FIRMWARE UPDATES FOR AUTOMOTIVE EDGE NODES

AMF-AUT-T2341

OSVALDO ROMERO
APPLICATIONS ENGINEER

STEVE MIHALIK
SENIOR FIELD APP ENGINEER

AGENDA

- FOTA Overview
- S32K Portfolio
- S32K Use cases
- Secure OTA in S32K144

Objective

- Overview of OTA and its challenges.
- Understand how NXP handles over the air updated in their portfolio.
- Understand how to handle over the air updates in low cost edge nodes MCUs such as S32K devices.

FW OVER THE AIR OVERVIEW

Today: 90% of Auto Innovation via electronics

NXP is #1

#1 INFOTAINMENT
TUNERS
SOFTWARE-DEFINED DIGITAL RADIO
MULTIMEDIA PROCESSORS
SOUND SYSTEM DSPs & AMPLIFIERS
NFC BT PAIRING
WIRELESS POWER CHARGING
POWER MANAGEMENT

ADAS & SECURITY

POWERTRAIN & CHASSIS
MICROCONTOLLERS
PRESSURE/ MOTION SENSORS
BATTERY MANAGEMENT
DRIVERS

STANDARD PRODUCTS
LOGIC
POWER
DISCRETES

#1 SECURE CAR ACCESS
IMMOBILIZER/ SECURITY
REMOTE KEYLESS ENTRY
PASSIVE KEYLESS ENTRY/ GO
BI-DIRECTIONAL KEYS
NFC
ULTRA WIDE BAND

#1 VEHICLE NETWORKING
CAN/LIN/ FLEXRAY
ETHERNET
CENTRAL GATEWAY CONTROLLER
SECURITY
RF

#1 BODY
MICROCONTROLLERS
POSITION/ ANGLE SENSORS
SYSTEM BASIS CHIPS

#1 SAFETY
MICROCONTROLLERS AIRBAG
ANALOG AIRBAG
MICROCONTROLLERS BRAKING
ANALOG BRAKING
SENSORS BRAKING
TIRE PRESSURE MONITORING

#1 Auto Analog/ RF | **#1 Auto MCU (ex JPN)** | **#1 Auto Merchant MEMS Sensors**

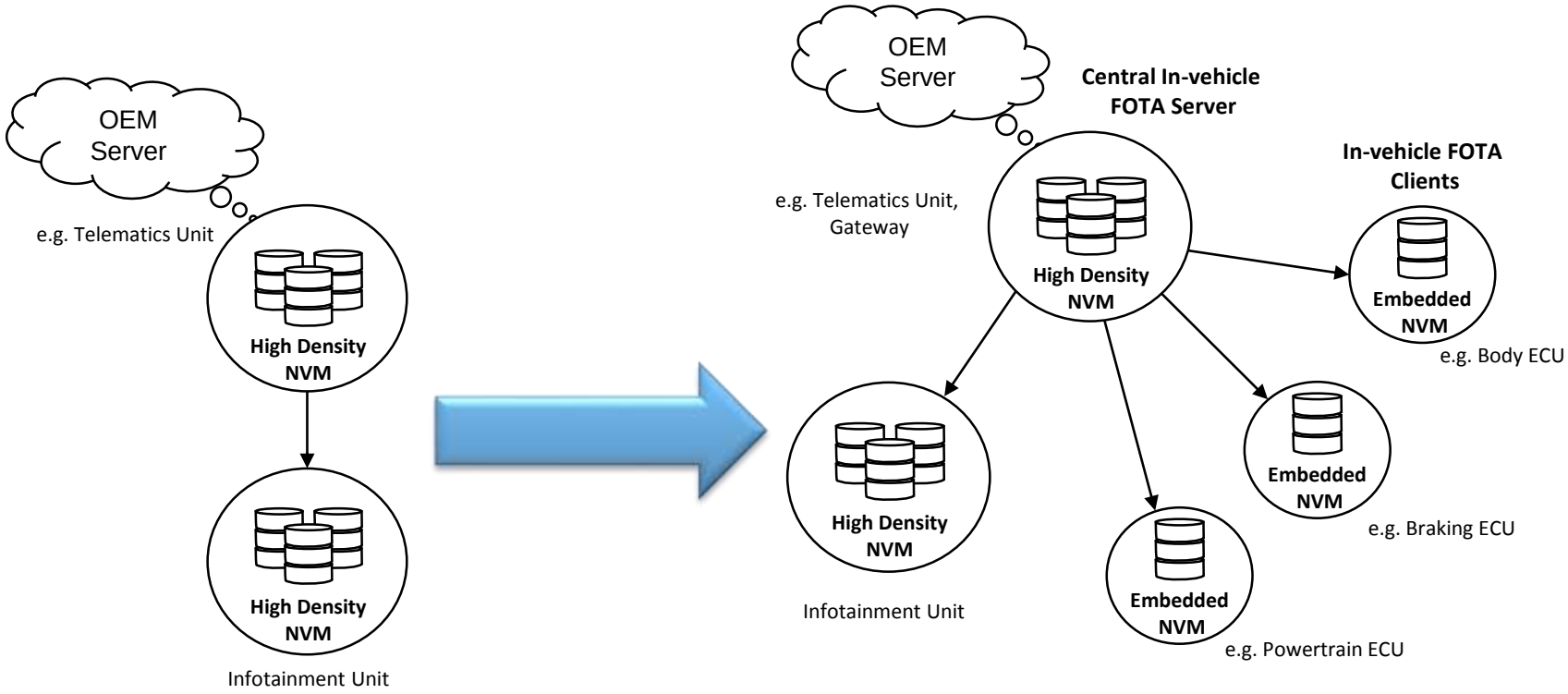
FOTA Overview: **Common Recall Process**

- Done at a dealer
- A special hardware tool is used
- Engine is not running
- The target node application is halted
- Main application erased and reprogrammed

FOTA Overview: **Motivations**

- Increasing number of recalls
- Dealer update $
- As firmware complexity increases, the probability of required firmware updates also increases
- User convenience vs going to dealer
- Safety can be improved with quicker updates

FOTA Overview: MOVING DEEPER INTO THE VEHICLE



FOTA Update of Infotainment & Telematics Systems

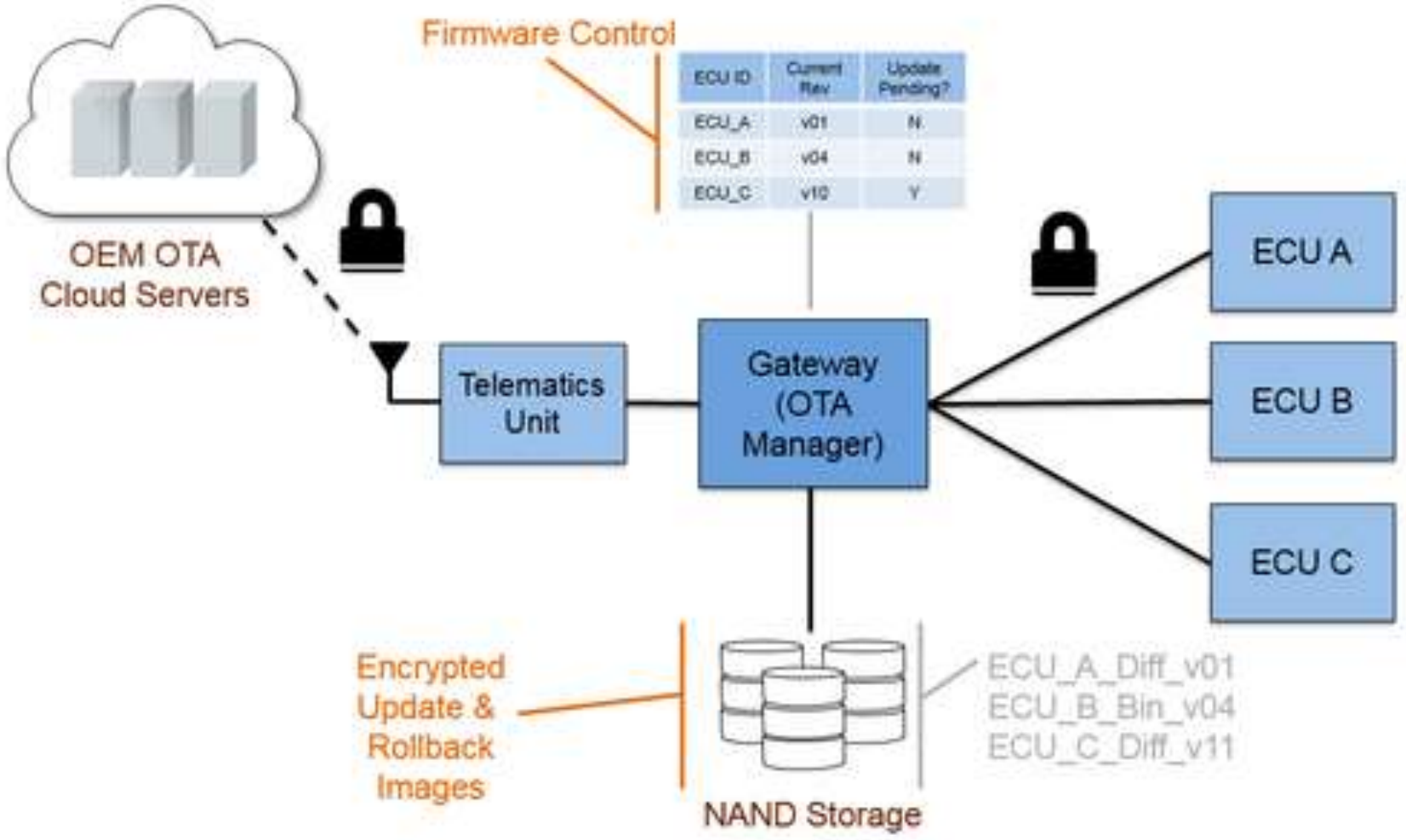
Focused on updates to software on the infotainment & telematics, but not propagating further into the vehicle architecture

FOTA Update of Major ECUs within the vehicle

New Challenges with this architecture:

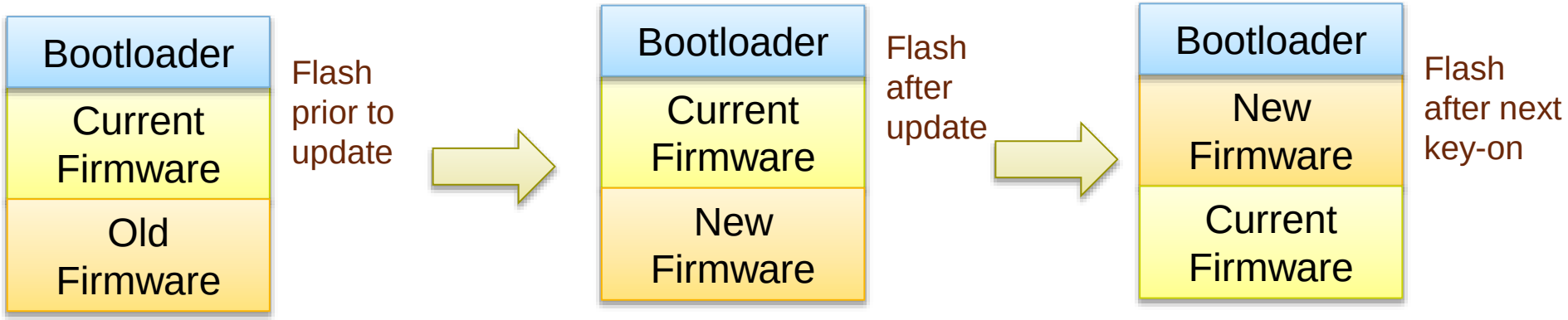
- Security throughout
- Cost sensitivity of embedded ECUs
- Embedded NVM vs High Density NVM
- Strategy of when & what to update

FOTA Overview: Moving Deeper in the Vehicle



FOTA Overview: A/B Swap Use Case

Reset vectors to bootloader, which is never erased



Advantages:

- Update can be carried out while current application is actively running from flash
- Always have original firmware to roll back to in case of issue
- Vehicle is always available – guaranteed no vehicle downtime regardless of update errors

Disadvantage:

- Requires ~2x flash application storage

FOTA Overview: In Place Use Case

Reset vectors to bootloader, which is never erased

Advantages:

- No need for additional flash

Disadvantage:

- Requires vehicle downtime during update process
- Not possible to instantly “roll-back” if an issue occurs

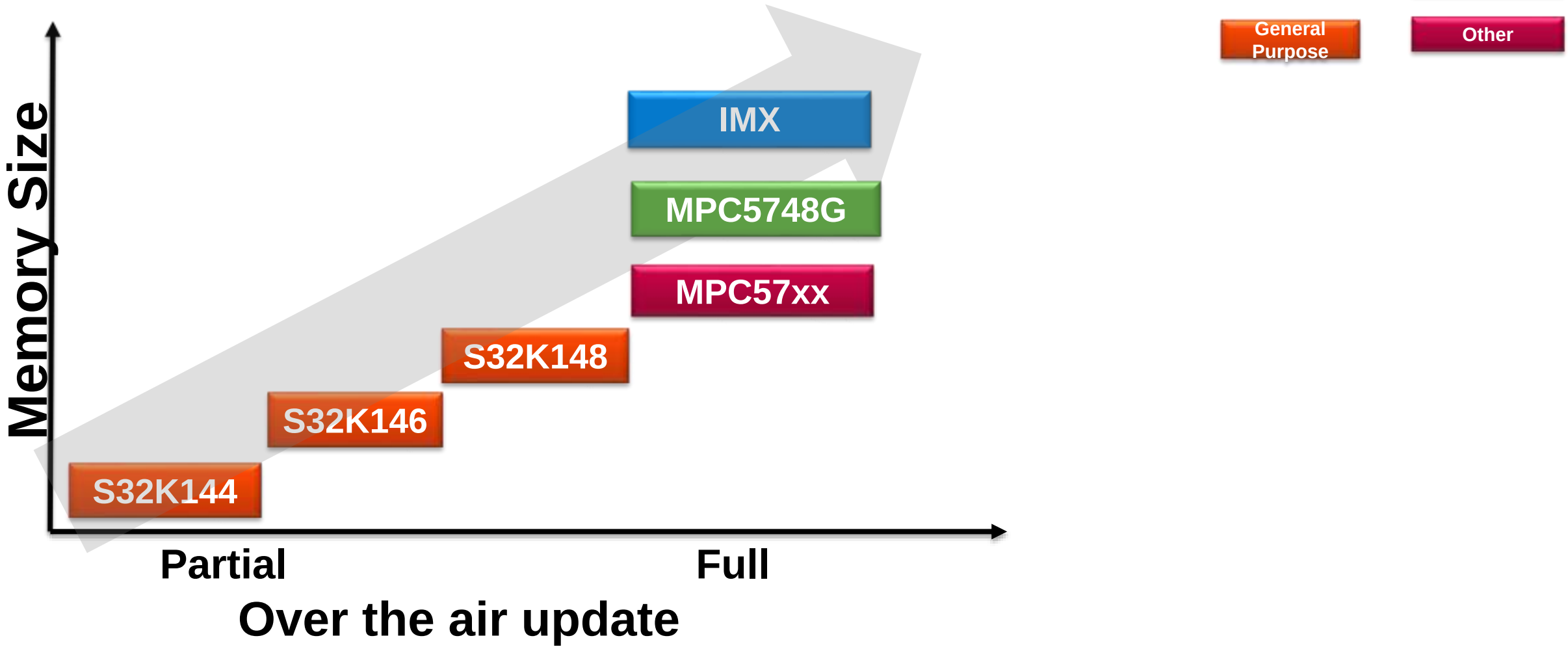
FOTA Overview: Assumptions

- End node:
  - gets partial or full image for flashing
  - will have at least enough spare erased flash for a full image
  - receives updated software over serial link
  - has boot block which never changes with OTA updates
- Best case: update is performed while running existing software
- Before new firmware becomes active, application/boot firmware can perform:
  - Security validation
  - Functional validation
- New firmware starts on reset following the update completion

FOTA Overview: Challenges AT CHIP

- Additional memory for AB swap
- Remapping
- Read while write
- Security

FOTA Overview: **Automotive FOTA MAP**



FOTA Overview: **FULL FOTA DEMO**

- This demo was designed to demonstrate firmware update capabilities common on many NXP devices. The demo platform uses two MPC5748G evaluation boards:
  - One will send update via CAN
  - Other receives update, programs into flash and makes it the default firmware for next boot

- Key features:
  - Flash remapping – map sections of flash to different addresses, providing a simple method to switch between firmware
  - Flash Read-While-Write (RWW) capability (Being able to erase and program a block of flash whilst simultaneously executing from another block)
  - Firmware Authentication (Confirming that the firmware is from a valid source and that it has not been tampered with during transmission)

S32K PORTFOLIO

S32K Portfolio: Targeting General Purpose Applications

Product Longevity


Body control module


Human machine interface

Wireless charging

Battery Management


Tire pressure receiver


Climate control


Door/Window/sunroof

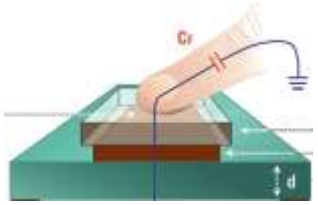
Near Field Communication


Lighting

Secure transmission / encryption in cars

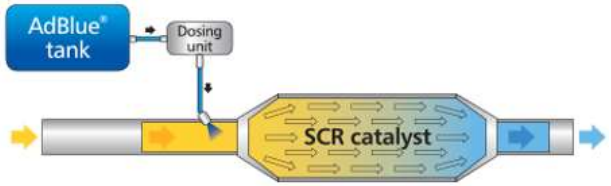

Chassis systems


PMSM/BLDC motorcontrol



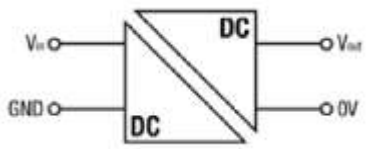
Touch sensing


Park assist



Nox reduction systems


Motorbike ECU/ABS



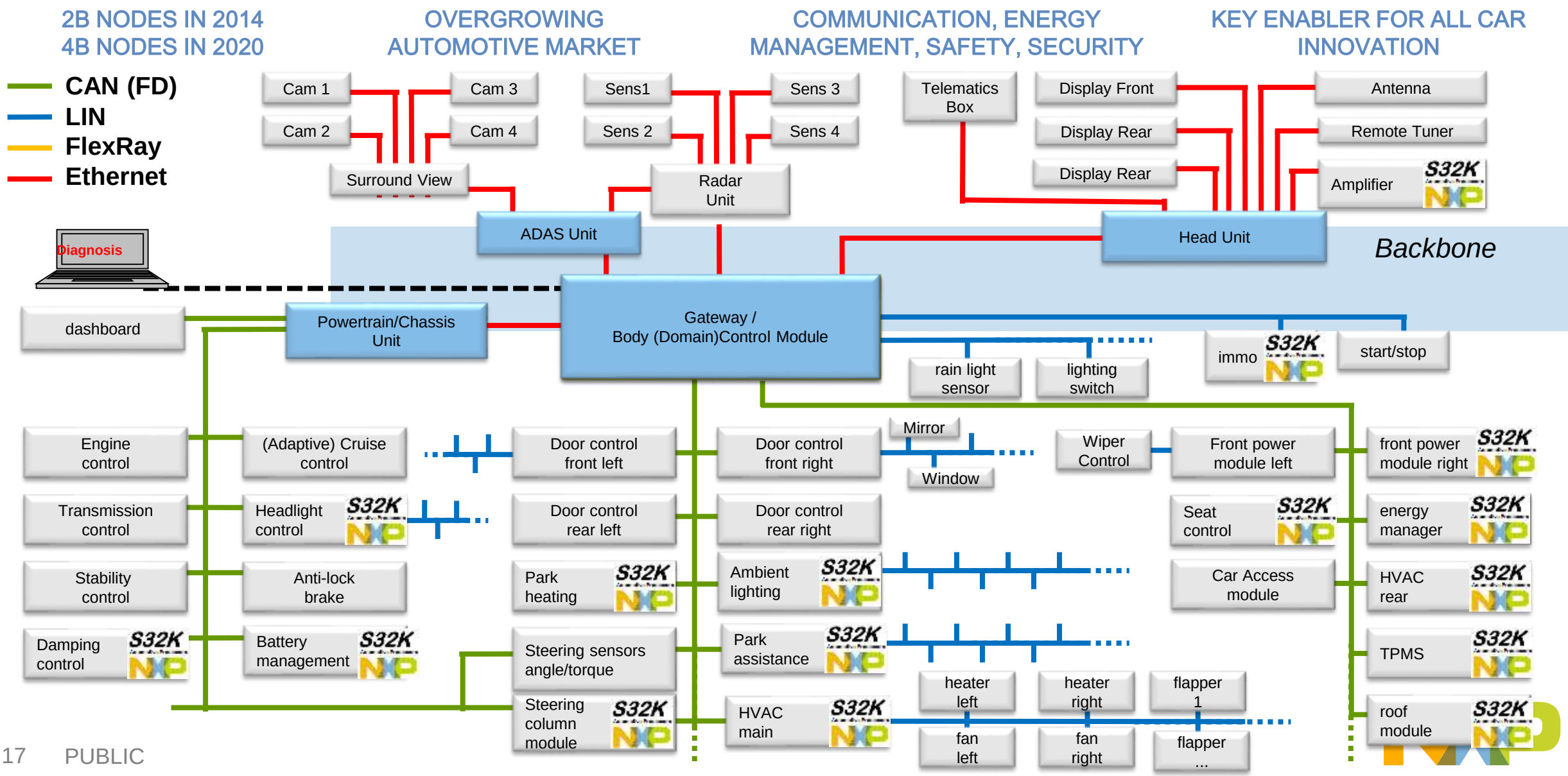
DC/DC converters


E-shifter


Rear view camera tilt


Steering wheel electronics

S32K Portfolio: **S32K For Edge Nodes**



S32K Portfolio: **S32K144 Block Diagram**

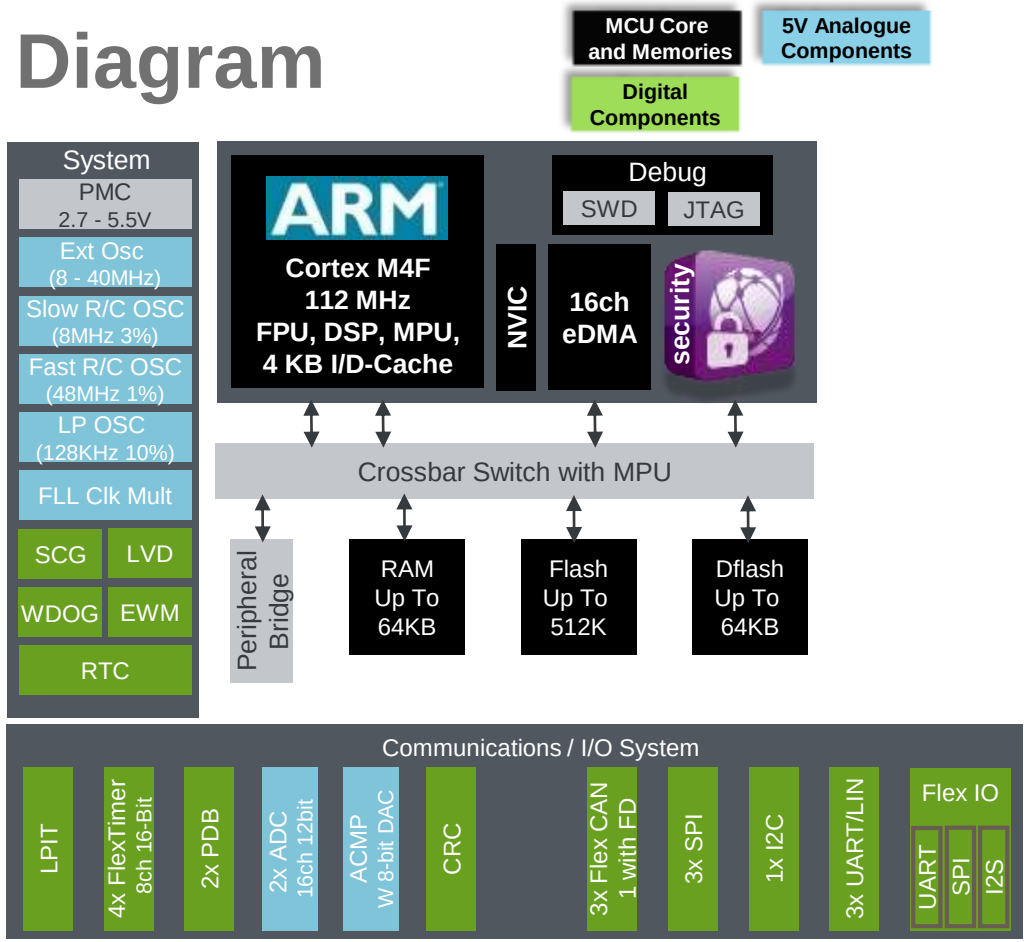
High performance
- ARM Cortex M4F up to 112MHz w FPU
- eDMA from 57xxx family

Software Friendly Architecture
- High RAM to Flash ratio
- Independent CPU and peripheral clocking
- 48MHz 1% IRC – no PLL init required in LP
- Registers maintained in all modes
- Programmable triggers for ADC → no SW delay counters or extra interrupts

Functional safety
- ISO26262 support for ASIL B or higher
- Memory Protection Unit
- ECC on 512K Flash / 64K Dataflash and RAM
- Independent internal OSC for Watchdog
- Diversity between ADC and ACMP
- Diversity between SPI/SCI and FlexIO
- Core self test libraries
- Scalable LVD protection
- CRC

Low power
- Low leakage technology
- Multiple VLP modes and IRC combos
- Wake-up on analog thresholds

Security
- CSEc (SHE spec)



Packages & IO
- Open-drain for 3.3 V and hi-drive pins
- Powered ESD protection
- Packages: 100 BGA, 64 LQFP, 100 LQFP

Operating Characteristics
- Voltage range: 2.7V to 5.5V
- Temperature (ambient): -40°C to +125°C

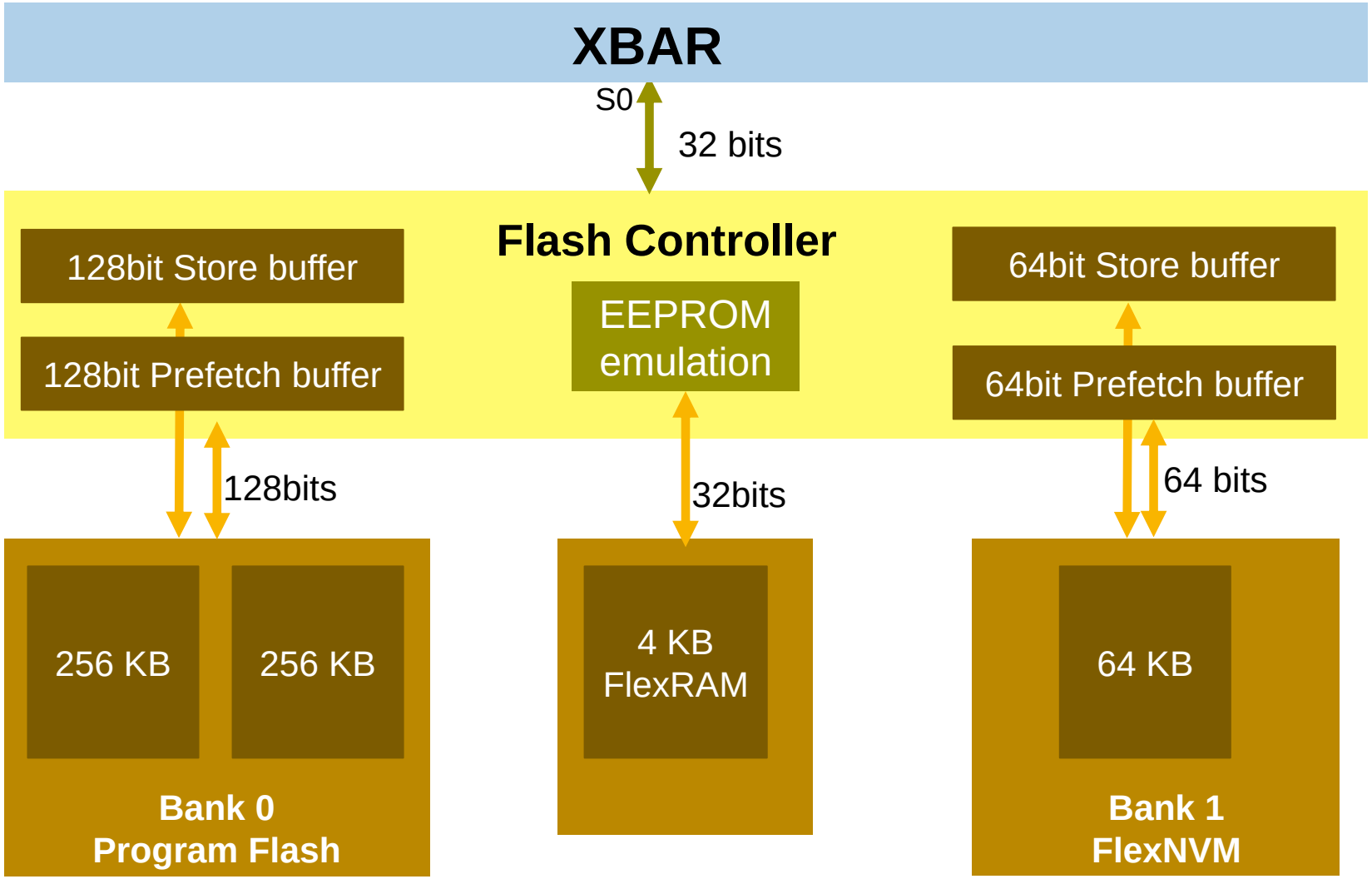
S32K Portfolio: **S32K1xx / KEA Product Series Compatibility**

- Pin Compatibility:
  - Within S32K1xx product series
  - To **KEA** products

- IP Compatibility:
  - With MPC55xx/MPC56xxx/MPC57xxx product series:
    - FlexCAN, eDMA, QuadSPI
  - With Freescale Kinetis and KEA products:
    - FlexTimer, IIC, LSPI, UART, ADC, CRC, FlexIO

Flash	Pin Count								
	16/24	32	48	64	80	100	100 BGA	144	176
2M							S32K148	S32K148	S32K148
1M							S32K146	S32K146	S32K146
512K				S32K144		S32K144	S32K144		
256K			S32K118	S32K142 / S32K118		S32K142			
128K		S32K116	S32K116	KEAZ128	KEA128				
64K		KEAZN64 / S32K114	S32K114	KEAZ(N)64	KEAZ64				
32K		KEAZN32		KEAZN32					
16K		KEAZN16		KEAZN16			*potential option		
8K	KEAZN8								

S32K Portfolio: **Flash System**



S32K Portfolio: **Flash Arrays**

FOTA relevant features:

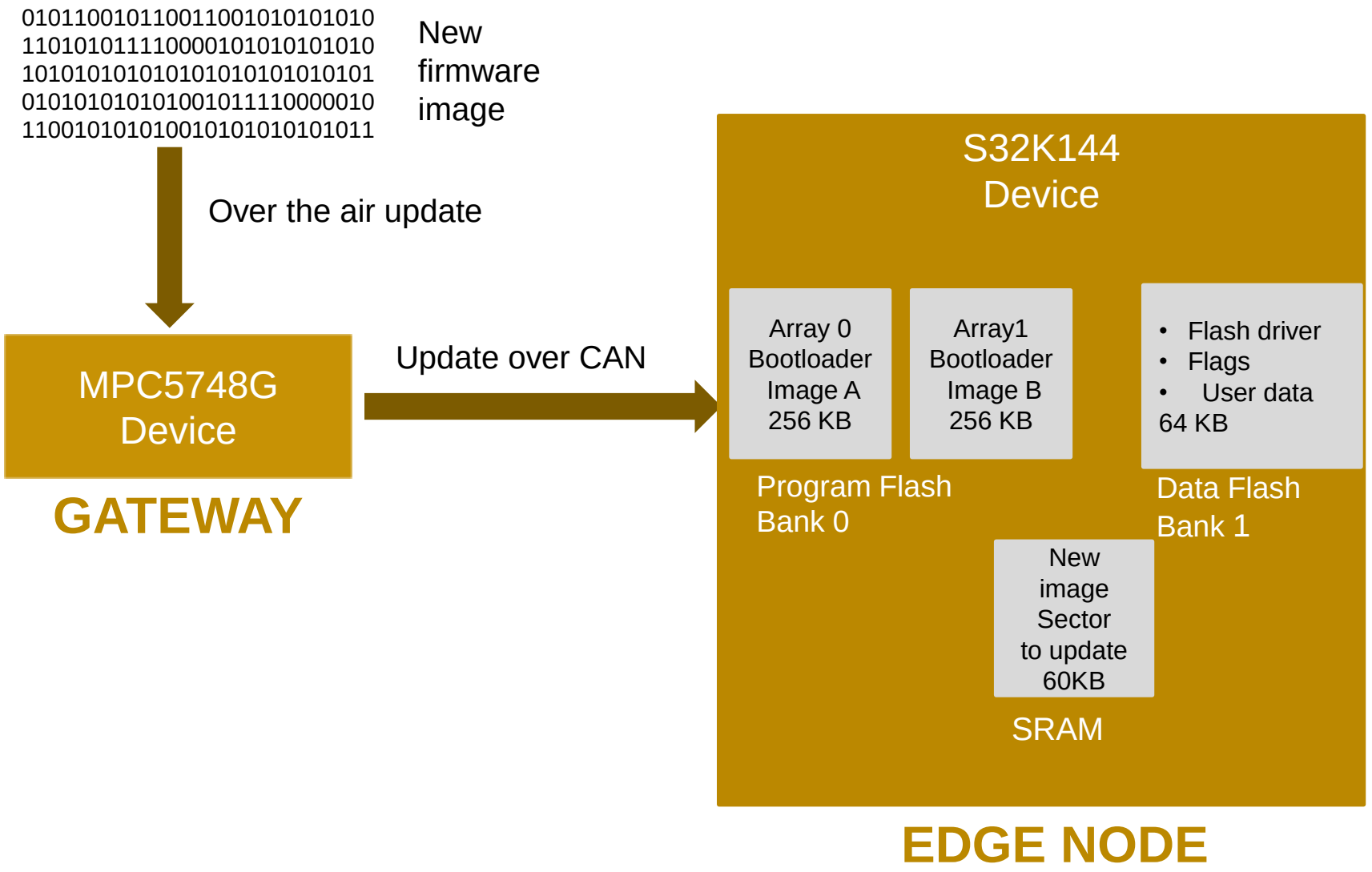
- Sector size (= minimum erase size)
  - **4K Bytes** in Program Flash (bank 0)
  - **2K Bytes** in Data Flash (bank 1)
- Read-While-Write (RWW) features between Bank0 (Program Flash) and Bank1 (Data Flash)

Key additional flash features:

- **C90TFS** (Thin-Film-Storage) technology
- ECC support: **Single Bit Error Correction and Double Bit Error Detection**
  - 32bit ECC word in data flash
  - 64bit ECC word in program flash
- Access time: **Flash clock is about #1/4 of the core clock**

S32K USE CASES

S32K Use Cases: S32K144 A/B Swap



S32K Use Cases: A/B Swap Steps (1 of 4)

1 No new image reset

S32K144
Device

Running: Bootloader

- No new image available
- Branch to image A

2 Update request

S32K144
Device

Running: Image A

- Update request
- New image flag set

Update image

CAN BUS

3 Next reset

S32K144
Device

Running: Bootloader

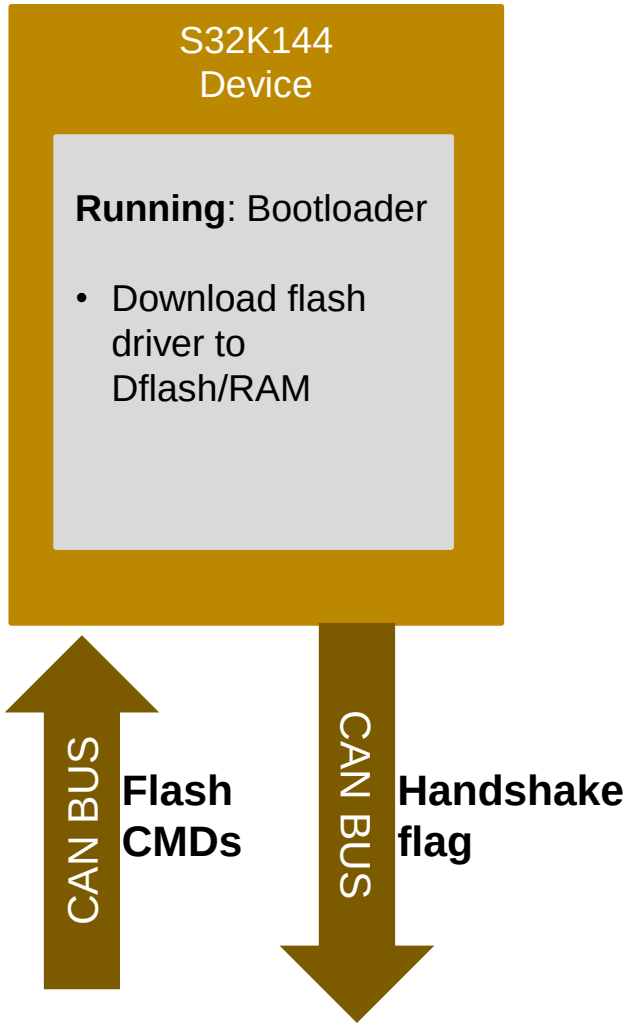
- New image request detected
- Check program flash array available

Handshake flag

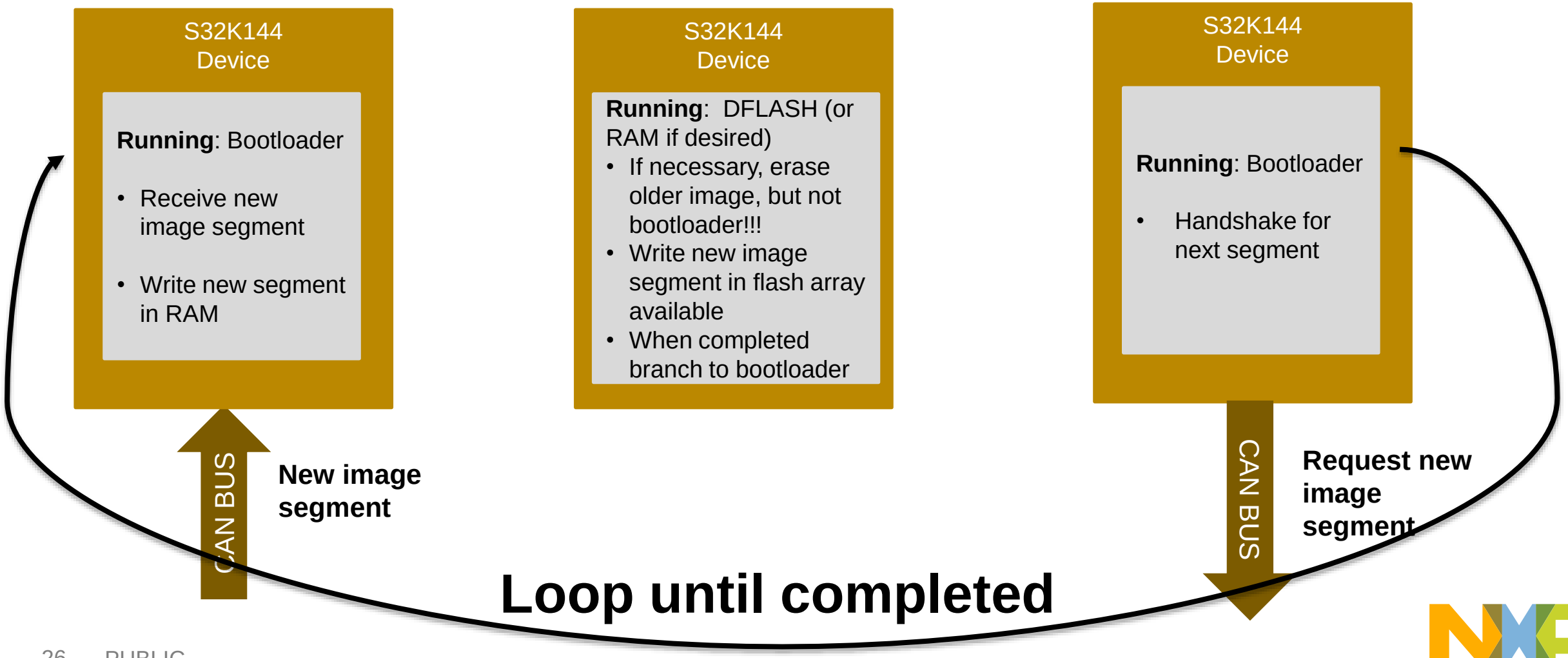
CAN BUS

S32K Use Cases: A/B Swap Steps (2 of 4)

4 Download Flash program/erase code to RAM or Dflash



5 Update Process



S32K Use Cases: A/B Swap Steps (4 of 4)

6 Update complete

S32K144
Device

Running: Bootloader

- Set update flag completed
- Issue a reset

7 Almost there

S32K144
Device

Running: Bootloader

- New image flag detected
- Update complete flag detected
- Update flash side available
- Branch to new image

8 Finished

S32K144
Device

Running: Image B

Erase update status flags

S32K Use Cases: A/B Swap Options without Flash Remapping

1. Have two separate object files
   - Requires more overhead in file management!

2. “Fix up” references to flash addresses in startup code.
   Examples: (assume one binary; all source is compiled at same time so there are no external references):
   - Masters (like DMA) reference to flash: boot code defines offset variable that is used in code

     DMA.SADDR = 0x100000 + OTA_offset;
   - Code constants: Use RAM based table for references that contain OTA offset variable
   - Function calls & branches

S32K Use Cases: A/B Swap Summary for S32K144

Pros/Limitations

- Pro: A-B swap allows backup immediately available
- Limitation: compared to large MCUs with multiple code partitions, updating the image cannot be done live

S32K Use Cases: Looking forward: S32K148

- Larger program flash and data flash

- External QuadSPI (serial flash) support
  - Enables option of storing current and new FW in serial flash.
    - Simpler recovery to prior version – no need to resend from gateway or OTA
    - New image can be stored “at leisure” then updated faster from local memory

S32K SECURITY

S32K14x Security: **Security – Why Worry?**

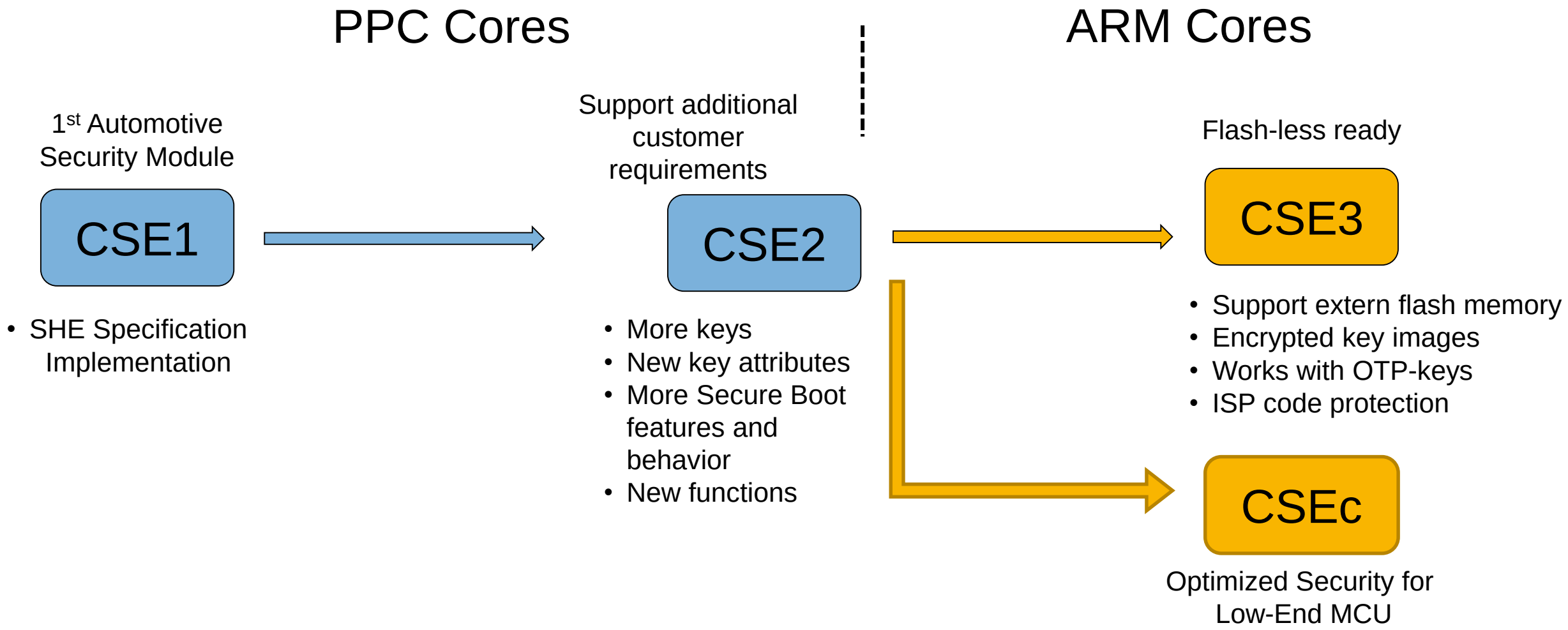
- Same problem which Julius Caesar faced 2000 years ago.
- Avoid hacker attacks
- Prevent reprogramming
- Steal OEM firmware
- Use cases
  - Immobilizer / Component Protection
  - Mileage Protection
  - Secure Boot
  - Secure Communication

S32K14x Security: SHE – An Early Automotive Security Standards

- Background:
  - Created by Audi (main driver), BMW and Escrypt
  - Published as a official HIS standard
    (HIS => Herstellerinitiative Software, German for 'OEM software initiative')

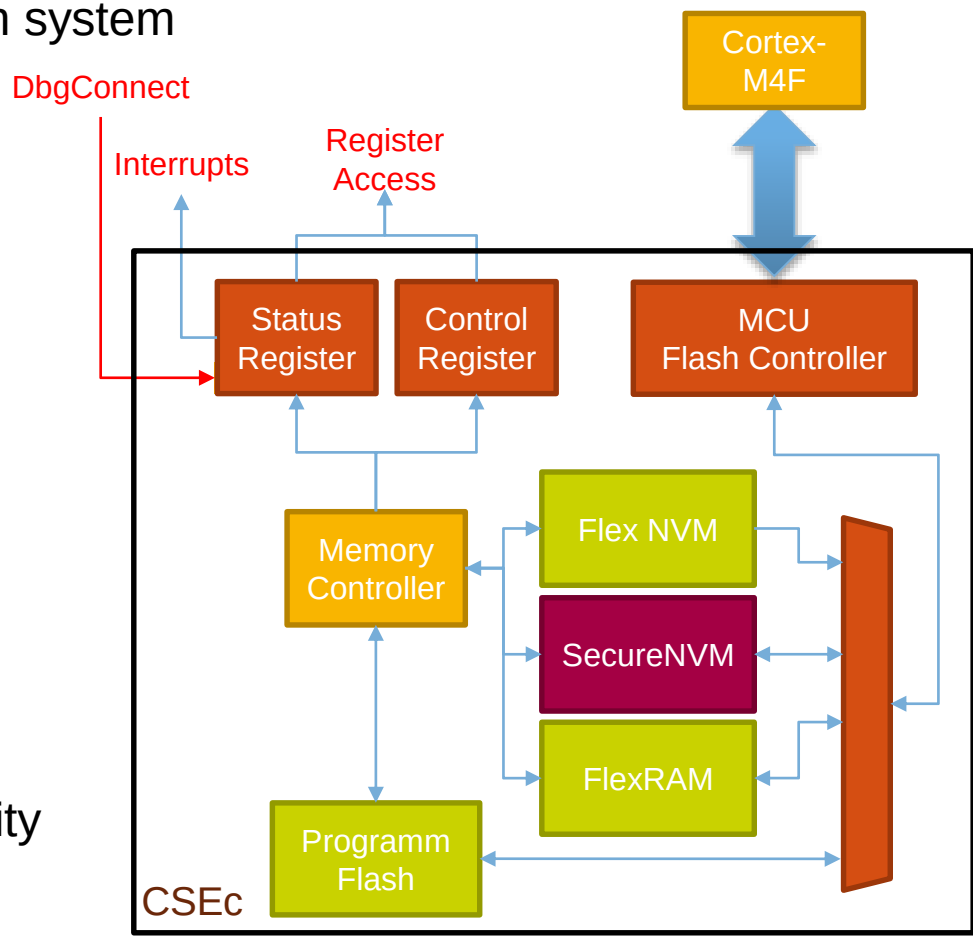
- Key features of the SHE specification:
  - A secure storage for crypto keys
  - Crypto algorithm acceleration (AES-128)
  - Secure Boot mechanism to verify custom firmware after reset
  - Offers 19 security specific functions
  - Up to 10 general and 5 special purpose crypto keys

S32K14x Security: **Cryptographic Secure Engine (CSE) uses SHE**



S32K14x Security: **S32K Security Module (CSEc) – Overview**

- SHE functionality moves from dedicated master module into the flash system
- Secure key storage only accessible by CSEc
- Crypto Keys
  - Several General-Purpose keys
  - Special Purpose keys
    (e.g. Secret, Master and Secure-Boot Key & CMAC)
  - Support of additional encrypted keys in public flash memory.
- True Random Number System
- CSEc supports AES-128 with
  ECB, CBC and CMAC mode\
- Use Cases
    - Secure Boot - Check Boot Loader for Integrity and Authenticity
    - Check parts of Flash Memory for Integrity and Authenticity
    - Secure Communication
    - Component Protection



SUMMARY

- Firmware is increasing in the vehicle.
- FOTA is necessary in today’s vehicles
- NXP portfolio can help in your FOTA application
- CSEc for secure FOTA

SECURE CONNECTIONS
FOR A SMARTER WORLD