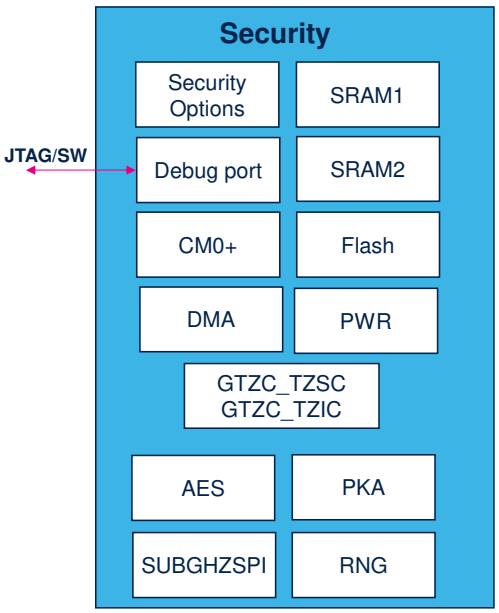
STM32WL5 – CM0+ security

Cortex-M0+ security

Revision 1.0

Hello, and welcome to this presentation of the STM32WL5 Cortex M0+ security features.

Overview



- The Cortex-M0+ security manages:
  - Exclusive Cortex-M0+ access.
  - Cortex-M0+ firmware security in:
    - Flash memory, SRAM1, and SRAM2, Debug access
  - Peripheral security for:
    - DMA, PWR, AES, PKA, TRNG, and SUBGHZSPI
- Control through Flash secure user options and GTZC.
- Security infringement monitoring through illegal access interrupt.

Application benefits

- Storage of application keys on the secure CM0+ side.
- Secure cryptography and secure radio communication
- Authentic and secure firmware installation and updates

2

The Cortex M0+ security manages the firmware and peripheral security, allowing the secure handling of cryptographic, and the sub-giga Hertz radio communication. It also provides secure firmware install and secure firmware update features.
The Cortex M0+ security uses secure options to control Flash memory, SRAM1, SRAM2, Debug and sub-giga Hertz serial peripheral interface security. Cryptographic peripherals like
Advanced Encryption Standard (AES), Private Key Accelerator (PKA), and True Random Number Generator (TRNG) security are managed dynamically at run time by the secure Cortex-M0+ core through secure register bits in the Global TrustZone Controller.
Security infringements are reported to the secure Cortex-M0+ through illegal access events, monitored in the Global TrustZone Controller.

Cortex M0+ security key features

Firmware authentication and secure key handling

- Secure Flash memory, SRAM1 and SRAM2 areas
  - Exclusively accessible by the Cortex-M0+.
- Secure peripherals
  - Exclusive access to SUBGHZSPI, AES, PKA, and TRNG by the Cortex-M0+.
  - Exclusive Cortex-M0+ access to secured DMA channels.
- Debug security
  - Secure memory areas and peripherals not accessible through debug port.
- Resource protection based on privilege
  - Memories and peripherals may be protected by privileged.

life.augmented

3

The Cortex-M0+ security is based on giving exclusive access to secure areas in Flash memory, SRAM1 and SRAM2.
Additionally, peripherals such as sub-giga Hertz serial peripheral interface, AES, Private Key Accelerator and True Random Number Generator can be made secure, to allow secure radio communication and cryptography and key generation.
Direct memory access channels can be secured on a channel base, allowing secure data transfer and channel control.
The secure memory areas and peripherals are not accessible by the Cortex-M4 and neither through the debugger when secure debugging is disabled.
In addition to security, memories and peripherals can be protected by privilege.

Cortex M0+ security

- Flash memory and SRAM areas and CM0+ Debug Security
  - Enabled by Flash user options.
  - Parameter can only be modified by secure Cortex-M0+ firmware
- Secure peripherals
  - Enabled by Flash user options.
    - for SUBGHZSPI, keeping sub-GHz radio communication secure even after a reset.
  - Enabled at run time by secure firmware running on Cortex-M0+
    - AES, PKA, and TRNG security, allows sharing with non-secure Cortex-M4 on a needed basis
    - DMA channels, allowing sharing with non-secure Cortex-M4 on a needed basis
- Secure privileged protection
  - Allows to protect Cortex-M0+ secure privileged resources from secure unprivileged accesses

life.augmented

The Cortex M0+ security is to be enabled by the customer when installing the Cortex-M0+ firmware. Once installed security is completely handled by the Cortex M0+ itself. At STM32WL5 production, the Cortex M0+ security is disabled, the Secure Firmware Install allows the secure installation of the Cortex-M0+ firmware. Any subsequent Cortex M0+ firmware update may be handled by the secure boot secure firmware update installed on the Cortex M0+.
Also, the sub-giga Hertz radio security shall be defined when installing the Cortex-M0+ firmware.
The AES, PKA, and RNG peripheral security is fully handled by the Cortex M0+ at run time whenever needed by the Cortex M0+ application. The direct memory access channels can also be secured when needed at run time by the Cortex M0+.
Furthermore, the Cortex M0+ is equipped with privileged protection, which can be enabled at run time by the Cortex-M0+ firmware. It allows to protect Cortex-M0+ secure

privileged resources from secure unprivileged accesses.

Cortex M4 privilege protection

- Non-secure privilege protection
  - Allows to protect Cortex-M4 non-secure privileged resources from unprivileged accesses.

life.augmented

5

The Cortex M4 privilege protection can be enabled at run time by the Cortex-M4 firmware. It allows to protect Cortex-M4 non-secure privileged resources from unprivileged accesses.

Secure options registers

- Cortex-M0+ security is configured by secure User Options.

Register	Fields									
OPTR (*)	C2BOOT_LOCK	User Options							ESE	RDP
SFR (*)	SUBGHZSPISD	res.	HDPAD		HDPSA	res.	DDS	res.	FSD	SFSA
SRRVR (*)	C2OPT	NBRSD	SNBRSA	res.	BRSD	SBRSA	SBRV			

*OPTR: Options Register
*SFR: Secure Flash Register
*SRRVR: Secure Ram and Reset Vector Register

- When the Cortex-M0+ security is enabled, the secure User Options are exclusively writable by the Cortex-M0+.
  - The non-secure Cortex-M4 can read the secure User Options allowing it to determine the security settings.

life.augmented

The Cortex-M0+ security is controlled through secure user options loaded at device startup in the Secure Flash Registers.
The secure user options can only be modified by the secure Cortex-M0+, i.e. to change parameters when a secure Cortex-M0+ software is updated.
The non-secure Cortex-M4 has read access to the secure user options to be able to determine the security configuration.

Secure user options 1/2

- Memory security handled by secure user options
- Flash memory security
  - Security enable (FSD) ➔ Global enable of the Cortex-M0+ security
  - Secure Flash Start Address (SFSA)
    - The Flash memory is secure from this start address watermark until the top of the Flash memory.
- RAM security
  - RAM security enable (BRSD: backup SRAM2) (NBRSD: non-backup SRAM1)
  - Secure RAM Start Address (SBRSA: backup SRAM2) (SNBRSA: non-backup SRAM1)
    - The RAM is secure from its start address watermark until the top of the RAM.
- Enable security environment (ESE)
  - This bit when read, indicates that the security is enabled.
  - When written, this bit allows the regression of the security when regressing also RDP.

life.augmented

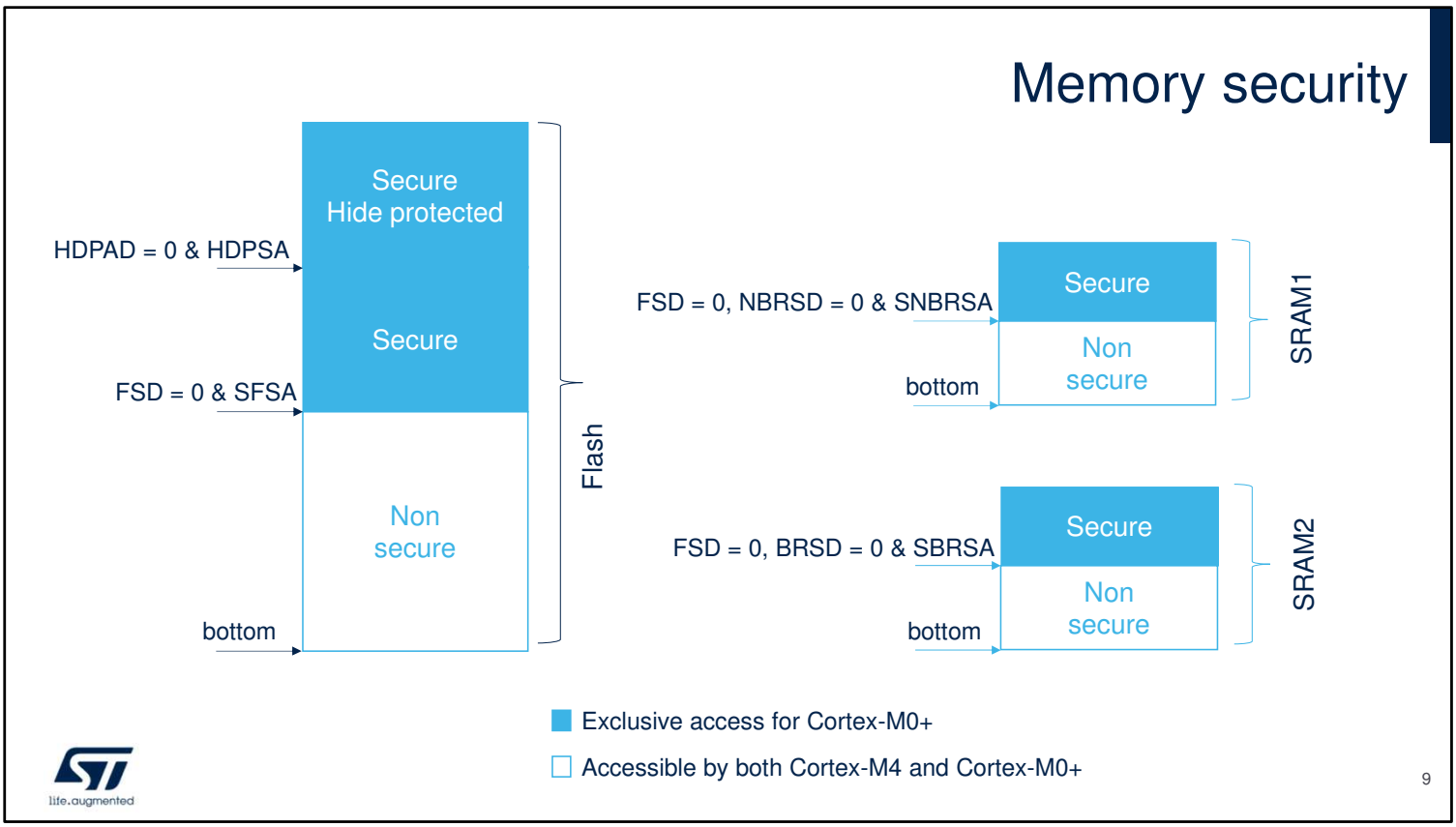
Memory security is enabled and configured by secure user options.
The Flash Security Disable bit (FSD) enables the Global Cortex-M0+ security.
The Secure Flash Start Address (SFSA) defines the start address watermark from which the Flash memory is secure.
The Backup RAM Security Disable bit (BRSD) controls the security on the backup SRAM2, and the Secure Backup RAM Start Address (SBRSA) defines the start address watermark from which the backup SRAM2 is secure.
The Non-Backup RAM Security Disable (NBRSD) bit is used to enable security on the SRAM1, and the Secure Non-Backup RAM Start Address (SNBRSA) defines the start address watermark from which the SRAM1 is secure.
The Enable Security Environment bit (ESE), when read, provides information whether the device is secured or bot.
When written, this bit allows the regression of the security at the same time when regressing RDP.

Secure user options 2/2

- Flash memory hide protection
  - Hide protection disable (HDPAD)
  - Hide protection Start Address (HDPSA)
    - The Flash memory is hide protected from this start address watermark until the top of the Flash memory.
    - The hide protection area is used for any secure boot and secure firmware update function.
- Disable Debug security (DDS)
  - This bit disables debug access to the Cortex-M0+.
- CPU2 boot lock (C2BOOT_LOCK)
  - This bit locks the boot mode of the Cortex-M0+.

life.augmented

The Flash memory Hide Protection Disable (HDPAD) bit enables the hide protected area in the Cortex-M0+ secure Flash area. The Hide Protection Start Address defines the start address watermark from which the Flash memory is hide protected. The secure boot and secure firmware update are located in this area. It is executed once after a Cortex-M0+ reset and subsequently hidden until a next reset.
The Debug access to the secure Cortext-M0+ and all secure resources is controlled by the Debug Disable Security bit (DDS).
The CPUs boot lock bit allows the creation of a root of trust for the Cortex-M0+ boot, which is useful with a secure boot or a secure firmware update.



The top of the memories can be secured for exclusive Cortex-M0+ access.
The top of the Flash memory, starting from the Secure Flash Start Address watermark, is secure when the Flash Security Disable bit is set to “0”.
The top of the backup SRAM2, starting from the Secure Backup RAM Start Address watermark, is secure when both the Flash Security Disable and Backup RAM Security Disable bits are set to “0”.
The top of the SRAM1, starting from the Secure Non-Backup RAM Start Address watermark, is secure when both the Flash Security Disable and Non-Backup RAM Security Disable bits are set to “0”.
It is possible to only secure the Flash memory without any RAM security; however, it is recommended to secure both the Flash memory and RAM used by the Cortex-M0+ software.
Within the secure Flash area, a hide protected area can be

defined by the Hide Protection Disable and the Hide Protection Start Address watermark.

Security & memory erase

- Flash Page Erase
  - Secure pages can only be erased by the secure Cortex-M0+.
- Flash Mass Erase
  - The Flash memory can only be mass erased when requested by the Cortex-M0+.
  - Flash Mass Erase operations requested by the non-secure Cortex-M4 are rejected.
- Flash Erase due to RDP regression
  - Only the non-secure Flash memory area is multiple page erased.
- Flash Mass Erase due to ESE and RDP regression
  - Flash Mass Erase and SRAM2 erase, allowing secure and non-secure Flash to be erased.

life.augmented

The STM32WL5 microcontroller has a single Flash memory for both the Cortex-M4 and Cortex-M0+ software. The Cortex-M0+ security prevents secure Flash memory pages from being erased by the non-secure Cortex-M4 core. A Cortex-M4 Flash Mass Erase operation will be rejected, and a Multiple Block Erase has to be used to erase the Cortex-M4 software.
When regressing the ReaD Protection (RDP) from Level 1 to Level 0, only the non-secure part of the Flash memory will be erased. The secure Cortex-M0+ software will be retained. The complete Flash memory is mass erased, and the security is removed only when regressing the ReaD Protection from Level 1 to Level 0 and at the same time Enable Security Environment. In this case all software, secure and non-secure is erased.

Cortex-m0+ boot reset vector

- The Cortex-M0+ boot reset vector is programmed in the Secure Boot Reset Vector (SBRV) option.
  - Word-aligned value.
- The Cortex-M0+ may boot from Flash memory or SRAM as selected by the Secure CPU2 option (C2OPT).
- At production time, the Cortex-M0+ boot reset vector is set to the middle of the Flash memory.

life.augmented

The Cortex-M0+ boot reset vector is to be programmed in the secure boot reset vector option and secure CPU2 option. At production time, the Cortex-M0+ boot reset vector points to the middle of the Flash memory. In Secure mode, the Cortex-M0+ boot reset vector can only be changed by the secure Cortex-M0+ side.

Debug disable

- **Debug access handled by secure options**

- Debug access handled by secure user options
- Controlled by the Debug Disable Secure option (DDS)
  - Disable debug port access to the Cortex-M0+.
- Debug can be enabled and disabled in Secure and Non-secure modes.
  - Debug access control is independent from security
  - In secure mode debug access can only be changed by the secure Cortex-M0+ side.

life.augmented

Cortex-M0+ debug access is controlled by the Debug Disable Option bit. It is independent from security and can be enabled and disabled in both Secure and Non secure modes. In Secure mode, debug access control can only be changed by the secure Cortex-M0+ side.

Sub-GHz radio security

- **Sub-GHz radio access handled by secure options**

- Sub-GHz radio access handled by secure user options
- Controlled by SUBGHZSPISD option
  - Allows to control access to the sub-GHz radio, to be exclusively accessible by the secure Cortex-M0+.
  - Security setting is applied from reset.

life.augmented

13

Sub-giga Hertz radio access can be secured by the sub-giga Hertz Radio Serial Peripheral Interface security disable user option. It allows to secure the sub-giga Hertz radio for exclusive Cortex-M0+ access. When enabled sub-giga Hertz radio access is secured from reset.

Secure peripheral configuration

- Peripheral security is handled by register bits.
- Peripheral security configured in the GTZC_TZSC.
  - Allows peripherals to be secured at run time.
  - Allows peripheral sharing on a need as basis between the secure CM0+ and the non-secure CM4.
  - Peripheral security is only available when Security is enabled in (FSD)
    - AES, PKA, and true RNG.
- DMA channel security configured in the DMA.
  - Allows DMA channels to be secured at run time.
  - Allows DMA channels sharing on a need as basis between the secure CM0+ and the non-secure CM4.

life.augmented

The AES accelerator 1, Public Key Accelerator and True Random Number Generator peripherals can dynamically be secured at run time by Cortex-M0+ firmware.
DMA channels can dynamically be secured at run time by Cortex-M0+ firmware.
The security information can be read by the non-secure Cortex-M4 to get information on the peripheral security status.

Privileged protection

- Privilege protection is handled by register bits in the GTZC_TZSC.
  - Allows privileged resources to be protected from unprivileged accesses.
- A single privileged watermark is available for each memory.
- Privileged protection is available only on resources that feature security protection
  - Memories, sub-GHZ radio access, AES, PKA, true RNG, DMA channels.

life.augmented

Privilege protection gives exclusively access to privileged accesses. Each memory has a single watermark allowing the memory to be split in a privileged part and an unprivileged part.
The securable peripherals also allow for privilege protection.
Privilege protection can be enabled at run time.

Secure firmware install / update

- Secure firmware can be installed by the Secure Firmware Install function.
  - Available from system memory (see Flash module)
- Secure firmware update feature can be installed in the hide protected secure Flash area.
- The secure Cortex-M0+ is able to update the user options in all RDP levels.

life.augmented

16

The STM32WL5 includes a preprogrammed secure firmware install (SFI) firmware in its system memory, which allows the securely installation of any Cortex-M0+ software.
For subsequent firmware updates, a secure firmware update function can be installed in the hide protected secure flash area.
A secure Cortex-M0+ software update is possible in all ReaD Protection (RDP) levels (0, 1, and 2).

Security illegal accesses

- illegal accesses to secure resources can be signaled to the secure Cortex-M0+.
- When enabled, an illegal access wakes the Cortex-M0+ up from any operating mode.
- It is up to the Cortex-M0+ firmware to take appropriate action.
- Illegal accesses information is available from:
  - Secure/privileged memory areas Flash, SRAM1, and SRAM2.
  - Secure/privileged peripherals DMA, DMAMUX, SUBGHZSPI, AES, PKA and true RNG.
  - Security and privilege control in GTZC and PWR.

life.augmented

Illegal accesses to secure and or privileged resources can be signaled to the Cortex-M0+. It is up to the Cortex-M0+ firmware to take appropriate action. An illegal access wakes the Cortex-M0+ up from any operating state, including reset.

Cortex-m4 events

Action:	CM4 Generated event:
Cortex-M4 execute fetch from secure memory area	Bus error
Cortex-M4 unprivileged execute fetch from privileged memory area	Bus error
Cortex-M4 read access to secure Flash memory area	Read zero value
Cortex-M4 read access to secure RAM memory area	Read zero value
Cortex-M4 read access to secure peripheral registers	Read zero value

life.augmented

This slide lists the events handled by the Cortex-M4 core resulting from the Cortex-M0+ security features. Any Cortex-M4 instruction fetch from secure memory areas generates a bus error. Reading secure areas returns data value zero. Only the security configuration user options and peripheral security configuration bits can be read by the non-secure Cortex-M4 core.

Cortex-m0+ events

Action:	CM0+ Generated event:
Cortex-M4 security illegal access	Wakeup and interrupt
Cortex-M0+ unprivileged execute fetch from privileged memory area	Bus error

life.augmented

This slide lists the events handled by the Cortex-M0+ resulting from the Cortex-M0+ security features. Any Cortex-M4 illegal access to secure resources generates an illegal access event sent to the Cortex-M0.

Related peripherals

- Refer to these trainings linked to this feature:
  - STM32WL5 Flash memory interface
    - Secure user options
  - STM32WL5 Global TrustZone Configuration (GTZC)
    - Peripheral security bits
    - Infringement illegal access control
  - STM32WL5 Power controller (PWR)
    - Infringement illegal access wakeup control
  - DMA and DMAMUX
    - Secure DMA channels

life.augmented

In addition to this training, you may find the flash memory interface, Global TrustZone Controller, Power controller and DMA and DMAMUX modules useful.