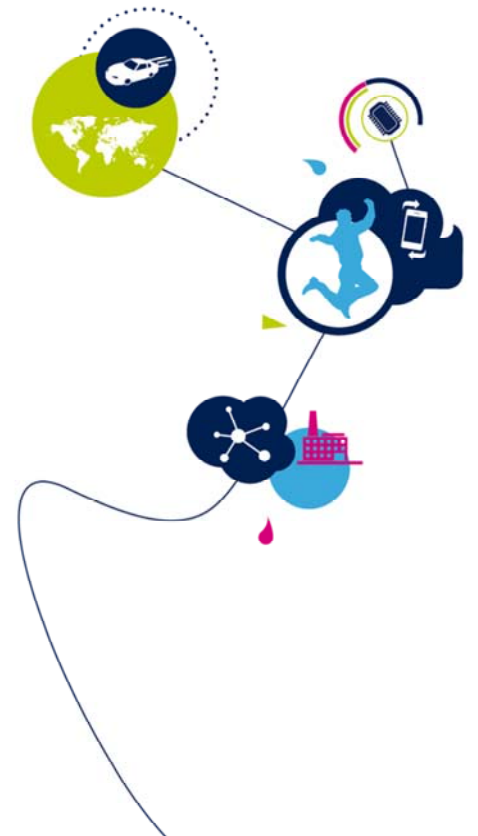


STM32MP1 – SECOVR

Security Architecture Overview
Revision 1.0



Hello, and welcome to this presentation of the STM32MP1 security architecture overview.

- STM32MP1 security architecture is based on Arm® TrustZone® technology.
- TrustZone splits resources between two execution environments (namely secure and normal non-secure worlds).
- Cortex A7 supports ARMv7-A Architecture with security extension. It is at the root of the split environment.
- SoC interconnect security gates (aka stubs) check for permissions at various levels (AHB and AHB2APB bridge level), and block unauthorized access to security sensitive resources.
- TrustZone Memory Adapters (TZMA) support division of on chip RAM/ROM in secure/non-secure in multiples of 4KB.
- TrustZone Address Space Controller (TZC) supports classification of DDR address ranges into regions with secure/non-secure access.



Security sensitive resources (TrustZone aware) with local access control.

The STM32MP1 security architecture is based on Arm® TrustZone® technology.

ARM TrustZone splits resources between two execution environments (namely secure and normal non-secure worlds)

Cortex A7 supports ARMv7-A Architecture with the security extension. It is at the root of the split environment.

SoC interconnect features security gates (also known as stubs) check for permissions at various levels of the Soc interconnect, at AHB bus and AHB2APB bridge level, and block any unauthorized access to security sensitive resources.

TrustZone Memory Adapters (TZMA) support division of on chip RAM/ROM memories in secure/non-secure regions with

a granularity of 4KB.

TrustZone Address Space Controller (TZC) supports classification of DDR address ranges into regions with secure/non-secure access.

Security sensitive resources (TrustZone aware) have local access control.

Security components & classification

3

- TrustZone capable IP:
 - Cortex-A7 subsystem (including L1 and L2 cache, MMU and GIC) with security extension .
 - MDMA implements security per channel.
 - DAP: Debug Access Port to secure Debug via authentication interface.
- Secure IPs:
 - Unconditionally secure or write-secure.
- Securable IPs
 - Peripherals and on-chip memories which can be programmed via ETZPC to be: secure, write-secure or non secure.
- TrustZone aware IPs
 - Peripherals sensitive to security with some local features to become secure.
- Non-Secure IPs
- Memory adapters (TZMA)
 - To segment SYSRAM and ROM memories into secure and non secure regions.
- TZC (DDR)
 - To segment DDR memory in multiple regions, with secure/non secure rights ; note non-secure regions may be filtered per master according to its NSAID.



The security properties of components can be enumerated as:

TrustZone capable IP:

- Cortex-A7 subsystem (including L1 and L2 cache, MMU and GIC) with security extension
- MDMA implements security per channel
- DAP: Debug Access Port to secure Debug via authentication interface

Secure IPs:

- Unconditionally secure or write-secure

Securable IPs:

- Peripherals and on-chip memories which can be programmed via ETZPC to be: secure, write-secure or non-secure.

TrustZone aware IPs

- Peripherals sensitive to security with some local features to become secure.

Non-Secure IPs

Memory adapters (TZMA)

- To segment SYSRAM and ROM memories into secure and non-secure regions

TZC (DDR)

- To segment DDR memory in multiple regions, with secure/non secure rights ; note non-secure regions may be filtered per master according to its NSAID.

- Access to non secure resources by secure world is always possible.
- Access is illegal when non-secure world attempts to access secure resources
- Error behavior for illegal access are:
 - Illegal Accesses are always denied : A write access is ignored and a read access returned with zero.
 - The options to flag errors can be either a silent fail, bus errors or interrupts.
- Default settings
 - There are no unique rule, but IPs are mostly non-secure by default.
 - for TZ aware IPs please refer to IP description
 - Securable IPs and TZMA are secure by default with bus error response on illegal access.



Access to non-secure resources by secure world is always possible.

Access is illegal when non-secure world attempts to access secure resources

Error behavior for illegal access are:

- Illegal Accesses are always denied : A write access is ignored and a read access returned with zero.
- The options to flag errors can be either a silent fail, bus errors or interrupts.

Default settings

- There are no unique rule, but IPs are mostly non-secure by default.
- for TZ aware IPs please refer to IP description.

- Securable IPs and TZMA are secure by default with bus error response on illegal access.

- Securable peripherals are controlled by ETZPC decprot bits.
- Decprot[1:0] bit are encoded as :
 - 0b00: secure
 - 0b01: write-secure
 - 0b11: non-secure
- Note: 0b10 is either reserved or used to control MCU
(please refer *ETZPC OLT training*)



Securable peripherals are controlled by ETZPC decprot bits.

Decprot[1:0] bit are encoded as :

- 0b00: secure
- 0b01: write-secure
- 0b11: non-secure

Note: 0b10 is either reserved or used to control MCU.

Securable IP's and ETZPC decprot

7

#	decprot bits	IP	BUS	default	bus master	type	attributes
0	DECPROT0[1:0]	STGENC	APB5	0b00		1	securable
1	DECPROT0[3:2]	BKPSRAM	AHB5	0b00		1	securable
2	DECPROT0[5:4]	IWDG1	APB5	0b00		1	securable
3	DECPROT0[7:6]	USART1	APB5	0b00		1	securable
4	DECPROT0[9:8]	SPI6	APB5	0b00		1	securable
5	DECPROT0[11:10]	I2C4	APB5	0b00		1	securable
7	DECPROT0[15:14]	RNG1	AHB5	0b00		1	securable
8	DECPROT0[17:16]	HASH1	AHB5	0b00		1	securable
9	DECPROT0[19:18]	CRYP1	AHB5	0b00		1	securable
10	DECPROT0[21:20]	DDRCTRL	APB4	0b00		1	securable
11	DECPROT0[23:22]	DDRPHYC	APB4	0b00		1	securable
12	DECPROT0[25:24]	I2C6	APB5	0b00		1	securable

#	decprot bits	IP	BUS	default	bus master	type	attributes
80	DECPROT5[1:0]	SRAM1	MLAHB	0b11		3	securable and MCU isolation support
81	DECPROT5[3:2]	SRAM2	MLAHB	0b11		3	securable and MCU isolation support
82	DECPROT5[5:4]	SRAM3	MLAHB	0b11		3	securable and MCU isolation support
83	DECPROT5[7:6]	SRAM4	MLAHB	0b11		3	securable and MCU isolation support
84	DECPROT5[9:8]	RETRAM	MLAHB	0b11		3	securable and MCU isolation support



The decprot bits associated to securable peripherals and to MCU RAMS are listed in this table

Securable IP's are:

- Service peripherals for secure application:
USART1, SPI6, I2C4, I2C6
- Cryptographic accelerators: CRYP1, HASH1, RNG1
- System peripherals: STENC, IWDG1
- BKPSRAM which is securable with erase on tamper.
- DDRCTRL and DDRPHYC are made securable if concerned by TrustZone Address Space Controller (TZC).

TrustZone Aware: BSEC

- BSEC is used to control the Device Life Cycle, Debug authentication and to store secrets in OTP
- BSEC is TrustZone aware (see BSEC training)
- BSEC is composed of 3 regions
 - Control Interface registers
 - Lower OTP shadow registers
 - Upper OTP shadow registers
- Read and Write permissions are set according to OTP modes (see below).

Read access permissions vs region

OTP mode	Control registers ⁽¹⁾		Lower OTP shadow registers		Upper OTP shadow registers	
	APB secure	APB non-secure	APB secure	APB non-secure	APB secure	APB non-secure
OTP-SECURED	Yes	Yes	Yes	Yes	Yes	No
OTP-INVALID	Yes	No	No	No	No	No

Write access permissions vs region

OTP mode	Control registers ⁽¹⁾		Lower OTP shadow registers		Upper OTP shadow registers	
	APB secure	APB non-secure	APB secure	APB non-secure	APB secure	APB non-secure
OTP-SECURED	Yes	No	Yes	No	Yes	No
OTP-INVALID	No	No	No	No	No	No



BSEC is used to control the Device Life Cycle, Debug authentication and to store secrets in OTP.

BSEC is TrustZone aware (see BSEC training)

BSEC is composed of 3 regions:

- Control Interface registers
- Lower OTP shadow registers
- Upper OTP shadow registers

Read and Write permissions are set according to OTP modes.

- Clock gating and reset control of a secure IP can only be modified by secure access
- RCC provides a dedicated secure interrupt about clock security.
- RCC security is controlled by 2 bits: TZEN and MCKPROT, which are write-secure.

** For more details see Product Reference Manual RCC section



Clock gating and reset control of a secure IP can only be modified by secure access.

RCC provides a dedicated secure interrupt about clock security.

RCC security is controlled by 2 bits: TZEN and MCKPROT, which are write-secure.

For more details see Product Reference Manual RCC section.

- Power mode control of a secure IP must be modified only by secure access.
- PWR security is controlled by the bit TZEN from RCC.
- PWR security consist in preventing a non-secure write to:
 - Change settings of VBAT and TEMP Monitor, PVD and AVD.
 - Change the low-power Deep sleep and RAM low-power settings.
 - Change the backup domain write protection.
 - Change the Backup regulator, Retention regulator, 1V8 regulator, 1V1 regulator and USB 3.3V voltage level detector settings.
 - Change the backup battery charging settings.
 - Change MPU power control register settings.
 - Change the Standby wakeup settings and flags

** For more details see Product Reference Manual PWR section



Power mode control of a secure IP must be modified only by secure access.

PWR security is controlled by the bit TZEN from RCC.

PWR security consist in preventing a non-secure write to:

- Change settings of VBAT and TEMP Monitor, PVD and AVD.
- Change the low-power Deep sleep and RAM low-power settings.
- Change the backup domain write protection.
- Change the Backup regulator, Retention regulator, 1V8 regulator, 1V1 regulator and USB 3.3V voltage level detector settings.
- Change the backup battery charging settings.
- Change MPU power control register settings.
- Change the Standby wakeup settings and flags

For more details see Product Reference Manual PWR

section.

- EXTI can protect sensitive events by restricting the access to control and configuration bits related to these events.
- Security can be activated per input with bit EXTI_TZENR
- Security prevents non-secure write access to change settings or mask and clear status of secure inputs

** For more details see Product Reference Manual EXTI section



life.augmented

EXTI can protect sensitive events by restricting the access to control and configuration bits related to these events.

Security can be activated per input with bit EXTI_TZENR.

Security prevents non-secure write access to change settings or mask and clear status of secure inputs.

For more details see Product Reference Manual EXTI section.

- Security is applicable only to GPIOZ.
- After reset all GPIOZ I/O pins are secure.
- GPIOZ I/O pins can be individually set as secure with the GPIOZ_SECCFGR register.
- When an I/O pin is secure, all its I/O configuration bits are write-secure.
- Input to a secure pin cannot be redirected to non-secure I/O whatever its configuration.
- Output data from a secure pin cannot be replaced by output from another peripheral.
- Secure I/O data cannot be redirected to non-secure I/O.
- Non-secure I/O data cannot be redirected to secure I/O.



Security is applicable only to GPIOZ.

After reset all GPIOZ I/O pins are secure.

GPIOZ I/O pins can be individually set as secure with the GPIOZ_SECCFGR register.

When an I/O pin is secure, all its I/O configuration bits are write-secure.

Input to a secure pin cannot be redirected to non-secure I/O whatever its configuration.

Output data from a secure pin cannot be replaced by output from another peripheral.

Secure I/O data cannot be redirected to non-secure I/O.

Non-secure I/O data cannot be redirected to secure I/O.

- 4 RTC functions: Alarm A, Alarm B, Wakeup Timer and Timestamp can be individually configured as secure.
- RTC can be configured secure (global)
- RTC initialization and calibration control can be configured secure.
- Write Secure RTC_SCMR is used to control RTC security settings
- A silent fail results from a non secure access to RTC_SCMR bits.
- Inheritance of RCC clock and reset control is attached to a resource.
- RTC is non secure by default
- Security settings are persistent in low power: the settings are reset only by backup domain POR, and not affected by system Reset.
- Interrupts control (masking and clearing) inherits the security properties of the features the interrupt is attached to.



4 RTC functions: Alarm A, Alarm B, Wakeup Timer and Timestamp can be individually configured as secure.

RTC can be configured globally secure.

RTC initialization and calibration control can be configured secure.

Write Secure RTC_SCMR is used to control RTC security settings.

A silent fail results from a non-secure access to RTC_SCMR bits.

Inheritance of RCC clock and reset control is attached to a resource.

RTC is non secure by default.

Security settings are persistent in low power: the settings are

reset only by backup domain POR, and not affected by system Reset.

Interrupts control (masking and clearing) inherits the security properties of the features the interrupt is attached to.

- The Tamper control can be configured as secure.
- The 128 Backup registers are organized in 3 Zones:
 - Zone1: Secure, Read and Write only by secure
 - Zone2: Write secure, Write only by secure
 - Zone3: Non secure:
- TAMP can be configured as secure (global).
- Write Secure TAMP_SCMR register is used to control TAMP security settings.
- The Backup registers Zone size are programmable.
- Inheritance of TAMP clock and reset control is attached to a resource.
- TAMP is non secure by default.
- Security settings are persistent in low power: the settings are reset only by backup domain POR, and not affected by a system Reset.



Interrupts control (masking and clearing) inherits the security properties of the features the interrupt is attached to.

The Tamper control can be configured as secure.

The 128 Backup registers are organized in 3 Zones:

- Zone1: Secure, Read and Write only by secure
- Zone2: Write secure, Write only by secure
- Zone3: Non secure:

TAMP can be configured as secure.

Write Secure TAMP_SCMR register is used to control TAMP security settings.

The Backup registers Zone size are programmable.

Inheritance of TAMP clock and reset control is attached to a resource.

TAMP is non secure by default.

Security settings are persistent in low power: the settings are reset only by backup domain POR, and not affected by a system Reset.

Interrupts control (masking and clearing) inherits the security properties of the features the interrupt is attached to.

TrustZone aware and capable IP: MDMA

15

- MDMA supports 32 channels
- A channel can be secured by setting the SM bit from MDMA_CxCR register where x is the channel number (0 to 31)
- SM bit can only be modified by a secure access (write-secure bit)
- MDMA is routing interrupts to secure and normal lines, according to the channel security attributes.
- When a channel is secure, all its associated registers are write-secure.
- MDMA AXI master port propagates the security attributes of corresponding channel.



MDMA supports 32 channels.

A channel can be secured by setting the SM bit from MDMA_CxCR register where x is the channel number (0 to 31).

The SM bit can only be modified by secure (write-secure bit).

MDMA is routing interrupt to secure and normal lines, according to channel security attributes.

When a channel is secure, all its associated registers are write-secure.

MDMA AXI master port propagates the security attribute of the corresponding channel.

- The Debug Access Port (DAP) is a non secure Bus Master.
- The Access to Debug resources is controlled by the Debug Authentication interface issued from BSEC.

** For more details see Product Reference Manual Debug section



The Debug Access Port (DAP) is a non-secure Bus Master. The Access to Debug resources is controlled by the Debug Authentication interface issued from BSEC. For more details see the Product Reference Manual Debug section.