L&T Technology Services

ENGINEERING **THE CHANGE**

Decoding Software Defined Vehicles: Insights, Innovations, and Impact
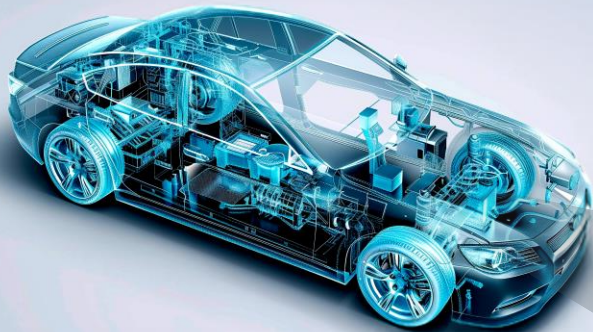
Rameshbabu S

Chief Engineer, Software Defined Mobility

Purposeful. Agile. Innovation.

Future of Software Defined Vehicles (SDV) : Exciting Journey !

SDVs are vehicles where most of their functions and features are enabled through software, rather than controlled by hardware components.

The future of driving is **smarter, safer, and always improving**

Think of your **Smartphone** but as a Car

EXPLOSIVE GROWTH BY 2030

$650+ Billion
Total Value Creation
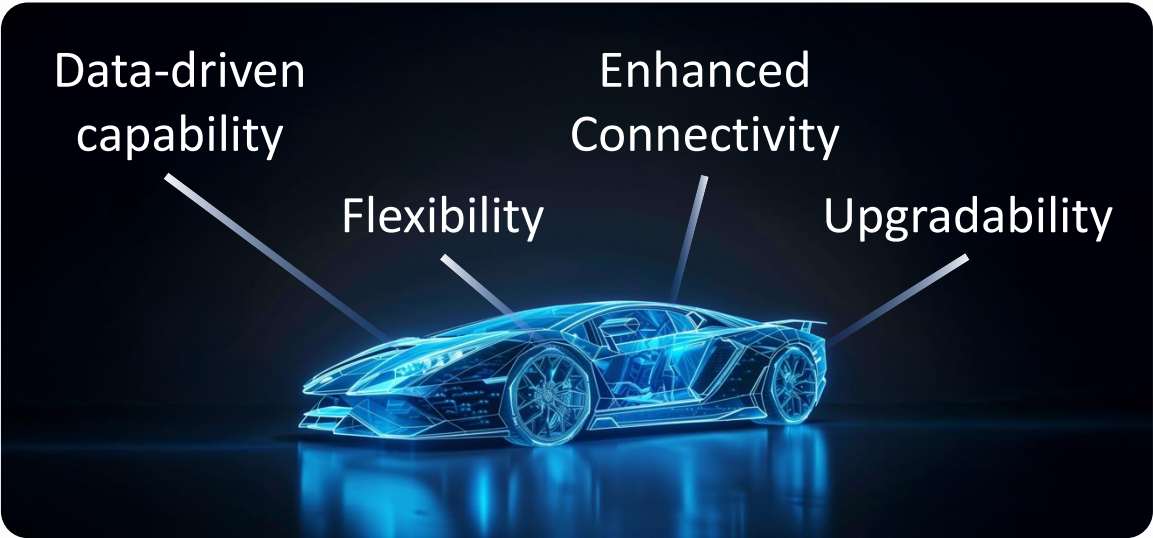
15-20%
Automotive Revenue Share
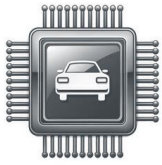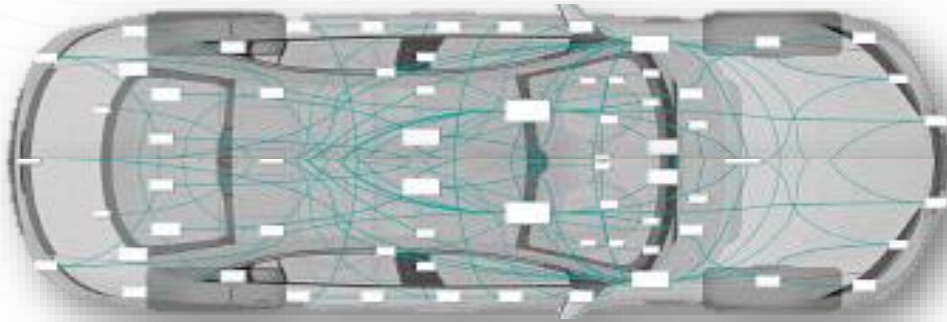
$248B
OEM Revenue

$411B
Supplier Market

Data-driven capability

Enhanced Connectivity

Flexibility

Upgradability

L&T Technology Services

SDV Platform Success Factors: An OEM Perspective and Motivation

Legacy Architecture

100-150 ECUs

40-50% Reduction
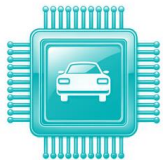
50-60 ECUs

1/3rd Supplier Count Reduction

HPC-Zonal-EDGE Architecture

Zonal Gateway

Zonal Gateway

High Performance Compute

High Compute Needs

Load Balancing

Zonal Gateway

Zonal Gateway
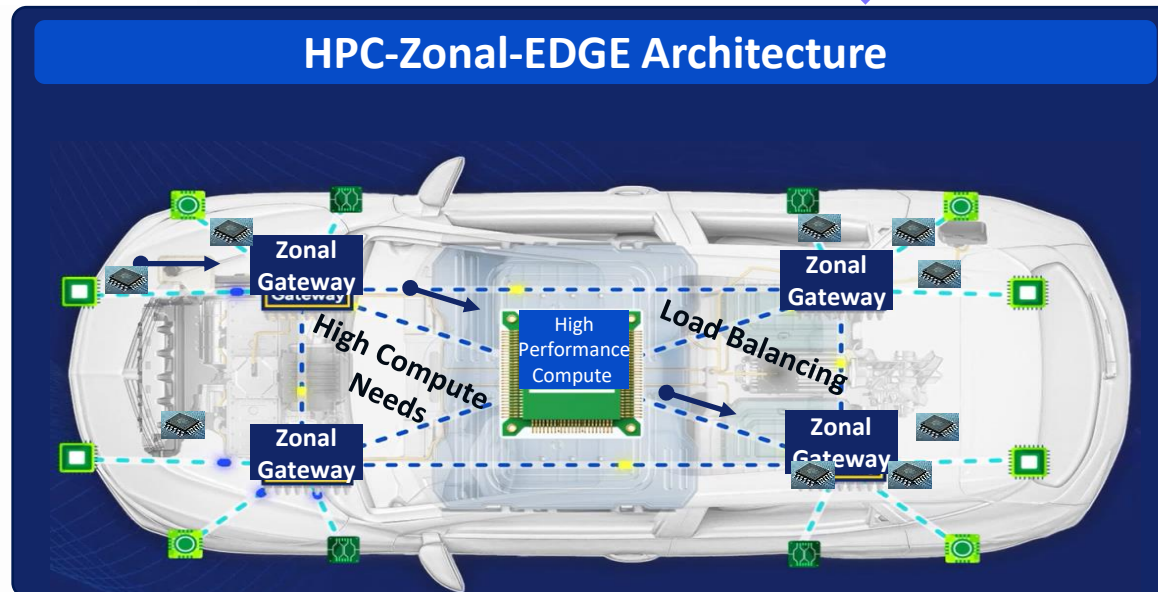
Harness Optimization
Reduce harness length, weight, and cost (Upto 30%)

Dynamic Load Balancing
Transfer load dynamically to free cores

Hardware Consolidation
Multiple function can be served by single Zonal Control

SDV Platform Success Factors: An OEM Perspective : Feature As A Service (FAAS)

" **Feature-As-A-Service**

is a **strategy** to

diversify OEMs

revenue stream

through **monetizing**

features

Faster Go-To-Market (GTM)

Continuous Revenue Stream

Vehicle Price Reduction

Nearly, half would keep their vehicles longer if FAAS are available

49%

40%

Likelihood of purchasing next vehicle from brands that offer FAAS

Three critical dimensions of Software Defined Vehicles

Virtualization

Modern Features

VMs/Containers [Development benches and test on cloud]

Real Time performance for testing

Digital Twins / Sesnor / actuator library

Secure APIs

OTA Updates

Cybersecurity

Zero Trust Security

Stack Layer

OS/Hypervisor   Middleware   Applications
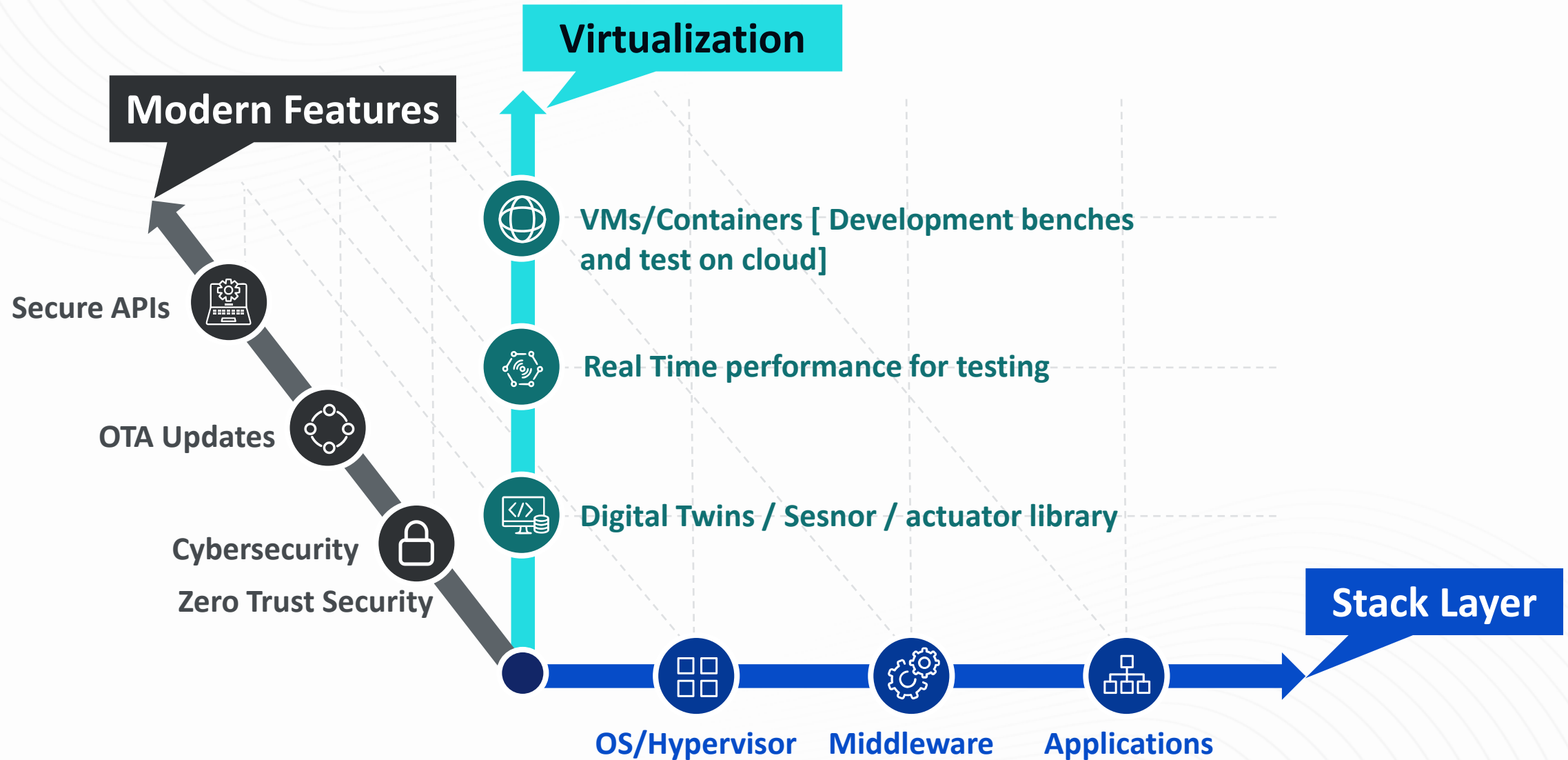
SDV: Easy Switch between Semiconductor platforms

Easy APP Portability

New Platform Support In few months

Pre-Configured Dev tools on Cloud

Software Development Time

Digital Cockpits · Electrification · Connectivity · Comfort & Conveience · AD-ADAS

Middleware and Third-Party Package (Classic and Adaptive AUTOSAR Services)

Operating System (OS) Android, QNX, and Linux

Embedded Hypervisors

Hardware High Performance Compute

Vehicle Applications (Safety | Non-Safety)

Middleware and Third-Party Package (Classic and Adaptive AUTOSAR Services)

Operating System (OS) Android, QNX, and Linux

Embedded Hypervisors

Vehicle Applications (Safety | Non-Safety)

Middleware and Third-Party Package (Classic and Adaptive AUTOSAR Services)

Operating System (OS) Android, QNX, and Linux

Reuseable stack development
Platform-A

Reused stack
Platform-B

Reused stack
Platform-C

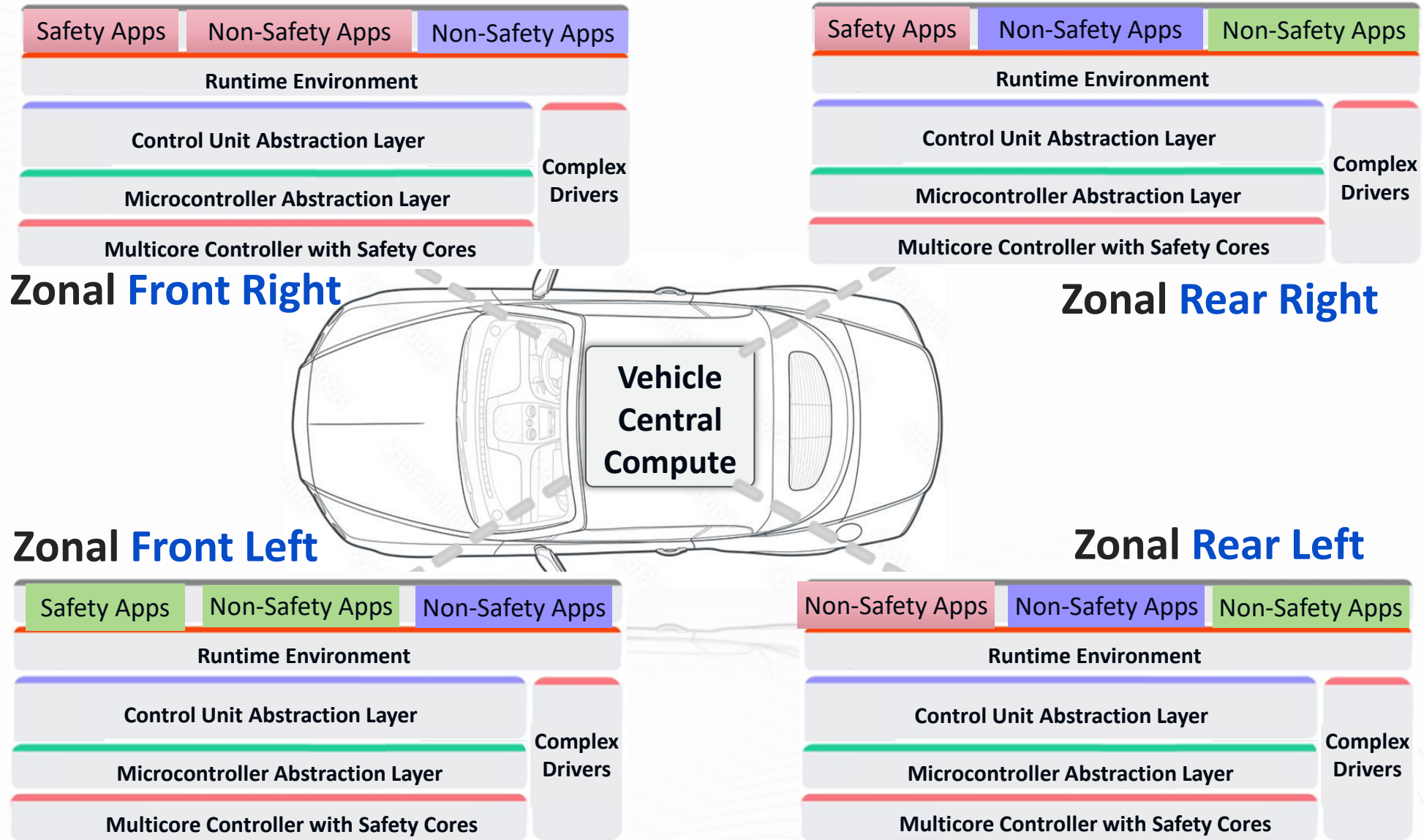**Stack & Libraries Reuseable Across Semicondutor Platforms**

Smart Zonal Controller [Reusable Middleware across all Zones]

Dynamic Load Balancing with Vehicle Central Compute.

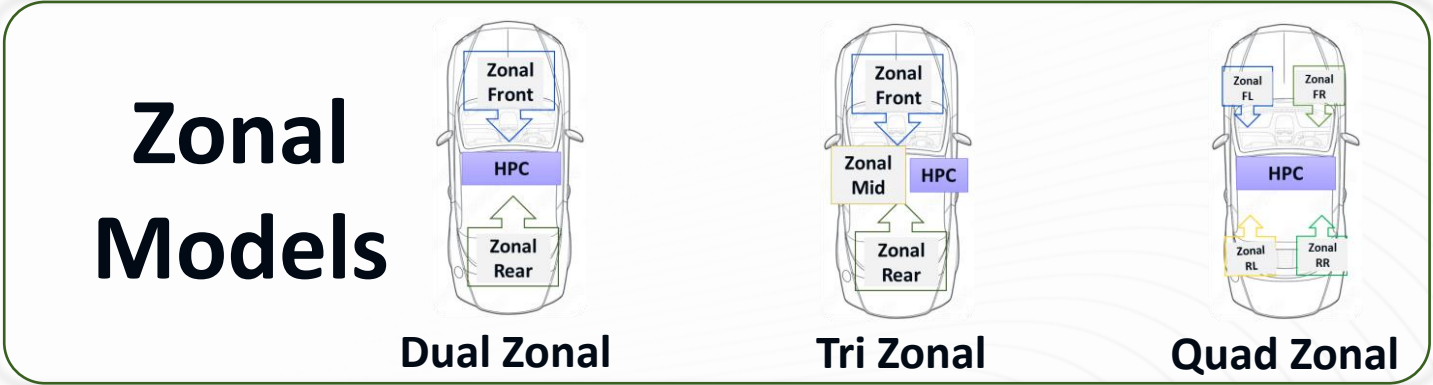**Easy to achieve with Ethernet and Some I/P**

Cockpit

Body Control

Chassis/Powertrain/AD-ADAS

Zonal Front Right

Safety Apps	Non-Safety Apps	Non-Safety Apps

Runtime Environment

Control Unit Abstraction Layer

Microcontroller Abstraction Layer

Multicore Controller with Safety Cores

Complex Drivers

Zonal Rear Right

Safety Apps	Non-Safety Apps	Non-Safety Apps

Runtime Environment

Control Unit Abstraction Layer

Microcontroller Abstraction Layer

Multicore Controller with Safety Cores

Complex Drivers

Vehicle Central Compute

Zonal Front Left

Safety Apps	Non-Safety Apps	Non-Safety Apps

Runtime Environment

Control Unit Abstraction Layer

Microcontroller Abstraction Layer

Multicore Controller with Safety Cores

Complex Drivers

Zonal Rear Left

Non-Safety Apps	Non-Safety Apps	Non-Safety Apps

Runtime Environment

Control Unit Abstraction Layer

Microcontroller Abstraction Layer

Multicore Controller with Safety Cores

Complex Drivers

Manage diverse applications | Shared infrastructure | Enhance modularity | Reduce wiring complexity

Zonal Architecture Challenges & Solutions

Challenge	Solution
Safety And Security	**Time-Division Multiple Access**
Time Synchronization Increase in bandwidth | Combine new computing resources with legacy	**Precision Time Protocol**
Communication ECUs into a zonal network must cover CAN -> Ethernet backbone -> CAN	**High-speed communication** and time-sensitive networking task group (TSN)
Network Configuration Migrating from single vehicle communication to multi zones	**Software Defined Networking**
Latency And Jitter Delays: Processing | Transmission | Scheduling | Queueing	**System with high-performance, multi-core processors** & advanced task scheduling algos

Zonal Models

**Dual Zonal**   **Tri Zonal**   **Quad Zonal**

Smart ASICs to Replace EDGE ECUs: A Micro-less Architecture

- ➢ **ASIC-Based Architecture:** Utilizes an ASIC-based architecture for last-mile features and functions (e.g., DOORS ,tail lighting, seat heating, ambient lighting,DOOR handle, Amplifiers, Sun roof).

- ➢ **Software Independence:** The architecture eliminates the need for software stacks, bootloaders, and configurators.

- ➢ **Lean FOTA Strategy:** Aligns with the lean FOTA strategy required by OEMs.
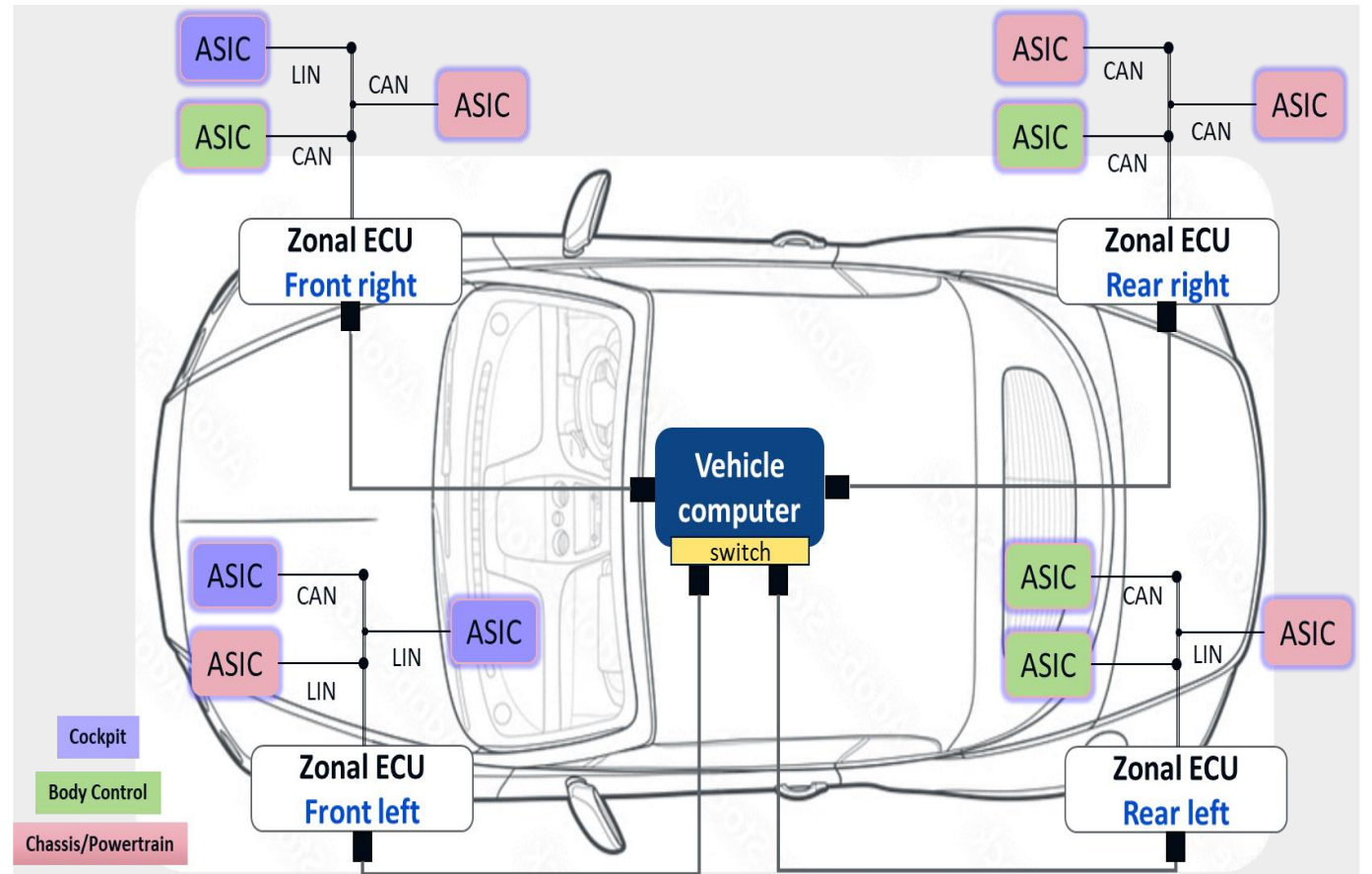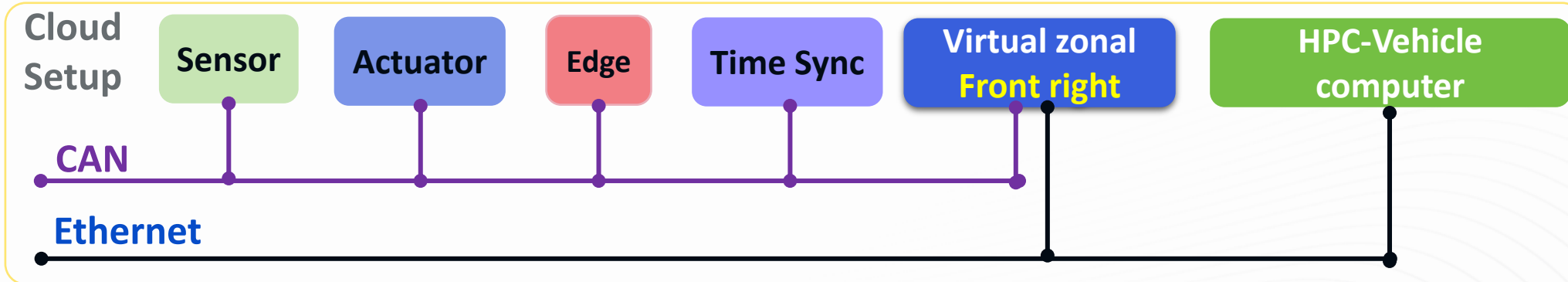

Operates on hardware logic | Do not require firmware | Diagnostics enabled

Virtualization Strategy for Easy Development and Testing
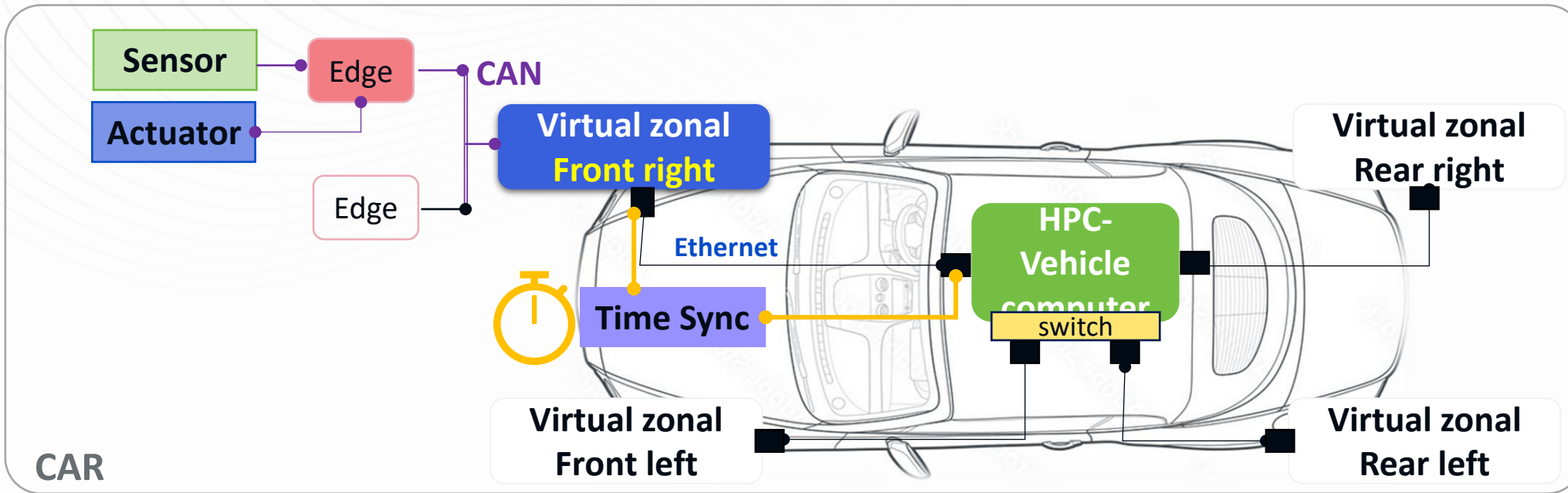
Assets

- Time Sync
- vComm Bus
- vZonal
- vEdge
- vHPC

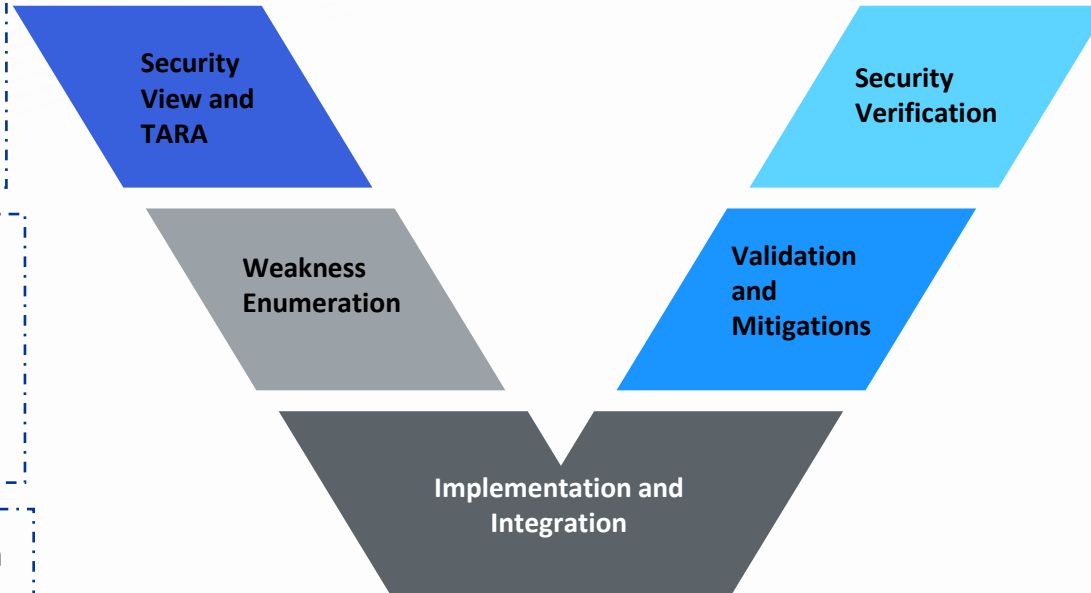L&T Technology Services

Automotive Security

Preparedness for Addressing Security Concerns

ISO 21434 offering a comprehensive set of guidelines for integrating Automotive Cybersecurity compliances into various phases of automotive development. It stresses on Continuous Assessment, checks on Security Validations and considerations of deploying Low-level Security Features

- Security Goals and Objectives
- System Reconnaissance
- Cybersecurity Management (roles / policies)

Security View and TARA

Security Verification

- Fuzz Testing
- Security Functional Testing
- Penetration Testing

- Vulnerability Analysis
- Cybersecurity case and plan
- Interface level, component level vulnerability analysis
- Update Vulnerabilities in tools

Weakness Enumeration

Validation and Mitigations

- Validation of Security Assessment identified vulnerabilities
- Attack vector Analysis
- Design mitigations, create requirements tracing

Implementation and Integration

- CMAC, HMAC bases Authentication
- AUTOSAR Cryptostack integration
- HSM-based Security Services

- Key Management
- HSM Crypto integration
- Secure Boot, Secure Flash, SecOC, Secure Diagnostic integration / implementation /

- Security Assessment
- Compliances based on ISO-21434 and UNECE R.155/R.156

- Security Validations (Fuzz Testing, Pen Testing, IDS)
- Security Testing (Functional, Integration Testing
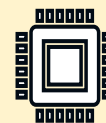
- HSM Based Security (Secure Boot, Secure Flashing, Secure logging, Secure On-Board Communication, Firewall, Secure Diagnostics, JTAG Protection, Memory (PFlash/DFlash) Protection, TLS, Secure Update (FOTA/SOTA),
- CAN based secure re-programming, Secure Lifecycle

Cybersecurity Validation, Secure Communication and Key Management, Secure Boot, Secure Flash, Secure Logging, Security Assessment

Cybersecurity System Validation

Security Features Testing

- Secure Boot, Secure ECU modes
  Secure Feature Activation, OS security
- Transport Layer Security
  Firewall Concept
- Flash Antiroll back
  Security Key Algorithm for Wi-Fi
- Firewall Concept
  Protection against Physical attacks

External Interfaces Testing

- IPSec, MacSec, SecOC
  CAN and Ethernet Interface
- Certificate download, message signing/verifying
- Bluetooth
  Wi-Fi
- Handling security Artifacts
  Handling security Artifacts

Secure Communication and Key Management

Implementation / Integration

KeyM / SWCrypto → **Created the SW Component for Key Manager**

Hardware Security Module (HSM) → **Integrated the CycurHSM**

CSM / CryIF - → **Configured CSM, CryIf and Crypto via ISOLAR tool**

SecOC → **Created the SecOC module for freshness value**
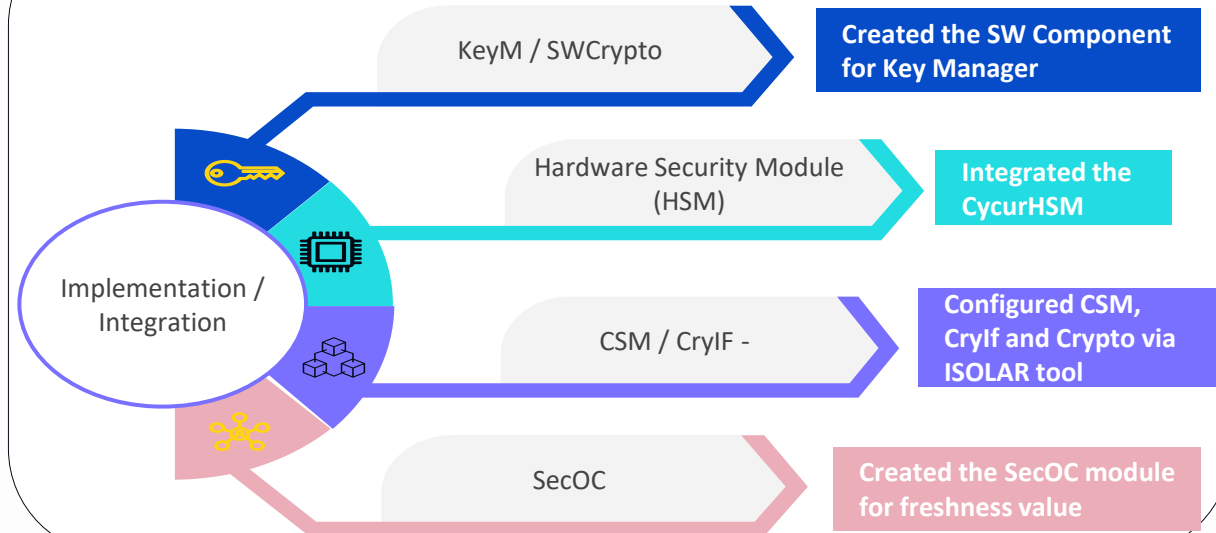
Secure Boot, Secure Flash, Secure Logging

BOOT ROM [Boot Manager]
Validate Boot Flash - HASH

↓

BOOT SFLASH [HSM Updater]
Validate Secure Image - PKCS

↓

SECURE IMAGE [HSM SW]
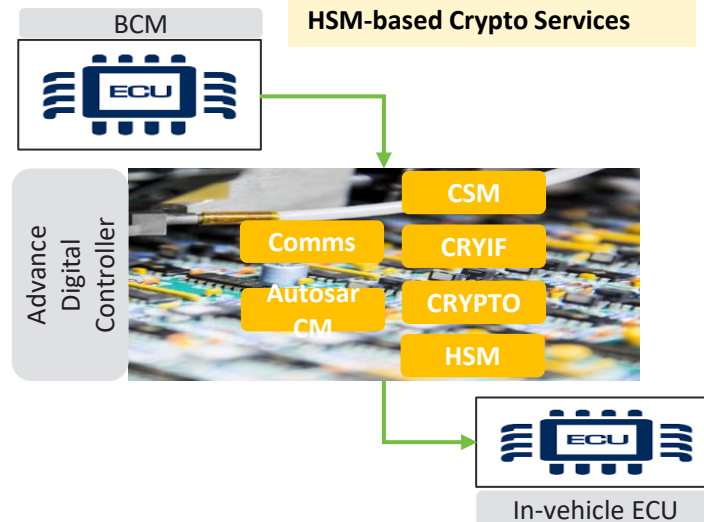Validate Application Bootloader/FBL

↓

APPLICATION BOOTLOADER
Validate FBL/Application

↓

APPLICATION SW

HSM Core / *HOST Core*

HSM-based Crypto Services

BCM
ECU

Advance Digital Controller

- CSM
- Comms
- CRYIF
- Autosar CM
- CRYPTO
- HSM

In-vehicle ECU

Security Assessment and Validation for various Automotive Systems based on ISO 21434 (e.g. Entire Vehicle Level, ECUs like Vehicular Gateway, BCM, Infotainment, Charging Control ECU, Braking Control ECU etc.)

- System Understanding – Item Definition, Asset Identification
- Threat Analysis and Risk Assessment
- Vulnerability Analysis
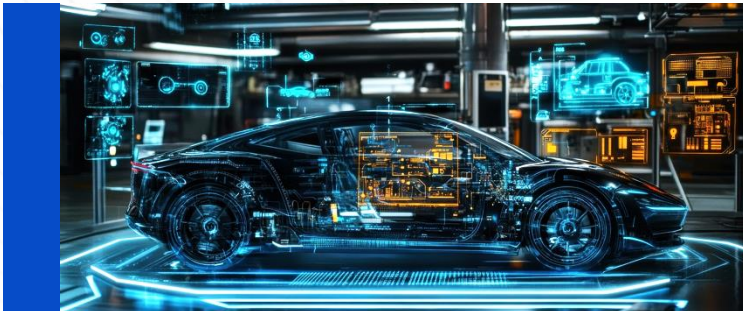- Attack Path Analysis and Attack Feasibility Rating
- Risk Treatment Determination
- Mitigations and Requirement Development
- Document preparation at above every stage for Security Assessment

Technical Realization of Software Defined Vehicles : Right Approach

Hardware-Software Decoupling
- Flexible Updates
- Faster innovation
- Enhanced Modularity
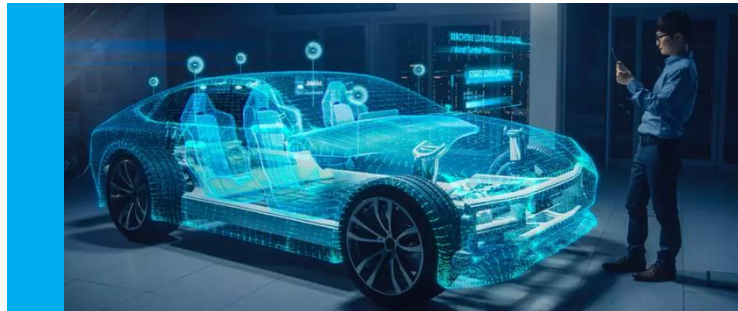
Virtualization of HPC/Zonal /EDGE
- Digital Twins
- Test Environments
- Cloud Development

OTA Updates & Security
- Remote Updates
- Secure Integration
- Real Time Protection

Function Migration
- Zone Flexibility
- Dynamic allocation
- Seamless Transfer
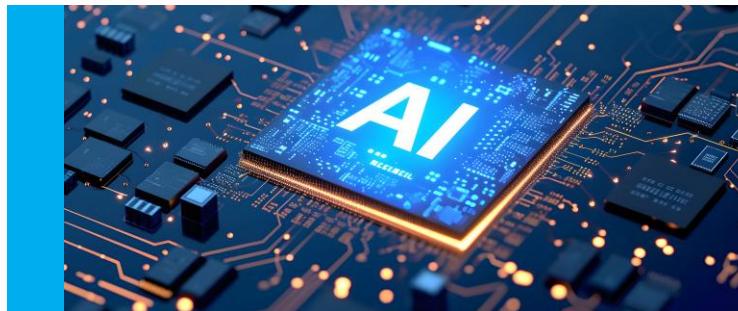
Semicon Agnostic Stack
- Hardware Portable
- Multi-Platform
- Minimal Changes

Industry Collaboration
- Standardization
- Unified Strategies
- Shared Resources
- Open source

LTTSiDriVe

In-house developed integrated solution to adapt and accelerate SDV journey
Development| Validation | Deployment
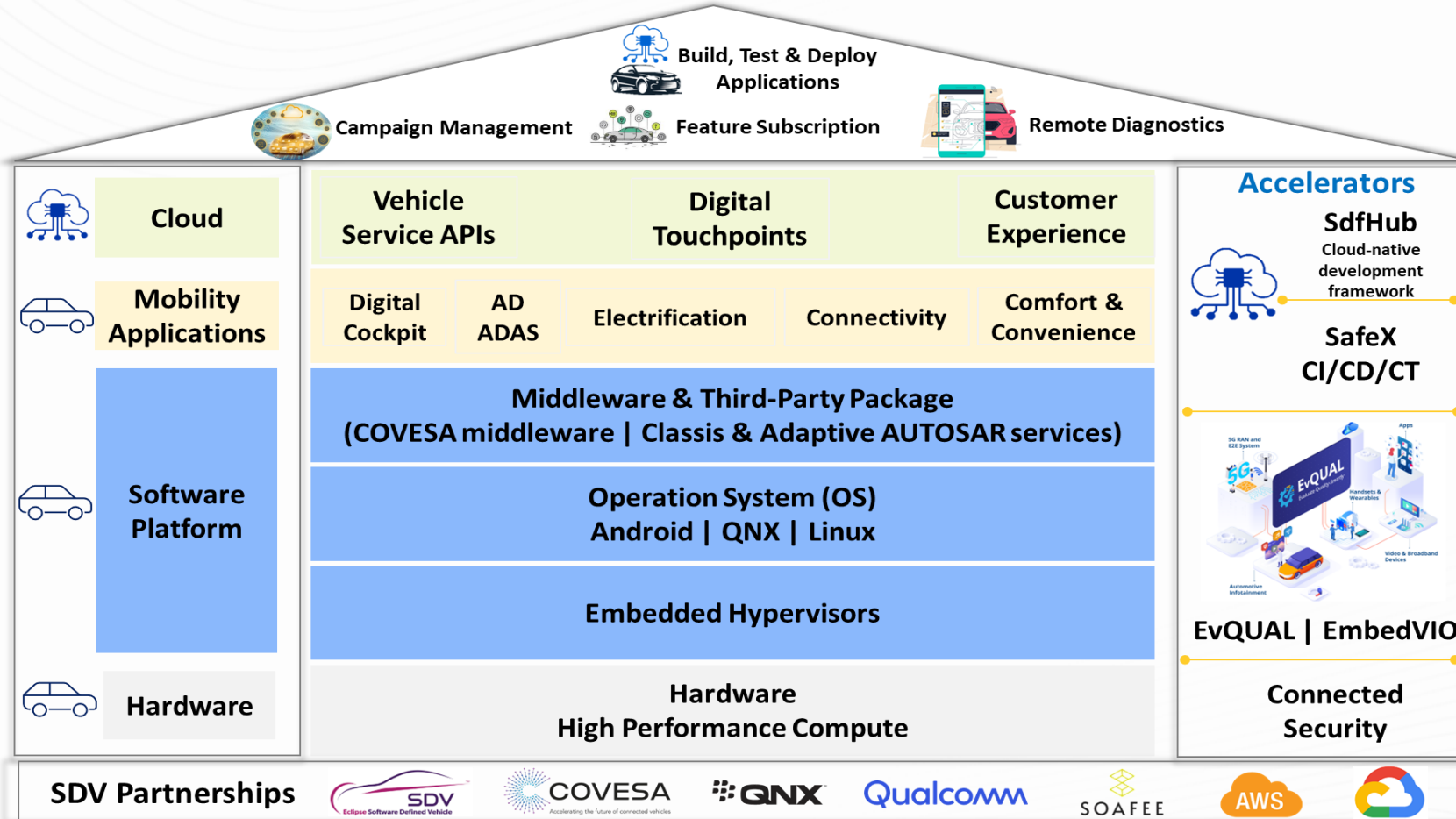
- ❖ **Semicon Agnostic Platform**
- ❖ **Feature as a Service (FaaS)**

Build, Test & Deploy Applications

Campaign Management   **Feature Subscription**   **Remote Diagnostics**

Cloud	Vehicle Service APIs	Digital Touchpoints	Customer Experience	**Accelerators**
				SdfHub Cloud-native development framework
Mobility Applications	Digital Cockpit	AD ADAS	Electrification	Connectivity	Comfort & Convenience	**SafeX CI/CD/CT**

Middleware & Third-Party Package
(COVESA middleware | Classis & Adaptive AUTOSAR services)

Operation System (OS)
Android | QNX | Linux

Software Platform

Embedded Hypervisors

EvQUAL | EmbedVIO

Hardware	Hardware High Performance Compute	Connected Security

SDV Partnerships   SDV Eclipse Software Defined Vehicle   COVESA Accelerating the future of connected vehicles   QNX   Qualcomm   SOAFEE   AWS

01 In-Cloud Development Environment

LTTSiDriVe

02 Virtualization & Digital Twin

03 GenAI Augmented SDLC

LTTSiDriVe Framework

- Cloud-native framework enabling development, build and testing of applications on the cloud

- Framework uses virtual targets with environment parity to test systems including AD/ADAS, DCU, Zonal, Edge ECU

- Campaign management (OTA) for software upgrade

- GenAI-based test case generation

USE CASES

	Auto Light Adaptation based on Ambient Environment		Driver Attention Monitoring
	Green Motion Drive Advisor		DoIP [Vehicle Health and Diagnostics]
	GenAI-based Interactive In-Vehicle Assistant		

L&T Technology Services

Restricted Circulation

Virtualization: Cloud Orchestration

High Performance Compute

QNX	Android	Linux

Hypervisor

Vehicle computer
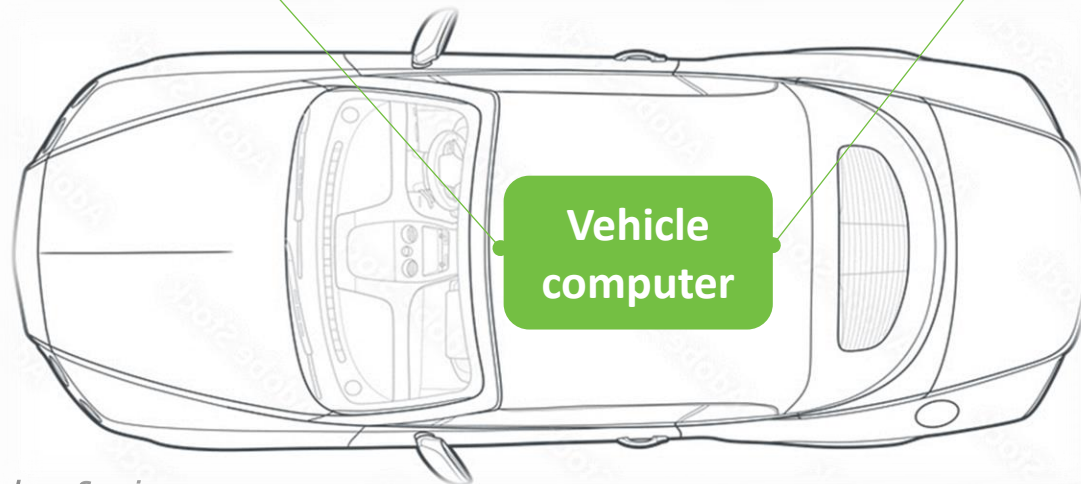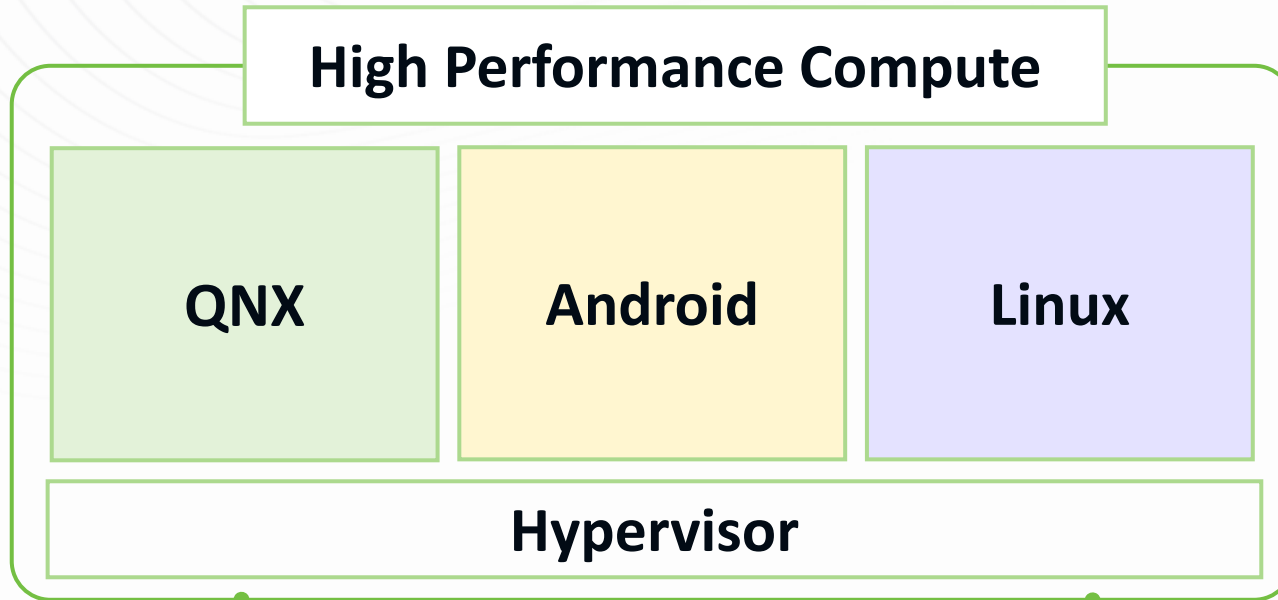
Use Cases

- **Safety**: Sensing & Actuation
- **Non-Safety**: Personalization

Success Factors

- Digital Twin libraries and car model
- Libraries: Simulators to test safety and non-safety applications

OTA : Test Rack and Configurable Zonal controllers

FOTA : Homologated Solution: Cybersecurity / UPTANE compliant Framework
Help leverage LTTS experience in OTA deployment

Vehicle

TCU
- Flash Agent(UDS DOIP)
- GPS Agent
- Cellular Agent
- CAN
- Ethernet
- 4G/LTE

← DOIP →

IVI
- Certificate Management
- Update Screen
- Flash Agent (UDS Over CAN/DOIP/A2B)
- CAN
- Ethernet
- A2B

← DOIP →
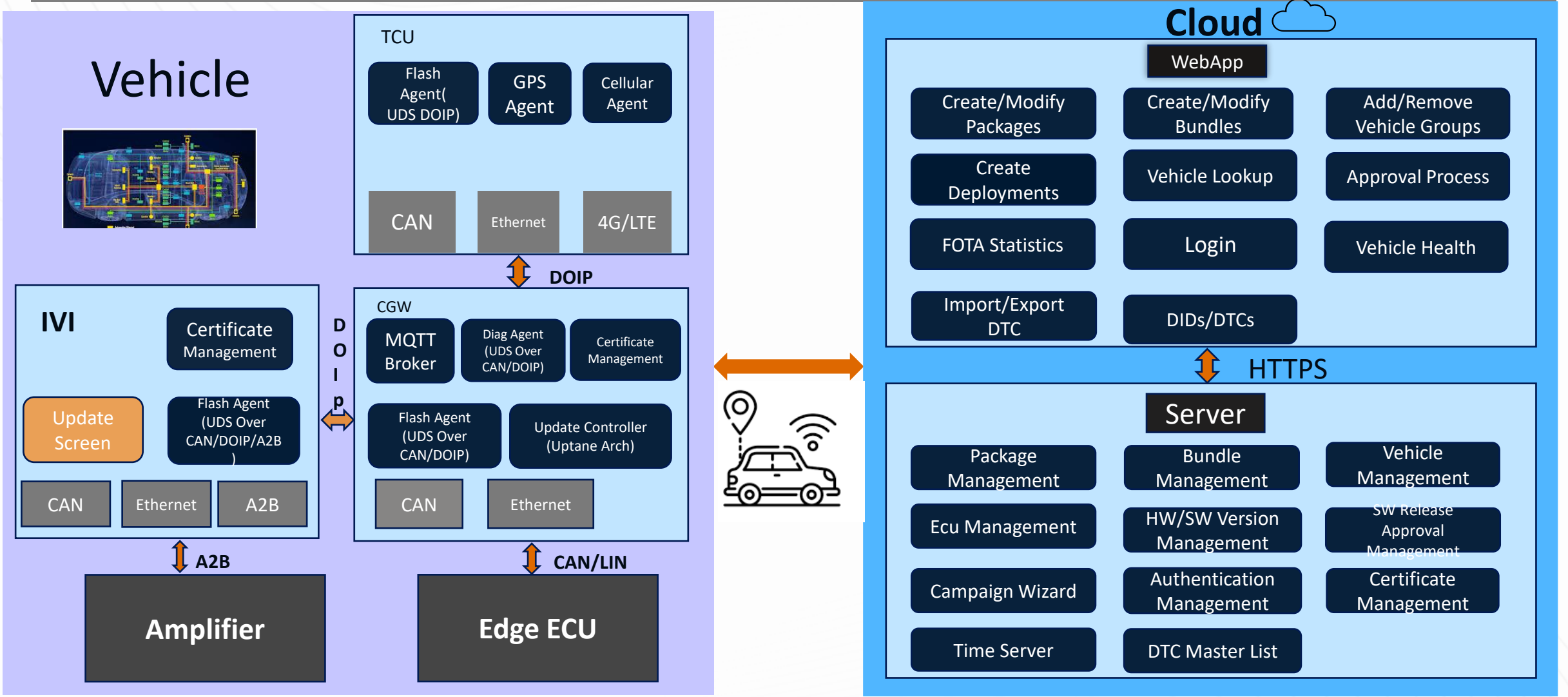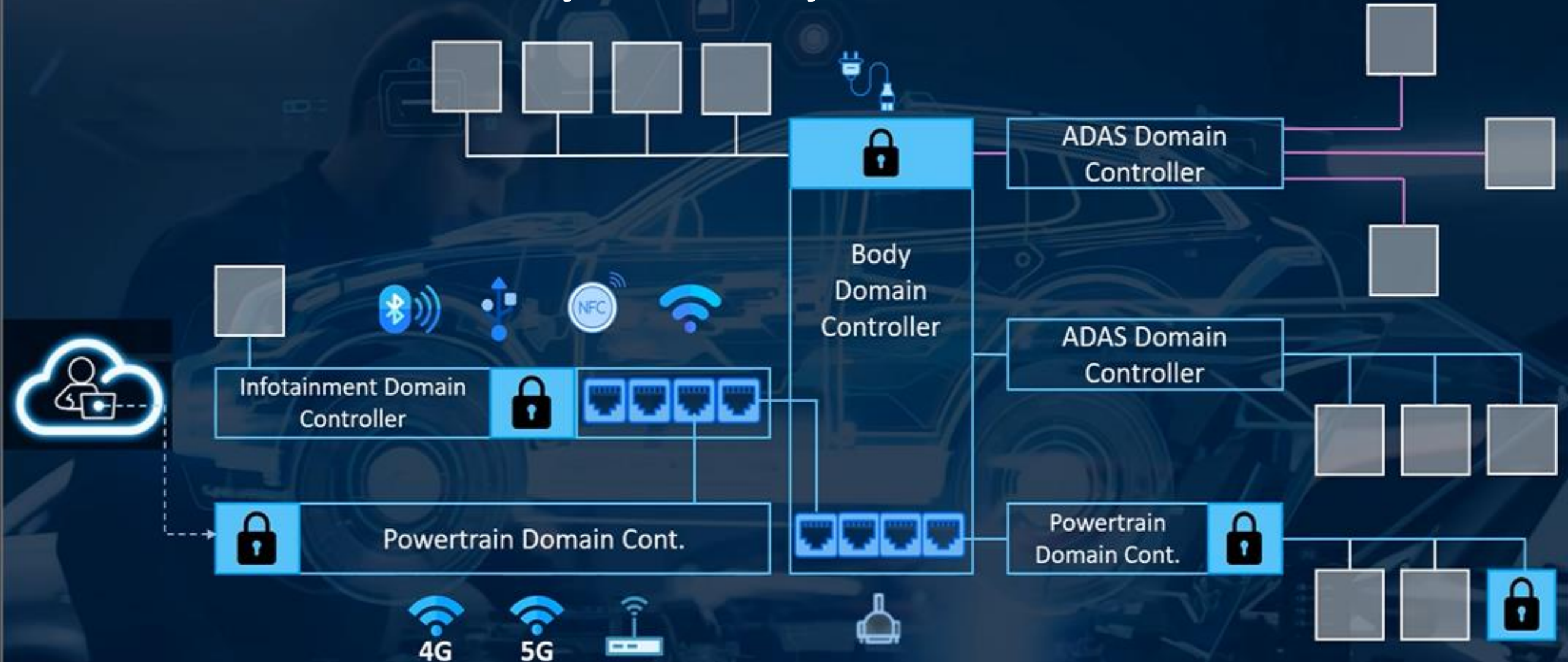
CGW
- MQTT Broker
- Diag Agent (UDS Over CAN/DOIP)
- Certificate Management
- Flash Agent (UDS Over CAN/DOIP)
- Update Controller (Uptane Arch)
- CAN
- Ethernet

← A2B → **Amplifier**

← CAN/LIN → **Edge ECU**

← HTTPS ↔ →

Cloud
WebApp
- Create/Modify Packages
- Create/Modify Bundles
- Add/Remove Vehicle Groups
- Create Deployments
- Vehicle Lookup
- Approval Process
- FOTA Statistics
- Login
- Vehicle Health
- Import/Export DTC
- DIDs/DTCs

← HTTPS →

Server
- Package Management
- Bundle Management
- Vehicle Management
- Ecu Management
- HW/SW Version Management
- SW Release Approval Management
- Campaign Wizard
- Authentication Management
- Certificate Management
- Time Server
- DTC Master List

- **Proven** and **robust OTA solution,** Successfully flashed 20+ major ECUs (BCM, EPS, ESP, TCU, Gateway and more)
- Campaign management framework for OTA updates with proven mule car and mobile HIL environment

Automotive Security

Automotive Cybersecurity Assessment Framework

L&T Technology Services

ADAS Domain Controller

Body Domain Controller

ADAS Domain Controller

Infotainment Domain Controller

Powertrain Domain Cont.

Powertrain Domain Cont.

NFC

4G   5G

Embedded ECU Security Assessment Tool - Power Apps

Embedded ECU Security Assessment Tool

Login

Embedded ECU Security Assessment Tool

As part of Automotive Security, LTTS has developed a **Process & Standard Adhered Tool** for **Embedded ECU Security Assessment**.

This tool focuses on

- **Security Study** (Reconnaissance, Items & Asset Identification, Security View)
- **Security Assessment** (Damage Scenarios, Threats, Impacts, Feasibility, Risk Determination)
- **Security Reporting** (Mitigations, Possible Solutions)

One-Stop Solution

Study & Assessment Framework, Project Management & Working Repository with Role based secure data Authentication

Process (ISO 21434) Governance

Enabled with Guidelines and Standards for zero deviation validated workflow supporting Quality Adherence

Reusability & Trend Study

Reusability in Study & Assessment enabling faster outcome. It enables multi-version studies and Risk Trend Analysis

Snapshots of CYSAF framework

Project Details

Create Project

Project ID	Customer	Project Category	Project Name	Status	Architect		
CySAF-100	Test Customer 1	Layering	Data Structuring Test	Assessment Pending	Amrutha lakshmi G L	Execute	
CySAF-101	Test Customer 2	Interacting	UI/UX Frontend Test	Study Pending	Amrutha lakshmi G L	Execute	
CySAF-102	Test Customer 3	Storing	Data Read/Writing and Compactibility test	Study Pending	V J Leo	Execute	
CySAF-103	Customer 1	Component	Infotainment Unit Usecases	Architect Approval Pending	V J Leo	View	
CySAF-104	Customer 1	Component	Anti lock braking system	Architect Approval Pending	V J Leo	View	
CySAF-105	Customer 2	Component	Airbag control system	Assessment Pending	Amrutha lakshmi G L	Execute	
CySAF-106	Customer 2	Component	TCU- GPS	Study Pending	Amrutha lakshmi G L	Execute	

System Study

Project ID : CySAF-105   Project Name : Airbag control system

System Reconnaissance Attachment — Airbag Control System11...

System Reconnaissance Remark

- System Reconnaissance ✓
- Items Identification ✓
- Assets Classification ✓
- System Security View ✓

Proceed to Assessment >>

Architecture of Airbag Control System

Upload & View

System Study

Project ID : CySAF-105   Project Name : Airbag control system

Add Items

Item ID	Item Name	Item details	
CySAF-I-116	Collision sensors		>
CySAF-I-117	Pressure Sensor		>
CySAF-I-118	Driver Positioning Sensor		>
CySAF-I-119	PSI5 Protocol Communication Medium		>
CySAF-I-120	SPI Protocol Communication Medium		>
CySAF-I-121	CAN Protocol Communication Medium		>
CySAF-I-122	LIN Protocol Communication Medium		>
CySAF-I-123	MCU		>
CySAF-I-124	Squib Drivers		>

Edit

Item/Component
Collision sensors

Functionality
It detects the collision and sends the signal to the airbag chip

Network Interfacing
External

Operational Environment
It detects the collision and sends the signal to the airbag chip

Product Lifecycle Phase

- System Reconnaissance ✓
- Items Identification ✓
- Assets Classification ✓
- System Security View ✓

Proceed to Assessment >>

System Study

Project ID : CySAF-105   Project Name : Airbag control system

System Security View Attachments — Airbag Control System2....

System Security View Remark

Threat Model File
There is no file.
Upload file

- System Reconnaissance ✓
- Items Identification ✓
- Assets Classification ✓
- System Security View ✓

Proceed to Assessment >>

Upload & View

Three Core dimensions of LTTSiDriVe™

High Performance Compute-Stack

Virtual Development

Tool Chains, Digital Twins & Libraries