AN3181
Application note

Guidelines for obtaining IEC 60335 Class B certification in an STM8 application

Introduction

The role of safety has become very important for electronics applications. The level of safety requirements for components used in electronic designs is steadily increasing. The manufacturers of electronic devices include many new technical solutions in the design of new components. Software techniques for improving safety are continuously being developed.

The current safety recommendations and requirements are specified at worldwide level by recognized international standards bodies such as IEC (International Electrotechnical Commission) and come under the compliance, verification and certification process of testing houses and authorities like VDE (Association for Electrical, Electronic and Information Technologies). The certification process is closely associated with ElectroMagnetic Compatibility (EMC) tests when the robustness of the system against noise emission and noise sensitivity is tested for compliance with international standards.

The main purpose of this application note and its associated software is to facilitate and accelerate user software development and certification processes for appliances which are subject to these requirements and certifications and are based on some of the ST 8-bit family of microcontrollers.

Three packages certified by VDE are provided for:

- Mainstream STM8S and automotive STM8A high, medium and low density devices,
- Ultra-low power medium-density STM8L and STM8AL devices
- Ultra-low power low density STM8L, STM8AL and STM8TL touch-sensing devices.

Due to limited memory capacity of most of 8-bit devices all these packages are optimized and independent from other firmware libraries published by ST. Proper headers *stm8xxx.h* and *stm8xxx_type.h* from ST standard peripheral libraries are included only to keep consistency of names of registers, bit masks and constants defined there. Optimized code reduces program memory overhead and increases the code execution speed.

All certified packages use similar principles described by this document, with focus on main differences. While using hardware and firmware (see *Appendix A: STM8 Class B firmware package variations*) compatibility between ST families, these packages can also be adapted for some other ST 8-bit microcontrollers not yet certified.

Table 1 lists the microcontrollers concerned by this application note.

Table 1. Applicable products

Type	Product category
Microcontrollers	STM8xxxx

Contents

List of figures

1 Package variation overview

Available configurations of **STM8S/A package** support the following devices in the families:

- STM8S high-density Performance line devices with 32-128 Kbytes Flash memory (like STM8S20x)
- STM8S medium- and low-density Access line devices with 4-32 Kbytes Flash memory (like STM8S105x, STM8S103x)
- STM8S high-, medium- and low-density Value Line devices with 4-64 Kbytes Flash memory (like STM8S007x, STM8S005x, STM8S003x)
- STM8S low-density Application specific devices with 8 Kbytes Flash memory (like STM8S903x)
- STM8A high-density CAN line devices with 32-128 Kbytes Flash memory (like STM8AF5xxx)
- STM8A high and medium density Standard line devices with 8-128 Kbytes Flash memory (like (STM8AF6xxx)

Available configurations of medium-density **STM8L/AL package** support the following devices in the ultra-low power families:

- STM8L medium density standard devices with 4-64 Kbytes Flash memory (like STM8L15xx)
- STM8L medium-density Value Line devices with 4-64 Kbytes Flash memory (like STM8L05xx)
- STM8AL medium-density devices with up to 32 Kbytes Flash memory (like STM8AL31xx, STM8AL3Lxx)

Available configurations of low-density **STM8L/AL/TL package** support the following devices in the ultra-low power families:

- STM8L low density standard devices with up to 8 Kbytes Flash memory (like STM8L10xx)
- STM8AL low density devices with up to 8 Kbytes Flash memory (like STM8AL30xx)
- STM8TL low density devices with up to 16 Kbytes Flash memory and touch sensing interface (like STM8TL53xxx)

All these firmware packages are available for free download from the ST web.

Three projects have been prepared and tested for each package under following environment and toolchains:

1. IAR Embedded Workbench® for STM8 IDE (EWSTM8™) with IAR C-Compiler™ version 1.30
2. ST Visual Develop (STVD) version 4.3.0 with Cosmic STM8 C-compiler 32 K version 4.3.6
3. ST Visual Develop (STVD) version 4.3.0 with Raisonance STM8/ST7 C-compiler version 2.38

For more ElectroMagnetic Compatibility (EMC) information please refer to the following related application notes:

- AN1015 application note, Software techniques for improving microcontroller EMC performance
- AN1709 application note, EMC design guide
- AN2860 application note, EMC guidelines for STM8S

2 Compliance with IEC and VDE standards

The IEC (International Electrotechnical Commission) is a non-profit and non-governmental authority recognized worldwide for preparing and publishing international standards for a vast range of electrical, electronic and related technologies. IEC standards are focused mainly on safety and performance, the environment, electrical energy efficiency and its renewable capabilities. The IEC cooperates closely with ISO (International Organization for Standardization) and ITU (International Telecommunication Union). Their standards define not only the recommendations for hardware, but also for software solutions. Standards are divided into a number of safety classes depending on the purpose of the application.

The other bodies that are recognized worldwide in the field of electronic standard organizations are VDE in Germany, IET in the United Kingdom and the IEEE in the United States. The VDE association also includes a Testing and Certification Institute which is a pioneer of software safety inspection. This is a registered National Certification Body (NCB) for Germany. The main purpose of this testing house is to offer standards compliance and quality testing services to manufacturers of electrical appliances.

One of the pivotal IEC standards is the IEC 60335-1 norm, which covers safety and security of household electronic appliances destined for domestic and similar environment. Appliances incorporating electronic circuits are subject to component failure tests. The basic principle is that the appliance must remain safe in the case of any component failure. The microcontroller is an electronic component just like any other from this point of view. If safety relies on an electronic component, it must remain safe after two consecutive faults. This means the appliance must stay safe with one hardware failure and with the microcontroller not operating (under reset or not operating properly).

If the safety depends on software, the software is taken into account with the second applied failure. The conditions required for software are defined precisely in Annex Q of the IEC 60335-1 norm. Three classes of appliances are defined here:

- **Class A**: Safety does not rely on software
- **Class B**: Software prevents unsafe operation
- **Class C**: Software is intended to prevent special hazards

This application note and the associated ST software package covers the group B specification. Appliances under group C need some other special requirements such as dual microcontroller operation, which is outside the scope of this document.

Class B compliance aspects for microcontrollers are related both to hardware and software. A list of microcontroller parts under compliance is evaluated at IEC 60335-1 Annex T which refers to IEC 60730 Annex H. This list can be divided into two groups - micro-specific and application-specific items. (see *Table 2: MCU components to be tested for Class B compliance*).

While application-specific parts rely on customer application structure and must be defined and developed by users (communication, I/O control, interrupts, analog inputs and outputs), micro-specific parts are related purely to the micro structure and can be made generic (core self-diagnostic, volatile and non-volatile memory integrity checking, clock system tests). This group of micro-specific tests is the focus of the ST solution based on powerful hardware features of STM8 MCU such as dual independent watchdogs or clock sources.

It is important to note that there are several other peer recognized bodies concerning electronic safety standards besides IEC, such as VDE in Germany, IET in the United Kingdom and the IEEE in the United States. In addition, an increasing number of product

safety standards are being harmonized to international safety standards. For example, the UL 60335-1, the DSA 60335-1 and the EN 60335-1 are all documents which are based on the IEC 60335-1. VDE also includes a Testing and Certification Institute which is a pioneer of software safety inspection. This is a registered National Certification Body (NCB) for Germany. The main purpose of this testing house is to offer standards compliance and quality testing services for electrical appliance manufacturers. The STM8 FW in this package has been VDE certified.

Table 2. MCU components to be tested for Class B compliance

Group	Components to be tested
Micro specific	CPU registers
	CPU program counter
	Clock
	Fixed and variable memory spaces
	Internal addressing
	Internal data path
Application specific	Interrupt handling
	External communication and addressing (if any)
	Timing
	I/O periphery
	ADC and DAC
	Analog multiplexer

2.1 Generic tests included in the ST firmware library

STM8 firmware library packages include the following microcontroller specific software modules, which have also been certified by VDE:

- CPU registers test
- clock monitoring
- RAM functional check
- FLASH checksum integrity check
- watchdog self-test
- stack overflow monitoring

An overview of the methods used for these MCU-specific tests is given in *Table 3* and they are described in more detail in the following chapters. The last two items from the list above are not explicitly asked for by the norm, but they improve overall fault coverage.

Table 3. Overview of methods used in micro-specific tests provided with this application note

Components to be verified	Method used
CPU registers	Functional test A, X and Y registers, flags and stack pointer is done at startup. In the run time flags are not tested. Stack pointer is tested for overflow and underflow. If any error is found, the software jumps directly to the Fail Safe routine.
Program counters	Two different watchdogs driven by two independent clock sources can reset the device when the program counter is lost. The Window watchdog (driven by main oscillator) performs time slot monitoring(1)while the Independent one (driven by low speed internal RC oscillator) is impossible to disable once enabled. Both watchdogs must be serviced at regular intervals. Program control flow is monitored by specific software method, additionally. (see *Section 3.1.3*).
Addressing and data path	This is tested indirectly by RAM functional and Flash integrity tests, stack overflow (a specific pattern is written at a low boundary of stack space and checked for corruption at regular intervals) and underflow (a second pattern is written at a high boundary if it is not at the RAM end).
Clock	Two independent internal frequencies are used for the dedicated timer clock and they are verified by reciprocal comparison. One frequency is fed into the dedicated timer while the other gates it.
Non-volatile memory	A 16-bit CRC software checksum test of the entire memory is done at startup and a partial memory test is repeated at runtime (block by block).
Variable memory space	March C- (March X optionally) full memory test is done at startup. Partial memory test is repeated at run time (block by block). Word protection with double inverse redundancy (inverse values stored in non-adjacent memory space) is used for safety critical Class B variables. Class A variable space, stack and unused space are not tested at run time.

1. Window WDG feature is not available at STM8L10x devices.

The user can include a part or all of these VDE certified software modules into his project. If the modules stay unchanged and are integrated in accordance with the guidelines provided in this application note, development time and costs to have end-application certification would be significantly reduced.

2.2 Application specific tests

The user should be aware that the following are also required for Class B certification but are not included in the ST firmware library:

- Analog: ADC/DAC & multiplexer
- I/Os
- Interrupts and external communication
- Timing
- External addressing

2.2.1 ADC/DAC

Analog components depend on device's application and peripheral capabilities. Used pins should be checked at correct intervals. Free analog pins can be used for checking user analog reference points. Internal references should be checked, too.

2.2.2 I/Os

Class B tests must detect any malfunction on digital I/Os. This could be covered by plausibility checks together with some other application parts (e.g. change in an analog signal from temperature sensor when heating/cooling digital control is switched on/off).

2.2.3 Interrupts and external communication

Application interrupts occurrence and external communications can be checked by different methods. One of them could be a control using a set of incremental counters where every interrupt or communication event increments a specific counter. The values in the counters are then verified at given time intervals by cross-checking against some other independent time base.

2.2.4 Timing

Timing could be verified by ensuring that the application routines execution times are correct and that there are no unexpected delays. A cross-check with a different time base could be done. Timing control is strictly dependent on the application.

2.2.5 External addressing

External addressing is not used with STM8 microcontrollers.

3 Class B software package

This section highlights the basic common principles used in ST software solution. The workspace organization under different tools is described together with its configuration and debugging capabilities.

3.1 Basic software principles

The basic software methods and common principles used for all the tests included in the ST firmware library are described in detail at this section.

3.1.1 Fail Safe mode

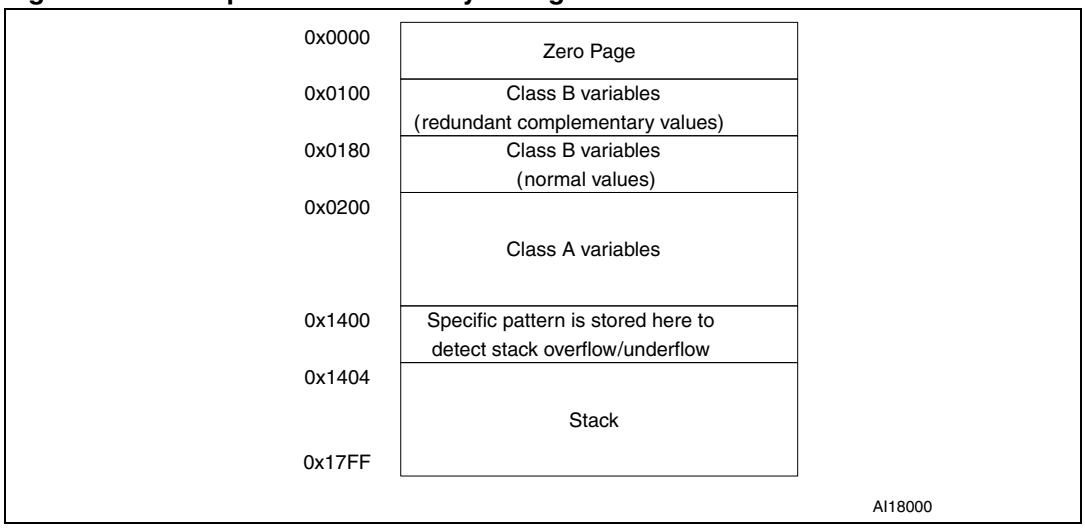
FailSafe() routine is called (defined in ***stm8x_stl_startup.c*** file) at any fail detection. The program stays in a never ending loop waiting for WDG reset. Except for some debugging features, the routine is almost empty. When editing this routine, the user must remember to include procedures necessary to keep the application in a safe state.

If the user wants to recognize the error raised, the debug or verbose mode described in *Section 3.3: Package configuring and debugging* can be used. In debug mode the independent WDG is refreshed inside the never ending loop to prevent resetting the microcontroller when a failure occurs.

3.1.2 Class B variables

Class B variables are dedicated variables defined by the user as critical to the application. They are always stored as a pair of complementary values in two separate RAM areas. Both normal and redundant values are always placed into non-adjacent memory locations. Partial transparent RAM March C- or March X test is performed permanently on these two regions through the system interrupt routines in run mode. The integrity of the pair is compared before the value is used. If any value stored is corrupted, ***FailSafe()*** routine is called. An example of RAM configuration is shown in *Figure 1*. The user can adapt the RAM space allocation according to application needs and with respect to device hardware capability.

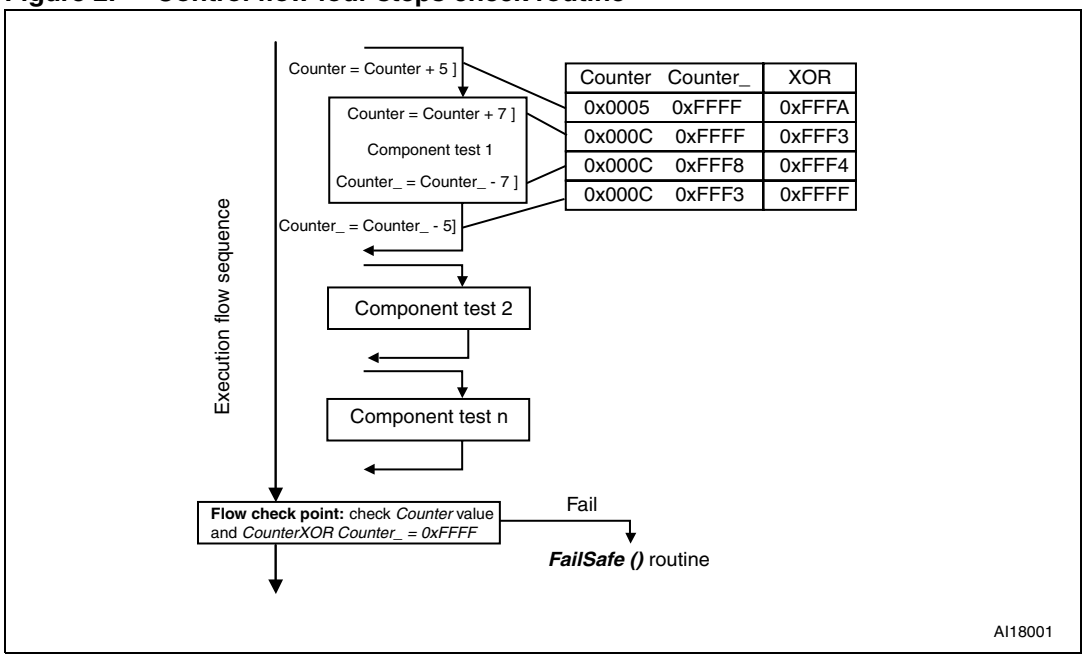
Figure 1. Example of RAM memory configuration for STM8S20x



3.1.3 Class B flow control

A specific method is used to test and check program execution flow. Unique user defined numbers are assigned for every software execution block. These unique numbers are stored in two complementary counters. When a block is executed, a symmetrical four step change of the counter pair content is done (add or subtract the label values). The first two steps check if the block is correctly called from main flow level (processed just before calling and just after return from the called procedure). The next two steps check if the block is correctly completed (processed just after enter and just before return from the procedure). An example is given in *Figure 2* where a routine performing a component test is called in the control flow sequence and the four step checking service is shown. This method decreases CPU load as the check is done by counting one member of the complementary counter pair only. As there is always the same number of call/return and entry/exit points, the value stored in the counter pair must be always complementary after any block is processed. Several flow check points are placed subsequently in the code flow. Counter integrity is always checked here and any unexpected value results in calling the ***FailSafe()*** routine.

Figure 2. Control flow four steps check routine



1. For this example, the unique number for Component test 1 is “5” and for the procedure itself it is defined as “7”. The counters are initialized to 0x0000 and 0xFFFF. The table in the upper right corner in *Figure 2* shows how the counters are changed in four steps. Also shown is their complementary value after the last step (return from procedure) is done.

3.2 Package organization

This section describes how the ST solution is organized.

3.2.1 Projects and workspaces included in the package

Three projects have been prepared for each package using different toolchains. The project for IAR C-compiler is done under IAR EWSTM8 environment, while projects for both Cosmic and Raisonance C-compilers are done as ST Visual Develop (STVD) project workspaces. The corresponding Project.eww or Project.stw project file must be configured for a specific STM8x device settings and adequate workspace configuration before any compilation.

3.2.2 Tool specific integration of the library

Each project covers all settings and includes needs for both compilation and linking processes. User has to check the symbols defined for preprocessor at project settings as these symbols configure the project main structure and used features. The user can make detailed configurations at library parametric header file (see *Section 3.3: Package configuring and debugging*). Predefined linker script files **.icf* are included at IAR projects for different microcontrollers. Linker script files **.lkf* for STVD projects are generated automatically and placed into DEBUG or RELEASE directories. User can make a copy of these files, edit them and force compiler to use the overwritten file.

Reset handler must be modified to perform *STL_StartUp* function after reset before standard C-compiler initialization starts. Therefore startup assembly file *csstartup.s* (IAR) or *startup.asm* (Raisonance) must be modified in that way. For Cosmic, the reset handler is changed at *stm8_interrupt_vector.c* file.

Caution: Be careful when invariable **memory checksum setting** is configured for the project. It is quite different for different compilers. IAR compiler uses project option setting applied at its specific Checksum card window of linker. When Raisonance C-compiler is used, user should define checksum range and its placement using user defines option declared at the project settings:

- CRCRANGE(*begin_address*, *end_address*) - continuous space under CRC computation
- CRCPLACE(*crc_address*) - placement of CRC result
- FILLGAP(*fill_constant*) - setup of unused memory areas

Cosmic C-compiler requires to define all the segments under checksum computation (by adding *-ck* parameter to each of them) and specific *checksum* segment keeping the checksum descriptor table must be included into the project and allocated at invariable memory additionally with applied *-ik* parameter.

Specific segments for Class B variables and checking stack overflow must be added into project and allocated at variable memory, too. Double storage in CLASS_B_RAM and CLASS_B_RAM_REV separated segments is necessary to ensure the redundancy of the safety critical data (Class B). All other variables defined without any particular attributes are considered as Class A variables and their storage area is not checked during the transparent RAM test. The size and allocation of these segments can be modified at linker script files or directly by project settings.

A new Class B variable must be declared as a complementary pair of two variables allocated at different segments by definition placed into proper part of the **stm32fxxx_STLclassBvar.h** header file.

The following syntax is used for the compilers:

Cosmic

EXTERN @near u16 MyClassBVariable;

....

EXTERN @near u16 MyClassBVariableInv;

IAR

EXTERN __near u16 MyClassBVariable @ "CLASS_B_RAM";

.....

EXTERN __near u16 MyClassBVariableInv @ "CLASS_B_RAM_REV";

Raisonance

EXTERN near u16 MyClassBVariable;

.....

EXTERN near u16 MyClassBVariableInv;

Note: When the version of STVD tool does not support including the vector table content into the checksum computation and the user wants to protect this part of the code, the proper linker script file must be modified by placing the vector table as follows:

The line: "+seg .const -b 0x8000 -k" must be replaced by: "+seg .const -b 0x8000 -k -ck".

Note: Previously, "__ckdend__" symbol definition needed to be to included into linker script file for some older versions of Cosmic compiler. There is no longer any need to use it.

3.2.3 Application demonstration example

A short example of user application is attached in each project ***main.c*** file with respect to the package integration criteria (see *Chapter 4: Class B solution structure*). Except for STM8L_10x, the examples were written to run on the corresponding STM8 evaluation boards (STM8S/128-EVAL and STM8L1526-EVAL) as Class B package demonstration firmware. They use on board LCD and LED diodes to display current versus initial master clock frequency measurement changes. Display or LED outputs can be disabled in ***main.h*** file. The main loop also performs initialization and calling all run mode tests at ordinary intervals.

3.3 Package configuring and debugging

A functional part of the package may need to be changed, suspended, excluded or included. For example the microcontroller type might need to be changed or there could be a non-volatile memory space limitation. Modifications are also required to debug the user application. This section describes how the ST solution can be configured, modified and debugged.

3.3.1 Configuration control

Software configuration is done at two levels. The first one is automatic and consists of configuring the project for a given microcontroller. This is done by selecting the corresponding device project while adapting its preprocessor user-defined options. The second one is done through user configuration. All user defined configuration settings are collected in the Class B configuration file ***stm8x_stl_param.h***. The user must be very careful when modifying this file. Most of the package functional blocks are under conditional compilation controlled by a predefined set of constants in this file.

It is possible to disable some part(s) of the library by putting definitions in comments. This is useful e.g. disable Flash CRC when break points are inserted to debug the code. The full Class B package, even optimized and with disabled verbose messages, takes about 3.5 Kbytes of code memory. Disabling some library parts could be required for microcontrollers where the memory space is too small for application needs or when the tested parts are not included in the application (e.g. HSE testing).

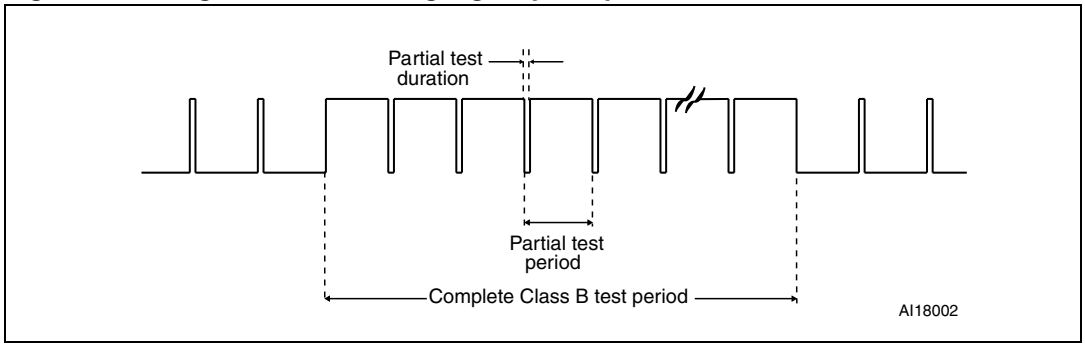
3.3.2 Verbose diagnostic mode

The Tx pin of dedicated UART interface is used to output text messages in verbose mode. This mode is useful in debug phase as the interface can be connected to an external terminal (the line setting is 115200 Bd, no parity, 8-bit data, 1 stop bit). However the text messages consume too much code space in this mode. Different levels of verbose mode can be enabled or disabled by the user through definition of constants in the Class B configuration file ***stm8x_stl_param.h***. For example, verbose mode could be limited to startup, run mode or fail case only.

LEDs toggling is another way to verify a Class B event. First LED toggles at each begin and end of run mode checks and with every successful finish of program memory test. Next LED toggles with each begin and end of RAM partial check called on at each tick interrupt and with every successful finish of the RAM memory test. LEDs slow toggling signals the main processes and quick pulses modulated on the slow signal correspond to the length of partial services, in other words, the loading time (see *Figure 3*). LED control can be disabled by user in Class B configuration file ***stm8x_stl_param.h***.

Note: Verbose mode via UART line is not used at STM8L10x package. Error codes are passed to FailSafe() routine instead.

Figure 3. Diagnostic LED timing signal principle



3.3.3 Debugging the package

While debugging the package, it is useful to disable:

- Reset in ***FailSafe()*** routine by servicing independent WDG,
- All program memory CRC checksum tests when using breaks in the code to prevent program memory checksum error occurrence
- Window WDG to prevent improper service out of the time slot window dedicated to refresh[(a)].
- Control flow monitoring (mostly done automatically by changing values of constants when some tests are omitted)

At the debugging phase it may be useful to enable:

- Verbose Diagnostic mode to watch messages at UART terminal
- LEDs toggling to see basic process flow

a.Window WDG feature is not available at STM8L10x devices

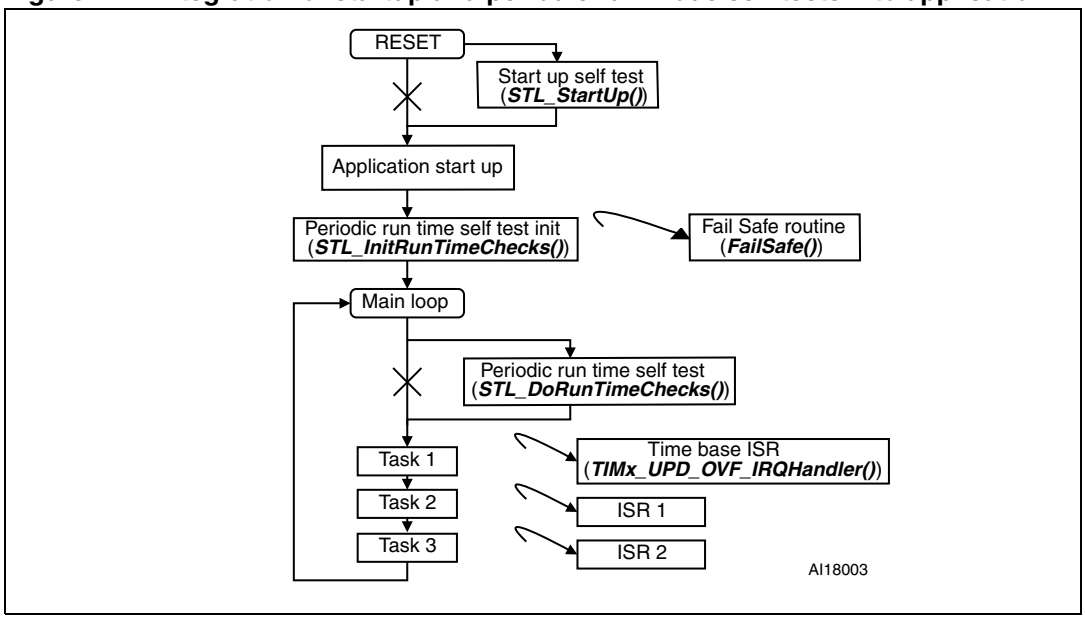
4 Class B solution structure

4.1 Integrating software into user application

Class B routines are divided into two main processes: periodic run mode self tests and startup tests. The periodic run mode test must be initialized by the set-up block before it is applied. All the blocks are checked by sufficient flow control checked at a number of flow check points (see *Section 3.1.3: Class B flow control*). All class B variables are kept redundantly in a pair of control registers stored in the Class B variable space defined by user (see *Section 3.1.2: Class B variables*). This variable space is split into two separate RAM regions which are permanently undergoing the transparent test as a part of run mode tests.

Figure 4: Integration of startup and periodic run mode self tests into application shows the basic principle of how to integrate the Class B software package into user software. The reset vector should be forced by the user to ***STL_StartUp()*** routine which collects all system startup self tests. If they pass successfully, then the standard initialization procedure of C-compiler routine is performed. While the application is running, periodic tests must be executed at regular intervals. To ensure this, the user must initialize these tests by calling the initialization routine ***STL_InitRunTimeChecks()*** before entering main loop and then inserting a periodical call of ***STL_DoRunTimeChecks()*** at main level. For best results, this should be inside the main loop. TIM4 (or TIM6 for some devices), which is configured during initialization routine to generate periodic system interrupts, provides the time base for all the tests. Short partial transparent RAM March C- or March X check is performed at each interrupt tick. If any self test fails, ***FailSafe()*** routine is called.

Figure 4. Integration of startup and periodic run mode self tests into application



4.2 Detailed description of startup self tests

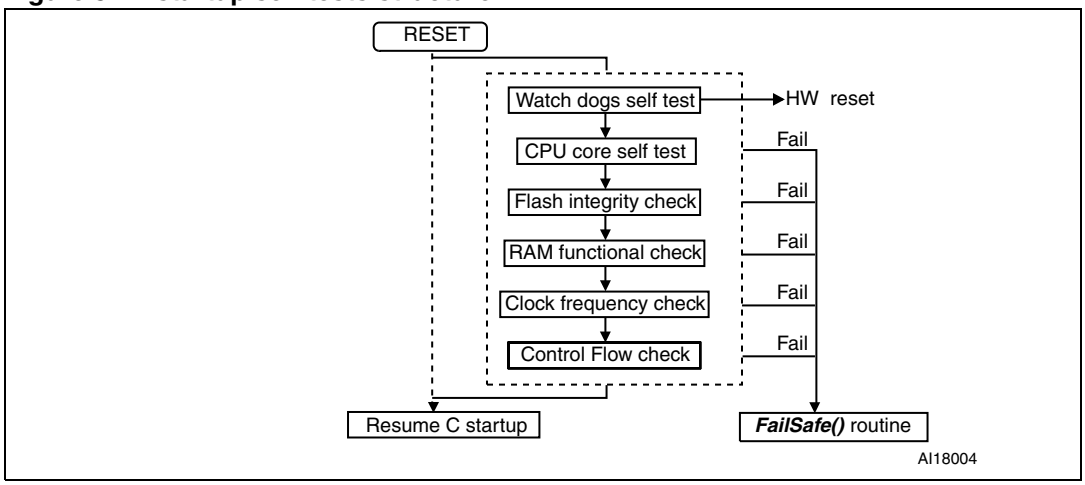
The startup self test is forced during initialization phase as the earliest checking process after resetting the microcontroller (see *Figure 4*) and before standard application startup

routine. The user must force the reset vector to the first address in ***STL_StartUp()*** routine. The startup tests block structure is shown in *Figure 5* and includes the following self tests:

- Watch dogs startup test
- CPU startup test
- Flash complete checksum test
- Full RAM March C-/X test
- Clock startup test
- Control flow checks

These blocks are described in more details in the next chapters. User can control including them as usual in the configuration file ***stm8_stl_param.h***.

Figure 5. startup self tests structure

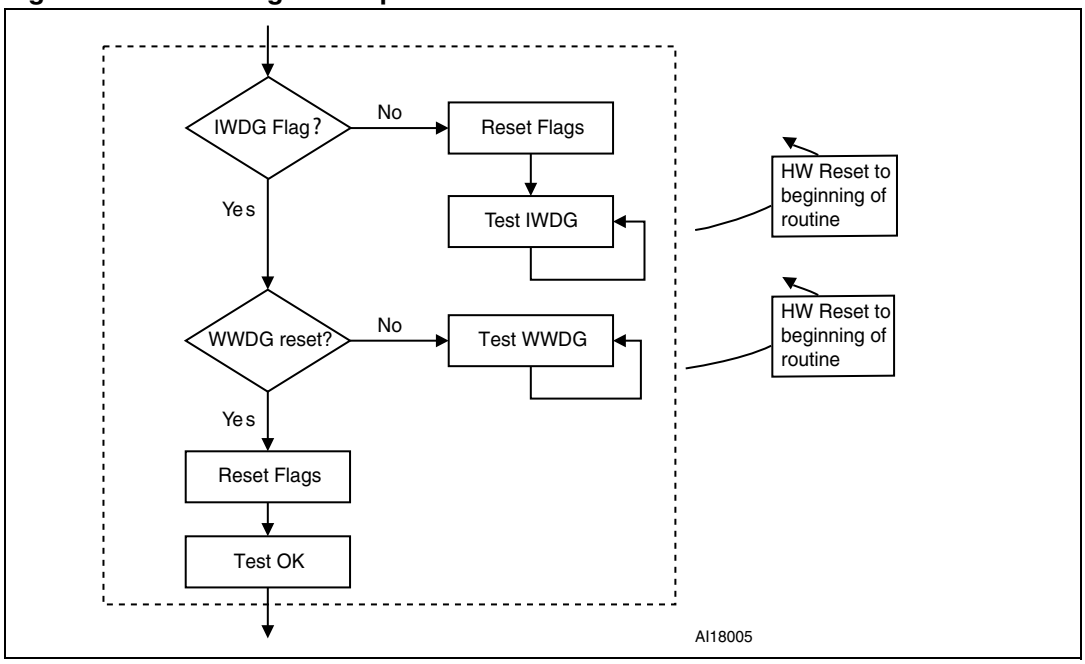


4.2.1 Watchdog startup self test

The first startup self test is to enter WDG self test routine. The program passes through this routine three times. First the routine checks the reset source in reset status register. If Independent watchdog (IWDG) is not flagged in reset status register, then reset sources is cleared and IWDG test begins. The IWDG is set to the shortest period and the microcontroller is reset by hardware and IWDG flag is set (see *Figure 6*). The routine comes back to the beginning and check WDG flags. When IWDG is recognized, it looks for WWDG flag. If WWDG is not flagged, the test continues a second time with window watchdog (WWDG) test. Again the microcontroller is reset by hardware and WWDG flag is set. When both WDG flags are set in the reset status register, the test is assumed as finished and both flags are cleared. WWDG is not present at STM8L10x devices, so WWDG test is not present.

User must carefully set both IWDG and WWDG periods. Time periods and window refresh parameters must be set according to the time base interval because refresh is done at the successful end of the periodical run mode test in main loop.

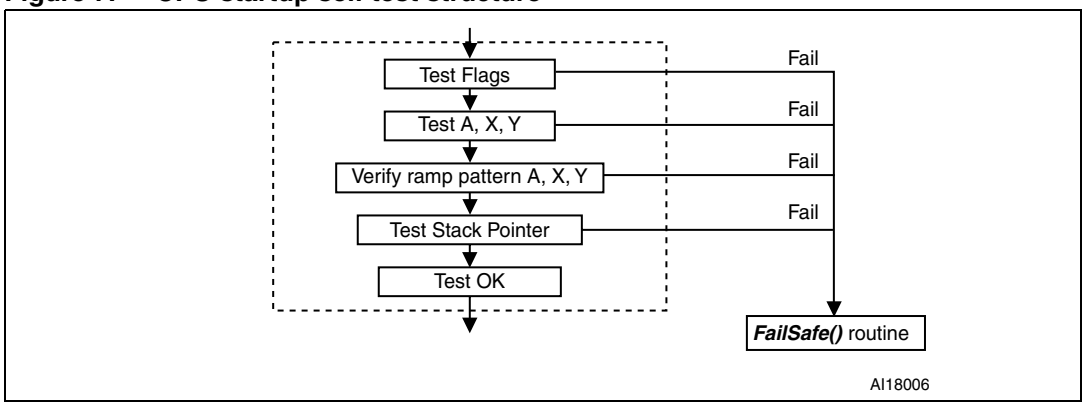
Figure 6. Watchdogs startup self test structure



4.2.2 CPU startup self test

Core flags, registers and stack pointer are tested for functionality. In case of any error, ***FailSafe()*** routine is called.

Figure 7. CPU startup self test structure



4.2.3 Flash complete checksum self test

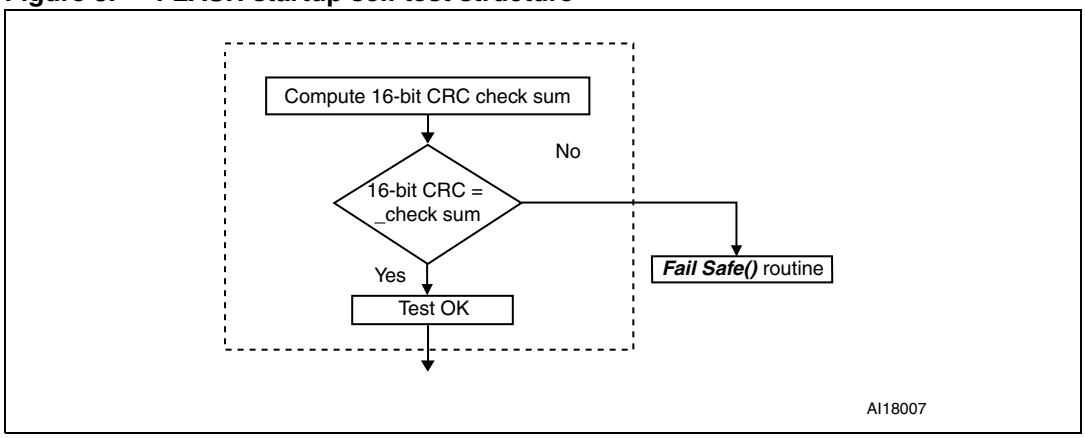
The CRC checksum computation is performed over the entire Flash memory space announced by linker checksum structure. The resulting computation is compared with the linker result. ***FailSafe()*** routine is called if there is an error.

The user actually has a choice of three different methods for calculating the CRC (see *Figure 8*) over the code memory content in the project.

- An 8-bit check sum calculation over the 16-bit address space can be used for checking up to 64 Kbytes of memory code, the simplest method.
- A 16-bit check sum calculation over the 16-bit address space can be used for checking up to 64 Kbytes of the memory code; this method is more precise and is the default method.
- A 16-bit check sum calculation over all the possible address space can be used when the code memory exceeds 64 Kbytes, 24-bit addressing must be used; this way uses the most code space and is the most time consuming.

The STM8 firmware includes six separate source files defined for each of these methods. There is one pair for each method: one used for startup and one for run time. The user should include the correct source file pair into the project.

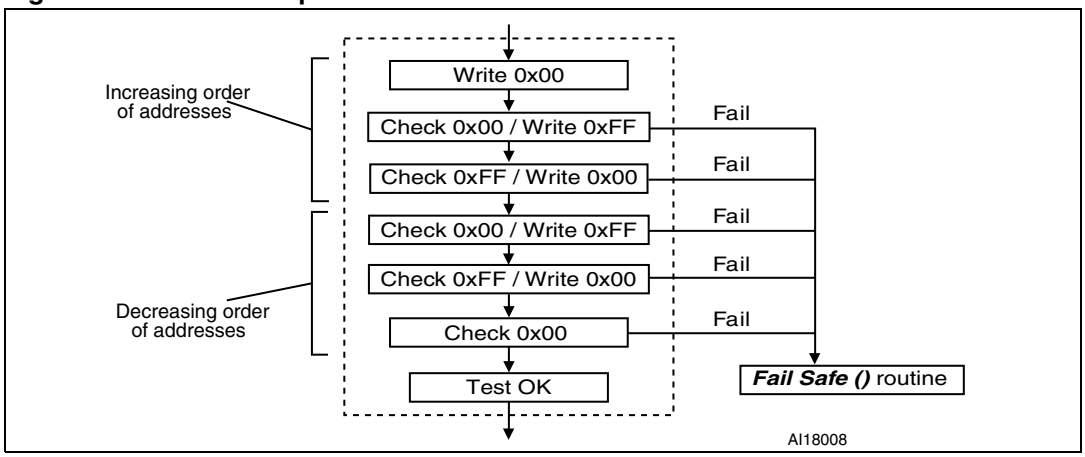
Figure 8. FLASH startup self test structure



4.2.4 Full RAM March C-/X self test

The whole RAM space is alternately filled and checked simultaneously by zero and 0xFF pattern in six loops, either by March C- or March X algorithms. March X algorithm is faster as the two middle steps are skipped over. The first three loops are performed in incremental order of addresses the last three in decremented order. In case of error, ***FailSafe()*** routine is called.

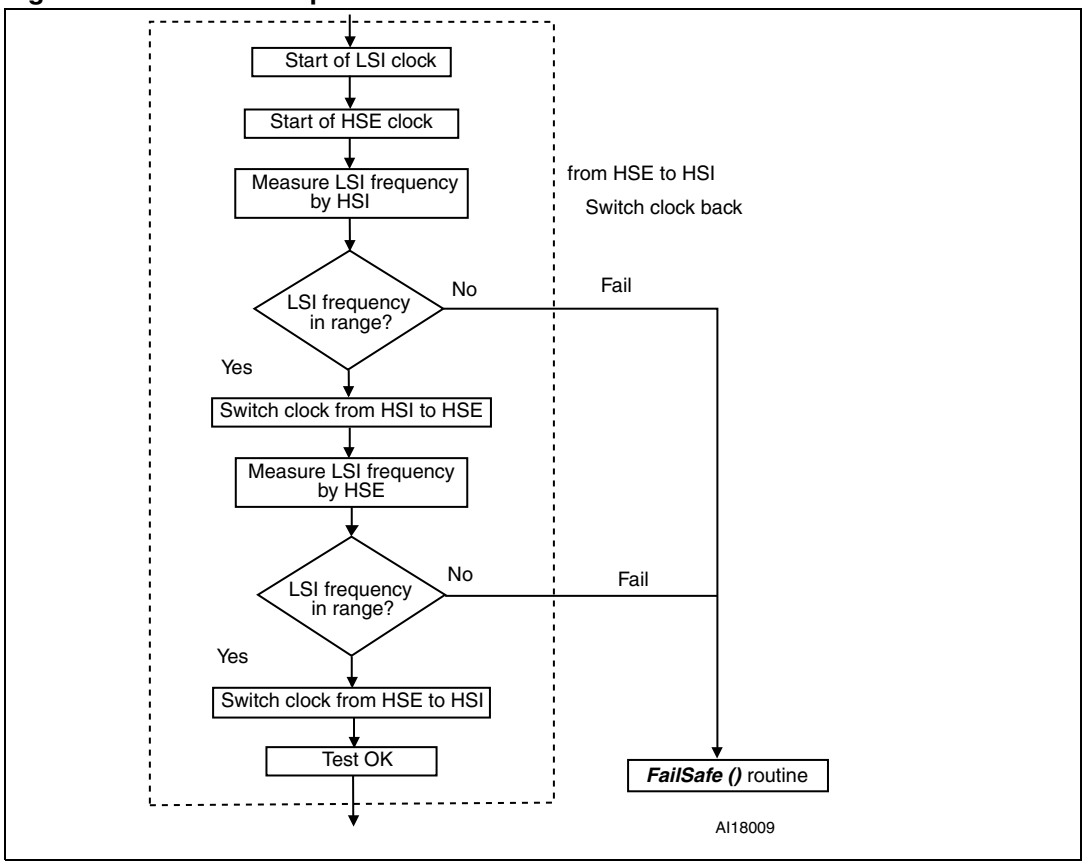
Figure 9. RAM startup self test structure



4.2.5 Clock startup self test

When the test begins, first the low speed internal clock (LSI) source is started, then the high speed external source (HSE). The CPU is running on the high speed internal source (HSI). HSI is switched onto a dedicated timer input, mainly TIM3, but TIM1 or TIM2 can also be used on some devices. The timer is gated by the LSI source. The number of gated ticks is compared and if it falls outside of the predefined interval (more than +/- 25% from nominal value) an HSI fail is signaled and ***FailSafe()*** routine is called. CPU clock continues with HSI, default source. If there is no error, the test continues with the next step and HSE is checked. HSE is switched on as the new CPU clock source and input into the dedicated timer. The same measurement and check of gated ticks are repeated but with HSE feeding the timer. If the measure falls out of the interval, CPU clock is immediately turned back to HSI and HSE fail is signaled with a ***FailSafe()*** routine being called. Otherwise, the test returns OK. CPU clock is switched back to default HSI source after the test is finished. All the parts of this test are under conditional compilation control, so the user can skip over some test e.g. HSE test when no external oscillator is used.

Figure 10. Clock startup self test subroutine structure



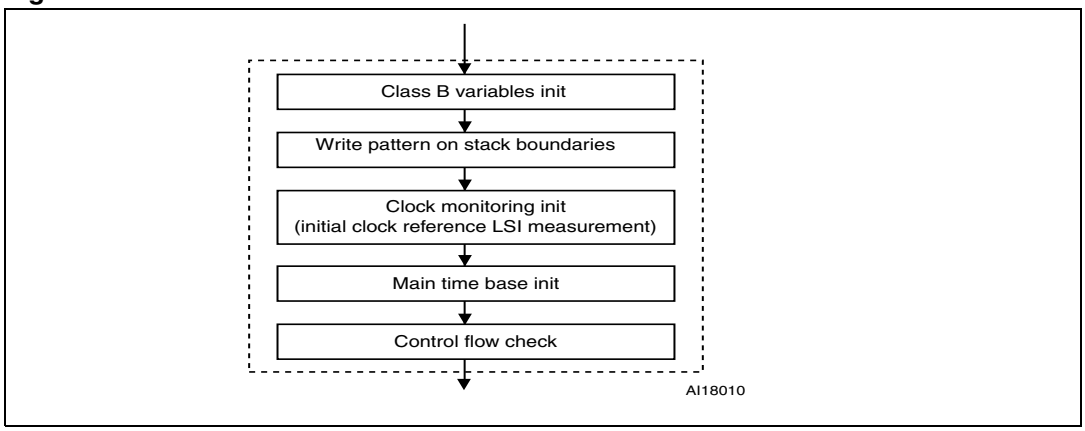
1. Low speed external (LSE) clock source can be started/checked at the beginning of the test and measured feeding the dedicated timer on STM8L15x devices. They can be inserted into the beginning of this routine.
2. High speed external (HSE) tests are skipped on STM8L10x devices.
3. LSI frequency is different for STM8S and STM8L devices. That is why the four consequent LSI periods are gated at STM8S devices (LSI=128 kHz) and only one period is used for measure on STM8L devices (LSI=38 kHz).

4.3 Periodic run mode self tests initialization

Run time self tests must be initialized just before the program enters the main loop performing the run mode self tests (refer to *Figure 4*). This must come just after start-up self tests have been executed and standard initialization done. The timing should be set to ensure that run mode tests are called properly and at regular intervals.

All class B variables must first be initialized. Zero and its complement value are stored in every class B variable complementary pair. The magic pattern is than stored at the top of stack space. Timer peripherals are configured for the tick interval measurement and master clock frequency measurement. Master frequency is gated by the LSI clock. The same method as for startup test is used. The resulting number of pulses is stored into the class B variable pair as an initial reference sample of master frequency measure.

Figure 11. Periodic run mode self test initialization structure



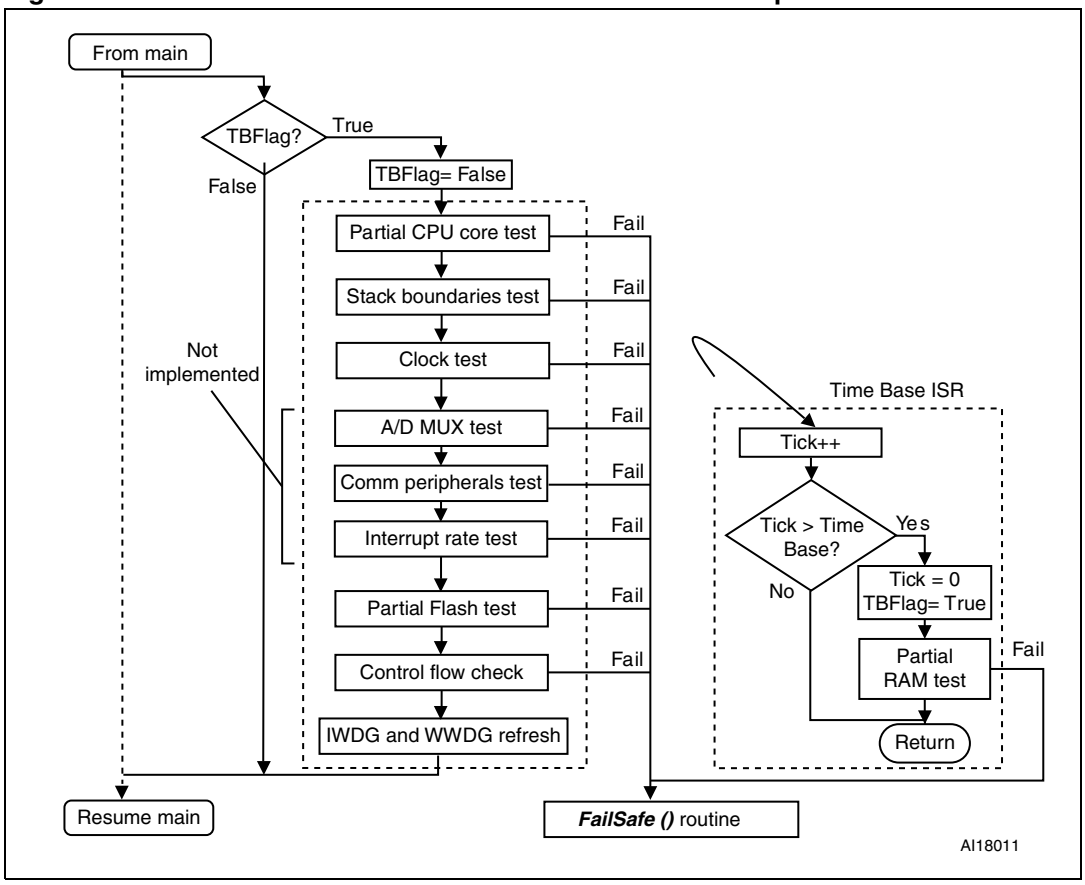
4.4 Detailed description of periodic run mode self tests

4.4.1 Run time self tests structure

Run time self tests are performed periodically, their period is based on time base interrupt settings. Before the first run, all tests must be initialized by run mode initialization routine (refer to *Figure 4*). All tests are performed in the main loop level except partial transparent RAM test, which is executed during the time base interrupt service. Some tests (analog, communication peripherals and application interrupts) are not automatically included. Depending on device capability and application needs, the user could implement them. The following is the list of the run mode self tests:

- CPU core partial run mode test
- Stack boundaries overflow test
- Clock run mode test
- AD MUX self test (not implemented)
- Interrupt rate test (not implemented)
- communication peripherals test (not implemented)
- Flash partial CRC test including evaluation of the complete test
- IWDG and WWDG refresh
- Partial transparent RAM March C-/X test (under system interrupt scope)

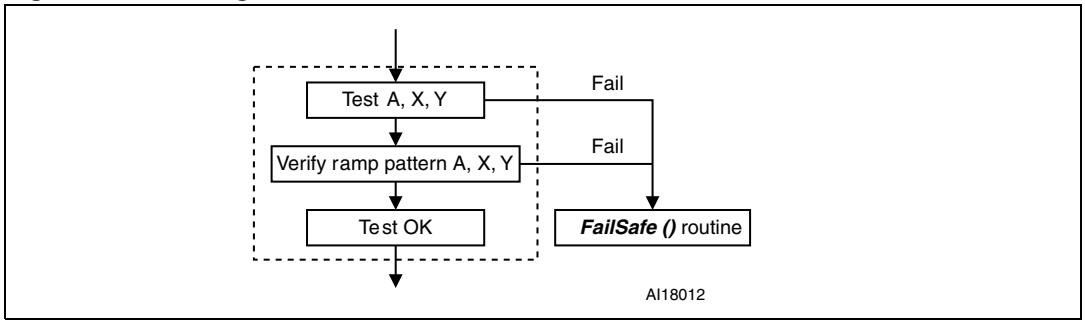
Figure 12. Periodic run mode self test and time base interrupt service structure



4.4.2 CPU light run mode self test

CPU core run mode self test is a simplified startup test where the flags and stack pointer are not tested. In case of error, ***FailSafe()*** routine is called.

Figure 13. CPU light run mode self test structure

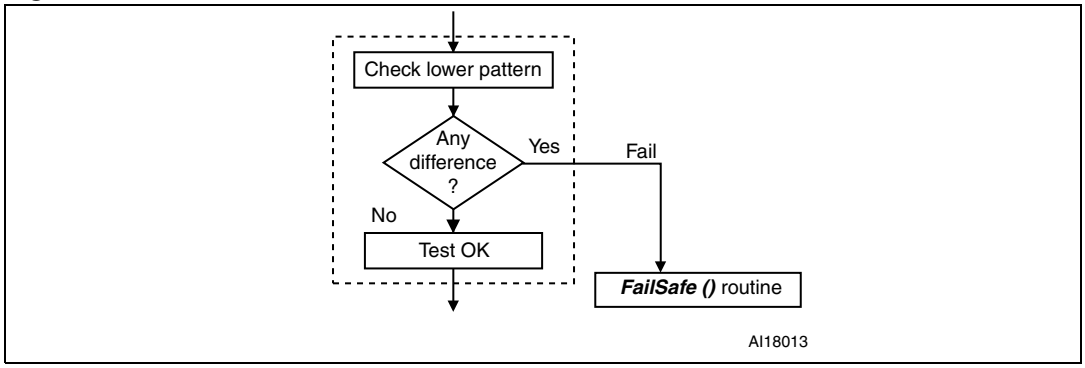


4.4.3 Stack boundaries run mode test

The magic pattern stored at the top of the stack is checked here. In case the original pattern is corrupted, ***FailSafe()*** routine is called. The pattern is placed at the lowest address dedicated for stack area.Overflow and underflow are detected as the stack pointer rolls over

inside this range in both cases. This area differs among the devices. The user must respect the dedicated stack area when the pattern location is changed.

Figure 14. Stack overflow run mode test structure



4.4.4 Clock run mode self test

The current master clock frequency selected by user application is gated by LSI internal clock source. The resulting number of pulses is compared with the initial master frequency reference sample measure which was stored during initial run mode self tests. When there is more than +/-25% difference found, ***FailSafe()*** routine is called. Occasional over captured measure is ignored. It can appear when a longer user interrupt service corrupts current measurement.

Figure 15. Clock run mode self test structure

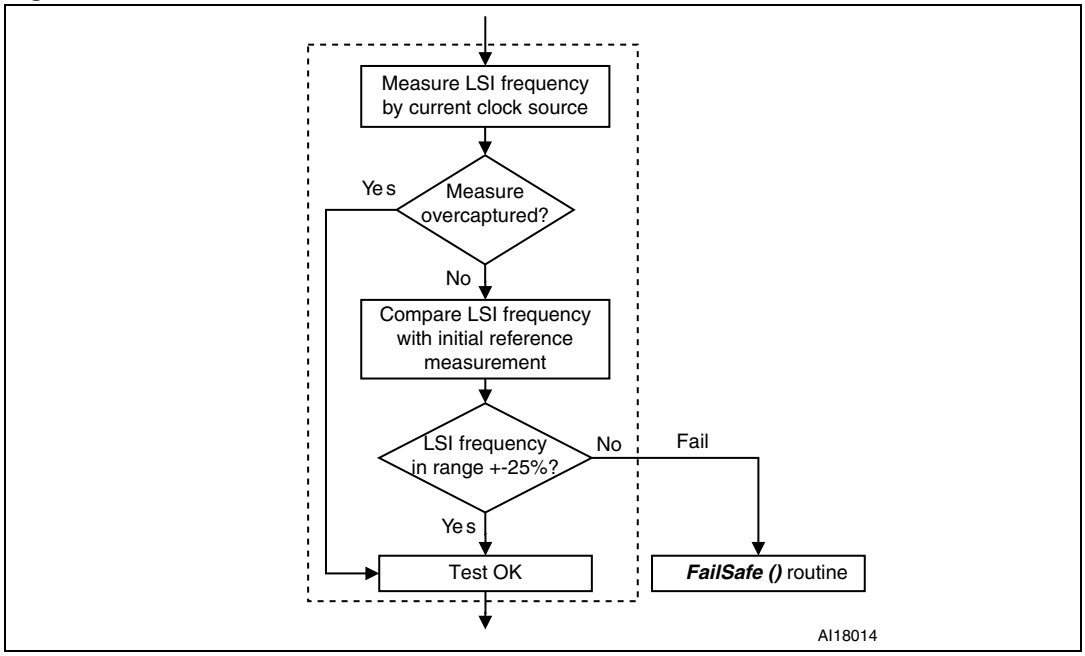
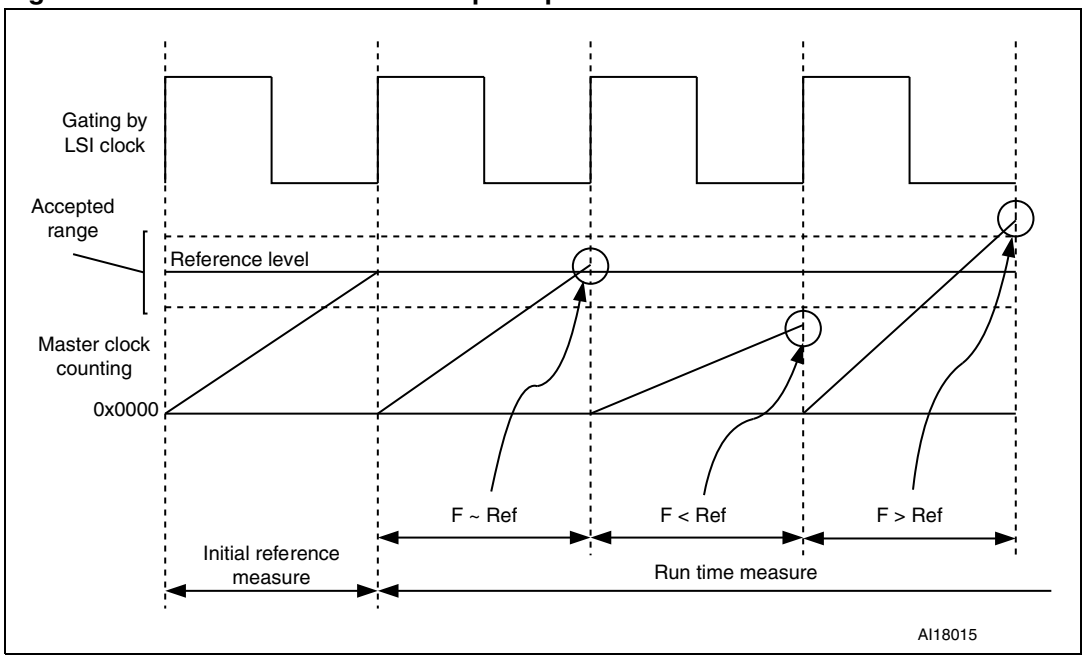


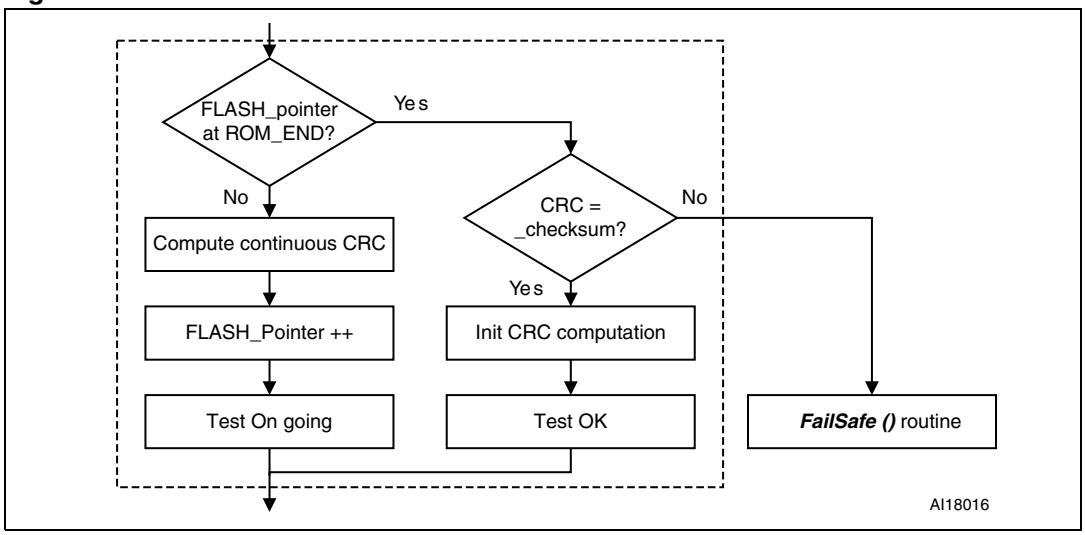
Figure 16. Clock run mode self test principle



4.4.5 Partial FLASH CRC run mode self test

Partial 16-bit CRC checksum over the Flash memory block is performed in every step. The boundaries are given in the segment table created by the linker. When the last block is reached the CRC checksum is compared with the value stored by linker at the last record in the segment table. In case of a difference, ***FailSafe()*** routine is called, otherwise a new computation cycle is initialized.

Figure 17. Partial FLASH CRC run mode self test structure



1. *For more details about CRC calculation, please refer to Section 4.2.3: Flash complete checksum self test.*

4.4.6 Watchdog service in run mode test

If the run mode service block is correctly completed, then both window and independent watchdogs (WDGs) are refreshed at the last step just before returning to the main loop. To correctly refresh watchdogs, the user must ensure calling ***STL_DoRunTimeChecks()*** routine (see *Figure 12*) at corresponding intervals in order to be able to properly react to the time base flag change.

Only one WDG refresh inside the main loop is necessary and contributes to overall efficiency. There should be no other WDG refresh except the one in ***STL_DoRunTimeChecks()*** routine. Sometimes it is necessary to refresh WDGs at initialization phase, too. In this instance, the refresh should be outside of any software infinite loop.

4.4.7 Partial RAM run mode self test

Partial transparent RAM test is performed inside the time base interrupt service. The test covers the part of the RAM containing the class B variables. One block of six bytes is tested at every test step. To guarantee coupling fault coverage, consecutive test steps are performed on memory blocks with an overlapping of two adjacent bytes. During the first phase, the block content is stored in the storage buffer. The next phase is to perform the marching destructive tests on all the bytes in the tested RAM block. Then, the final step is to restore the original content. March X algorithm is faster as two middle marching steps are skipped over (see *Table 4*). The last test sequence step is to perform a marching test on the storage buffer itself, again with the next two additional bytes to cover coupling faults. Then the whole test is re-initialized and it begins again. In case any fault is detected, ***FailSafe()*** routine is called.

Figure 18. Partial RAM run mode self test structure)

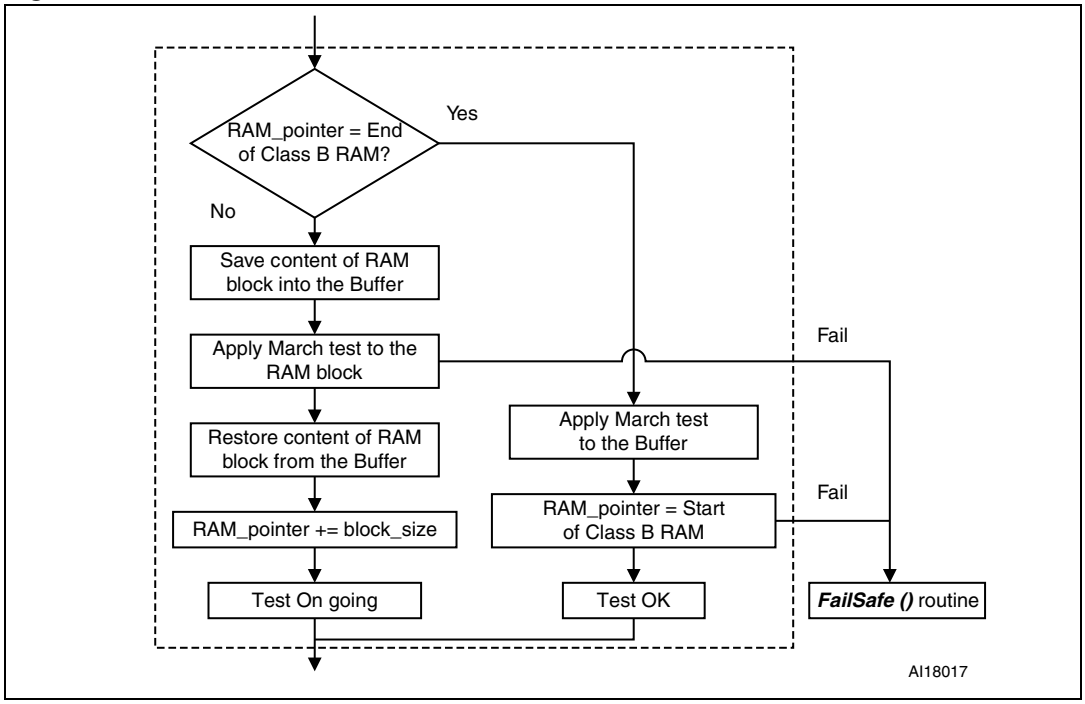


Figure 19. Fault coupling principle used at partial RAM run mode self test

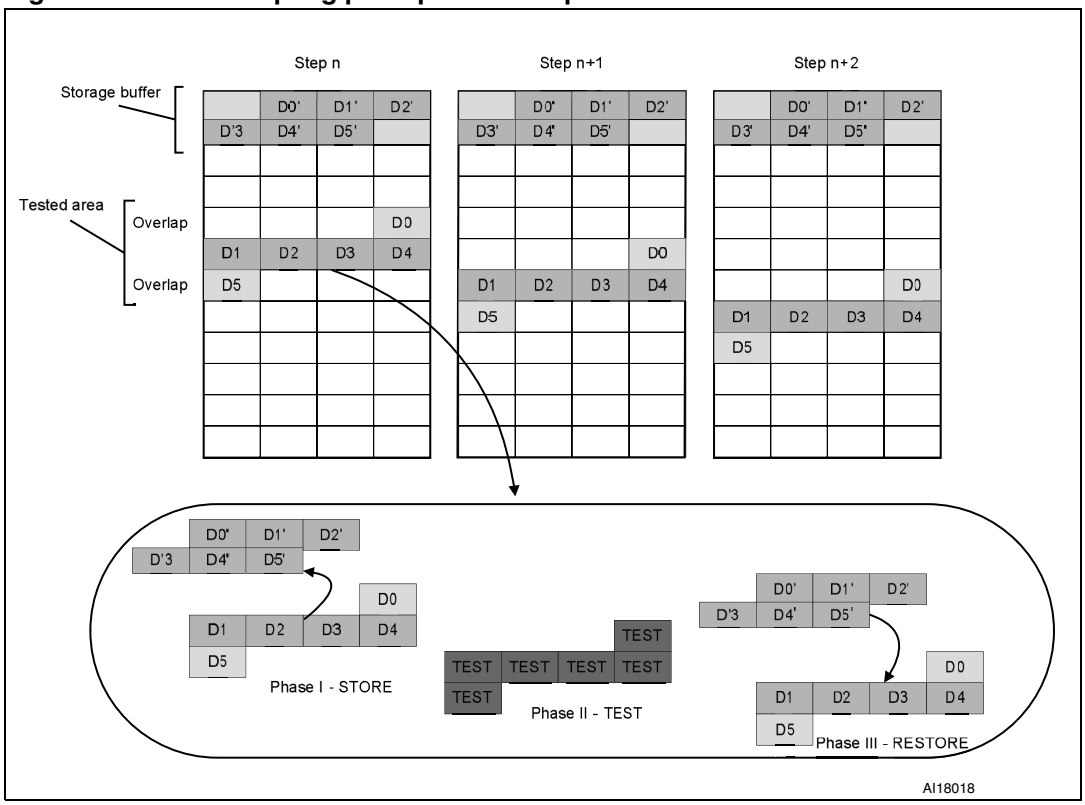


Table 4. March C- phases at RAM partial test

March phase	Partial bytes test over the block	Address order
Initial	Write 0x00 pattern	Increasing
1	Test 0x00 pattern, write 0xFF pattern	Increasing
2(1)	Test 0xFF pattern, write 0x00 pattern	Increasing
3(1)	Test 0x00 pattern, write 0xFF pattern	Decreasing
4	Test 0xFF pattern, write 0x00 pattern	Decreasing
5	Test 0x00 pattern	Decreasing

1. Steps 2 and 3 are skipped over when March X algorithm is used.

Appendix A STM8 Class B firmware package variations

Table 5. STM8 Class B firmware packages

	STM8S/A package	Medium density STM8L/AL package	Low density STM8L/AL/TL package
Optional UART verbose mode	YES	YES	NO(1)
Demo mode with optional LCD screen	YES	YES	NO
Window watchdog test	YES	YES	NO(2)
High speed external (HSE) clock test	YES	YES	NO
Low speed external (LSE) clock test	NO	YES	NO
Low speed internal (LSI) frequency / number of LSI periods used at clock tests (measurement)	128 kHz / 4	38 kHz / 1	38 kHz / 1
Stack space at the top of RAM [bytes]	1024 / 512(3)	513	513(4)

1. Errors are manifested by error codes passed to *FailSafe()* routine.
2. Window watchdog is available at STM8TL5x devices only.
3. The stack is limited for some STM8S Access line devices and STM8A devices with up to 32 Kbytes non-volatile memory; for proper values, see the corresponding datasheets.
4. Stack is not limited for STM8TL5x devices; there is rollover (due to over/underflow) only if the stack overlaps the 4 Kbytes.

Revision history

Table 6. Revision history

Date	Revision	Description of changes
01-Jun-2010	1	Initial release
29-Nov-2012	2	Modified *Introduction* and document throughout to include all new members of the STM8 family. Added *Section 1: Package variation overview* and *Table 1: Applicable products*. Modified *Table 3: Overview of methods used in micro-specific tests provided with this application note* and *Appendix A: STM8 Class B firmware package variations*.

Please Read Carefully:

Information in this document is provided solely in connection with ST products. STMicroelectronics NV and its subsidiaries (“ST”) reserve the right to make changes, corrections, modifications or improvements, to this document, and the products and services described herein at any time, without notice.

All ST products are sold pursuant to ST’s terms and conditions of sale.

Purchasers are solely responsible for the choice, selection and use of the ST products and services described herein, and ST assumes no liability whatsoever relating to the choice, selection or use of the ST products and services described herein.

No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted under this document. If any part of this document refers to any third party products or services it shall not be deemed a license grant by ST for the use of such third party products or services, or any intellectual property contained therein or considered as a warranty covering the use in any manner whatsoever of such third party products or services or any intellectual property contained therein.

UNLESS OTHERWISE SET FORTH IN ST’S TERMS AND CONDITIONS OF SALE ST DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY WITH RESPECT TO THE USE AND/OR SALE OF ST PRODUCTS INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE (AND THEIR EQUIVALENTS UNDER THE LAWS OF ANY JURISDICTION), OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

UNLESS EXPRESSLY APPROVED IN WRITING BY TWO AUTHORIZED ST REPRESENTATIVES, ST PRODUCTS ARE NOT RECOMMENDED, AUTHORIZED OR WARRANTED FOR USE IN MILITARY, AIR CRAFT, SPACE, LIFE SAVING, OR LIFE SUSTAINING APPLICATIONS, NOR IN PRODUCTS OR SYSTEMS WHERE FAILURE OR MALFUNCTION MAY RESULT IN PERSONAL INJURY, DEATH, OR SEVERE PROPERTY OR ENVIRONMENTAL DAMAGE. ST PRODUCTS WHICH ARE NOT SPECIFIED AS "AUTOMOTIVE GRADE" MAY ONLY BE USED IN AUTOMOTIVE APPLICATIONS AT USER’S OWN RISK.

Resale of ST products with provisions different from the statements and/or technical features set forth in this document shall immediately void any warranty granted by ST for the ST product or service described herein and shall not create or extend in any manner whatsoever, any liability of ST.

ST and the ST logo are trademarks or registered trademarks of ST in various countries.

Information in this document supersedes and replaces all information previously supplied.

The ST logo is a registered trademark of STMicroelectronics. All other names are the property of their respective owners.

STMicroelectronics group of companies

Australia - Belgium - Brazil - Canada - China - Czech Republic - Finland - France - Germany - Hong Kong - India - Israel - Italy - Japan - Malaysia - Malta - Morocco - Philippines - Singapore - Spain - Sweden - Switzerland - United Kingdom - United States of America

www.st.com