# STM32CubeProgrammer OTP management

# Contents

Stable: 27.01.2020 - 10:35 / Revision: 27.01.2020 - 10:33

Stable: 27.01.2020 - 10:39 / Revision: 27.01.2020 - 10:39

A quality version of this page, approved on *27 January 2020*, was based off this revision.

STM32CubeProgrammer can be used to read and update the OTP of the device which is seen as a partition on the device .

This page describes the format of the partition used by embedded programming service to allow OTP access by STM32CubeProgrammer (see AN5275: USB DFU/USART protocols used in STM32MP1 Series bootloaders for protocol details).

Refer to STM32CubeProgrammer article to know how to use the STM32CubeProgrammer that is the official STMicroelectronics tool for update OTP on STM32 platforms.

Contents

1 OTP partition ..... 4
1.1 Access operation ..... 4
1.2 Data structure ..... 4
2 Reference list ..... 10

# 1 OTP partition

The OTP partition is identified by the reserved Id 0xF2 and is exported as a specific alternate setting of the USB DFU [1].

This is used to access the STM32MP's on-chip one time programmable memory, and is only supported in U-Boot.

The OTP partition must be programmed without a header and must have a fixed size of 1024 bytes = 256 words (32 bits), following the structure described in chapter #Data Structure.

## 1.1 Access operation

For read operation, the host requests the OTP partition data, and the platform replies with all the partition content (1024 bytes).

For write operation, the host needs to send the full structure containing one or more modifications. Each field is analyzed by the platform. First the OTP values are updated, then the OTP controls (such as lock) are updated.

After any write operation, a read must be done to update the Host information.

## 1.2 Data structure

The data structure for the STM32MP15x Series is described in the table below.

Access can be RWS = Read / Write / Sticky

| Word | Field name | Description | RWS |
|---|---|---|---|
| 0 | Version | Version of this structure | R |
| 1 | Configuration | • Bit 8:7 TREAD[1:0]: set SAFMEM reading current level (default = 0b00)<br>• Bit 6:3 PRGWDTH[3:0] : SAFMEM programming pulse width (default = 0b0001)<br>• Bit 2:1 FRC[1:0]: SAFMEM CLOCK frequency range selection:<br>  • 00: 10 MHz <= Freq <= 20 MHz<br>  • 01: 20 MHz <= Freq <= 30 MHz<br>  • 10: 30 MHz <= Freq <= 45 MHz<br>  • 11: 45 MHz <= Freq <= 67 MHz<br>• Bit 0 PWRUP: SAFMEM power-up control<br>  • 0: SAFMEM is powered down.<br>  • 1: SAFMEM is powered up | RW |
| 2 | Reserved | | |
| | | • Bits 7 BIST2LOCK: BIST2 LOCKED<br>  • 0: SAFMEM BIST2 is not locked<br>  • 1: SAFMEM BIST2 is locked<br>• Bits 6 BIST1LOCK: BIST1 LOCKED<br>  • 0: SAFMEM BIST1 is not locked<br>  • 1: SAFMEM BIST1 is locked<br>• Bits 5 PWRON: SAFMEM Power Status<br>  • 0: SAFMEM is in power off | |

| Word | Field name | Description | RWS |
|---|---|---|---|
| 3 | Status | • 1: SAFMEM is in power on<br>• note: used to poll pwrok signal value<br>• Bits 4 PROGFAIL: Last programming status<br>• 0: SAFMEM last programming was successful<br>• 1: SAFMEM last programming failed<br>• Bits 3 BUSY: SAFMEM operation status<br>• 0: SAFMEM is Idle<br>• 1: SAFMEM operation is on going<br>• note: bit polling is used to determine operation completion<br>• Bits 2 INVALID: OTP mode invalid<br>• 0: OTP mode is not OTP-INVALID<br>• 1: OTP mode is OTP-INVALID<br>• Bits 1 FULLDBG: OTP mode in full debug<br>• 0: OTP mode is OTP-OPEN1<br>• 1: OTP mode is OTP-OPEN2<br>• Bits 0 SECURE: OTP mode secured<br>• 0: OTP mode is not OTP-SECURED<br>• 1: OTP mode is OTP-SECURED | R |
| 4 | General Lock conf | • Bit4 GPLOCK: SAFMEM programming sticky lock<br>• 0: SAFMEM programming allowed<br>• 1: SAFMEM programming is disabled until the next system-reset<br>• Bit 3 FENREG feature enable register sticky lock<br>• 0: BSEC_FENABLE register is not locked<br>• 1: BSEC_FENABLE register is locked until the next system reset<br>• Bit 2 DENREG debug enable register sticky lock<br>• 0: BSEC_DENABLE register is not locked<br>• 1: BSEC_DENABLE register is locked until the next system reset<br>• Bit 1 : Reserved, must be kept at reset value.<br>• Bit 0 OTP: upper OTP region access:<br>• 0: not locked<br>• 1: Locked until the next system reset, when locked, the upper region OTP can not be read out from SAFMEM. | RWS |
| | | • Bits 31:11 Reserved, must be kept at reset value.<br>• Bit 10 DBGSWENABLE: Control self-hosted debug enable with signal dbgswenable<br>• 0: memory-mapped accesses to all ETM registers are disabled and return error<br>• 1: no effect on external debugger accesses<br>• Bit 9 CFGDISABLE: Write access to secure GIC registers disable with signal: cfgsdisable<br>• 0: no effect, all GIC registers can be accessed<br>• 1: Disable write access to some Secure GIC registers | |

| Word | Field name | Description | RWS |
|---|---|---|---|
| 5 | Debug conf | • Bit 8:7 CP15SDISABLE[1:0]: Write access to some secure Cortex-A7 CP15 registers is disabled<br>  • CPDISABLE[0] applies to CPU0.<br>  • CPDISABLE[1] applies to CPU1<br>  • 0: All CP15 registers can be accessed<br>  • 1: Disable write access to some secure CP15 registers into Cortex-A7 corresponding CPU<br>• Bit 6 SPNIDEN: Secure privilege non-invasive debug enable with signal spiden<br>  • 0: Secure privilege non-invasive debug disabled<br>  • 1: Secure privilege non-invasive debug enabled<br>• Bit 5 SPIDEN: Secure privilege invasive debug enable with signal spniden<br>  • 0: Secure privilege invasive debug disabled<br>  • 1: Secure privilege invasive debug enabled<br>• Bit 4 HDPEN: Hardware debug port enable with signal hdpen<br>  • 0: Hardware debug port disabled<br>  • 1: Hardware debug port enabled<br>• Bit 3 DEVICEEN: Controls the access to debug component via external debug port by signal deviceen<br>  • 0: Disabled<br>  • 1: Enabled<br>• Bit 2 NIDEN: Non-invasive debug enable with signal niden<br>  • 0: Non-invasive debug disabled<br>  • 1: Non-invasive debug enabled<br>• Bit 1 DBGEN: Debug enable with signal dbgen<br>  • 0: Disabled<br>  • 1: Enabled<br>• Bit 0 DFTEN: DFT enable with signal dften<br>  • 0: DFT disabled<br>  • 1: DFT enabled | RW |
| 6 | Reserved | | |
| 7 | Reserved | | |
| 8 | Disturbed status 1 | • Bit 31 : OTP 31 status<br>• ...<br>• Bit 0 : OTP 0 status | R |
| 9 | Disturbed status 2 | • Bit 31 : OTP 63 status<br>• ...<br>• Bit 0 : OTP 32 status | R |
| 10 | Disturbed status 3 | • Bit 31 : OTP 95 status<br>• ...<br>• Bit 0 : OTP 64 status | R |
| 11 | Reserved | | |

| Word | Field name | Description | RWS |
|---|---|---|---|
| 12 | Reserved | | |
| 13 | Reserved | | |
| 14 | Error status 1 | • Bit 31 : OTP 31 status<br>• ...<br>• Bit 0 : OTP 0 status | R |
| 15 | Error status 2 | • Bit 31 : OTP 63 status<br>• ...<br>• Bit 0 : OTP 32 status | R |
| 16 | Error status 3 | • Bit 31 : OTP 95 status<br>• ...<br>• Bit 0 : OTP 64 status | R |
| 17 | Reserved | | |
| 18 | Reserved | | |
| 19 | Reserved | | |
| 20 | Permanent lock 1 | • Bit 31 : OTP 31 permanent lock<br>• ...<br>• Bit 0 : OTP 0 permanent lock | RWS |
| 21 | Permanent lock 2 | • Bit 31 : OTP 63 permanent lock<br>• ...<br>• Bit 0 : OTP 32 permanent lock | RWS |
| 22 | Permanent lock 3 | • Bit 31 : OTP 95 Permanent lock<br>• ...<br>• Bit 0 : OTP 64 permanent lock | RWS |
| 23 | Reserved | | |
| 24 | Reserved | | |
| 25 | Reserved | | |
| 26 | Programming lock 1 | • Bit 31 : OTP 31 programming lock<br>• ...<br>• Bit 0 : OTP 0 programming lock | RWS |
| 27 | Programming lock 2 | • Bit 31 : OTP 63 programming lock<br>• ...<br>• Bit 0 : OTP 32 programming lock | RWS |
| 28 | Programming lock 3 | • Bit 31 : OTP 95 programming lock<br>• ...<br>• Bit 0 : OTP 64 programming lock | RWS |
| 29 | Reserved | | |

| Word | Field name | Description | RWS |
|---|---|---|---|
| 30 | Reserved | | |
| 31 | Reserved | | |
| 32 | Shadow write lock 1 | • Bit 31 : OTP 31 shadow write lock<br>• ...<br>• Bit 0 : OTP 0 shadow write lock | RWS |
| 33 | Shadow write lock 2 | • Bit 31 : OTP 63 shadow write lock<br>• ...<br>• Bit 0 : OTP 32 shadow write lock | RWS |
| 34 | Shadow write lock 3 | • Bit 31 : OTP 95 shadow write lock<br>• ...<br>• Bit 0 : OTP 64 shadow write lock | RWS |
| 35 | Reserved | | |
| 36 | Reserved | | |
| 37 | Reserved | | |
| 38 | Shadow read lock 1 | • Bit 31 : OTP 31 shadow read lock<br>• ...<br>• Bit 0 : OTP 0 shadow read lock | RWS |
| 39 | Shadow read lock 2 | • Bit 31 : OTP 63 shadow read lock<br>• ...<br>• Bit 0 : OTP 32 shadow read lock | RWS |
| 40 | Shadow read lock 3 | • Bit 31 : OTP 95 shadow read lock<br>• ...<br>• Bit 0 : OTP 64 shadow read lock | RWS |
| 41 | Reserved | | |
| 42 | Reserved | | |
| 43 | Reserved | | |
| 44 | OTP 0 | Value of OTP 0 | RW |
| 45 | OTP 1 | Value of OTP 1 | RW |
| ... | OTP ... | Value of OTP ... | RW |
| 139 | OTP95 | Value of OTP 95 | RW |
| 140 | Reserved | | |
| ... | Reserved | | |
| 251 | Reserved | | |
| | | • Bit 7:4 ECC_USE[3:0]:<br>  • 0x0: No | |

| Word | Field name | Description | RWS |
|---|---|---|---|
| 252 | Configuration register | • 0x1: SAFMEM use ECC for upper OTP bits<br>• others: Reserved<br>• Bit 3:0 SAFMEM_SIZE[3:0]:<br>• 0x2: 2 Kbytes<br>• 0x4: 4 Kbytes<br>• 0x8: 8 Kbytes<br>• others: Reserved | R |
| 253 | IP version | • Bit 7:4 MAJREV[3:0]: IP version major revision information<br>• Bit 3:0 MINREV[3:0]: IP version minor revision information | R |
| 254 | IP ID | | R |
| 255 | IP_Magic_ID | | R |

# 2 Reference list

- https://en.wikipedia.org/wiki/USB#Device_Firmware_Upgrade

One Time Programmed

Device Firmware Upgrade

Das U-Boot -- the Universal Boot Loader (see U-Boot_overview)

Boot and Security and OTP control

Embedded Trace Macrocell

Generic Interrupt Controller

Cortex®

Central processing unit

Techniques implemented during semiconductor development to improve device testability (Scan, BIST…).

Elliptic curve cryptography

Error Correction Capability