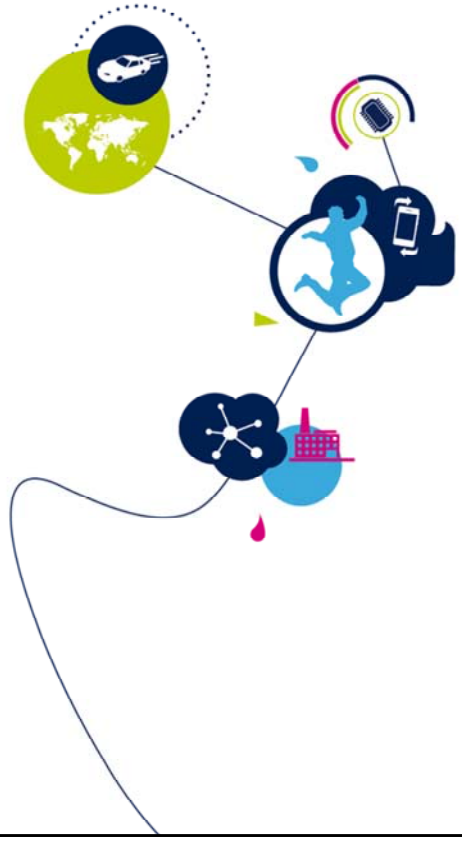
STM32L5 - BOOT

Boot configuration

Revision 1.0



life.augmented

Hello, and welcome to this presentation describing the various Boot configurations of the STM32L5.

Overview

- STM32L5 boot configuration when TrustZone® is disabled
  - Booting from user selected address (internal flash or SRAM)
  - Booting from system bootloader
- STM32L5 boot configuration when TrustZone® is enabled
  - Booting from user selected secure address (internal flash or SRAM)
  - Booting from Root Security service (RSS)

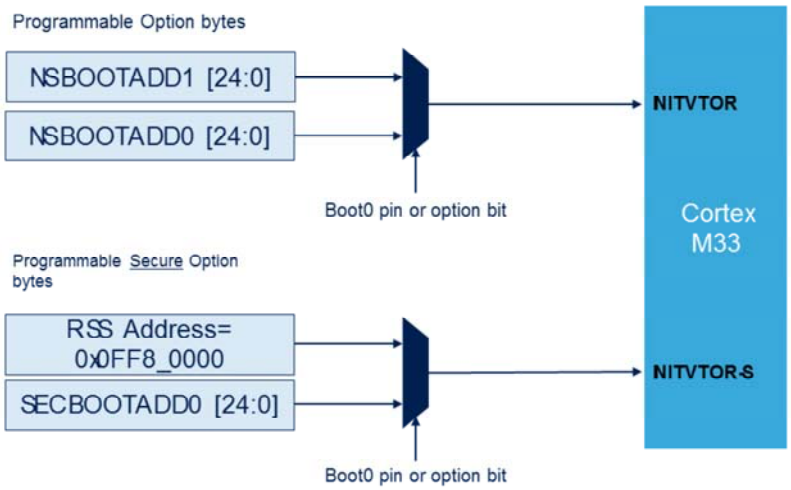
Application benefits

- Selection of the boot address
- Enforcing a unique boot entry by using the BOOT_LOCK feature
- Relying on the system bootloader to download the user image from a serial interface
- Taking benefit of the RSS to perform a secure image download

life.augmented

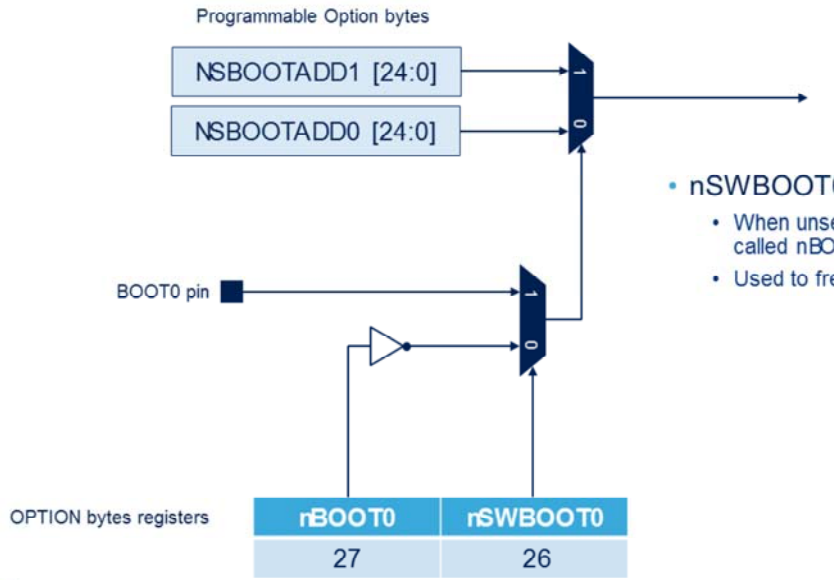
The STM32L5 offers multiple boot options according to Trustzone activation.
When TrustZone is disabled (TZEN=0), the Cortex-M33 core can boot from either the user image present in internal memory or the system bootloader, which downloads the user image from a serial interface.
When TrustZone is enabled (TZEN=1), the Cortex-M33 core can boot from either the user image present in secure internal memory or the RSS.
RSS is the secure part of the secure bootloader, in charge of user image decryption amongst other things.

System Boot overview



Unlike the Cortex-M4, which always boot at address 0, the Cortex-M33 samples inputs that determine the boot address.
When TrustZone is disabled, INITVTOR inputs are used, which receives an address programmed in option bytes.
The state of the BOOT0 pin selects either Non Secure boot address 0 or Non Secure boot address 1.
When TrustZone is enabled, INITVTOR_S inputs are used, which receives an address programmed in option bytes or a fixed address when RSS is selected.
The state of the BOOT0 pin or option bit nBOOT0 selects which of the two addresses will be used.

nBOOT0 option bit vs. BOOT0 pin

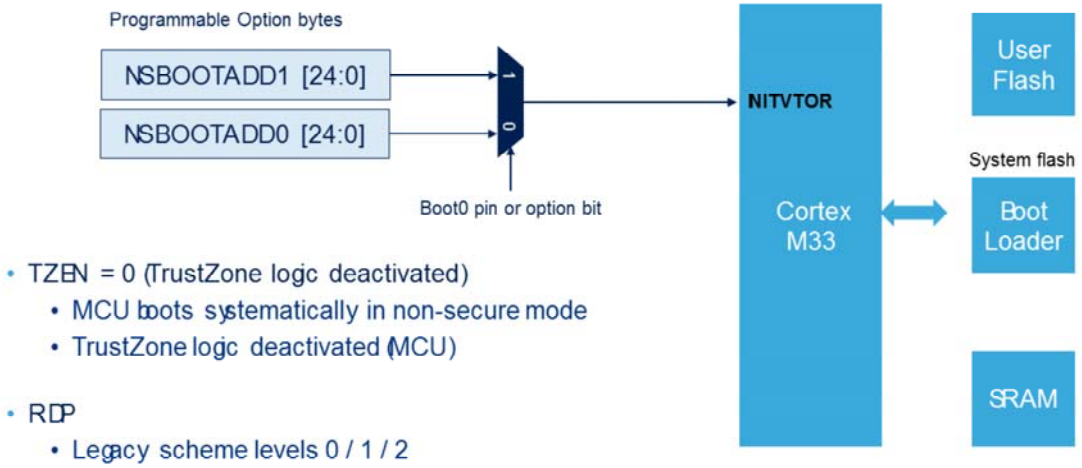


- nSWBOOT0 option bit
  - When unset (=0) the BOOT0 pin is replaced by an option bit called nBOOT0
  - Used to free the boot pin in order to reuse it for other purpose

life.augmented

The state of the BOOT0 pin selects which boot address is used on the condition that the nSWBOOT0 option bit is equal to one.
When the nSWBOOT0 option bit is equal to zero, the state of the BOOT0 pin is ignored and replaced with the state of another option bit called nBOOT0.
In this case, the Port H3 pin, which supports the BOOT0 functionality, becomes a general purpose IO.

Boot configuration when TZEN=0



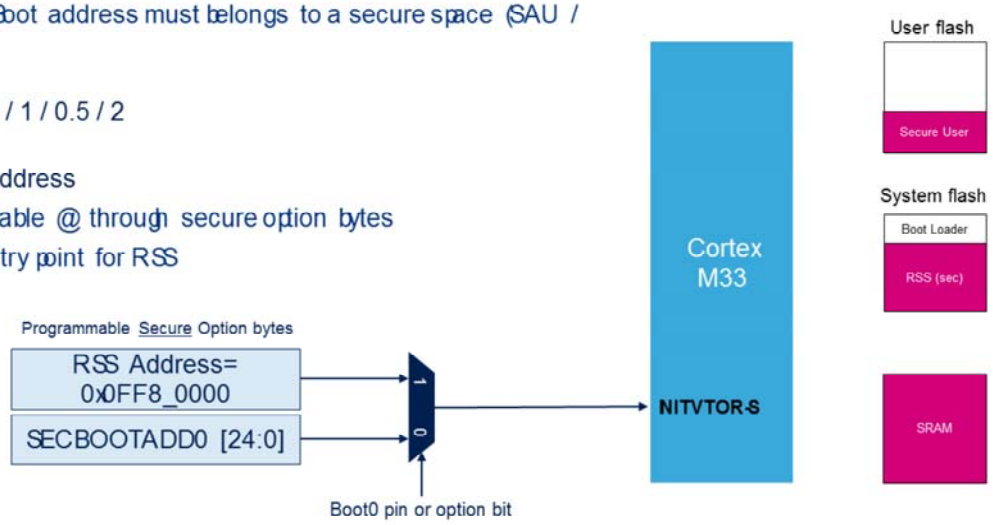
- TZEN = 0 (TrustZone logic deactivated)
  - MCU boots systematically in non-secure mode
  - TrustZone logic deactivated (MCU)
- RDP
  - Legacy scheme levels 0 / 1 / 2
- Boot address
  - Programmable address through non secure option bytes
  - Unique entry point for system flash (Boot Loader)

life.augmented

This slide details the boot configuration when TrustZone is disabled.
The microcontroller boots in non-secure mode.
The Readout protection can be set to levels 0, 1 or 2.
The boot address is programmable through non-secure option bytes. The boot program can be mapped anywhere in the internal memories, flash or SRAM.
The boot loader has a unique entry point in system flash, which is the default value of NSBOOTADD1.

Boot configuration when TZEN=1

- TZEN = 1 (TrustZone logic activated)
  - TrustZone logic activated
  - MCU boots systematically in secure mode
  - Selected Boot address must belongs to a secure space (SAU / IDAU)
- RDP levels: 0 / 1 / 0.5 / 2
- Secure Boot address
  - Programmable @ through secure option bytes
  - Unique entry point for RSS

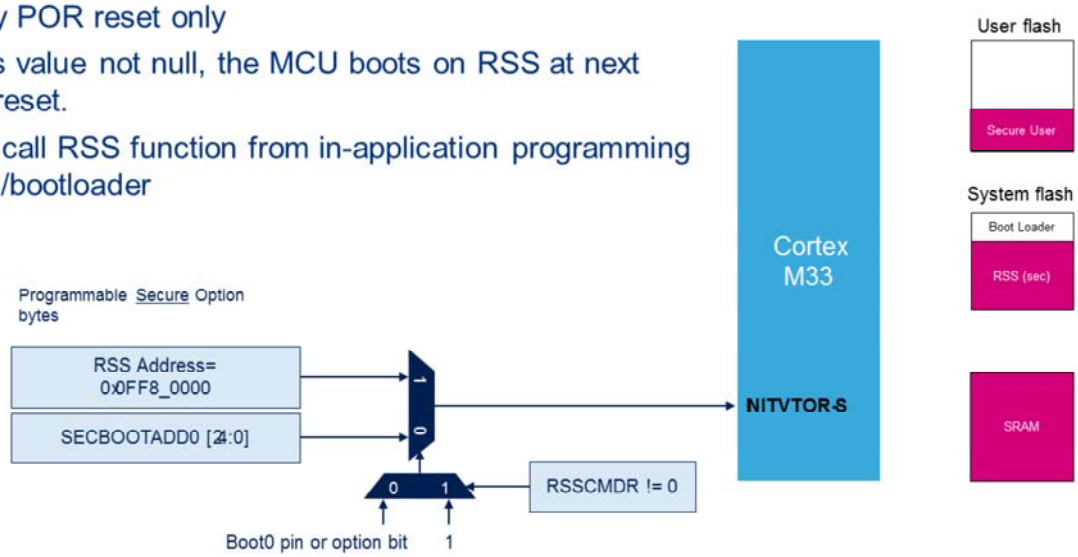


life.augmented

This slide details the boot configuration when TrustZone is enabled.
The microcontroller boots in secure mode and the boot space must be located in secure area.
The Readout protection can be set to levels 0, 0.5, 1 or 2.
The boot address is programmable through secure option bytes. The boot program can be mapped anywhere in the internal secure memories, flash or SRAM.
The RSS has a unique entry point in system flash.

RSSCMDR register

- RSSCMDR is secure register defined in SYSCONF registers
  - Reset by POR reset only
  - When its value not null, the MCU boots on RSS at next system reset.
  - Used to call RSS function from in-application programming or JTAG/bootloader

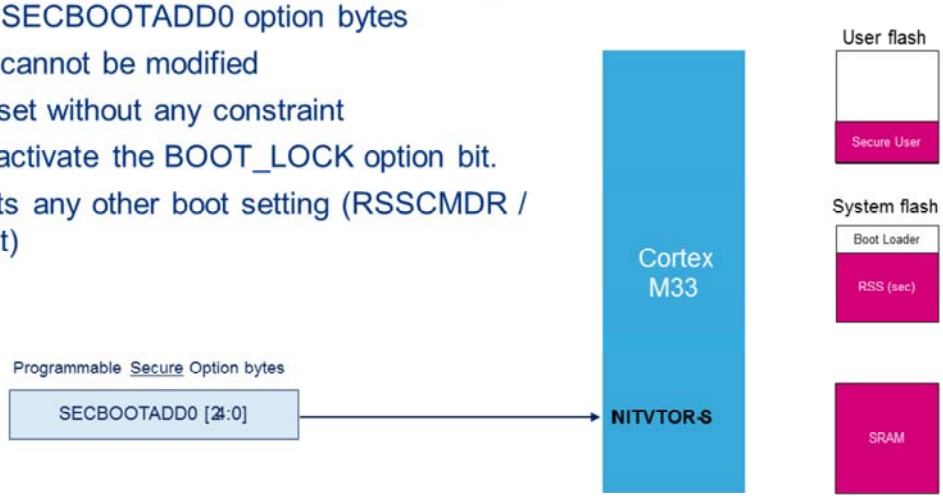


RSSCMDR is a register defined in the SYSCONF module.
It is used to pass a command to be executed by the RSS.
When the value in this register is non null, the MCU will boot on RSS at the next system reset, knowing that this register is only reset by a Power-On Reset.
Therefore the RSSCMDR register enables a bootloader to call RSS after applying a warm reset to the microcontroller.
This can be done by an in-application programming bootloader or a JTAG/Serial Wire bootloader.

BOOT_LOCK

8

- BOOT_LOCK (option bit) is used to guaranty a UNIQUE BOOT ENTRY
  (Secure Boot) on the FLASH
  - When BOOT_LOCK is set, the system boots systematically on the address set in the SECBOOTADD0 option bytes
  - The SECBOOTADD0 cannot be modified
  - BOOT_LOCK can be set without any constraint
  - It is not possible to deactivate the BOOT_LOCK option bit.
  - BOOT_LOCK preempts any other boot setting (RSSCMDR / BOOT0 pin / Option bit)



BOOT_LOCK is an option bit that guarantees a unique boot entry when it is set.
When BOOT_LOCK is set, system boots systematically on address set in Secure Boot Address 0 option bytes.
This address cannot be modified.
BOOT_LOCK can be set without any constraint.
It is not possible to deactivate the BOOT_LOCK option bit.
BOOT_LOCK has the precedence over other boot configuration selection features: RSSCMDR, BOOT0 pin and nBOOT0 option bit.

Boot summary (TZEN=0)

	nBOOT0 FLASH_OPTR[27]	BOOT0 Pin PH3	nSWBOOT0 FLASH_OPTR[26]	BOOT address Option Byte selection	Boot area	ST programmed default value
Pin PH3 = BOOT0	-	0	**1**	NSBOOTADD0	Boot address defined by user option bytes NSBOOTADD0	Flash 0x0800 0000
	-	1	**1**	NSBOOTADD1	Boot address defined by user option bytes NSBOOTADD1	System bootloader 0x0BF9 0000
Pin PH3 = GPIO	1	-	**0**	SECBOOTADD0	Boot address defined by user option bytes NSBOOTADD0	Flash 0x0800 0000
	0	-	**0**	NSBOOTADD1	Boot address defined by user option bytes NSBOOTADD1	System bootloader 0x0BF9 0000

life.augmented

This table summarizes the boot options when TrustZone is disabled.
When the nSWBOOT0 option bit is equal to one, the boot address depends on the state of the BOOT0 pin: either NSBOOTADD0 pointing to the user image entry point in an internal memory or NSBOOTADD1, which is by default the entry point of the system bootloader.
When the nSWBOOT0 option bit is equal to zero, the option bit nBOOT0 replaces the BOOT0 pin state.

Boot summary (TZEN=1)

BOOT_LOCK	RSSCMDR	nBOOT0 FLASH_OPTR[27]	BOOT0 Pin PH3	nSWBOOT0 FLASH_OPTR[26]	BOOT address Option Byte selection	Boot area	ST programmed default value
0	0	-	0	1	SECBOOTADD0	Secure boot address defined by user option bytes SECBOOTADD0	Flash 0x0C00_0000
	0	-	1	1	n/a	RSS : 0x0FF8_0000	RSS 0x0FF8_0000
	0	1	-	0	SECBOOTADD0	Secure boot address defined by user option bytes SECBOOTADD0	Flash 0x0C00_0000
	0	0	-	0	n/a	RSS : 0x0FF8_0000	RSS 0x0FF8_0000
	≠ 0	-	-	-	n/a	RSS : 0x0FF8_0000	RSS 0x0FF8_0000
1	-	-	-	-	SECBOOTADD0	Secure boot address defined by user option bytes SECBOOTADD0	Flash 0x0C00_0000

life.augmented

This table summarizes the boot options when TrustZone is enabled.
The center of the table is similar to the table on the previous slide, except that NSBOOTADD0 is replaced with SECBOOTADD0 and NSBOOTADD1 is replaced with the fixed address of the RSS.
The two additional columns BOOT_LOCK and RSSCMDR are specific to secure boot.
When BOOT_LOCK is set to one, the boot address is unique and defined in SECBOOTADD0, whatever the other parameters.
When RSSCMDR is non null and BOOT_LOCK is set to zero, boot in RSS is performed.

Related peripherals

11

- Refer to these peripheral trainings linked to this peripheral
  - Memory protection (MEMPROTECT)
  - System Configuration (SYSCONF)

life.augmented

The Boot configuration module has relationships with the following other module:

- Memory protection
- System configuration.