STM32WL5 – SYSCFG

System Configuration Controller

Revision 1.0

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

Overview

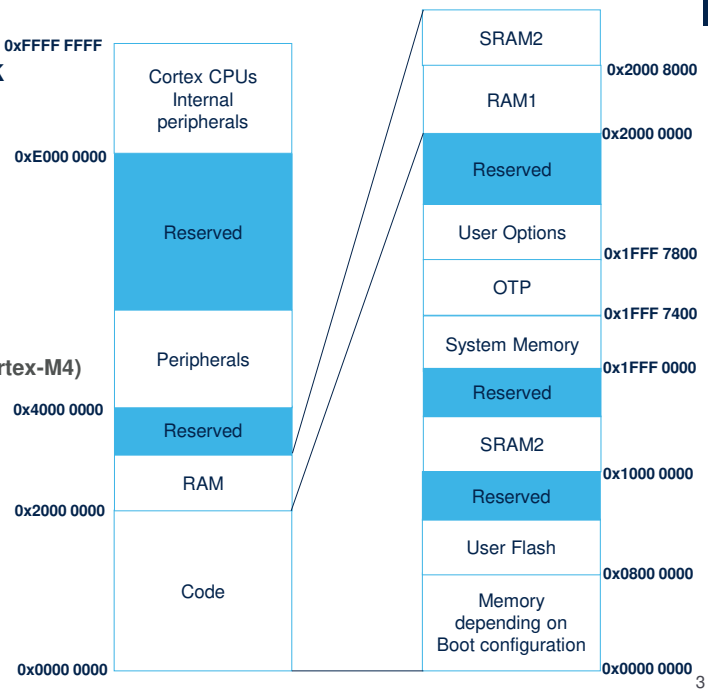
- All STM32WL5 devices feature a “System Configuration Controller”
  - Remap memory areas
  - Manage GPIO EXTI multiplexing
  - Manage “robustness” features
  - SRAM2 protection features
  - I2C Fast-mode Plus configuration
  - Independent CPU interrupt pre-masking

life.augmented

STM32WL5 devices feature a set of configuration registers. The System Configuration Controller gives access to the following features: Remapping memory areas to Cortex-M4 address 0, multiplexing GPIOs to the internal interconnect EXTI signals, certain robustness features, SRAM2 write-protection and erase, the configuration of the 20 mA high-drive I/Os used for I²C Fast-mode Plus, and peripheral interrupt pre-masking for the two CPUs.

Memory mapping

- **Flash memory: up to 256 Kbyte, single bank**
  - @0x0800 0000
- **SRAM: 64 Kbytes split in 2 parts:**
  - SRAM1:
    - 32 Kbyte @ 0x2000 0000
  - SRAM2 (backup):
    - 32 Kbytes @ 0x2000 8000
    - 32 Kbytes @ 0x1000 0000 **(Only accessible by Cortex-M4)**
- **Cortex-M4 bus relation**
  - Memories below address 0x2000 0000 are accessed by D-code and I-code bus
  - Memories from address 0x2000 0000 and above are accessed by S-bus



life.augmented

Pictured here is the 4-gigabyte linear address mapping of the STM32WL5 microcontroller.
The Flash memory is up to 256 Kbytes, in a single-bank configuration.
The SRAM total size is 64 Kbytes. It is split into 2 parts: SRAM1 is 32 Kbytes starting from address 0xx2000 0000 and SRAM2 backup RAM is 32 Kbytes starting from address 0x2000 8000 and also aliased at Cortex-M4 address 0x1000 0000. Both SRAM1 and SRAM2 are located in the usual ARM memory space for RAM on the S-bus. SRAM2 can also be accessed directly through Cortex-M4 Data code and Instruction code buses allowing zero wait states, used for code execution.

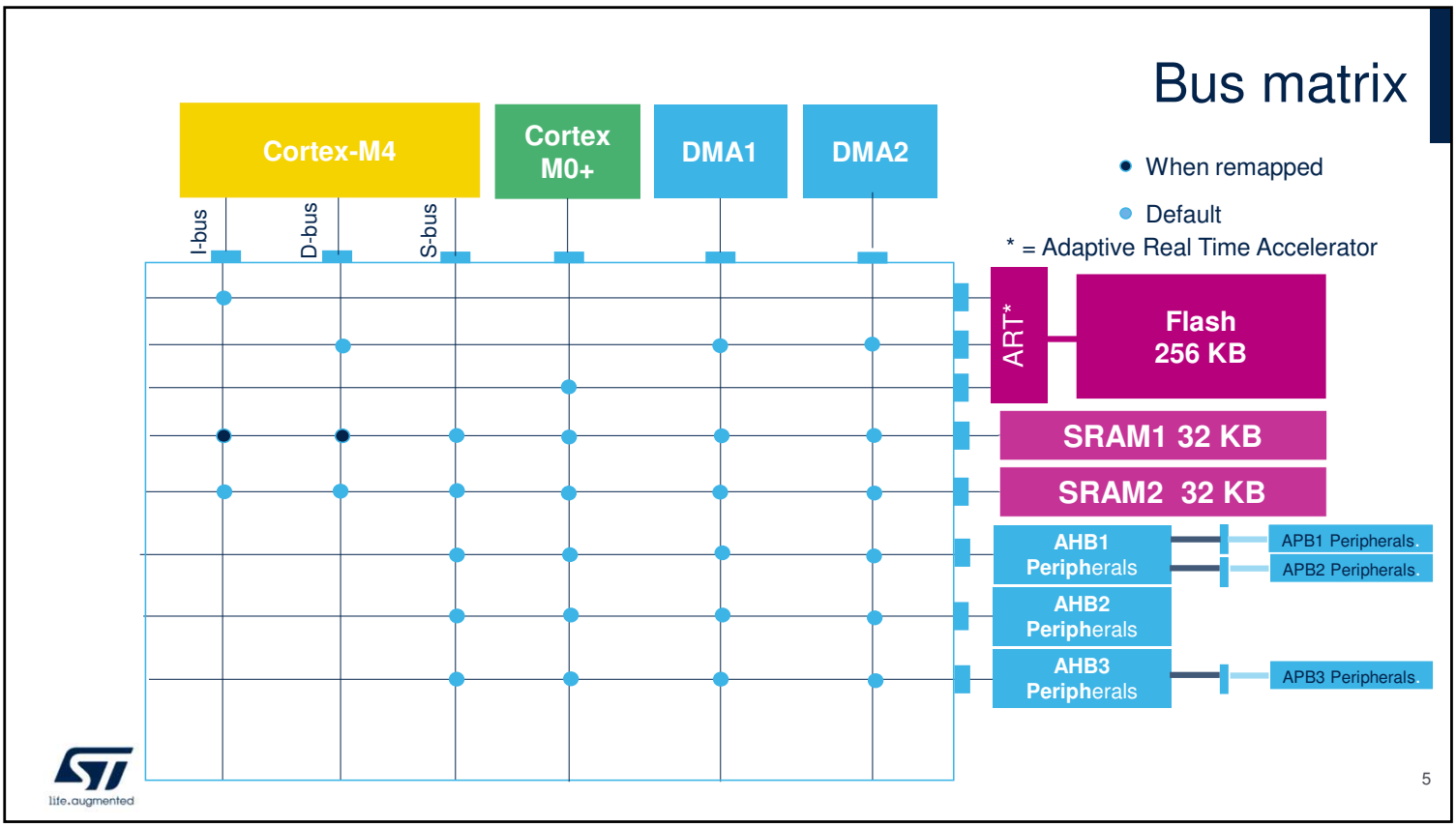
Memory remap

Performance booster!

- CPU1 Cortex-M4 address 0x0000 0000 remapping options (MEM_MODE)
  - Main Flash memory
  - System Flash memory (Bootloader)
  - SRAM1
  - Boosts performance thanks to I-Code/D-Code accesses instead of System Bus

life.augmented

The memory remap at CPU1 Cortex-M4 address 0 allows the boost of the performance thanks to Instruction and Data bus access instead of using the System bus.
The memory remapping at address 0 is selected using the MEM_MODE bits in the System Configuration Remap register. They allow the selection of either the main Flash memory, or the system Flash memory, or the SRAM1.



Here we have the STM32WL5 bus matrix. The bus masters are shown on top, the Cortex-M4 core, the Cortex-M0+ core and the two DMA controllers communicate with the bus slaves, shown on the right via the circled intersections.

The Flash memory is read through the accelerator. Cortex-M4 instructions are fetched through the Instruction bus and Literal Pools are read through the Data bus. The SRAM1 is accessed by default by the System bus and can be accessed though I-bus and D-bus when it is remapped at address 0, shown by the dark blue circles in order to increase performance. SRAM2 is accessible through the I-bus and D-bus allowing zero-wait-state code execution and through the S-bus. The AHB1, AHB2 and AHB3 peripherals are also accessible through the S-bus.

The Cortex-M0+ also reads the Flash memory through the Adaptive Real Time accelerator (ART) and has access to the

SRAM1 and SRAM2 memories and the AHB1, AHB2 and AHB Shared peripherals.

The two DMAs can access all memories and peripherals.

Different bus masters are able to access different memories and peripherals simultaneously via the bus matrix, enabling high performance computing operations. Simultaneous master accesses to the same bus is handled via round-robin arbitration.

Cortex-m4 boot modes

- BOOT0 pin or nBOOT0 option bit is selected through option bit nSWBOOT0

Boot mode selection			CPU1 Cortex-M4 Boot mode
nBOOT1 (option bit)	BOOT0 (pin) (or nBOOT0 option bit)	BOOT_LOCK (option bit)	
1	0	0	User Flash memory
1	1	0	System memory (bootloader)
0	1	0	SRAM1
0	0	0	Hold, Cortex-M4 will NOT boot. Boot Cortex-M0+ instead.
x	x	1	User Flash memory

life.augmented

There are three Cortext-M4 boot modes User Flash, System memory Boot loader, and SRAM1. Which are selected by the nBOOT0 option bit or the BOOT0 pin, the option bit named nBOOT1 and the option bit named BOOT_LOCK. When the BOOT0, nBOOT1, and BOOT_LOCK option bits are set to 0, the STM32WL5 holds the Cortex-M4 and boots on the Cortex-M0+. The standard method to get the STM32WL5 Cortex-M4 core booting from User Flash is to set nBOOT1 = 1 and BOOT0 and BOOT_LOCK option bits to 0.

Cortex-m0+ boot modes

- (
- |

Boot mode selection			CPU2 Cortex-M0+ Boot mode
nBOOT1 (option bit)	BOOT0 (pin) (or nBOOT0 option bit)	C2BOOT_LOCK (option bit)	
1	x	x	option Secure Boot Reset Vector (SBRV) and C2OPT
x	1	x	option Secure Boot Reset Vector (SBRV) and C2OPT
0	0	0	System memory (Secure Firmware Install)
x	x	1	option Secure Boot Reset Vector (SBRV) and C2OPT

life.augmented

There are two Cortext-M0+ boot modes. One is defined by the Secure Boot Reset Vector and the CPU2 boot Option. The other boot mode starts from System Memory Secure Firmware Install. The 2 modes are selected by the nBOOT0 option bit or the BOOT0 pin, the option bit named nBOOT1 and the option bit named C2BOOT_LOCK. When the BOOT0, nBOOT1, and BOOT_LOCK option bits are set to 0, the STM32WL5 holds the Cortex-M4 and boots on the Cortex-M0+ Secure Firmware Install located in the System Memory. The standard method to get the STM32WL5 booting on the Cortex-M4 core in User Flash and then the Cortex-M0+ booting id to set the C2BOOT bit in the power Controller.

The memory address the Cortex-M0+ boots from is defined by the secure boot reset vector and the CPU2 boot option. This allows the Cortex-M0+ to boot from any word-aligned address in User Flash or SRAM memory.

The BOOT0 pin or nBOOT0 option bit is selected by another option bit nSWBOOT0.

Bootloader

Protocol	I/Os and Comments	Comments
USART	USART1 on pins PA9/PA10 USART2 on pins PA2/PA3	
SPI	SPI1 on pins PA4/PA5/PA6/PA7 SPI2 on pins PB12/PB13/PB14/PB15	

life.augmented

The on-chip bootloader allows the user to program the Flash memory through a serial communications peripheral. The supported protocols are USART and SPI.

Secure firmware install

- Securely install Cortex-M4 and/or Cortex-M0+ software in User Flash.

life.augmented

The on-chip Secure Firmware Install allows the user to securely install Cortex-M4 and Cortex-M0+ software in the Flash memory.

SRAM2 features (1/2)

Performance, integrity and safety (Class B, SIL), retention in Standby

- 32 Kbytes of SRAM2
  - with access through Cortex-M4 D-code and I-code:
    - Code execution maximum performance without remap
  - with access through S-bus:
    - Continuous RAM address space with SRAM1
- HW parity check: 4 bits per word
  - NMI generated on parity error
  - Optional Break to Timers
- Optional retention in Standby

life.augmented

10

The 32 Kbytes of SRAM2 is particularly suitable for performance, integrity and safety, and low power operations. From the Cortex-M4 core, the SRAM2 is accessed through the Data and Instruction busses without any remapping, which enables code execution at zero-wait-states. The SRAM2 memory is accessible by Both CPUs through the S-bus allowing RAM address continuity between SRAM1 and SRAM2 memories.
The SRAM2 supports parity check. The Data bus width is 36 bits with 4 bits available for parity check (1 bit per byte) in order 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 memory. Then, they are automatically checked when reading. If one bit fails, a Non-Maskable Interrupt (NMI) is generated. The same error can also be linked to the

Break input of the timers.
The 32-Kbyte SRAM2 content can optionally be retained in Standby mode.

SRAM2 features (2/2)

Secured SRAM

- Write protection with 1-Kbyte granularity
  - SYSCFG_SWPRn write protection register
- Read/Write protection with RDP
  - Erased when RDP changed from Level 1 to Level 0
- Software reset and optional Hardware reset when system reset
  - Erased when setting SRAM2ER bit
  - Erased with system reset with SRAM2_RST in user option bytes
- Cortex-M0+ security
  - Cortex-M0+ exclusive access to SRAM2 areas.

life.augmented

11

The SRAM2 memory is also suitable for secure applications. It 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 the serial wire debug (SWD) port, when the boot in System flash or boot from SRAM memory 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.
Part of the SRAM2 can be made secure via user option bytes, only giving the Cortex-M0+ core exclusive access to

those areas.

SYSCFG other features

Safety and robustness

- Safety & Robustness features in Configuration register 2
  - SRAM2 Parity error flag
  - ECC lock to connect Flash ECC error connection to TIM1/15/16/17 Break input
  - PVD lock to connect PVD interrupt to TIM1/16/17 Break input
  - SPL lock to connect SRAM2 parity error to TIM1/16/17 Break input
  - CLL lock to connect Cortex-M4 Hard Fault interrupt to TIM1/16/17 Break input

  - => Put timers in application safe state in case of application crash

life.augmented

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 steer 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, a SRAM2 parity error event, and the Cortex M4 hard fault.

SYSCFG other features

- Manage interconnect signal selection from GPIOx (x=A,…H)
  - 16 Multiplexers to select EXTI[n] signal between PA[n] PB[n] …. PH[n] (n=0,…15)
  - select a GPIO[n] pin to be used as
    - Internal interconnect trigger signals. (see Interconnect matrix for more information)
    - CPU interrupt and wakeup from Stop mode. (see EXTI for more information)
- Other configurations
  - I2C GPIO Fast-mode-Plus 20 mA drive enable
    - I2C1 and I2C3 pins, high drive can be enabled even when not used for I2C.
  - I/O analog switches voltage booster

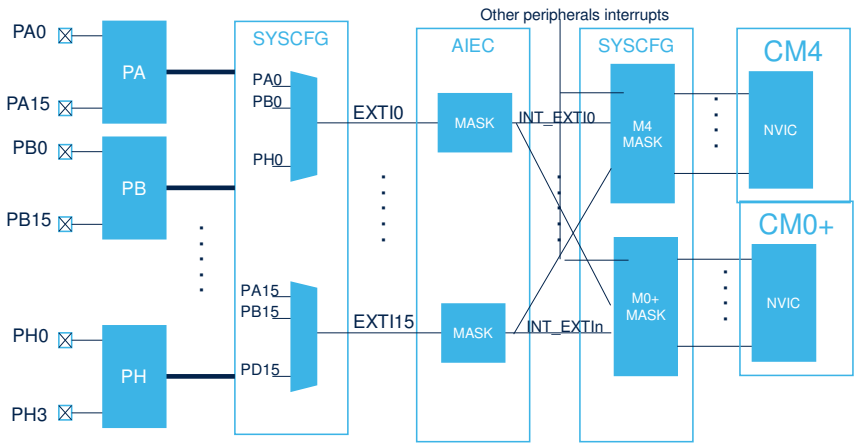
life.augmented

The System Configuration Controller manages the selection of the GPIO as interconnect EXTI signal.
This can be used as asynchronous external interrupt or event with capability to wake any MCU up from Stop state, and also as an internal interconnect trigger signal to peripherals. See interconnect matrix training for more information.

Other configurations are the I²C Fast-mode-Plus 20 mA drive enable on the I2C1 and I2C3 I/Os. The high drive mode can even be used when the pins are not used as I2C alternate functions. For instance, they can be used to drive LEDs.
The I/O analog switch voltage booster can also be enabled.

CPU interrupt pre-masking

- To prevent peripheral interrupt to interrupt both CPUs a pre-masking is provided.
  - Individual masks for interrupts sharing the same CPU NVIC vector.
    - EXTIs
    - PVD and PVM
    - ADC, DAC
    - Comparator
    - AES
    - PKA
    - Flash
    - RCC
    - RTC
    - DMA, DMAMUX



Peripheral interrupts sharing the same NVIC vector have a pre-mask to prevent them from interrupting both CPUs.

Related peripherals

- Refer to these training modules linked to this peripheral:
  - Reset and clock control (RCC)
  - Power controller (PWR)
  - Interrupts (NVIC and EXTI)
  - Flash memory (Flash)
  - System memory protections
  - Inter-Integrated Circuit (I^2C)

life.augmented

In addition to this training, you can refer to the Reset and Clock Control, Power Controller, Interrupts, Flash and System Memory Protections, I^2C trainings.

References

- For more details, please refer to following resources:
  - AN2606: STM32 microcontroller system memory boot mode
  - AN4435: Guidelines for obtaining UL/CSA/IEC 60335 Class B certification in any STM32 application

life.augmented

For more details, please refer to application notes AN2606 STM32 microcontroller system memory boot mode and AN4435 Guidelines for obtaining UL/CSA/IEC 60335 Class B certification in any STM32 application.