Application Note

N32G45x Series Security Startup Application Note

Introduction

Security plays an increasingly important role in the field of electronic applications. In electronic design, the level of component safety requirements is increasing, and electronic equipment manufacturers are incorporating many new technology solutions into new component designs. Software technologies are emerging to improve security. Standards for hardware and software security requirements are also under continuous development.

This document describes how the project in N32G45x MCU to perform the requirements of IEC60730 software safety related operations and related application code content.

This document applies to the N32G45x series products of National Technologies.

Nations Technologies Inc.
Tel：+86-755-86309900
Email：info@nationstech.com
Address: Nations Tower, #109 Baoshen Road, Hi-tech Park North.
Nanshan District, Shenzhen, 518057, P.R.China

Content

Nations Technologies Inc.
Tel：+86-755-86309900
Email：info@nationstech.com
Address: Nations Tower, #109 Baoshen Road, Hi-tech Park North.
Nanshan District, Shenzhen, 518057, P.R.China

1. IEC60730 Class B software standard introduction

To ensure the safety of electrical appliances, risk control measures during software operation need to be evaluated.

IEC60730, issued by the International Electrotechnical Commission, introduces the requirements for the evaluation of software for household appliances. In Appendix H(H.2.21), software is classified as follows:

Category A software: the software only realizes the functions of the product and does not involve the security control of the product. Software for room thermostats, lighting controls...

Category B software: software designed to prevent unsafe operation of electronic devices. For example, the washing machine software with automatic door lock control, the induction cooker software with overheating control...

Category C software: software designed to avoid certain specific hazards. Such as automatic burner control and hot break of closed water heater (mainly for some explosive equipment)

The specific evaluation requirements of class B software include components to be tested and related faults and test schemes, which are sorted out in the following table (refer to IEC60730 Table H.11.12.7) :

Components to be detected		Fault/error	Fault classification	Nations with library	Test Solution Overview
1.CPU	1.1 register	Hysteresis (Stuck at)	MCU related	Y	Write relevant registers and check
	1.3 Program counter	Hysteresis (Stuck at)	MCU related	Y	When the PC runs fly start the watchdog reset
2.Interruption		No interrupts or interrupts too frequently	Application of the relevant	N	Count the number of interrupts
3. The clock		Wrong frequency	MCU related	Y	Use HSI to measure HSE clock frequency
4. Memory	4.1 Non-volatile memory	All single bit errors	MCU related	Y	FLASH CRC integrity check
	4.2 Volatile memory	DC fault	MCU related	Y	1. SRAM March C test 2. Stack overflow detection
	4.3 Addressing (related to non-volatile and volatile memory)	Hysteresis (Stuck at)	MCU related	Y	FLASH/SRAM tests are included
5. Internal data path	5.1 data	Hysteresis (Stuck at)	MCU related	N	Only for MCU using external memory, monolithic MCU is not required
	5.2 addressing	Wrong address	MCU related	N	

Nations Technologies Inc.
Tel：+86-755-86309900
Email：info@nationstech.com
Address: Nations Tower, #109 Baoshen Road, Hi-tech Park North. Nanshan District, Shenzhen, 518057, P.R.China

External communication	6.1 data	The Hamming distance is 3	Application of the relevant	N	Add verification in data transfer
	6.2 addressing	Wrong address	Application of the relevant	N	
	6.3 sequential	Wrong timing	Application of the relevant	N	Count the number of communication events
7. Input and output	7.1 digital I/O	Error defined in H27	Application of the relevant	N	None
	7.2 Analog input and output	Error defined in H27	Application of the relevant	N	None

2. Test point process description

Class B software package program inspection content is divided into two main parts: self-check at startup and periodic self-check at runtime.Self-test at startup includes:

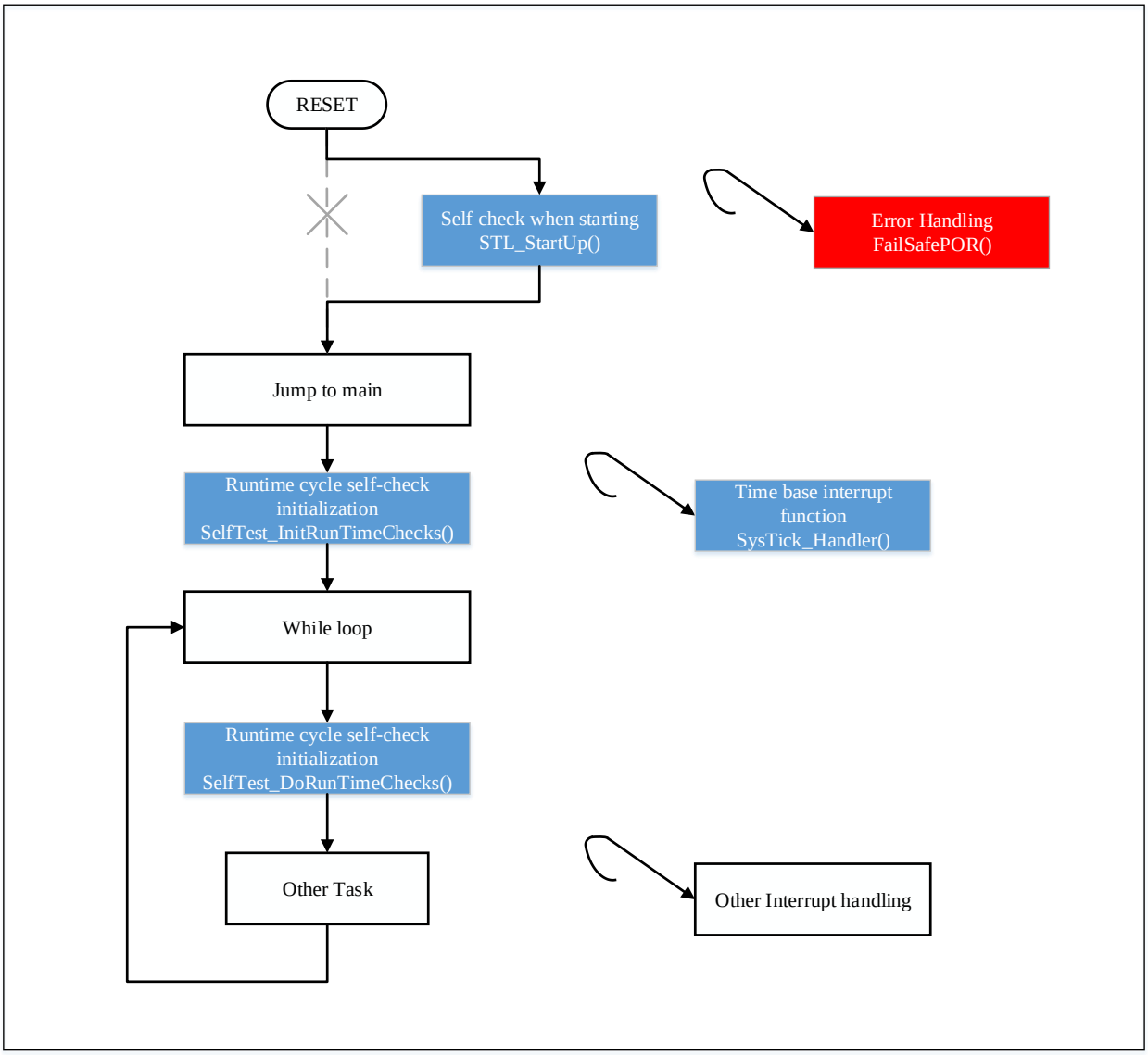
- CPU detection
- Watchdog detection
- Flash integrity detection
- RAM function detection
- System clock Detection
- Control flow detection

Periodic self-check at runtime:

- Local CPU kernel register detection
- Stack boundary overflow detection
- System clock running detection
- Flash CRC segmentation detection
- Watchdog detection
- Local RAM self-check (in interrupt service routines)

The overall flow diagram is as follows:

Nations Technologies Inc.
Tel：+86-755-86309900
Email：info@nationstech.com
Address: Nations Tower, #109 Baoshen Road, Hi-tech Park North.
Nanshan District, Shenzhen, 518057, P.R.China

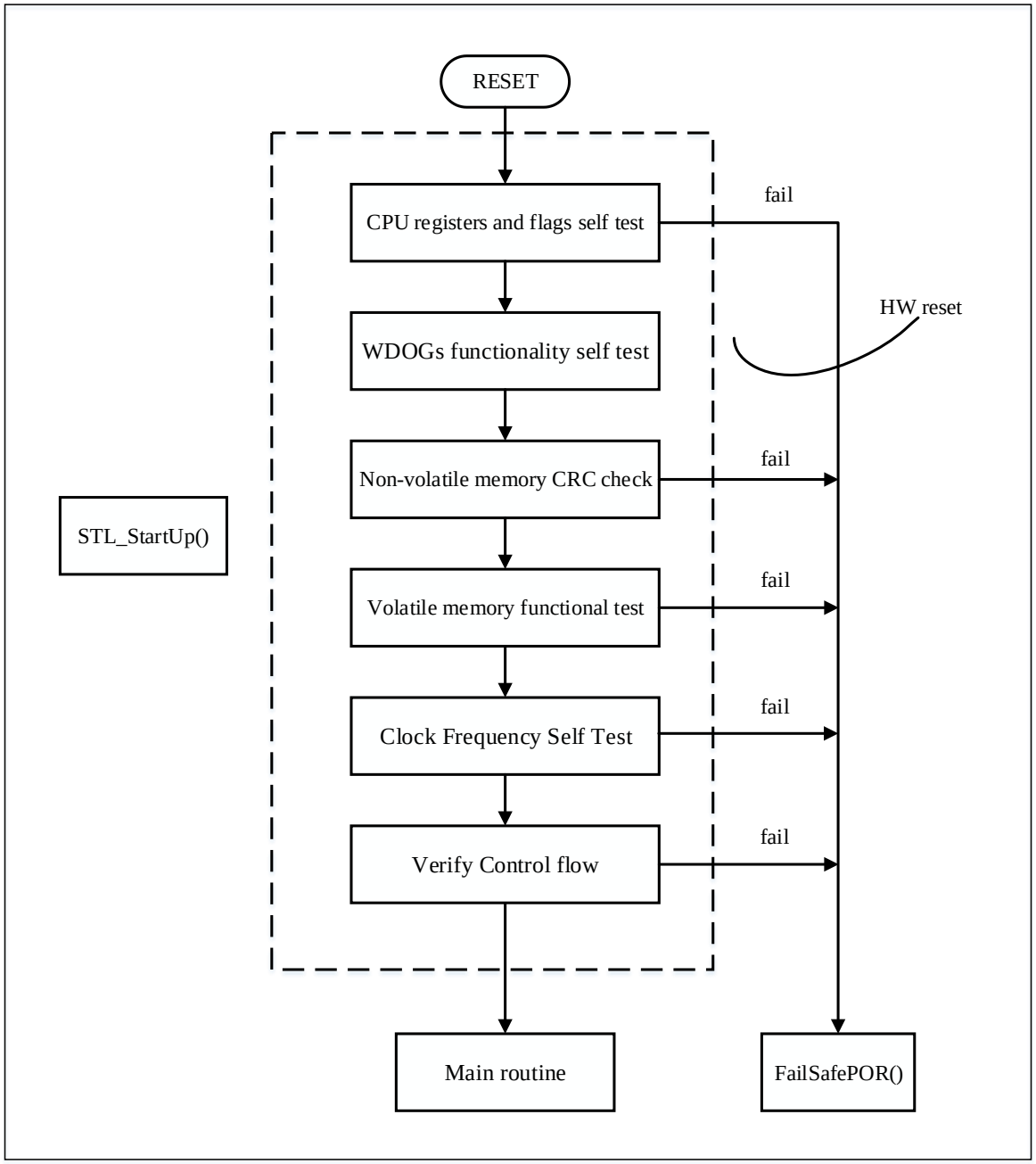


2.1 Check flow at startup

Before the chip enters **main** function from startup, the startup detection is carried out first, and the startup file is modified to execute this part of the code. After the detection process is over, the **__iar_program_start** function is called to jump back to **main** function.

The following is a flow diagram for performing a bootstrap self-check:

Nations Technologies Inc.
Tel：+86-755-86309900
Email：info@nationstech.com
Address: Nations Tower, #109 Baoshen Road, Hi-tech Park North.
Nanshan District, Shenzhen, 518057, P.R.China



2.1.1 CPU startup detection

CPU self-check mainly checks whether the kernel flags, registers and so on are correct. If an error occurs, **FailSafePOR ()** is called.

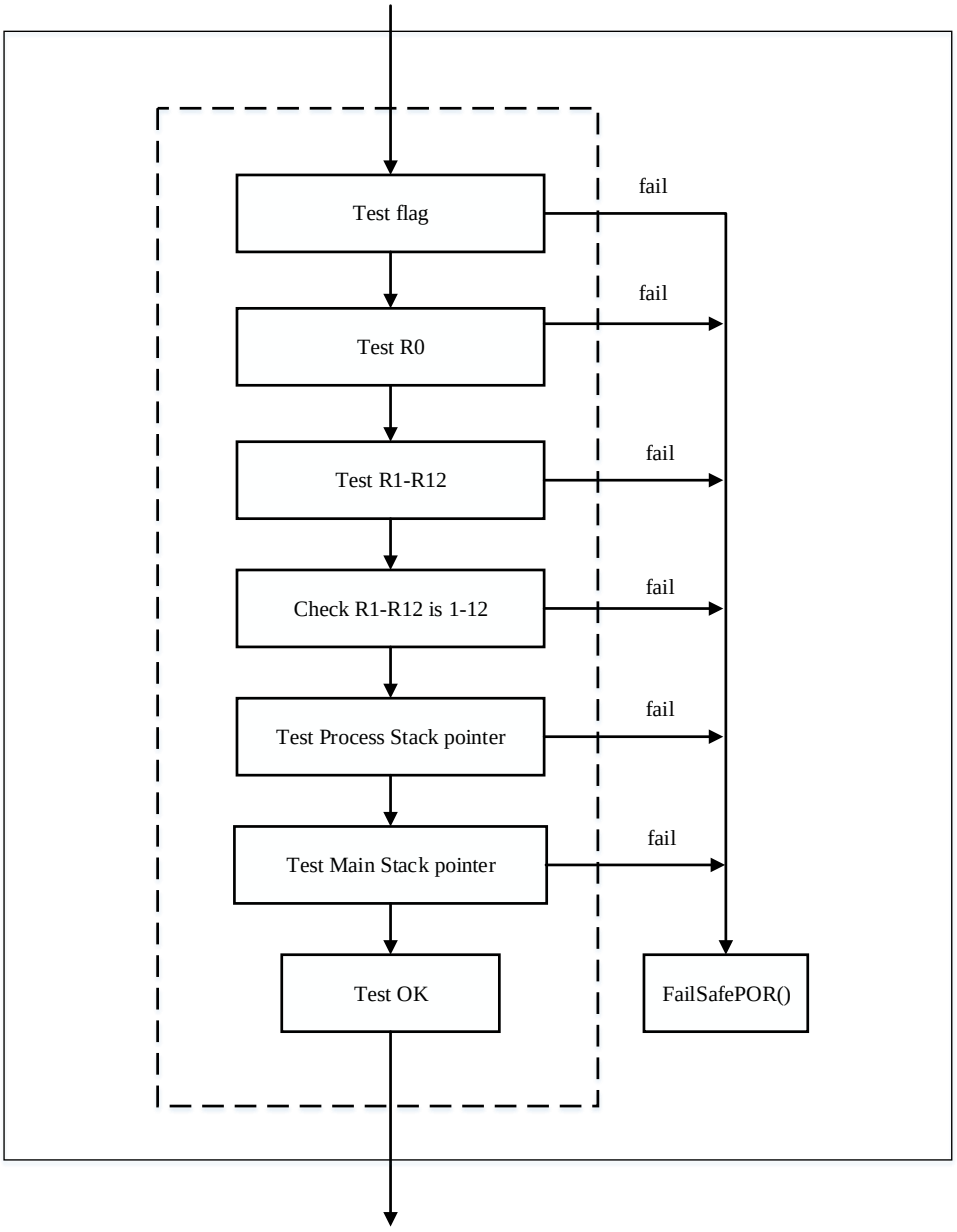
CPU self-check at startup and runtime will be carried out, at startup, R0~R12, PSP, MSP register and Z(zero), N(negative), C(carry), V(overflow) flag bit function test will be a self-check; When run, periodic self-check, only detect registers R1~R12.

Register detection is implemented as follows: write 0xAAAAAAAA and 0x55555555 to the register respectively, and then compare whether the read value is the written value. Write 1 after R1 is tested, write 2 after R2 is tested, and so on.

The specific implementation method of flag bit detection is as follows: set the flag position bits respectively. If the flag bit is checked incorrectly, the fault function will be entered. The

Nations Technologies Inc.
Tel：+86-755-86309900
Email：info@nationstech.com
Address: Nations Tower, #109 Baoshen Road, Hi-tech Park North.
Nanshan District, Shenzhen, 518057, P.R.China

detection flow diagram is as follows:



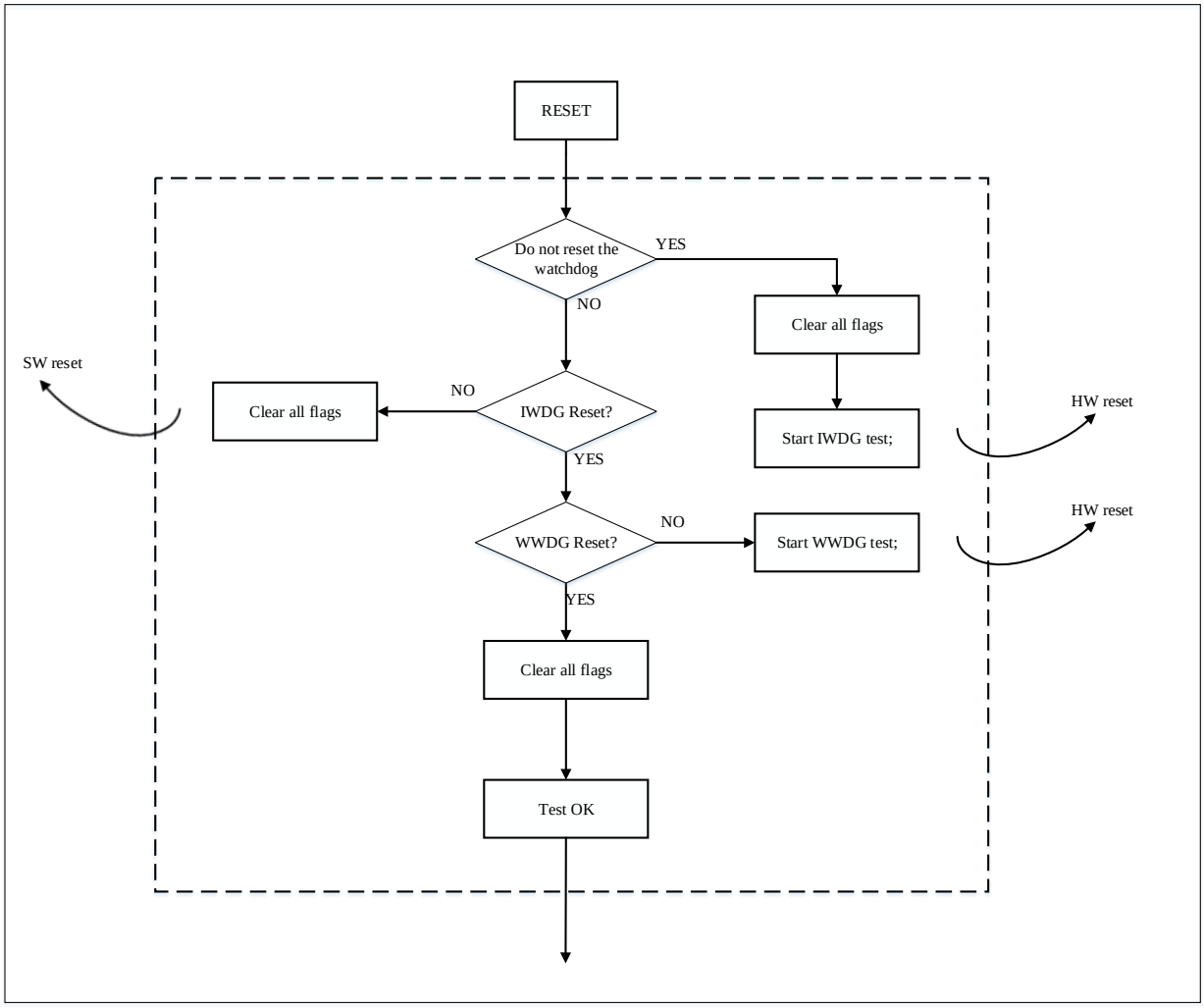
2.1.2 Detection when watchdog starts

Test to verify that independent watchdog and window watchdog can be reset correctly to ensure that runfly can be reset in time to prevent jam when the program is running.

After the initial reset, clear all reset status register flag bits, start the IWDG test, reset the chip, and judge whether it is the IWDG reset flag bit; if it is set, start the WWDG test to reset the chip, if the WWDG reset flag bit is set, the watchdog test passes,clear all flags.

The flow diagram is as follows:

Nations Technologies Inc.
Tel：+86-755-86309900
Email：info@nationstech.com
Address: Nations Tower, #109 Baoshen Road, Hi-tech Park North.
Nanshan District, Shenzhen, 518057, P.R.China

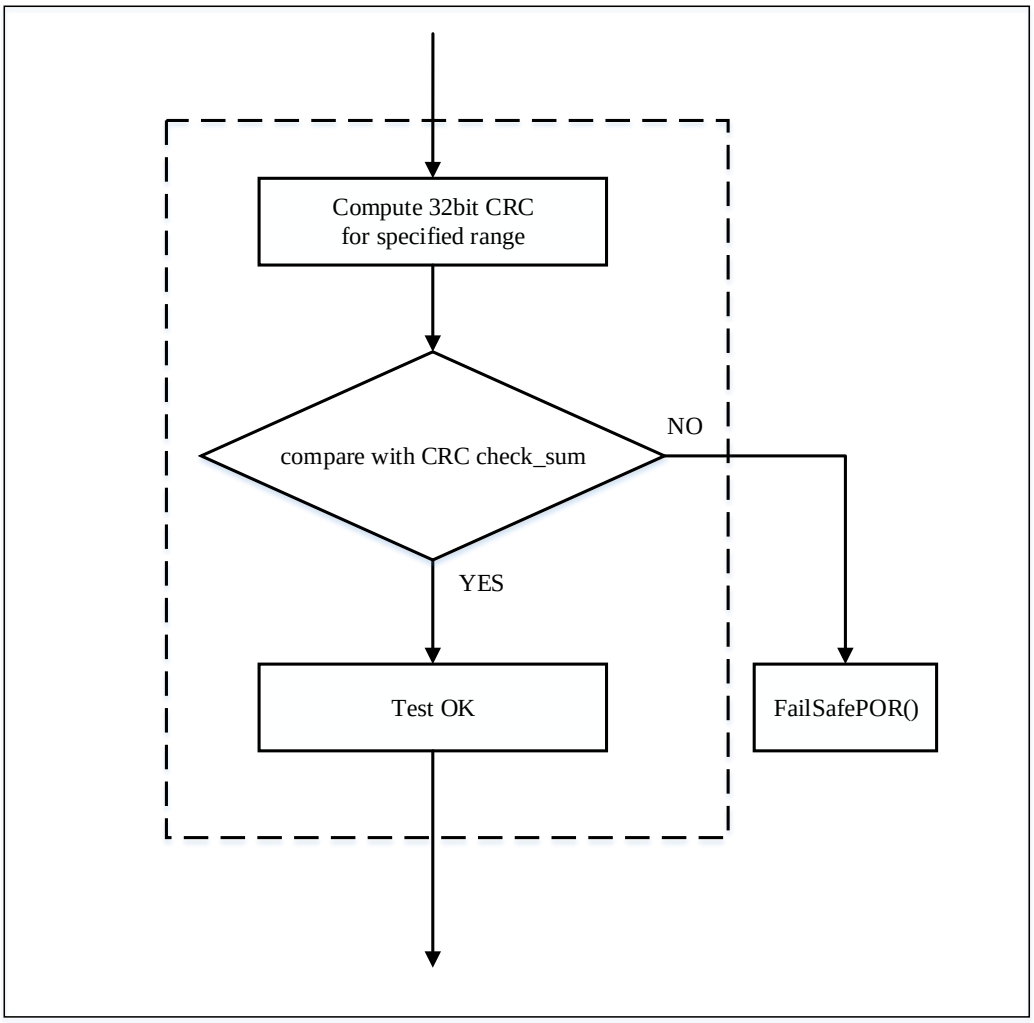


2.1.3 FLASH startup detection

FLASH self-check is a program that calculates FLASH data with CRC algorithm and compares the result value with the CRC value calculated during compilation and stored in the specified location of FLASH to confirm the integrity of FLASH.

The flow diagram is as follows:

Nations Technologies Inc.
Tel：+86-755-86309900
Email：info@nationstech.com
Address: Nations Tower, #109 Baoshen Road, Hi-tech Park North.
Nanshan District, Shenzhen, 518057, P.R.China

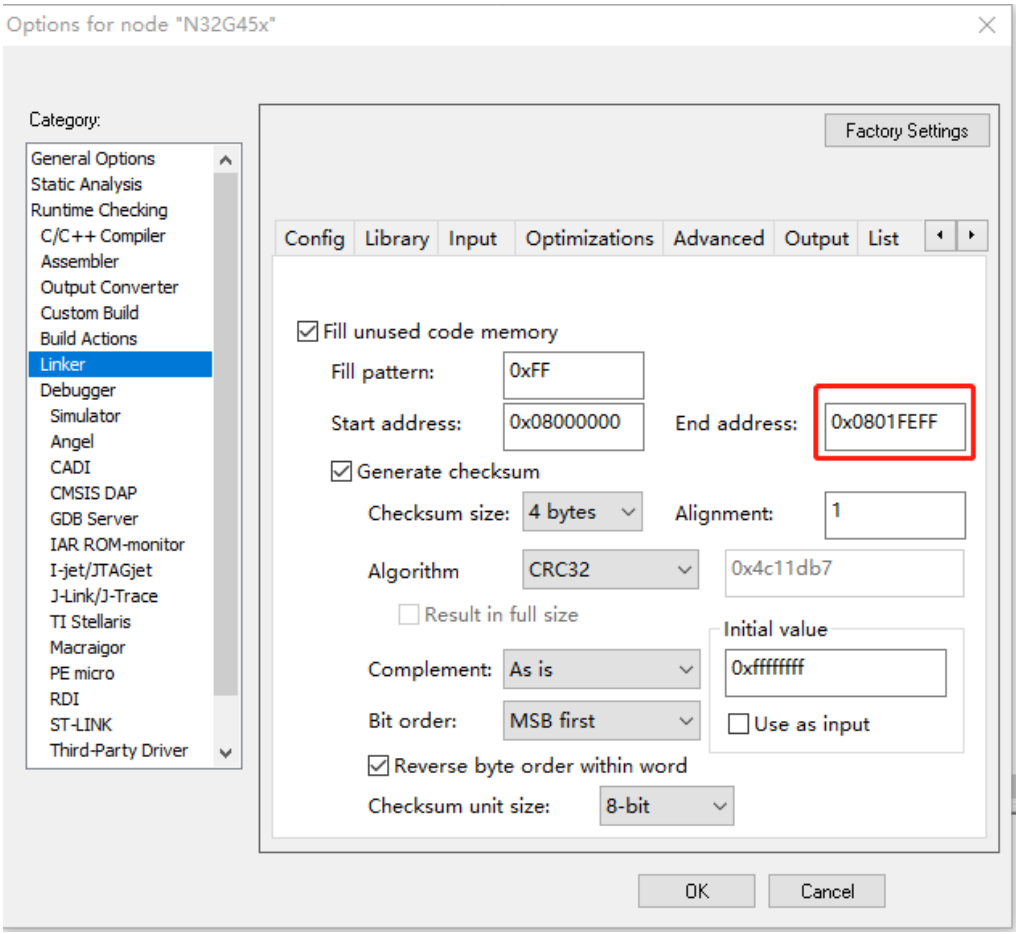


FLASH range of CRC calculation is configured according to the actual situation of the whole program, and the method is different on KEIL and IAR.

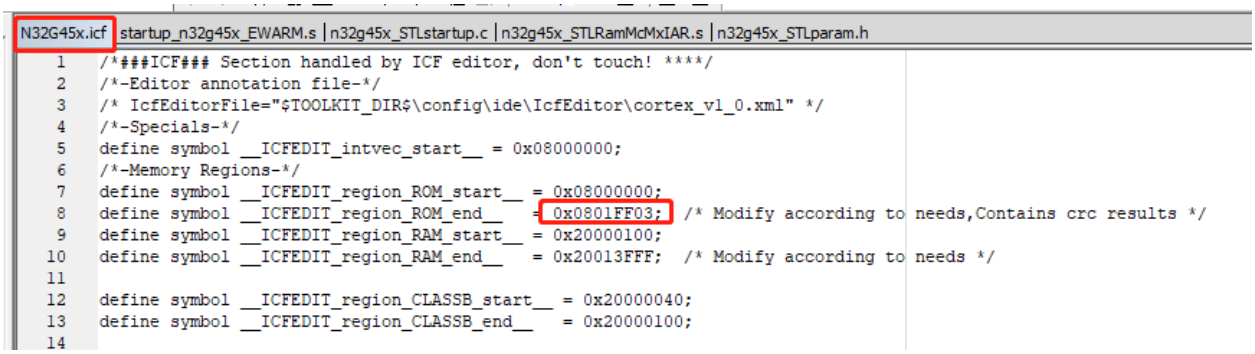
IAR configuration:

The CRC calculation is supported in the IAR configuration options. Just configure the parameters, and the compiled file will automatically add the CRC check_sum value to the selected FLASH calculation range:

Nations Technologies Inc.
Tel：+86-755-86309900
Email：info@nationstech.com
Address: Nations Tower, #109 Baoshen Road, Hi-tech Park North.
Nanshan District, Shenzhen, 518057, P.R.China



The range of calculating CRC in the program is configured according to the .icf file, which can be modified according to the needs. Add 4 to the above configuration:

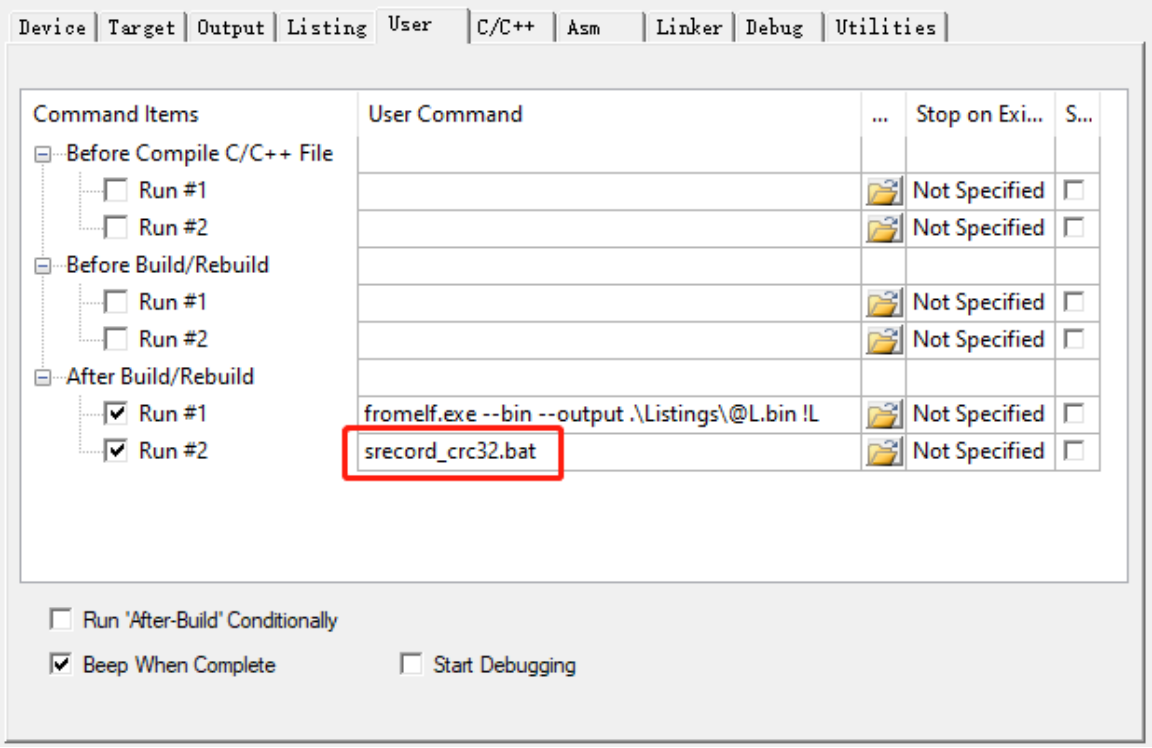


Keil configuration:

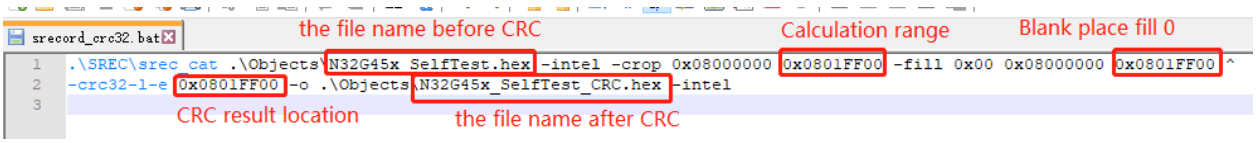
Configuration of Keil is more complicated. ARM officially recommends using the third-party software SRecord for ROM Self-Test in MDK-ARM.

According to the project configuration, after the compilation is completed, the script file srecord_crc32.bat will be called. Through the srec_cat.exe software, the data in the N32G45x_SelfTest.hex file generated by Keil will be calculated by CRC, and the CRC check result will be generated. Add it to the specified location to get a new N32G45x_SelfTest_CRC.hex file:

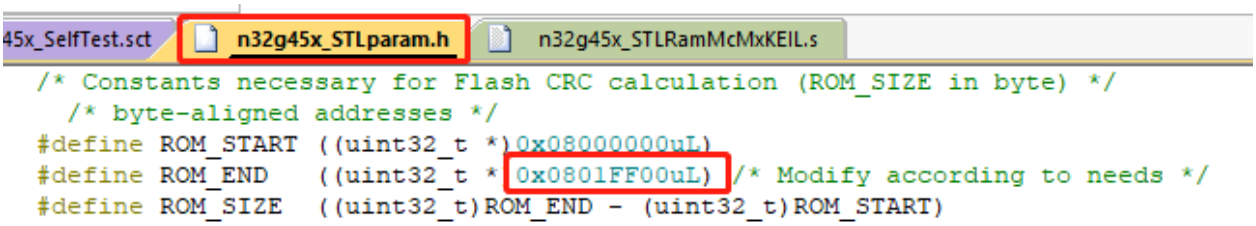
Nations Technologies Inc.
Tel：+86-755-86309900
Email：info@nationstech.com
Address: Nations Tower, #109 Baoshen Road, Hi-tech Park North.
Nanshan District, Shenzhen, 518057, P.R.China



Open the .bat file with Notepad or other tools, and modify the following according to the actual application:

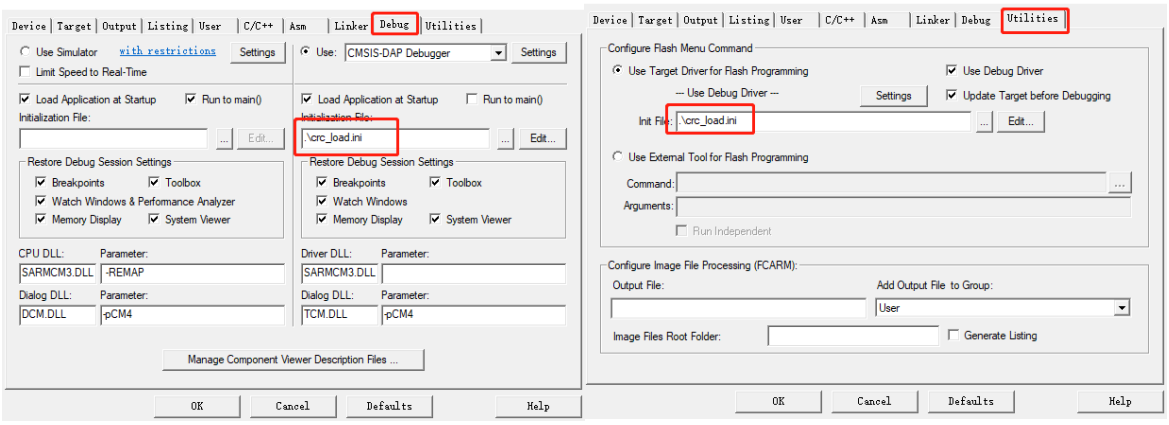


Range of calculating CRC in the program is configured according to the N32G45x_STLparam.h file, which can be modified according to the requirements, which is consistent with the above configuration:

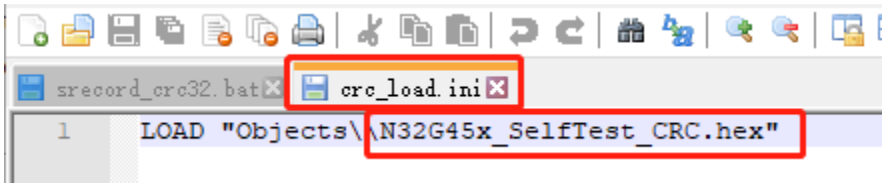


Therefore, whether it is downloading or debugging, the final generated N32G45x_SelfTest_CRC.hex file needs to be used, so the .ini file needs to be added to the Keil configuration option to download the new .hex file. The configuration is as follows:

Nations Technologies Inc.
Tel：+86-755-86309900
Email：info@nationstech.com
Address: Nations Tower, #109 Baoshen Road, Hi-tech Park North.
Nanshan District, Shenzhen, 518057, P.R.China



It should be noted that the .ini file should also modify the content file name configuration according to the actual application:



2.1.4 RAM startup detection

SRAM detection detects errors not only in the data region, but also in its internal address and data path.

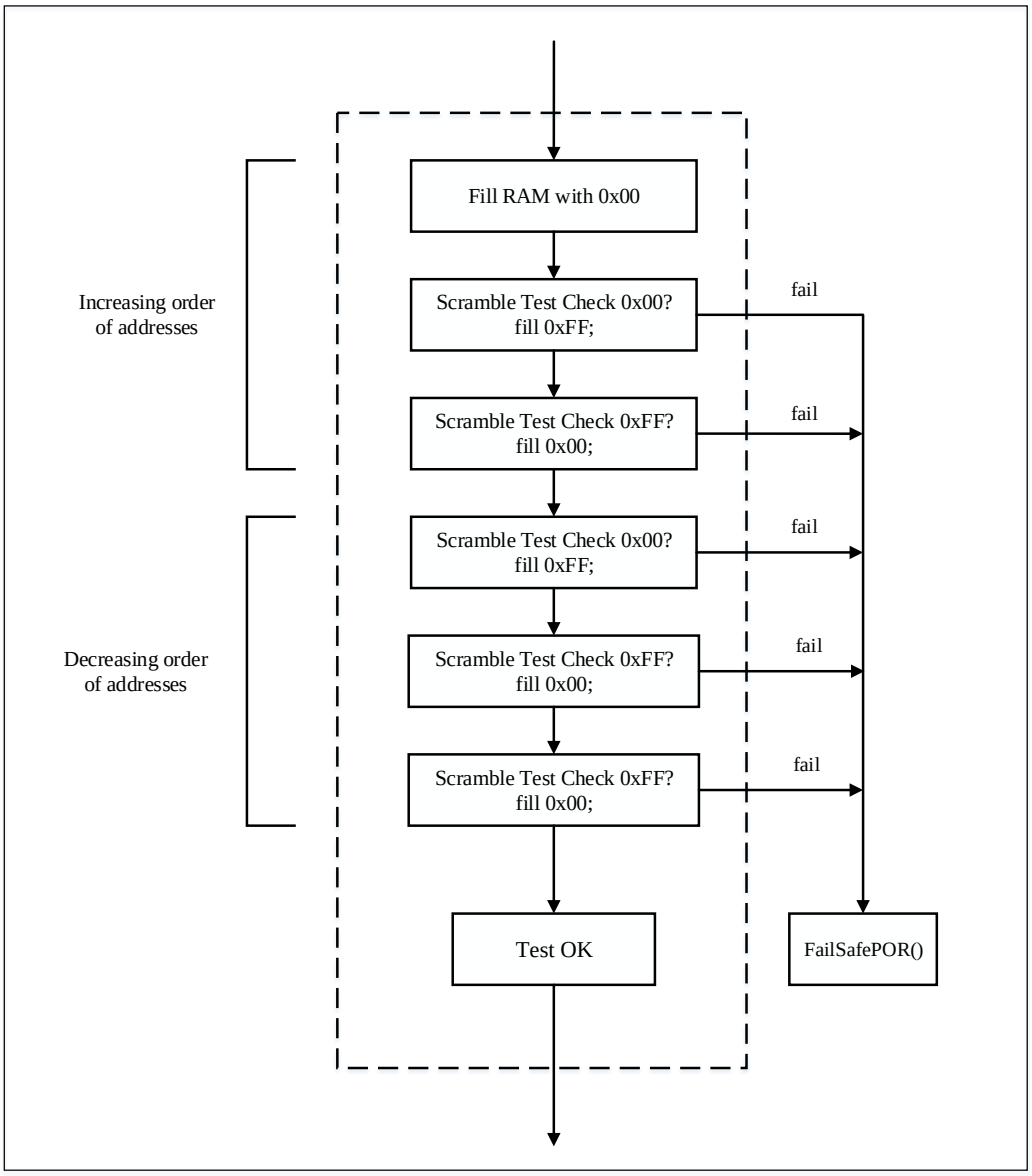
SRAM self-check uses The Mar-C algorithm, which is an algorithm used for SRAM testing of embedded chips as part of security certification.All ranges of SRAM are detected at startup.

First, the whole SRAM is cleared, and then 1 bit by bit, each set one bit, test whether the bit is 1, if it is, continue, if not, an error is reported; After all are set, clear 0 bit by bit. After clearing a bit, test whether the bit is cleared to 0 or not. If it is, it is correct, otherwise, an error is reported. Until the test of the entire RAM space is completed.

The test is 6 cycles, and the whole RAM is checked and filled word by word alternately with the values 0x00 and 0xFF. The first 3 cycles are executed according to increasing address, and the last 3 cycles are executed according to decreasing address.

The whole RAM detection algorithm process is shown in the figure below:

Nations Technologies Inc.
Tel：+86-755-86309900
Email：info@nationstech.com
Address: Nations Tower, #109 Baoshen Road, Hi-tech Park North. Nanshan District, Shenzhen, 518057, P.R.China



2.1.5 Clock startup detection

The test principle is as follows:

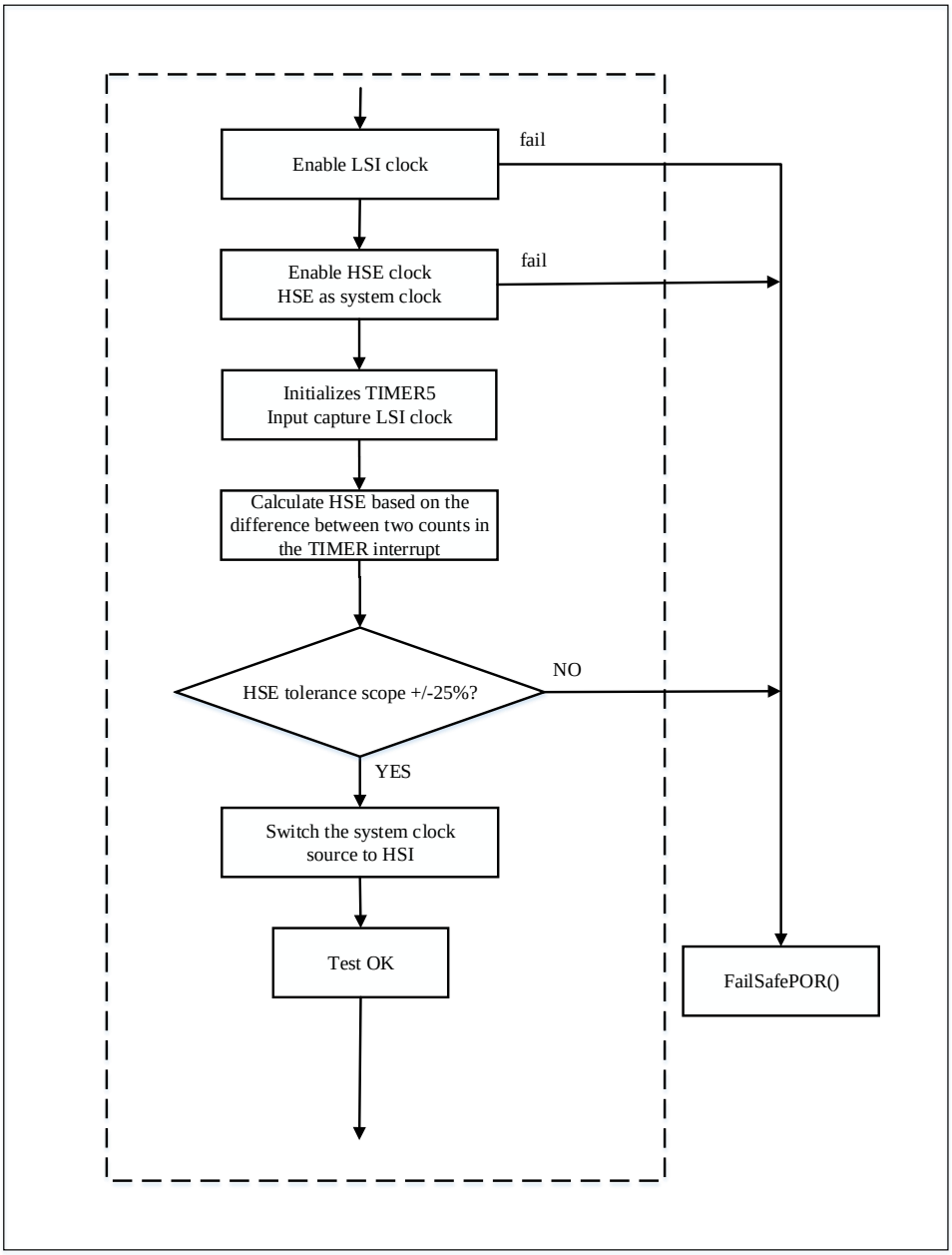
1. Start the internal low-speed clock (LSI) source.

2. To measure HSE, the macro definition selects HSE, starts the external high-speed clock (HSE) source, and configures it as the system clock, otherwise the macro definition selects HSI, and configures the system clock to select PLL (the source is HSI).

3. Initialize TIMER5, input the capture LSI clock; judge in the interrupt, the value obtained by the timer counter two consecutive times is different, so that the ratio between the LSI and HSE frequencies can be obtained.

4. Calculate the HSE frequency and compare the frequency value to the expected range value: if it exceeds +/- 25%, the test fails. Switch the system clock source HSI after the test. The expected range value can be adjusted by the user according to the actual application. The macros are defined as HSE_LimitHigh() and HSE_LimitLow().

Nations Technologies Inc.
Tel：+86-755-86309900
Email：info@nationstech.com
Address: Nations Tower, #109 Baoshen Road, Hi-tech Park North.
Nanshan District, Shenzhen, 518057, P.R.China



2.1.6 Control flow startup detection

The self-check part of the startup ends with the control flow detection pointer program.

Initialize the variables CtrlFlowCnt to 0, CtrlFlowCntInv to 0xFFFFFFFF. In each test step, CtrlFlowCnt adds a fixed value, CtrlFlowCntInv subtracting the same fixed value. At the end of the start self-check, judge whether the sum of the two values is still 0xFFFFFFFF.

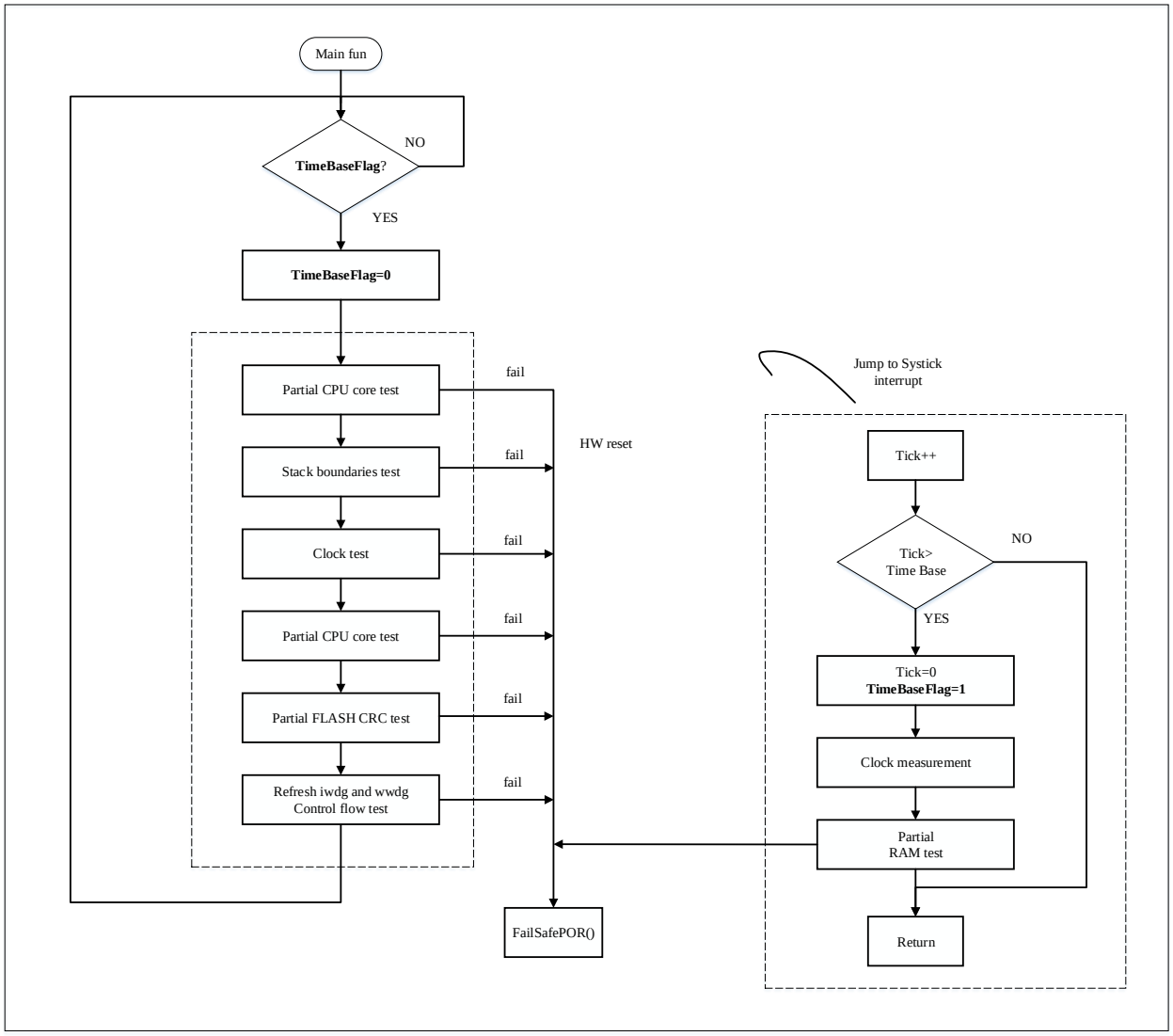
2.2 Run time inspection process

If the startup self-check passes successfully, the run-time periodic self-check must be initialized before entering the main loop.

The runtime checks periodically based on Systick.

The run-time periodic detection process is as follows:

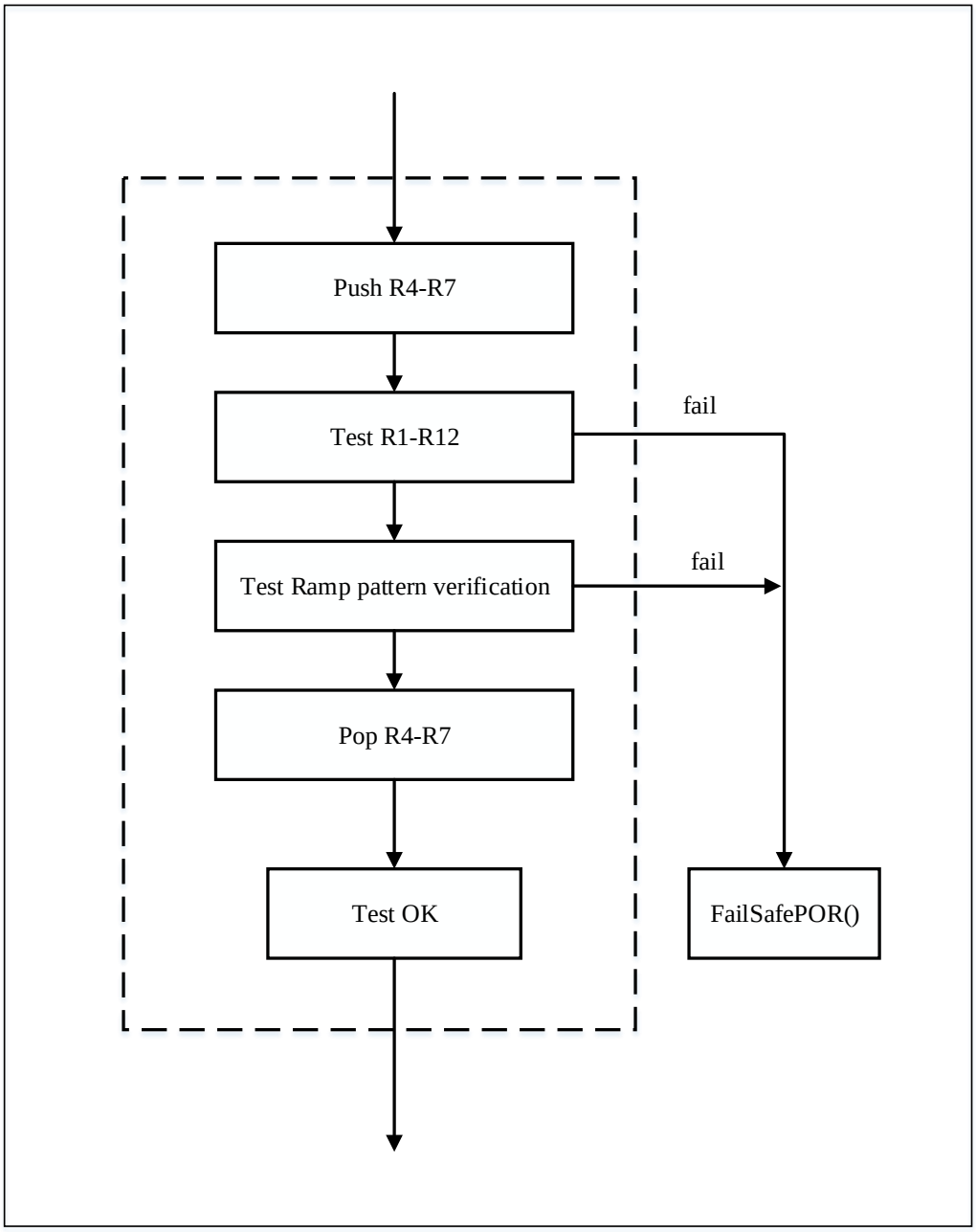
Nations Technologies Inc.
Tel：+86-755-86309900
Email：info@nationstech.com
Address: Nations Tower, #109 Baoshen Road, Hi-tech Park North.
Nanshan District, Shenzhen, 518057, P.R.China



2.2.1 CPU runtime detection

The CPU runtime periodic self-check is similar to the self-check at startup, except that the kernel flags and stack Pointers are not detected.

Nations Technologies Inc.
Tel：+86-755-86309900
Email：info@nationstech.com
Address: Nations Tower, #109 Baoshen Road, Hi-tech Park North.
Nanshan District, Shenzhen, 518057, P.R.China

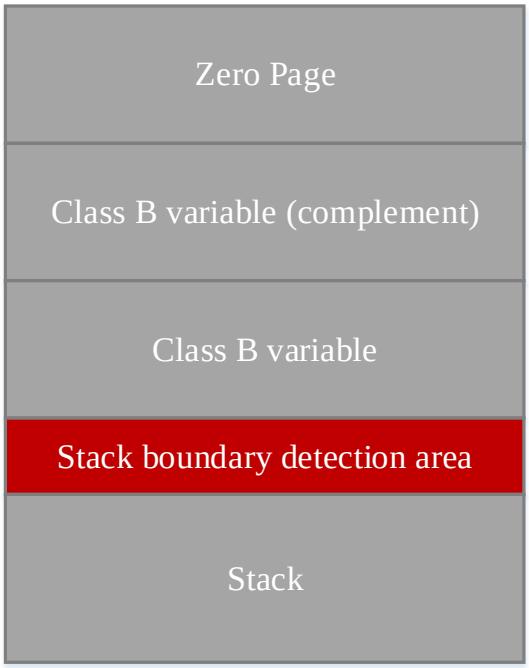


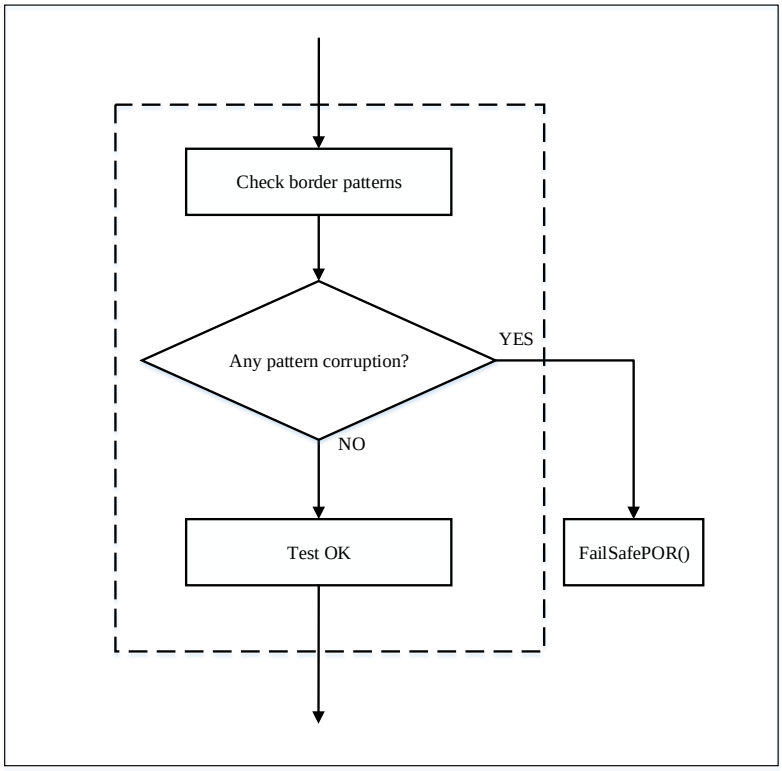
2.2.2 Stack boundary runtime overflow detection

This test detects stack overflow by determining the data integrity of pattern array in the boundary detection area. If the original pattern data is corrupted, the test fails and a fail-safe program is invoked.

The lower address closely following the stack area is defined as the stack boundary detection area. This area can be configured differently depending on the device. The user must define enough areas for the stack and ensure that pattern is placed correctly.

Nations Technologies Inc.
Tel：+86-755-86309900
Email：info@nationstech.com
Address: Nations Tower, #109 Baoshen Road, Hi-tech Park North.
Nanshan District, Shenzhen, 518057, P.R.China

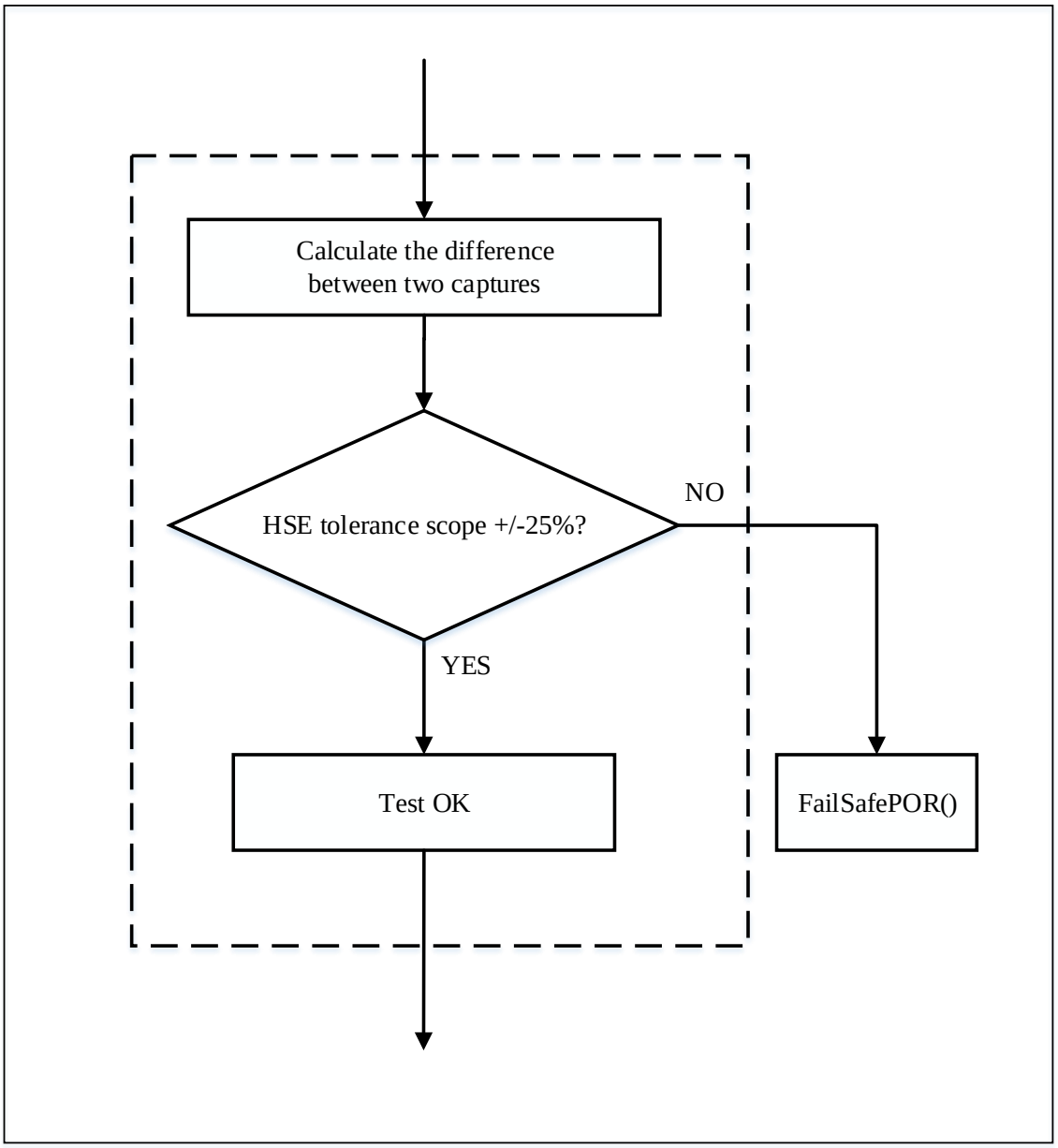




2.2.3 System clock running detection

The detection of the system clock at runtime is similar to the detection of the clock at startup. The HSE frequency is calculated from the difference between the two captures. The process is as follows:

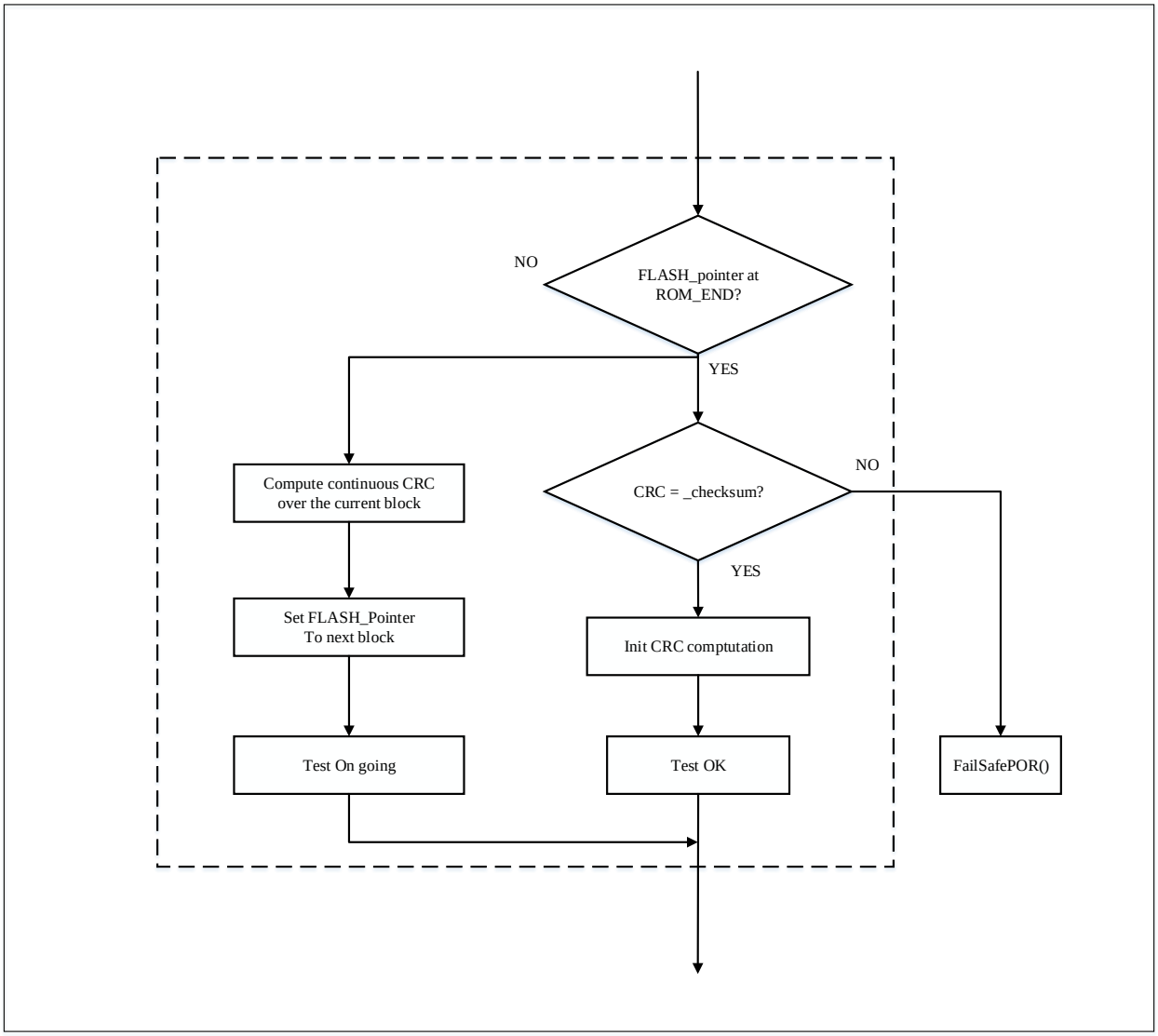
Nations Technologies Inc.
Tel：+86-755-86309900
Email：info@nationstech.com
Address: Nations Tower, #109 Baoshen Road, Hi-tech Park North.
Nanshan District, Shenzhen, 518057, P.R.China



2.2.4 FLASH runtime detection

The Flash CRC self-check is performed during the runtime. Because the detection range varies with the time required, you can configure segmented CRC calculation based on the size of the user application. When the CRC values are calculated to the last range, the CRC values are compared.

Nations Technologies Inc.
Tel：+86-755-86309900
Email：info@nationstech.com
Address: Nations Tower, #109 Baoshen Road, Hi-tech Park North.
Nanshan District, Shenzhen, 518057, P.R.China



2.2.5 Watchdog running detection

During runtime, dogs need to be fed regularly to ensure the normal operation of the system. The watchdog dog feeding part is placed at the end of STL_DoRunTimeChecks().

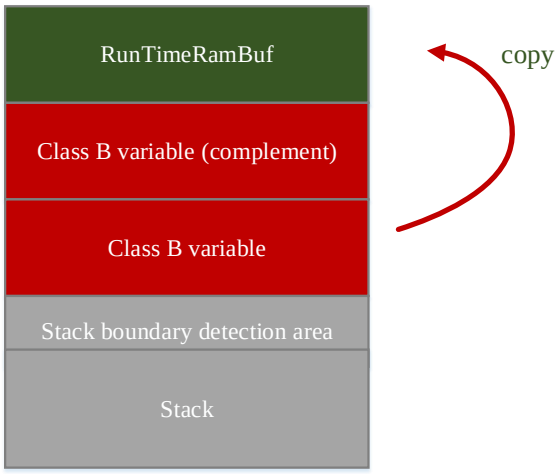
2.2.6 Local RAM runtime self-check

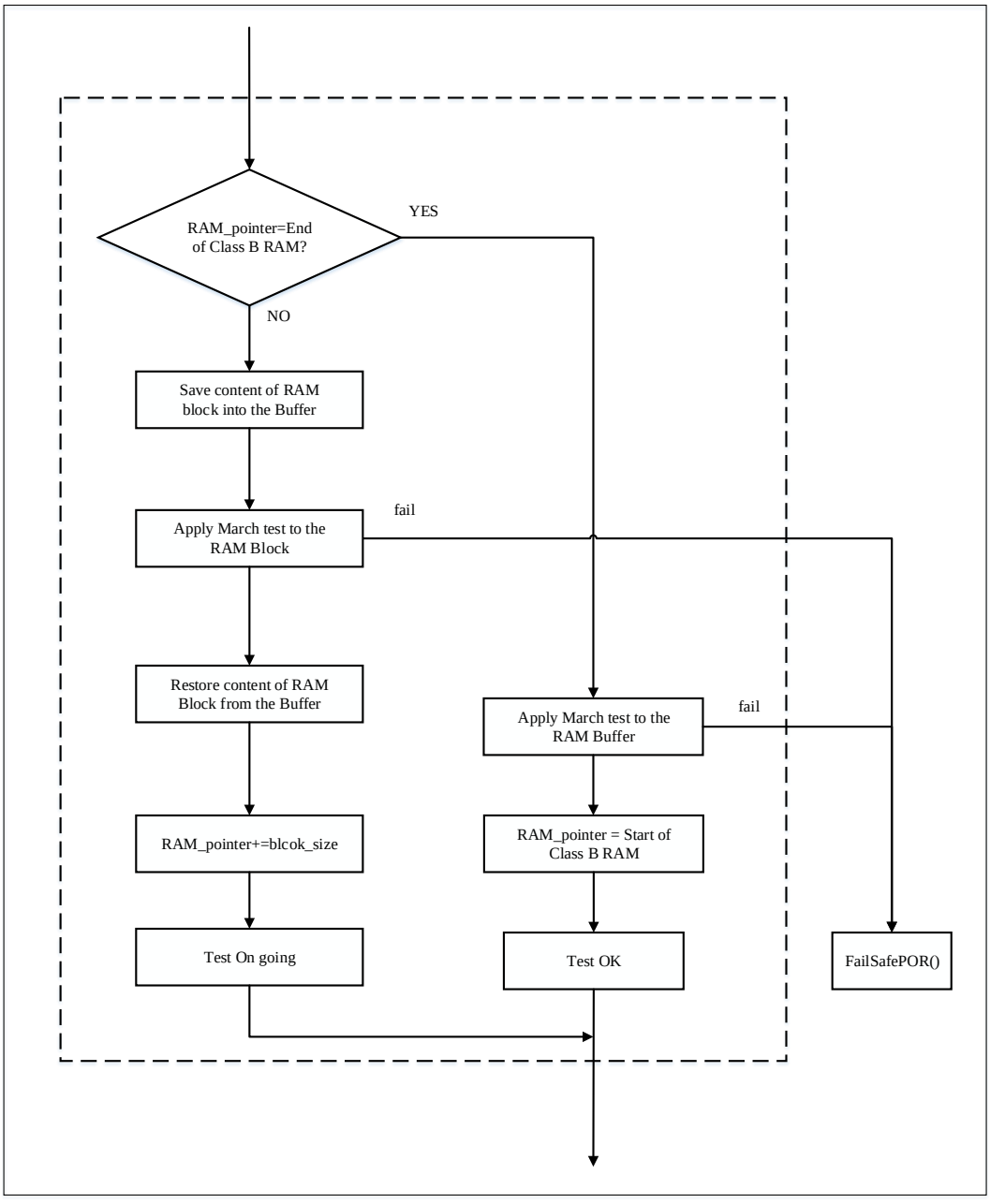
The RAM self-check at run time is done in the Systick interrupt function.The test covers only the portion of memory allocated to the class B variable.

According to the area divided by the class B variable, every 6 bytes is a block. Before the March-C test, save the block data in the RunTimeRamBuf, and then put the RunTimeRamBuf back to the original area of the class B after the test is completed. Until all tests in the class B area are completed.

After the class B zone test is complete, the RunTimeRamBuf zone is march-c tested. After the test is complete, the pointer is restored to the class B start address for the next test.

Nations Technologies Inc.
Tel：+86-755-86309900
Email：info@nationstech.com
Address: Nations Tower, #109 Baoshen Road, Hi-tech Park North.
Nanshan District, Shenzhen, 518057, P.R.China





Nations Technologies Inc.
Tel：+86-755-86309900
Email：info@nationstech.com
Address: Nations Tower, #109 Baoshen Road, Hi-tech Park North.
Nanshan District, Shenzhen, 518057, P.R.China

3. Key points of software library migration

- Before executing the user program, execute the STL_StartUp function (to start the self-check);
- Set WWDG and IWDG to prevent them from being reset when the program is running properly;
- Set up RAM and FLASH detection range at startup and runtime;
  - The range of CRC checksum, and the location where the checksum is stored in the Flash
  - The range of storage addresses for ClassB variables
  - Location of stack boundary detection area
- Troubleshoot detected faults.
- Add user-related fault detection content based on specific applications;
- Define the frequency of program runtime self-check according to the specific application;
- After the chip is reset, the STL_StartUp function must be called for startup self-check before initialization.
- Call STL_InitRunTimeChecks() before entering the main loop, and call STL_DoRunTimeChecks() in the main loop;
- Users can release Verbose comments to enter diagnostic mode and output text information through the Tx pin(PA9) of USART1.

Set the serial port to 115200Bits/s, no parity, 8-bit data, and 1 stop bit.

Nations Technologies Inc.
Tel：+86-755-86309900
Email：info@nationstech.com
Address: Nations Tower, #109 Baoshen Road, Hi-tech Park North.
Nanshan District, Shenzhen, 518057, P.R.China

4. Version history

Version	Date	Note
V1.0	2021-11-06	Create a document
V1.1	2022-2-14	Modify the clock detection method to timer capture

Nations Technologies Inc.
Tel：+86-755-86309900
Email：info@nationstech.com
Address: Nations Tower, #109 Baoshen Road, Hi-tech Park North.
Nanshan District, Shenzhen, 518057, P.R.China

5. Legal Notice

This document is the exclusive property of Nations Technologies Inc. (Hereinafter referred to as NATIONS). This document, and the product of NATIONS described herein (Hereinafter referred to as the Product) are owned by NATIONS under the laws and treaties of the People's Republic of China and other applicable jurisdictions worldwide.

NATIONS does not grant any license under its patents, copyrights, trademarks, or other intellectual property rights. Names and brands of third party may be mentioned or referred thereto (if any) for identification purposes only.

NATIONS reserves the right to make changes, corrections, enhancements, modifications, and improvements to this document at any time without notice. Please contact NATIONS and obtain the latest version of this document before placing orders.

Although NATIONS has attempted to provide accurate and reliable information, NATIONS assumes no responsibility for the accuracy and reliability of this document.

It is the responsibility of the user of this document to properly design, program, and test the functionality and safety of any application made of this information and any resulting product. In no event shall NATIONS be liable for any direct, indirect, incidental, special, exemplary, or consequential damages arising in any way out of the use of this document or the Product.

NATIONS Products are neither intended nor warranted for usage in systems or equipment, any malfunction or failure of which may cause loss of human life, bodily injury or severe property damage. Such applications are deemed, "Insecure Usage".

Insecure usage includes, but is not limited to: equipment for surgical implementation, atomic energy control instruments, airplane or spaceship instruments, all types of safety devices, and other applications intended to support or sustain life.

All Insecure Usage shall be made at user's risk. User shall indemnify NATIONS and hold NATIONS harmless from and against all claims, costs, damages, and other liabilities, arising from or related to any customer's Insecure Usage.

Any express or implied warranty with regard to this document or the Product, including, but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement are disclaimed to the fullest extent permitted by law.

Unless otherwise explicitly permitted by NATIONS, anyone may not use, duplicate, modify, transcribe or otherwise distribute this document for any purposes, in whole or in part.

Nations Technologies Inc.
Tel：+86-755-86309900
Email：info@nationstech.com
Address: Nations Tower, #109 Baoshen Road, Hi-tech Park North.
Nanshan District, Shenzhen, 518057, P.R.China