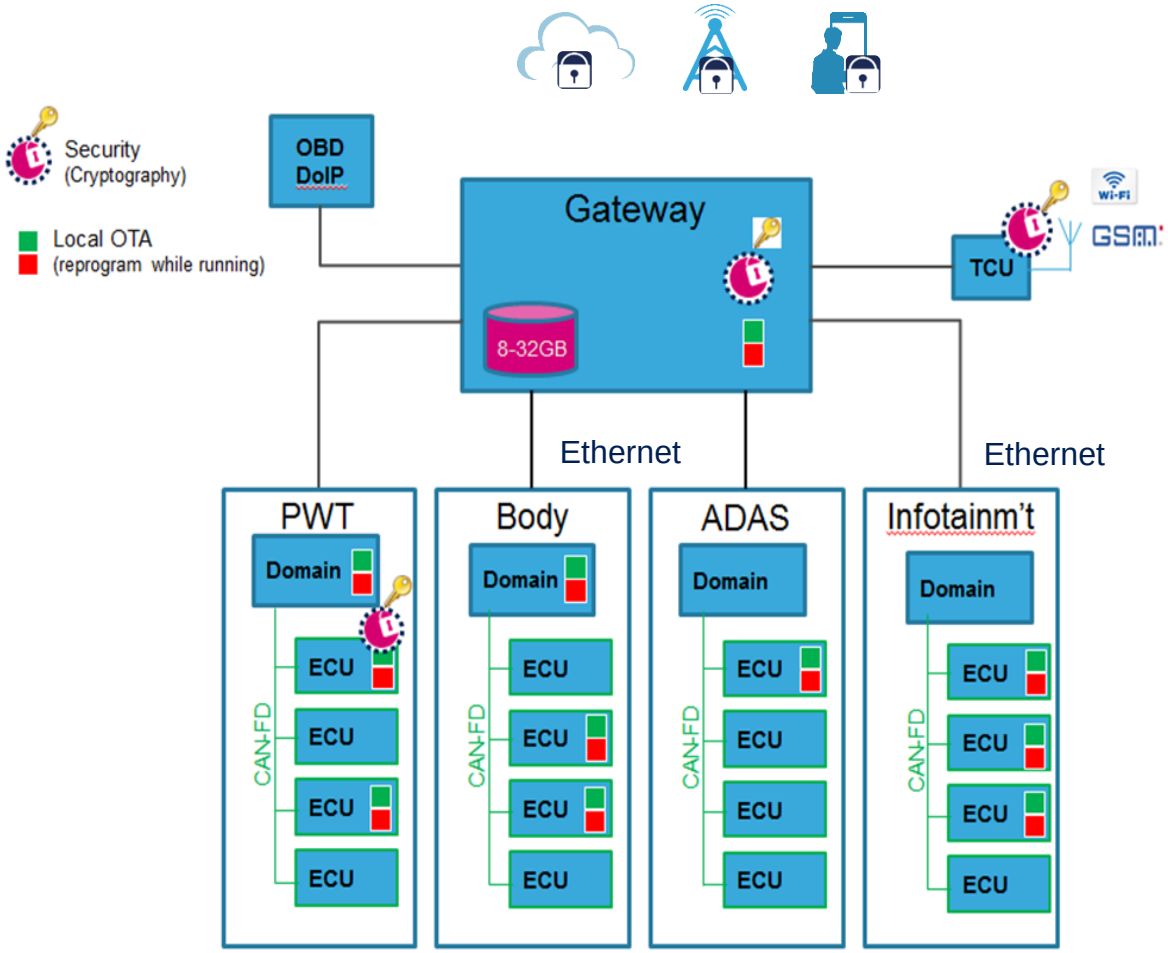
SPC5 MCU NEV applications and safety, security, OTA

Fanny XU
Application Manager, Micro BU
ADG Marketing and Application
Greater China & South Asia Region
STMicroelectronics

life.augmented

NEV Architecture Evolution



Computation Capability

- High Performance
- Powerful
- Diversification
- Fault manage & self-test

DATA Routing

- Ethernet back-bone network
- Diversity network interface
- HW gateway data routing
- Global time synchronization

FOTA

- Flash context manage by HW
- Interface for external memory
- Ultra fast communicate interface
- Advanced security features

Security

- Protection & authentication
- Isolation
- Encryption & Decryption
- Secure data storage & routing

Functional Safety

- HW Safety mechanism
- Safety SW ecosystem
- Fail safe architecture
- Fault collection and reaction

life.augmented

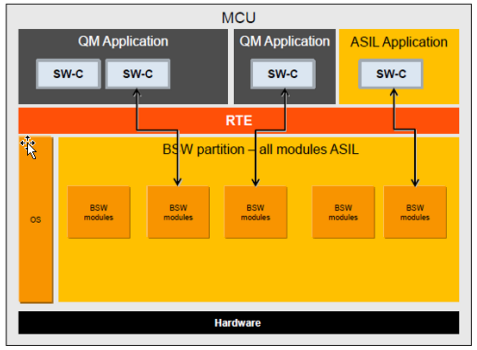
CPU Architecting Secure Foundation

SW differentiate criticality

SW Complexitity Multiple sources

SW Safety and Security

- Software separation support for safety and security
- High throughput combined with deterministic responsiveness
- Comprehensive protection, monitoring and reporting
- Extensive fault detection and control capabilities
- Managing both random and systematic faults in processor, memories and peripherals
- Multi-core capability, Advanced SIMD.
- Embedded Flash memory interface



Example for usage of method (1)

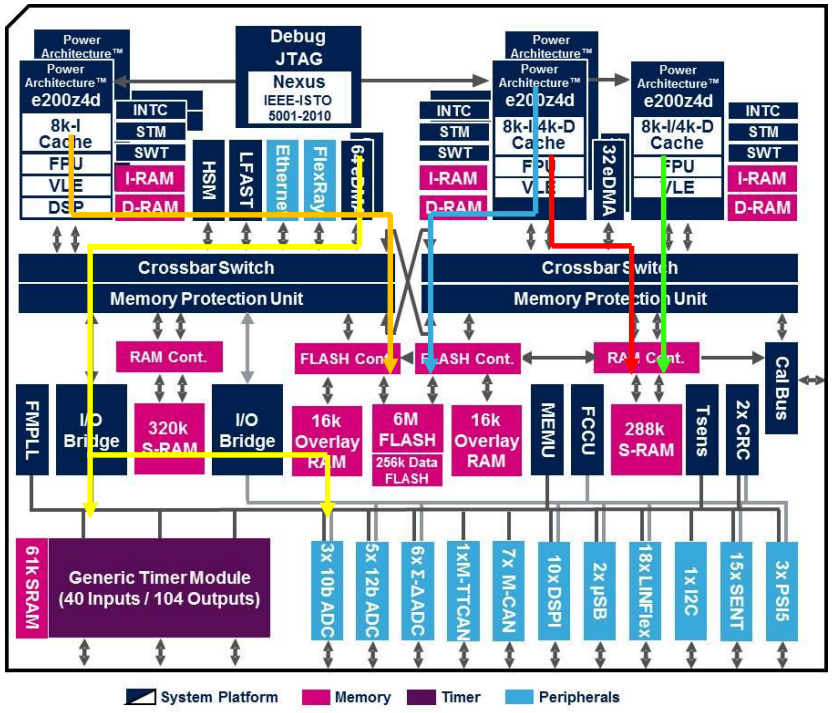
AUTOSAR™
Enabling continuous innovations

life.augmented

Spc5x High Performance Architecture

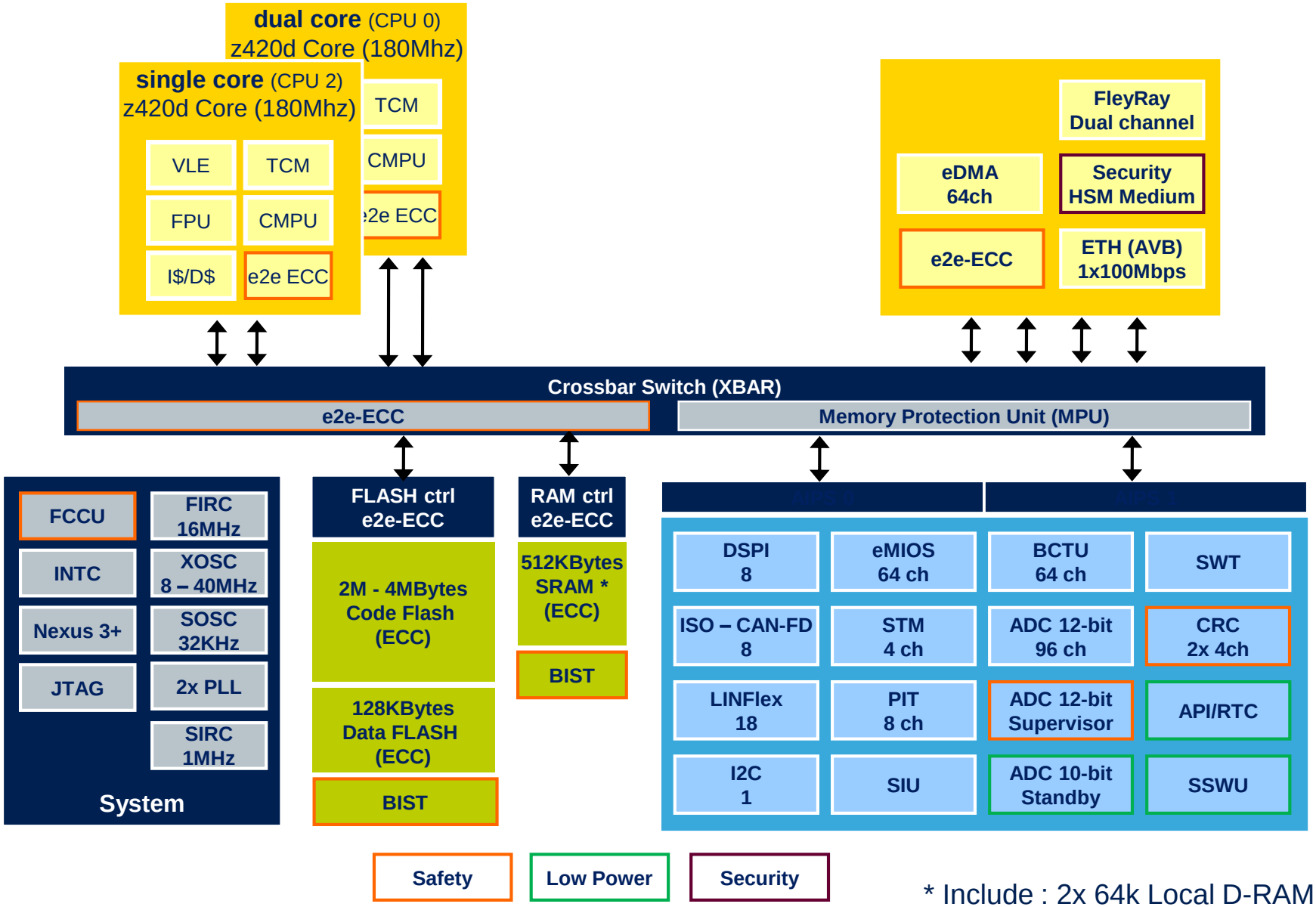
Answering System Performance Requirements

Increasing system performance requirements are managed through more optimized MCU architectures on platform :



- Highly multi-thread optimized platform architecture allowing concurrent tasks up to :
  - 10 simultaneous switches on crossbars
  - 2 simultaneous Flash read accesses (True Read-while-Read Flash Module)
  - 4 simultaneous SRAM accesses
  - 2 simultaneous eDMA data transfers
  - 3 simultaneous peripheral accesses
- Whole platform running at core speed to avoid system performance loss from clock synchronizations.
- Same platform architecture across all devices and same peripheral implementation

Chorus 4M – Generic Block Diagram

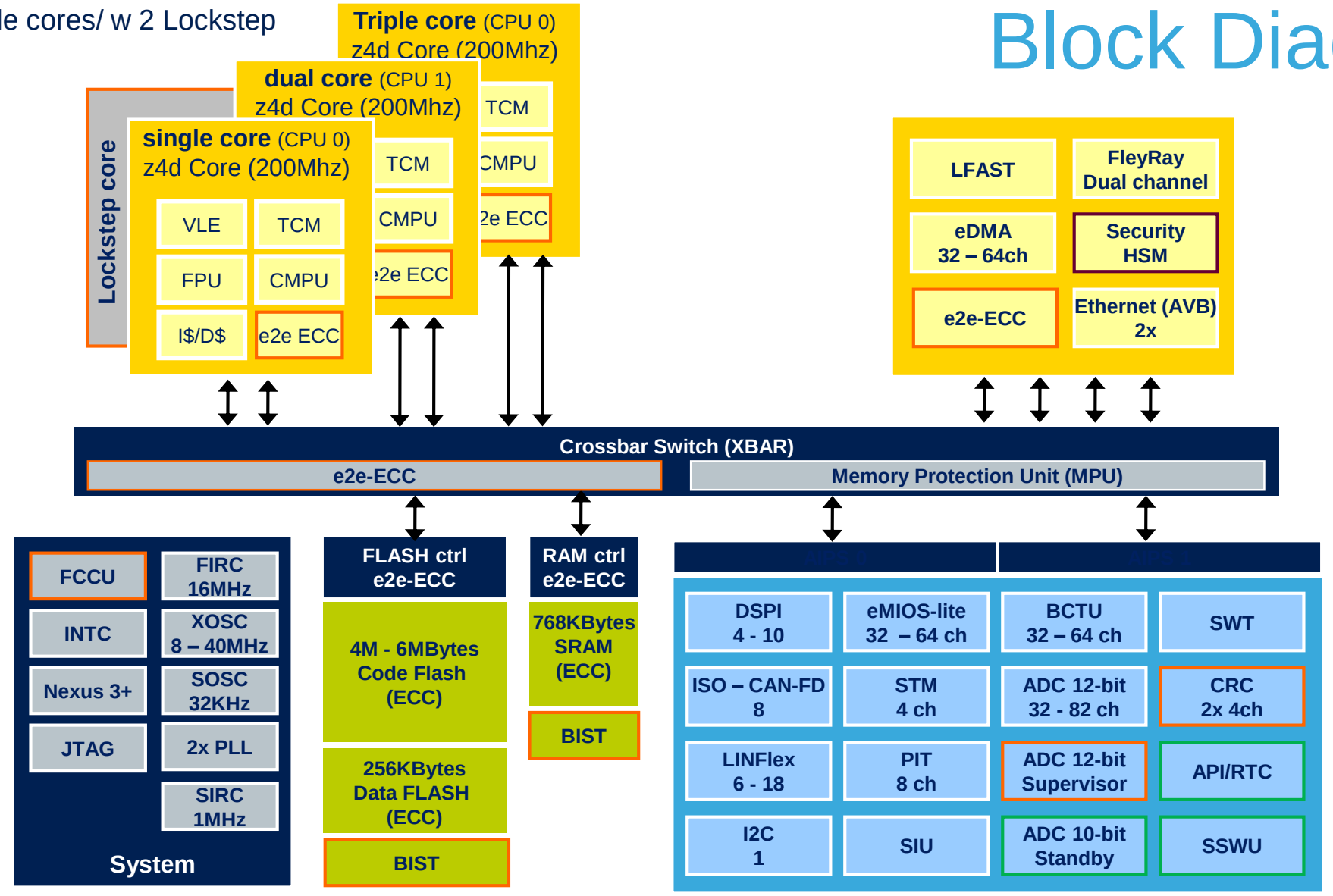


* Include : 2x 64k Local D-RAM inside core

life.augmented

Chorus 6M – Generic Block Diagram

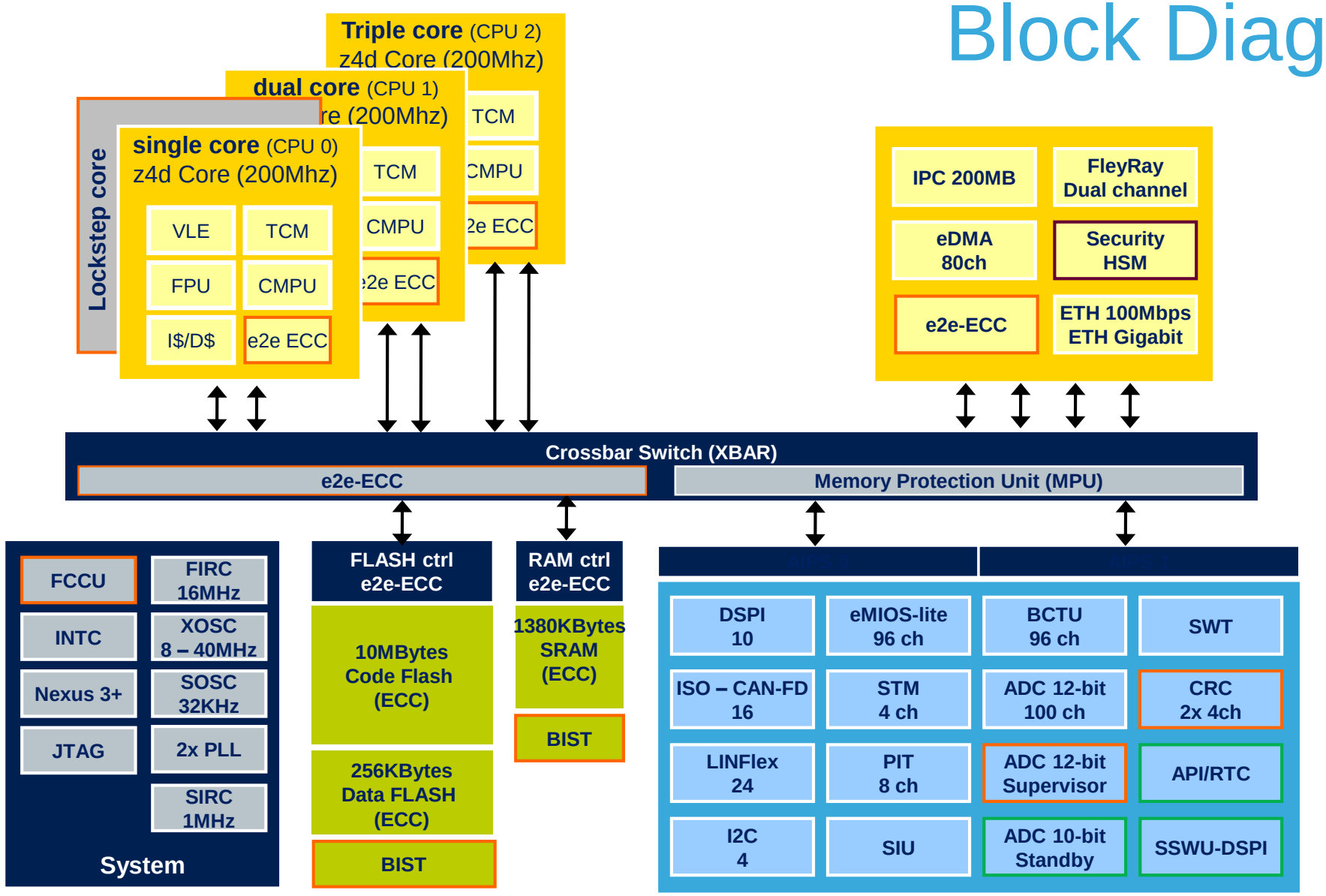
* SPC58NN84: triple cores/ w 2 Lockstep



* Include : 160k D/I-RAM inside core

life.augmented

Chorus 10M – Generic Block Diagram



* Include : 192k I-RAM + 96k D-RAM inside core

life.augmented

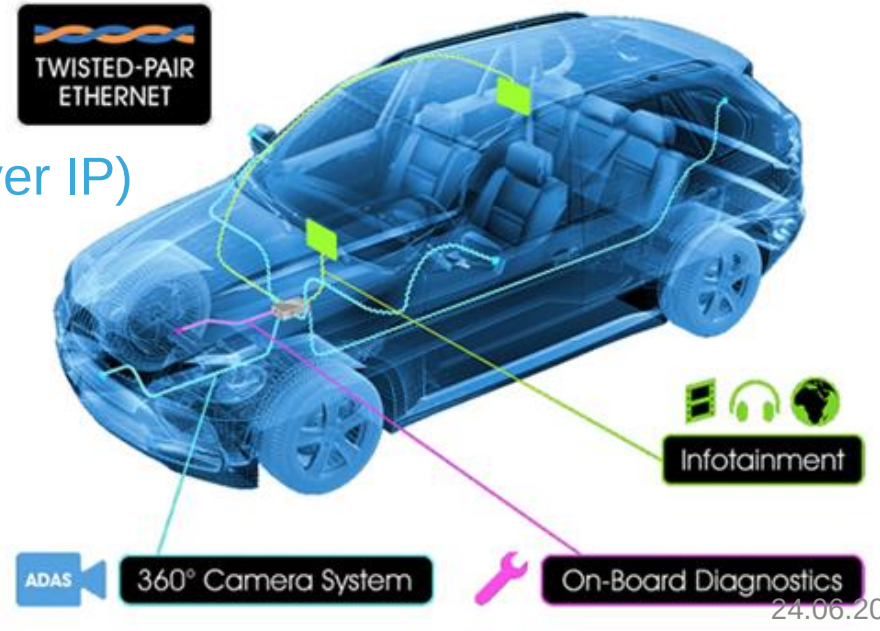
Data Routing

life.augmented

Ethernet in Automotive

Market Trends

- Ethernet is becoming the standard automotive high speed network as it can be implemented at reasonable costs with the **Unshielded-Twisted-Pair** BroadR-Reach technology
- Standardization driven by the OPEN Alliance consortium (**O**ne-**P**air **E**ther-**N**et)
- Application domains for ethernet in automotive
  - Advanced OBD with **Fast-Flashing and DoIP** (Diagnostic over IP)
  - **Back-bone** networks
  - **ADAS** for camera connection
  - Replace **MOST** in infotainment
  - **Inter-processor** communication



ST Network Interface

CAN/LIN/Ethernet

	1 CAN	2 LIN	3 Ethernet
Bernina, Eiger Chorus B/C/G Lines	Up to 8x ISO CANFD	Up to 18x LINFlexD	Up to 2x 100M Ethernet
Chorus H Line	16x ISO CANFD	24x LINFlexD	1x 100M Ethernet 1x 1000M Ethernet
	Hardware FIFO/Queue Shared Message RAM	FIFO/DMA support HW master/slave	Qos support Time synchronization Checksum offload

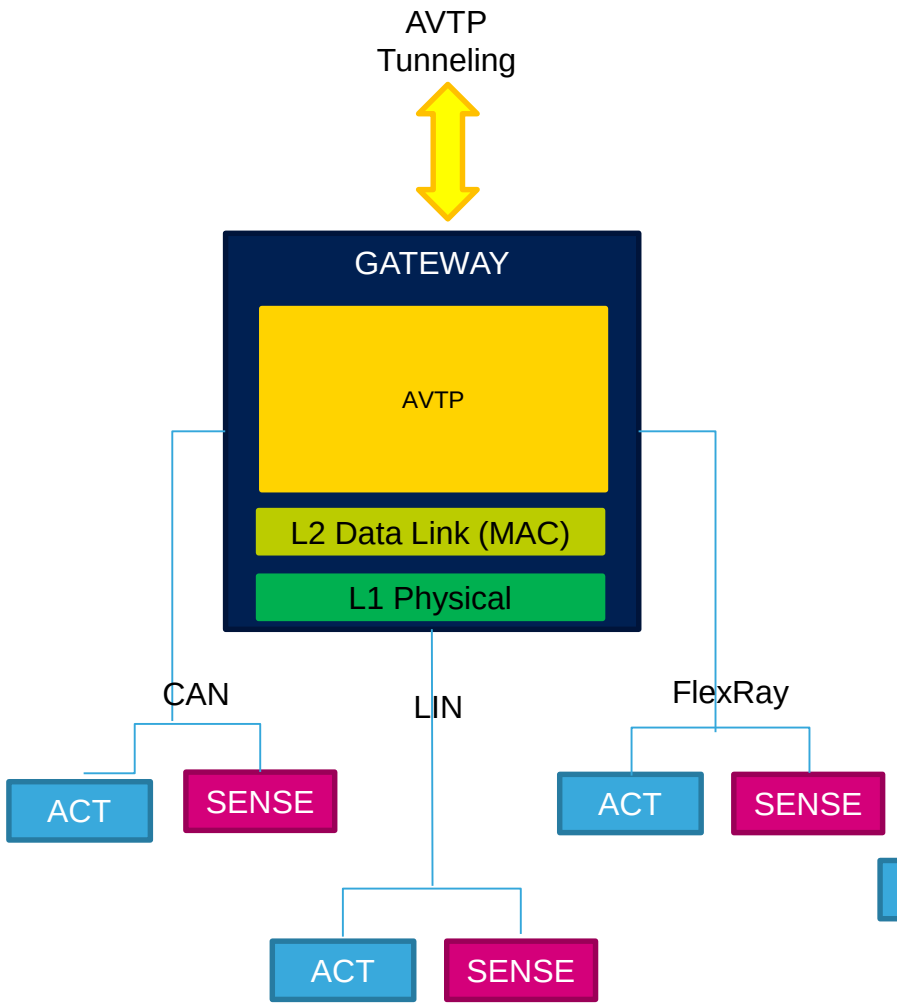
life.augmented

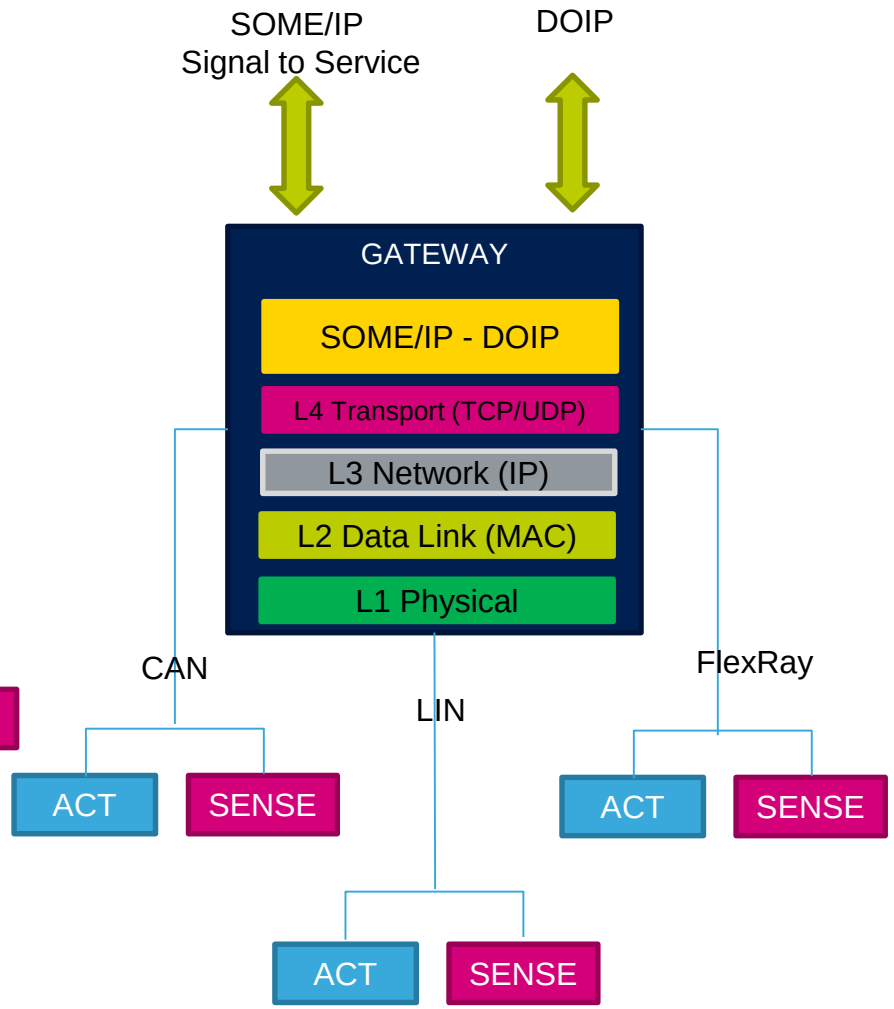
SPC58 product portfolio is READY for Network Communication.

GW ETH Protocol Stacks

- SOME/IP introduces *service-oriented* transmission of information in contrast of all the prior standards and protocols that have been signal-oriented.

- AVTP is a ETH L2 protocol that uses the TSN feature to implement a communication with Low Latency. It allows the encapsulation (tunnelling) of real time buses as CAN and FR





FOTA

life.augmented

Flash-over-the-air Concepts and Basic Requirements

- The advantages of being able to perform in-the-field software updates to cars are well established
  - To enable critical bugs to be patched immediately without returning to dealership
  - To allow compelling new features to be added to the vehicle at any time during its lifecycle
  - To save money

- Unlike consumer devices like smartphone, car owners do not tolerate downtime of their vehicles while updating. Therefore, updates critical to vehicle operation should ideally take place
  - seamlessly and invisibly in background (thus → several RWW partitions, see next slides)
  - with a data integrity security schema in place

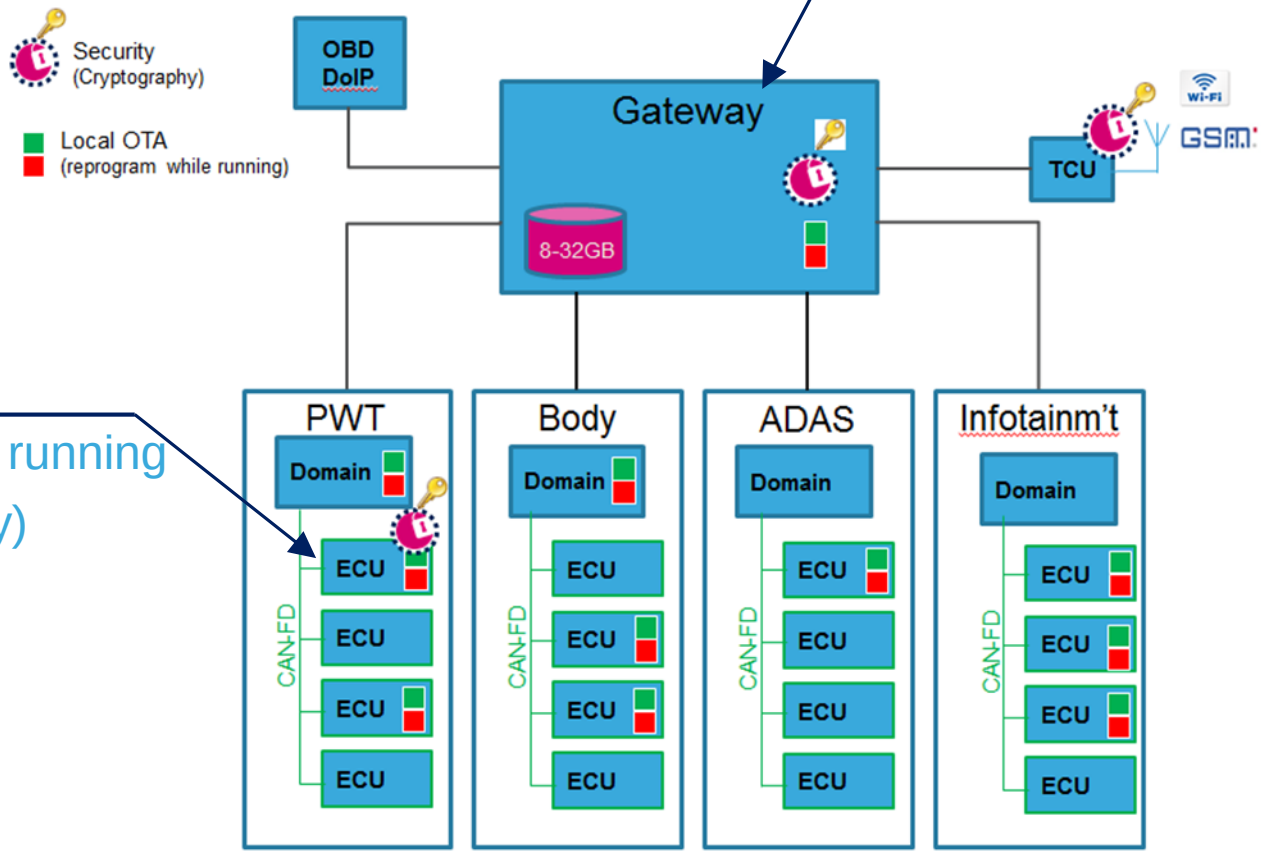
- Unlike infotainment and telematics systems, ECUs controlling key cars' features are placed deeper within vehicle' network architecture, with small and embedded Flash and RAM

life.augmented

FOTA Requirements
Applications Scheme

- Application with central OTA management capability, like gateway and/or storage
  - Flash context management by HW
  - Interface for external memory
  - Ultra fast communication interface
  - Advanced security features

- Application supporting local OTA
  - Flash erasing/program while the application is running
  - Security features (authentication, cryptography)
  - Fast communication interface



CHORUS family full supports both kind of applications

ST Solutions for FOTA

Building Blocks

	1 Security	2 Memory Partition	3 Fast Interfaces form Communication & Storage
Bernina, Eiger Chorus B/C/G Lines	From Evita Medium	From SW handling	From Fast SPI and 100Mbit Ethernet
Chorus H Line	To Evita Full	to Hardware address switch	eMMC, Hyperflash, Gbit Ethernet

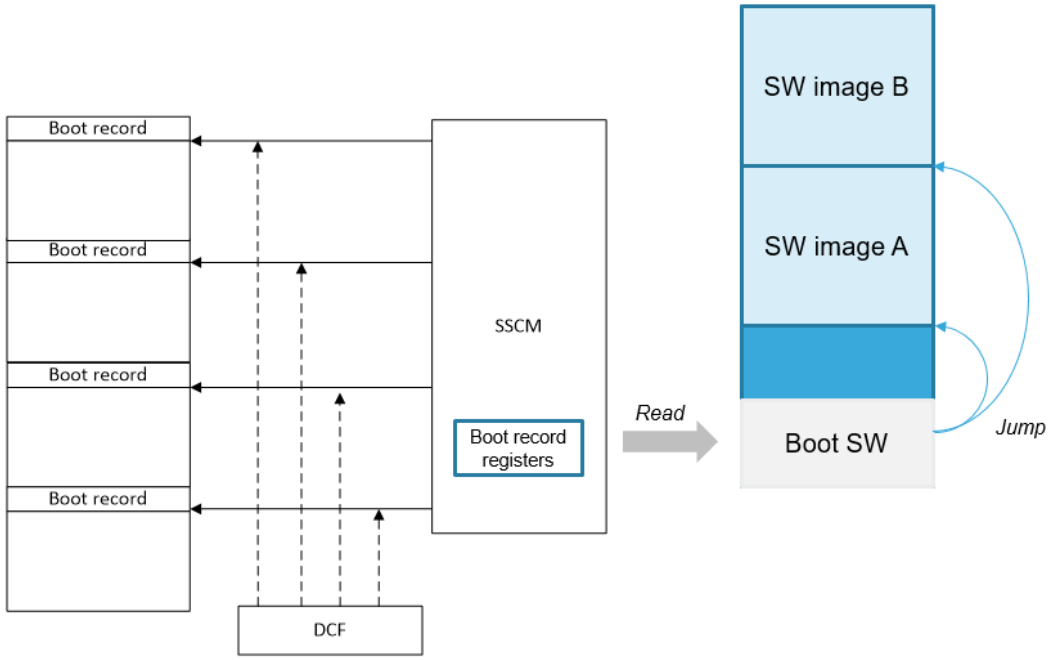
SPC58 product portfolio is READY for FOTA

life.augmented

FOTA Diagrams and Features

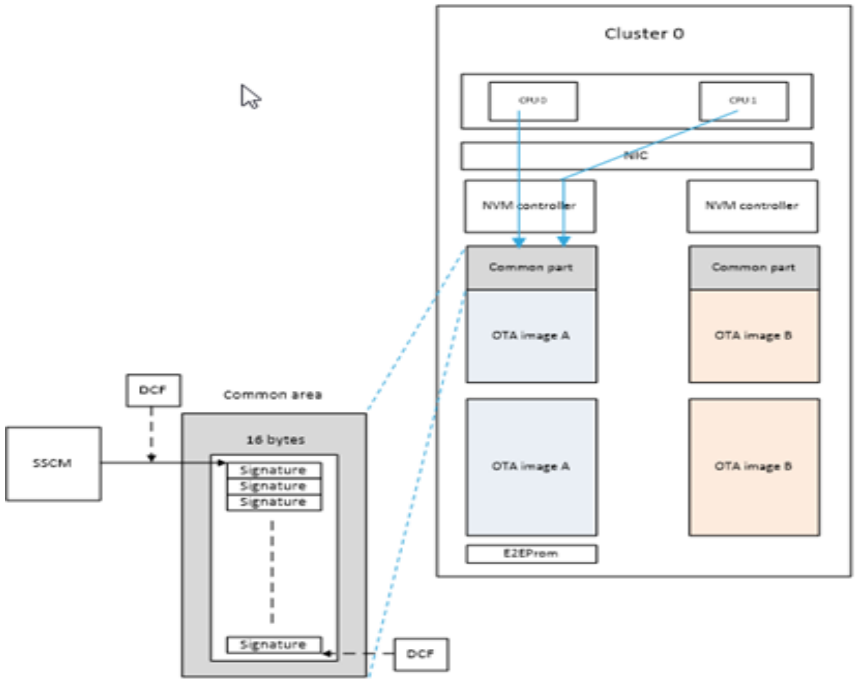
life.augmented

HOST “OTA“ X0



- Available since 55nm products
- The new image can be written only if the SW is not accessing the same RWW partition
- The active SW images is seen (read) at different addresses
- SW image switch is not a atomic operation
- Logical memory space is reduced
- HW complexity

HOST “OTA“ X1



- Available since 40nm products (Chorus10M)
- The new image can be written while the SW is fetching (no constraint)
- The active SW images is always seen (read) at the same address
- SW image switch is an atomic operation
- Logical memory space is reduced
- HW complexity

life.augmented

FOTA - CHORUS Family Features

Overview

- CHORUS 4M – 6M
  - feature several RWW partitions allowing flash update in background while application is running (see backup slides for further details)
  - support very fast SPI to connect to external memory (also an important aspect of OTA)
  - security level: HSM medium
  - Ethernet 100Mbps

- CHORUS 10M enhancements
  - HW support for flash A/B context switching to manage two application versions
  - dedicated very fast external memory interfaces like eMMC and Hyperbus
  - inter-processor interfaces for domain ECU
  - security level: HSM full
  - Ethernet 1000Mbps to receive the bundle Flash images for the whole set of ECUs subsystem

Hardware Support Mechanism for FOTA Applications

Overview – Basic Concepts - CHORUS 10M – 2 of 7

- The new image programming while the application is still running can be done by any core
- The first 2 Mbyte, the common section, is not part of FOTA mechanism
  - No HSM and Flash Data sectors can be updated via OTA
- FOTA split FLASH In three main areas: Common, Context A and Context B
- FOTA swap involve partitions 4,5 (Context A) and 6,7 (Context B) only
- Once FOTA activated, the new SW image is always visible at the same addresses
  - Thus neither application code nor Make file/linker scripts needs modifications

OTA context mapping

Context	RWW
A	4, 5
B	6, 7

	Write ADD swap=X	Read ADD swap=0	Read ADD swap=1
common	0x0000.0000	0x0000.0000	0x0000.0000
Context A	0x011C.0000	0x011C.0000	0x015C.0000
Context B	0x015C.0000	0x015C.0000	0x011C.0000

- Whereas If FOTA disabled, Flash blocks addresses are fixed (like in 1st column)

life.augmented

Hardware Support Mechanism for FOTA Applications

Overview – FOTA steps - CHORUS 10M – 3 of 7

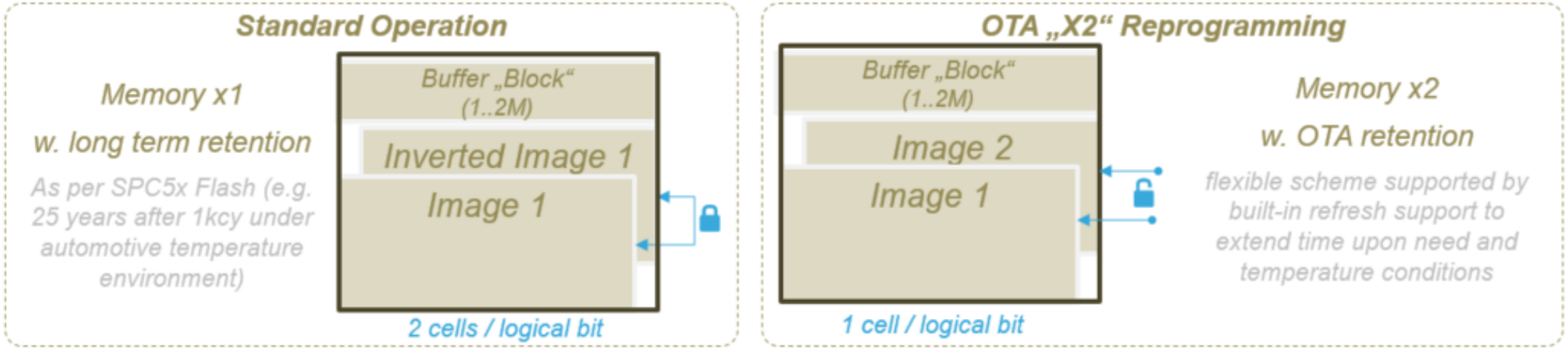
- Here below an overview about the steps needed to enable and apply FOTA swapping

DCF to Enable OTA and select Active context → Program the new immage → Update signature to identify the new active context → Enable the swapping

New HOST “OTA” X2

OTA, X2“ Principle: Based on built-in memory replication and lower memory retention need for the period of 2x simultaneous images in OTA reprogramming mode

- The new image can be written while the SW is fetching (no constraint)
- The active SW image is always seen (read) at the same address
- SW image switch is an atomic operation
- Logical is not reduced (except for the spare buffer)
- HW complexity



life.augmented

Security & HSM

life.augmented

Security in STM Automotive Products

Mass production

202x	28nm	• Asymmetric HW cryptographic • Full isolation of security island • New concepts and IPs
2017	40nm	• HSM • Security architecture enhancements • Asymmetric HW cryptographic (CH10M only) • Below features avaiable at 55nm product
2015	55nm	• Secure system configuration • Extended Flash memory protection • Extended external tool protection • Security vs. Testability
2013	90nm	• SHE-compliant • External tool protection • Basic Flash memory protection

Complexity (*)

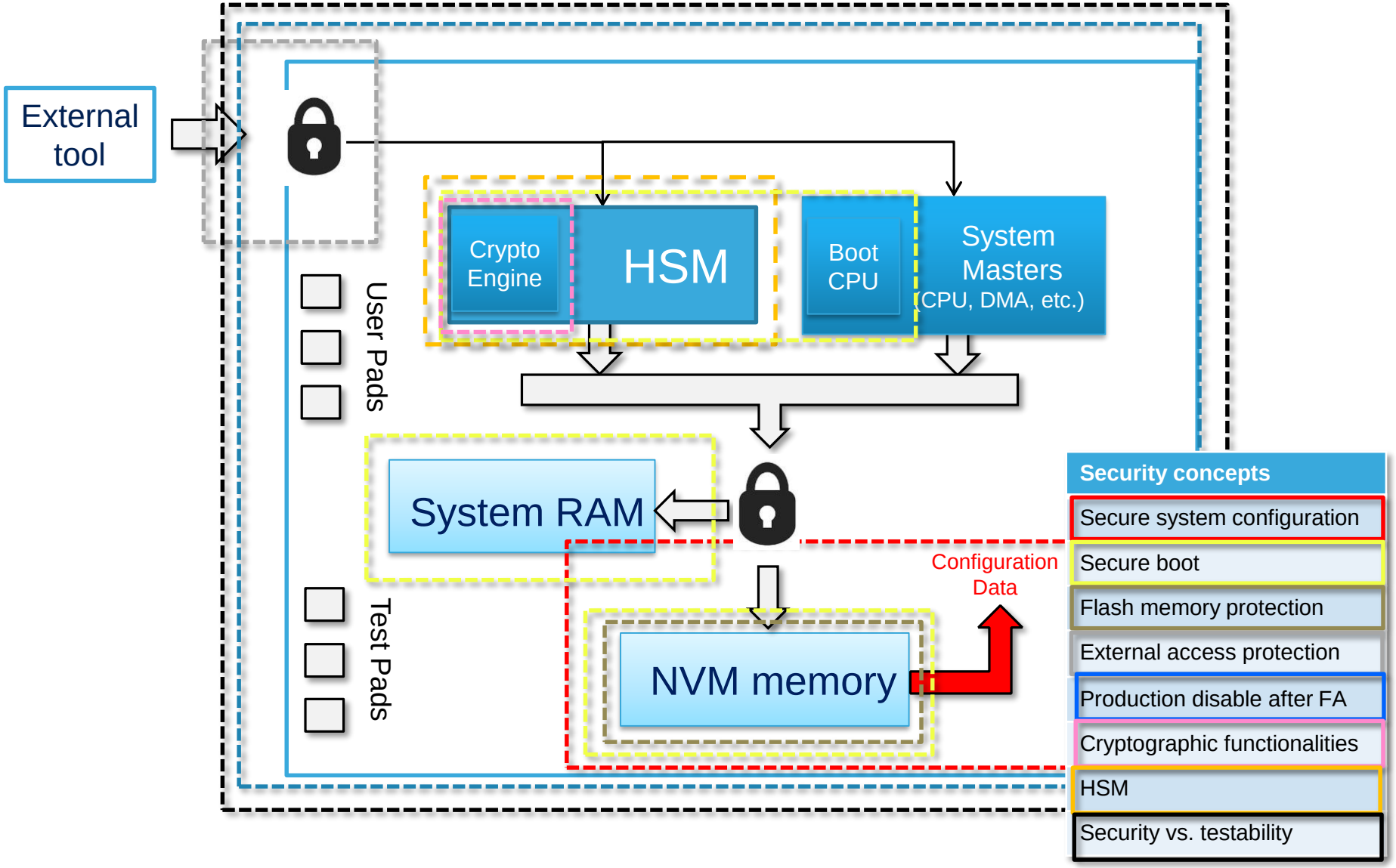
(*) Driven by enhancements and innovations

life.augmented

Common Security (But Wrong...) Assumption

Security = HSM

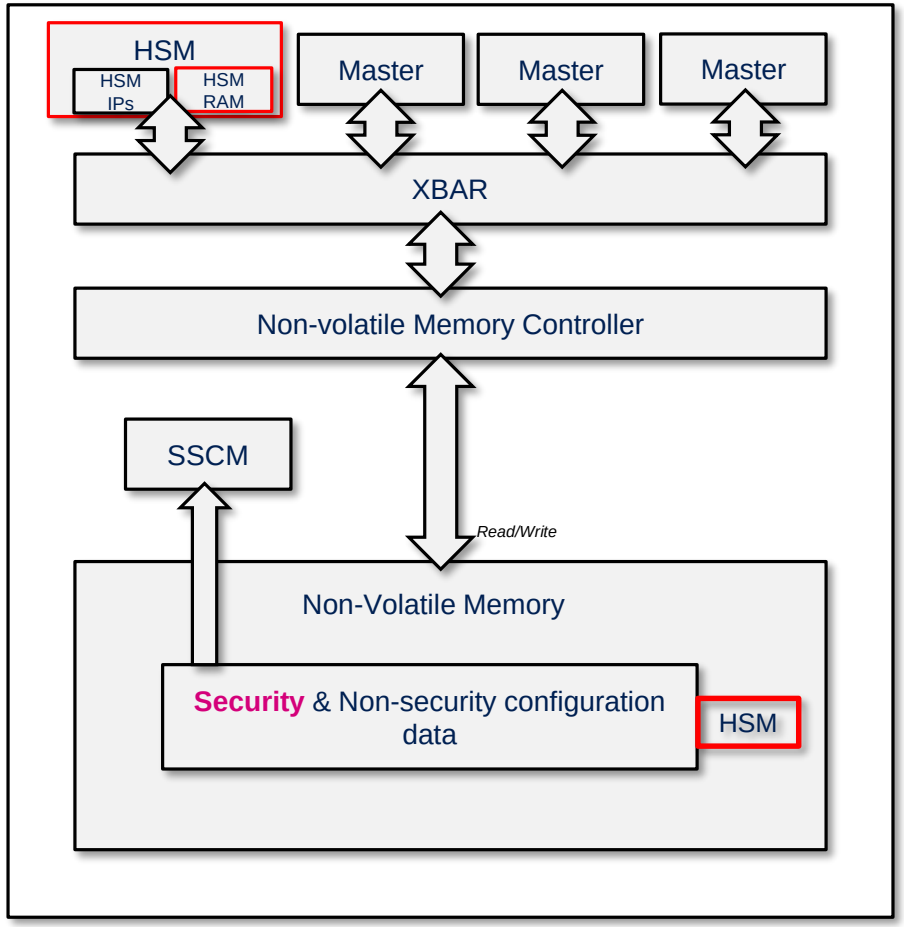
ST MCU Security Concepts



life.augmented

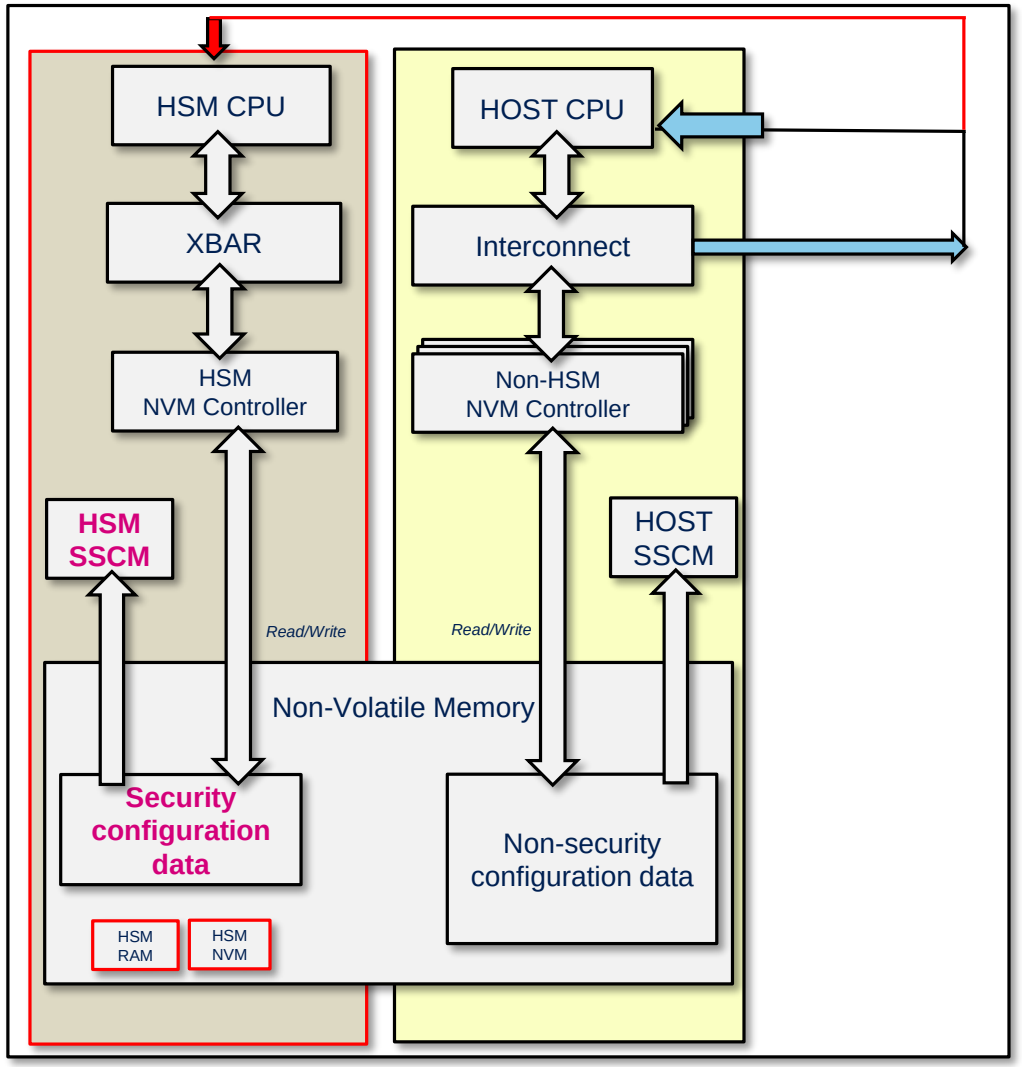
SPC58 Family - NVM

SPC58xB/xC/xG/xN/xH



Tomorrow

HW-protected path



life.augmented

Automotive Security

STELLAR MCUs Built-in Security

SR6 Family
28nm

SPC58 Family
40nm

SPC56 Families
90nm

HSM2

- Public Key / Asymetric HW cryptography
  Enhanced performance from z0h @ 100MHz to Cortex-M4 @ 200MHz
  Increased memory sizes
- Enhanced performance for faster message processing with new mailbox mechanism
- Enhanced Security architecture with more stringent isolation of the security subsystem
- ASILD capability w. AES light concept for e.g. support of ASIL D fast authentication over CAN network (AES Light @ 400MHz)

HSM

- Stronger HW cryptography support and configurability for e.g. hash and asymetric cryptography support
- Higher protection through life cycle management
- Enhancement with Public Key / Asymetric HW cryptography support on SPC58NH

CSE

- Protection against Flash Alteration (secure boot, application code/data)
- Secure applications (e.g. immobilizer) and Secure data (e.g. Mileage) through cryptography and secure key storage/management

EVITA
Full
w. ASIL D capability

EVITA
Medium / Full

EVITA
Medium

HIS
SHE

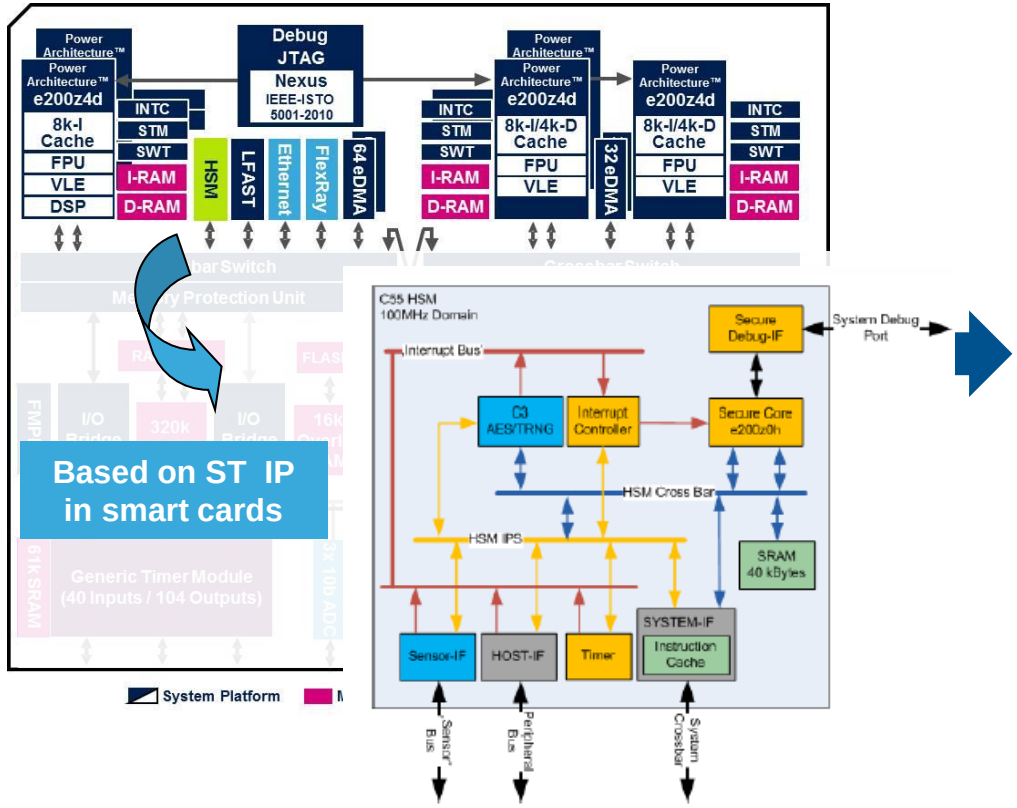
EVITA
Low

life.augmented

SPC5 x High Performance Architecture

Answering System Security Requirements

security requirements are managed through fully independent Security Module (HSM) able to fulfill <u>SHE+ / EVITA medium standards</u>:



ECU protection is key for future ECU MCUs

- Software protection
- Car stealing protection
- Engine tuning protection

<u>Hardware Security Module (**HSM**) :</u>

- Secure storage of encryption/decryption keys in dedicated flash sectors.
- AES 128-bit cryptographic engine, 25MB/s throughput
- Host interface to allow communication and control through status bits and interrupts.
- 2 read only secret keys, unreadable, only manipulated through key index; 8 other user keys
- 1µs latency for AES encryption/decryption
- True Random number generator

SHE – Secure Hardware Extension

- SHE in nutshell
  - BMW and Audi commissioned to Escrypt (part of ETAS) the development of the SHE specification
  - The SHE specification only describes the technical parts. Implementation, process or backend are not subject of the specification.
  - Version 1.1 published April 2010
  - SHE specification is an official specification of HIS (*)

HIS Herstellerinitiative Software

BMW Audi escrypt Embedded Security

- ST has consolidated know-how in security embedded micro
  - ST make available the SHE based on HW – CSE in 2011 - ***SPC56EC (Bolero 3M) microcontroller***
  - In 2016 SHE is based on HW – HSM - ***SPC58XB/C/G/E/N (Chorus/Eiger/Bernina) microcontrollers***.
  - In2018 EVITA FULL on HW – eHSM – ***SPC58NH (Chorus 10M) microcontroller***

life.augmented

Automotive Security Standard vs MCU

	Full EVITA HSM	Medium EVITA HSM	Light EVITA HSM
Internal RAM	✓ (e.g. 64 kByte)	✓ (e.g. 64 kByte)	optional
Internal NVM (Non-volatile memory)	✓ (e.g. 512 kByte)	✓ (e.g. 512 kByte)	optional
Symmetric Cryptographic Engine (e.g. AES-128 CCM, GCM f/AE)	✓	✓	✓
Asymmetric Cryptographic Engine (e.g. ECC-256-GF(p) NIST FIPS 186-2 prime field)	✓		
Hash engine (e.g. Whirlpool)	✓		
Counters	✓ (e.g. 16 × 64-bit monotonic counter)	✓ (e.g. 16 × 64-bit monotonic counter)	optional
Random Number Generator	✓ (e.g. AES-PRNG with TRNG seed)	✓ (e.g. AES-PRNG with TRNG seed)	optional
Secure CPU (e.g. ARM Cortex-M3 32 bit, 50–250 MHz)	✓	✓	
Hardware Interface	✓	✓	✓

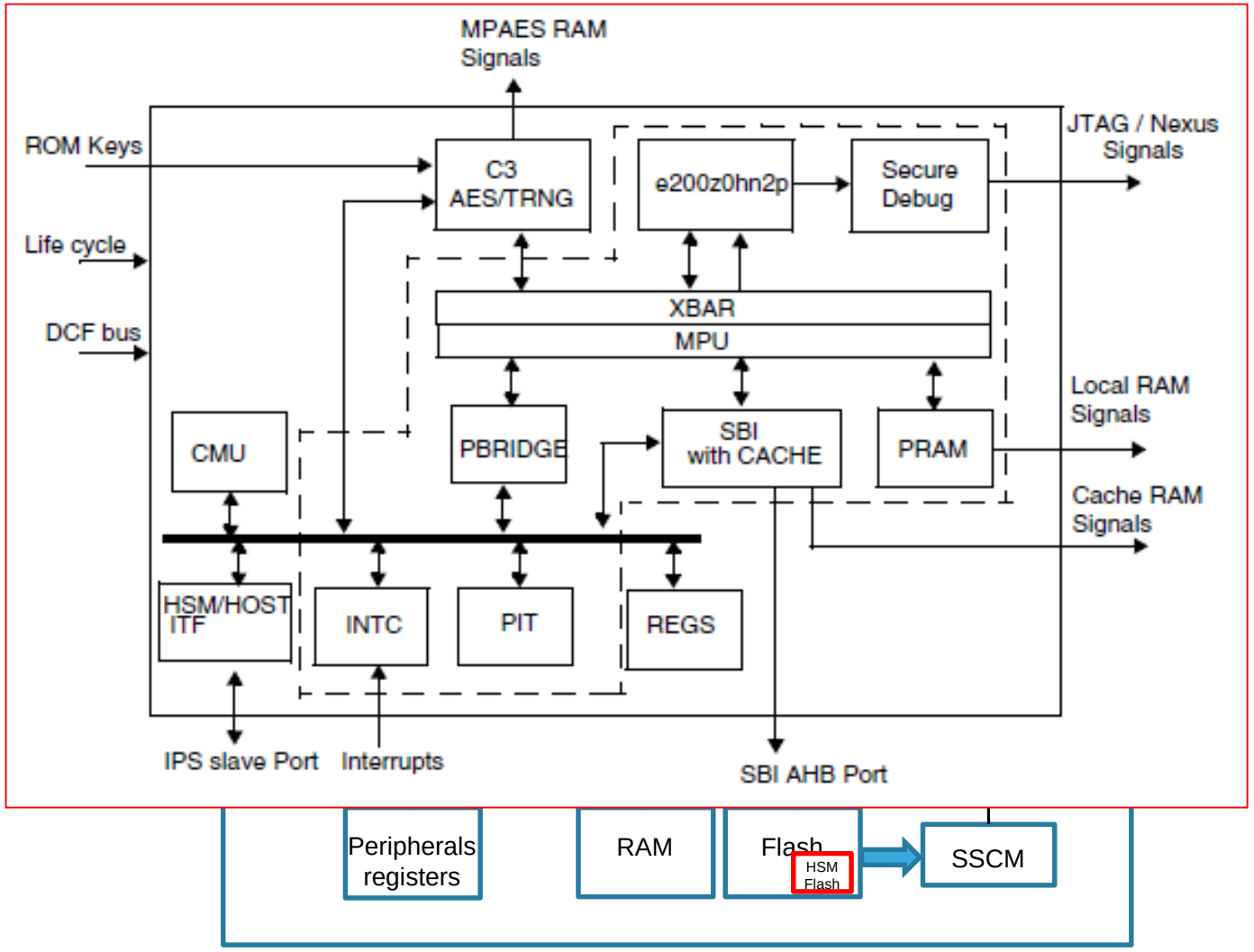
ST Microcontroller with HSM on board

- SPC58xB/C/G/N
- SPC58NH (Chorus 10M)

life.augmented

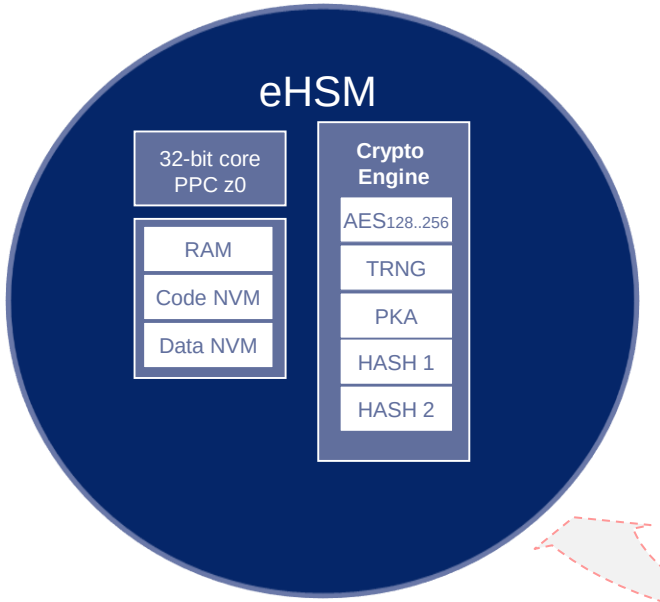
SPC57/SPC58 – HSM

- HSM module implements the EVITA MEDIUM
  - HSM is a protected sub system
  - User program and debug capabilities
- e200Z0 local CPU working at Max 100 MHz
  - Crossbar, with associated MPU
  - Interrupt controller
  - CMU (Clock Monitoring Unit)
  - HSM/HOST interface (async dual port register)
- Secure Debugger Interface
- Memory
  - SRAM 40 Kbytes
  - Flash
    code: 2 x 64 Kbytes + 1 x 16KBytes
    data : 2 x 16 Kbytes
- The TRNG embedded in the HSM complies with BSI AIS-31 and US NIST SP800-90B/C



life.augmented

HSM Evolution

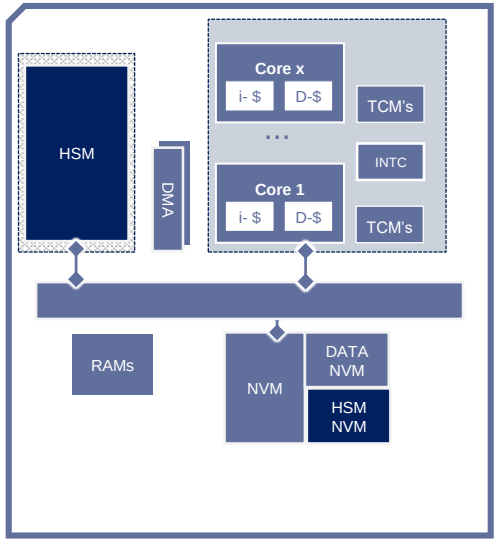


AES modes:
ECB, CBC, CTR, CMAC,
OFB, CFB, GCM, CCM, XTS

AES Key sizes:
128, 192, 256 bits

SP800-90B compliant

ECC over Gf(p) up to 640 bits
RSA up to 3072
SHA1, SHA224, SHA256, SHA384, SHA512

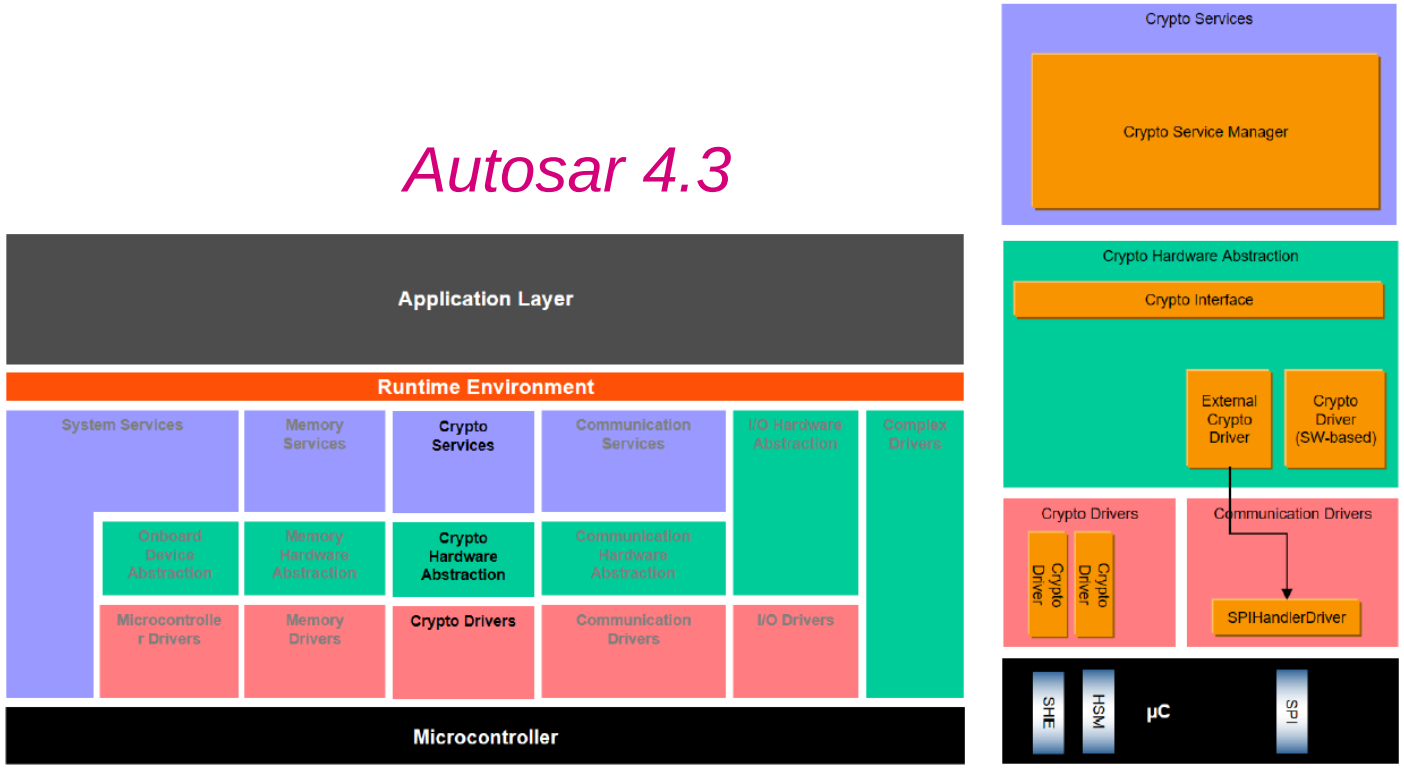


Chorus10M

AUTOSAR Crypto Support

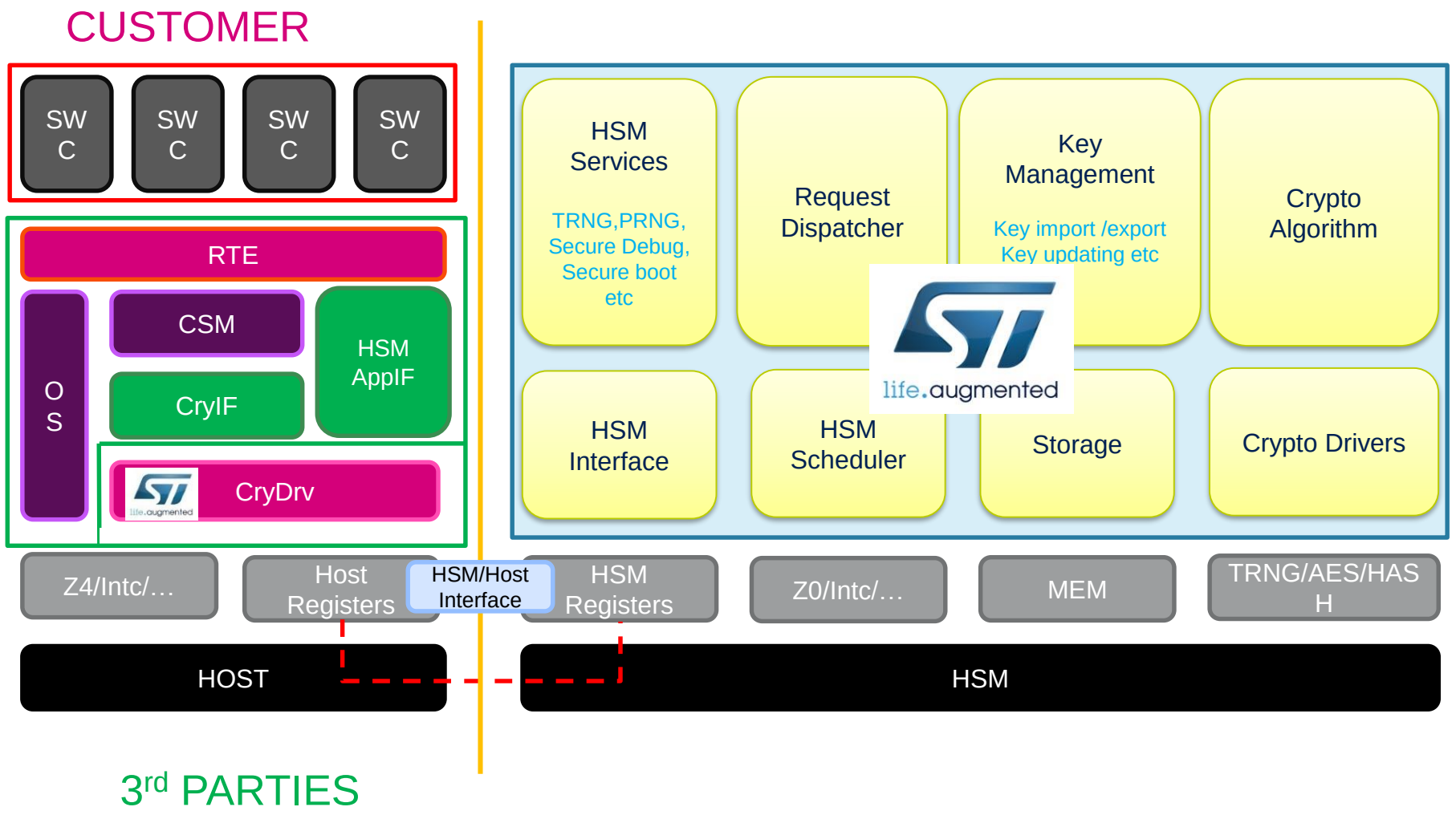
- The Crypto Driver module is located in the micro controller abstraction layer and is below the Crypto Interface module and Crypto Service Manager module. It implements a generic interface for synchronous and asynchronous cryptographic primitives. It also supports key storage, key configuration, and key management for cryptographic services.

Autosar 4.3



AUTOSAR Layered View with Crypto Driver Module

HSM SW Platform Architecture



Support for asymmetric cryptography (RSA, ECC, PKCS) and **HASH algorithms** (SHA256)

Chorus10M by HW

SHE+ service set

AES ECB, CBC, CMAC: by HW

ProMik Key Programming Solution

- ProMik is offering solutions for different approaches, they have implemented several solutions for different Tier1 and OEMs worldwide.

- ProMik offers on-board programming of flash devices.

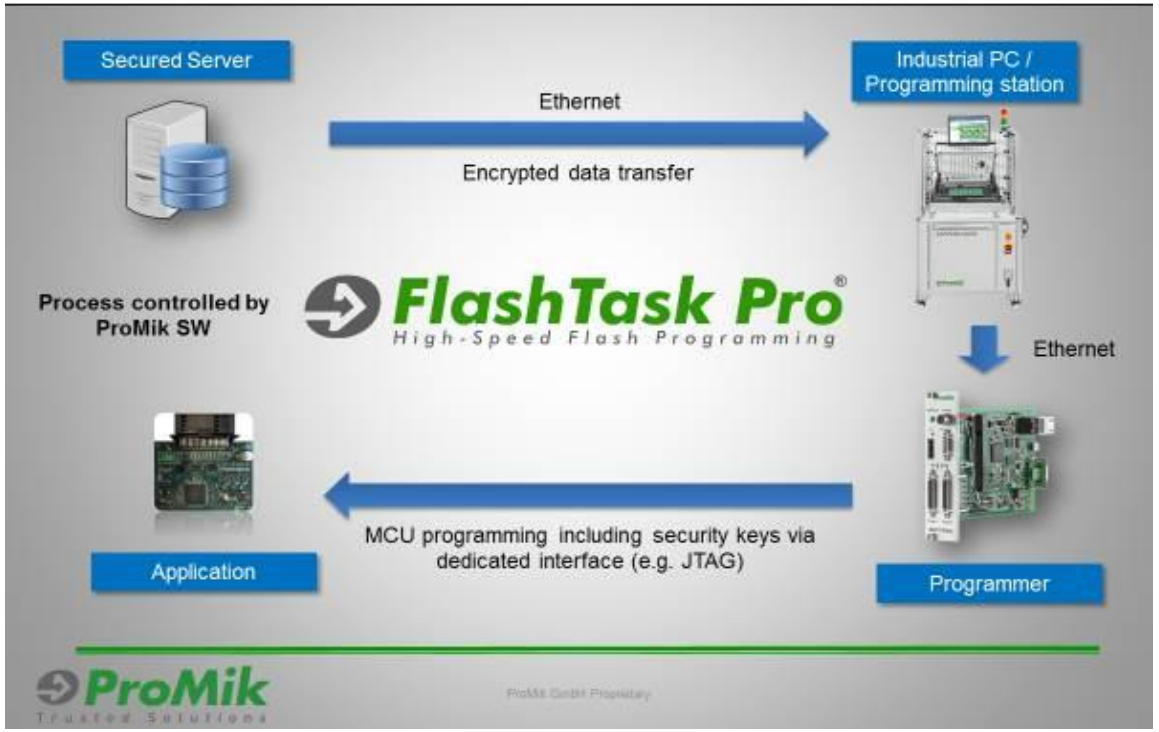
Cyber Security solution

ProMik`s production Software FlashTask Pro is running on a semi-automated programming station (ProMik`s SAP2100-AUTO).

Based on customer specifications the software is fetching keys from a secured server.

These keys are then programmed to the application via JTAG in a bed of needles using our MSP2100Net programmer.

Cyber Security in production



typical set-up of a manufacturing solution requiring key programming

Safety

life.augmented

ST MCUs Safety Concept Evolution

ASILD SEooC

The manufacturer may use the mark:

exida CERTIFIED ISO 26262 ASIL D

Certificate / Certificat
Zertifikat / 合格証

STM 1108067 P0028 C001

exida Certification S.A. hereby confirms that the:

MICROCONTROLLER SPC56EL60

STMicroelectronics
Agrate Brianza, Italy

Reports:
STM 11/08-067-C R011 V2 R1
Results of the ISO 26262 Functional Safety Assessment

Validity:
This assessment is valid for Microcontroller SPC56EL60

This assessment is valid until March 31, 2016.

V1 R0 March, 2013

Has been assessed per the relevant requirements regarding µC development and verification & validation of:

ISO 26262 : 2011 Parts 2, 4, 5, 7, 8, 9 and 10 (to the extent applicable)

and meets requirements providing:

Systematic Integrity: ASIL D

Safety related function:
The µC supports the execution of safety-related software by a dual-core lock-step architecture with memory protection and centralized fault collection and control unit.

Application restrictions:
The microcontroller shall be used per the Safety Application Guide requirements.

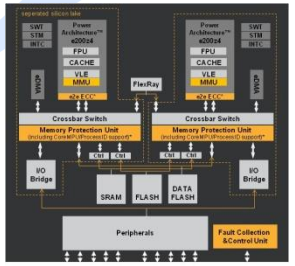
exida CERTIFICATION

Evaluating Assessor

Certifying Assessor

Page 1 of 2

GEN1 — 90nm - Leopard

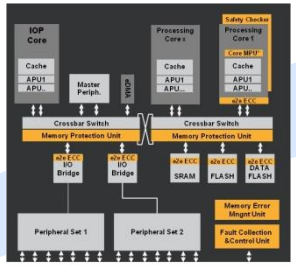


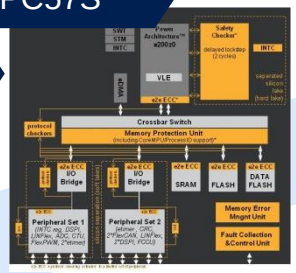
definition of a lead & generic ASILD Arch. certified ASILD by independant assessor

GEN2+ — 40nm – SPC58

GEN2 — 55nm – SPC57S

55nm – SPC57K





Safety Extend (DMA, INTC, peripherals, ..)

Redundant motor control & supply (SPC574S Sphaero)

Reduced cost of Safety
- e.g. end-to-end ECC instead of full replication

Increased Availability
- end-to-end ECC (correcting)
- Increased failure visibility/identification and reaction configurability for user recovery strategy (e.g. MEMU, enh´d FCCU)

GEN3 — 28nm – Stellar

Stellar

Real-time, deterministic virtualization & virtual ECU support
- HW based virtualization (CPU and overall architecture) built around Cortex-R52 new CPU privilege Hypervisor mode
- Up to 4 Error out channels

Increased configurability (cross domain family)

Increased Availability
(FDSOI, error localization and reaction configurability)

life.augmented

ASILD
SEooC

ASIL-D

Yes, we are !!!!

Really ?
Please, show me...

Safety Goal

ASILD
SEooC

Detect a fault and manage it within a constrained time

Ingredients for the safety “cake“ 

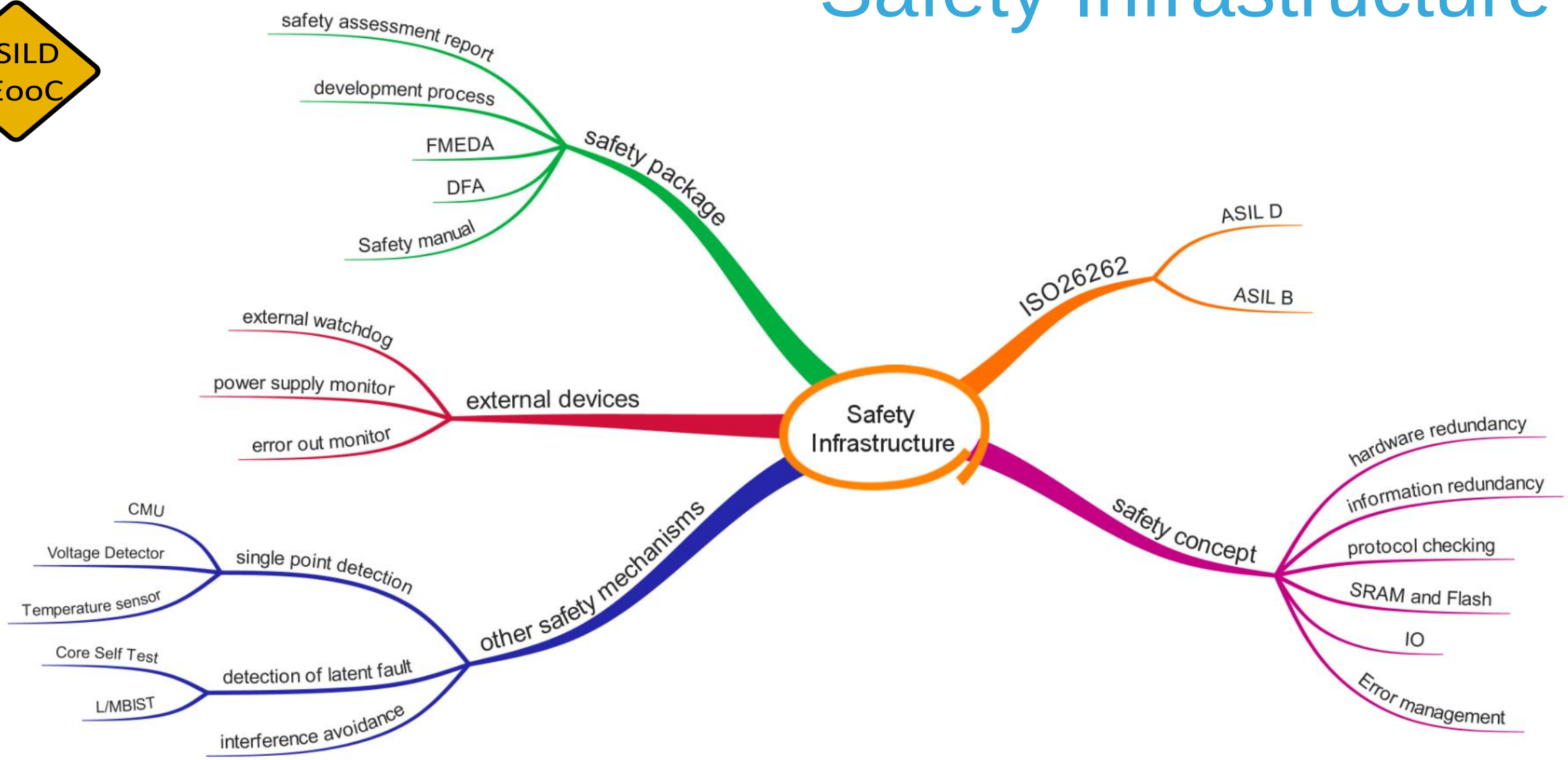
1. Safety monitors, checking the correct functionality of certain part of the silicon
2. Fault collector, receiving the errors reported by the safety monitors
3. Internal and external reactions, driven by the fault collector

A: Time to cook the “cake“ (FTTI : Fault Tolerance Time Interval) ?
10 ms for SPC58 family
B: How many faults can we detected, out of all the possible ones ?
Dictated by ISO26262 according to ASIL level
C: Safety monitor functionality coverage ?
Dictated by ISO26262 according to ASIL level

life.augmented

Safety Infrastructure

ASILD
SEooC



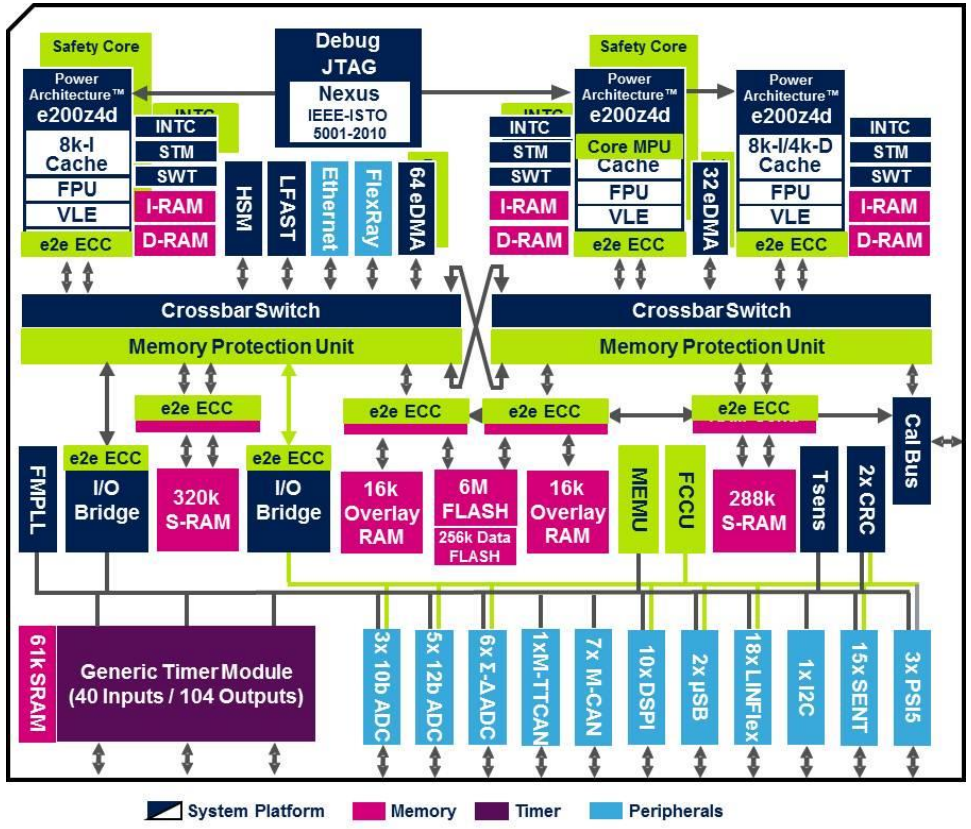
life.augmented

SPC5x High Performance Architecture

Answering System Safety Requirements

ASILD SEooC

Increasing safety system requirements are managed through state-of-the-art ASIL-D concepts



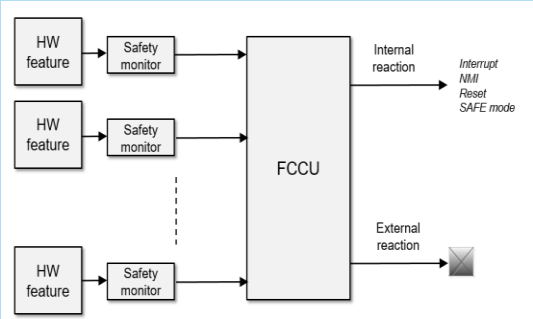
- True ASIL-D concept relying on HW measures
- Provide necessary HW support to implement the application dependent ASIL-D Concept
- Key pillars of SPC57/58 safety architecture:
  - ASIL-D Development Process in place during product development processes
  - Lockstep on each ASILD processing channel (Cores, DMA, Interrupt Controller)
  - Access protection at all Levels of the Architecture (MPUs, e2e ECC)
  - HW Built-In-Self Test for Memory, Logic and specific IPs
  - Clock, Power, Temp., Debug/Test signal supervisions
  - Fault Collection, Control and Identification

life.augmented

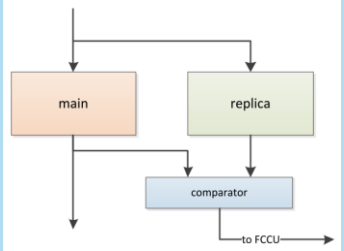
Safety HW Concepts

ASILD SEooC

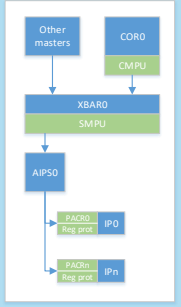
Fault collector



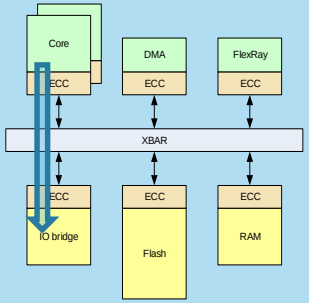
Redundancy



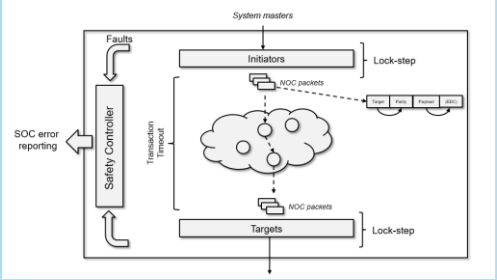
MPU



ECC & e2e ECC



NOC Protection

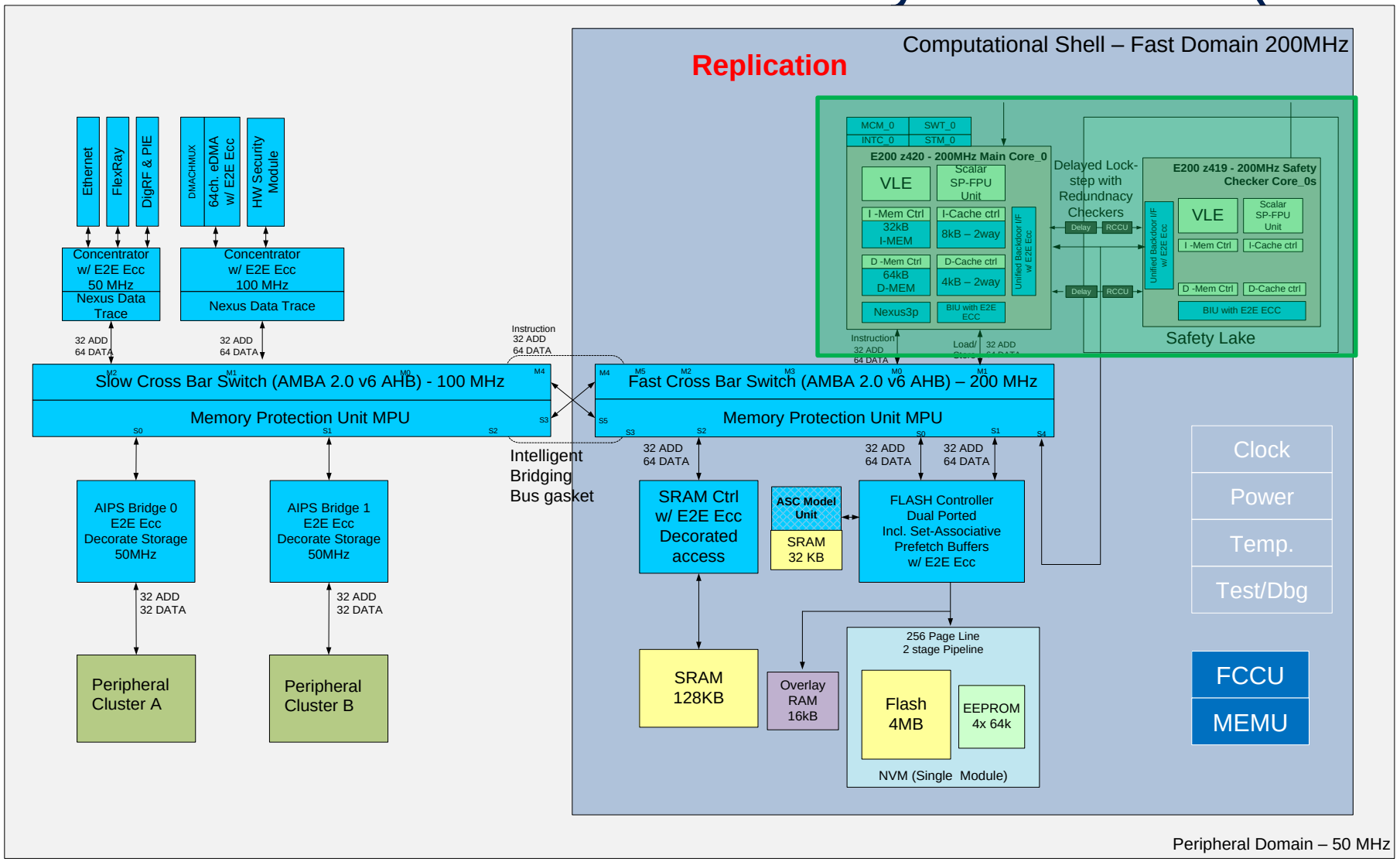


life.augmented

Safety Concept Overview

- MCU Safety Measures (ASIL D) -

ASILD SEooC

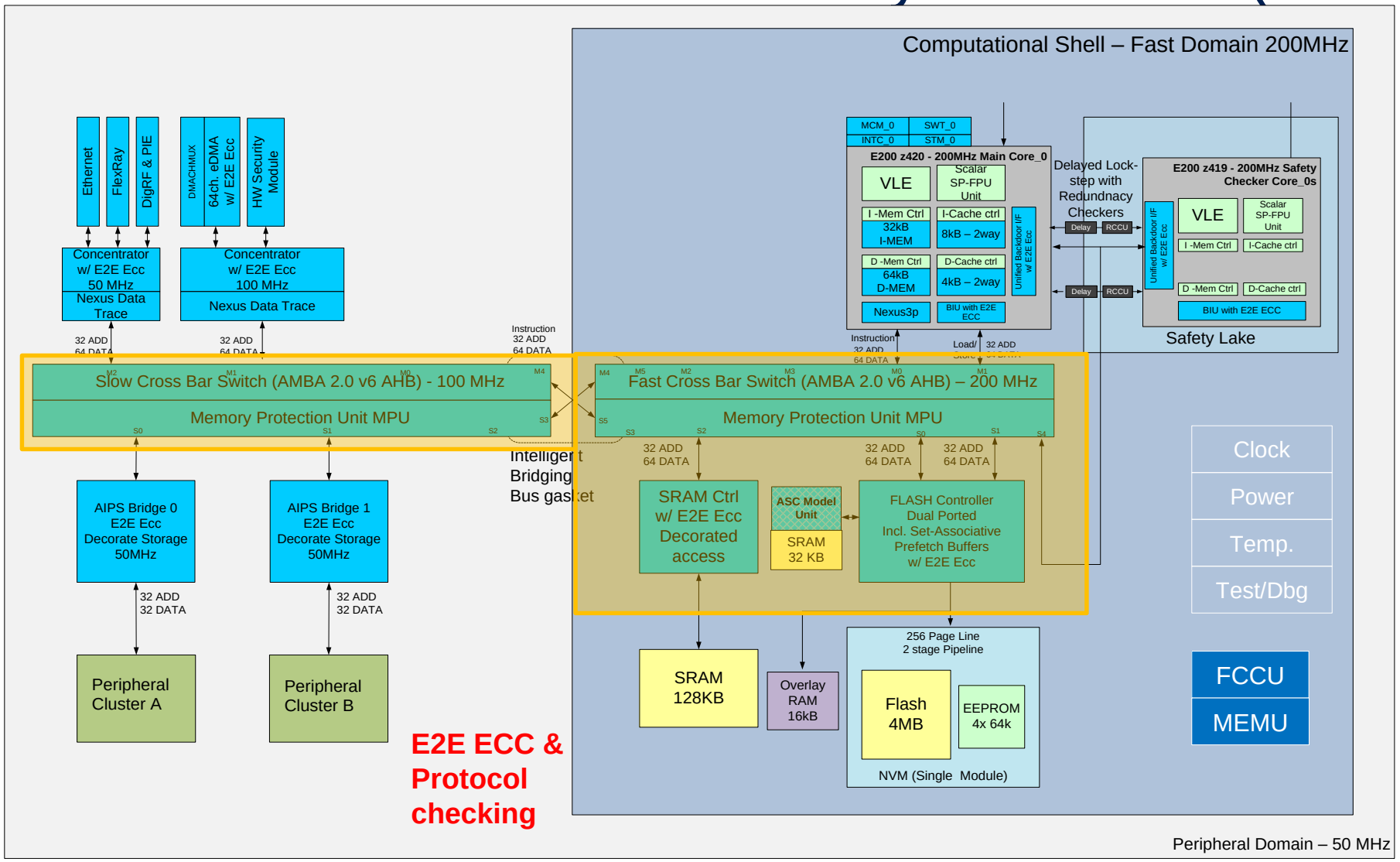


life.augmented

Safety Concept Overview

- MCU Safety Measures (ASIL D) -

ASILD SEooC

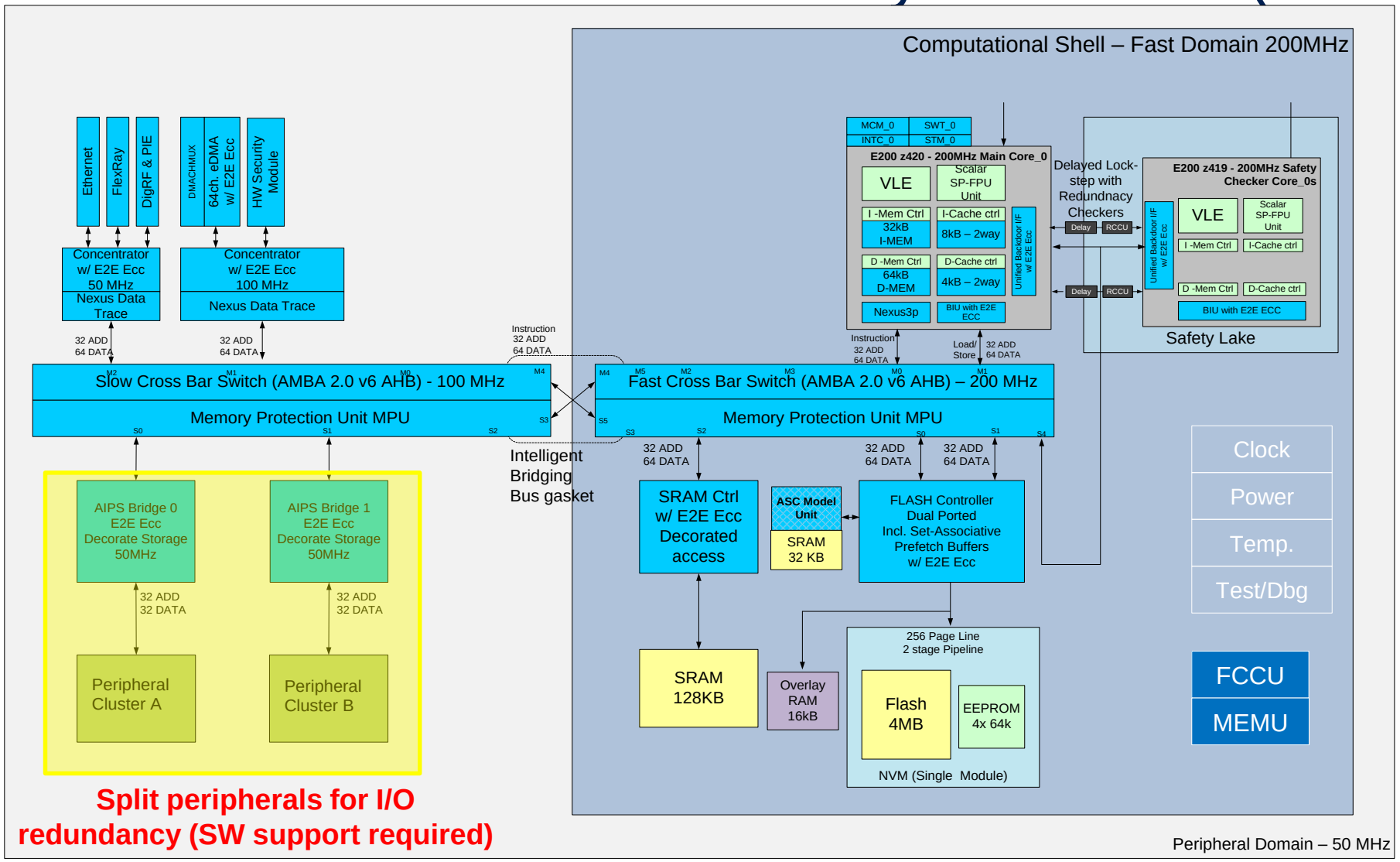


life.augmented

Safety Concept Overview

- MCU Safety Measures (ASIL D) -

ASILD SEooC



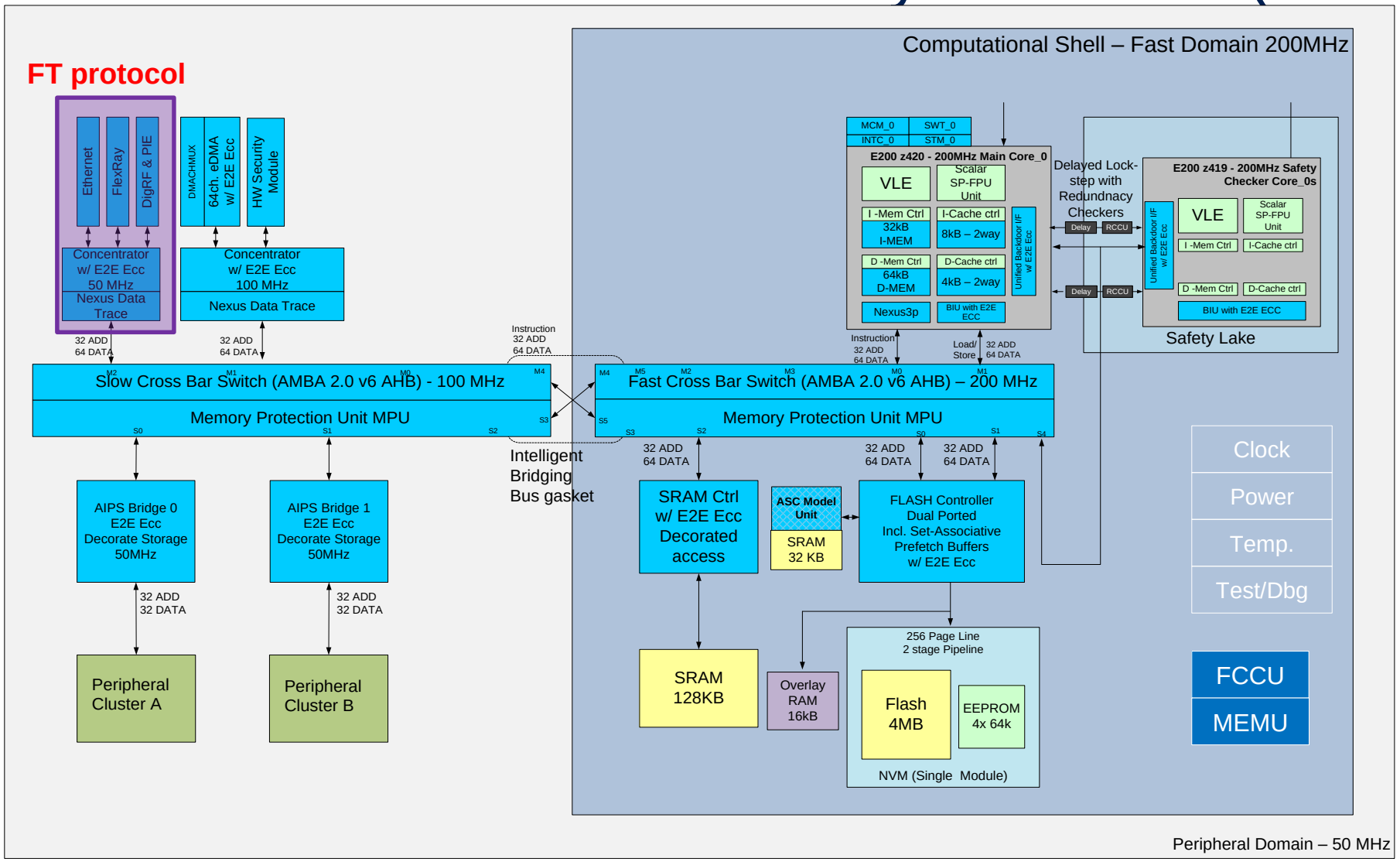
Split peripherals for I/O redundancy (SW support required)

life.augmented

Safety Concept Overview

- MCU Safety Measures (ASIL D) -

ASILD SEooC

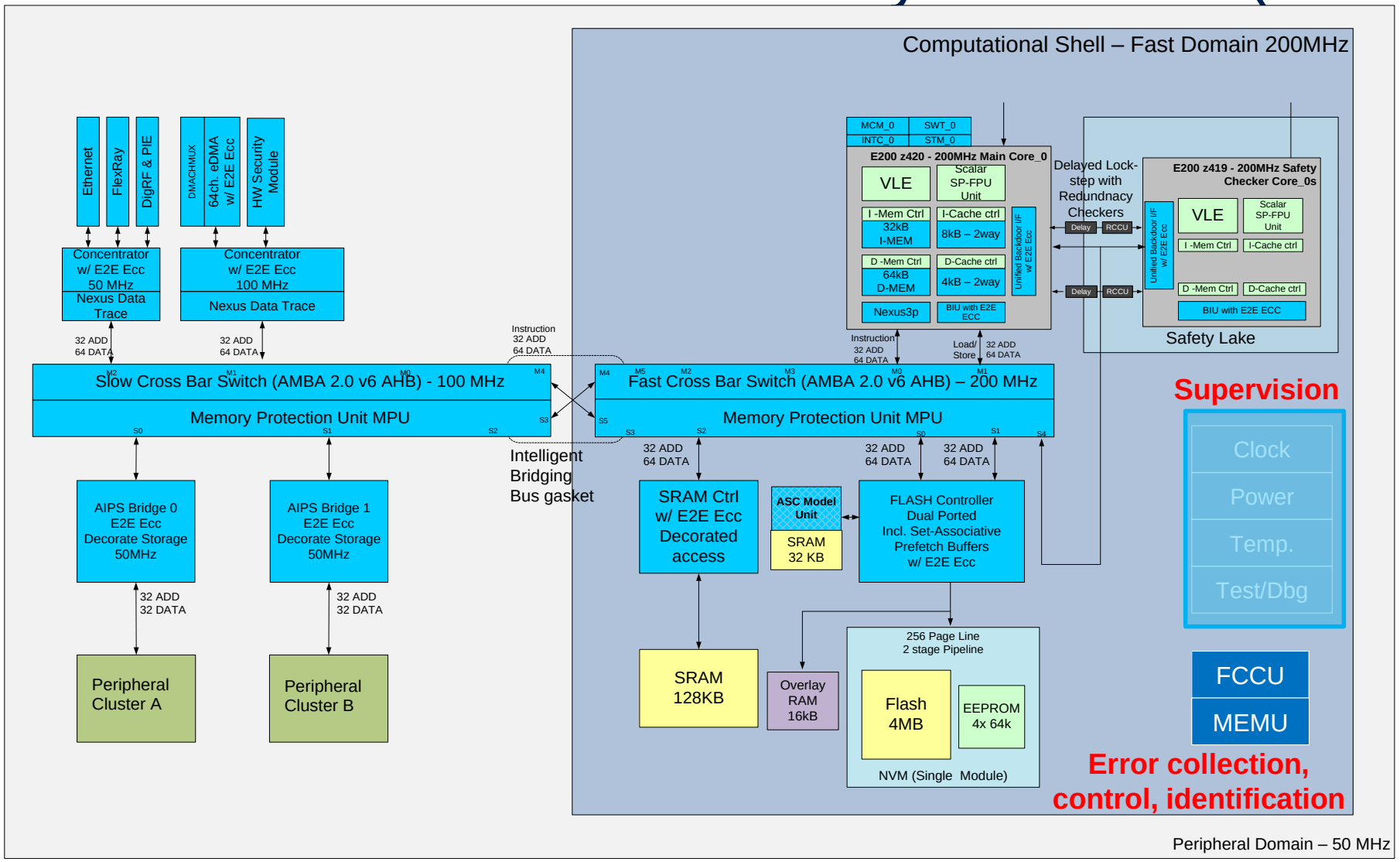


life.augmented

Safety Concept Overview

- MCU Safety Measures (ASIL D) -

ASILD SEooC

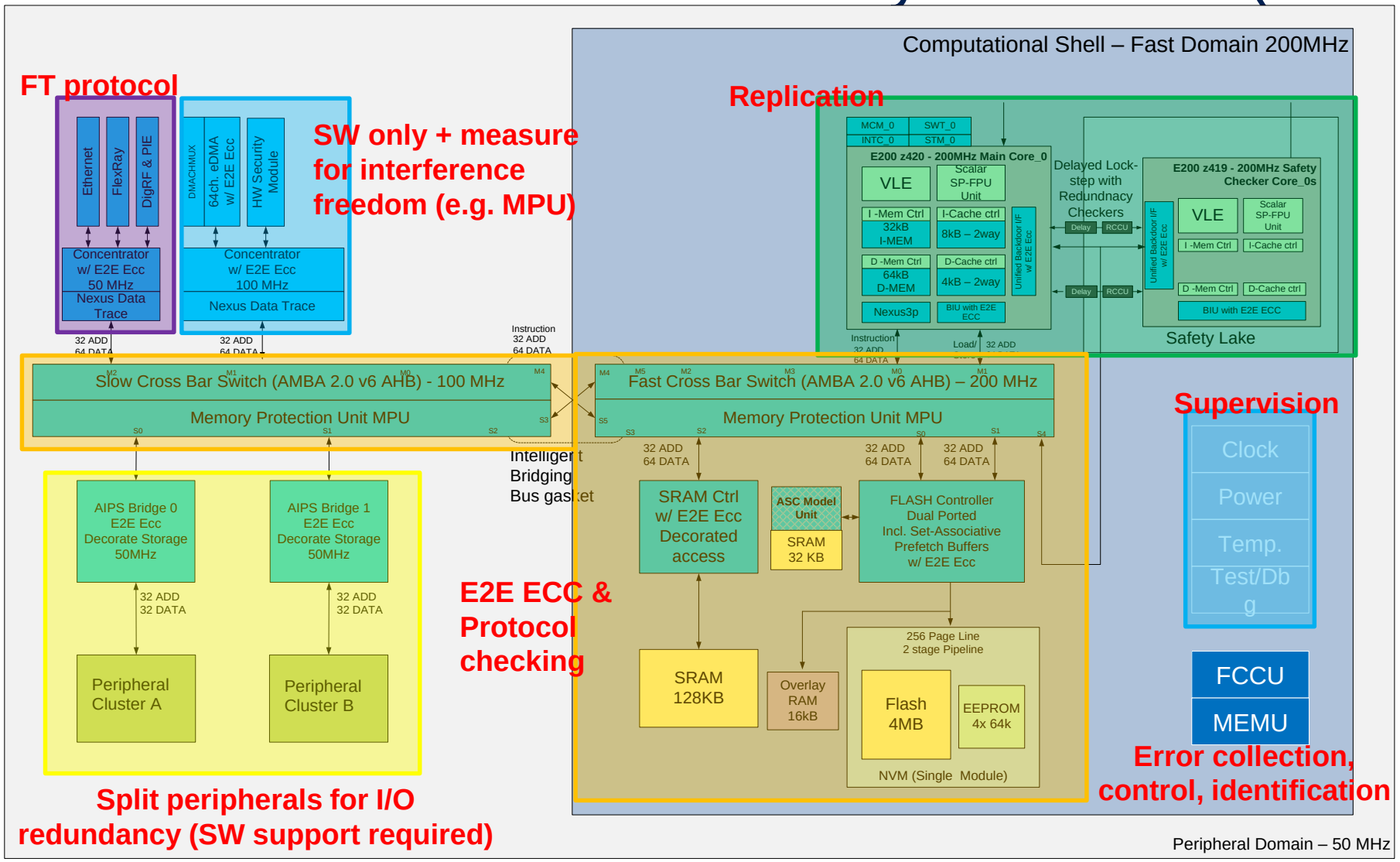


life.augmented

Safety Concept Overview

- MCU Safety Measures (ASIL D) -

ASILD SEooC



life.augmented

Safe MCAL SW Deliverables

MCAL Safety Level

ASIL C/D

- Qualification Report

ASIL A/B

- Static Analysis according to H
- Dynamic Test Coverage
  - Statement
  - Branch
  - MC / DC
- Safety Manual

Quality Managed

- User Manual (UM)
- Integration Manual (IM)
- MISRA Reports
- Traceability Matrix

Cu

datory

(1) **Certificate**

(2) Number of Certificate: **ZP/C033/18**

(3) Subject of inspection: **Conformity of software development processes for functional safety for automotive according to ISO 26262**

(4) Manufacturer: **STMicroelectronics Srl**

(5) Address: **Via Remo de Feo 1**
Arzano
Italy

(6) The certification body of DEKRA EXAM GmbH certifies that the subject of inspection has been found to comply with the essential requirements pursuant to the standard(s) referred in section 7. The examination and test results are recorded in the test and assessment report 20170323.

(7) The essential requirements are assured by compliance with the following standard(s):

ISO 26262:2011
(up to and including ASIL D)

(8) This certificate only relates to the subject of inspection in accordance with the mentioned standard(s). Further requirements of the ISO 26262 apply to the application and execution of the software development process. These are not covered by this certificate.

(9) This certificate is valid until 2021-10-30.

DEKRA EXAM GmbH
Bochum, 2018-10-31

Certification body

Special services unit

MCAL Certificate

Work Product	Format	Nb of instances	Delivered to Customer for QM MCAL	Delivered to Customer for ASIL A/B MCAL	Delivered to Customer for ASIL C/D MCAL
MCAL plugins	.zip	one per product	X	X	X
CDD safety plugin	.zip	one per product			On request
CDD plugins	.zip	one per product	X	X	X
				X	X
			On request	On request	On request
			On request	On request	On request
			X	X	X
				X	X
				X	X
					X
			X	X	X
			X	X	X
			On request	On request	On request
			X	X	X
			X	X	X
			X	X	X
			X	X	X
			X	X	X
			On request	On request	On request
			X	X	X
			X	X	X
				X	X
				X	X
			On request	X	X
			X	X	X
			On request	On request	On request
Release Note	.PDF	one per product	X	X	
compiler options for doc generation	.XML	one per product			

ASILB SEooC

(*) *Provived that compiler / Linker options as for QM package and no HFs requested*

life.augmented

Safety Solutions in a Nutshell

ASILB SEooC

ASILD SEooC

ISO 26262

Software

Hardware

DIA Required

SW-C | SW-C | ------ | SW-C

RTE

BSW

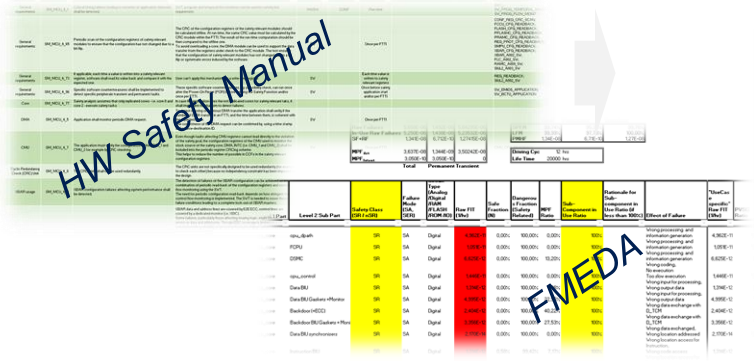
MCAL-SQ(*)

External WDG
Voltage Monitoring
Error Out monitoring

Core Self Test

MCAL Safety Quality Package

MCAL Certificate



HW Safety Manual

FMEDA

DFA

Safety assessment Report

life.augmented

What you takeaway from ST 32-bit MCU?

Functional Safety

- HW Safety mechanism
- Safety SW ecosystem
- Fail safe architecture
- Fault collection and reaction

Security

- Protection & authentication
- Isolation
- Encryption & Decryption
- Secure data storage & routing

FOTA

- Flash context manage by HW
- Interface for external memory
- Ultra fast communicate interface
- Advanced security features

DATA Routing

- Ethernet back-bone network
- Diversity network interface
- HW gateway data routing
- Global time synchronization

Computation Capability

- Performance
- Power
- Diversification
- Fault manage & self-test

life.augmented

life.augmented

Lunch

G层广场咖啡厅

微信号：意法半导体Automotive