TC375 usermanual 번역

Infineon-AURIX_TC3xx_Part1-UserManual-v02_00-EN.pdf

SOTA

Overview

TC33x와 TC33xED를 제외한 모든 TC3xx 장치는 PFLASH를 A와 B의 두 그룹의 은행으로 분할할 수 있는 기능을 제공하여 소프트웨어 업데이트 Over The Air(SOTA)를 수신할 수 있습니다. SOTA가 활성화되면 이러한 그룹 중 하나의 은행에서 읽고 실행할 수 있으며, 다른 그룹은 새로운 코드를 작성할 수 있습니다. 따라서 단일 물리적 PFLASH 은행 내에서 동시 읽기 및 쓰기(RWW) 기능이 지원되지 않지만, SOTA는 사용되지 않는 은행 그룹에 대해 안전하고 안전하게 쓰기 및 지우기 작업을 수행할 수 있는 기능을 제공함으로써 지원됩니다.

Functional Description

SOTA가 활성화되면 PFLASH 뱅크 그룹은 CPU 실행 주소 공간('활성' 뱅크로 정의됨)에 매핑되고, 다른 그룹은 읽기 및 쓰기가 가능한 주소 집합('비활성' 뱅크로 정의됨)에 매핑됩니다. SOTA 업데이트가 완료되고 뱅크가 교체되면 주소 매핑만 변경됩니다. 즉, 데이터를 복사할 필요가 없으며 실행 중인 주소 범위는 항상 동일합니다. PFLASH 뱅크의 물리적 주소는 주소 맵 장의 표준 주소 맵에 설명된 대로입니다. 표준 주소 맵에서 SOTA 주소 맵 전환이 수행되면 읽기/코드 실행을 위한 PFLASH 뱅크 매핑이 주소 맵 장의 대체 주소 맵에 설명됩니다. 이 장에서는 표준 주소 맵에서 활성화된 뱅크 그룹을 'A'라고 하고 대체 주소 맵에서 활성화된 뱅크 그룹을 'B'라고 합니다.

모든 NVM 작업은 PFLASH의 물리적 시스템 주소를 사용하여 DMU를 통해 수행되며, 즉 NVM 작업은 스왑 설정에 관계없이 항상 표준 주소 맵을 사용합니다. 'NVM 작업'은 FLASH를 대상으로 하는 프로그램, 지우기 등 모든 명령 시퀀스에 사용되는 용어이며 읽기는 포함되지 않습니다.
SOTA 주소 맵 스위칭 및 관련 기능을 제어하는 매개변수는 UCB에서 미리 구성되며, 하드웨어 구성은 후속 시스템 리셋 중에만 칩 내 시스템 펌웨어를 통해 업데이트됩니다.
이렇게 하면 애플리케이션 실행 중 의도치 않은 변경을 방지할 수 있습니다. 일부 제품 변형에서는 1MB 블록이 3MB 블록으로 교체됩니다. 코드 이미지는 그룹 A 또는 B 중 하나에 들어갈 수 있어야 하므로 3MB 블록의 상단 2MB는 프로그램 코드에 사용할 수 없습니다.

Performance considerations

로컬 프로그램 플래시 뱅크에 대한 CPU 액세스는 최대 성능을 위해 최적화됩니다. 따라서 서로 다른 물리적 PFLASH 뱅크에서 실행될 때 성능 변화가 발생할 수 있습니다. 이를 완화하기 위해 SOTA가 활성화되면 로컬 PFLASH로 가는 CPU 빠른 경로를 비활성화해야 합니다. 이렇게 하면 성능이 다소 저하되지만, 두 뱅크 그룹에서 실행할 때는 동일한 시스템 성능을 보장할 수 있습니다.
또 다른 주목할 점은 prefetch 액세스입니다. 각 그룹 간의 정확한 성능 패리티가 필요하다면 prefetch 액세스를 완전히 비활성화해야 합니다. 그러나 대략적인 패리티만 필요하다면, 네 개의 사용자 할당 가능한 prefetch 버퍼 중 하나를 각 non-local CPU에 할당해야 합니다(첫 번째 prefetch 버퍼는 로컬 CPU에 영구적으로 할당됩니다)

Configuring for SOTA

Table 21 Configuration Parameters related to SOTA

Parameter	Overview Description	Copied into register (by SSW during start-up)	See Chapter
SOTA Mode Enable (UCB_OTP.PROCONTP.SWAPEN)	유효하고 활성화된 경우 다음 후에 SOTA 모드가 시작됩니다 시스템 재설정. 유효하고 활성화된 경우 PROCONHSMCXx 및 활성 은행을 위해 구성된 PROCONHSMC OTP 설정은 다음 시스템 재설정 후 비활성 은행에도 적용됩니다.	DMU_HF_PROCONTP.SWAPEN SOTA bank 스왑을 활성화합니다. 두 bank 그룹 모두 PROCONHSMCx/PROCONHSMCO TPx 에 프로그래밍된 것과 동일한 HSM 섹터 보호 기능을 보장합니다(HSM이 있는 경우)	DMU
Bank Swap (UCB_SWAP_ORIG,	사용자 프로그래밍 가능한 활성 주소 맵은 표준 또는 대체 주소 맵입니	SCU_SWAPCTRL	SCU

UCB_SWAP_COPY)	다. SOTA 모드가 유효하고 활성화되어 있고 스왑 정보가 있는 경우 UCB_SWAP에서 구성된 것은 유효하며, 다음 시스템 재설정 후에도 유효합니다 주소 맵은 표준 또는 대체 주소 맵에 따라 설정됩니다.		
CPUx Fast Path Disable (UCB_OTP_PROCONTP.CPUxDDIS)	다음 시스템 리셋 후 로컬 프로그램 플래시 뱅크에 대한 CPU 직접 액세스를 비활성화합니다. 대신 SRI를 통해 라우팅된 로컬 프로그램 플래시에 대한 액세스를 비활성화합니다.	DMU_HF_PROCONTP.DDISx CPUx_FLASHCON4.DDIS	DMU, CPU

Initial device configuration for SOTA
(A/B 가능하게 초기 설정만 해주는듯)

다음은 SOTA가 활성화된 장치의 초기 장치 구성을 설치하기 위한 권장 사항입니다.
전달 상태부터 초기 실행 이미지는 활성 뱅크의 프로그램 플래시 뱅크에 프로그래밍됩니다. 그런 다음 사용되는 섹터는 UCB_PFLASH에 섹터별 쓰기 보호를 설치하여 보호하는 것이 좋습니다(이와 이후의 모든 UCB 프로그래밍에 대해서는 표준 ORIG 및 COPY 프로그래밍 시퀀스가 적용됩니다). 자세한 내용은 DMU 챕터의 '보안' 섹션에서 확인할 수 있습니다).
초기 이미지의 시작 주소는 UCB_BMHD로 프로그래밍되며, 부팅 모드 헤더 UCB의 표준 프로그래밍이 수행됩니다.

표준 주소 맵(그룹 A에서 실행, 그룹 B로 쓰기)을 선택하려면 00000055_H를 UCB_SWAP의 MARKERL0.SWAP 필드에 프로그래밍해야 합니다.

그런 다음 MARKERL0.SWAP의 시스템 주소를 MARKERH0.ADDR에,
CONFIRMATIONL0.CODE의 시스템 주소를 CONFIRMATIONH0.ADDR에,
확인 코드 $57B5327F_H$를 CONFIRMATIONL0.CODE에 기록하여 이를 확인해야 합니다.
이러한 UCB_SWAP 필드에 대한 자세한 내용은 NVM 하위 시스템 챕터에 위치한 UCB 챕터에서 확인할 수 있습니다.

UCB_OTP는 필요한 OTP, WOP 및 튜닝 보호를 설정하는 데 필요한 값으로 프로그래밍됩니다. OTP 또는 WOP 보호 섹터는 새 이미지로 다시 프로그래밍할 수 없습니다.
HSM이 필요한 경우, 초기 이미지를 HSM 프로그램 코드와 함께 로드해야 하며, 이 코드는 그룹 A와 그룹 B의 첫 번째 PFLASH 모듈의 PFLASH 논리 섹터 S0에서 S39에 포함되어야 합니다. 고객 HSM 구성은 UCB_HSMCOTP와 UCB_HSM에 로드되어야 합니다. OTP로 보호된 HSM 섹터는 새 이미지로 다시 프로그래밍할 수 없습니다.
마지막으로, SWAPEN은 UCB_OTP에서 활성화되도록 설정되어 있어 다음 시스템 리셋 시 SOTA 모드를 활성화합니다.

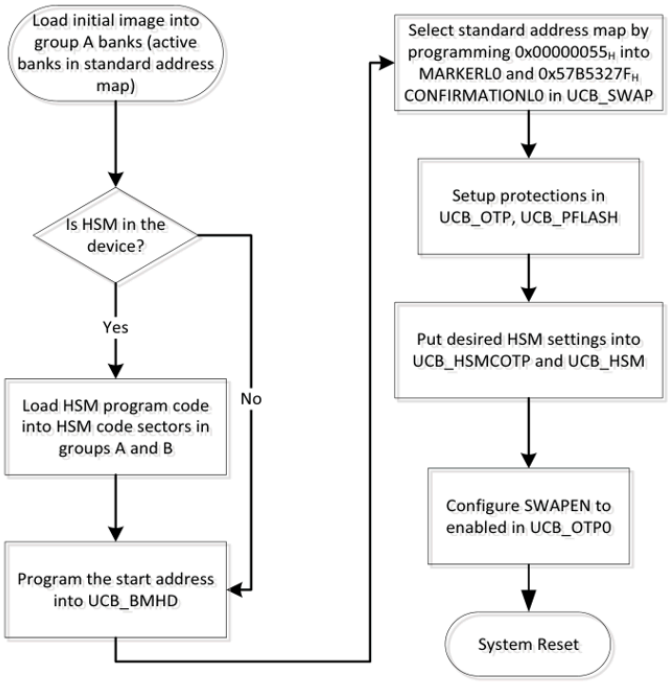


Figure 14 Initial SWAP configuration

Runtime SWAP configuration

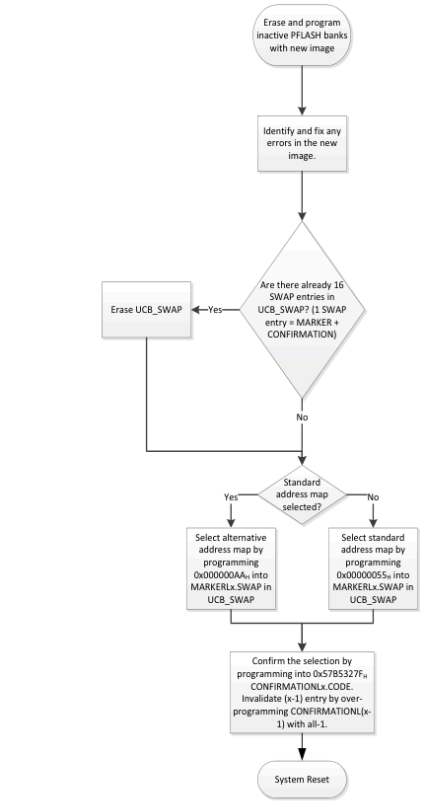
다음은 애플리케이션을 실행하는 동안 새 이미지를 설치하고 장치를 새 이미지로 전환하도록 구성하기 위한 권장 사항입니다.

새 이미지로 전환하려면 먼저 새 프로그램 이미지를 비활성 PFLASH 뱅크 그룹에 로드해야 합니다.
이를 위해서는 해당 뱅크에 대해 첫 번째 섹터별 쓰기 보호를 비활성화해야 합니다(DMU에서 '보호 비활성화' 명령 시퀀스에 대한 UCB_PFLASH 비밀번호를 제시함으로써).
PFLASH와 DFLASH에 대한 동시 NVM 작업(예: 프로그램 또는 지우기)이 지원되지 않으므로, PFLASH 작업이 발생하지 않을 때를 위해 PFLASH 작업을 예약하거나 진행 중인 DFLASH 작업을 일시 중지해야 PFLASH 작업이 발생할 수 있습니다.
따라서 애플리케이션에서 실행 중인 EEPROM 드라이버와 업데이트를 수행하는 보안 플래시 부트로더 간에 동기화가 필요합니다.
새로 작성된 이미지는 쓰기 보호 기능이 다시 활성화되기 전에 오류를 식별하고 수정해야 합니다.
SOTA가 PFLASH를 재프로그래밍/소거하는 동안 심각한 장애가 발생한 경우, 논리 섹터 교체 기능을 사용할 수 있습니다(자세한 내용은 DMU 장을 참조하십시오).
이 기능을 사용하면 '논리 섹터 교체' 명령 시퀀스를 사용하여 장애가 발생한 논리 섹터를 중복 섹터로 매핑할 수 있습니다.

다음 단계는 UCB_SWAP에서 SWAP 정보를 구성하는 것입니다.
UCB_SWAP 비밀번호가 제시된 후,
그룹 B에 새 이미지가 포함된 경우 MARKERLx.SWAP는 $0000AA_H$로 변경되며,
그룹 A에 새 이미지가 포함된 경우 00000055_H로 변경됩니다.
그런 다음 MARKERHx.ADDR, CONFIRMATIONHx.ADDR 및 CONFIRMATIONLx.CODE는 초기 설정과 동일하게 프로그래밍됩니다.
이전 (x-1) UCB_SWAP 항목은 all-1을 CONFIRMATIONL(x-1)로 오버-프로그래밍하여 무효화됩니다.
이 모든 항목에 대해 'x'는 초기 구성 후 처음으로 이미지가 교체될 때마다 한 번씩 증가해야 합니다.

UCB_SWAP가 가득 차면(즉, 'x'가 15에 도달함), 전체 UCB가 지워지고 새 항목이 추가되기 전에 'x'가 0으로 다시 설정될 수 있습니다. 그런 다음 'Resume Protection' DMU 명령 시퀀스를 사용하여 쓰기 보호가 다시 설치됩니다.
SWAP 정보의 마지막 유효한 항목(즉, 'x'의 최대값으로 저장된 SWAP 정보)은 시스템에서 SOTA를 구성하기 위해 스타트업 소프트웨어에 의해 사용된다는 점에 유의하세요.
따라서 삭제가 필요하기 전에 UCB_SWAP에서 16개의 스왑을 구성할 수 있습니다.
장치의 수명 동안 가능한 최대 스왑 수는 PFLASH 삭제/프로그램 주기(NE_P = 1000 사이클)의 데이터시트 매개변수에 따라 달라집니다.
1000개의 스왑 구성을 수행하려면 수명 동안 최소 124개의 UCB 삭제/프로그램 주기가 필요합니다(UCB_SWAP_ORIG와 UCB_SWAP_COPY 모두 삭제 및 업데이트가 필요하므로 16개의 스왑 업데이

트당 두 개의 UCB 삭제가 필요합니다).
이는 UCB 프로그램/erase 주기(tRTU)의 데이터시트 매개변수를 준수하기 위해 다른 UCB를 업데이트할 때 고려해야 합니다.
새 이미지 실행을 시작하려면 시스템 재설정을 트리거해야 합니다(애플리케이션 재설정은 아무런 영향을 미치지 않습니다).



Runtime SOTA configuration

Safety

SOTA가 비활성화되면 프로그램 플래시 전체가 safety_endinit으로 보호되므로 프로그램 플래시 내용에 의도치 않은 변경이 발생하지 않습니다. SOTA가 활성화되면 비활성 뱅크 그룹에 대한 safety_endinit 보호가 자동으로 제거되어 업데이트할 수 있습니다. 그러나 활성 뱅크의 경우에도 실행 전에 안전 애플리케이션 소프트웨어를 확인해야 하는 요구 사항은 남아 있습니다. safety_endinit 보호에 대한 자세한 내용은 NVM 하위 시스템 장의 '기능적 안전 기능' 섹션에서 확인할 수 있습니다.

Security

PFLASH에서 NVM 작업에 제공되는 보안 보호는 PFLASH 뱅크의 활성 또는 비활성 특성에 관계없이 DMU 챕터의 '보안' 섹션에 정의된 것과 동일합니다.

그러나 PFLASH에서 HSM 독점 섹터를 처리하기 위한 추가 조치가 시행되었습니다.
SOTA가 활성화되면 PROCONHSMCX 및 PROCONHSMCOTP 레지스터에 구성된 모든 보호가 A 그룹과 B 그룹의 PFLASH 논리 섹터 S0에서 S39로 미러링됩니다. 이는 은행 스왑을 통해 HSM 코드에 대한 무단 액세스를 방지하기 위한 것입니다. 사용자는 두 그룹 간에 보안 콘텐츠 이미지가 복제되었는지 확인해야 합니다. HSM 전용으로 표시된 재프로그래밍 섹터는 비활성 상태에서도 HSM 디버그가 활성화된 경우에만 HSM 또는 Cerberus에서 수행할 수 있습니다.

Memory Maps (MEMMAP)

Table 34 TC37x Alternate Address Map for SOTA of Segment 8 PFLASH

Segment	Address Range	Size	Description	Access Type	
				Read	Write
8	$8000\ 0000_H$ - $802F\ FFFF_H$	3 Mbyte	Program Flash 1 (PF1)	Access	SRIBE
	$8030\ 0000_H$ - $805F\ FFFF_H$	3 Mbyte	Program Flash 0 (PF0)	Access	SRIBE
	$8060\ 0000_H$ - $81FF\ FFFF_H$	-	Reserved	SRIBE	SRIBE

Table 35 TC37x Alternate Address Map for SOTA of Segment 10 PFLASH

Segment	Address Range	Size	Description	Access Type	
				Read	Write
10	$A000\ 0000_H$ - $A02F\ FFFF_H$	3 Mbyte	Program Flash 1 (PF1)	Access	SRIBE
	$A030\ 0000_H$ - $A05F\ FFFF_H$	3 Mbyte	Program Flash 0 (PF0)	Access	SRIBE
	$A060\ 0000_H$ - $A1FF\ FFFF_H$	-	Reserved	SRIBE	SRIBE

Table 36 TC37x Alternate Address Map for SOTA of Segment 10 Erase Counters and Registers

Segment	Address Range	Size	Description	Access Type	
				Read	Write
10	$A800\ 0000_H$ - $A800\ 3FFF_H$	16 Kbyte	Erase Counter 1 (EC1)	Access	SRIBE
	$A800\ 4000_H$ - $A807\ FFFF_H$	-	Reserved	SRIBE	SRIBE
	$A808\ 0000_H$ - $A80B\ FFFF_H$	256 Kbyte	PFI User Registers 1 (PFI1)	Access	SRIBE
	$A80C\ 0000_H$ - $A82F\ FFFF_H$	-	Reserved	SRIBE	SRIBE
	$A830\ 0000_H$ - $A830\ 3FFF_H$	16 Kbyte	Erase Counter 0 (EC0)	Access	SRIBE
	$A830\ 4000_H$ - $A837\ FFFF_H$	-	Reserved	SRIBE	SRIBE
	$A838\ 0000_H$ - $A83B\ FFFF_H$	256 Kbyte	PFI User Registers 0 (PFI0)	Access	SRIBE
	$A83C\ 0000_H$ - $AEFF\ FFFF_H$	-	Reserved	SRIBE	SRIBE

Platform Firmware

Firmware Flow

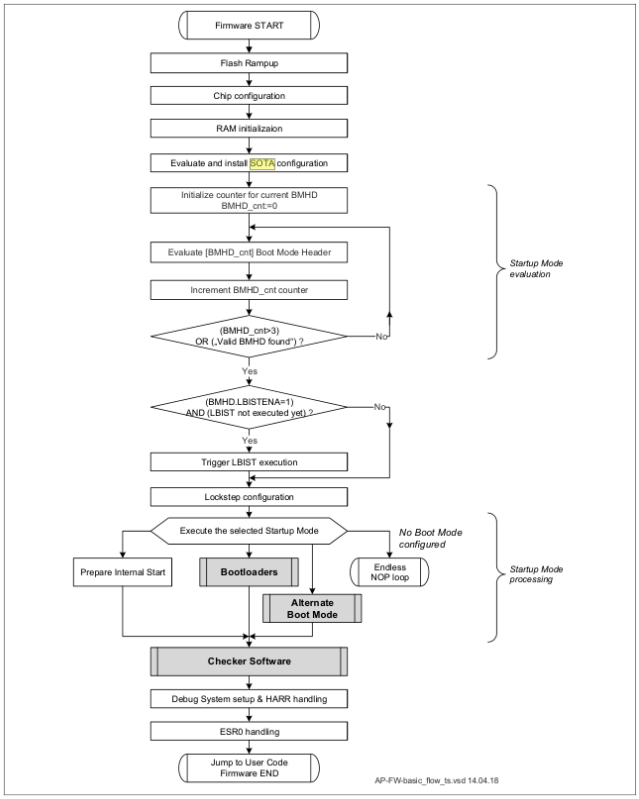


Figure 21 AURIX™ TC3xx Platform Firmware: main flow

Support for Software over the Air (SOTA)

전원을 켜고 시스템을 재설정한 후, AURIX™ TC3xx 플랫폼 SSW는 UCB_SWAP_ORIG/COPY에 설치된 SOTA 구성을 평가하고, 이에 따라 디바이스 PFLASH의 뱅크 간 전환을 가능하게 하는 SWAP 기능을 활성화합니다.
UCB_SWAP_ORIG/COPY에서 유효한 SOTA 구성이 발견되면 SSW는 다음을 실행합니다:

- 모든 CPUx_FLASHCON4.DDIS 비트에 1을 설치하여 PFLASH(직접 읽기 경로 CPUx-PFLx)에 대한 직접 액세스를 비활성화합니다.

- install into SRU_SWAPCTRL.ADDRCFG register:
  – Address region A active - if SWAP_A marker is found
  – Address region B active - if SWAP_B marker is found

Non Volatile Memory(NVM) System

Multiple PFLASH TP and HSM PCODE configuration

"소프트웨어 업데이트 오버 더 에어(SOTA)"를 지원하기 위해, 다른 PFLASH 은행은 PFLASH0 외에도 TP 또는 HSM PCode에 대해 섹터 S0에서 S39를 구성할 수 있습니다. 이 보조 PFLASH 은행 번호는 장치에 따라 다르며, MEMMAP 장에서 제공하는 대체 주소 맵에서 시스템 주소가 가장 낮은 PFLASH 은행입니다.
동일한 레지스터인 DMU_SP_PROCONHSMCX0-1과 DMU_SP_PROCONHSMCOTP0-1은 HSM PCode에 사용되는 이 보조 PFLASH의 섹터를 구성하는 데 사용됩니다. 보조 PFLASH 뱅크에서 HSM PCode에 사용되지 않는 섹터는 PF0와 유사한 TP에 사용할 수 있으며, 보조 PFLASH 뱅크의 DMU_HP_PROCONOTP/DMU_HP_PROCONOP 레지스터에서 섹터별 보호를 가능하게 하여 보호할 수 있습니다.

Safety Endinit protection

PFLASH 콘텐츠를 수정할 수 있는 모든 명령 시퀀스는 Safety Endinit에 의해 보호됩니다. Safety Endinit 보호를 제거하지 않고 PFLASH에 액세스하려는 경우 PROER가 생성됩니다.
"소프트웨어 오버 더 에어(SOTA)"를 지원하기 위해 DMU_HP_PROCONTP.SWAPEN이 "Enabled"되어 있으면 DMU는 현재 실행 중인 애플리케이션에서 코드 실행에 사용되지 않는 비활성 PFLASH, 즉 PFLASH에 대한 Safety Endinit protection를 제거합니다. DMU는 SCU_SWAPCTRL 비트를 사용하여 시스템이 표준 주소 맵에 있는지 또는 대체 주소 맵에 있는지 확인하고, 이를 통해 '활성' 및 '비활성' PFLASH 뱅크를 도출합니다. 대체 주소 맵은 MEMMAP 장에서 설명합니다. 표준 또는 대체 주소 맵 모드의 '활성' 뱅크는 AURIXTC39x 및 AURIXTC38x 파생 모델의 물리적 주소(표준 주소 맵에 설명된 대로)를 가진 PFLASH 뱅크입니다. 나머지 뱅크는 '비활성' 뱅크입니다. 다른 파생 모델의 경우 '활성' 뱅크는 물리적 주소를 가진 PFLASH0 뱅크입니다.
SCU_SWAPCTRL의 잘못된 값이 감지되면, DMU는 PFLASH 뱅크의 다음 프로그램/삭제가 요청될 때 SQER을 생성합니다.

UCB_SWAP_ORIG and UCB_SWAP_COPY

UCB_SWAP은 SSW에서 평가하여 실행 중인 애플리케이션(이 장에서는 'SWAP'이라고 함)에서 사용하는 PFlash를 결정합니다. 자세한 내용은 사용 설명서의 "소프트웨어 오버 더 에어(SOTA)" 섹션을 참조하세요.

UCB_OTPy_ORIG and UCB_OTPy_COPY (y = 0-7)

UCB_OTPy_ORIG와 UCB_OTPy_COPY는 일회성 프로그래밍 가능한 "OTP"와 한 번 "WOP" 보호 페이지 세트를 구성합니다. 각 OTP 및 WOP 구성 세트는 PFLASH 섹터에 OTP 및 WOP 보호를 점진

적으로 추가하는 것을 지원합니다. 또한 UCB_OTP에는 디바이스에서 튜닝 보호 및 SOTA(Software Update Over the Air)를 구성하는 데 사용되는 HF_PROCONTP 레지스터가 포함되어 있습니다.

6.8.2.12 UCB_SWAP_ORIG and UCB_SWAP_COPY

The UCB_SWAP (ORIG and COPY) contain the user defined SWAP configuration. It is protected with the password PW0 to PW7. The SWAP configuration is evaluated by the SSW (see “Software update Over The Air (SOTA) chapter).

6.8.3.2 UCB_SWAP_ORIG and UCB_SWAP_COPY

UCB_SWAP_ORIG_MARKERLx

Determines the system address map used by the current running application. For more details please refer to the "Software update Over The Air(SOTA)" chapter.

9.3.6.5 SOTA Address Map Control

Address Map Control Register

Provides the capability for firmware to install the currently used address map - to support SOTA