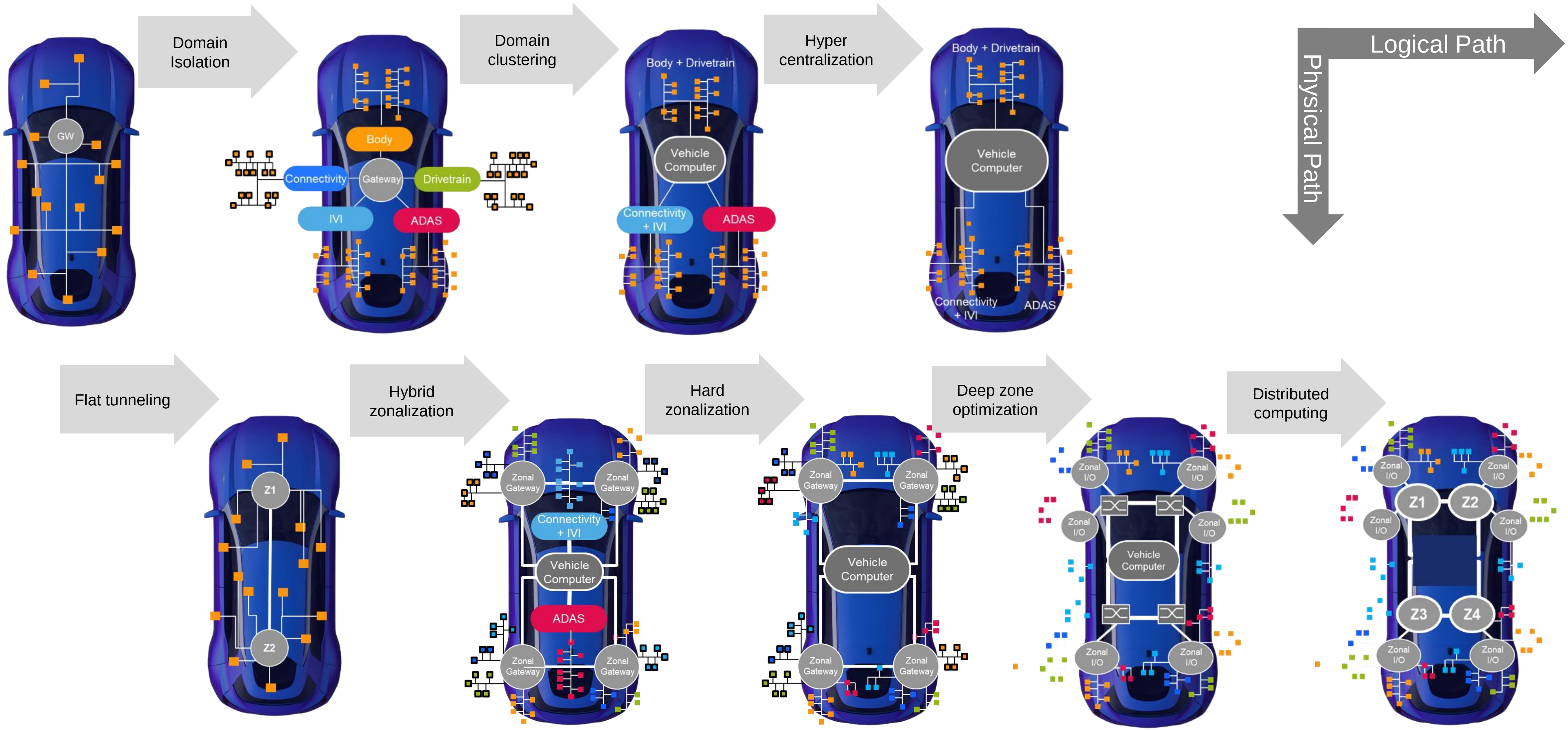
TRANSITIONING TO A SAFE AND SECURE ZONAL ARCHITECTURE

S32G Vehicle Network Processor as the Foundation

GUARDKNOX | Green Hills SOFTWARE | NXP

Automotive E/E Architecture Evolution Paths: Logical and Physical



Domain Isolation

Domain clustering

Hyper centralization

Logical Path

Physical Path

Flat tunneling

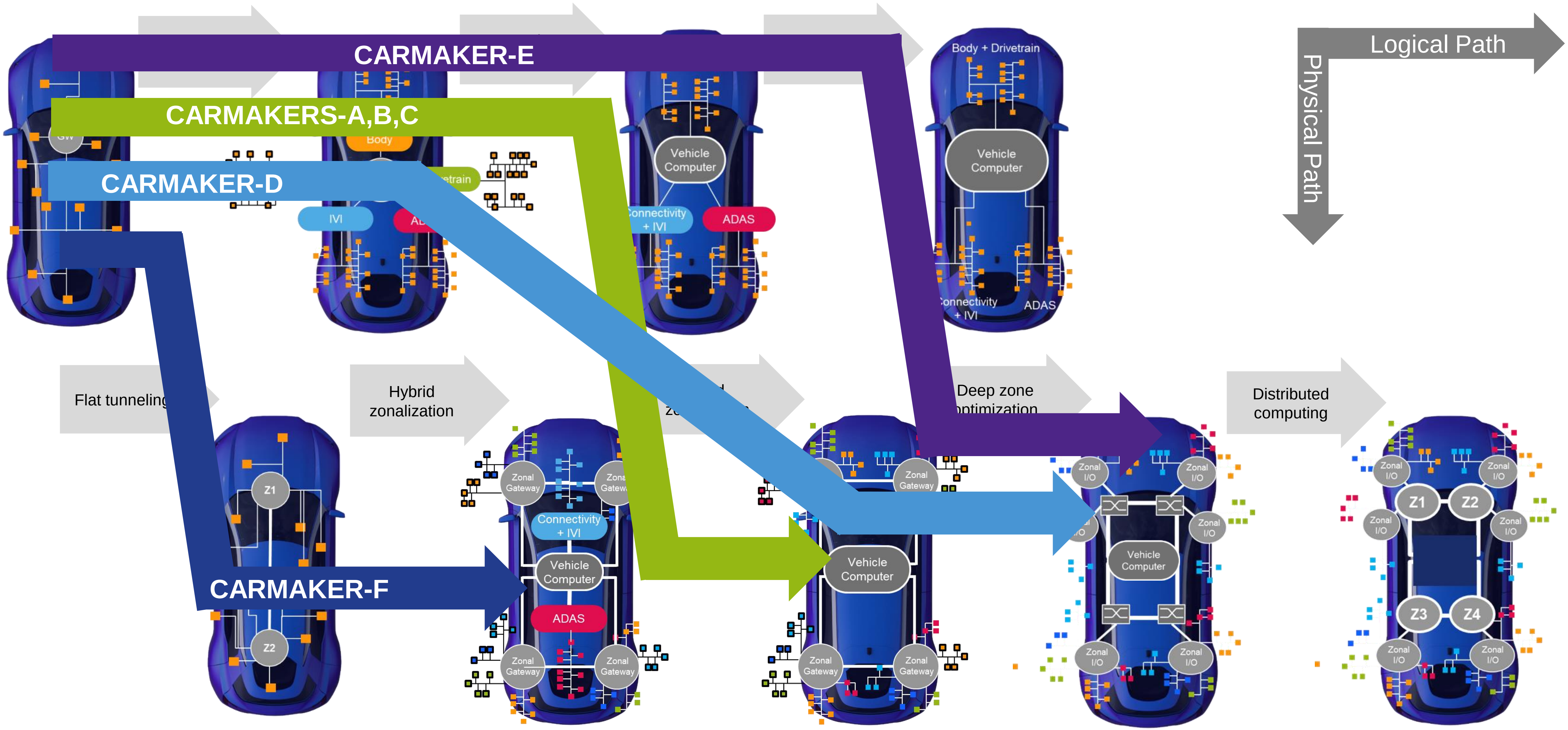
Hybrid zonalization

Hard zonalization

Deep zone optimization

Distributed computing

Potential Automotive OEM Architecture Migration Paths → Logical + Physical



OVERVIEW

- We're tasked with transitioning legacy to Zonal E/E Architecture
    - GuardKnox will assume the role of OEM engineering
- We'll have a workshop with suppliers
    - NXP and Green Hills Software

APPROACH

- WHY … ?
- WHAT … ?
- WHERE … ?
- HOW … ?
- WHEN … ?

WHY?

PROBLEMS & CHALLENGES

SCALABILITY WALL

- Too many ECUs
- Too much wiring
- Limited network configurations
- Coupled functionality

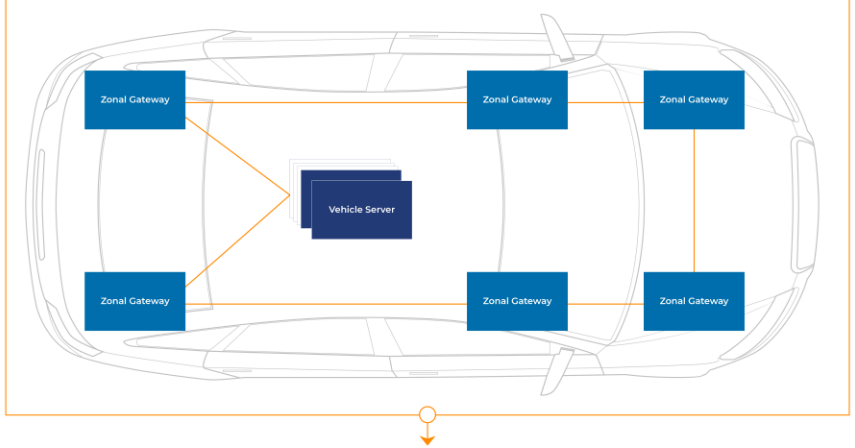
INDUSTRY LANDSCAPE

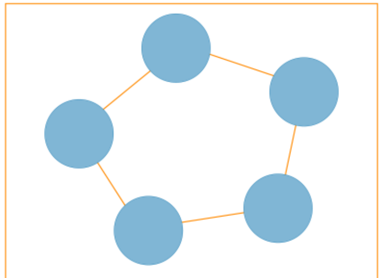
- New propulsion
- New consumer
- New competitors
- Upcoming regulation

THE AUTOMOTIVE INDUSTRY IS IN THE MIDST OF A PARADIGM SHIFT

ETHERNET BACKBONE – TOPOLOGY OPTIONS

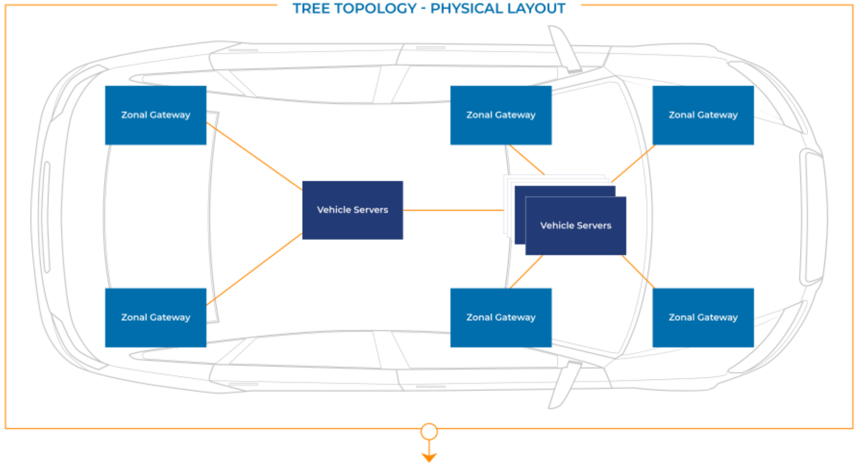
PHYSICAL TOPOLOGY

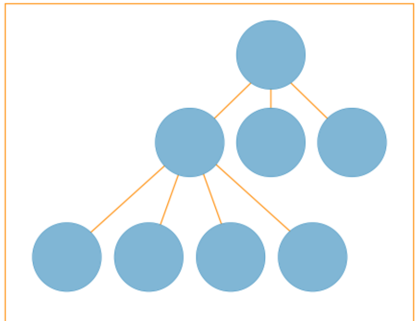




LOGICAL TOPOLOGY

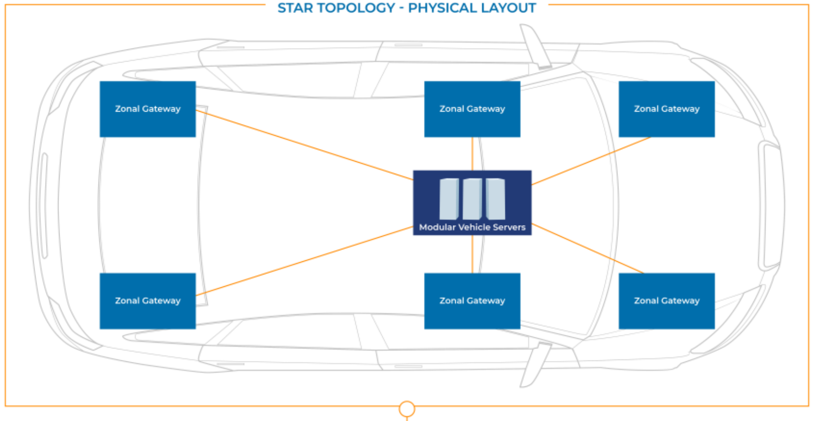
TREE TOPOLOGY - PHYSICAL LAYOUT

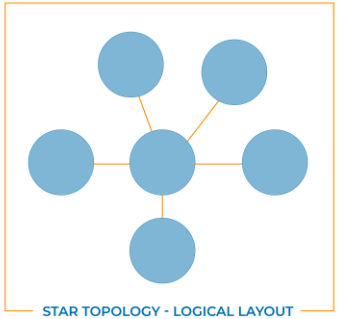




TREE TOPOLOGY - LOGICAL LAYOUT

STAR TOPOLOGY - PHYSICAL LAYOUT

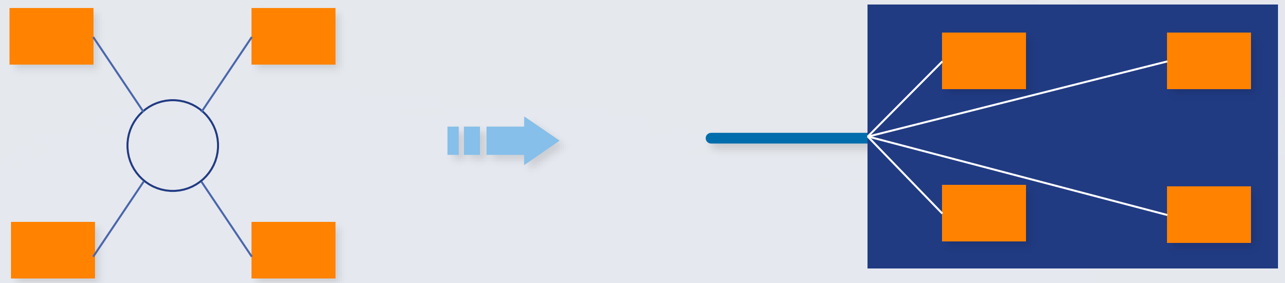




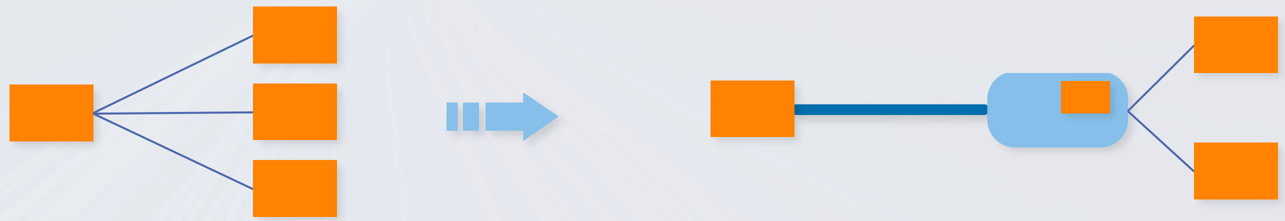
STAR TOPOLOGY - LOGICAL LAYOUT

ZONAL ARCHITECTURE DEVICE CLASSES

VEHICLE SERVER
(general purpose computer)



ZONAL GATEWAY
(localized connectivity hub)



🟧 ECU ○ CAN ▣ Vehicle server ▬ Ethernet ▢ Zonal Gateway

GOALS

01 END UP WITH A ZONAL ARCHITECTURE

02 REDUCE COSTS AS FAST AS POSSIBLE

03 BACKWARD AND FORWARD COMPATIBLE

WHAT?

WHICH DEVICE?

VEHICLE SERVER – ECU REDUCTION

- Transition to server(s)
- Network agnostic
- Agnostic to physical layout
- Cost reduction for any car
- Scales up / down
- Major impact on cost (engineering)

MEETS OUR GOALS

VS.

ZONAL GATEWAY – WIRING REDUCTION

- Introduce new gateway(s)
- Changes to backbone
- Depended on physical layout
- Cost reduction for wiring burdened car
- Unclear scaling
- Some impact on cost (material and labour)

WE'LL KEEP THAT IN MIND

OBJECTIVES

CONSOLIDATED PLATFORM

- Function = software package
- Stop ordering individual ECUs

DE-FRAGMENT ECO-SYSTEM

- Runtime environments and versions
- Shorten development, certification and integration times

FUTURE PROOF

- Single design fits many use cases
- Incremental functionality development

COMMONALITY

- Powertrain = µC + Interfaces
- Cockpit = µP + µC + Interfaces + GPU
- Connectivity = µP + Interfaces + Wireless
- Body = µP + µC + Interfaces
- Autonomy / ADAS = µP + µC + Interfaces + Vision / GPU
- Battery = µC + Interfaces + PLC / Wireless
- Gateway = µP + µC + Interfaces
- Legacy = µP / µC + Interfaces + ASICs

SERVER = µP + µC + Interfaces

WHERE?

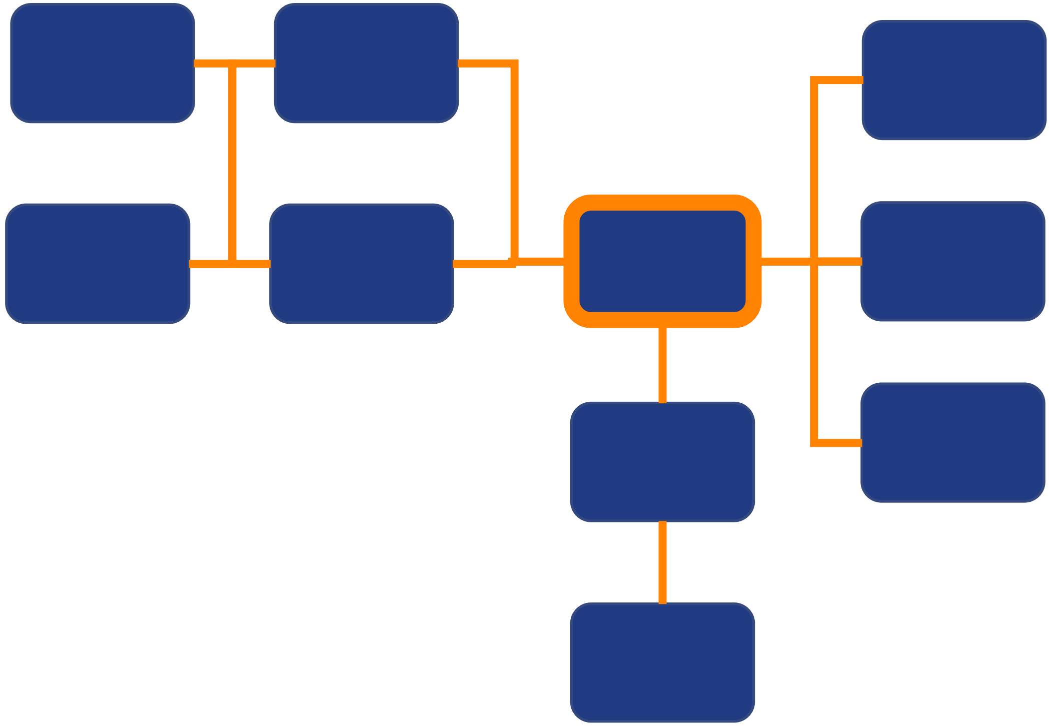
CONSTRAINTS

- Replace an existing ECU
- Biggest network outreach
- Place to scale

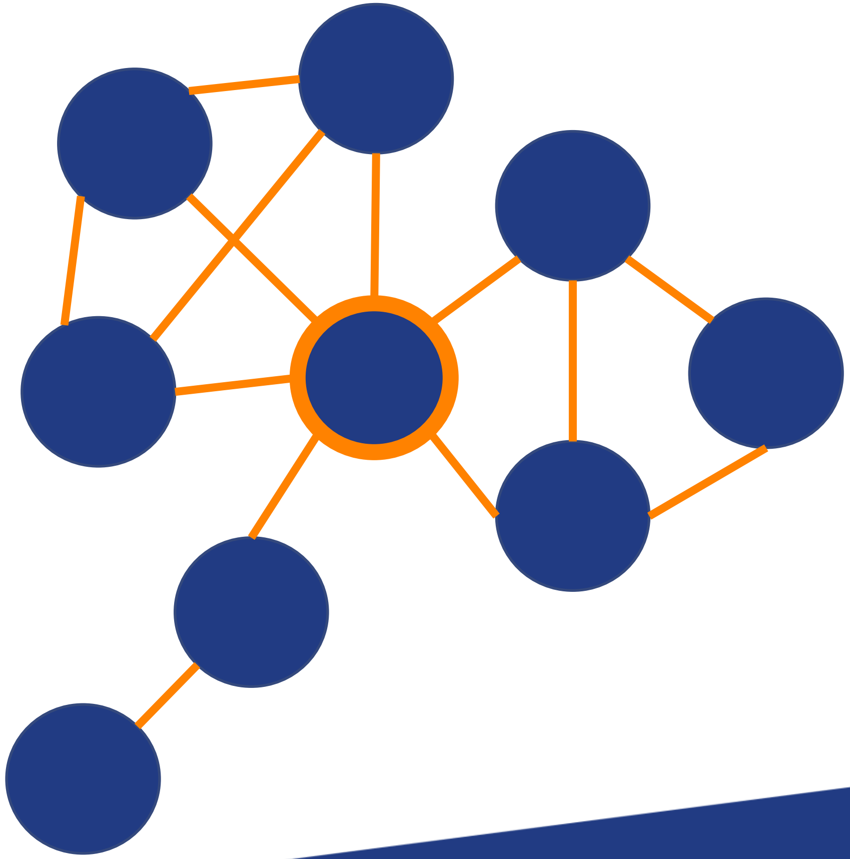
"CENTRAL" EXISTING ECU → SERVER PLATFORM

GATEWAY ARCHITECTURE

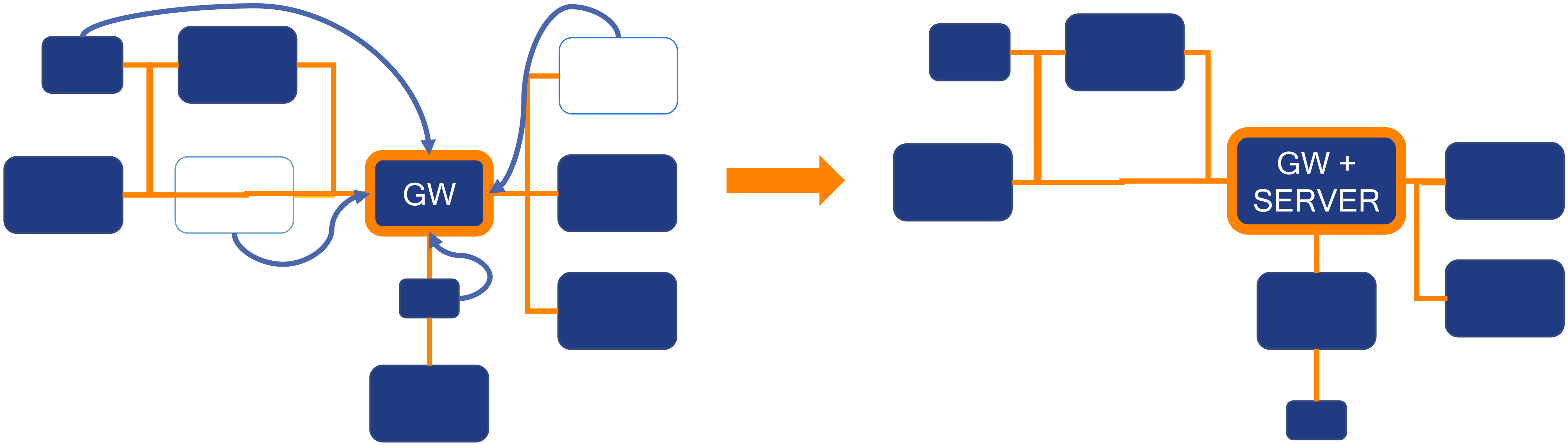
BLOCK DIAGRAM



NETWORK TOPOLOGY
(STAR-ISH)

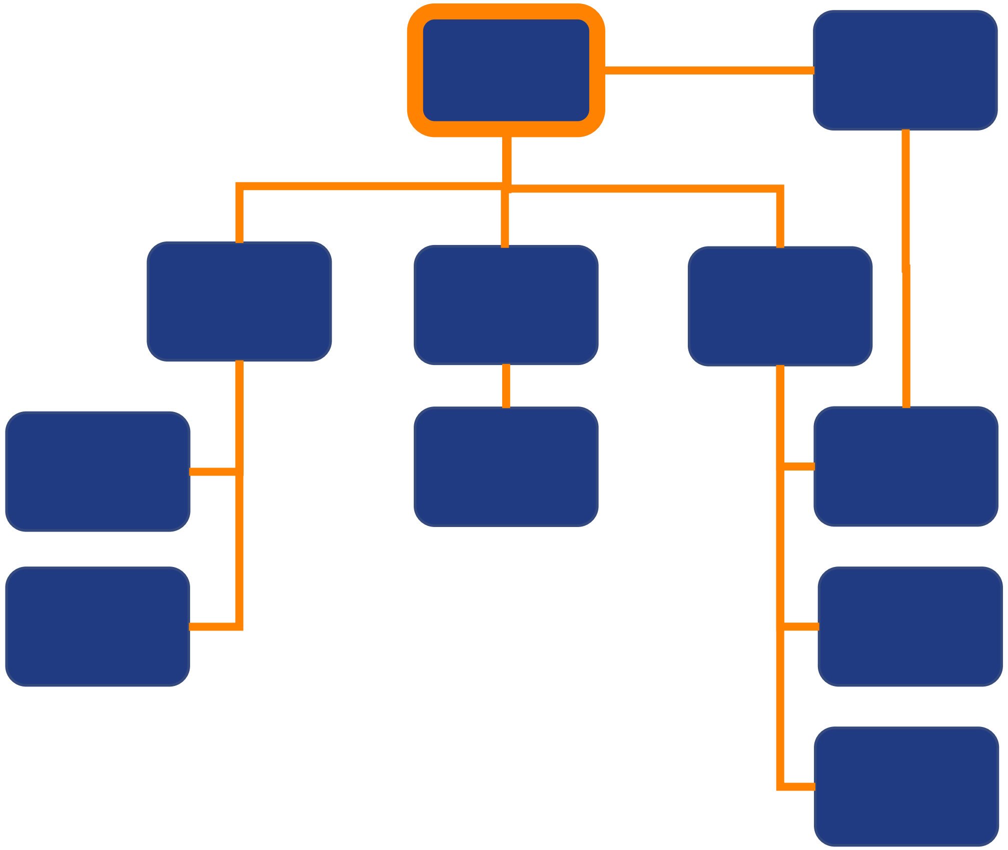


GATEWAY TO ZONAL

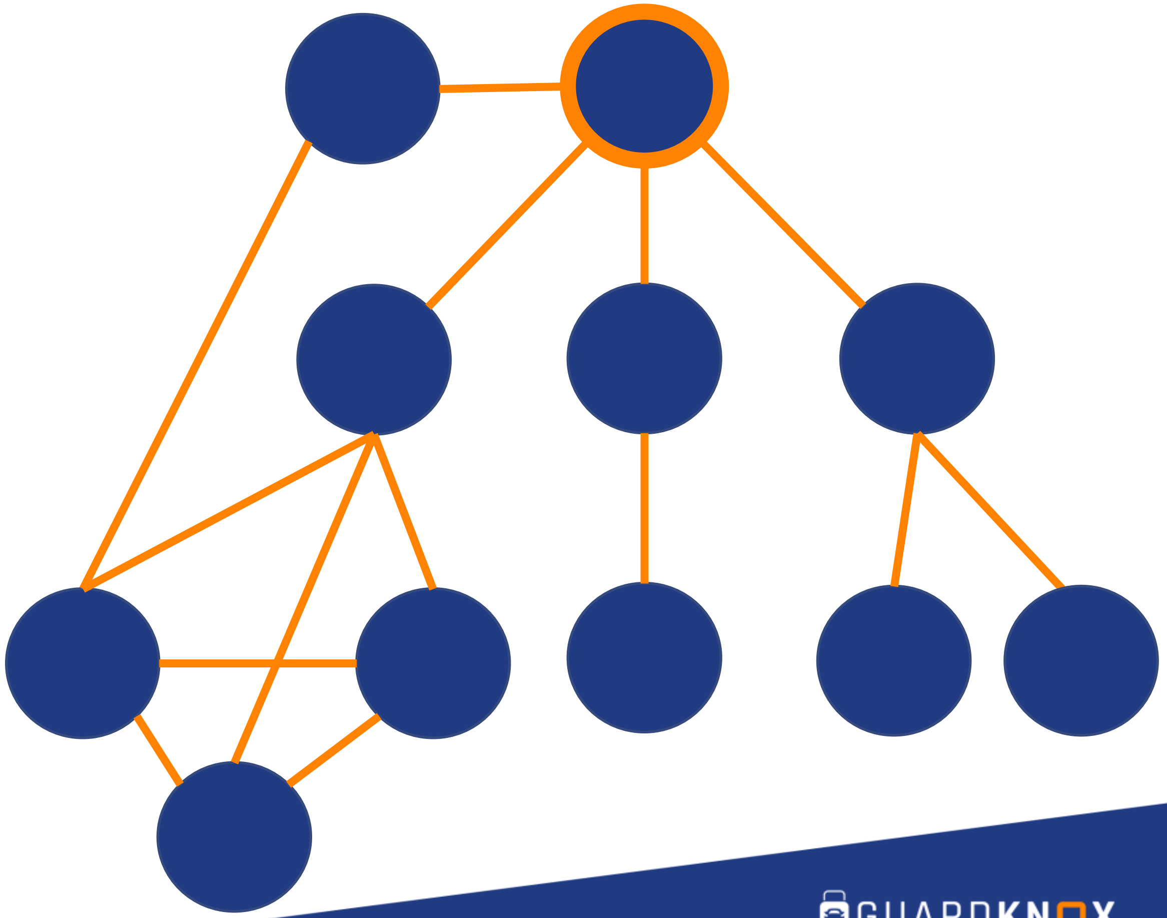


DOMAIN CONTROLLER ARCHITECTURE

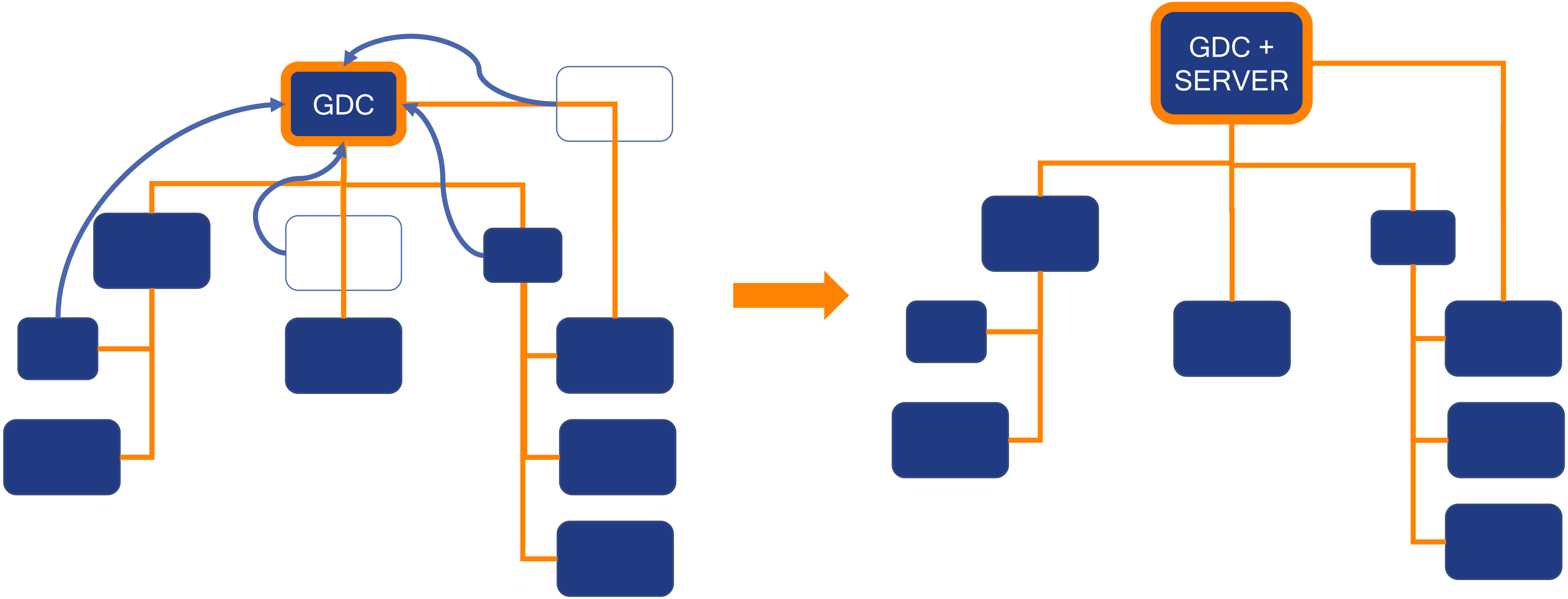
BLOCK DIAGRAM



NETWORK TOPOLOGY
(TREE-ISH)



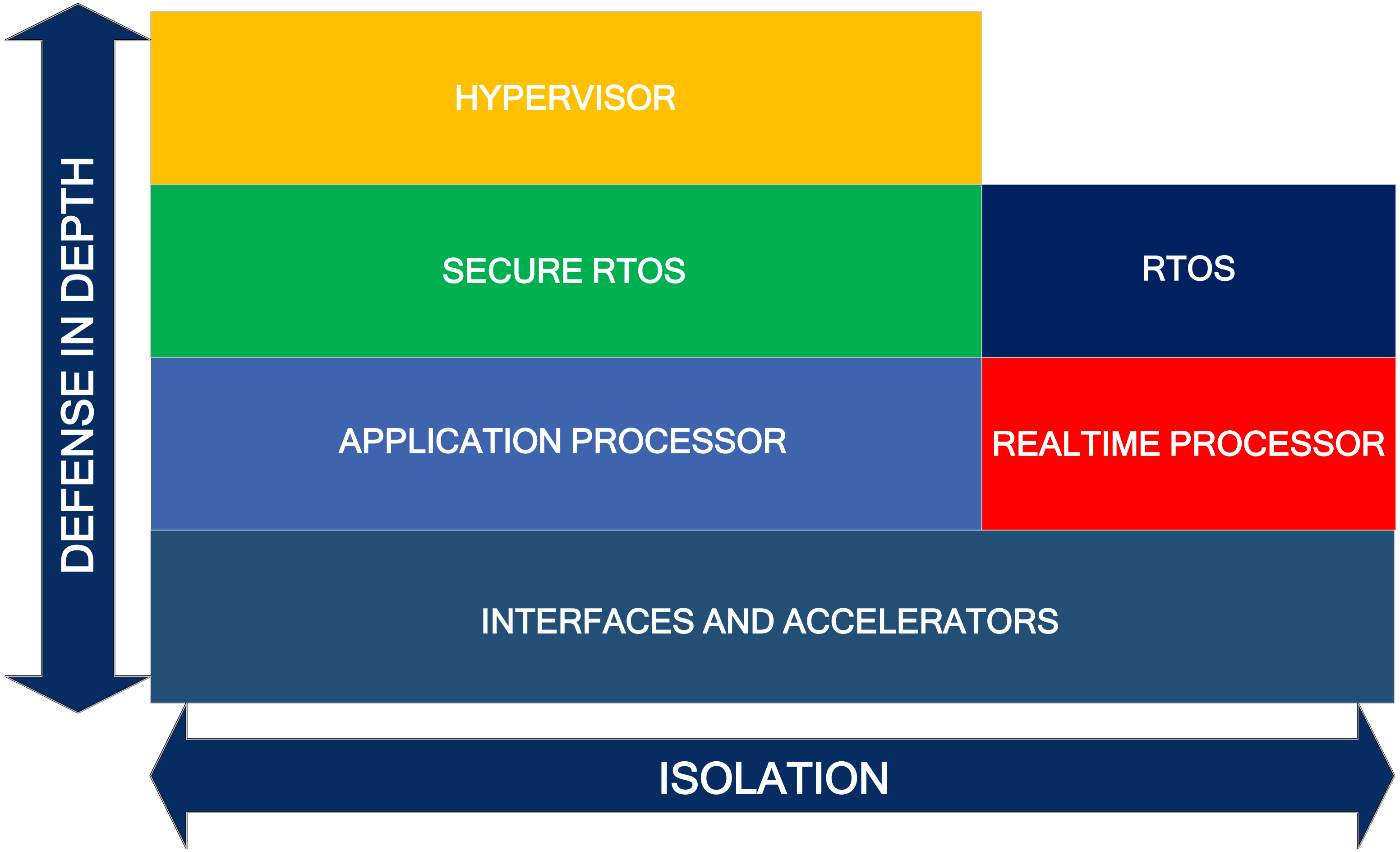
DOMAIN TO ZONAL



HOW?

VEHICLE SERVER "TEMPLATE"

- Consolidated
  - Single SoC
  - Software modules
- Mixed criticality
  - Safety
  - Security
- Scalable
  - Clustering
  - Device family
  - Runtime environments
- Secure (inclusive safety)
  - Defense in depth
  - Logical / physical isolation



REQUIREMENTS

01 Micro-processor (application)

02 Micro-controller (real-time)

03 Up to ASIL-D (applications are unknown)

04 All automotive interfaces (legacy and Ethernet)

05 Multiple runtime environments (hypervisor / processors)

06 Scalable platform (hardware family variants)

07 Strong isolation (safety and security)

08 NO APPLCATION RE-DEVELOPMENT!

S32G is a New Type of Automotive Processor: Vehicle Network Processor

PROCESSING

Lockstep Microcontrollers

Cluster Lockstep Microprocessors

Automotive Networks Acceleration

Ethernet Packet Acceleration

NETWORKING

20 x CAN/CAN FD Interfaces

LIN and FlexRay™ Interfaces

4 x Gigabit Ethernet Interfaces

PCI Express Gen 3 Interfaces

SAFETY & SECURITY

ASIL D Functional Safety Support

Advanced Hardware Security Engine

APPLICATIONS

Service-oriented Gateway

Domain Controller

ADAS/AD Safety Controller

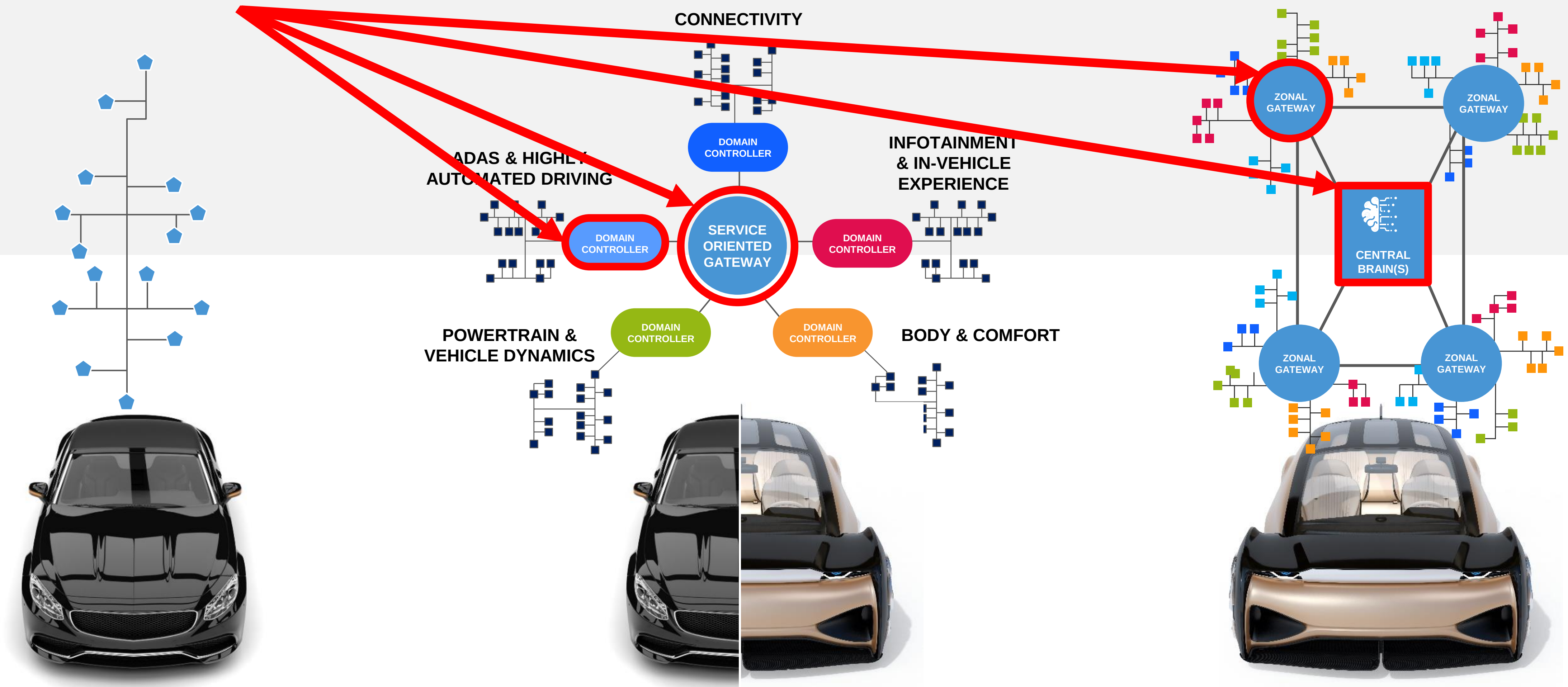
Vehicle Compute / Zonal Gateways

SAFE ASSURE by NXP

EDGELOCK™ ASSURANCE by NXP

www.nxp.com/S32G

S32G Processor Supports Vehicle Architecture Transformation



LEGACY APPROACH | FLAT

UNFIT TO FUTURE MOBILITY – SECURITY AND SCALABILITY ISSUES

Low bandwidth,
one MCU per application

LOGICAL RESTRUCTURE | DOMAINS

ENABLING SCALABLE GROWTH, CONSOLIDATION AND NEW FEATURES LIKE AUTONOMOUS VEHICLE

High bandwidth network
Gateway key to communication between domains
Domain Controllers for local networking and ECU consolidation

PHYSICAL RESTRUCTURE | ZONES

REDUCING WIRING COMPLEXING AND ENABLING THE USER-DEFINED CAR

Domains virtualized by SW – enabling high flexibility
Easy enable/disable or update functions

S32G274A: ASIL D Vehicle Network Processor

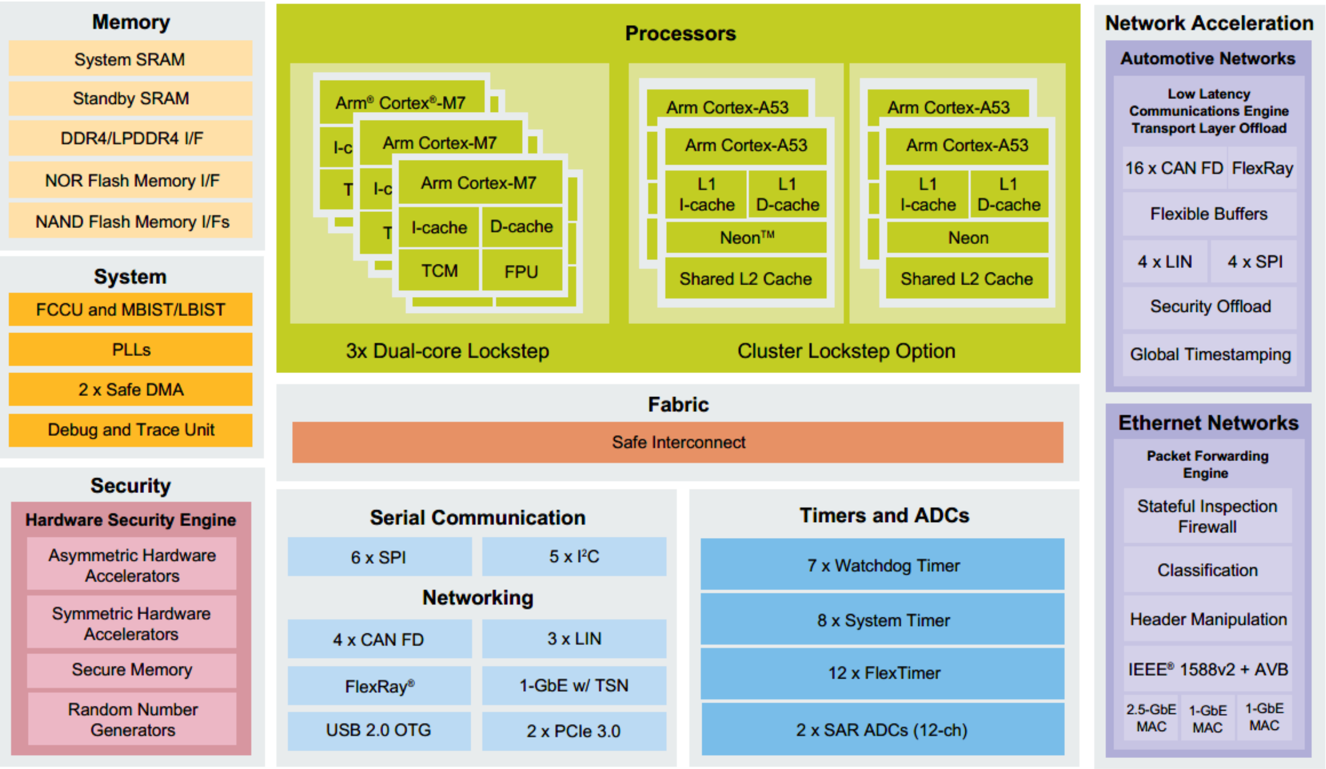
On-the-Fly Secure External Flash Memory

Functional Safety Design

Embedded Hardware Security with PKI Support

MCUs for real-time processing

MPUs for apps and services



Memory
- System SRAM
- Standby SRAM
- DDR4/LPDDR4 I/F
- NOR Flash Memory I/F
- NAND Flash Memory I/Fs

System
- FCCU and MBIST/LBIST
- PLLs
- 2 x Safe DMA
- Debug and Trace Unit

Security

Hardware Security Engine
- Asymmetric Hardware Accelerators
- Symmetric Hardware Accelerators
- Secure Memory
- Random Number Generators

Processors

Arm® Cortex®-M7, Arm Cortex-M7, Arm Cortex-M7: I-cache, D-cache, TCM, FPU

3x Dual-core Lockstep

Arm Cortex-A53, Arm Cortex-A53: L1 I-cache, L1 D-cache, Neon™, Shared L2 Cache

Arm Cortex-A53, Arm Cortex-A53: L1 I-cache, L1 D-cache, Neon, Shared L2 Cache

Cluster Lockstep Option

Fabric

Safe Interconnect

Serial Communication
- 6 x SPI
- 5 x I²C

Networking
- 4 x CAN FD
- 3 x LIN
- FlexRay®
- 1-GbE w/ TSN
- USB 2.0 OTG
- 2 x PCIe 3.0

Timers and ADCs
- 7 x Watchdog Timer
- 8 x System Timer
- 12 x FlexTimer
- 2 x SAR ADCs (12-ch)

Network Acceleration

Automotive Networks

Low Latency Communications Engine Transport Layer Offload
- 16 x CAN FD
- FlexRay
- Flexible Buffers
- 4 x LIN
- 4 x SPI
- Security Offload
- Global Timestamping

Ethernet Networks

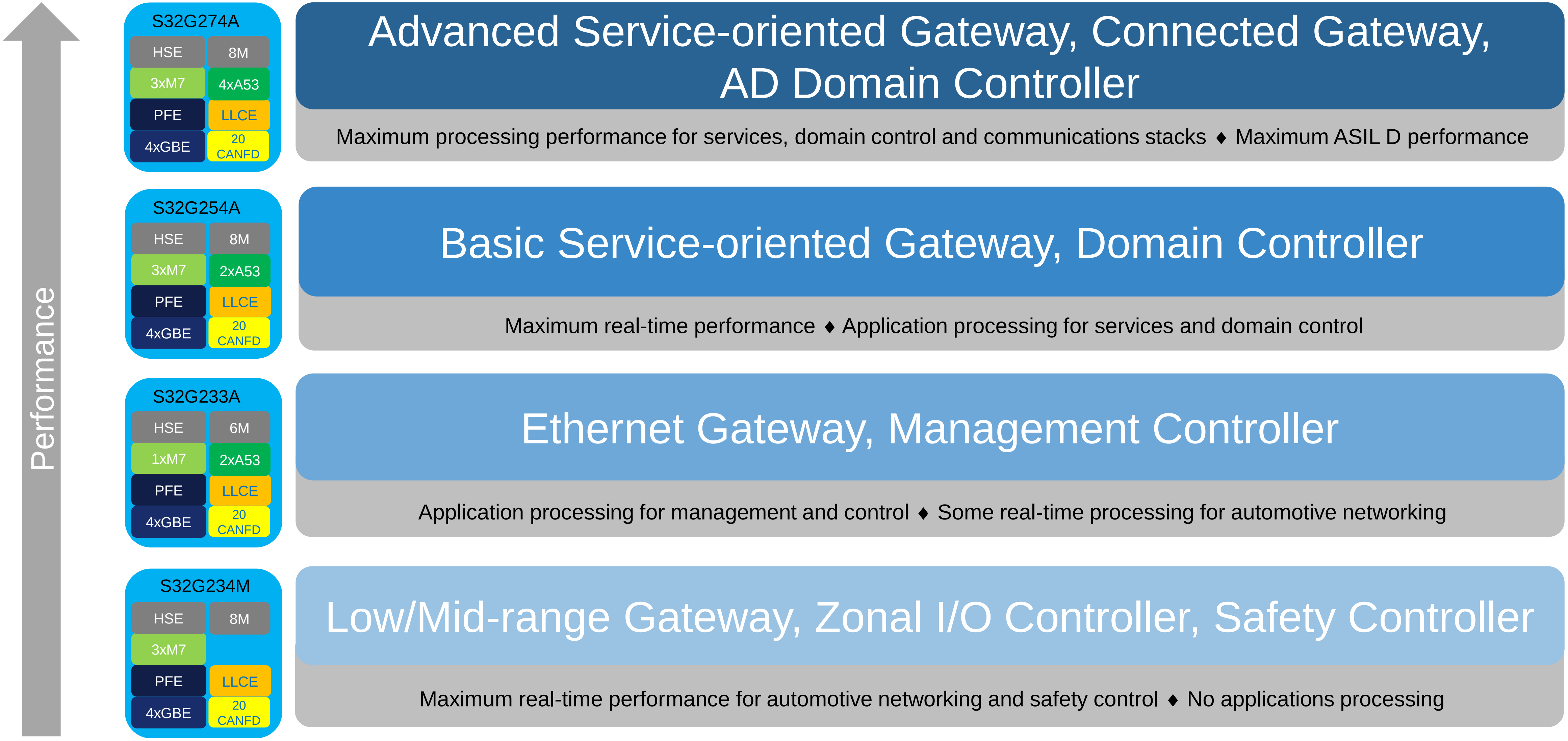
Packet Forwarding Engine
- Stateful Inspection Firewall
- Classification
- Header Manipulation
- IEEE® 1588v2 + AVB
- 2.5-GbE MAC
- 1-GbE MAC
- 1-GbE MAC

Automotive Networks (CAN/LIN/FlexRay) Hardware Acceleration

Automotive Gigabit Ethernet Hardware Acceleration

System Peripherals and Interfaces including 2x2 PCI 3.0

S32G Scalable Family Applications*



S32G274A

HSE	8M
3xM7	4xA53
PFE	LLCE
4xGBE	20 CANFD

Advanced Service-oriented Gateway, Connected Gateway, AD Domain Controller

Maximum processing performance for services, domain control and communications stacks ♦ Maximum ASIL D performance

S32G254A

HSE	8M
3xM7	2xA53
PFE	LLCE
4xGBE	20 CANFD

Basic Service-oriented Gateway, Domain Controller

Maximum real-time performance ♦ Application processing for services and domain control

S32G233A

HSE	6M
1xM7	2xA53
PFE	LLCE
4xGBE	20 CANFD

Ethernet Gateway, Management Controller

Application processing for management and control ♦ Some real-time processing for automotive networking

S32G234M

HSE	8M
3xM7	
PFE	LLCE
4xGBE	20 CANFD

Low/Mid-range Gateway, Zonal I/O Controller, Safety Controller

Maximum real-time performance for automotive networking and safety control ♦ No applications processing

*These applications are only for guidance and can vary based on customer requirements.

NXP S32G Reference Design Board Accelerates Development

Carmakers

Proof of concept

Benchmarking

Vehicle data insights

New services deployment

Application Developers

Innovation platform

Software development

Test and validation

Demo showcase

Cloud & Service Providers

Symbiotic compute

Over-the-Air (OTA) updates

Machine learning deployment

Edge service deployment

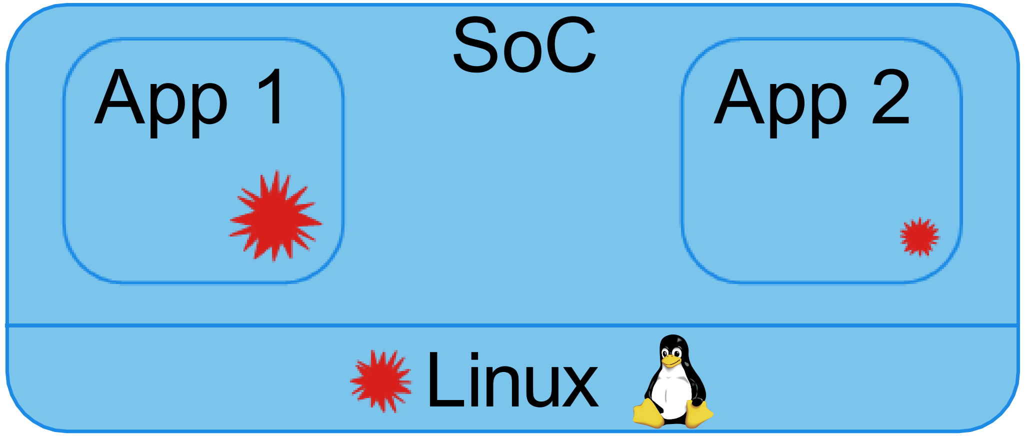
Accelerating Transformation Across the Automotive Ecosystem

Mixed-Criticality as an Enabler

- ❑ The main driver is the application landscape
  - Domain controllers & vehicle computers
  - ADAS/AD Applications
  - Gateways
  - Modular software deployment
  - ‘App-store’ like software distribution
- ❑ Heterogeneous computing platforms to the rescue
  - Require vast middleware packages
  - Enable rich connectivity functions
- ❑ Mixed criticality on a single platform is the key

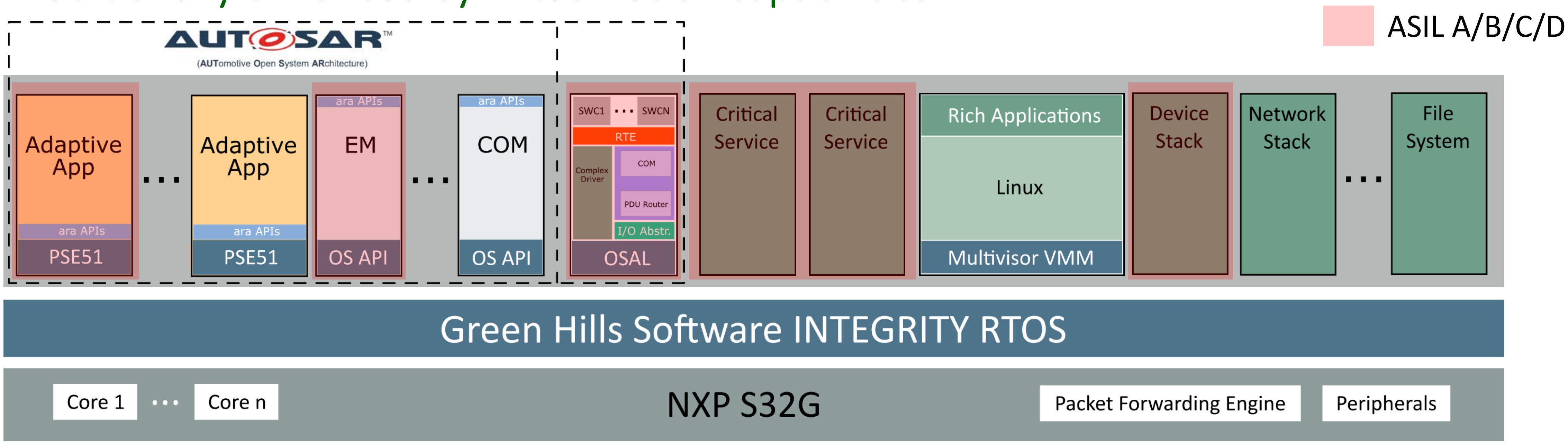
Freedom-From-Interference

- ❑ A failure in an element is caused by a fault
- ❑ Faults can have diverse root causes
  - Hardware faults – bit flips, erratas, etc.
  - Software faults – bugs
  - Malicious attacks
- ❑ FFI prevents failures from propagating (cascading)
  - Relevant for the safety functions of an ECU
- ❑ FFI is critical for separating mixed-criticality systems
  - Prevents failures to cascade from “lower” ASIL to “higher” ASIL
  - Prevents failures to cascade within the same ASIL domain



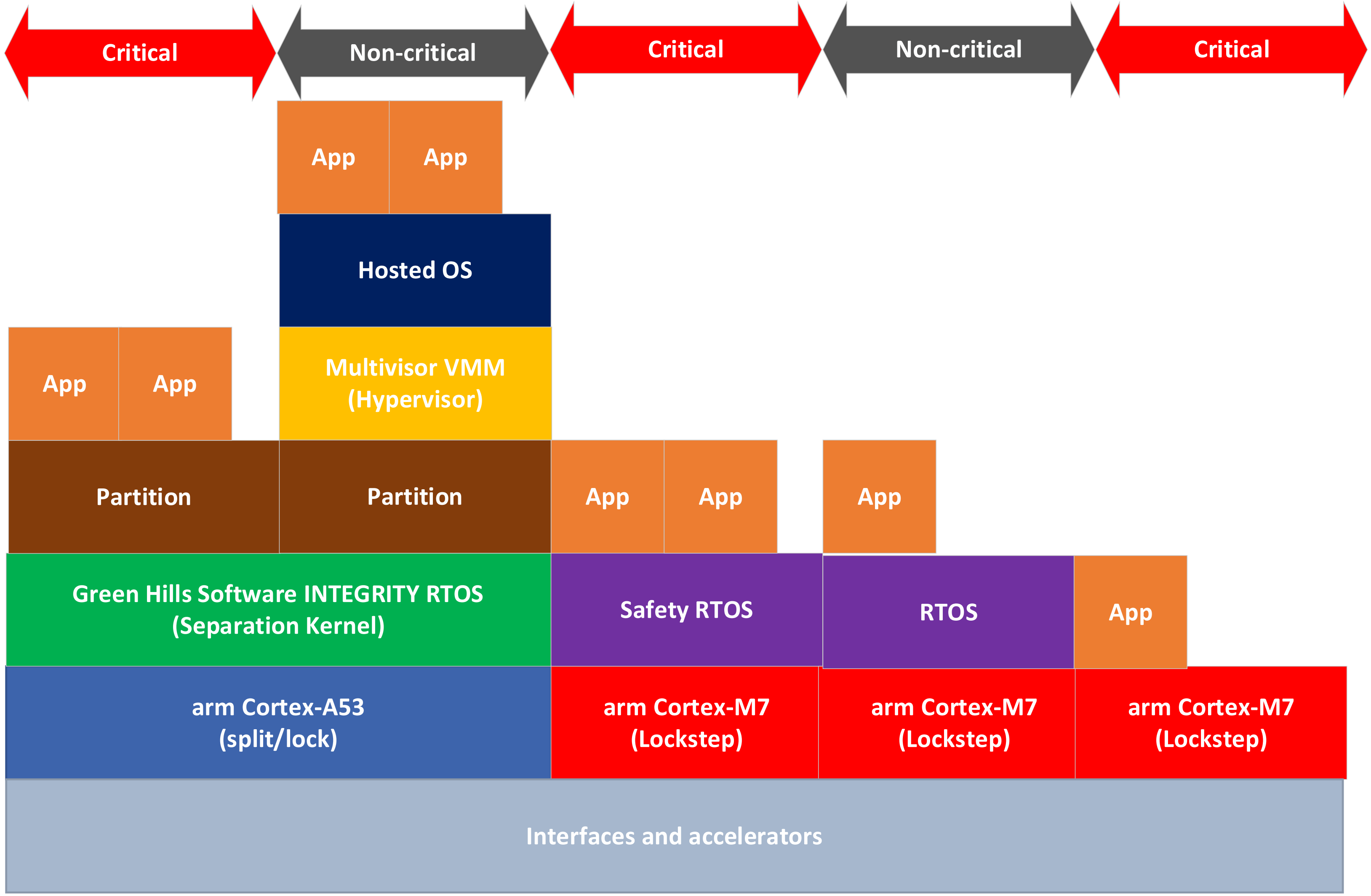
Mixed-Criticality in Action

- A pre-certified secure microkernel
  - Minimal codebase, low footprint, efficient hardware resource usage
  - Trusted secure base for separation
- Least privilege model provides “containerization”
  - Additionally enhanced by virtualization capabilities



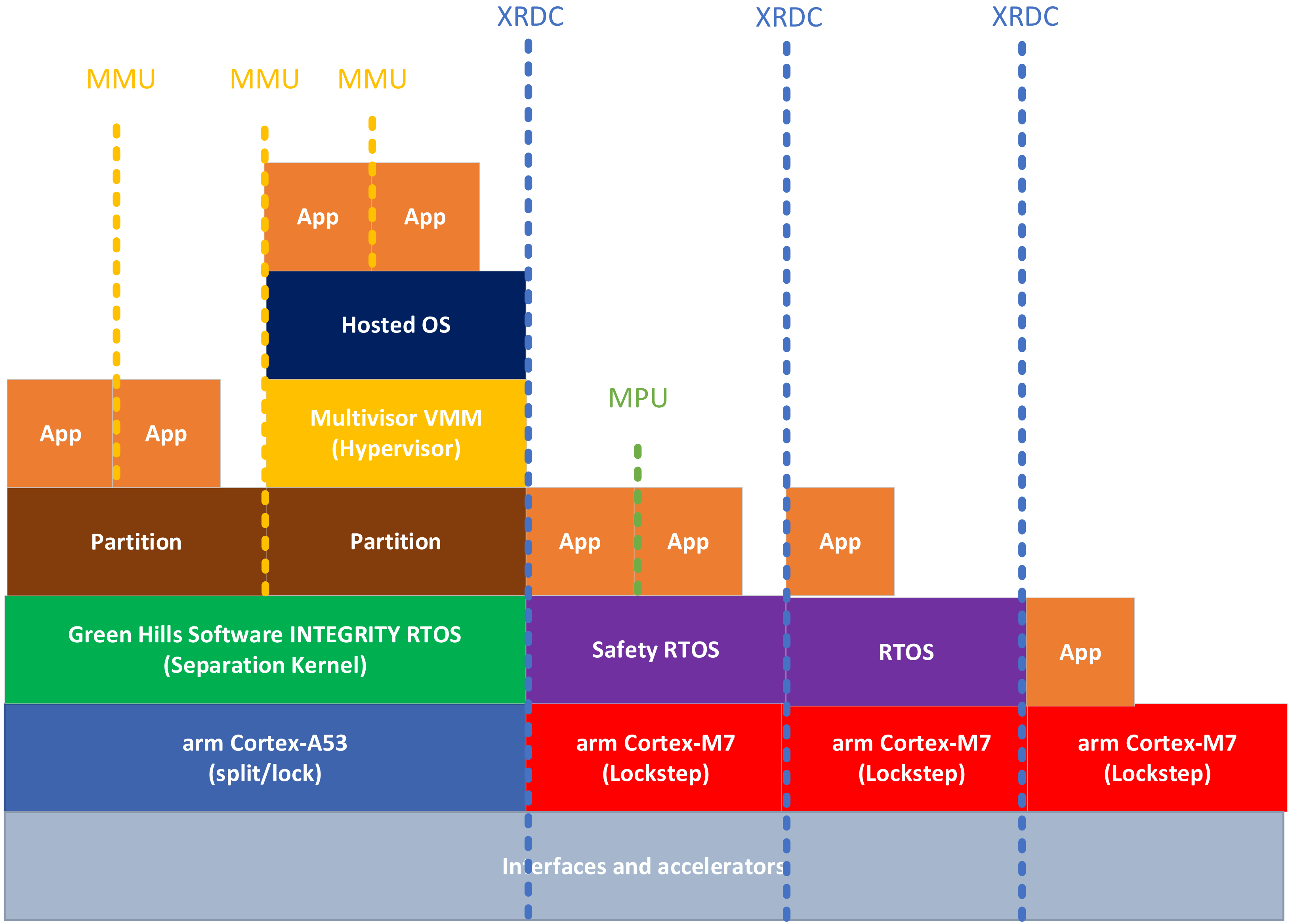
SOFTWARE STACK LAYOUT

- App domain
  - Quad A53
  - Split/lock
  - RTOS
  - Hypervisor
- RT domain
  - Triple M7
  - Lockstep
  - RTOS
  - Bare metal
- Accelerators
  - Network
  - Security



HARDWARE ENFORCED ISOLATION

- App domain → MMU
- RT domain → MPU
- Interconnect → XRDC

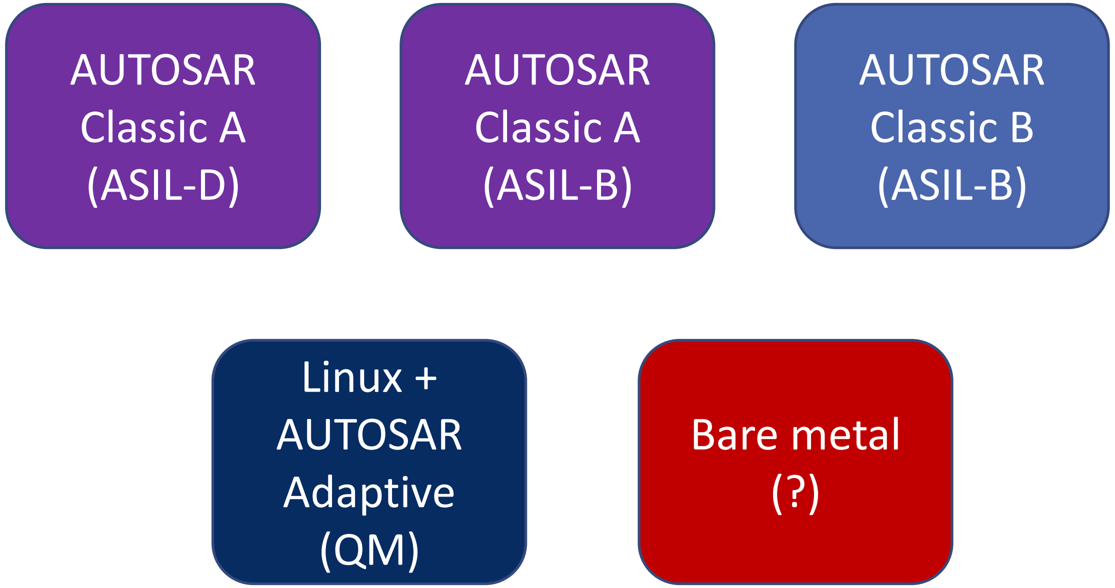


GUARDKNOX

CONSOLIDATION: USE CASE

- Runtime
  - AUTOSAR Classic
  - AUTOSAR Adaptive
  - Linux
  - Bare metal
- Vendors
  - AUTOSAR Classic
  - ECU suppliers
- Criticalities
  - ASIL-D
  - ASIL-B
  - QM
  - Unspecified

Legacy ECUs



AUTOSAR Classic A (ASIL-D)

AUTOSAR Classic A (ASIL-B)

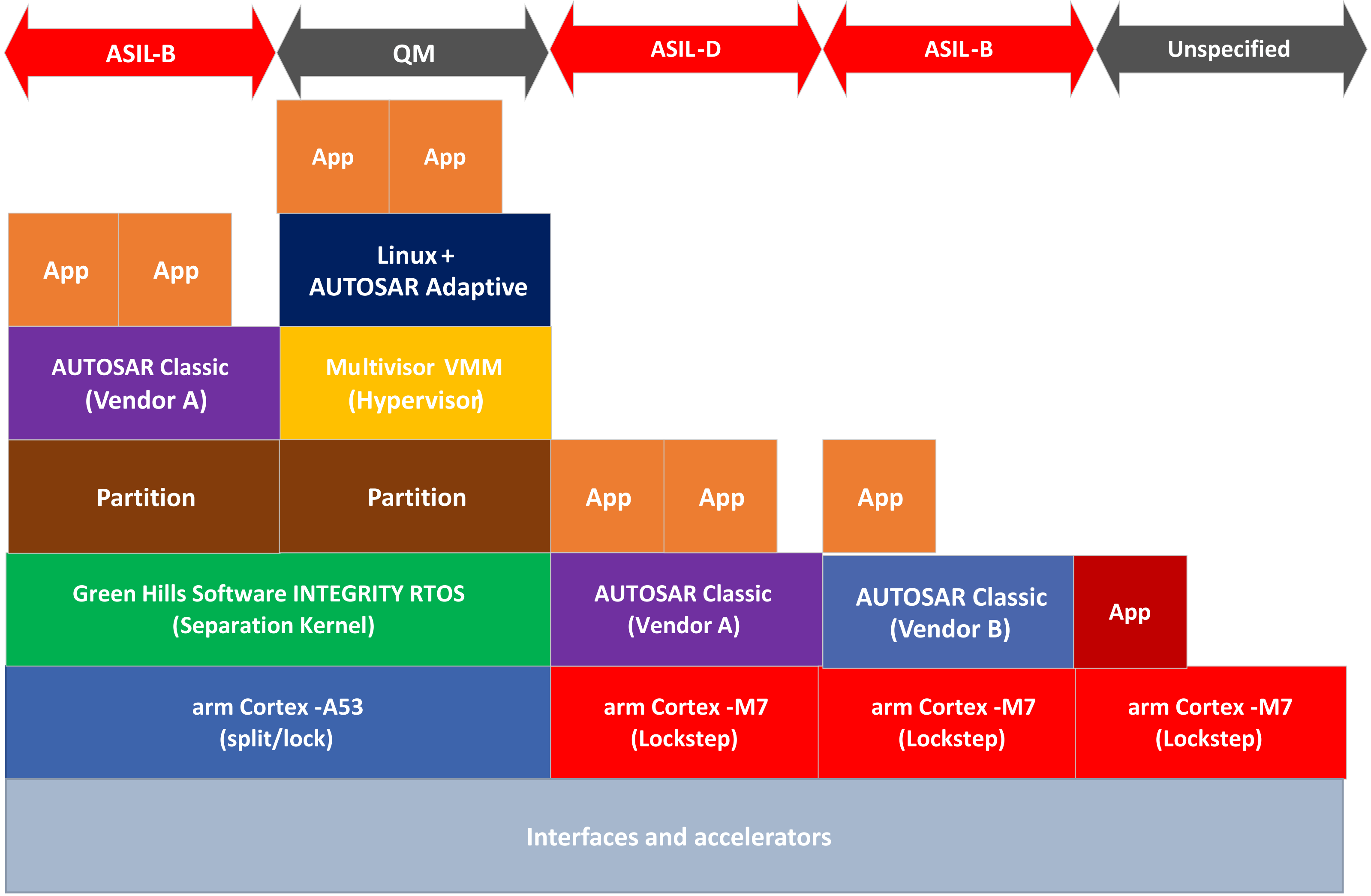
AUTOSAR Classic B (ASIL-B)

Linux + AUTOSAR Adaptive (QM)

Bare metal (?)

USE CASE IMPLEMENTATION A

- App domain
  - Quad A53
  - Split/lock
  - RTOS
  - Hypervisor
- RT domain
  - Triple M7
  - Lockstep
  - RTOS
  - Bare metal
- Accelerators
  - Network
  - Security



ASIL-B

QM

ASIL-D

ASIL-B

Unspecified

App App

App App

Linux + AUTOSAR Adaptive

AUTOSAR Classic (Vendor A)

Multivisor VMM (Hypervisor)

Partition

Partition

App App

App

Green Hills Software INTEGRITY RTOS (Separation Kernel)

AUTOSAR Classic (Vendor A)

AUTOSAR Classic (Vendor B)

App

arm Cortex -A53 (split/lock)

arm Cortex -M7 (Lockstep)

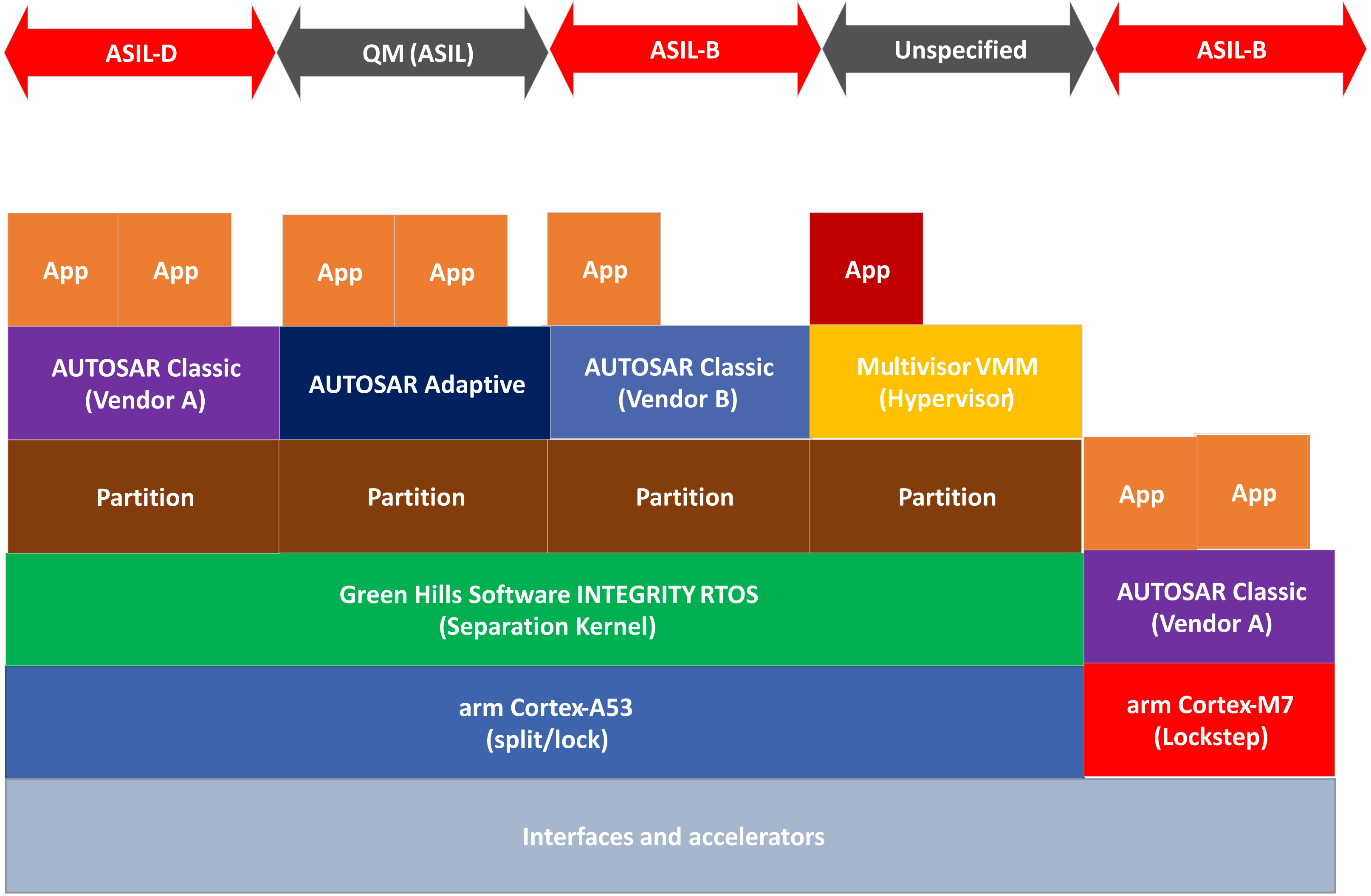
arm Cortex -M7 (Lockstep)

arm Cortex -M7 (Lockstep)

Interfaces and accelerators

USE CASE IMPLEMENTATION B

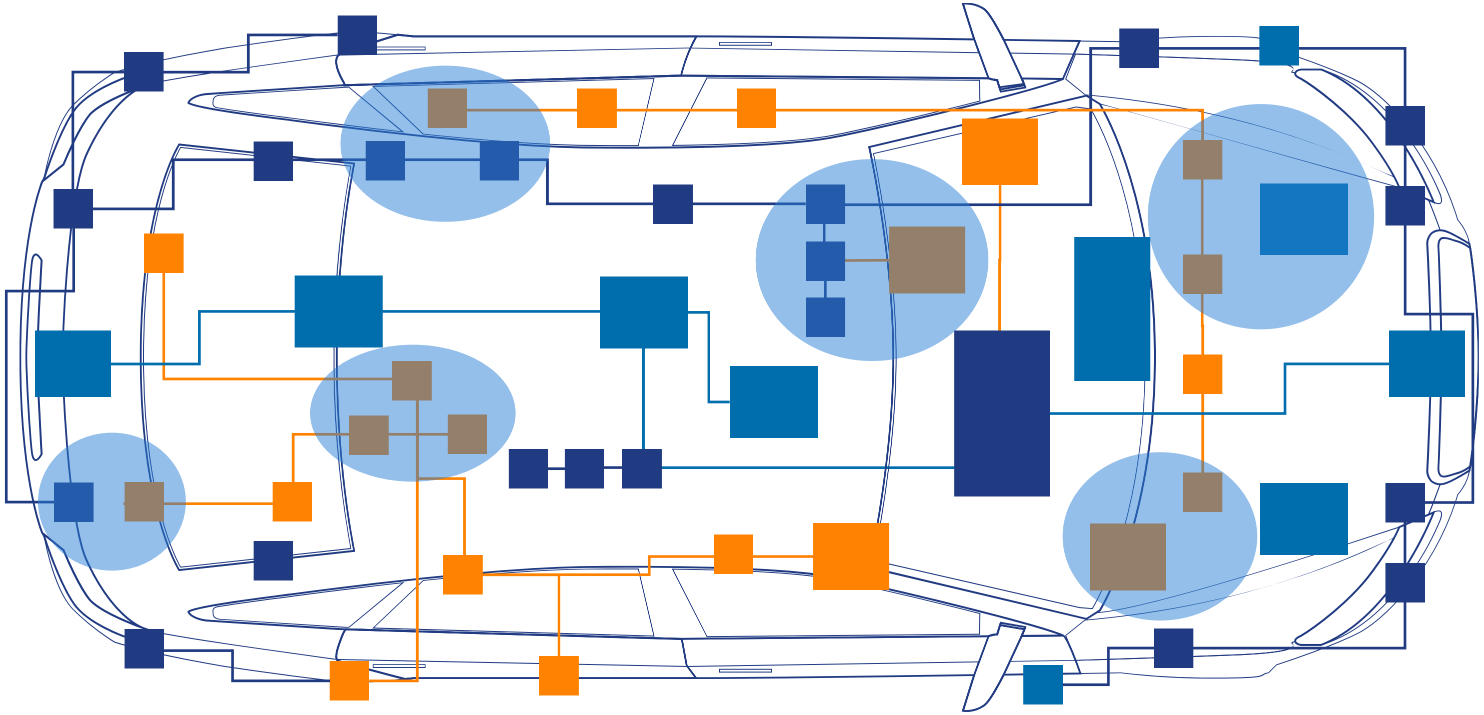
- App domain
  - Dual A53
  - Split/lock
  - RTOS
  - Hypervisor
- RT domain
  - Single M7
  - Lockstep
  - RTOS
- Accelerators
  - Network
  - Security


ASIL-D
QM (ASIL)
ASIL-B
Unspecified
ASIL-B
App
App
App
App
App
App
AUTOSAR Classic (Vendor A)
AUTOSAR Adaptive
AUTOSAR Classic (Vendor B)
Multivisor VMM (Hypervisor)
Partition
Partition
Partition
Partition
App
App
Green Hills Software INTEGRITY RTOS (Separation Kernel)
AUTOSAR Classic (Vendor A)
arm Cortex-A53 (split/lock)
arm Cortex-M7 (Lockstep)
Interfaces and accelerators

GUARDKNOX

ZONAL GATEWAY

- Re-use gateway + server design
- Optimize case by case



GUARDKNOX

UNIFORMITY

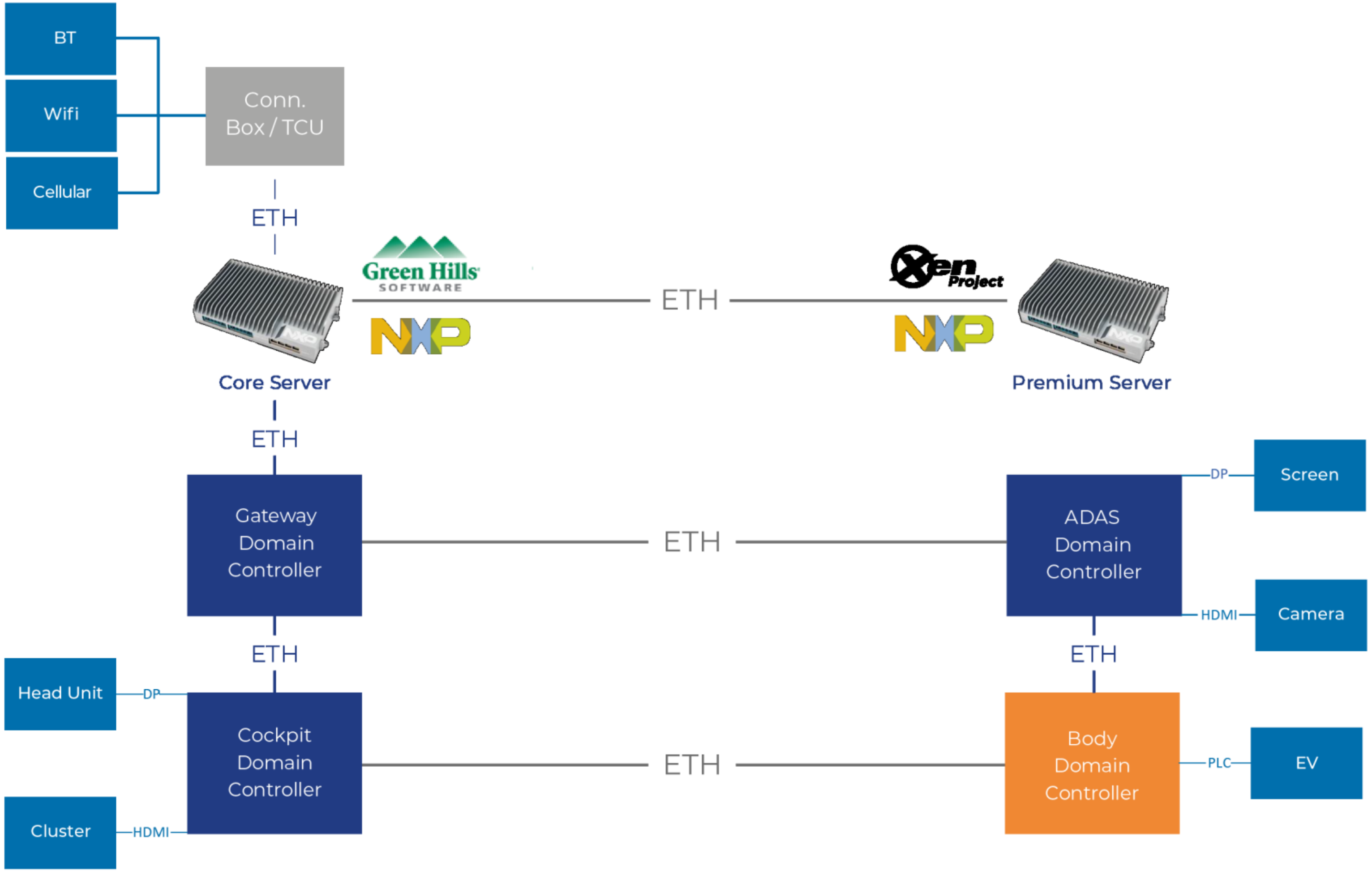
- Maximize software re-use
  - MCAL / BSP
  - Applications
  - Guest OS / middleware / eco-system
- Hardware scaling up / down
  - Pin compatibility
  - Vendor roadmap
  - Product / chip family and variants
- Interchangeable parts
  - May not need to maintain old ECUs
  - May not need to stock up parts for over a decade
  - Used car factory options “retrofitting”
- Vendor complementary peripherals
  - Design optimized PMIC, Ethernet switches, transceivers…

CHALLENGES AND PITFALLS

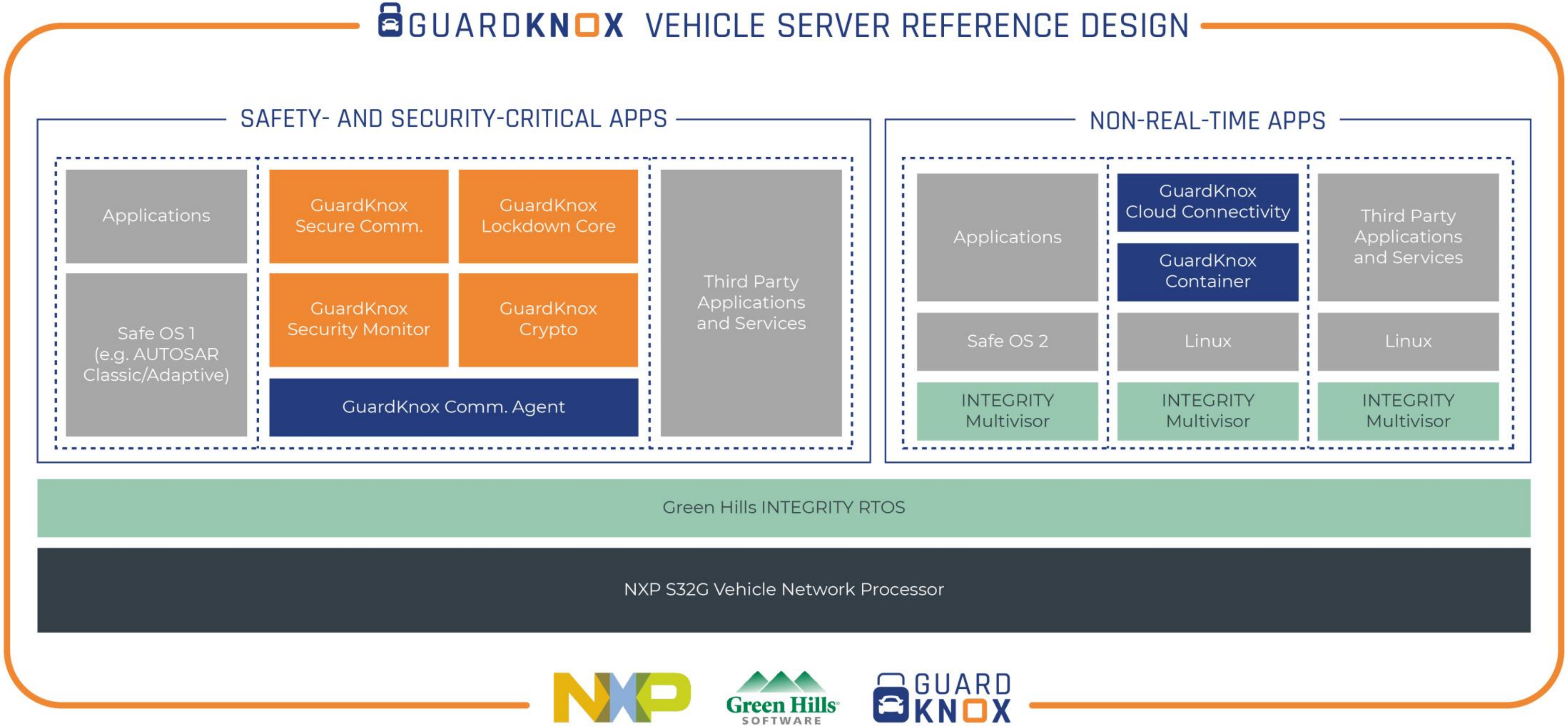
- Cost reduction
  - Across entire E/E
  - Vehicle lifecycle
- Not a traditional supplier engagement
  - Requires expertise - no general solution
  - Can’t spec-out “make me have zonal”
- DMIPS performance rating
  - Accelerators and offloaders are left out
  - Today mostly a compiler optimizer benchmark

WHEN?

GUARDKNOX ZONAL E/E ARCHITECTURE DEMO RACK SET-UP



PARTNER MAPPING


GUARDKNOX VEHICLE SERVER REFERENCE DESIGN
SAFETY- AND SECURITY-CRITICAL APPS
Applications
Safe OS 1 (e.g. AUTOSAR Classic/Adaptive)
GuardKnox Secure Comm.
GuardKnox Lockdown Core
GuardKnox Security Monitor
GuardKnox Crypto
GuardKnox Comm. Agent
Third Party Applications and Services
NON-REAL-TIME APPS
Applications
Safe OS 2
INTEGRITY Multivisor
GuardKnox Cloud Connectivity
GuardKnox Container
Linux
INTEGRITY Multivisor
Third Party Applications and Services
Linux
INTEGRITY Multivisor
Green Hills INTEGRITY RTOS
NXP S32G Vehicle Network Processor
NXP
Green Hills SOFTWARE
GUARD KNOX

THANK YOU

Idan Nadav

Idan@guardknox.com

http://www.guardknox.com

Nikola Velinov

Nvelinov@ghs.com

http://www.ghs.com

Brian Carlson

Brian.carslon@nxp.com

http://www.nxp.com