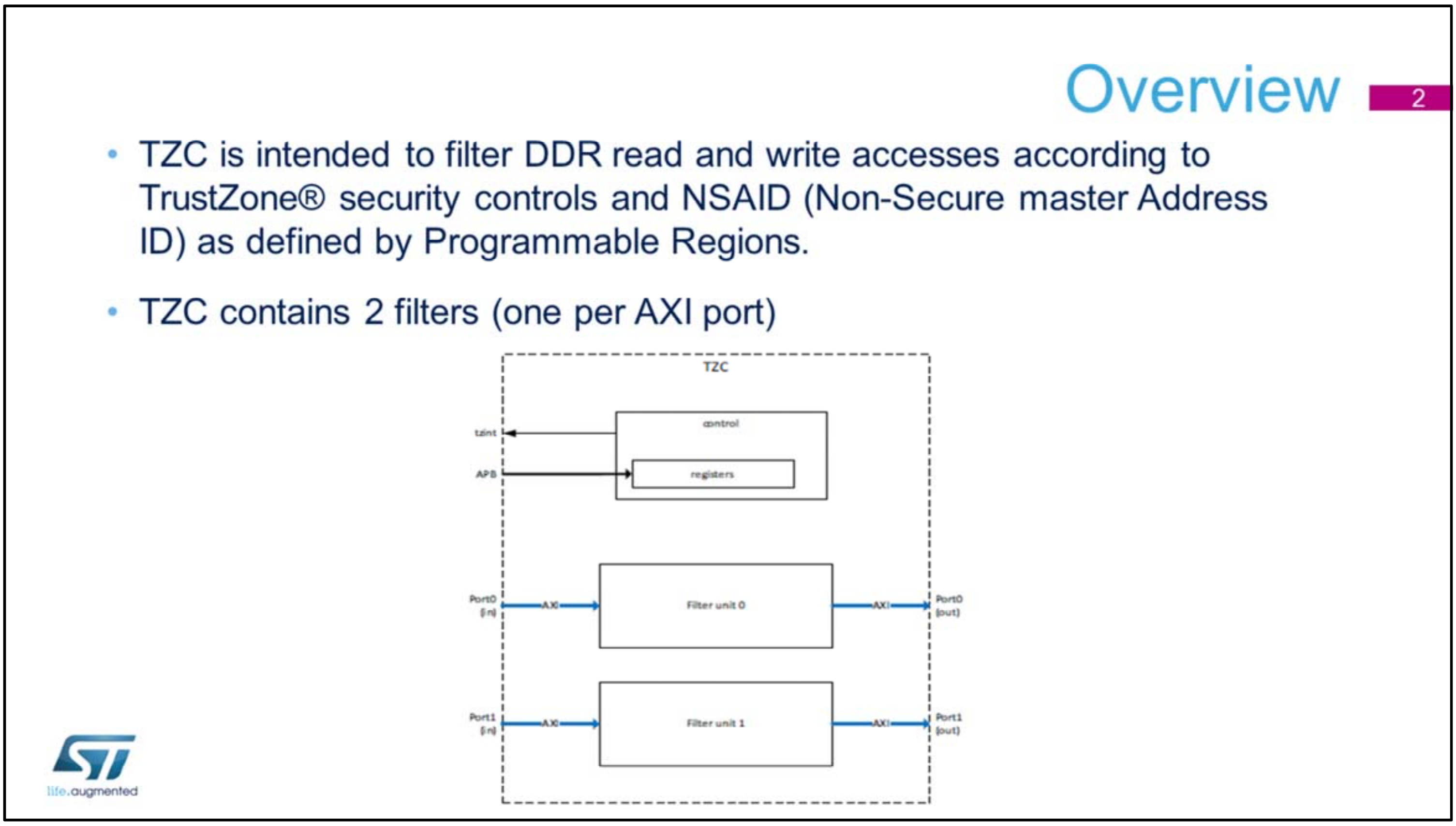
STM32MP1 - TZC

TrustZone Address Space Controller

Revision 1.0

life.augmented

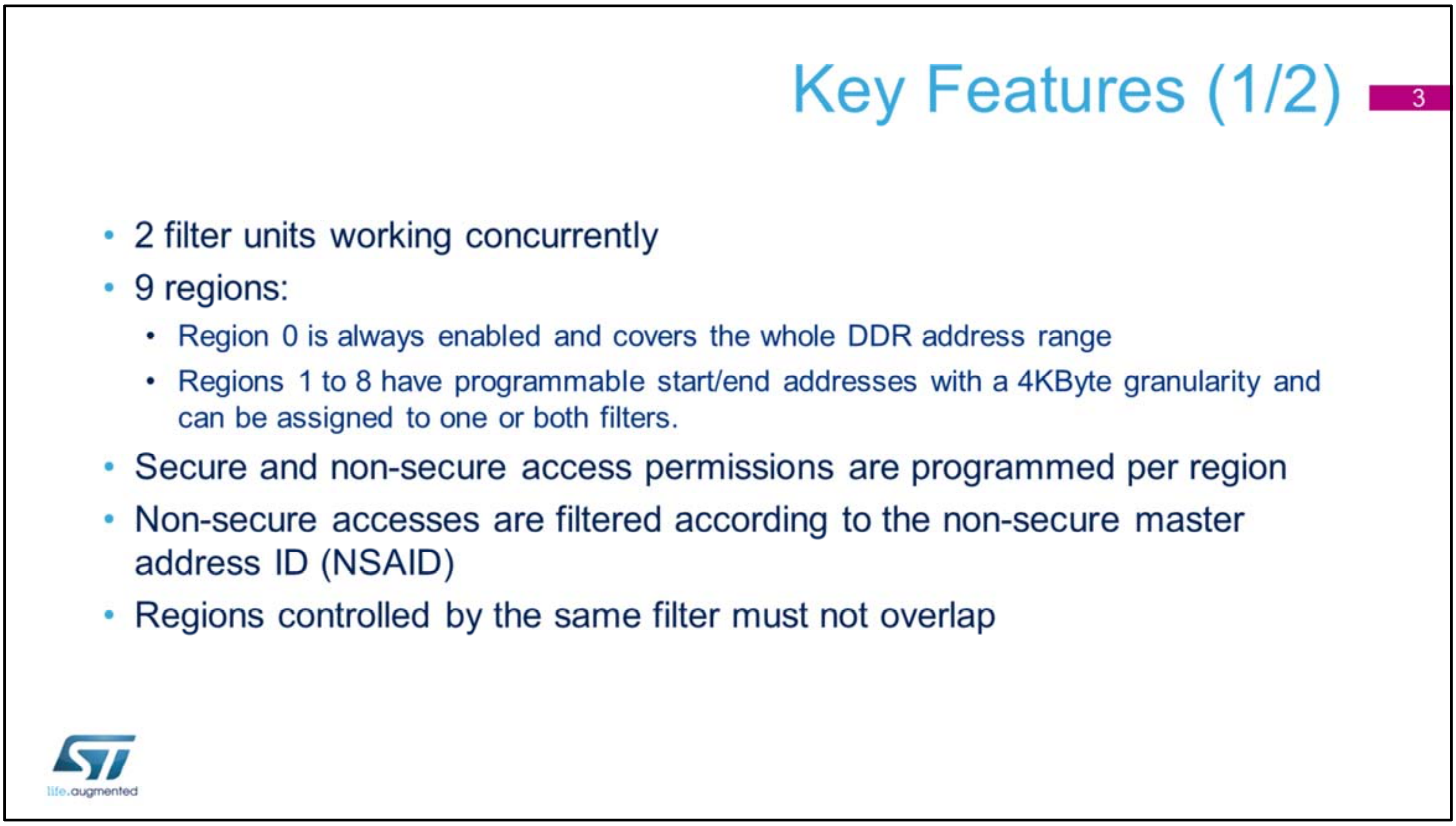
Hello, and welcome to this presentation of the STM32MP1 TrustZone Address Space Controller.



Overview

- TZC is intended to filter DDR read and write accesses according to TrustZone® security controls and NSAID (Non-Secure master Address ID) as defined by Programmable Regions.
- TZC contains 2 filters (one per AXI port)

The TrustZone® Address Space Controller (TZC) is intended to filter DDR accesses according to security rules and non-secure master address ID.
This is a simplified diagram of TZC.
TZC is composed of two filter units, one per AXI port. Filters are working concurrently.
The two filters are controlled by a common control register set via the APB interface.



Key Features (1/2)

3

- 2 filter units working concurrently
- 9 regions:
  - Region 0 is always enabled and covers the whole DDR address range
  - Regions 1 to 8 have programmable start/end addresses with a 4KByte granularity and can be assigned to one or both filters.
- Secure and non-secure access permissions are programmed per region
- Non-secure accesses are filtered according to the non-secure master address ID (NSAID)
- Regions controlled by the same filter must not overlap

TZC is composed of 2 filter units working concurrently on two AXI ports

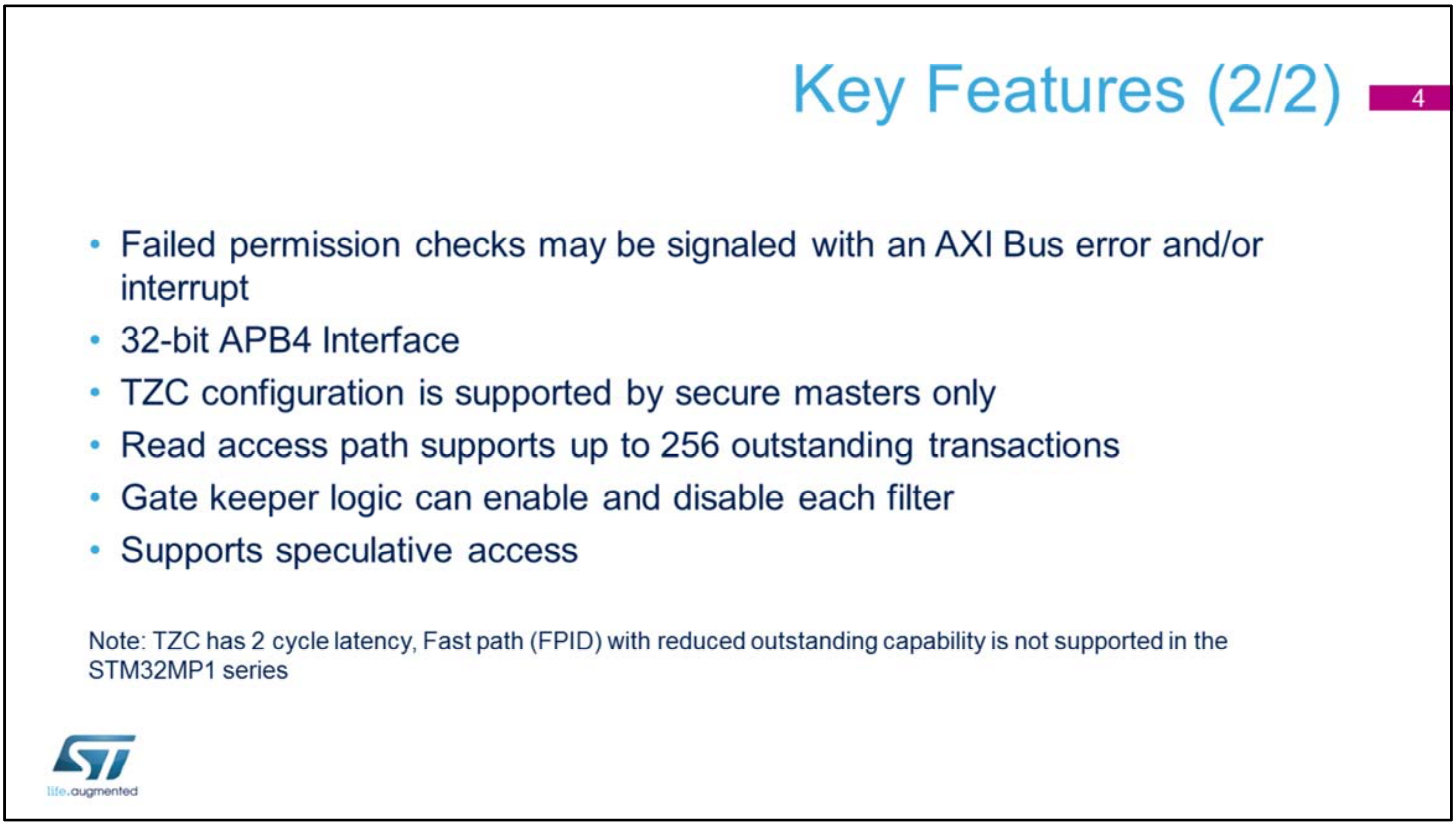
Access filtering can support up to 9 regions:

- Region 0 is always enabled and covers the whole DDR address range
- Regions 1 to 8 have programmable start and end addresses with a 4 KByte granularity. A region can be assigned to one or both filters.

Secure and non-secure access permissions are defined per region.

Non-secure accesses are filtered according to the non-secure master address ID.

Regions controlled by the same filter must not overlap.



Key Features (2/2)

4

- Failed permission checks may be signaled with an AXI Bus error and/or interrupt
- 32-bit APB4 Interface
- TZC configuration is supported by secure masters only
- Read access path supports up to 256 outstanding transactions
- Gate keeper logic can enable and disable each filter
- Supports speculative access

Note: TZC has 2 cycle latency, Fast path (FPID) with reduced outstanding capability is not supported in the STM32MP1 series

Failed permission checks can be signaled either with an AXI Bus error or with interrupt or both.

TZC is programmed via a 32-bit APB4 Interface.

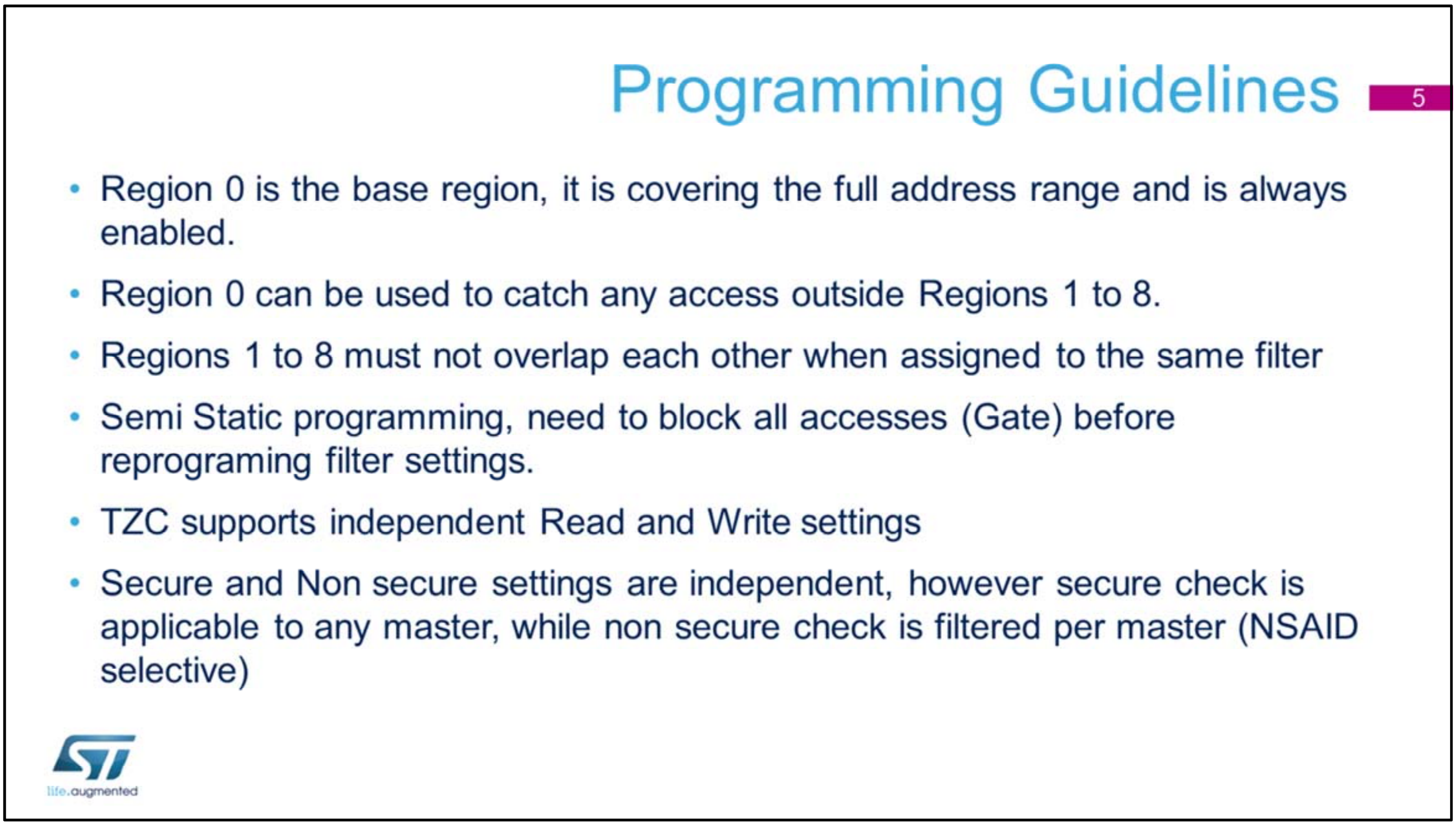
TZC configuration is supported by secure masters only.

Read access path supports up to 256 outstanding transactions to DDR.

Some Gate keeper logic is used to enable and disable each filter.

TZC can support speculative accesses.

Note: TZC has 2 cycle latency, Fast path (FPID) with reduced outstanding capability is not supported in the STM32MP1 series.



Programming Guidelines

5

- Region 0 is the base region, it is covering the full address range and is always enabled.
- Region 0 can be used to catch any access outside Regions 1 to 8.
- Regions 1 to 8 must not overlap each other when assigned to the same filter
- Semi Static programming, need to block all accesses (Gate) before reprograming filter settings.
- TZC supports independent Read and Write settings
- Secure and Non secure settings are independent, however secure check is applicable to any master, while non secure check is filtered per master (NSAID selective)

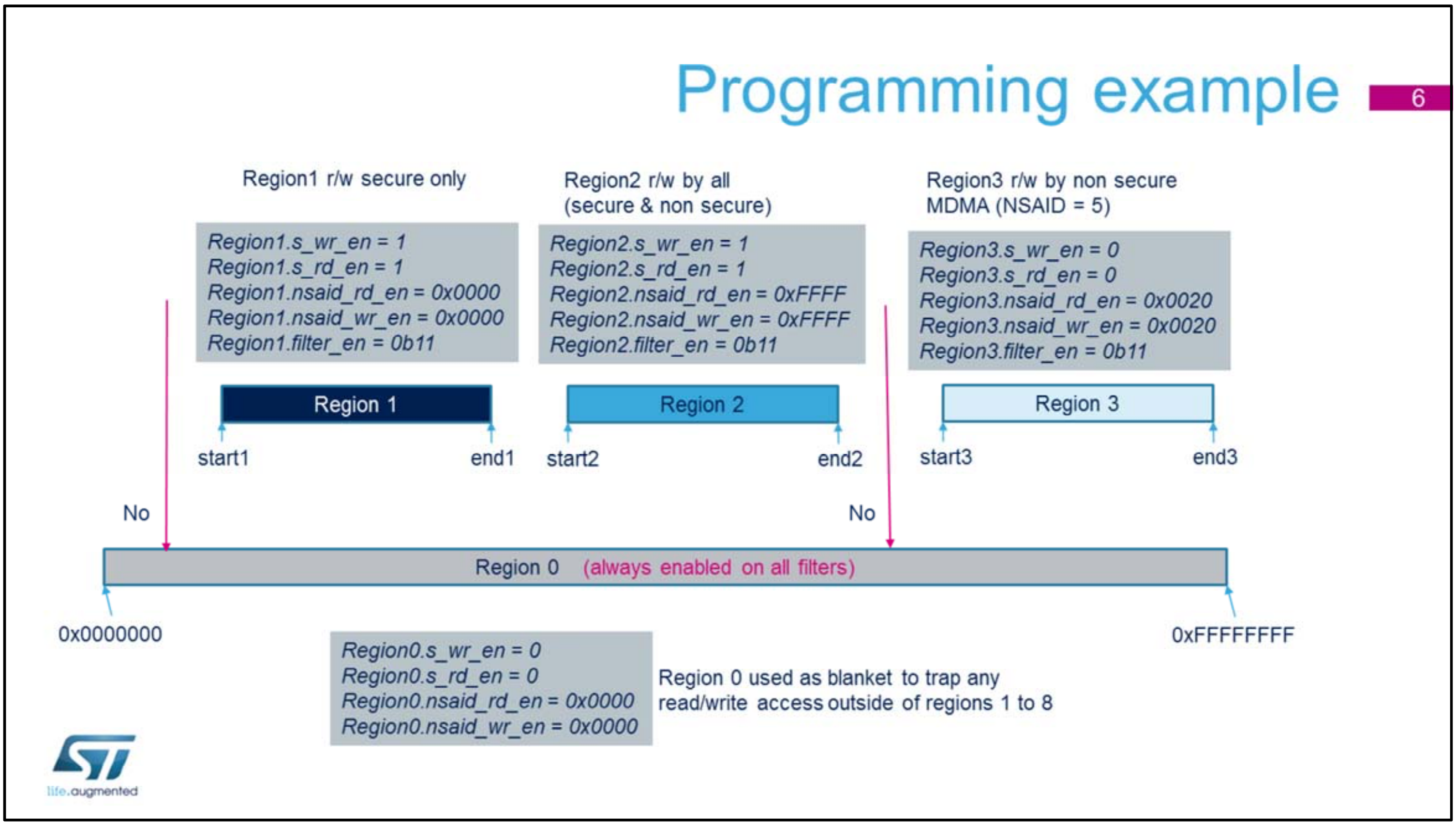
TZC programming should observe the following guidelines:

- Region 0 is the base region covering the full address range and is always enabled.
- Region 0 can be used to catch any access outside Regions 1 to 8.
- Regions 1 to 8 must not overlap each other when assigned to the same filter.
- In case of reconfiguration by Semi Static programming, all accesses (Gate) must be blocked before reprograming filter settings.

TZC access filtering is based on:

- Independent Read and Write settings (read-only, write only , read-write, no access)

- Secure and Non secure settings are independent, however secure check is applicable to any master, but non secure check is filtered per master (NSAID selective).



Programming example

6

Region1 r/w secure only

Region1.s_wr_en = 1
Region1.s_rd_en = 1
Region1.nsaid_rd_en = 0x0000
Region1.nsaid_wr_en = 0x0000
Region1.filter_en = 0b11

Region2 r/w by all
(secure & non secure)

Region2.s_wr_en = 1
Region2.s_rd_en = 1
Region2.nsaid_rd_en = 0xFFFF
Region2.nsaid_wr_en = 0xFFFF
Region2.filter_en = 0b11

Region3 r/w by non secure
MDMA (NSAID = 5)

Region3.s_wr_en = 0
Region3.s_rd_en = 0
Region3.nsaid_rd_en = 0x0020
Region3.nsaid_wr_en = 0x0020
Region3.filter_en = 0b11

Region0.s_wr_en = 0
Region0.s_rd_en = 0
Region0.nsaid_rd_en = 0x0000
Region0.nsaid_wr_en = 0x0000

Region 0 used as blanket to trap any read/write access outside of regions 1 to 8

life.augmented

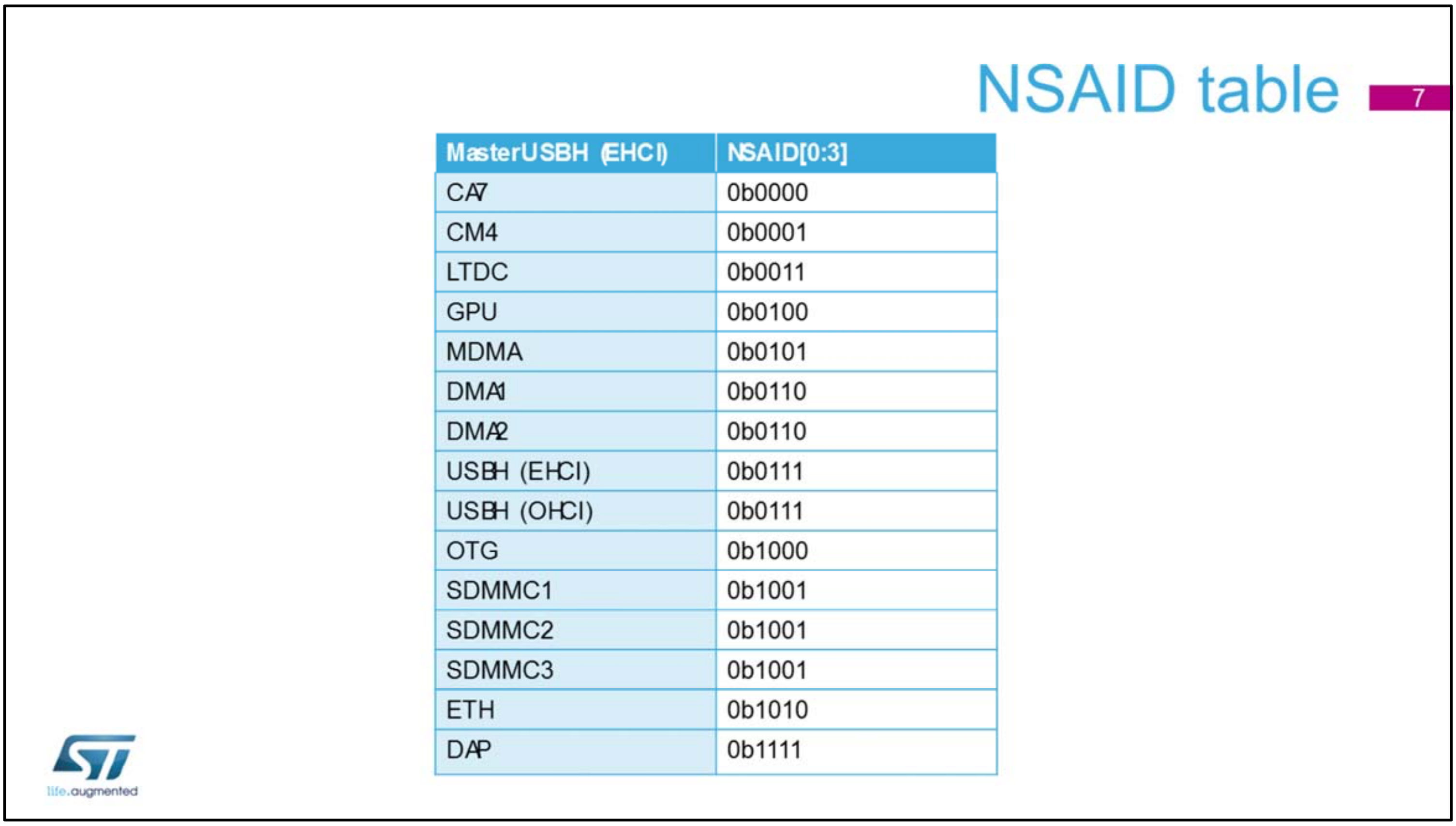
This slide shows a simple programming example.
The DDR space supports 3 non overlapping regions.

- Region 1 is defined between start1 and end1 addresses. Region 1 is read and write accessible only by secure applications.
- Region 2 is defined between start2 and end2 addresses. Region 2 is a shared region read and write accessible by secure and non-secure applications.
- Region 3 is defined between start3 and end3 addresses. Region 3 is read and write accessible only by the non-secure MDMA engine (with NSAID=5).

The register settings and programing sequence are for wr_en and rd_en parameters. NSAID are listed in the table next slide.

Region 0 is always enable and covers the full DDR address space, it is set as a blanket to trap any access outside of

these regions.
Hence no access is allowed outside of the 3 defined regions.



NSAID table

MasterUSBH (EHCI)	NSAID[0:3]
CA7	0b0000
CM4	0b0001
LTDC	0b0011
GPU	0b0100
MDMA	0b0101
DMA1	0b0110
DMA2	0b0110
USBH (EHCI)	0b0111
USBH (OHCI)	0b0111
OTG	0b1000
SDMMC1	0b1001
SDMMC2	0b1001
SDMMC3	0b1001
ETH	0b1010
DAP	0b1111

life.augmented

Non-secure master address ID (NSAID) is encoded on 4 bits according to Master as listed in this table.