设计指导。

#### 3.3.2 使用简单的背景和单色位图

由于本 GUI 实际上不支持图层叠加和半透明混合，因此其抗锯齿位图绘制功能要求传入固定的背景色来参与运算。如果采用非单色背景，那么该功能将无法使用。实际上在绝大多数界面中也用不到复杂的背景图片，因为往往一个深灰色背景就足够了。

同时，也要尽量避免使用单色位图以外的图形。这主要是由于灰度位图和彩色位图非常占用 Flash 空间。使用单色位图比起使用灰色或彩色位图可以节约大概 90% 以上的存储空间。

#### 3.3.3 字库的设计和实现

在使用本 GUI 库时，可以采用两种方法来实现字库。第一种方法是将使用的字做成单色位图，并且存储在单片机的 ROM 中；另一种则是使用外挂的字库芯片。对于界面美观度要求较高，但是不要求显示全字符集的，建议使用前一种方法；对于那些要求使用全字符集的则要求使用后一种方法。

#### 3.3.4 复杂控件的设计和实现



由于本 GUI 仅仅提供了那些最基本的控件，而这些最基本的控件在某些对美观程度要求较高的场合往往达不到要求，因此要自行设计控件。要显示自行设计的控件，可以使用本 GUI 提供的位图绘制功能对其进行绘制，在检测到控件状态变化之后去更新该控件到一个新的位图即可。

### 3.4 本章参考文献

无

## 第 4 章 形式化验证

### 4.1 形式化验证简介

嵌入式实时操作系统的本质是复杂性、多样性和可靠性。**RMP** 操作系统的硬件无关部分包括大约 2000 行代码，各个部分之间具有较复杂的作用和联系方式。作为一个操作系统又要应付不同应用的各种需求，并且需要保证功能的正确性。同时，我们还需要提高开发效率，控制成本和开发周期，以及保证软件的顺利交付。

传统的软件设计方法基于自然语言的思考、设计和描述，往往片面和模糊，极易引起误解。它也无法进行严格的检查，只能通过人的心智进行分析。基于 **UML** 等半形式化的方法采用一些相对清晰的图形化描述，一些工具也能自动生成代码框架并检查分析。以上两种方法在测试系统时，均是设计一系列用例对其进行测试，最多有结构化测试的参与。但是，它们都无法保证系统中没有错误，均不适用于性命攸关的系统的分析和开发，因此我们需要更为严格的开发设计流程。完全的形式化方法则基于严格定义的数学概念和语言，可以开发自动化工具进行检查和分析。它把数学的严格性带入软件开发的各个阶段，通过严格的数学证明保证系统中没有漏洞。

软件安全性的 **EAL** 标准分为 7 个等级<sup>[1]</sup>，分别如下<sup>[1]</sup>：

表 4-1 EAL 等级及其描述

EAL 级别	描述
EAL1	<b>EAL1</b> 是经过功能性测试的系统。它提供基本的安全保障目标描述。这些描述中包含了系统的功能规范和潜在错误分析。在 <b>EAL1</b> 中，每一个安全保障目标都要列出并且评估测试。相比于未评估系统， <b>EAL1</b> 仅仅是一个小规模的安全提升。
EAL2	<b>EAL2</b> 是使用基本软件工程方法论进行结构化开发的系统。它提供全面的安全保障目标描述。这些描述中包含了系统的基本功能规范和基本安全架构。在 <b>EAL2</b> 中，每一个安全保障目标都要列出并且进行独立的评估测试；此外还需要有一定攻击能力的安全测试人员对这些安全保障目标进行攻击，以确定没有问题。 <b>EAL2</b> 相比于 <b>EAL1</b> 有更严格的测试规范和系统弱点分析。
EAL3	<b>EAL3</b> 是使用强化的软件工程方法论进行系统性测试和检查的系统。它提供全面的安全保障目标描述。这些描述中包含了系统的基本功能规范和安全架构的详细设计。在 <b>EAL3</b> 中，每一个安全保障目标都要列出并且进行独立的评估测试；此外还需要有一定攻击能力的安全测试人员针对安全架构的详细设计进行攻击，以确定没有问题。 <b>EAL3</b> 相比于 <b>EAL2</b> 有更严格的系统架构规范和相应的测试。
EAL4	<b>EAL4</b> 是使用强化的软件工程方法论进行系统性设计、测试和评估的系统。它提供全面的安全保障目标描述。这些描述中包含了系统的详细功能规范和安全架构的详细设计，还要包含一部分关键模块的划分和具体实现。在 <b>EAL4</b> 中，每一个安全保障目标都要列出并且进行独

<sup>[1]</sup> **EAL7+**也列入在内

立评估测试；此外还需要有高于平均水平攻击能力的安全测试人员针对安全架构的详细设计进行攻击，以确定没有问题。

EAL4 相比于 EAL3 有更严格的设计描述、实现审查和更强大的测试。

#### EAL5

EAL5 是使用半形式化方法进行设计和测试的系统。它提供全面的安全保障目标描述。这些描述中包含了系统的详细功能规范和安全架构的详细设计，还要包含半形式化方法描述的全部关键模块的划分和一部分模块的具体实现。在 EAL5 中，每一个安全保障目标都要列出并且进行独立评估测试；此外还需要有相当程度攻击能力的安全测试人员针对安全架构的详细设计进行攻击，以确定没有问题。

EAL5 相比于 EAL4 有半形式化的设计描述、更清晰的架构和更强大的测试。

#### EAL6

EAL6 是使用半形式化方法进行设计、测试和验证的系统。它提供全面的安全保障目标描述。这些描述中包含了系统的详细功能规范和安全架构的详细设计，还要包含全部关键模块的划分和全部模块的具体实现。EAL6 要求对于安全保障目标的策略有完整的形式化描述，对其功能则要有半形式化描述。具体的功能设计必须是模块化的、分层的、和简明的。在 EAL6 中，每一个安全保障目标都要列出并且进行独立评估测试；此外还需要有较强攻击能力的安全测试人员针对安全架构的详细设计进行攻击，以确定没有问题。

EAL6 相比于 EAL5 有更全面的设计分析和弱点测试、以及结构化的实现描述。

#### EAL7

EAL7 是形式化方法进行设计、测试和验证的系统。它提供全面的安全保障目标描述。这些描述中包含了系统的详细功能规范和安全架构的详细设计，还要包含全部关键模块的划分和全部模块的结构化的具体实现。EAL7 要求对于安全保障目标的策略有完整的形式化描述，对其功能则要有半形式化描述。具体的功能设计必须是模块化的、分层的、和简明的。在 EAL6 中，每一个安全保障目标都要列出并且针对实现进行完整的独立评估测试；此外还需要有极强攻击能力的安全测试人员针对安全架构的详细设计进行攻击，以确定没有问题。

EAL7 相比于 EAL6 有更进一步的形式化设计和更全面的测试。

#### EAL7+

EAL7+是严格形式化方法进行设计、测试和验证的系统。它提供全面的安全保障目标描述。这些描述中包含了系统的详细功能规范和安全架构的详细设计，还要包含全部关键模块的划分和全部模块的结构化的具体实现。EAL7+要求对于安全保障目标的功能和策略有完整的形式化描述。具体的功能设计必须是模块化的、分层的、和简明的，并且要证明具体的实现完全符合形式化描述本身。在 EAL7+中，每一个安全保障目标都要列出并且针对实现进行完整的独立评估测试，测试用例必须由形式化工具自动生成；此外还需要有极强攻击能力的安全测试人员针对安全架构的详细设计进行攻击，以确定没有问题。

EAL7+相比于 EAL7 有更进一步的形式化实现和形式化测试。

RMP 系统是采用 EAL7+标准设计和测试的。

绝大多数操作系统如 [FreeRTOS](#)、[Windows](#)、[Linux](#) 的认证级别都在 [EAL4](#)。少数几款其他系统的认证在 [EAL5](#)，[INTEGRITY-178B](#) 的认证级别在 [EAL6+](#)。由于 [RMP](#) 的结构相对简单，而且其安全目标中只包括功能正确性目标而不包括信息安全目标<sup>[1]</sup>，因此较为容易取得更高的认证水平。

## 4.2 系统的形式化规范

在 [RMP](#) 中，由于架构相关部分非常短小<sup>[2]</sup>，容易保证其正确性，因此不对该部分进行形式化验证。另一个原因是架构相关部分往往随芯片而发生变化，而 [RMP](#) 要支持的平台多达数十，从人力成本上讲不方便对其一一建立形式化模型进行验证。因此，主要的验证工作集中在 [rmp\\_kernel.c](#) 文件的 1500 行代码上。注释不计算在内，约有 1000 行之多。基于同样的多架构支持原因，对这些代码的正确性，我们仅验证至 [C](#) 语言语义的层面，并不进行二进制指令级别的验证。这意味着，最终可执行文件的正确性仍然需要依赖于编译器的正确性。由于在实践中编译器通常具备较高的认证等级，因此信任编译器的做法是合理的。当然，如果不希望信任编译器，也可以采用经形式化验证的 [CompCert](#)<sup>[2]</sup> 编译器。

形式化验证并不能够完全杜绝软硬件系统错误操作的发生，尤其是硬件错误导致的问题<sup>[3]</sup>。对于硬件错误和硬件抽象层（Hardware Abstraction Layer, HAL）实现错误导致的系统失灵，[RMP](#) 的形式化验证是无能为力的。

## 4.3 形式化证明

将完成的后续工作。

## 4.4 其他文档

将完成的后续工作。

## 4.5 本章参考文献

[1] Common Criteria. "Common Criteria for Information Technology Security Evaluation", Part 3: Security assurance components, 2012.

[2] X. Leroy, "The CompCert verified compiler," Documentation and user manual. INRIA Paris-Rocquencourt, 2012.

---

<sup>[1]</sup> 多数 [CC/CAPP/LSPP](#) 等设计规范不适用

<sup>[2]</sup> 往往在 50 行代码以内

<sup>[3]</sup> 比如 CPU 或外设的硅片错误，这些错误的描述常常可以在各个厂商的芯片勘误手册内找到

## 第 5 章 移植 RMP 到新架构

### 5.1 移植概述

操作系统的移植是指将一个操作系统加以修改从而使其能运行在一个新的体系架构上的工作。有时，我们也把使得能用一款新编译器编译该操作系统的工作叫做移植工作。相比较于 uC/OS 和 RT-Thread 等系统的移植，RMP 的移植是非常简单的。RMP 的所有代码都用相对符合 MISRA C 规范的 ANSI/ISO C89 代码写成，并包含有最小量的汇编，因此其移植工作仅仅需要几步。

在移植之前，我们要先做一些准备工作，以确定移植可以进行；然后，分别针对各个部分，编写相应的移植代码即可。最后，还可以用一些测试用例来测试系统是否正确移植成功。由于 RMP 的非架构相关部分代码经过了形式化验证，因此不要对非架构相关部分进行任何修改，否则会造成系统认证被破坏。

### 5.2 移植前的检查工作

#### 5.2.1 处理器

RMP 要求所选择的处理器具备至少两个中断向量和一个定时器。除此之外，RMP 对处理器没有其他任何要求。RMP 不能在少于 8kB 闪存存储器的平台上运行，也不能在低于 16 位的处理器上运行。如果要在这些平台上运行操作系统，采用基于状态机的 RMS 可能是一个更好的选择。如果所选择的处理器是多核的或具备 MMU，那么运行基于微内核的 RME 可能是一个更好的选择。RMP 不支持硬件堆栈机制，堆栈必须是由软件实现的<sup>[1]</sup>，而不能在处理器内部通过硬件实现<sup>[2]</sup>。

#### 5.2.2 编译器

RMP 要求编译器是 C89 标准的，并能够根据一定的函数调用约定生成代码。由于 RMP 的代码非常标准，也不使用 C 运行时库中的库函数，因此只要编译器符合 ANSI C89 标准即可。通常的 GCC、CLANG/LLVM、MSVC、ARMCC、ICC、IAR、TASKING 等编译器都是满足这个需求的。RMP 没有使用位段、enum 和结构体对齐等各编译器实现差别较大的编译器扩展，也尽量避开了 C 语言中的未定义操作，因此保证了最大限度的兼容性。

在使用编译器时，要注意关闭低质量编译器的死代码消除功能和链接时优化功能，最好也要关闭低质量编译器的循环不变量外提优化。不要使用任何激进的编译优化选项，在一般的编译器上，推荐的优化选项是 GCC -O2 或相当的优化水平。

#### 5.2.3 汇编器

RMP 要求汇编器能够引入 C 中的符号，并根据函数调用约定进行调用；此外，也要求汇编器产生的代码能够导出并根据函数调用约定被 C 语言调用。这通常是非常好满足的要求。如果编译器可以内联汇编，那么不需要汇编器也是可以的。

---

<sup>[1]</sup> 也即堆栈指针可以由用户修改，堆栈实现在内存中

<sup>[2]</sup> 这是 PIC 单片机等少数架构的典型实现方式

### 5.2.4 调试器

RMP 对调试器没有特别的要求。如果有调试器可用的话，当然是最好的，但是没有调试器也是可以移植的。在有调试器的情况下可以直接用调试器查看内核变量；在没有调试器的情况下，要先实现内核最底层的 `RMP_Putchar` 函数，实现单个字符的打印输出，然后就可以用该打印输出来输出日志了。关于该函数的实现请看下节所述。

## 5.3 RMP 架构相关部分介绍

RMP 的架构相关部分代码的源文件全部都放在 `Platform` 文件夹的对应架构名称下。如 `Cortex-M` 架构的文件夹名称为 `Platform/CortexM`。其对应的头文件在 `Include/Platform/CortexM`，其他架构以此类推。

每个架构都包含一个或多个源文件和一个或多个头文件。内核包含架构相关头文件时，总是会包含 `Include/rmp_platform.h`，而这是一个包含了对应架构顶层头文件的头文件。在更改 RMP 的编译目标平台时，通过修改这个头文件来达成对不同目标的相应头文件的包含。比如，要针对 `Cortex-M` 架构进行编译，那么该头文件就应该包含对应 `Cortex-M` 的底层函数实现的全部头文件。

在移植到其他架构时，可以用 `Cortex-M` 架构的底层作为一套模板并在它的基础上展开新架构的移植工作。

### 5.3.1 类型定义

对于每个架构/编译器，首先需要移植的部分就是 RMP 的类型定义。对于类型定义，只需要确定处理器的字长在编译器中的表达方法，使用 `typedef` 定义即可。需要注意的是，对于某些架构和编译器，`long`（长整型）类型对应的是两个机器字的长度，而非一个机器字；此时应当使用 `int` 类型来表达一个机器字的长度。对于另一些架构和编译器，`int` 是半个机器字的长度，`long` 是一个机器字的长度，此时应当注意用 `long` 来定义一个机器字。

在必要的时候，可以使用 `sizeof()` 运算符编写几个小程序，来确定该编译器的机器字究竟是何种标准。为了使得底层函数的编写更加方便，推荐使用如下的几个 `typedef` 来定义经常使用到的确定位数的整形。在定义这些整形时，也需要确定编译器的 `char`、`short`、`int`、`long` 等究竟是多少个机器字的长度。

表 5-1 类型定义一览

类型	意义
<code>rmp_s8_t</code>	一个有符号八位整形。 例子： <code>typedef char rmp_s8_t;</code>
<code>rmp_s16_t</code>	一个有符号十六位整形。 例子： <code>typedef short rmp_s16_t;</code>
<code>rmp_s32_t</code>	一个有符号三十二位整形。



	例子: <code>typedef int rmp_s32_t;</code>
<code>rmp_u8_t</code>	一个无符号八位整形。 例子: <code>typedef unsigned char rmp_u8_t;</code>
<code>rmp_u16_t</code>	一个无符号十六位整形。 例子: <code>typedef unsigned short rmp_u16_t;</code>
<code>rmp_u32_t</code>	一个无符号三十二位整形。 例子: <code>typedef unsigned int rmp_u32_t;</code>

对于 RMP 而言, 必须被定义的的类型定义一共有如下三个:

表 5-2 必要类型定义一览

类型	作用
<code>rmp_ptr_t</code>	指针整数的类型。这个类型应该被 <code>typedef</code> 为与处理器字长相等的无符号整数。 例子: <code>typedef unsigned long rmp_ptr_t;</code>
<code>rmp_cnt_t</code>	计数变量的类型。这个类型应该被 <code>typedef</code> 为与处理器字长相等的有符号整数。 例子: <code>typedef long rmp_cnt_t;</code>
<code>rmp_ret_t</code>	函数返回值的类型。这个类型应该被 <code>typedef</code> 为与处理器字长相等的有符号整数。 例子: <code>typedef long rmp_ret_t;</code>

### 5.3.2 宏定义

其次, 需要移植的是 RMP 的宏定义。RMP 的宏定义一共有如下几个:

表 5-3 宏定义一览

宏名称	作用
<code>EXTERN</code>	编译器的 <code>extern</code> 关键字。某些编译器可能具有不标准的 <code>extern</code> 关键字, 此时用这个宏定义来处理它。 例子: <code>#define EXTERN extern</code>
<code>RMP_WORD_ORDER</code>	处理器字长 <sup>[1]</sup> 对应的 2 的方次。比如, 32 位处理器对应 5, 64 位处理器对应 6, 依此类推。 例子: <code>#define RMP_WORD_ORDER 5</code>
<code>RMP_INIT_STACK</code>	初始线程堆栈起始地址。如果堆栈向下生长, 这就是堆栈的顶部; 如果堆

<sup>[1]</sup> 按 Bit 计算

宏名称	作用
	<p>栈向上生长，这就是堆栈的底部。</p> <p><code>RMP</code> 声明了另外两个宏 <code>RMP_INIT_STACK_HEAD(X)</code> 和 <code>RMP_INIT_STACK_TAIL(X)</code>，可以利用这两个宏来实现。前者的意义是从内核中定义的初始线程堆栈头部开始往后部偏移一段距离，后者则是从后部向前部偏移一段距离，距离的单位是机器字长。</p> <p>例子：</p> <pre>#define RMP_INIT_STACK RMP_INIT_STACK_TAIL(16)</pre> <p>从初始堆栈数组的后部向前部偏移 16 个机器字长。</p>
<code>RMP_INIT_STACK_SIZE</code>	<p>初始线程堆栈大小，单位为字节。</p> <p>例子：</p> <pre>#define RMP_INIT_STACK_SIZE 1024</pre>
<code>RMP_MAX_PREEMPT_PRIO</code>	<p>内核支持的抢占优先级的最大数量。这个数字必须大于等于 3。在实践中，如果内存不是特别紧张，推荐配置为处理器字长<sup>[1]</sup>的整数倍。通常而言，把这个值定义为处理器字长就可以了。</p> <p>例子：</p> <pre>#define RMP_MAX_PREEMPT_PRIO 32</pre>
<code>RMP_MAX_SLICES</code>	<p>内核允许的线程时间片或延时时间片的最大数量。</p> <p>例子：</p> <pre>#define RMP_MAX_SLICES 100000</pre>
<code>RMP_SEM_MAX_NUM</code>	<p>内核允许的信号量计数的最大数量。</p> <p>例子：</p> <pre>#define RMP_SEM_MAX_NUM 100</pre>
<code>RMP_USE_HOOKS</code>	<p>是否使用钩子函数。如果使用钩子函数，那么用户需要提供 <a href="#">2.5.3</a> 中所述的四个额外钩子函数的实现。</p> <p>例子：</p> <pre>#define RMP_USE_HOOKS RMP_TRUE</pre>
<code>RMP_MASK_INT()</code> <code>RMP_UNMASK_INT()</code>	<p>是否在锁调度器时屏蔽能调用中断发送函数的中断。如果不使用该功能，这两个宏可以定义为空，此时调用中断发送函数的一系列中断仍然可能在锁调度器时发生，但它们的中断发送函数均会因调度器被锁而出错。如果使用该功能，<code>RMP_MASK_INT()</code> 可以定义为掩蔽所有系统中断，而 <code>RMP_UNMASK_INT()</code> 可以定义为解除系统中断掩蔽，这样就能保证那些调用中断发送函数的中断在锁调度器期间不发生。当然，处理器不具备该</p>

<sup>[1]</sup> 按 Bit 计算



宏名称	作用
	功能时也可将两宏简单定义为开关全局中断,但这样做会影响系统的实时性。
	例子:
	<pre>#define RMP_MASK_INT      MASK(SYSPRIO) #define RMP_UNMASK_INT    MASK(0x00)</pre>
	更详细的例子请参看 Cortex-M3 处理器上的 RMP 移植。 <code>MASK(SYSPRIO)</code> 的意义是掩蔽所有的优先级为 <code>SYSPRIO</code> 及以下的中断, <code>MASK(0x00)</code> 则为解除所有掩蔽。具体的 <code>SYSPRIO</code> 值应该被定义为能调用中断发送函数的中断的优先级的最高值。

### 5.3.3 底层汇编函数

RMP 仅要求用汇编或内联汇编实现 4 个短小的底层汇编函数。这些函数的名称和意义如下:

表 5-4 底层汇编函数一览

函数名	意义
<code>RMP_Disable_Int</code>	禁止处理器中断。
<code>RMP_Enable_Int</code>	使能处理器中断。
<code>_RMP_Yield</code>	触发线程切换。
<code>_RMP_Start</code>	启动初始线程。

这些函数的具体实现方法和实现要求将在后面章节加以讲解。

### 5.3.4 系统中断向量

RMP 最低仅仅要求用汇编或内联汇编实现 2 个中断向量。这些中断向量的名称和意义如下:

表 5-5 系统中断向量一览

中断向量名	意义
系统定时器中断向量	处理系统定时器中断, 管理时间片使用。
线程上下文切换中断向量	处理线程上下文切换时使用。

这些中断向量的具体实现方法和实现次序将在后面章节加以讲解。

### 5.3.5 其他底层函数

这些底层函数涉及 RMP 的启动、调试等其他方面。这些函数可以用汇编实现，也可以不用汇编实现，也可以部分使用 C 语言，部分使用内联汇编实现。这些函数的列表如下：

表 5-6 其他底层函数一览

函数	意义
RMP_Putchar	打印一个字符到内核调试控制台。
RMP_MSB_Get	得到一个字的最高位（MSB）位置。
_RMP_Low_Level_Init	底层硬件初始化。
_RMP_Stack_Init	初始化某线程的线程栈。

## 5.4 底层汇编函数的移植

汇编底层函数的原型和移植要求详述如下。

### 5.4.1 RMP\_Disable\_Int 的实现

该函数需要关闭处理器的中断，然后返回。实现上没有特别需要注意的地方，通常而言只需要写一个 CPU 寄存器或者外设地址，关闭中断，然后返回即可。

表 5-7 RMP\_Disable\_Int 的实现

函数原型	void RMP_Disable_Int(void)
意义	关闭处理器中断。
返回值	无。
参数	无。

### 5.4.2 RMP\_Enable\_Int 的实现

该函数需要开启处理器的中断，然后返回。实现上没有特别需要注意的地方，通常而言只需要写一个 CPU 寄存器或者外设地址，开启中断，然后返回即可。

表 5-8 RMP\_Enable\_Int 的实现

函数原型	void RMP_Enable_Int(void)
意义	开启处理器中断。
返回值	无。
参数	无。

### 5.4.3 \_RMP\_Yield 的实现

该函数需要软件触发可悬起的线程切换中断向量。通常而言这是写入某个内存地址或者执行某条特殊指令。

表 5-9 \_RMP\_Yield 的实现

函数原型	void _RMP_Yield(void)
意义	软件触发可悬起的线程切换中断向量。
返回值	无。
参数	无。

#### 5.4.4 \_RMP\_Start 的实现

该函数实现从内核栈到线程栈的切换，仅在系统启动阶段的最后被调用。在此之后，系统进入正常运行状态。该函数只要将 [Stack](#) 的值赋给堆栈指针，然后直接跳转到 [Entry](#) 即可。该函数将永远不会返回。

表 5-10 \_RMP\_Start 的实现

函数原型	void _RMP_Start(rmp_ptr_t Entry, rmp_ptr_t Stack)
意义	开始执行初始线程。
返回值	无。
参数	<a href="#">rmp_ptr_t Entry</a>
	初始线程的入口地址，实际上就是 <a href="#">RMP_Init</a> 。
	<a href="#">rmp_ptr_t Stack</a>
	初始线程的栈地址。

## 5.5 系统中断向量的移植

[RMP](#) 系统需要移植两个中断向量，分别是系统定时器中断向量和线程上下文切换中断向量。系统定时器中断向量没有必须使用汇编编写的要求，而线程切换中断向量则必须使用汇编编写。

### 5.5.1 定时器中断向量

在定时器中断处理向量中，仅仅需要调用如下定时器中断处理函数：

表 5-11 定时器中断处理函数

函数原型	void _RMP_Tick_Handler(rmp_ptr_t Ticks)
意义	执行定时器中断处理。
返回值	无。

参数	<code>rmp_ptr_t Ticks</code> 在本次时钟中断与上次时钟中断之间经过的嘀嗒数。
----	---

这个函数是系统实现好的，无需用户自行实现。

### 5.5.2 线程上下文切换中断向量

线程上下文切换中断向量必须使用汇编编写，并且按顺序完成以下步骤：

1. 先切换到内核栈，再将 CPU 的基本寄存器全部压入线程栈；
2. 再调用 `RMP_Save_Ctx` 保存多余的上下文，如 FPU 寄存器组等；
3. 然后将现在的线程堆栈指针存入变量 `RMP_Cur_SP`；
4. 然后调用 `_RMP_Get_High_Rdy` 进行线程切换；
5. 然后将变量 `RMP_Cur_SP` 赋给现在的线程堆栈指针；
6. 再调用 `RMP_Load_Ctx` 恢复多余的上下文，如 FPU 寄存器组等；
7. 最后将 CPU 的基本寄存器全部从线程栈恢复，并切换到线程栈，退出中断。

其中 `RMP_Save_Ctx` 和 `RMP_Load_Ctx` 两个函数在第二章已经介绍过，在这里不再赘述。这里仅简要介绍线程上下文切换中断处理函数。

表 5-12 线程上下文切换中断处理函数

函数原型	<code>void _RMP_Get_High_Rdy(void)</code>
意义	执行线程上下文切换处理。该切换会更新变量 <code>RMP_Cur_SP</code> 和 <code>RMP_Cur_Thd</code> ，供上下文切换汇编段和其他内核函数使用。
返回值	无。
参数	无。

这个函数也是系统实现好的，无需用户自行实现。

## 5.6 其他底层函数的移植

在剩下的底层函数中，`RMP_Putchar` 和 `RMP_MSB_Get` 在第二章已经讨论过，我们在这里仅讨论 `_RMP_Low_Level_Init` 和 `_RMP_Stack_Init`。

### 5.6.1 底层硬件初始化

该函数初始化所有的底层硬件。在初始化中断系统时，应当把系统嘀嗒定时器的优先级设为最低，将线程切换中断的优先级设置得次低，并且两者不能和任何其他中断有嵌套关系。调用了 `RMP_Thd_Snd_ISR` 和 `RMP_Sem_Post_ISR` 的中断向量也不允许和其他中断向量出现嵌套关系。对于其他的中断向量，则没有此种约束，可以任意嵌套。

表 5-13 \_RMP\_Low\_Level\_Init 的实现

函数原型	void _RMP_Low_Level_Init(void)
意义	初始化包括 PLL、CPU、中断系统、系统嘀嗒计时器在内的所有系统基本硬件。
返回值	无。
参数	无。

### 5.6.2 初始化某线程的线程栈

该函数在系统中会被线程创建函数调用。由于线程切换中断的后半段会从该栈中弹出寄存器，因此这里应当按照同样的顺序放置各个寄存器，尤其是线程入口和参数。具体的序列依各个处理器而有不同，和线程切换中断中具体压栈弹栈的实现顺序也有关系。

表 5-14 \_RMP\_Stack\_Init 的实现

函数原型	void _RMP_Stack_Init(rmp_ptr_t Entry, rmp_ptr_t Stack, rmp_ptr_t Arg)
意义	填充线程的线程栈，以便在新线程第一次运行时模拟出返回至此处的假象。
返回值	无。
参数	<a href="#">rmp_ptr_t Entry</a> 该线程的入口。
	<a href="#">rmp_ptr_t Stack</a> 该线程的初始堆栈地址。
	<a href="#">rmp_ptr_t Arg</a> 给该线程传入的参数。

### 5.7 本章参考文献

无

第 6 章 附录

6.1 特殊内核功能的实现

在 RMP 中，有一部分功能没有被内核默认实现。但是在 RMP 中实现这些功能是可能的；具体的实现原理如下所列，如果用户需要这些功能则要自行实现。

6.1.1 无节拍内核的实现

无节拍内核通常要求系统具备一个高精度定时器，并且由该高精度定时器产生系统的调度器时间中断。此时只需要在系统上下文恢复钩子 `RMP_Sched_Hook` 和系统定时器钩子 `RMP_Timer_Hook` 中检查一遍当前选中的线程的剩余时间，再检查一遍最近超时的定时器的剩余时间，然后选择最小的那个剩余时间，将其设置成硬件定时器的下一次超时时间即可。内核为此提供了函数 `_RMP_Get_Near_Ticks` 用于得到这个数值。这个函数不是必须被调用的，如果不实现无节拍内核可以不必理会。如果这段时间的长度超过了硬件定时器能支持的范围，那么可以将这个时间长度分成几段来执行，比如将其保存在一个临时变量中，然后进行多轮延时。在每轮延时的定时器钩子中将其每次减去本轮延时时间，直到剩余时间可以在一轮之内用尽为止。

表 6-1 得到最近超时嘀嗒数

函数原型	<code>rmp_ptr_t _RMP_Get_Near_Ticks(void)</code>
意义	得到距离未来最近一次超时的嘀嗒数，可根据此设置系统定时器的下一次超时时间。
返回值	<code>rmp_ptr_t</code> 距离未来最近一次超时的嘀嗒数。
参数	无。

这个函数是系统实现好的，无需用户自行实现。

6.1.2 浮点处理器上下文的保存和恢复

要保存和恢复浮点处理器的寄存器，应当使用 `RMP_Save_Ctx` 和 `RMP_Load_Ctx` 两个钩子。在保存钩子内，先要探测当前线程是否使用了浮点寄存器，如果是那么保存浮点寄存器到堆栈或者其他地方。在恢复钩子内也要先探测浮点寄存器是否被使用，如果是的话那么需要从刚刚保存的地方恢复它。在 RMP 上，推荐的浮点处理器使用方法是仅仅让一个线程使用浮点处理器，这样就可以不必保存和恢复浮点处理器的上下文，从而提高系统的实时性和效率。

6.1.3 线程内存保护的实现

在微控制器中用于限制访问属性的通常是内存保护单元（Memory Protection Unit，MPU）。MPU 由一系列的寄存器组成，这些寄存器里面填充着各个被保护的内存区域的访问属性。每个线程可以拥有

一套不同的 MPU 寄存器设置，并以此来限制自己的访问属性。一个推荐的实现是将 MPU 的寄存器看作协处理器寄存器，也在 `RMP_Save_Ctx` 和 `RMP_Load_Ctx` 内保存和恢复。需要注意的是，每个线程的 MPU 设置都应当允许读写 RMP 的内核内存和执行 RMP 的代码；这是因为 RMP 没有真正的用户态和内核态，而且所有的系统调用都被直接实现为函数调用的缘故。也正是因为这个原因，基于 RMP 实现的内存保护仅能防止线程跑飞或者出错，而不具备任何信息安全属性。

#### 6.1.4 低功耗设计注意事项

在低功耗设计中，推荐使用无节拍内核，此外还要在 `RMP_Init_Idle` 钩子内插入能让处理器进入休眠状态的指令<sup>[1]</sup>。

### 6.2 RMP 中已知的影响实时性的因素

在 RMP 中已知的影响实时性的因素只有两个，分列如下。这两个因素在实际的应用程序中都很好避免；通常而言，如果因为这些因素使系统的实时性受到损伤，应用程序就不是良好设计的。

#### 6.2.1 延时队列

RMP 使用一个延时队列管理所有的延时<sup>[2]</sup>。这个延时队列从前向后，各线程的超时时间依次增加。这样，每次时钟中断，RMP 都只需要检查队列中的第一个线程即可。但是，这个设计要求每当插入线程时都要遍历队列找到合适的插入位置以使得线程超时时间仍然递增。这个遍历的最坏时间复杂度对队列中已有的线程数量是  $O(n)$  的。从数学上可以证明，不存在一种算法或数据结构能够使得定时器的所有操作总为  $O(1)$ ，因此这必然要求应用程序不要特别大量地使用延时等待或延时阻塞。

#### 6.2.2 锁调度器和关中断

RMP 提供了锁调度器和关中断的接口。但是，这对系统实时性是有显而易见的损害的，因此在应用程序中应当尽量避免此类操作。比如，如果已知只有一个线程会在某内存池中做操作，那么再分配和释放内存时就可以不用锁调度器。

### 6.3 缩减 RMP 的存储器占用

在内存特别宝贵的场合，有必要小心配置 RMP 以节省本就不多的 RAM 和 ROM。此种状况多见于 MSP430 等 16 位单片机和 Cortex-M0 等低端 32 位单片机上。在实践中，可以采用如下手法缩减 RMP 的内存占用：

#### 6.3.1 降低系统支持的优先级的数量

---

<sup>[1]</sup> 在 ARM 架构上，WFI 和 WFE 指令可以达到这个效果，而在 MSP430 处理器上则必须修改 STATUS 寄存器的某些位让处理器进入休眠。

<sup>[2]</sup> 也即 `RMP_Thd_Delay`

不同于其他的操作系统，RMP 的线程邮箱是零开支内建于线程之中的，而其它功能在不使用时则不占用任何存储。因此，RMP 的编译时选项中只有一个会决定其内核 RAM 占用大小。这个选项就是 RMP 支持的优先级个数<sup>[1]</sup>。由于 RMP 的每个优先级都使用一个双向循环链表来管理，因此每个优先级都会消耗 2 个机器字长的 RAM。在一些微型系统上，配置过多的优先级是完全没有必要的，因此可以将 RMP 支持的优先级调整成 3 个来最大限度节省 RAM。在这种用例下，RMP 本身的 RAM 消耗甚至可以被挤压到 130 字节以内<sup>[2]</sup>。

### 6.3.2 调整厂商提供的库

某些厂商提供的 HAL 库和启动文件可能会静态分配一些堆和栈<sup>[3]</sup>。在使用 RMP 的场合，厂商分配的堆是完全没有必要的，可以置 0；而厂商分配的栈则会被 OS 内核在响应中断时使用<sup>[4]</sup>，因此只要确认中断处理程序的最大栈消耗，然后将厂商分配的栈大小设置到比这一数字稍多<sup>[5]</sup>即可。此外，HAL 库中不用到的文件可以不包括进工程，这也有助于减少 RAM 和 ROM 用量。如果 HAL 库占用的存储器不可忍受，那么也可以不使用 HAL 库而选择直接读写外设寄存器。

### 6.3.3 调整编译器选项

通过调整编译器选项，也有可能减小 ROM 和 RAM 占用。调整编译器选项为代码体积优化对减小 ROM 占用尤其有效，对减小 RAM 占用有时也有效果。

### 6.3.4 不使用动态内存管理

RMP 内建了一个动态内存分配器。该分配器在小内存设备上不推荐使用，因为分配器本身也会有一定的固定内存消耗。在小内存设备上，推荐静态分配所有的内核对象和变量。

## 6.4 本章参考文献

无

---

<sup>[1]</sup> 也即 RMP\_MAX\_PREEMPT\_PRIO

<sup>[2]</sup> 如果不算内核中断响应堆栈，那么实际大小是 66 字节

<sup>[3]</sup> 比如 Cortex-M 系列微控制器的汇编启动文件的最前面

<sup>[4]</sup> 也即作为内核栈使用

<sup>[5]</sup> 一般推荐多几十字节