应用笔记

N32G033系列60730 ClassB应用笔记

简介

安全在电子应用领域起着越来越重要的作用。在电子设计中，组件的安全要求水平不断上升，电子设备制造商将很多新技术解决方案纳入了新组件设计。用于提高安全的软件技术不断涌现。硬件和软件的安全要求相关标准也在持续开发中。

国民技术提供了安全相关自测库，本文档介绍了该工程在 MCU 中如何执行 IEC 60730 所要求的软件安全性相关的操作及相关应用代码内容。

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900　　传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

目录

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

表目录

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

图目录

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

1 概述

为确保电器使用安全，需要对软件运行时的风险控制措施进行评估，国际电工委员会颁布的 IEC60730 标准引入了家用电器软件评估要求，附录 H(H.2.21)中对软件进行了分类：

A 类软件：软件仅实现产品的功能，不涉及产品的安全控制。比如室用恒温器的软件，灯光控制的软件；

B 类软件：软件的设计要防止电子设备的不安全操作。例如带自动门锁控制的洗衣机软件，带过热控制的电磁炉软件；

C 类软件：软件的设计为了避免某些特殊的危险。例如自动燃烧器控制和封闭的热水器的热切断（主要针对一些会引起爆炸的设备）。

其中 B 类软件的具体评估要求，包含了需要检测的组件及相关故障和测试方案，根据 IEC60730 Class-B 认证需求，国民提供了 STL 库，以帮助用户快速导入产品。

本文旨在描述 STL 库对 CPU、Clock、FLASH、RAM 等关键组件的检测需求，以确保用户产品系统具有足够的可靠性和安全性。参考 IEC60730 表 H.11.12.7，包含了需要检测的组件及相关故障和测试方案，整理见下表：

表 1-1 IEC60730 表 H.11.12.7 描述

需要检测的组件		故障/错误	故障分类	国民 STL 库	测试方案概述
1.CPU	1.1 寄存器	滞位(Stuck at)	MCU 相关	是	写相关寄存器并检查
	1.3 程序计数器	滞位(Stuck at)	MCU 相关	是	PC 跑飞则启动看门狗复位
2.中断		没有中断或者中断太频繁	应用相关	否	计算进中断次数
3.时钟		错误的频率	MCU 相关	是	使用 HSI 测 LSI 时钟频率
4.存储器	4.1 非易失存储器	所有的单比特错误	MCU 相关	是	FLASH CRC 完整性校验
	4.2 易失存储器	DC fault	MCU 相关	是	1. SRAM March C测试 2. 堆栈溢出检测
	4.3 寻址（与非易失和易失存储器相关）	滞位(Stuck at)	MCU 相关	是	FLASH/SRAM 测试已包含
5.内部数据路径	5.1 数据	滞位(Stuck at)	MCU 相关	否	仅针对使用外部存储器的 MCU，单片 MCU 不要求
	5.2 寻址	错误的地址	MCU 相关	否	
6.外部通信	6.1 数据	汉明距离 3	应用相关	否	数据传输中增加校验
	6.2 寻址	错误的地址	应用相关	否	
	6.3 时序	错误的时序	应用相关	否	计算通信事件的次数
7.输入输出	7.1 数字 I/O	H27 中定义的错误	应用相关	否	无
	7.2 模拟输入输出	H27 中定义的错误	应用相关	否	无

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

2 术语和缩写

2.1 本文档使用的术语和缩写

表 2-1 术语和缩写

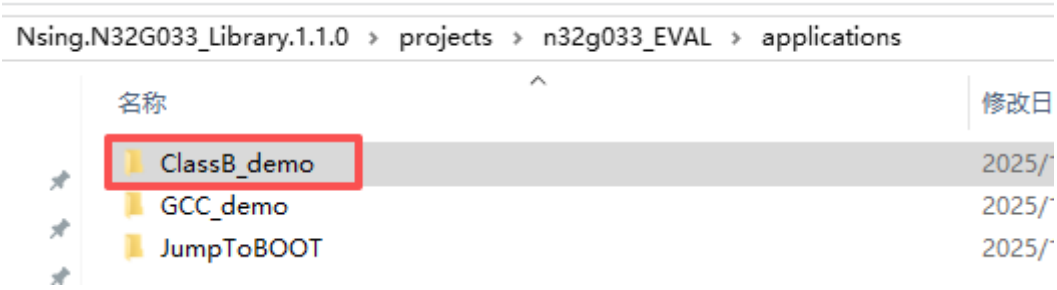
编号	术语&缩写	说明
1	N32	国民技术 32 位芯片
2	MCU	微控制器单元
3	CPU	中央处理器单元
4	STL	自检库
5	RAM	随机存取存储器
6	CRC	循环冗余校验
7	IO	输入输出接口
8	USARTx	通用同步异步收发器，x 指示序号，如 USART1
9	LSI	低速内部时钟
10	TIMx	定时器，x 指示序号，如 TIM7

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

3 软件包架构

该应用笔记代码部分随 SDK 发布，工程目录如下（以 Nsing.N32G033_Library.1.1.0 版本为例）：

图 3-1 SDK 应用笔记位置



Class B 检测诊断软件包，基于 N32 MCU 芯片固件库的文件结构，添加集成 IEC60730 安全检测相关代码。软件包文件夹总体结构框架如下表所示：

表 3-1 Class B 软件包结构

主目录	二级目录	备注
firmware	CMSIS	内核相关驱动
	n32g033_std_periph_driver	N32G033 系列外设驱动
middlewares	N32_SelfTest_Library	N32 MCU STL 代码库
projects	n32g033_EVAL/applications/ClassB_demo	基于评估板的集成示例，包含 Keil® 和 IAR™ 工程

特定的 N32 MCU 产品及评估板的所含项目已开发完备，并在以下开发环境和工具链下进行了测试：

- Keil®/MDK-ARM® v5.34 版本
- IAR™-EWARM v8.50.1 版本

3.1 软件架构设计说明

STL 软件由芯片外设驱动 libraries、Class B STL 和 user application 组成，其中 Class B STL 分为两个主要部分：启动阶段的测试和运行阶段的周期性测试。

3.2 软件架构框图

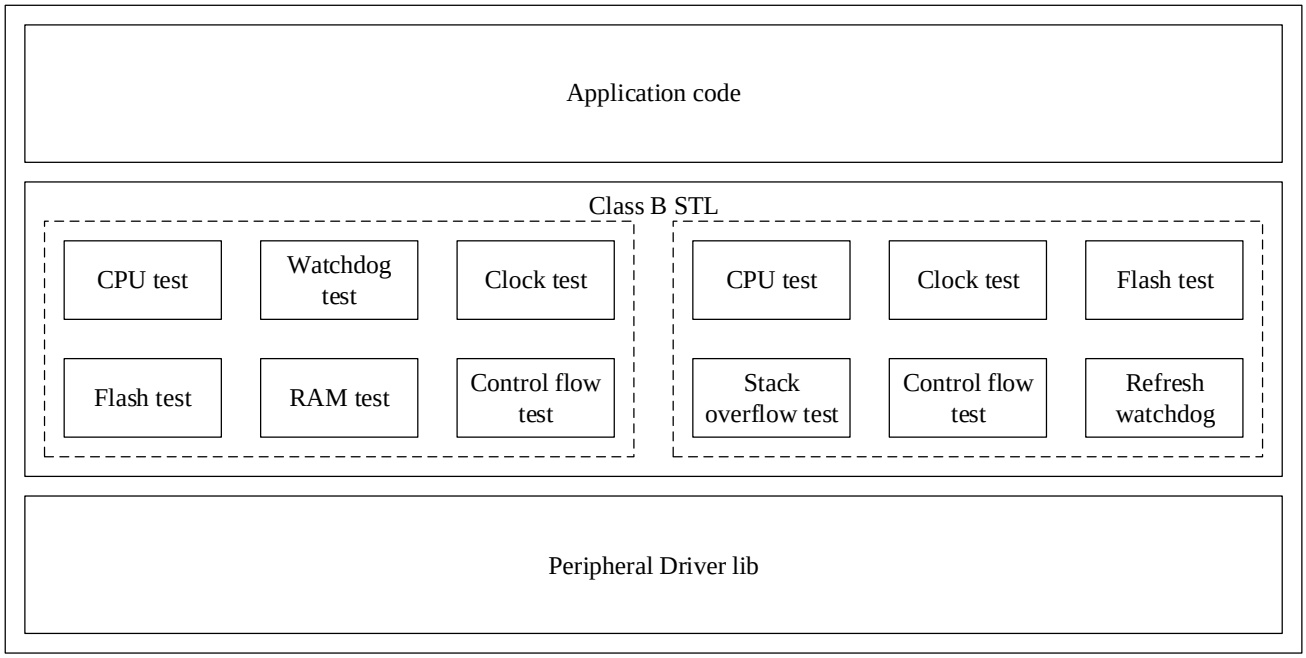
STL 软件架构整体框图如图 3-2 所示。

其中，Class B STL 中的两个部分分别包含：

- 启动阶段的 CPU 测试、看门狗测试、时钟测试、Flash 测试、RAM 测试和控制流测试
- 运行阶段的周期性 CPU 测试、时钟测试、Flash 测试、栈溢出测试、控制流测试和刷新看门狗

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

图 3-2 软件架构框图



国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

4 软件包组件

软件包组件包含通用部分和特定部分。下文各表列出了对应的文件及其描述。

4.1 软件组件概要

通用 STL 软件组件文件描述如下表所示：

表 4-1 通用 STL 软件文件描述

STL	通用 STL 源和头文件	
	文件	描述
启动阶段 API	n32_cm0_STLstartup.c	用于启动阶段 STL 流程控制的相关代码
运行阶段 API	n32_cm0_STLmain.c	用于运行阶段 STL 流程控制的相关代码
STL 源文件	n32_cm0_STLclock.c	用于时钟测试的相关代码
	n32_cm0_STLcrc32.c	用于 Flash CRC 测试的相关代码
	n32_cm0_STLtranspRam.c	用于 RAM 测试的相关代码
	n32_cm0_STLcpurunKEIL.s	用于启动和运行阶段 CPU 和 RAM 测试的相关代码，由汇编语言编写，分别针对 Keil®和 IAR™
	n32_cm0_STLcpustartKEIL.s	
	n32_cm0_STLRamMcMxKEIL.s	
	n32_cm0_STLcpurunIAR.s	
	n32_cm0_STLcpustartIAR.s	
	n32_cm0_STLRamMcMxIAR.s	
头文件	n32_cm0_STLparam.h	用于 STL 相关功能变量用户自定义的头文件
	n32_cm0_STLclassBvar.h	用于 Class B 类变量声明的头文件
	n32_cm0_STLclock.h	用于时钟测试的头文件
	n32_cm0_STLcpu.h	用于 CPU 测试的头文件
	n32_cm0_STLcrc32.h	用于 Flash CRC 测试的头文件
	n32_cm0_STLlib.h	用于所有源文件 include 的头文件，为其他头文件的集合
	n32_cm0_STLmain.h	用于运行阶段 STL 流程控制的头文件
	n32_cm0_STLRam.h	用于 RAM 测试的头文件
	n32_cm0_STLstartup.h	用于启动阶段 STL 流程控制的头文件

4.2 软件组件接口定义

STL 软件包组件中供用户调用的接口定义分别如下变所示：

表 4-2 STL 接口定义

No.	Name	Interface definition	Type	Remarks
1	STL_VerbosePORInit	初始化用于串口打印的 USART 以及测试中用到的 IO 管脚	void	示例中用的是 UART1
2	STL_StartUp	启动阶段的自检流程	void	此阶段运行于复位与应用（main 函数）之间
3	STL_InitRunTimeChecks	初始化 B 类变量及其反向冗余对应变量，以及初始化用于时钟频率监控的定时器	void	SysTick 生成 1ms 时基

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

No.	Name	Interface definition	Type	Remarks
4	STL_DoRunTimeChecks	运行阶段的自检流程	void	周期性的调用运行，示例中调用执行周期为 20ms
5	SysTick_Handler	SysTick 中断处理函数	void	包含 RAM March 检查流程，但执行周期与运行阶段的自检流程的执行周期相同（示例为 20ms）
6	FailSafePOR	错误处理函数	void	提供三种错误处理方式： 1. 软件复位 2. IWDG 喂狗 3. WWDG 喂狗

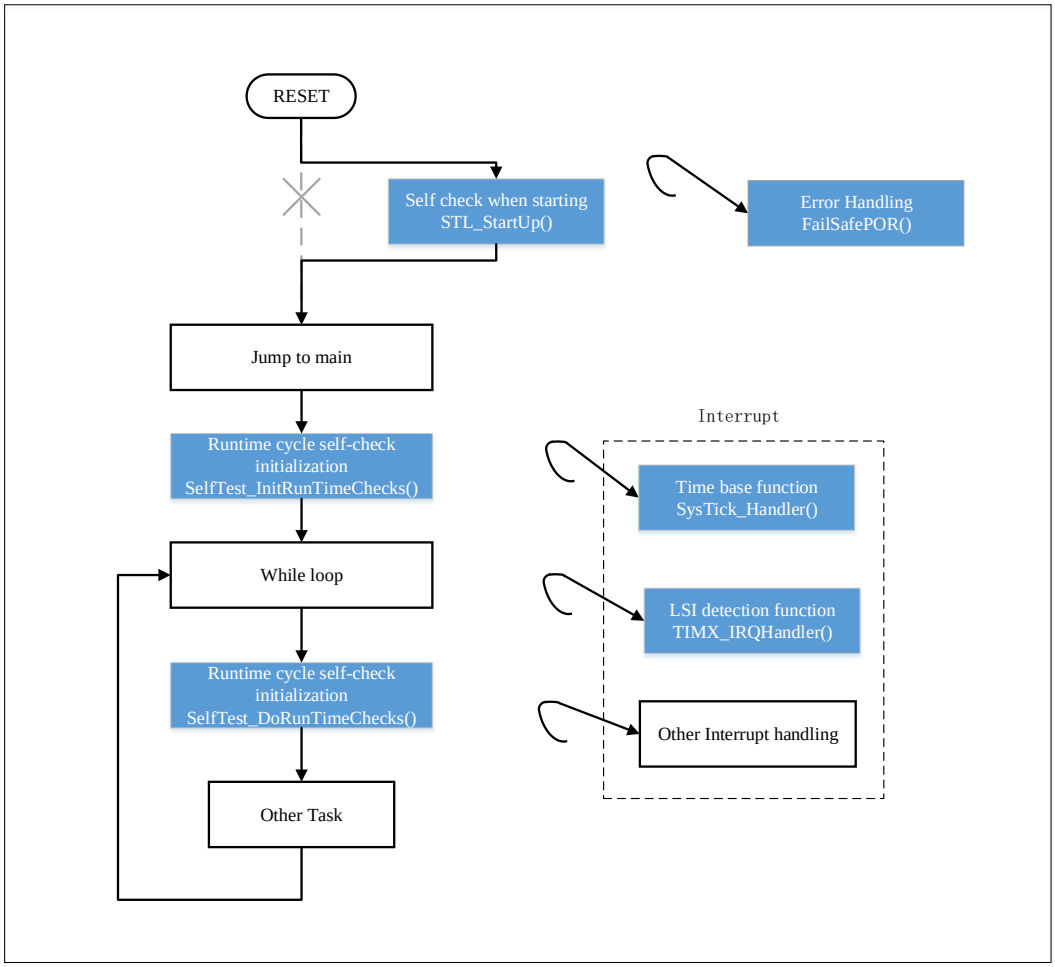
国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

5 软件包设计

5.1 模块详细设计说明

Class B软件包程序检测内容分为两个主要部分：启动时的自检和运行时的周期自检。总体流程框图如下图所示，图中蓝色框图是相对于原应用程序，执行Class B需添加的部分：

图 5-1 软件包流程框图



MCU 复位后，执行首次检查时，需在应用程序执行前运行 STL_StartUp()自检程序；自检完成进入 main 函数，在进入主循环前先调用 STL_InitRunTimeChecks()做周期性自检的初始化配置；在 systick 中断中调用 STL_InterruptRunTimeChecks() 做 RAM 检测并获取周期检测的时基，然后在主循环中调用 STL_DoRunTimeChecks()做周期性自检。

注意：运行时如果自检程序耗时太长，可以将自检流程进行拆分，用 systick 中断进行周期性的自检。

原则上，将自检模块集成到应用程序中，用户需要提供以下步骤：

- 用户程序开始前执行自检测试
- 定期执行专门时间段（与安全时间相关）设置的运行时自检
- 应用运行时，设置独立和窗口看门狗，以防止其到期（可通过 STL 测试实际运行周期对其刷新进行微调）

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

- 为 RAM 和 Flash 的启动和运行时测试设置正确的测试区
- 注意测试的错误结果，并进行合适的操作来保证系统的安全
- 防止可能与应用 SW 发生的冲突（尤其是中断、DMA、CRC 等）
- 排除所有与任何安全任务不相关的调试功能，仅将其用于调试或测试

5.2 启动时检测流程

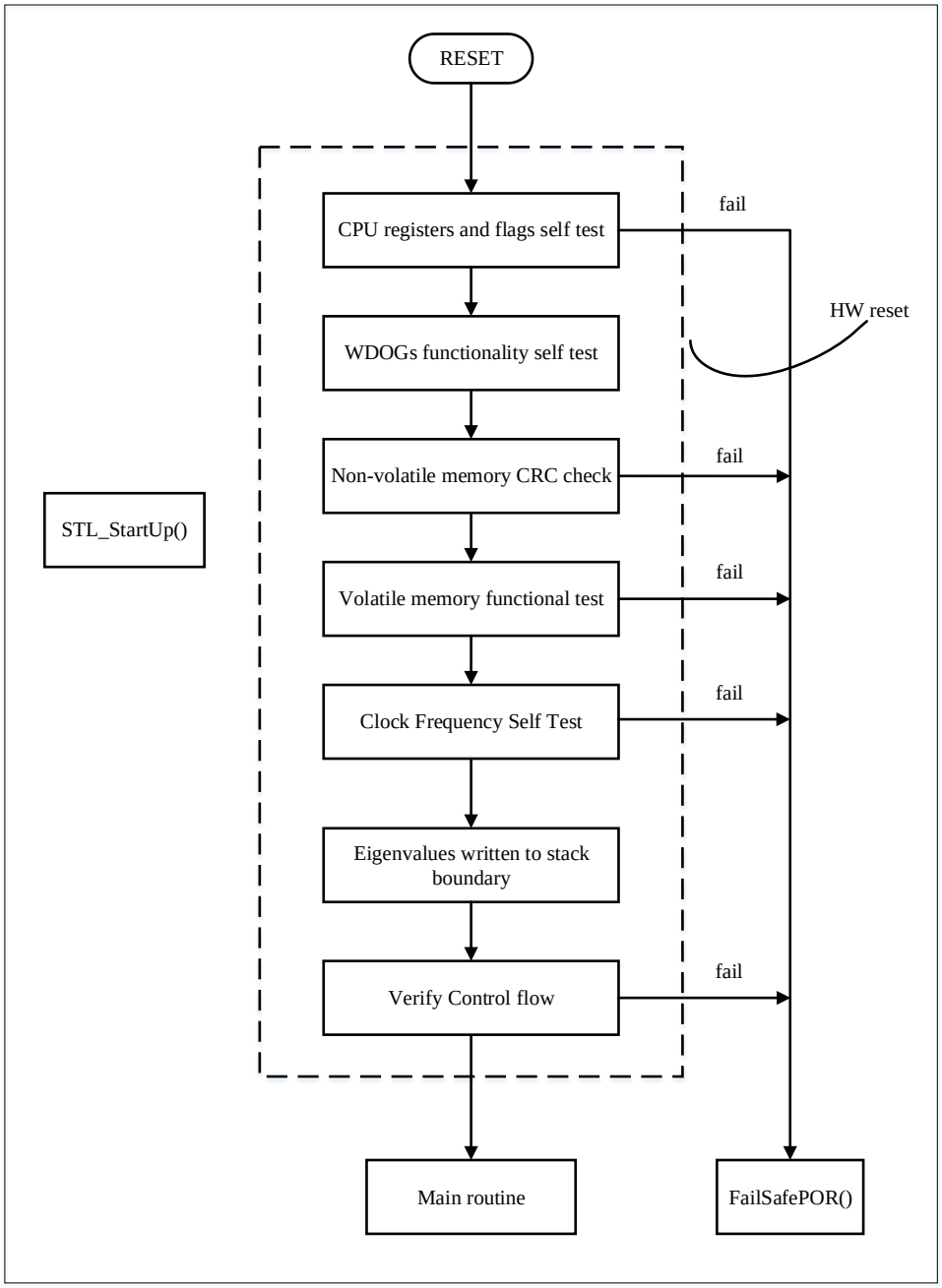
在芯片由启动到进入main函数之前，先进行启动检测。
启动时的自检包括：

- CPU检测
- 看门狗检测
- Flash完整性检测
- RAM功能检测
- 交叉时钟检测
- 特征值写入栈边界
- 控制流检测

下图是执行启动时自检的流程框图：

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

图 5-2 启动时自检流程框图



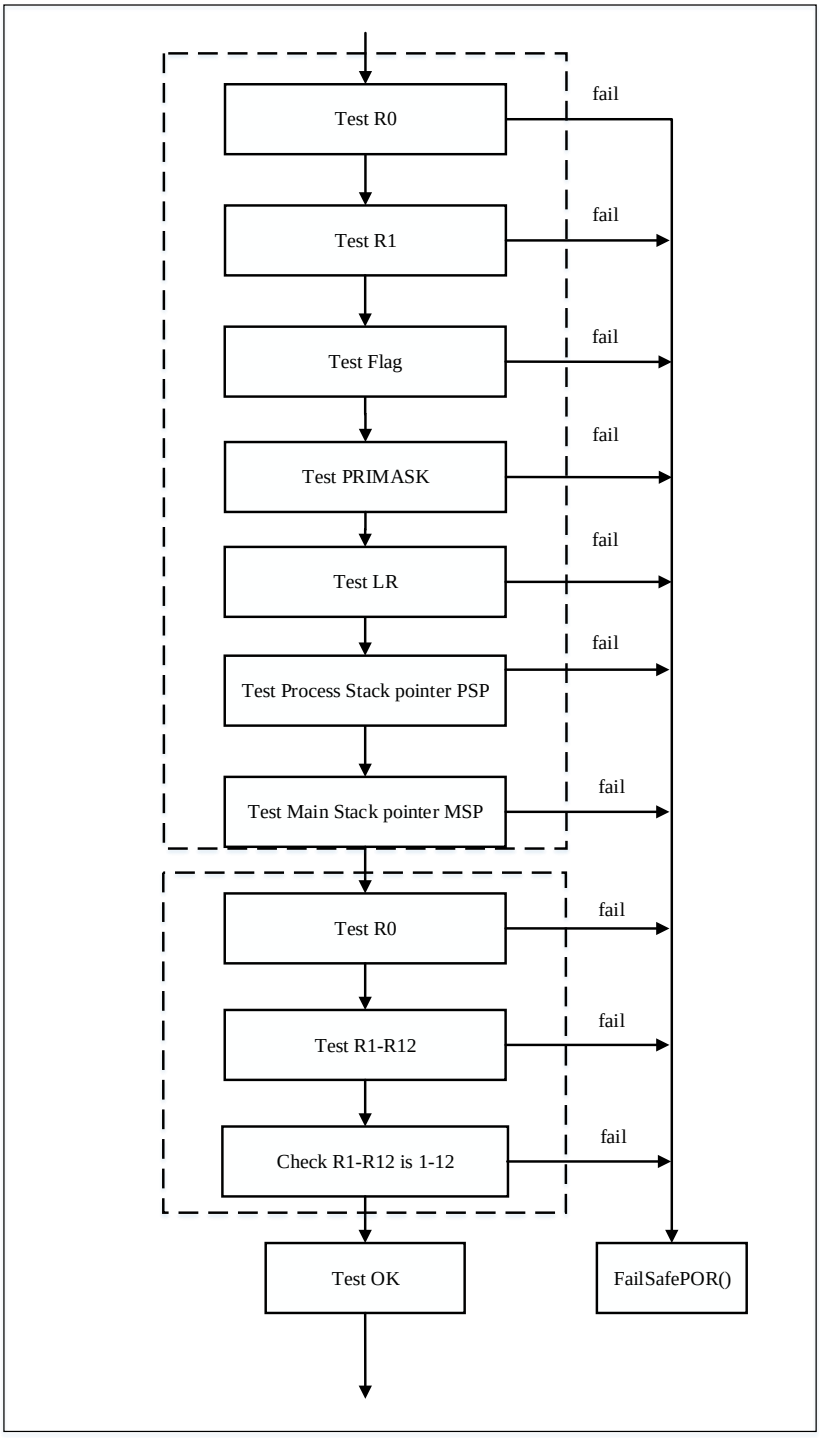
5.2.1 CPU 启动时检测

CPU上电自检主要检查内核标志、寄存器等是否正确。如果发生错误，就会调用故障安全处理函数FailSafePOR()。

在启动时，R0~R12、LR、PSP、MSP、PRIMASK、FAULTMASK、BASEPRI寄存器和APSR寄存器的Z(zero)、N(negative)、C(carry)、V(overflow)、Q(saturation)标志位的功能测试都会进行一次自检。

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

图 5-3 CPU 启动时检测流程框图



5.2.2 看门狗启动时检测

测试确认独立看门狗及窗口看门狗能正确复位，以确保在程序运行时跑飞能及时复位防止卡死。测试流程如下：

1 判断 IWDG 复位标志没有置起，如果是则跳转到步骤 2 开始 IWDG 测试，否则跳转到步骤 3；

2 清除所有复位标志，开始 IWDG 测试，使能 IWDG，不喂狗等待复位；

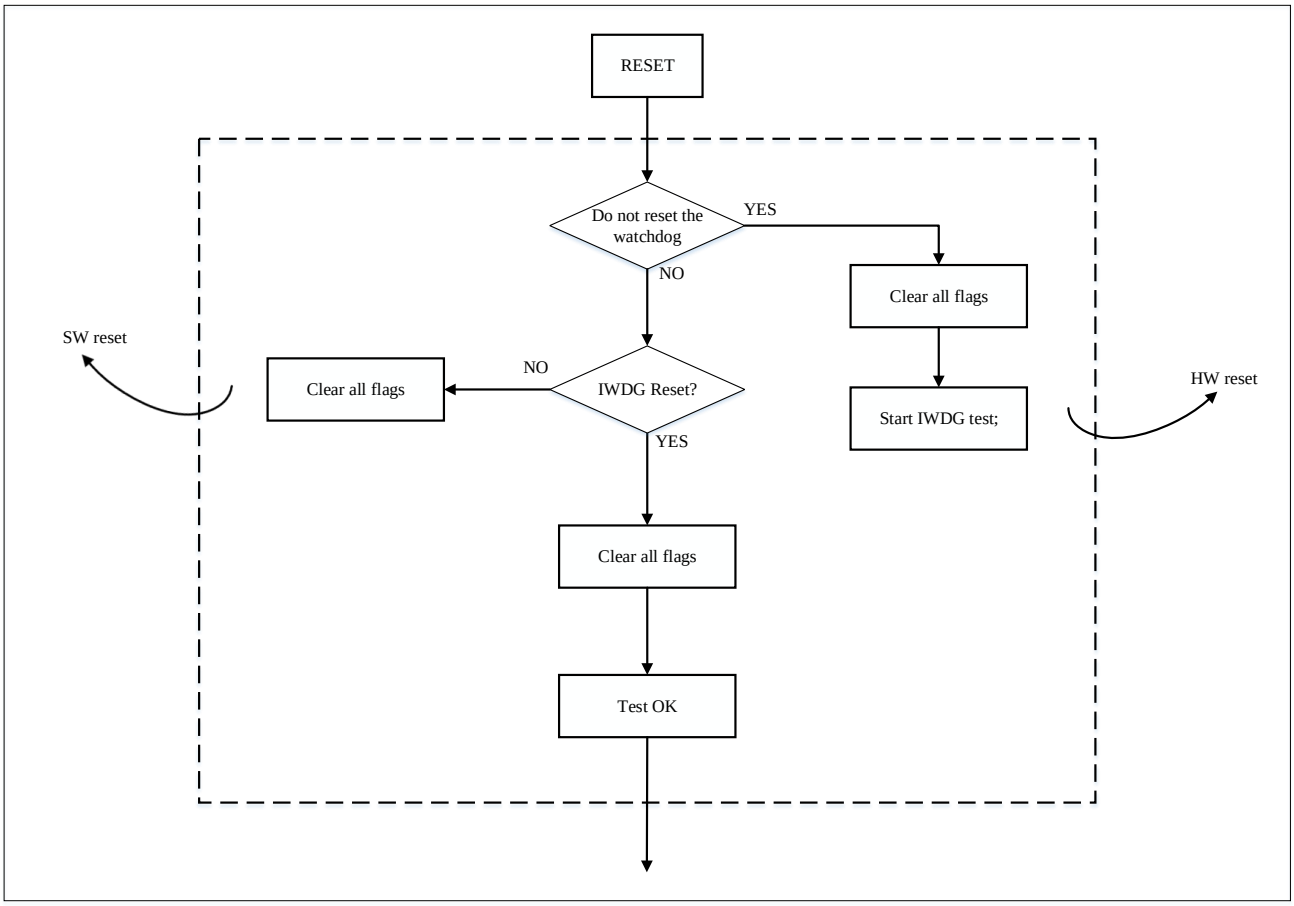
国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

3　判断 IWDG 复位标志是否置起，如果是则跳转到步骤 4，否则清除所有复位标志并软件复位；

4　清除所有复位标志，测试通过。

流程框图如下：

图 5-4 看门狗启动时检测流程框图



5.2.3 FLASH 启动时检测

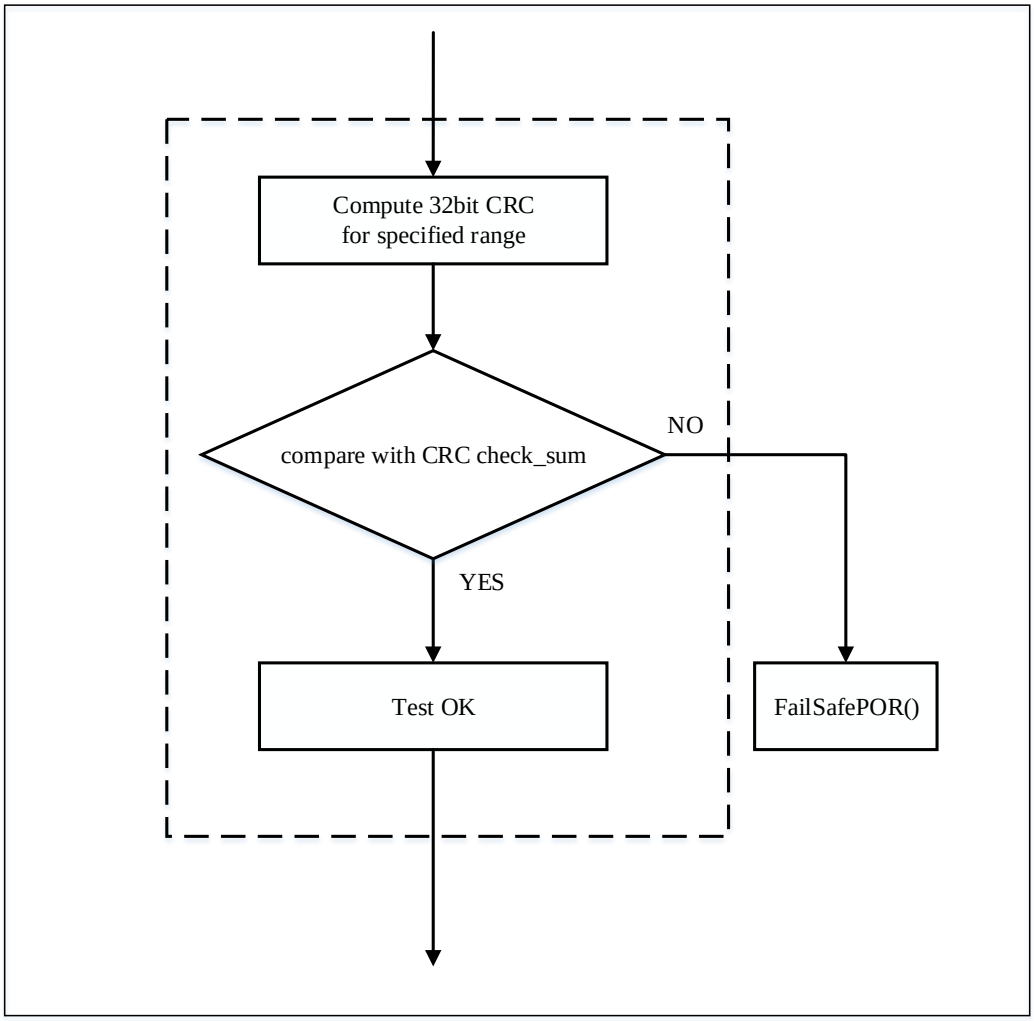
FLASH自检是在程序中对FLASH数据使用CRC算法进行计算，将结果值跟编译时计算好并且存储在FLASH指定位置的CRC值进行比较，以此确认FLASH完整性。

同时，在启动检测时会提前对CRC32数据寄存器进行检测：复位CRC后，对数据寄存器写0x55555555，判断校验结果是否为0x85F89652，再次复位CRC，对数据寄存器写0xAAAAAAAA，判断校验结果是否为0x42FC4B29。

流程框图如下：

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900　　传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

图 5-5 FLASH 启动时检测流程框图



其中CRC计算的FLASH范围根据整个程序的实际情况进行配置，并且需要保证检测范围为64字节的整数倍。

Flash的CRC值需要在调试或者烧录阶段跟正常应用代码一起下载到芯片Flash，所以需要在集成开发环境(IDE)编译生成的HEX中进行添加CRC，下面分别介绍Keil、IAR如何配置。

IAR配置：

IAR配置选项中支持CRC计算，只需要配置好参数，编译生成的文件就会自动将CRC校验结果check_sum值添加到选定FLASH计算范围后面。

客户根据实际应用配置IAR工程选项及SelfTest.icf文件，举例如下：

CRC计算范围为0x8000000~0x800FEFF，检验结果存储位置为0x800FF00

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

图 5-6 IAR CRC 计算配置示例

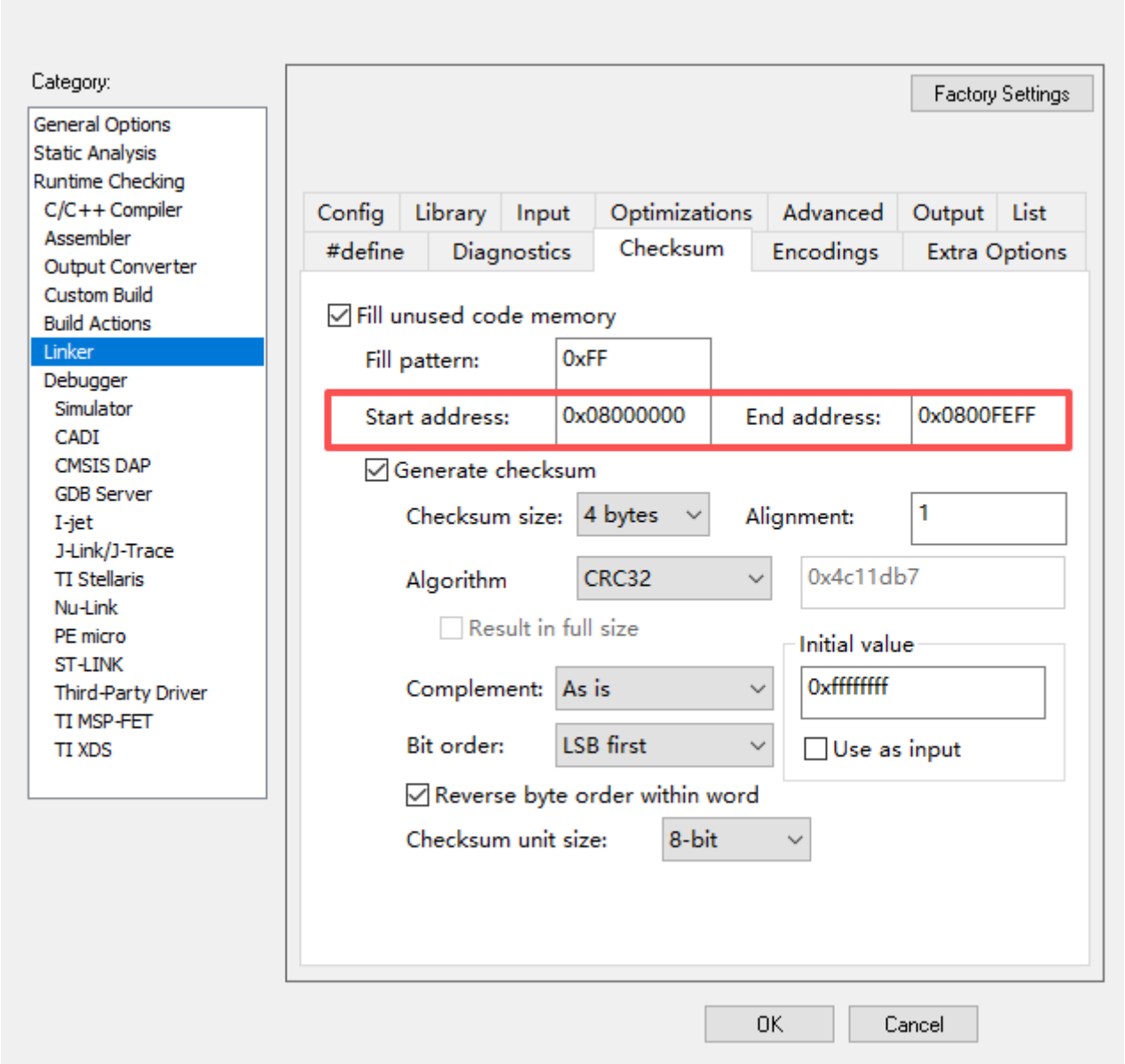


图 5-7 SelfTest.icf 文件

```
SelfTest.icf  srecord_crc32.bat  SelfTest.map
1  /*###ICF### Section handled by ICF editor, don't touch! ****/
2  /*-Editor annotation file-*/
3  /* IcfEditorFile="$TOOLKIT_DIR$\config\ide\IcfEditor\cortex_v1_0.xml" */
4  /*-Specials-*/
5  define symbol __ICFEDIT_intvec_start__ = 0x08000000;
6  /*-Memory Regions-*/
7  define symbol __ICFEDIT_region_ROM_start__ = 0x08000000;
8  define symbol __ICFEDIT_region_ROM_end__   = 0x0800FF03;  /* Modify according to needs,Contains crc results */
9  define symbol __ICFEDIT_region_RAM_start__ = 0x20000000;
10 define symbol __ICFEDIT_region_RAM_end__   = 0x20003FF0;  /* Modify according to needs */
```

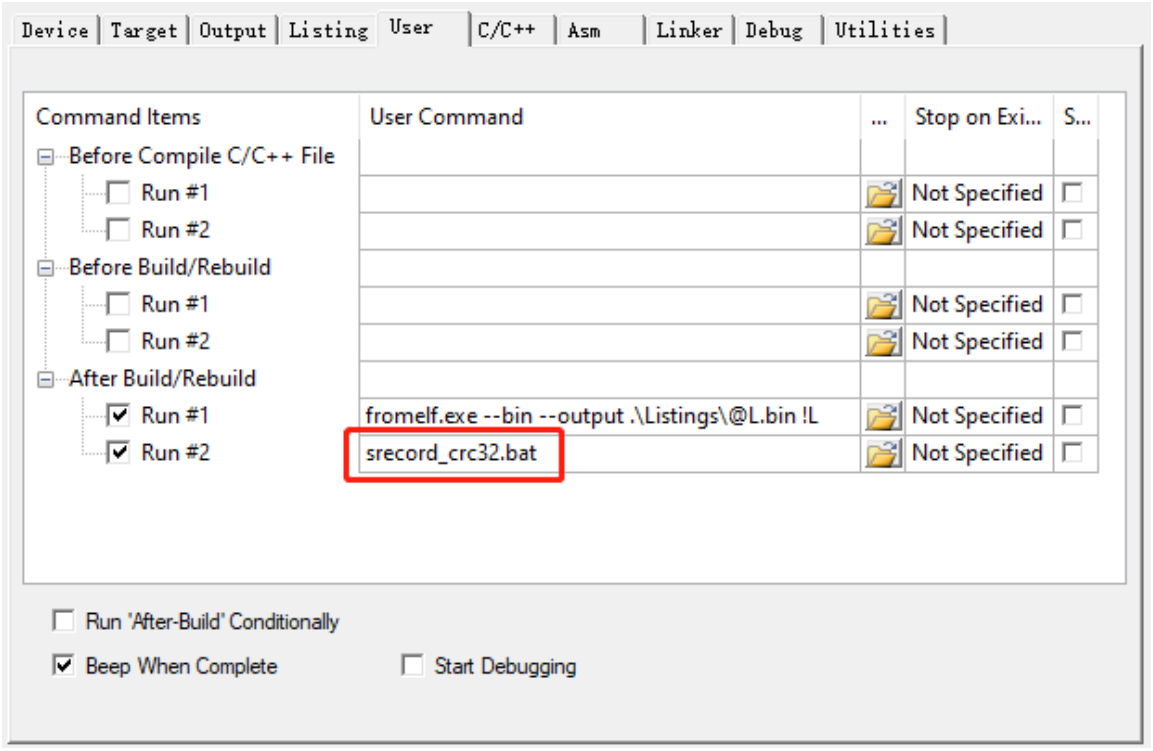
Keil配置：

Keil的配置较为复杂，ARM官方对于ROM Self-Test in MDK-ARM推荐使用第三方软件SRecord进行CRC测试。

根据工程配置，编译完成后会调用脚本文件srecord_crc32.bat，通过srec_cat.exe软件，将Keil编译生成的SelfTest.hex文件中的数据进行CRC计算，生成CRC校验结果，添加到指定位置得到新的SelfTest_CRC.hex文件：

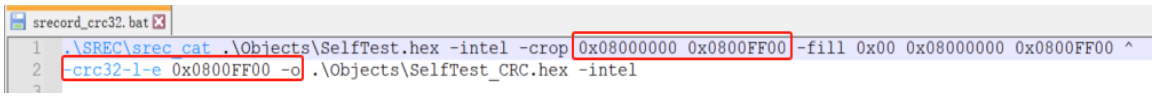
国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

图 5-8 Keil CRC 计算配置示例



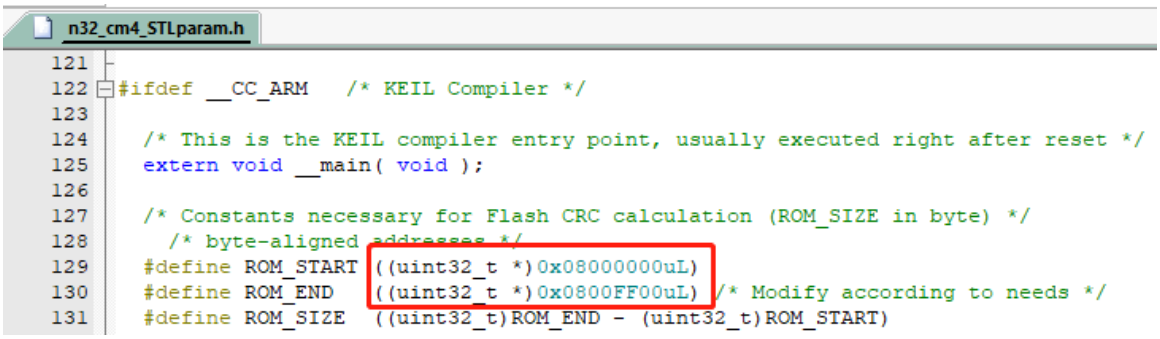
使用Notepad或其他工具打开srecord_crc32.bat文件，客户根据实际应用修改以下内容，CRC计算范围为0x8000000~0x800FEFF,检验结果存储位置为0x800FF00：

图 5-9 srecord_crc32.bat 文件



程序中计算CRC的范围根据n32_cm0_STLparam.h文件配置，与以上配置保持一致：

图 5-10 n32_cm0_STLparam.h 文件



并且通过配置如下crc_load.ini文件，使KEIL下载调试时使用最终生成的SelfTest_CRC.hex文件：

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

图 5-11 Keil 设置

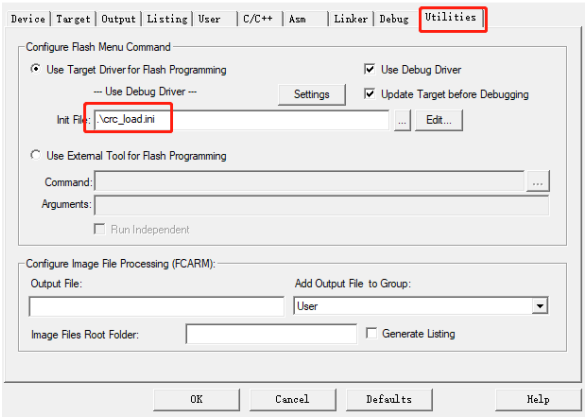
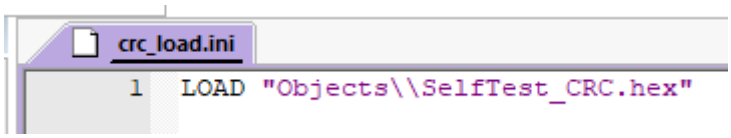


图 5-12 crc_load.ini 文件



5.2.4 RAM 启动时检测

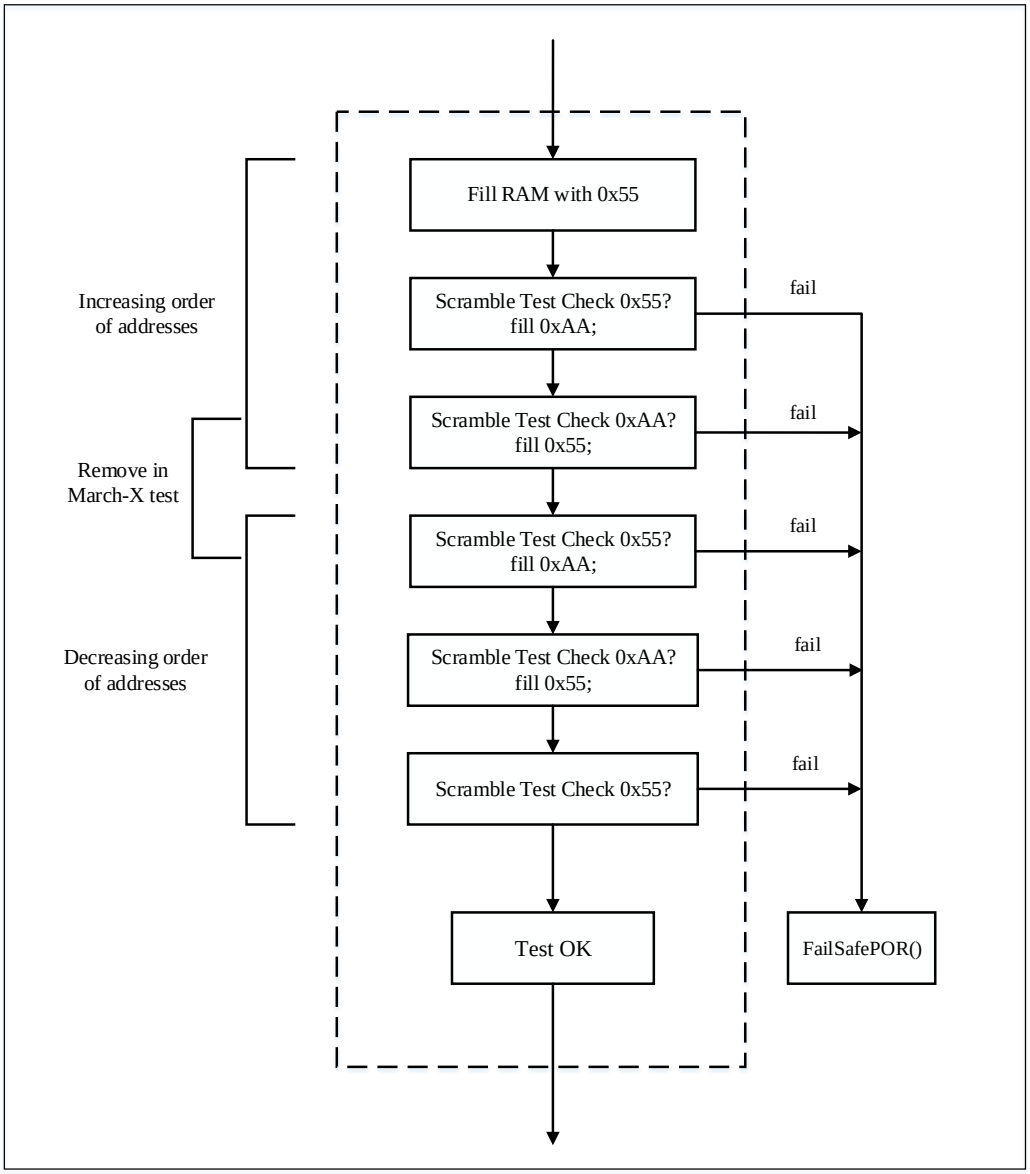
SRAM检测不仅检测数据区域的错误，还检测其内部地址和数据路径的错误。
SRAM自检采用March-C算法，March-C是一种用于嵌入式芯片SRAM测试的算法，是安全认证的一部分。
启动时对SRAM所有范围进行检测。
测试时分6个循环，用值0x55和0xAA逐字交替检查和填充整个RAM，前3个循环按照地址递增执行，后3个循环按照地址递减执行。
详细流程如下，如果采用March X算法则省略步骤3和4：

1. 全部范围写0x55555555，按照地址递增顺序执行；
2. 检测是否全部范围为0x55555555，然后全部范围写0xAAAAAAAA，按照地址递增顺序执行；
3. 检测是否全部范围为0xAAAAAAAA，然后全部范围写0x55555555，按照地址递增顺序执行；
4. 检测是否全部范围为0x55555555，然后全部范围写0xAAAAAAAA，按照地址递减顺序执行；
5. 检测是否全部范围为0xAAAAAAAA，然后全部范围写0x55555555，按照地址递减顺序执行；
6. 检测是否全部范围为0x55555555，按照地址递减顺序执行。

流程框图如下：

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

图 5-13 RAM 启动时检测流程框图



也可以对测试地址顺序进行加扰操作，因为加扰测试遵循物理地址顺序，从而防止并识别相邻物理存储单元之间的任何串音。

基本物理单元是一个覆盖 4 个字的模型（一行），见下表：单元格内的编号代表逻辑地址，而其他顺序则代表物理布局，粗框架强调逻辑顺序被加扰的位置。

用户通过在汇编栏配置 ARTISAN 参数开启加扰测试。

表 5-1 基本物理单元示例

	物理地址顺序--->			
行--->	0	1	3	2
	4	5	7	6
	8	9	11	10
	12	13	...	

启动时的 RAM 检测范围通过如下宏定义配置：

图 5-14 RAM 启动时检测范围

```
151  /* Constants necessary for execution initial March test */
152  #define RAM_START ((uint32_t *)0x20000000uL)
153  #define RAM_END   ((uint32_t *)0x200017FFuL) /* Modify according to needs */
```

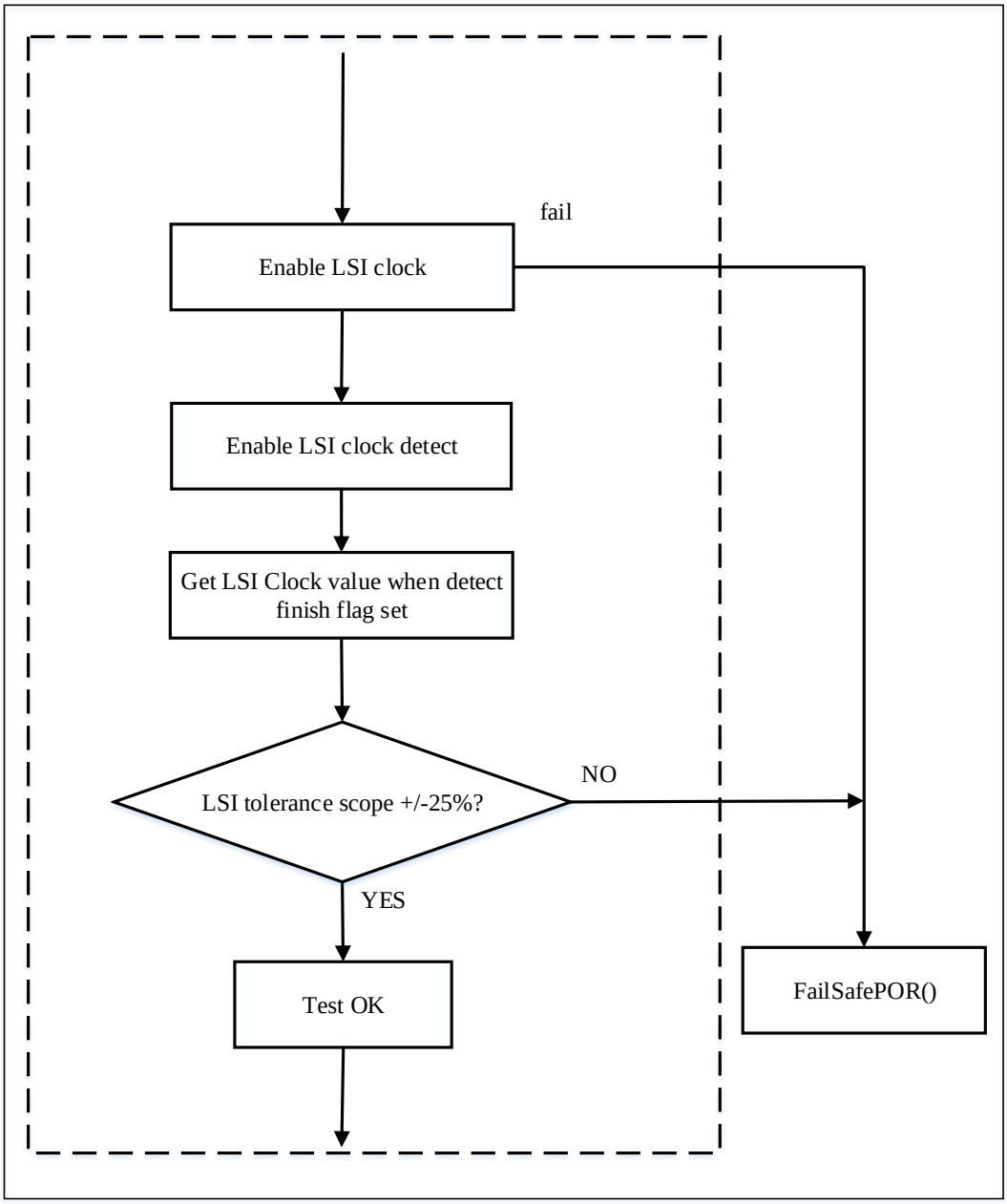

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

5.2.5 时钟启动时检测

内置HSI、LSI互相检测功能，步骤如下：

1. 使能 LSI 检测功能；
2. 查询 LSIDETFF 标志位，为 1 时检测结束，读取寄存器计数值，将该频率值与预期的范围值进行比较：如果超过范围，则测试失败。

图 5-15 时钟启动时检测流程框图



5.2.6 特征值写入栈边界

定义一个数组在栈底相邻的位置，写入 0xAAAAAAAAuL、0xBBBBBBBBuL、0xCCCCCCCCuL、

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

0xDDDDDDDDuL 特征值到数组中，便于后续运行中检测栈是否有溢出情况。

5.2.7 控制流启动时检测

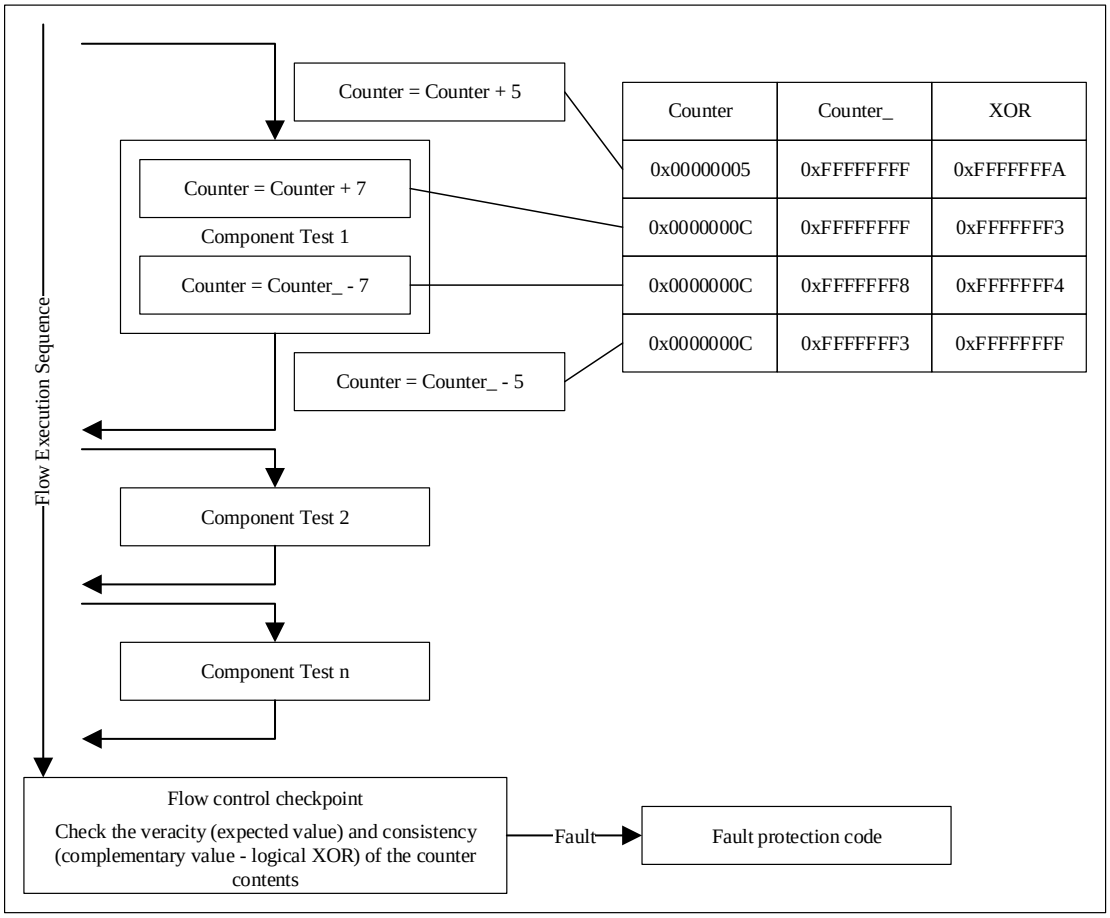
控制流检测可以检查每个ClassB检测函数是否正确调用(CALLER)，及该函数是否被正确执行(CALLEE)，检测方法概述如下：

1. 定义两个变量指示控制流进度，设置初始值 CtrlFlowCnt 为 0x00000000，CtrlFlowCntInv 为 0xFFFFFFFF，其初始状态互为取反；
2. 给每项测试模块定义两个固定数值分别表示 CALLER 和 CALLEE，并赋予不同的值；
3. 调用一项检测模块前，将 CtrlFlowCnt 增加 CALLER 的固定值，标示该模块已经调用；
4. 进入对应检测模块内部，将 CtrlFlowCnt 增加 CALLEE 的固定值，标示该模块正在执行；
5. 执行完对应检测模块内部，退出前 CtrlFlowCntInv 减少 CALLEE 的固定值，标示该模块执行正确；
6. 完成对应检测模块，进入下一项检测模块前，将 CtrlFlowCntInv 减少 CALLER 的固定值，标示该模块调用正确；
7. 检查 CtrlFlowCnt 是否为期望值，并且和 CtrlFlowCntInv 是否仍互为取反的，如果是则表明对应检测模块流程上被正确调用，并且该检测模块被正确执行。

流程图如下：

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

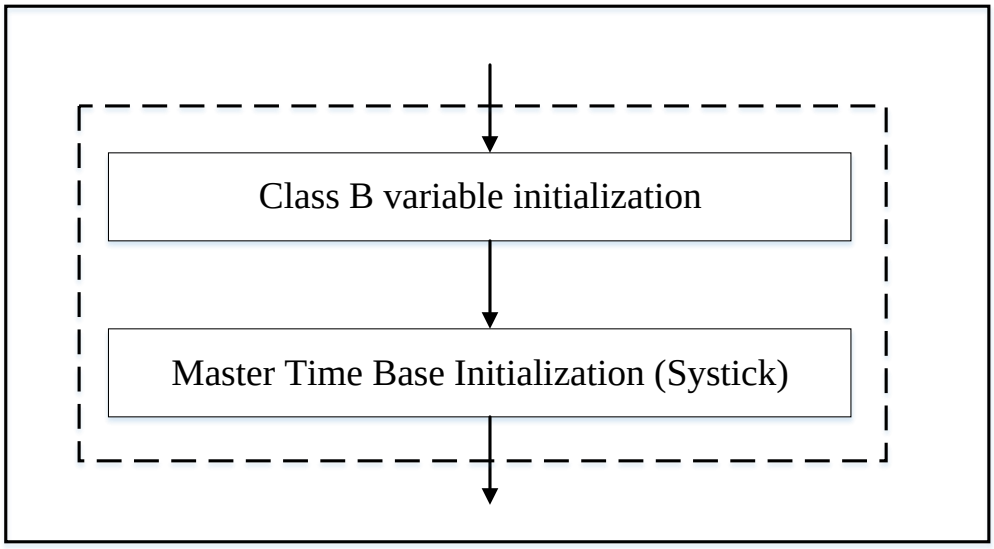
图 5-16 控制流启动时检测流程框图



5.3 运行时自检初始化

如果启动时自检全部成功通过，运行时自检必须在程序进入主循环前进行初始化（见下图），同时执行运行时自检的定期调用。应正确设置定时，以确保运行时测试程序按周期被调用，从而保证足够的应用运行时间。

图 5-17 运行时自检初始化框图



国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

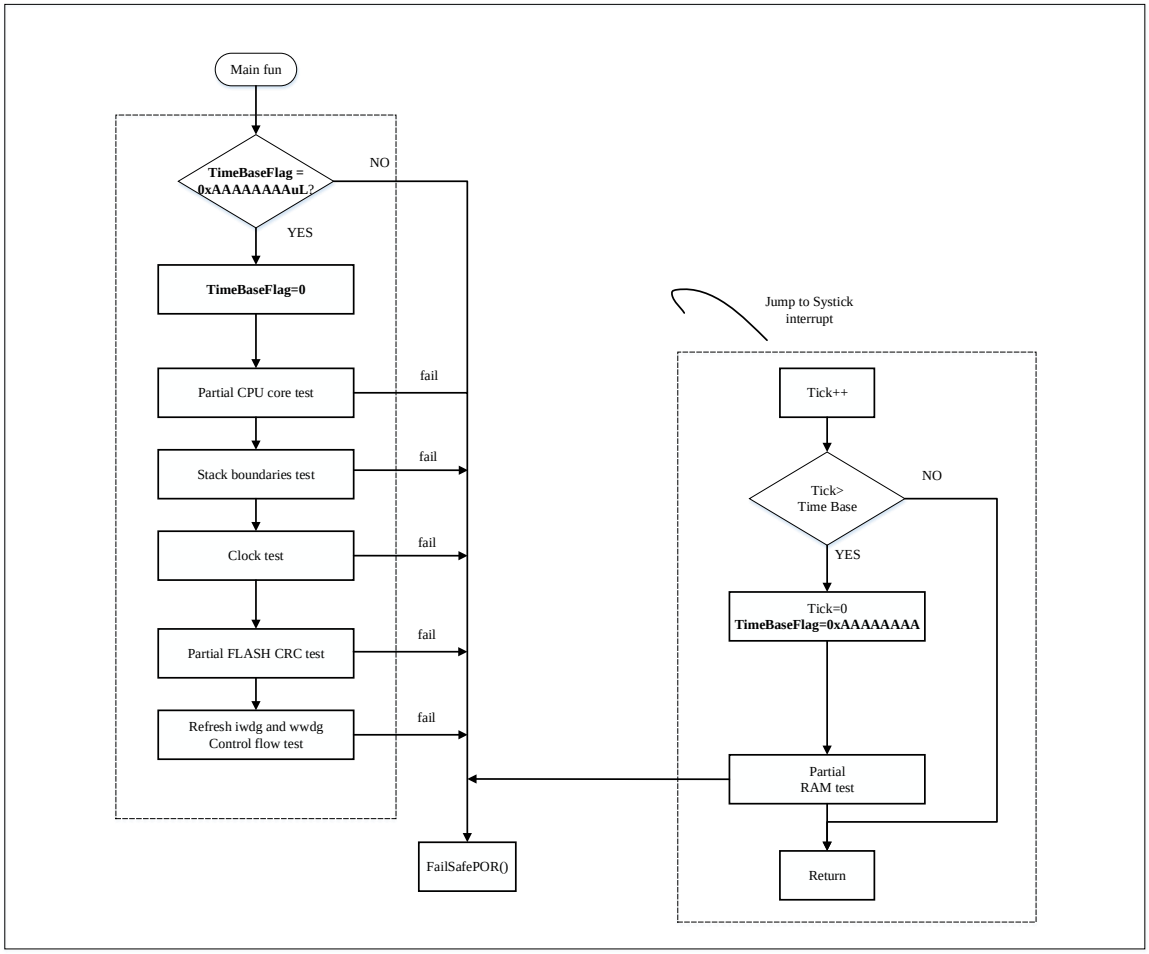
5.4 运行时检测流程

运行时的检测是以SysTick作为时基，进行周期性的检测，运行周期根据需要配置。
运行时的周期自检：

- 局部CPU内核寄存器检测
- 堆栈边界溢出检测
- 时钟运行检测
- Flash CRC分段检测
- 看门狗运行时刷新
- RAM March-C分段检测(在中断中进行）

运行时周期检测流程如下：

图 5-18 运行时周期检测流程框图

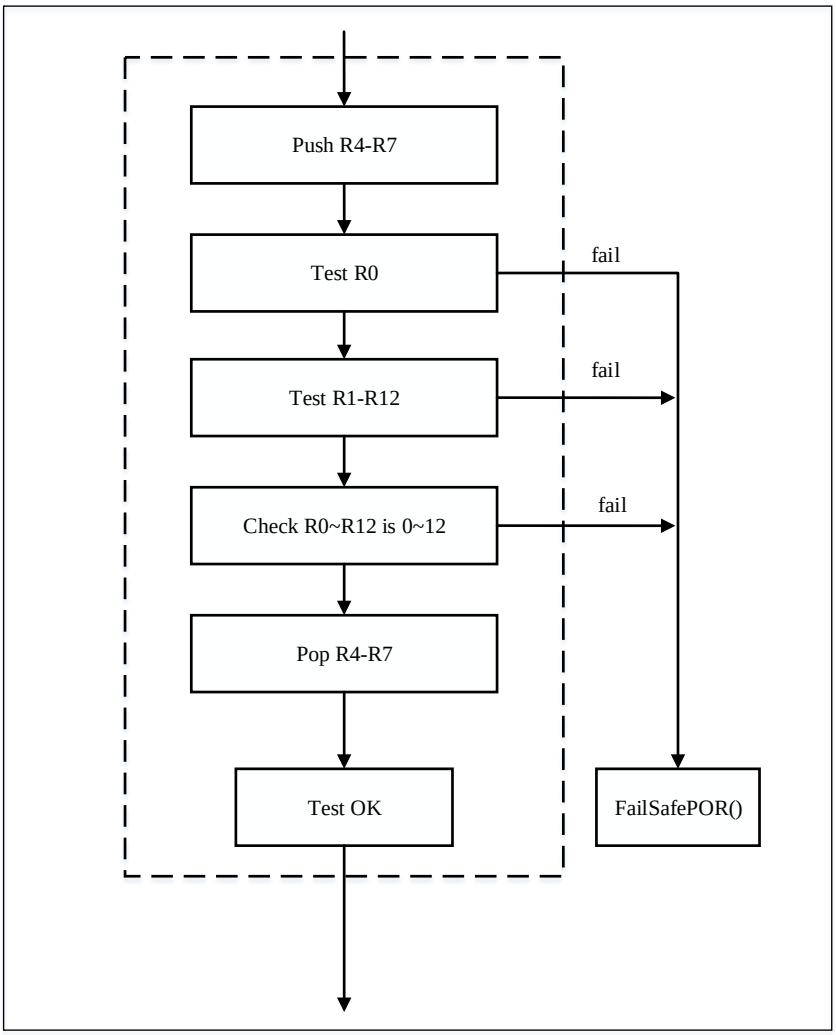


5.4.1 CPU 运行时检测

CPU 运行时周期自检只检测 R0~R12 通用寄存器，检测原理跟启动时的自检类似，并会对 R4~R7 寄存器进行压栈出栈处理。

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

图 5-19 CPU 运行时检测流程框图



5.4.2 堆栈边界运行时溢出检测

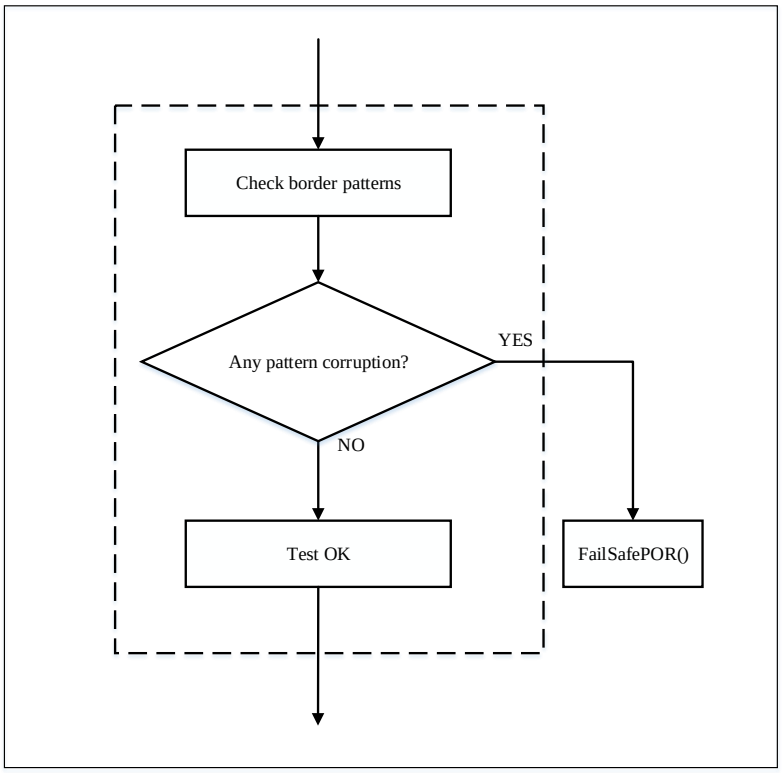
该测试通过判断边界检测区的pattern数组数据完整性来检测堆栈是否溢出。如果原始pattern数据被破坏，则测试失败，调用故障安全程序。

在紧跟堆栈区的低地址位置，定义为堆栈边界检测区。用户必须为堆栈定义足够的区域，并保证pattern正确放置。

检测流程如下：

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

图 5-20 堆栈边界运行时溢出检测流程框图

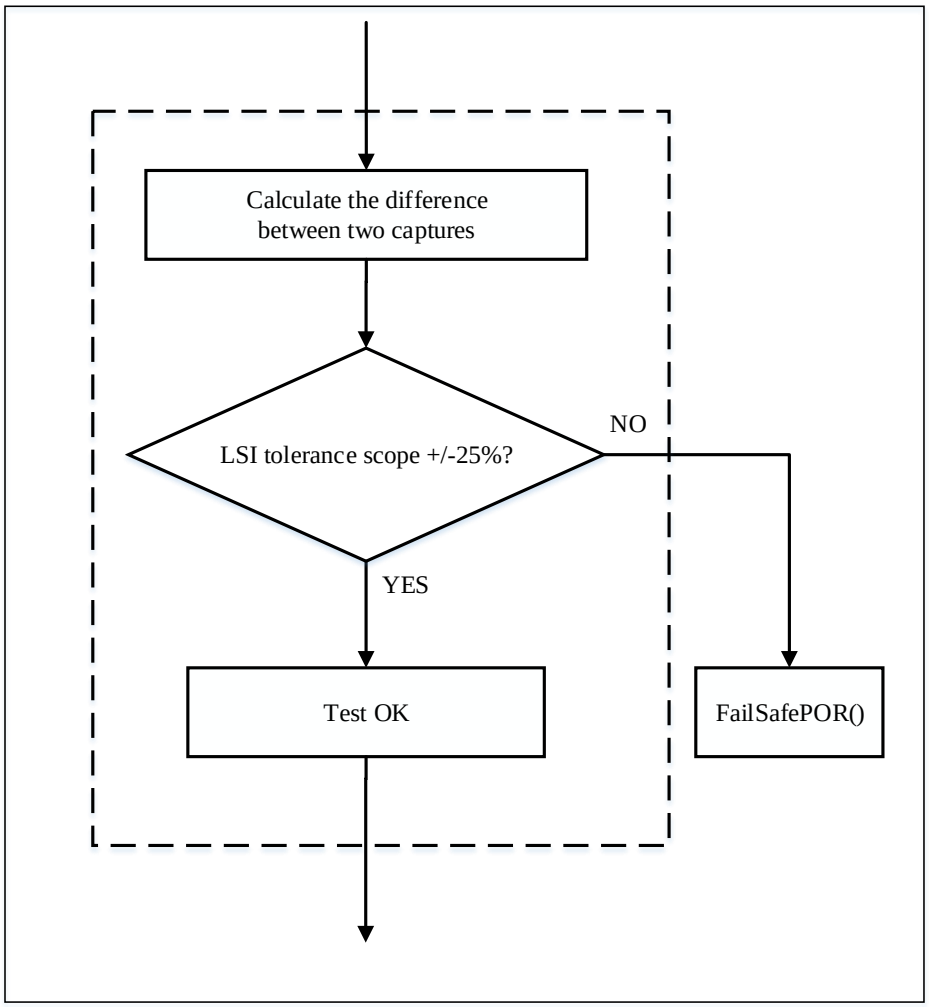


5.4.3 时钟运行时检测

运行时时钟的检测跟启动时时钟检测类似，通过两次捕获的差值计算出LSI的频率，流程如下：

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

图 5-21 时钟运行时检测流程框图

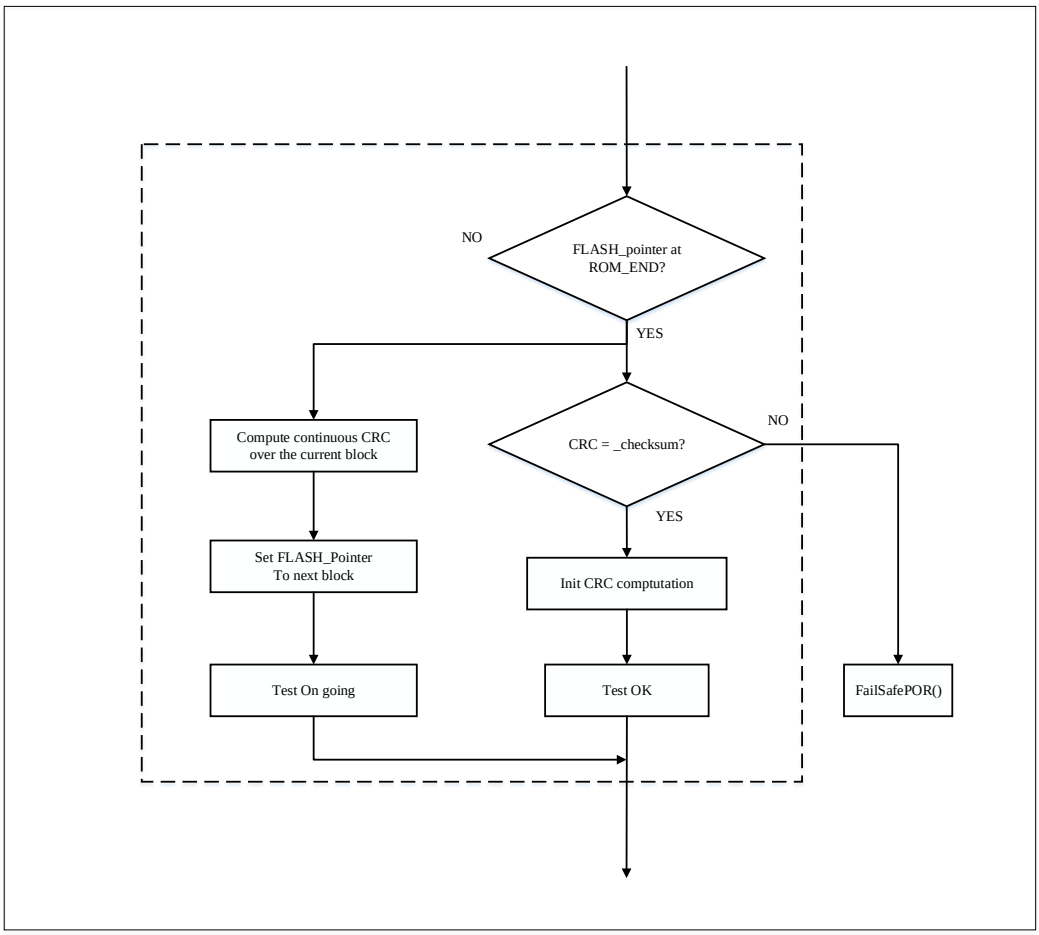


5.4.4 FLASH 运行时检测

运行时进行Flash CRC的自检，因为检测范围不同耗时不同，如果一次计算检测全部范围CRC可能耗时过长，影响应用代码的正常执行，因此可以根据运行周期进行分段CRC计算，当计算到最后一段范围时，进行CRC值比较，如果不一致则测试失败。

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

图 5-22 FLASH 运行时检测流程框图



5.4.5 看门狗运行时刷新

运行时需要定期喂狗保证系统正常运行，看门狗喂狗的部分放置在STL_DoRunTimeChecks()最后部分，用户可以根据实际应用情况选择是否开启看门狗。

5.4.6 RAM 运行时自检

运行时的RAM自检是在systick中断函数中进行的，测试范围可以通过如下宏定义调整，需注意的是因为测试包括了测试区域前后相邻的字，所以测试范围前后要保留适当余量，不要覆盖临时保存数据的缓冲块(Buffer block)和溢出芯片RAM范围，且需要保证检测范围为16字节的整数倍：

图 5-23 RAM 运行时检测范围

n32_cm0_STLparam.h

```
155  /* Constants necessary for execution of transparent run time March tests */
156  #define CLASS_B_START       ((uint32_t *)0x20000000uL)
157  #define CLASS_B_TESTSTART   ((uint32_t *)0x20000030uL)
158  #define CLASS_B_END         ((uint32_t *)0x200017F0uL) /* Modify according to needs: RAM_END - 0xF */
```

RAM区域分布如下图，KEIL通过SelfTest_N32XXXX.sct文件、IAR通过SelfTest.icf文件，将RAM划分为预留Buffer区，Class B变量区，用户变量区，栈边界区，栈区：

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

图 5-24 RAM 区域分布图

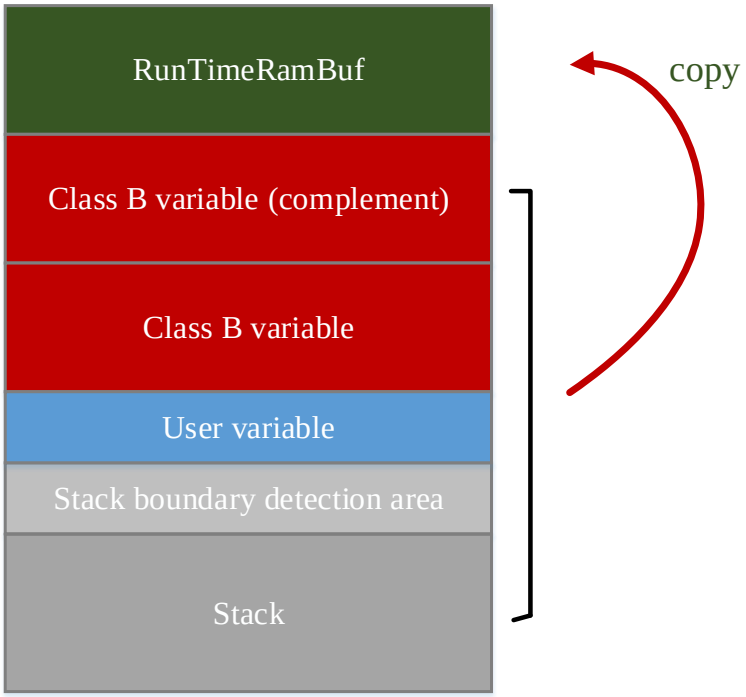


图 5-25 分散加载文件示例

```
RAM_BUF 0x20000000
{ ⟶ ⟶ ⟶; Run-time transparent RAM test buffer
  n32_cm0_STLstartup.o (RUN_TIME_RAM_BUF)
}

RAM_PNT 0x20000030 →
{ ⟶ ⟶ ⟶; Run-time transparent RAM test pointer
  n32_cm0_STLstartup.o (RUN_TIME_RAM_PNT)
}

CLASSB 0x20000040 UNINIT
{ ⟶ ⟶ · · · · · · · · ; Class B variables
n32_cm0_STLstartup.o (CLASS_B_RAM)
}

CLASSB_INV 0x20000090 UNINIT
{ · · · · · · · · · · · · · ; Class B inverted variables
n32_cm0_STLstartup.o (CLASS_B_RAM_REV)
}

RW_IRAM1 0x200000E0 UNINIT 0x00001300
{ · · · · · ; RW data (Class A variables)
  .ANY (+RW +ZI)
}

STACK_NO_HEAP 0x200013E0 UNINIT 0x410  { ; Stack and magic pattern for stack overflow detection
  n32_cm0_STLstartup.o (STACK_BOTTOM)
  startup_n32g033.o (STACK, +Last) ;select right startup file
}
```

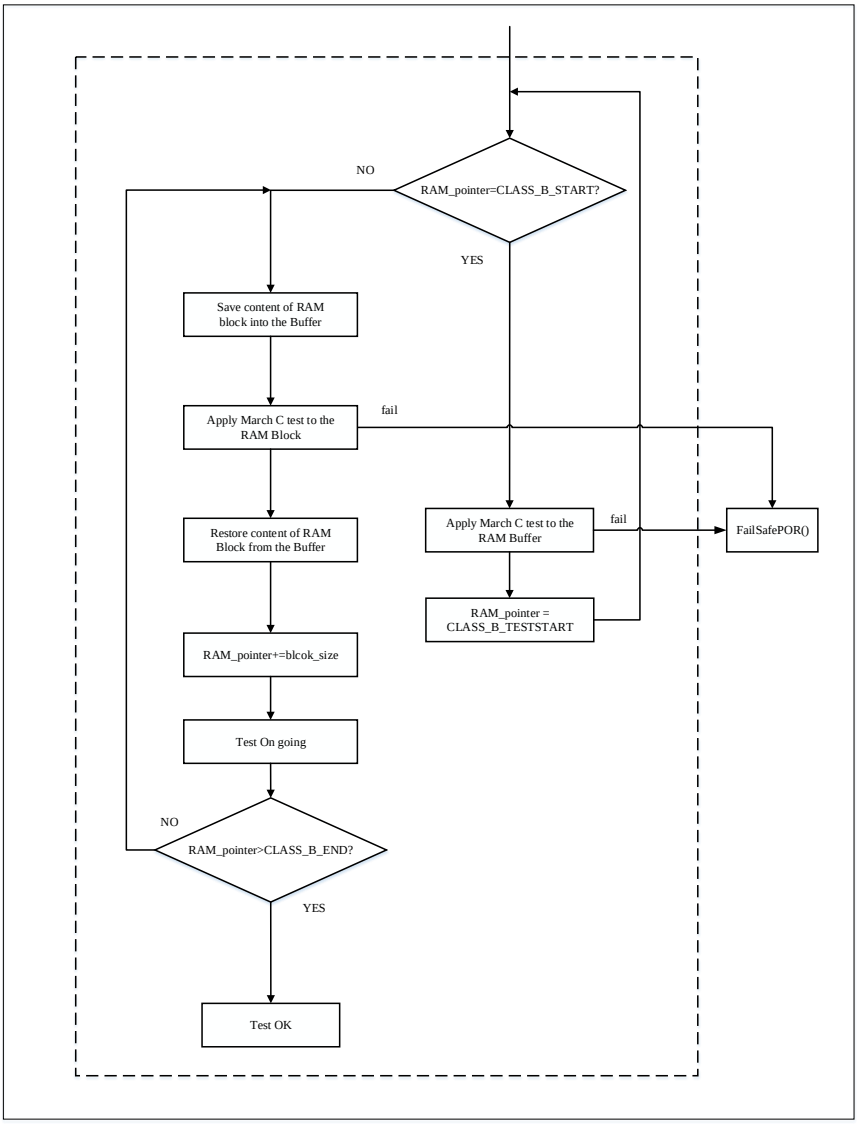
测试流程如下：

1. 对预留Buffer区进行March-C检测，确保预留Buffer区是OK的，之后根据中断周期分批次进行其他区域的检测；
2. 将待测试内存块(RAM block)的数据存储到专门用于测试过程中临时保存数据的缓冲块(Buffer block)；
3. 然后跟启动时检测RAM类似，对测试内存块(RAM block)采用March-C算法测试；

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

4. 测试完成后将缓冲块(Buffer block)中保存的数据恢复至测试内存块(RAM block)。

图 5-26 RAM 运行时检测流程框图

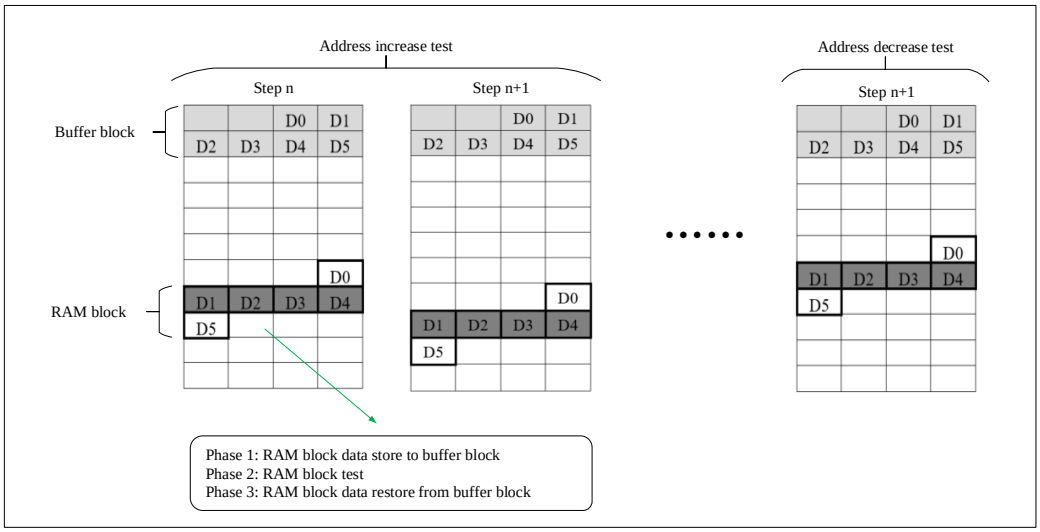


每次检测4个字的区域，但为保障耦合故障覆盖率，每次测试的实际内存块还包括测试区域前后各1个相邻字，总共6个字。

下图描述了故障耦合的基本原理，数据编号表示操作的先后顺序：

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

图 5-27 故障耦合



5.4.7 控制流运行时检测

运行时的自检以控制流检测指针程序结束。检测机制与启动时类似，在SysTick中断中的RAM检测和主函数的其他检测分开进行控制流检查。

初始化变量CtrlFlowCnt为0，CtrlFlowCntInv为0xFFFFFFFF，每测试一个步骤CtrlFlowCnt加一个固定值，CtrlFlowCntInv减同一固定值，自检结束时判断两个值相加是否仍为0xFFFFFFFF。

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

6 注意事项

用户使用过程中，如果需要按实际情况修改软件包相关代码，必须按照示例工程并结合上文的相关描述正确修改，否则可能导致检测失败。另外，开发时一些 IDE 相关的事项也需要用户关注，比如：

1 编译器的优化（设置编译器的优化等级）不仅会导致程序分析调试困难，还可能导致程序出现非预期的结果，所以强烈建议在使用过程中不要优化 Class-B 部分的代码。

2 使用不同版本的 IAR 开发时，可能会导致程序出现非预期的结果，所以强烈建议基于集成示例的版本环境开发。

3 运行时 RAM 检测期间会暂时关闭全局中断，结束后放开中断，因此用户需要注意防止应用代码与 RAM 检测发生冲突，如 I2C 模块，需要确认数据收发成后再进行 RAM 检测

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

7 历史版本

版本	日期	备注
V1.0.0	2025-11-26	创建文档

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057

8 声明

国民技术股份有限公司（下称“国民技术”）对此文档拥有专属产权。依据中华人民共和国的法律、条约以及世界其他法域相适用的管辖，此文档及其中描述的国民技术产品（下称“产品”）为公司所有。
国民技术在此并未授予专利权、著作权、商标权或其他任何知识产权许可。所提到或引用的第三方名称或品牌（如有）仅用作区别之目的。
国民技术保留随时变更、订正、增强、修改和改良此文档的权利，恕不另行通知。请使用人在下单购买前联系国民技术获取此文档的最新版本。
国民技术竭力提供准确可信的资讯，但即便如此，并不推定国民技术对此文档准确性和可靠性承担责任。
使用此文档信息以及生成产品时，使用者应当进行合理的设计、编程并测试其功能性和安全性，国民技术不对任何因使用此文档或本产品而产生的任何直接、间接、意外、特殊、惩罚性或衍生性损害结果承担责任。
国民技术对于产品在系统或设备中的应用效果没有任何故意或保证，如有任何应用在其发生操作不当或故障情况下，有可能致使人员伤亡、人身伤害或严重财产损失，则此类应用被视为“不安全使用”。
不安全使用包括但不限于：外科手术设备、原子能控制仪器、飞机或宇宙飞船仪器、所有类型的安全装置以及其他旨在支持或维持生命的应用。
所有不安全使用的风险应由使用人承担，同时使用人应使国民技术免于因为这类不安全使用而导致被诉、支付费用、发生损害或承担责任时的赔偿。
对于此文档和产品的任何明示、默示之保证，包括但不限于适销性、特定用途适用性和不侵权的保证责任，国民技术可在法律允许范围内进行免责。
未经明确许可，任何人不得以任何理由对此文档的全部或部分进行使用、复制、修改、抄录和传播。

国民技术股份有限公司 NSING TECHNOLOGIES INC.
地址：深圳市南山区高新北区宝深路109号国民技术大厦
电话：+86-755-86309900 传真：+86-755-86169100
网址：https://www.nsingtech.com 邮编：518057