SDV and new vehicle architectures: challenges and solutions from a semiconductor perspective

Franck Galtié

Safety Fellow, NXP Semiconductors

Dr. Franck Galtié – Functional Safety Fellow, NXP Central Technical Office (CTO)

- 26 years of experience in Semiconductor and Automotive System development.
- Fellow at NXP covering both Automotive and Industrial Safety
- Various experience like STM, Freescale, Renesas, Siemens VDO, Continental and Hella
- Ph.D in Engineering Sciences with a specialization in Semiconductors
- Located in NXP Toulouse, France
- Member of ISO TC22/SC32/WG8 covering ISO26262 & ISO21448

Functional safety is the absence of **unreasonable risk** due to **hazards** caused by **malfunctioning** behavior of electrical or electronic **systems**

Functional Safety Standard « jungle »

PAS: Publicly Available Specification

KEY STANDARDS RELEVANT FOR ALL APPLICATIONS

* TC22/SC32

Standard	Owner	Status	Next step
ISO26262 (Road vehicle, functional safety)	ISO WG8*	2nd edition published in 2018	3rd edition not expected before 2027
ISO PAS 8926 (use of pre existing SW)	ISO WG8*	1st edition published in January 2024 New	Integration into ISO26262 3rd edition?
JA1020: "recom. for the Rust Progr. Language in Safety-Related Systems"	SAE	1st draft being created with target publication in Q4/2024 Soon	Not defined yet
SAE J2980 (Considerations for ISO26262 ASIL Hazard Classification)	SAE	2nd edition published in 2018 and 3rd (to align to 2nd edition of ISO26262 and cover trucks) in October 2023 New	Considerations about SOTIF, STPA, …
P2851 (Standard for functional safety data format for interoperability within the dependability lifecycle)	IEEE	Based document published in Dec 2023 New	P2851.1 (FuSa and reliability) approved aiming publication by end of 2025
Accellera (standardize exchange of data related to functional safety)	accellera FS WG	1st whitepaper published in May 2021 2nd whitepaper published in Dec 2023 New	Continue with the Data Model for FMEDA
J3187: "recom. for the System Theoretic Process Analysis (STPA)"	SAE	2nd edition published in May 2023 Appendixes 1 (HMI) and 2 (SOTIF) published in September 2023 New	Appendix 4 (security) in preparation

List not completed

ADAS/AD

* TC22/SC32

Standard	Owner	Status	Next step
ISO26262 (Road vehicle, functional safety)	ISO WG8*	2nd edition published in 2018	3rd edition not expected before 2027. Including better link to SOTIF?
SAE J3016 / ISO/SAE PAS 22736 (Taxonomy and Definitions for Terms of Driving Automation Systems)	ISO TC204 SAE ORAD	4th edition of SAE RP published in 2021 1st combined SAE/ISO in 2021	Several possible mods in discussion for 5th edition of J3016 and liaison with ISO ongoing for 2nd edition of PAS 22736
ISO/SAE 21434 (Automotive Security)	ISO WG11 SAE	1st edition published in 2021	One PAS and one TR in preparation. Due e/o 2024
ISO21448 (SOTIF – Safety of the Intended Function)	ISO WG8*	1st edition published in 2022	Integration into ISO26262?
UL4600 (Safety for the Evaluation of Autonomous Products)	UL	3rd edition published in March 2023	4th edition under consideration
UN R157 (ALKS – Automated Lane Keeping System)	UNECE	1st edition published in March 2021 4th amendment in March 2023	Not yet defined
ISO TS 5083 (Safety for automated driving systems) Derived from TS 4804 (and from SaFAD)	ISO WG13*	Publication planned for 2nd half of 2024 Soon	Waiting for finalization and publication
ISO TR 9839 (predictive maintenance)	ISO WG8*	Published in August 2023 New	Integration into ISO26262?
ISO/IEC TR 5469 (Functional safety and AI systems)	ISO IEC JTC1/SC42	Published in January 2024 New	Extension into ISO/IEC TS 22440
ISO PAS 8800 (Safety and artificial intelligence)	ISO WG14*	Waiting for publication (2H24?) Soon	Integration into ISO26262?

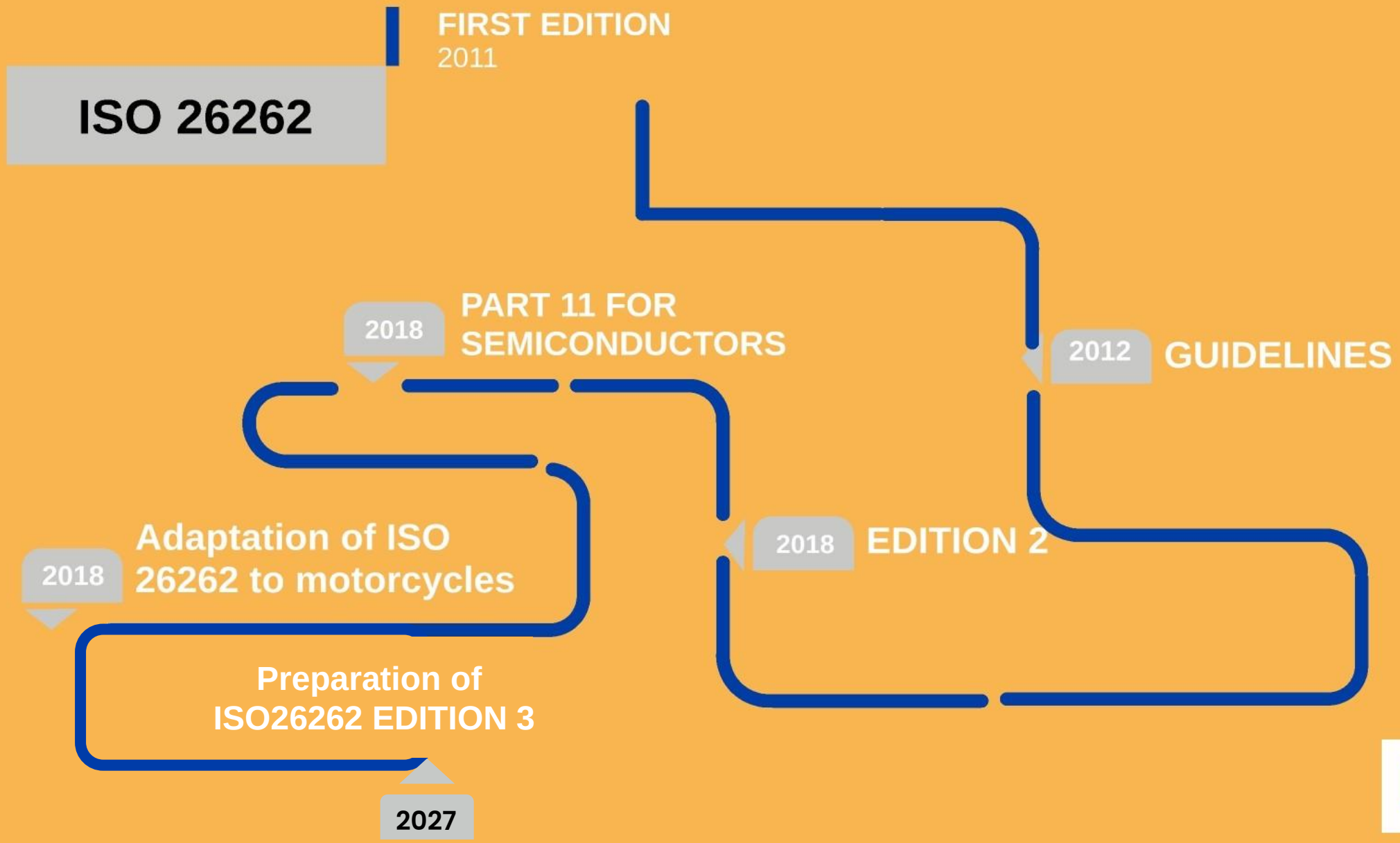
List not completed

GREEN VEHICLES

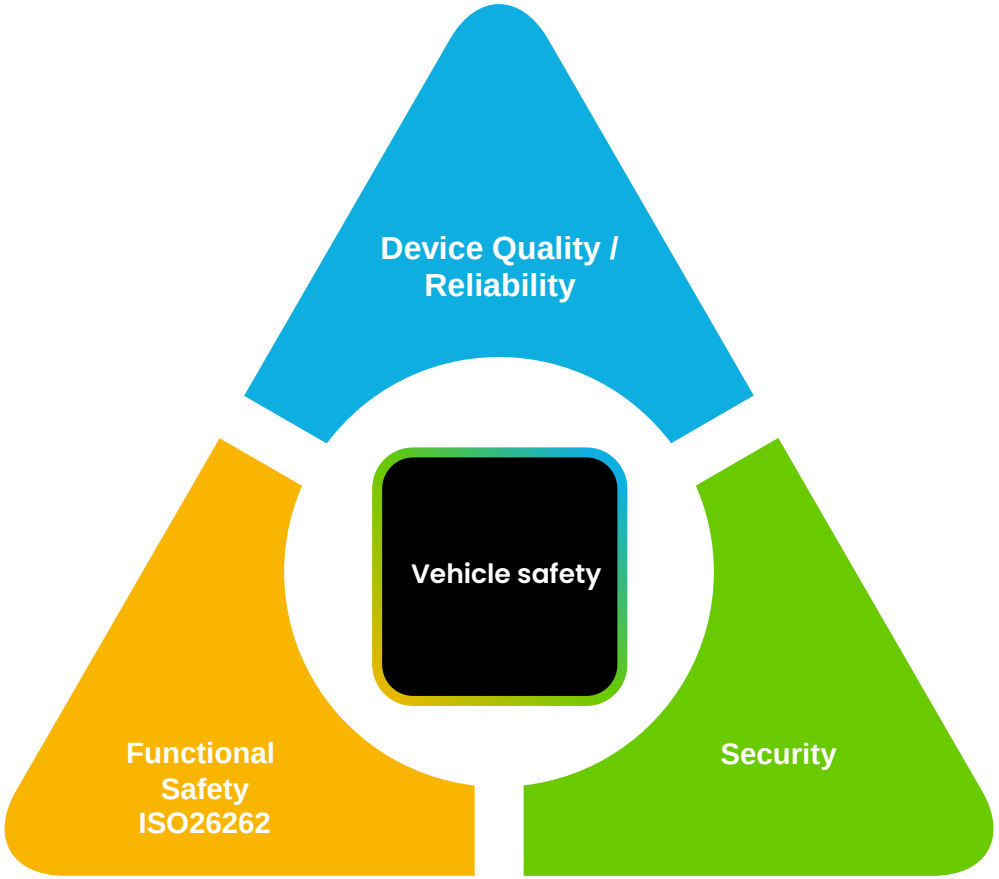
* TC22/SC32

Standard	Owner	Status	Next step
ISO26262 (Road vehicle, functional safety)	ISO WG8*	2nd edition published in 2018	3rd edition not expected before 2027
ISO TR 9968 (Application to generic rechargeable energy storage systems for new energy vehicles)	ISO WG8*	1st edition published in June 2023 New	Integration into ISO26262 3rd edition?

Credits: Riccardo Vincelli – Renesas
IQPC Safety week 2025


ISO 26262
FIRST EDITION
2011
2012
GUIDELINES
2018
EDITION 2
2018
PART 11 FOR SEMICONDUCTORS
2018
Adaptation of ISO 26262 to motorcycles
Preparation of ISO26262 EDITION 3
2027

Elements of a safe system



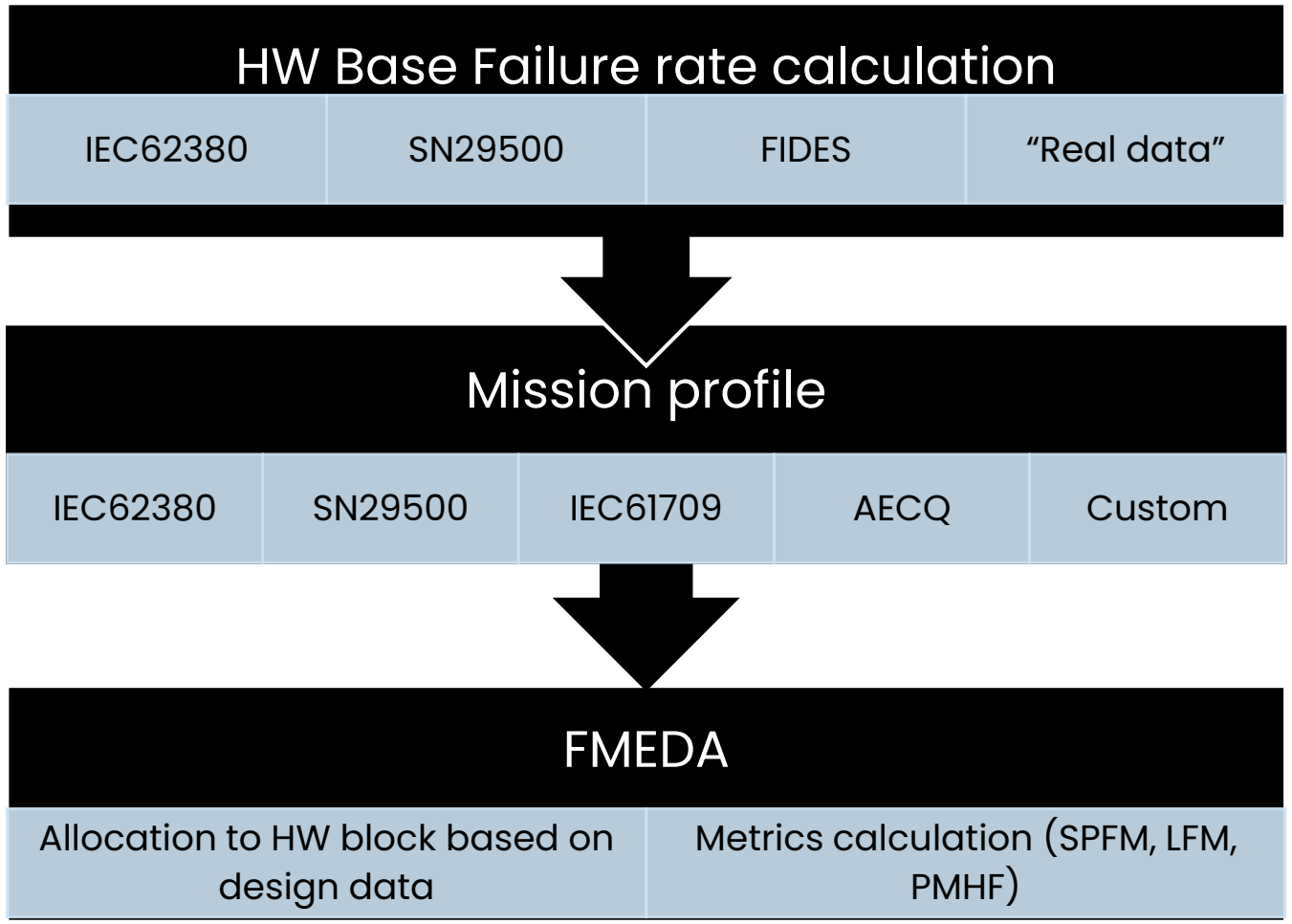
Functional safety
Reduce accident by system failures
ISO 26262

Security
Reduce accident by system hack
ISO21434

Device reliability
Zero component failures & systematic fault
AITF 16949 / AECQ / etc…

Vehicle Safety
Reduce Human errors / system limitation
ISO 21448

Base failure rate, mission profile and FMEDA – a complex relationship



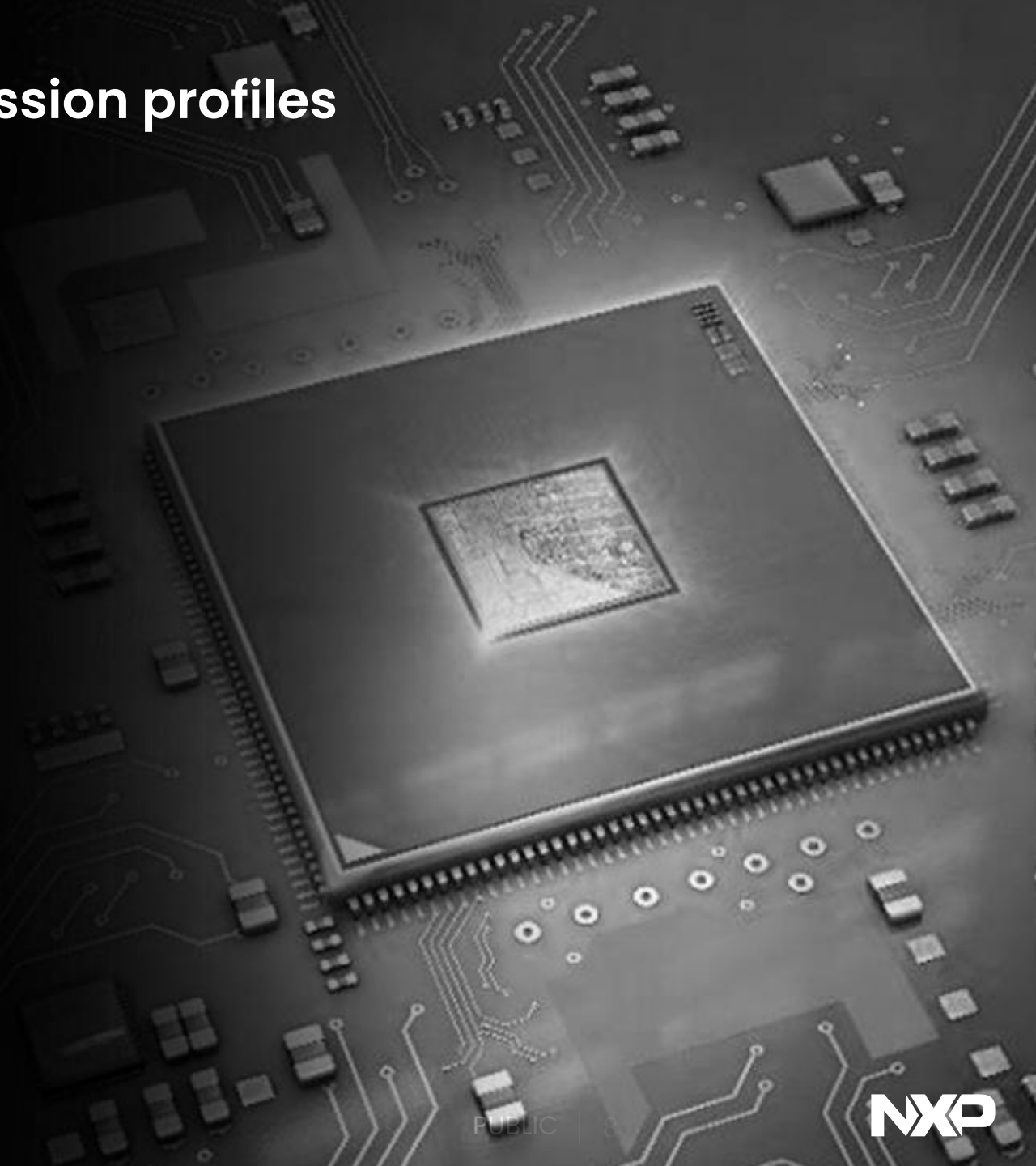
- Outdated reliability handbooks
- Hard to use real data, except for specific techno
- Major objective: compare apples with apples

- Huge impact on the base failure rate
- Not representative to real usage
- Different approach than for device qualification

- Metrics are mandatory
- PMHF targets down to 10 FIT (ie. Residual failure rate after diagnostic)
- Can heavily impact safety concept

Electric Vehicle leads to Extended mission profiles

- High impact on design
- High impact on reliability
- High impact on base failure rate
- Regular safety approach may not be the most appropriate



Is Silicon prognostic a solution ?

Silicon prognostic is few words

Objectives

- Predict failures and estimate remaining lifetime
- Improve reliability and reduce downtime
- Enable proactive maintenance strategies
- Support low-power design methodologies
- Facilitate root cause analysis and closed-loop reliability modeling

Use cases

- Automotive: battery monitoring, mission profiling
- Industrial: equipment health monitoring
- Data centers: silent data corruption detection
- Avionics: engine tracking and airframe maintenance

Technologies

- Embedded sensors (temperature, voltage, current)
- Margin detection flops, ring oscillators, LTUs
- Data analytics and AI/ML algorithms
- Silicon odometer, PoST, Ring OSC

Standards

- ISO TR9839 – Predictive Maintenance
- IEEE FSSC Prognosis Workgroup
- ISO 26262 (3rd Edition) – Functional Safety

New challenges
Functional Safety

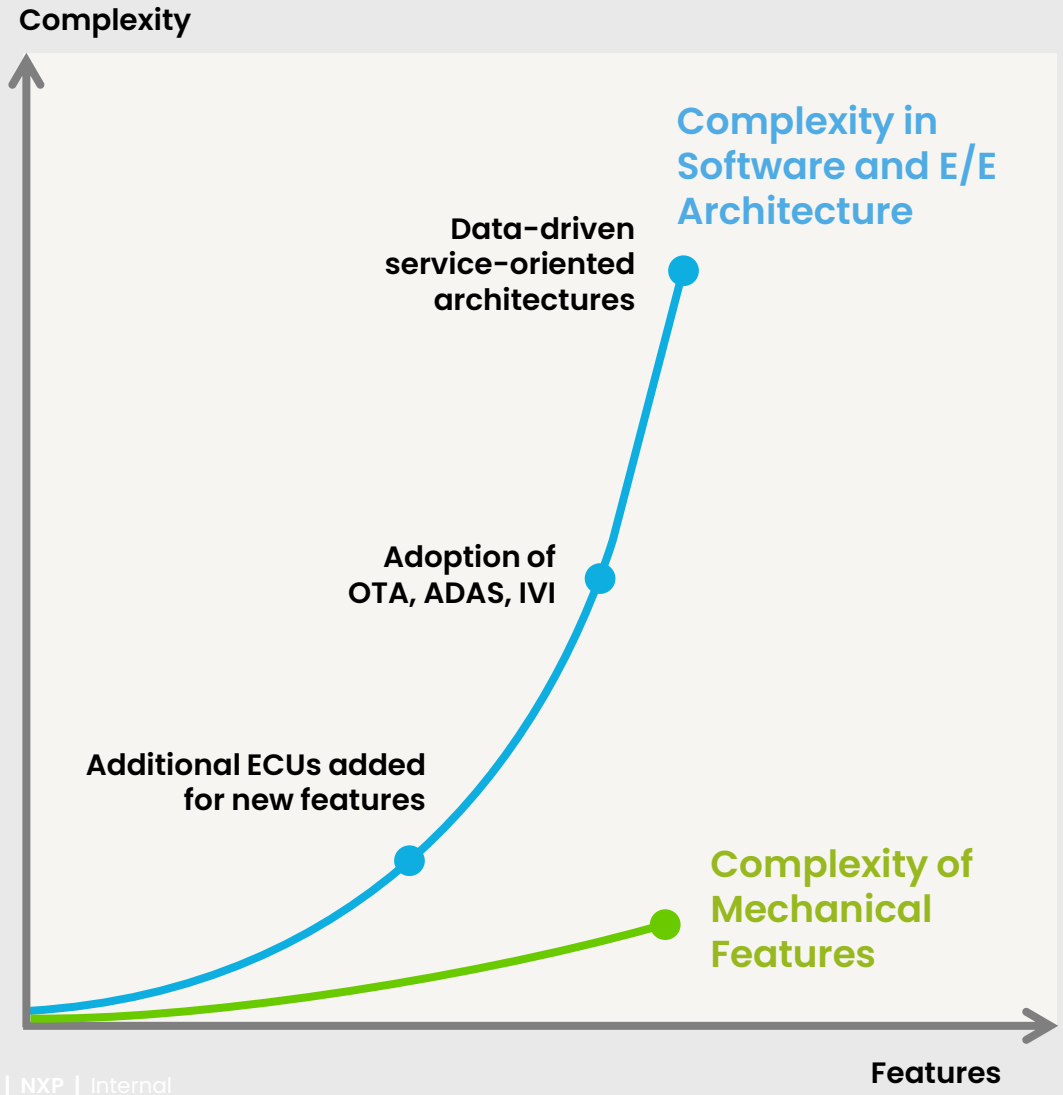
Massive disruption underway

Electric

Data-driven

Safe

Automotive industry must navigate mounting challenges



Rising cost and complexity of architectures in a hypercompetitive market

- Automakers reducing EV vehicle ASPs by ~20% to stay competitive
- ECU and software growth exponentially increasing in complexity

Leveraging vehicle data for new revenue streams

- OEMs have multi-billion-dollar revenue targets from software revenue by 2030

Reducing design cycle of new models from ~5 years to ~2 years

- New entrants pushing faster design cycles for new model introductions

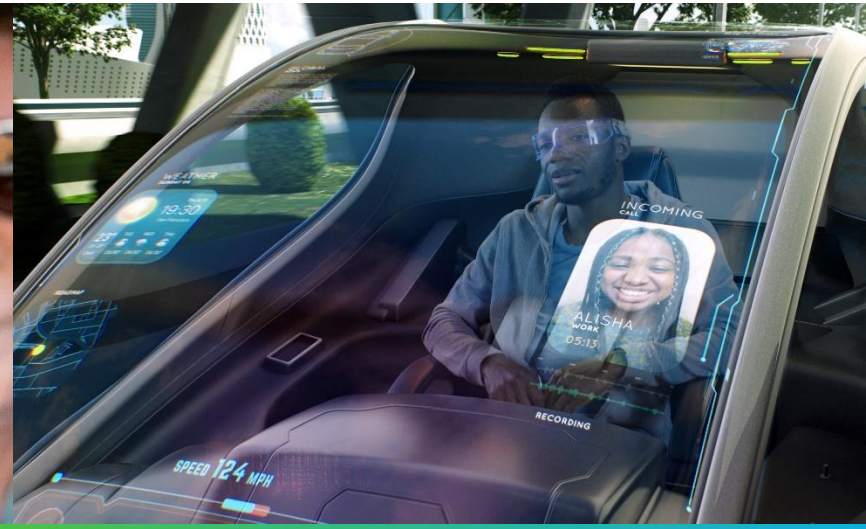
How will SDV help you differentiate?

What software-defined innovation, for which evolution …

Or merely an engineering execution issue: reducing complexity by decoupling hardware from software?

Efficiency

Safety and reliability



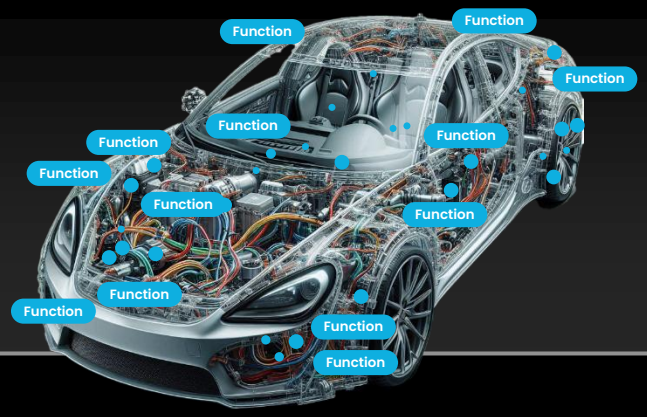
Personalized

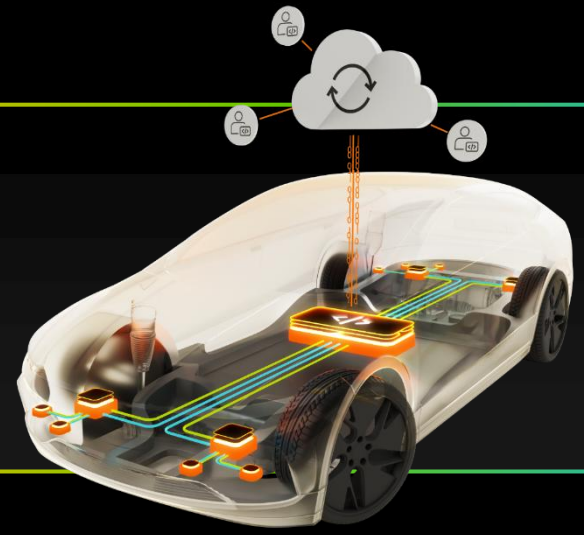
Software-defined vehicle

Modularity, flexibility, and speed enables lower Total Cost of Ownership (TCO)

Before SDVs	With SDVs
Static	Dynamic, updatable
Best performance when new	Performance increases over time
Loses value over time	Value increases over time

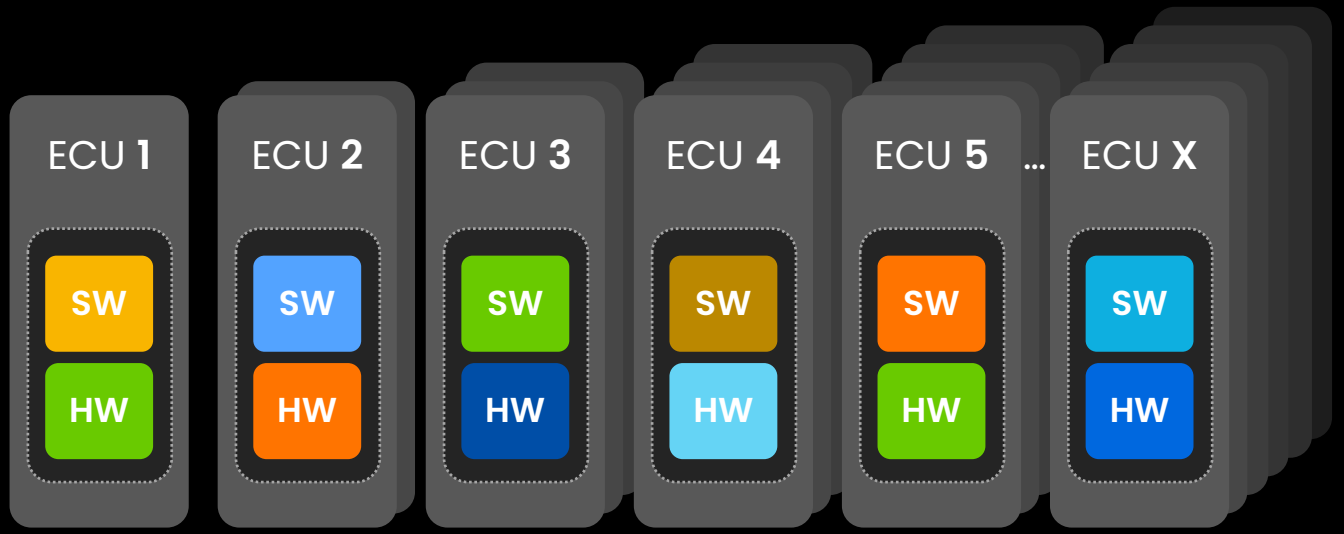
Hardware oriented vehicle

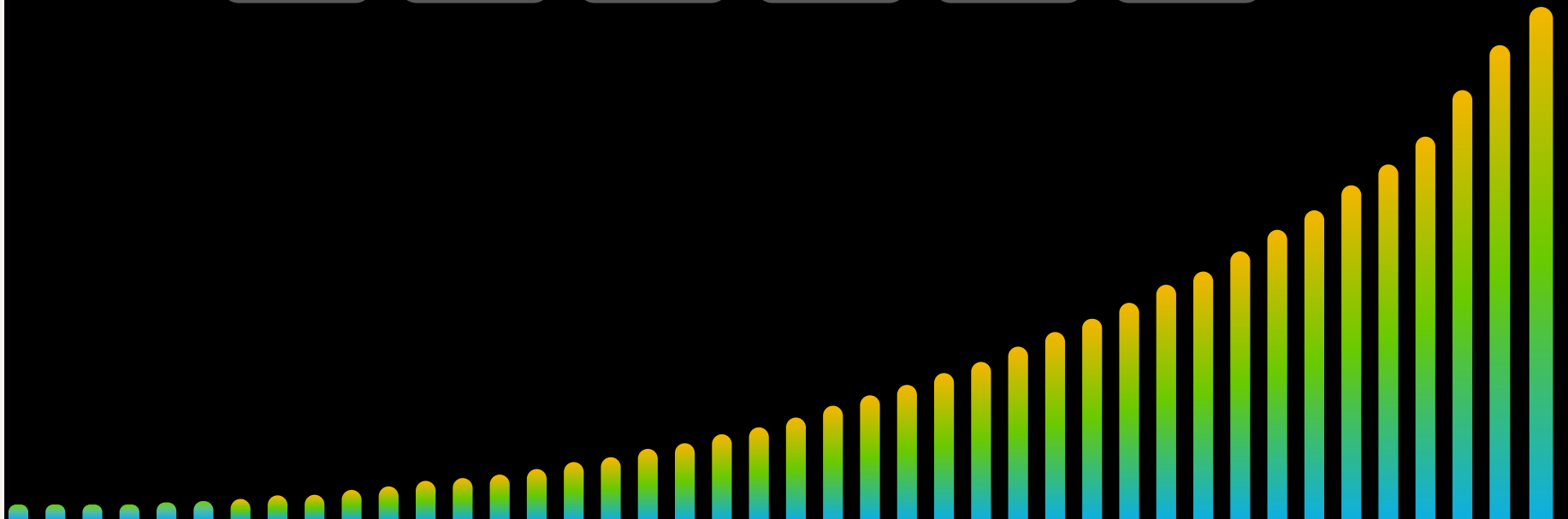




Efforts exponentially **increases with more ECUs**

Separate integration **efforts for every ECU**





Software-Defined EV platform

HW compute platform for vehicle computer, zones and end nodes, battery management, networking and power management

Safe automation
Radar, driver monitoring, safety systems

Software-Defined EV platform

HW compute platform for vehicle computer, zones and end nodes, battery management, networking and power management


User interaction
Telematics, car access, eCockpit, radio, touch systems
Safe automation
Radar, driver monitoring, safety systems
Software-Defined EV platform
HW compute platform for vehicle computer, zones and end nodes, battery management, networking and power management
NXP

Software
Vehicle-integration platform, middleware, firmware, machine learning

User interaction
Telematics, car access, eCockpit, radio, touch systems

Safe automation
Radar, driver monitoring, safety systems

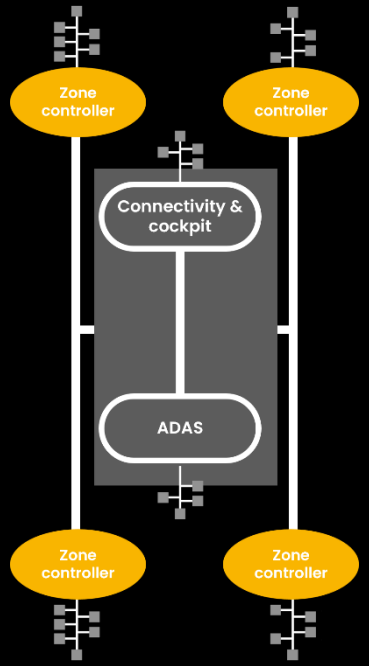
Software-Defined EV platform

HW compute platform for vehicle computer, zones and end nodes, battery management, networking and power management

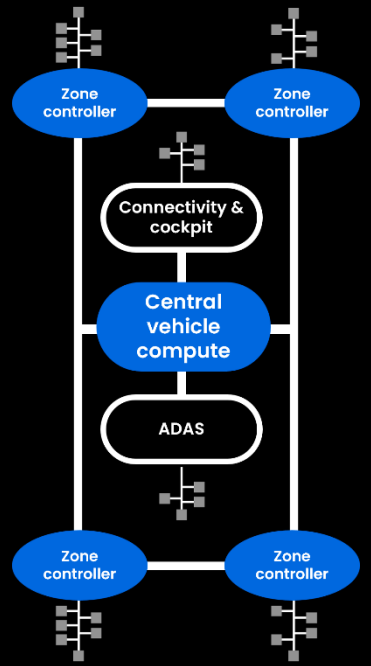

Cloud
Virtual SoCs, lifecycle management
Software
Vehicle-integration platform, middleware, firmware, machine learning
User interaction
Telematics, car access, eCockpit, radio, touch systems
Safe automation
Radar, driver monitoring, safety systems
Software-Defined EV platform
HW compute platform for vehicle computer, zones and end nodes, battery management, networking and power management

Trending to three different E/E architectures

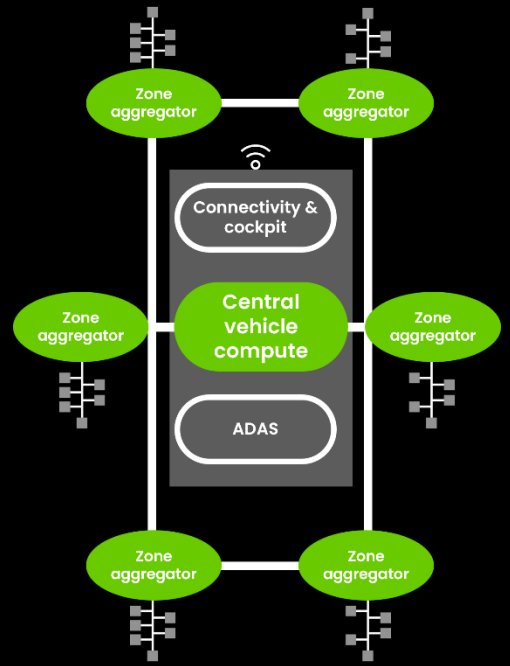
Distributed Zonal



Vehicle Compute & Zonal



Consolidated Compute



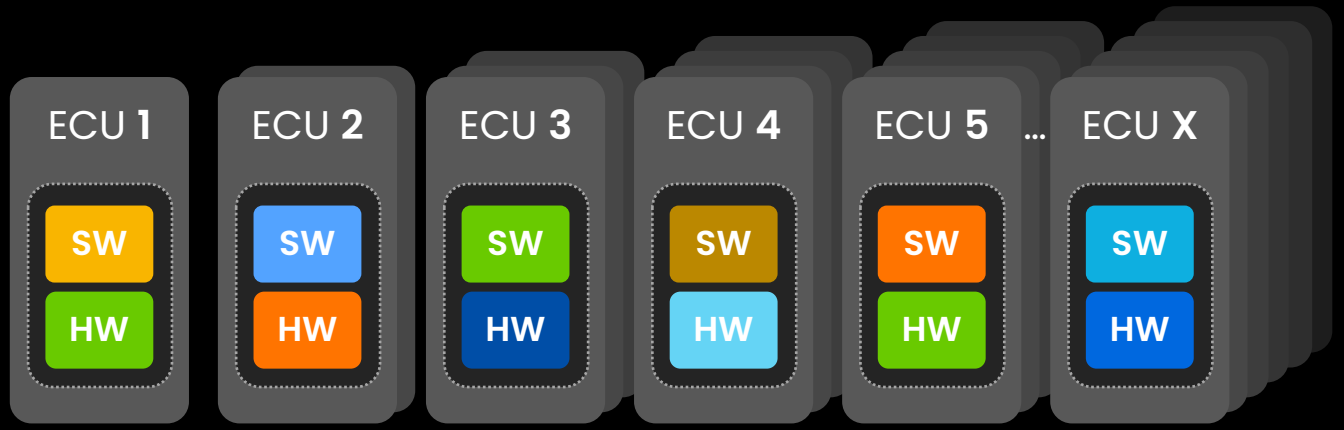
Initial development effort	+	+ +	+ + +
Scalability across fleet	+	+ + +	+ +
Upgradability beyond IVI (ease of adding new SW functions)	+	+ +	+ + +
BoM cost (electronics + harness)	+ +	+	+ +

Next generation
Functional Safety

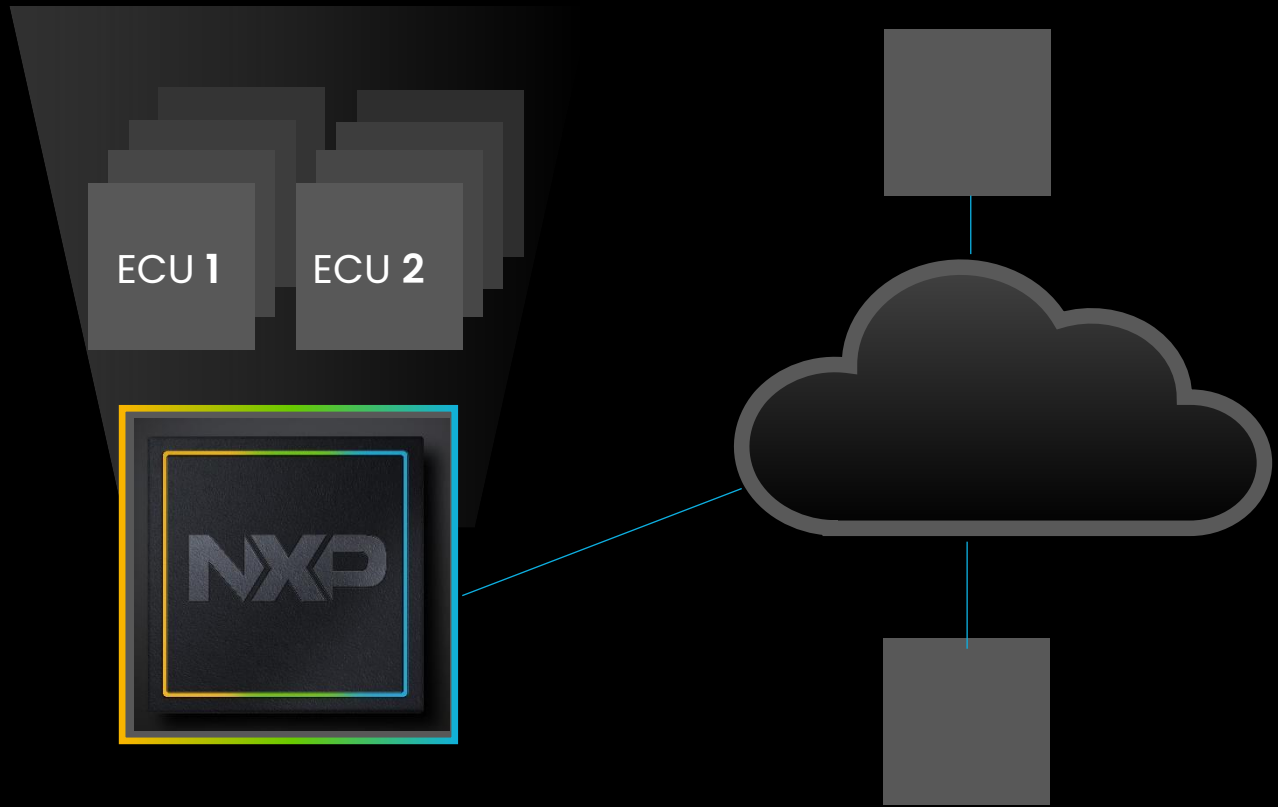
Integration challenge

New concept of Virtual ECU

Consolidation requires isolation and virtualization technologies



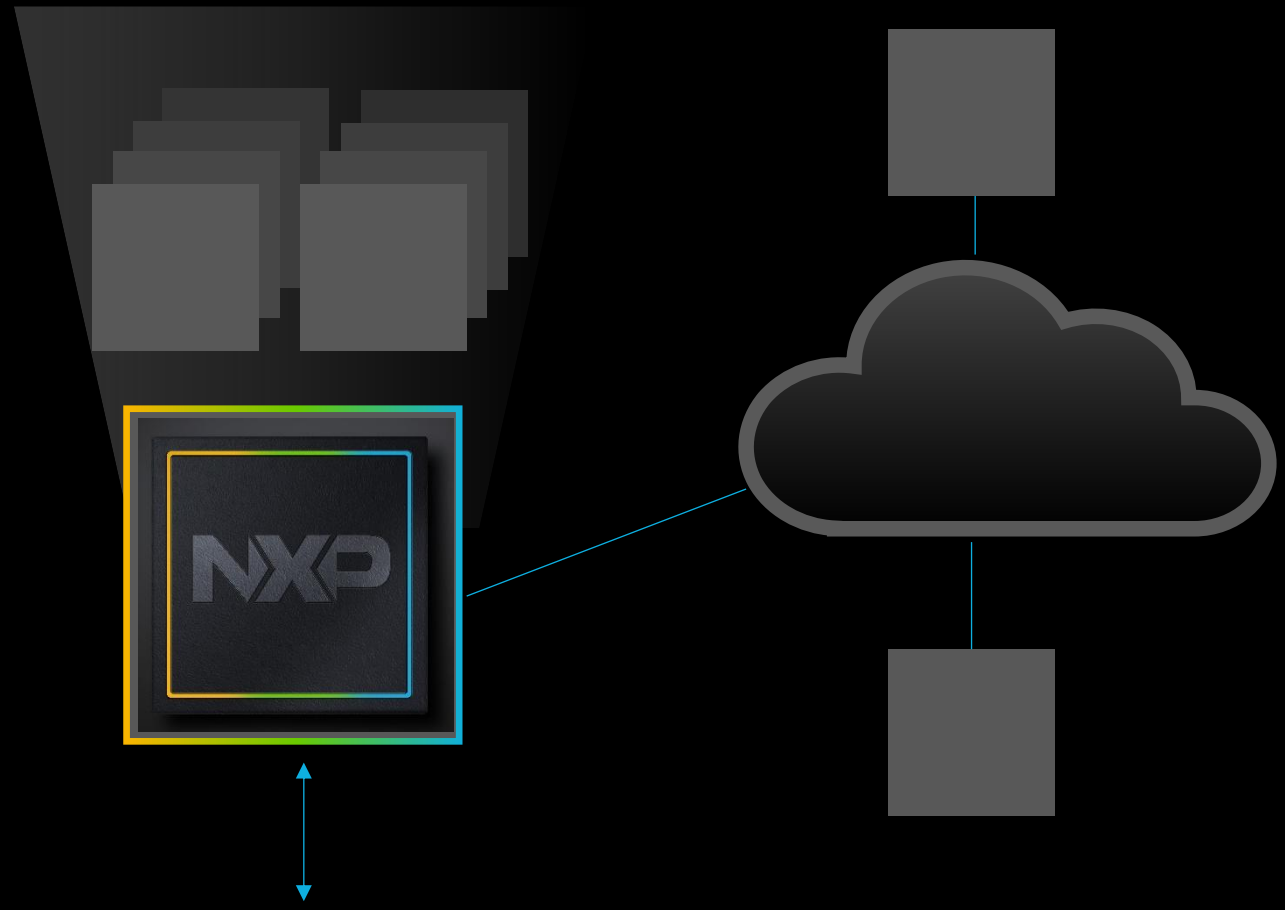
Hosting multiple ECUs in a single central compute



Virtual ECU concept

- Safety multi-criticality
- Avoid interferences
- Individual runtime
- Different vendor per VECU

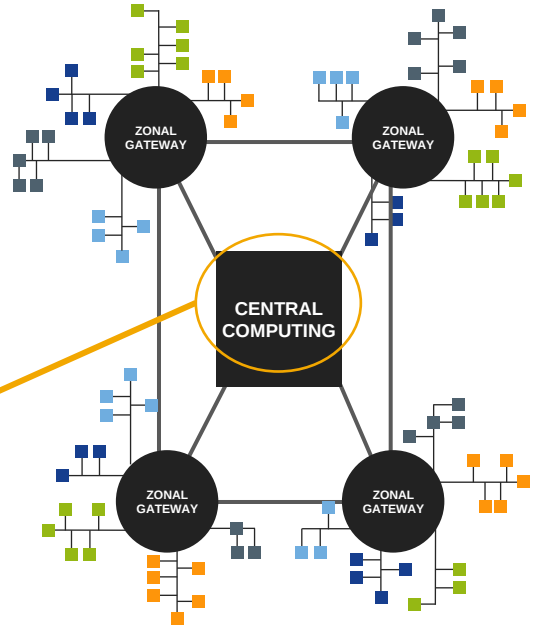
Hosting multiple ECUs in a single central compute

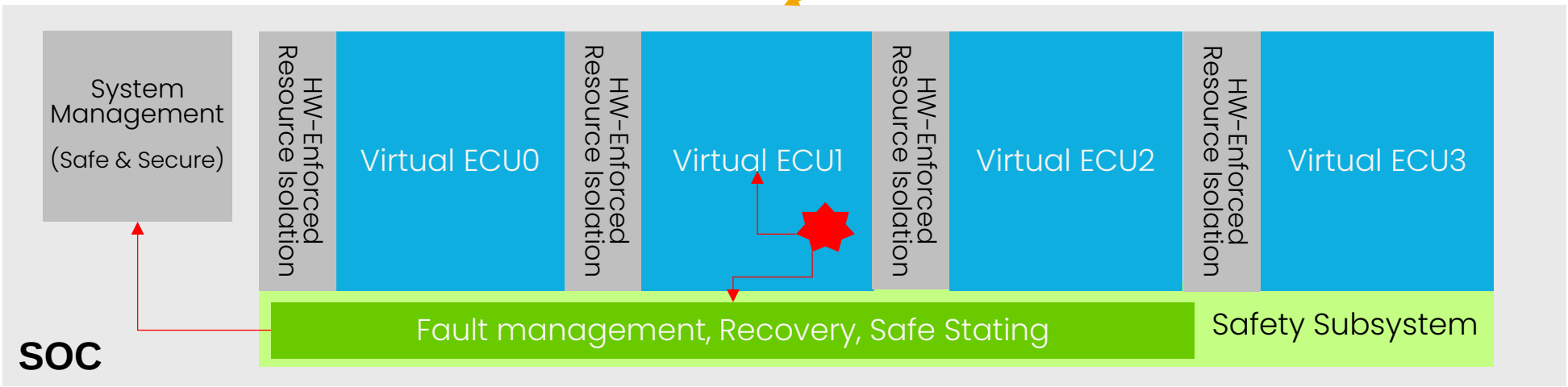


Availability: multi-application isolation & fault reaction

- Central and Zonal gateway's managing data for multiple ECU's

- Critical to ensure isolation between virtual ECU's
  - Functional isolation
  - Independent fault detection and reaction
  - Enable virtual ECU restart, minimize SoC reset as recovery

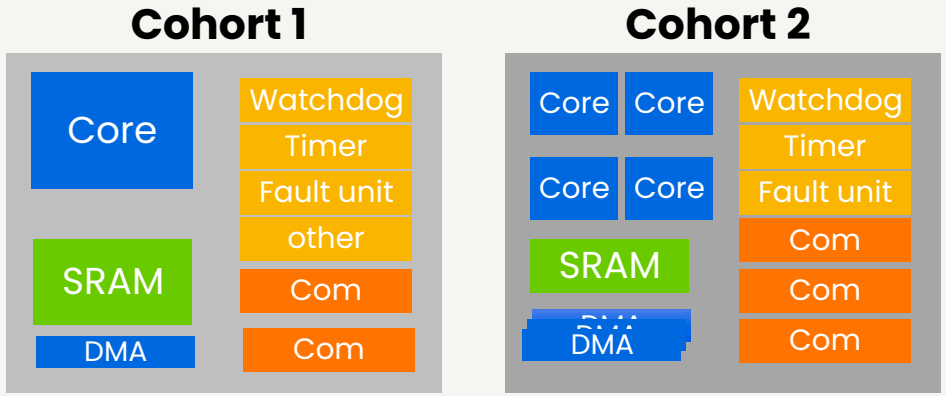




Virtual ECU: cohort concept – a collection of SOC resources (HW and SW)

- Cohort characteristics:
  - A Cohort runs one or more applications
  - Defines a 'clean' boundary between SoC resources
  - HW and SW architectures ensure no interference among Cohorts
  - Each Cohort can be independently managed (run, idle, safe, etc…)
  - Each Cohort can be split into multiple "Domains"

- Overall partitioning ownership
  - System Cohort partitioning Manager runs at boot
  - System Base Cohort controls the runtime
  - Foundation SS (FSS) is System Base Cohort



Safety envelope – Fault reactions

Detection

Isolation

Local Reactions

Escalations

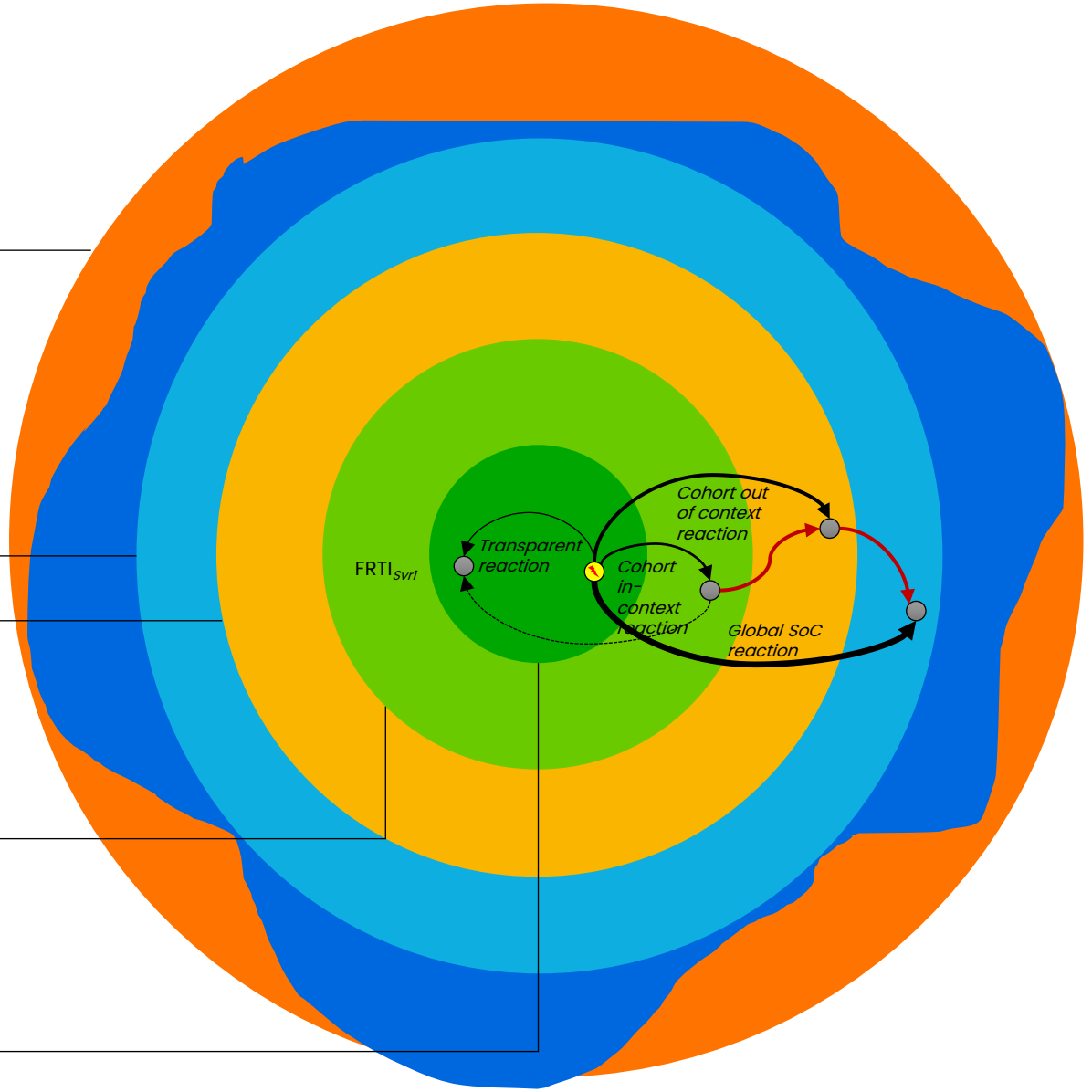
Unsafe states

SoC safe states

Cohort safe states

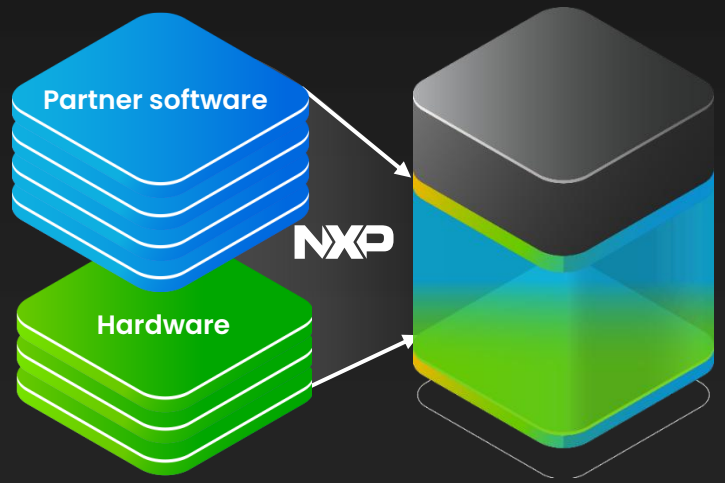
Application safe states

Normal operation

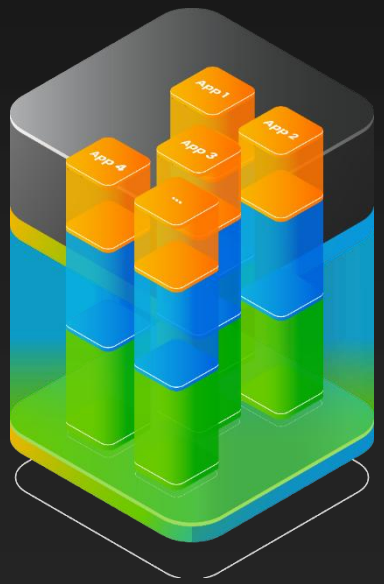


Making SDV a reality, step by step …

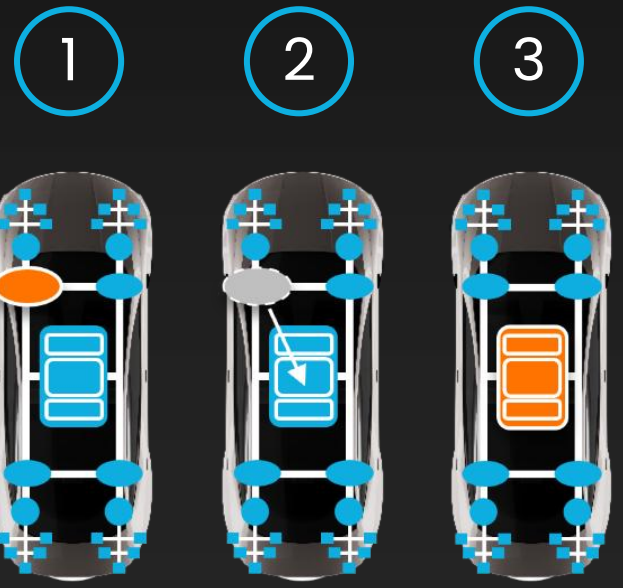
Streamline development with pre-integrated software

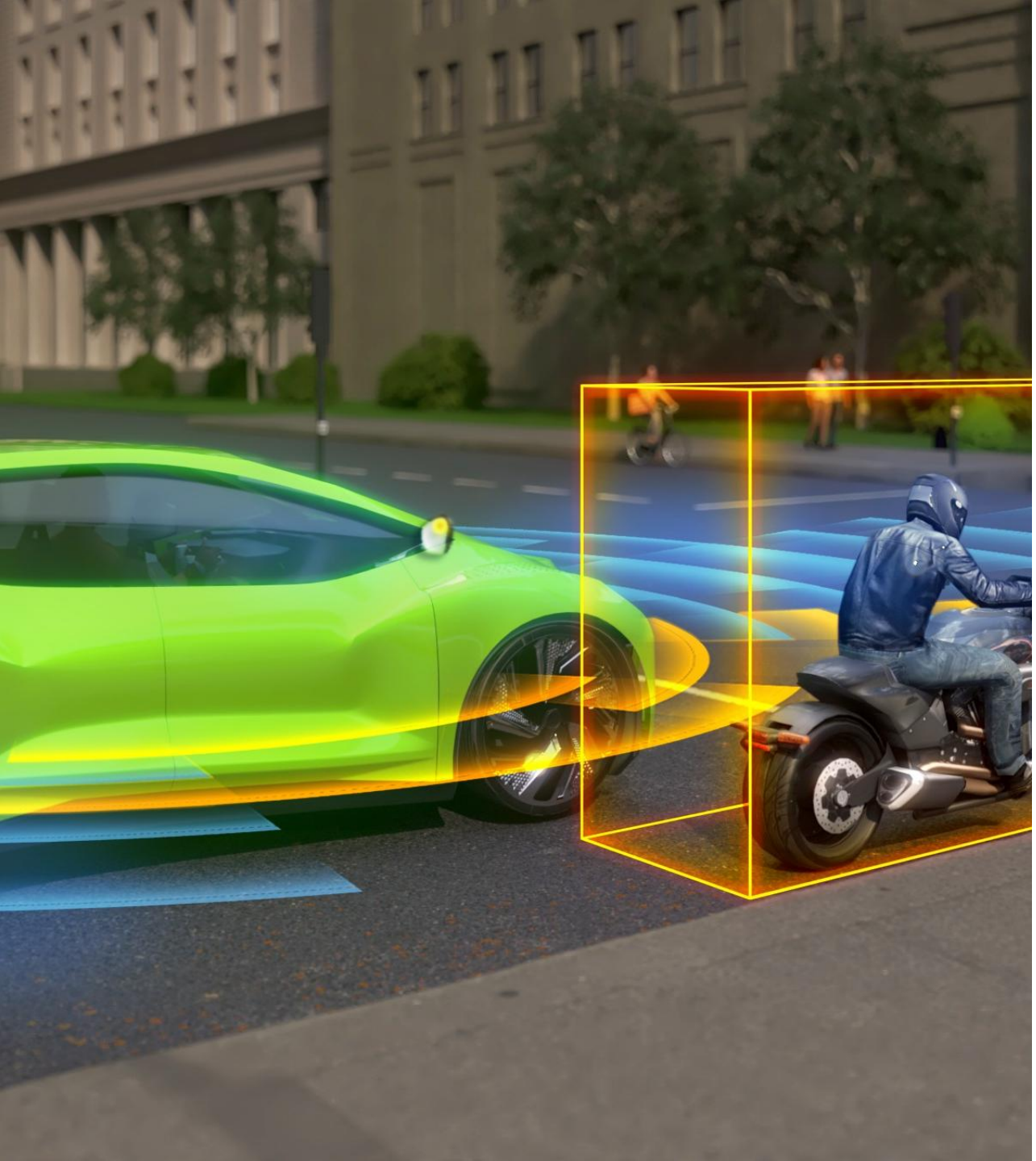


Consolidate without compromising safety and security



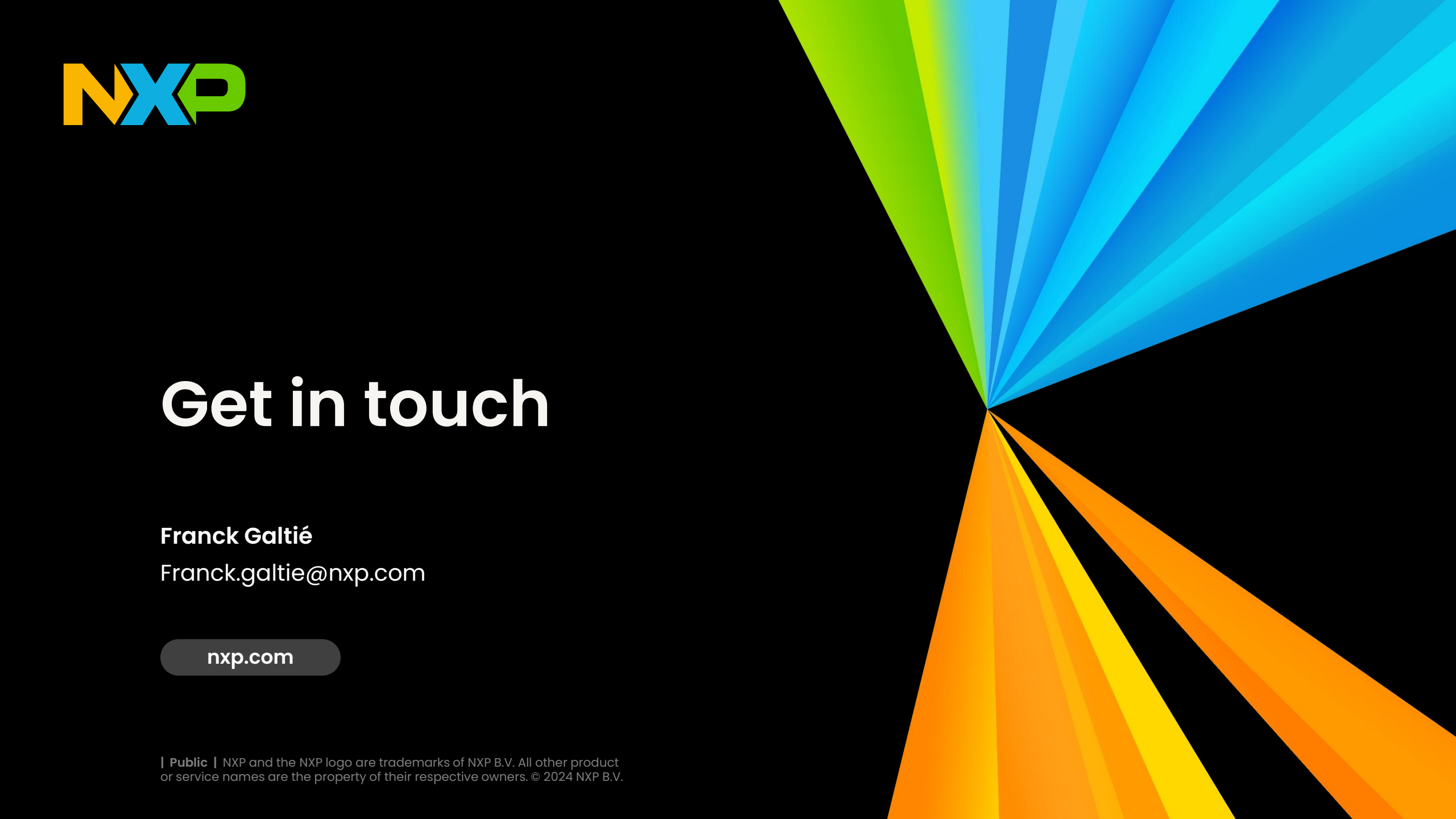
A platform to scale, reconfigure, move functions





Making mobility safe and secure

ECU Consolidation	Vehicle network architecture evolution domain to zonal, high bandwidth comms, mixed criticality processing
Isolation & Availability	Enable high performance mixed criticality processing and multi-application fault handling and recovery
Predictive Maintenance	Enable in-field silicon lifecycle health monitoring and predictive maintenance



Get in touch

Franck Galtié
Franck.galtie@nxp.com

nxp.com