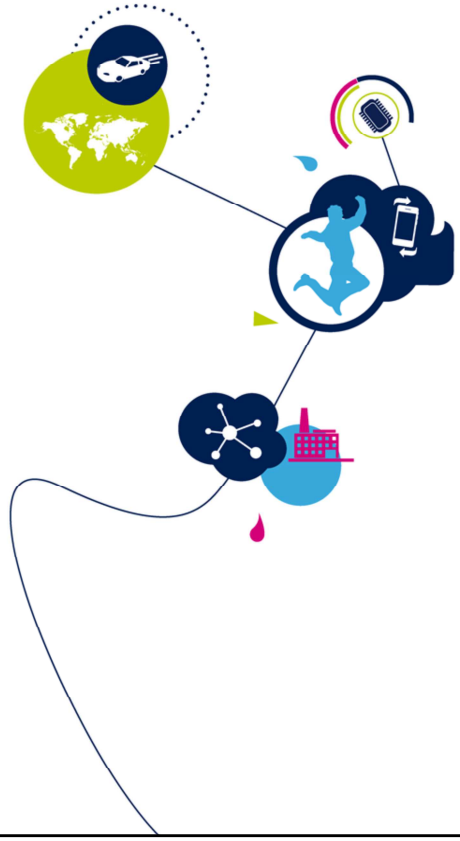
STM32L5 – SYSCFG

System Configuration Controller

Revision 1.0



life.augmented

Hello, and welcome to this presentation of the STM32L5 System Configuration Controller.

Overview

- STM32L5xx microcontrollers feature a set of configuration registers
- The main purposes of the system configuration controller are the following:
  - Managing the robustness feature
  - Setting SRAM2 write protection and software erase
  - Configuring FPU interrupts
  - Enabling/disabling the I2C fast-mode plus driving capability on some I/Os and voltage booster for I/O analog switches
  - Configuring TrustZone® security register access

life.augmented

STM32L5 microcontrollers feature a set of configuration registers located in the SYSCFG module.
The System Configuration Controller gives access to the following features:

- Managing the robustness feature
- Setting SRAM2 write protection and software erase
- Configuring FPU interrupts
- Enabling/disabling I2C Fast-mode Plus driving capability on some I/Os and voltage booster for I/O analog switches
- Configuring TrustZone security register access.

The 64 Kbytes of SRAM2 is particularly suitable for performance, integrity and safety, and low power.
Code execution maximum performance when accessed through the C-bus.
The SRAM2 supports parity check. The Data bus width is 36 bits because 4 bits are available for parity check, 1 bit per byte is used to increase memory robustness, as required, for instance, by Class B or SIL standards. Class B and SIL are safety standards: Class B is for Home Appliances and SIL for the Safety Integrity Level.
The parity bits are computed and stored when writing into the SRAM. Then, they are automatically checked when reading. If one bit fails, an NMI is generated. The same error can also be linked to the Break input of the timers. Note that the SRAM2 parity check is disabled by default.
Either 64 Kbytes or upper 4 Kbytes of SRAM2 content can optionally be retained in Standby.

The SRAM2 is also suitable for secure applications.
The SRAM2 can be write-protected with a 1-Kbyte granularity.
The SRAM2 can also be readout-protected via the RDP option byte. When protected, the SRAM2 cannot be read or written by the JTAG or serial wire debug port, and when the boot in System flash or boot in SRAM is selected. The SRAM2 is erased when the readout protection is changed from Level 1 to Level 0. Please refer to the System Memory Protections training for further details.
The SRAM2 can be erased by software by setting the SRAM2ER bit in the SRAM2 System Configuration Control and Status register. The SRAM2 can also be erased with the system reset depending on the option bit SRAM2_RST in the user option bytes.

The System Configuration Register 2 contains the control and status bits linked to safety and robustness such as the SRAM2 parity error flag, and the control bits to direct some error detection events to the timers' break inputs. This allows timer outputs to be placed in a known state during an application crash. Once programmed, the connection is locked until the next system reset. These internal events include a Flash error-code-correction event, a power voltage detector event, SRAM2 parity error event, and the Cortex-M33 lockup state.

The System Configuration Controller manages the selection of the GPIO to the external interrupt or event signal, which is used as an asynchronous external interrupt or event with wakeup from Stop capability.
Configuration register 1 contains the floating point unit interrupt control bits. It also contains the I²C Fast-mode-Plus 20 mA drive enable control bits. Four I/Os can be configured with high drive mode even if they are not used as I2C alternate functions. They can be used to drive LEDs for instance.
The I/O analog switch voltage booster is also selected in this register.

SYSCFG and TrustZone

7

- The SYSCFG is a TrustZone® -aware peripheral
- When the TrustZone® security is activated, the SYSCFG is able to secure registers from being modified by non-secure accesses

life.augmented

The SYSCFG is a Trustzone-aware peripheral, meaning that secure and non-secure registers co-exist within the peripheral.
TrustZone-aware peripherals are non-secure after reset.
Their secure configuration registers are secure.

SYSCFG Secure Configuration register

- Enable/disable non-secure software to configure the resources controlled by the SYSCFG
  - By default, the resources can be configured by both secure and non-secure software

Resource	Registers that can be protected against non-secure software access
Floating Point Unit	SYSCFG_FPUIMR
SRAM2	SYSCFG_SKR, SYSCFG_SCR and SYSCFG_SWPRx
ClassB	SYSCFG_CFGR2
SYSCFG clock control security	SYSCFG configuration clock in the RCC registers

- When the registers are configured to be accessed by secure software only, non-secure access attempts returns zero on reads (RAZ) and writes are ignored (WI)
  - An illegal access event is generated, and an illegal access interrupt request is generated if the SYSCFG illegal access event is enabled in the GTZC

life.augmented

When TrustZone is active, the secure software is in charge of selecting the secure attributes of the following features:

- Floating point unit
- SRAM2
- ClassB
- SYSCFG clock control configuration registers located RCC.

Here is the list of ClassB features:

- SRAM2 parity error flag
- Definition of events that can lead to a timer break, supported by timers 1, 8, 15, 16, and 17.

When the registers are configured to be accessed by secure software only, non-secure access attempts return zero on reads (RAZ), writes are ignored (WI) and a SYSCFG illegal access is signaled to the Global TrustZone Controller GTZC.

SYSCFG CPU secure/non secure lock registers

- The secure software can lock:
  - The SAU registers
  - The Secure/Non-secure MPU registers
  - The Secure/Non-secure Vector Table Offset Registers(VTOR_S/VTOR_NS)
  - The Secure exception priority boosting
  - BusFault, HardFault, and NMI Non-secure enable

life.augmented

For security purposes, some readable / writeable registers can be dynamically programmed as read only, in order to avoid any subsequent modification of their value.
Both secure features and non-secure features can be locked against further changes.
The SYSCFG_CSLOCKR register enables secure software to lock the setting of the following features:

- System Attribution Unit, SAU
- Secure Memory Protection Unit, SMPU
- Secure vector table base address
- Secure exception priority boosting
- Configuration of bus fault, hard fault and NMI events to generate non-secure exceptions.

This register is only accessible by secure privileged software.
The SYSCFG_CNSLCKR register enables non-secure software as well as secure software to lock the setting of the following features:

- Non-secure Memory Protection Unit, NSMPU
- Non-secure vector table base address.

This register is accessible by both non-secure and secure privilege software.
Lock applies until the next system reset.

ROOT Security Service

- The Root Security Service (RSS) is available only when TrustZone is enabled
- SYSCFG_RSSCMDR[RSSCMD] is used to pass a command to be executed by the Root Security Service (RSS)

life.augmented

A customer application can request the execution of a secure service, by writing a command into the RSSCMD field of SYSCFG_RSSCMDR register.
Secure services are pre-encoded by ST into a portion of the flash memory called Root Security Service, also known as RSS.
When the system is secure (TZEN =1), this register can be read and written only when the APB access is secure.

References

- For more details, please refer to:
  - Reference manuals for STM32L5 microcontrollers
  - Peripherals trainings linked to this peripheral
    - TrustZone® (TRZ)
    - Global TrustZone® Controller (GTZC)
    - Arm Cortex®-M33 core (CM33)
    - Memory protection (MEMPROTECT)
    - Timers (TIM)
    - Inter-Integrated Circuit controllers (I2C)

life.augmented

For more details about the System Configuration module, refer to the reference manual for STM32L5 microcontrollers.
Refer also to these trainings for more information if needed:

- TrustZone,
- Global TrustZone Controller,
- Arm Cortex-M33 core,
- Memory protection,
- Timers,
- Inter-Integrated Circuit controllers.