Functional Safety in Highly Autonomous Vehicles - Microcontroller Perspectives

Mathieu Blazy-Winning

Functional Safety Director NXP Semiconductors

September 2019

NXP

SECURE CONNECTIONS FOR A SMARTER WORLD

Global Mega Trends
An Incredible Opportunity

CONNECTIVITY

AUTONOMY

ELECTRIFICATION

SAFE AND SECURE MOBILITY

AND AN INCREDIBLE RESPONSIBILITY

1.3 MILLION

Road traffic deaths occur every year

OUT OF ALL ACCIDENTS GLOBALLY,

90% are caused by

HUMAN ERROR

Source: Seattle's Vision Zero Plan/Documents/Departments/beSuperSafe/VisionZeroPlan, ASIRT.ORG

NXP

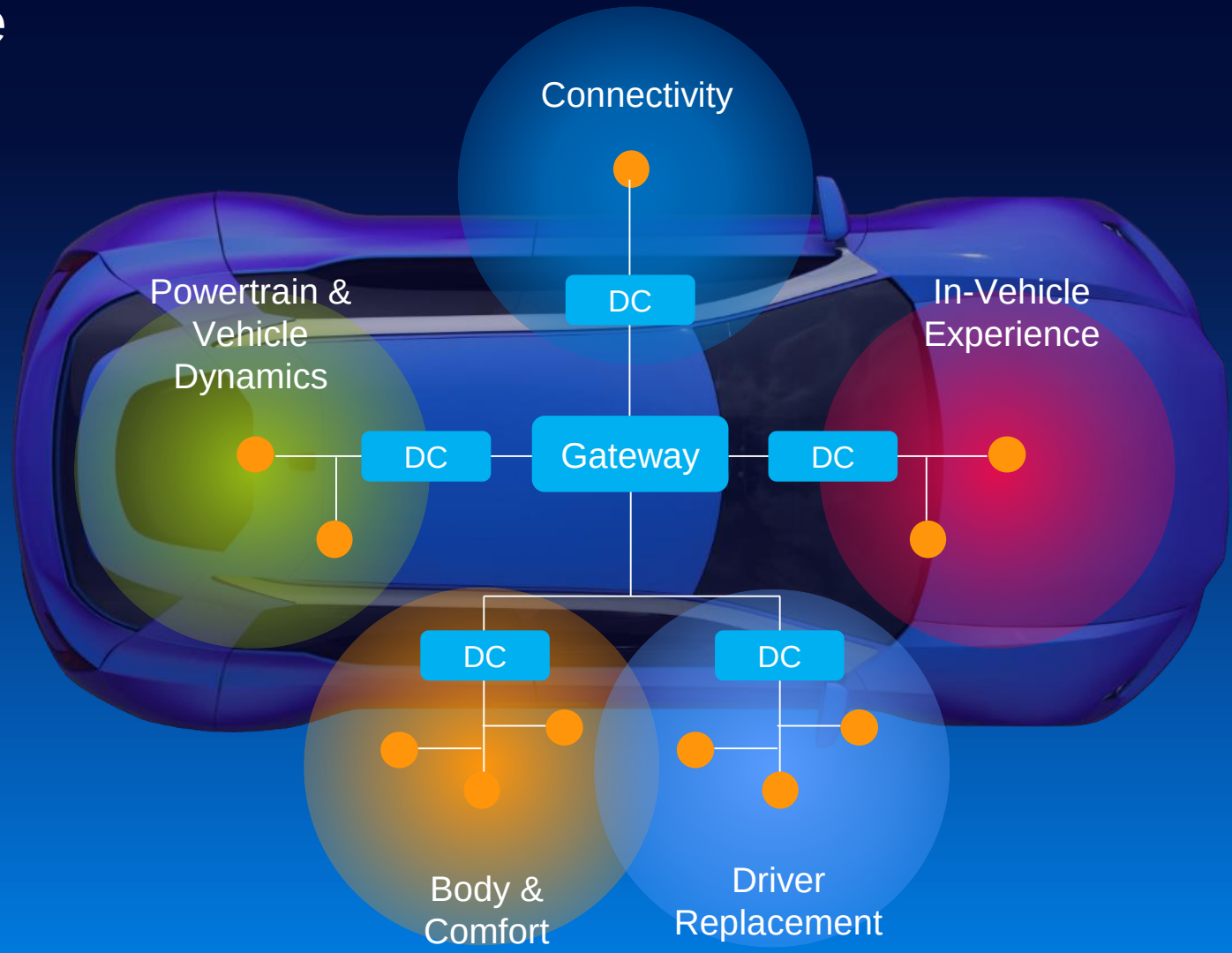
AUTONOMY

SAFE AND SECURE AUTONOMY

Automated Driving
Evolving Vehicle Architecture

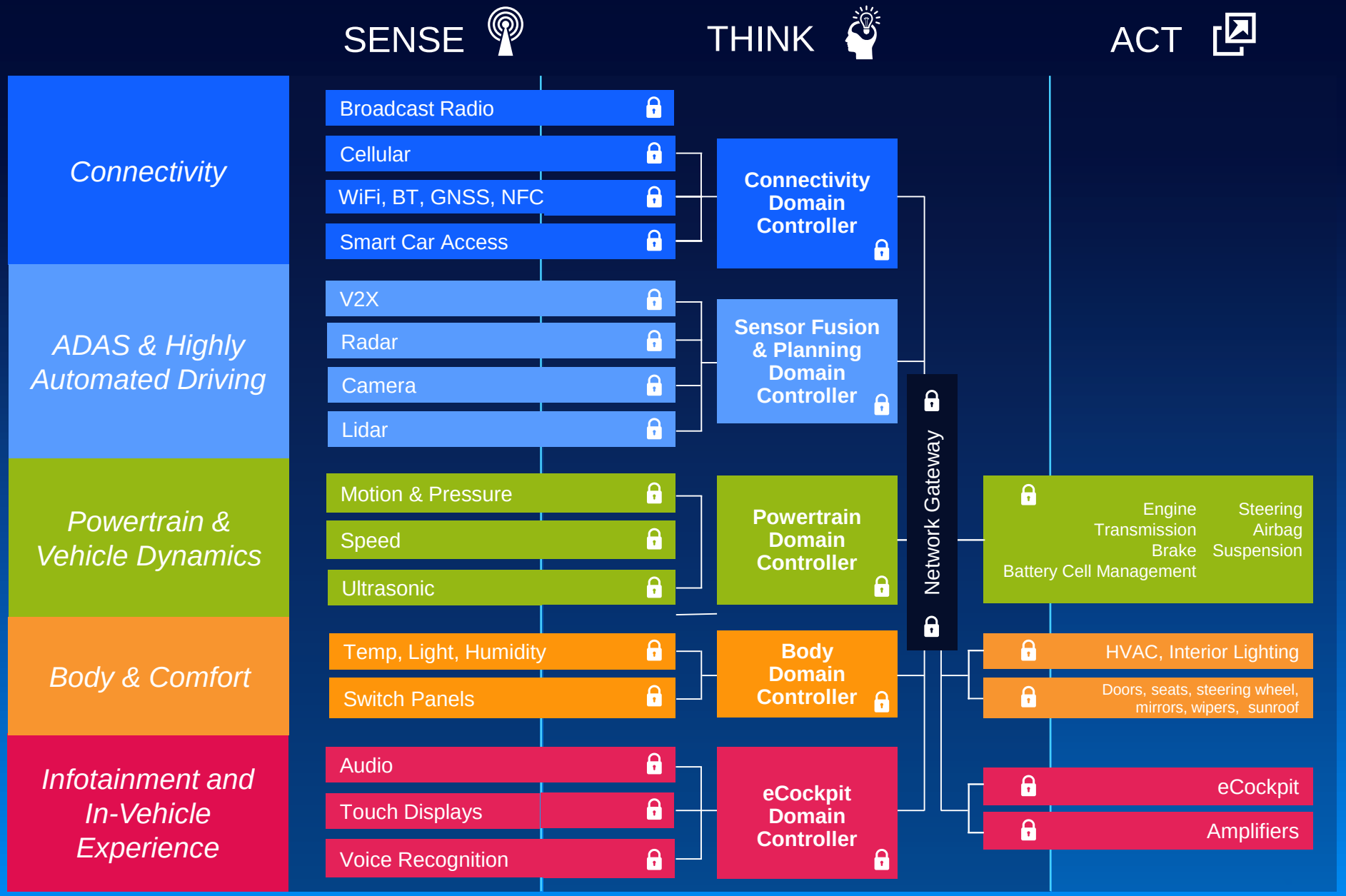
Secure Gateways & Networks

- Connectivity
- ADAS & Highly Automated Driving
- Powertrain & Vehicle Dynamics
- Body & Comfort
- Infotainment & In-Vehicle Experience



Automated Driving

Evolving Vehicle Architecture



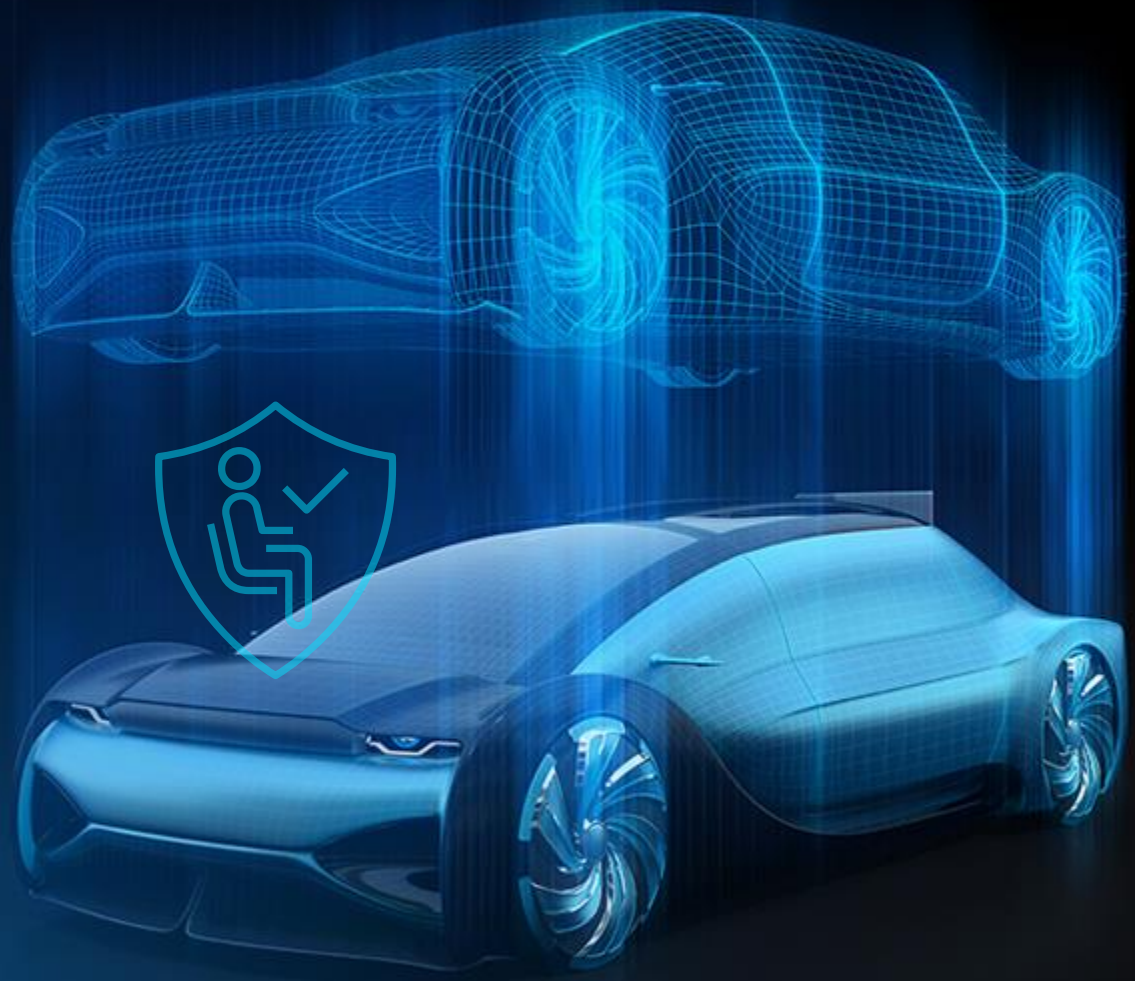
Requirements for a Safe System

Functional Safety
Zero accidents due to system failures

Cyber Security
Zero accidents due to system hacks

Vehicle Safety
Zero accidents due to human error

Device Reliability
Zero accidents due to device defects



Safety and Security Are Closely Linked

>25

Vehicle hacks
published since 2015

1.4M

Vehicles recalled
in the largest incident to date

Why hacking?

Valuable Data
attracts hackers

Car-generated data may become a 750B USD market by 2030

Why is it possible?

High System Complexity
implies high vulnerability

Up to 150 ECUs per car, up to 200M lines of software code

Why now?

Wireless Interfaces
enable scalable attacks

250M connected vehicles on the road in 2020

Why Safety Is Important

Legal – knowing who is responsible

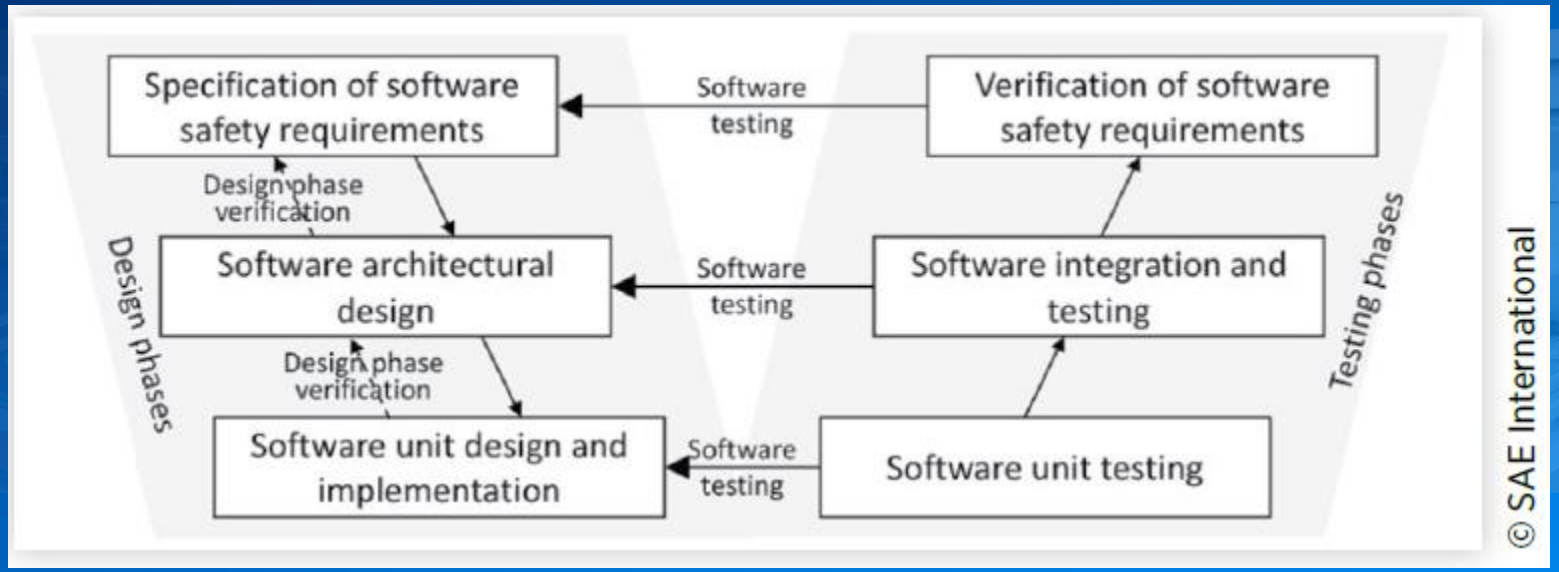
Trust – knowing the car will do what it's meant to do

Standardization – consolidating platforms and harmonizing systems

Automotive Functional Safety Standards

- Indicator of industry maturity
- Evolving to address the challenges of Autonomous, but not there yet

Safety: Functional Safety



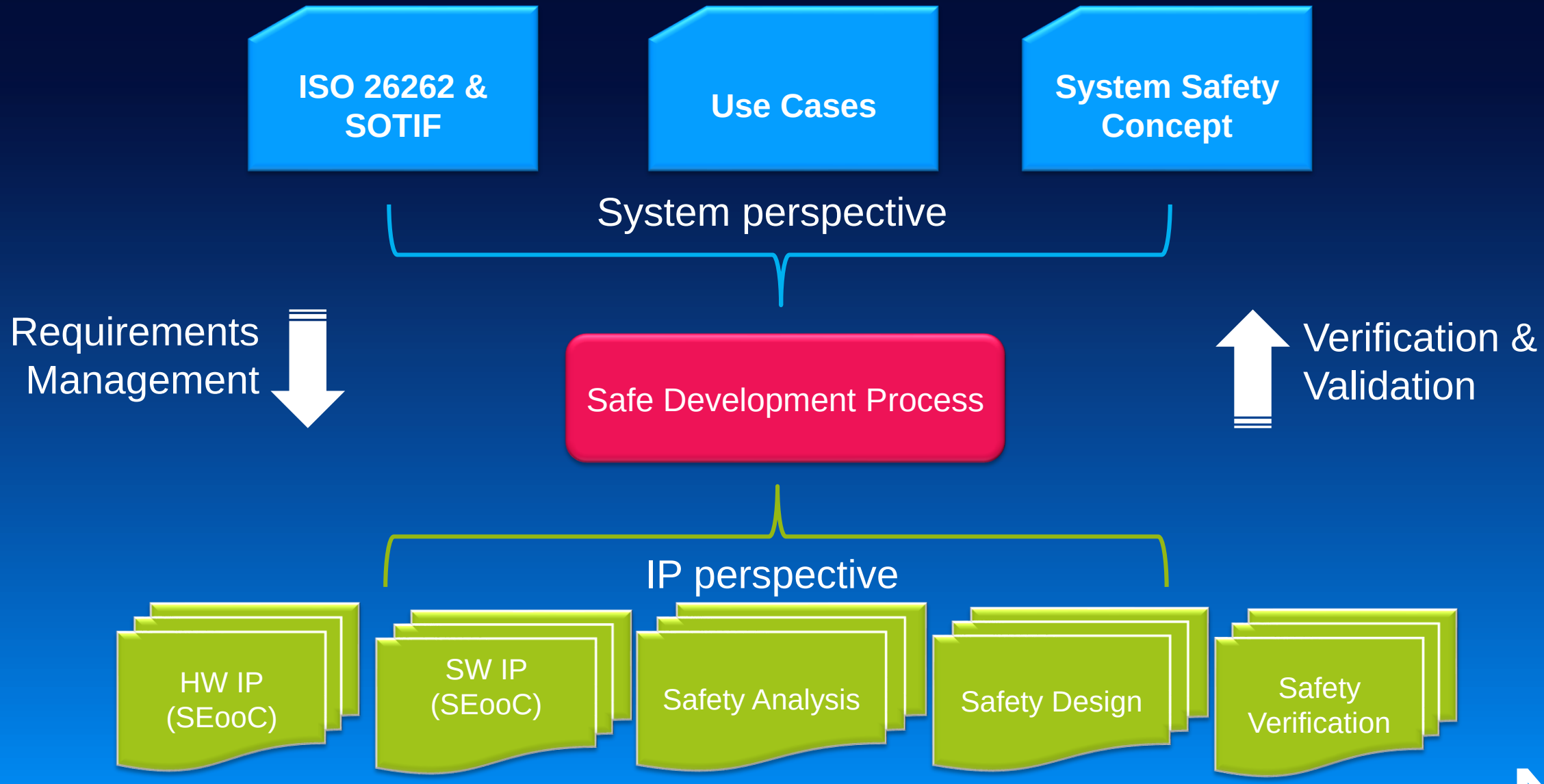
- "Traditional" Auto safety defined by standards: ISO 26262
- Automotive Safety Integrity Level (ASIL)
- ML introduces COMPLEXITY in proving FUNCTIONAL Safety

Severity	Exposure	Controllability
How much harm is done?	How often is it likely to happen?	Can the hazard be controlled

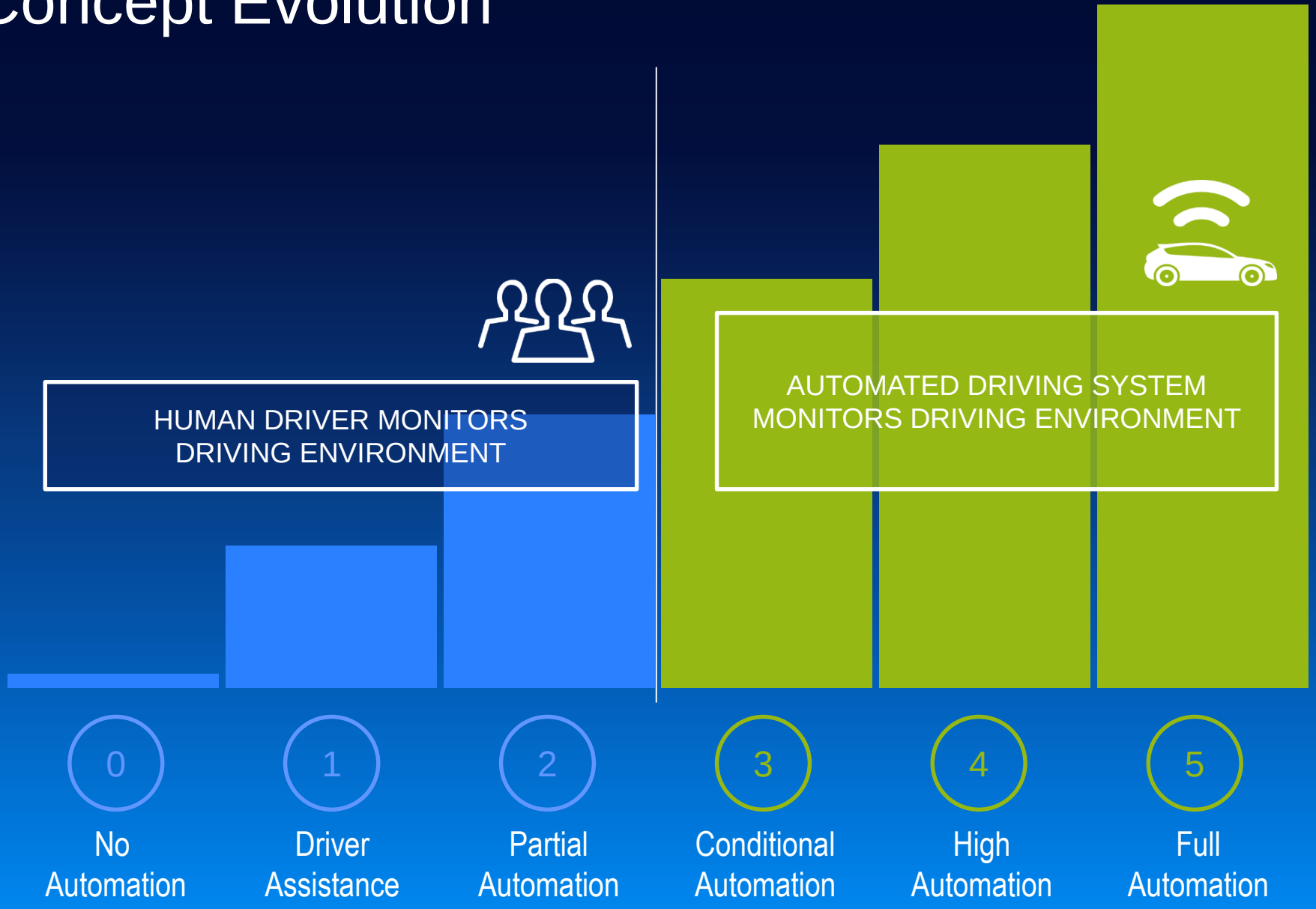
Safety: Behavioral Safety

- Learn to interact with non-automated vehicles and pedestrian – Driving Policy
- Predict the behavior of other agents
- Predict dangerous or safety critical situation
- Follow the rules all the time? Break them in certain circumstances? When?

Managing Complexity of System & IP Perspectives



Safety Concept Evolution



SAE standard J3016

Safety Concept Evolution - Industry Approach

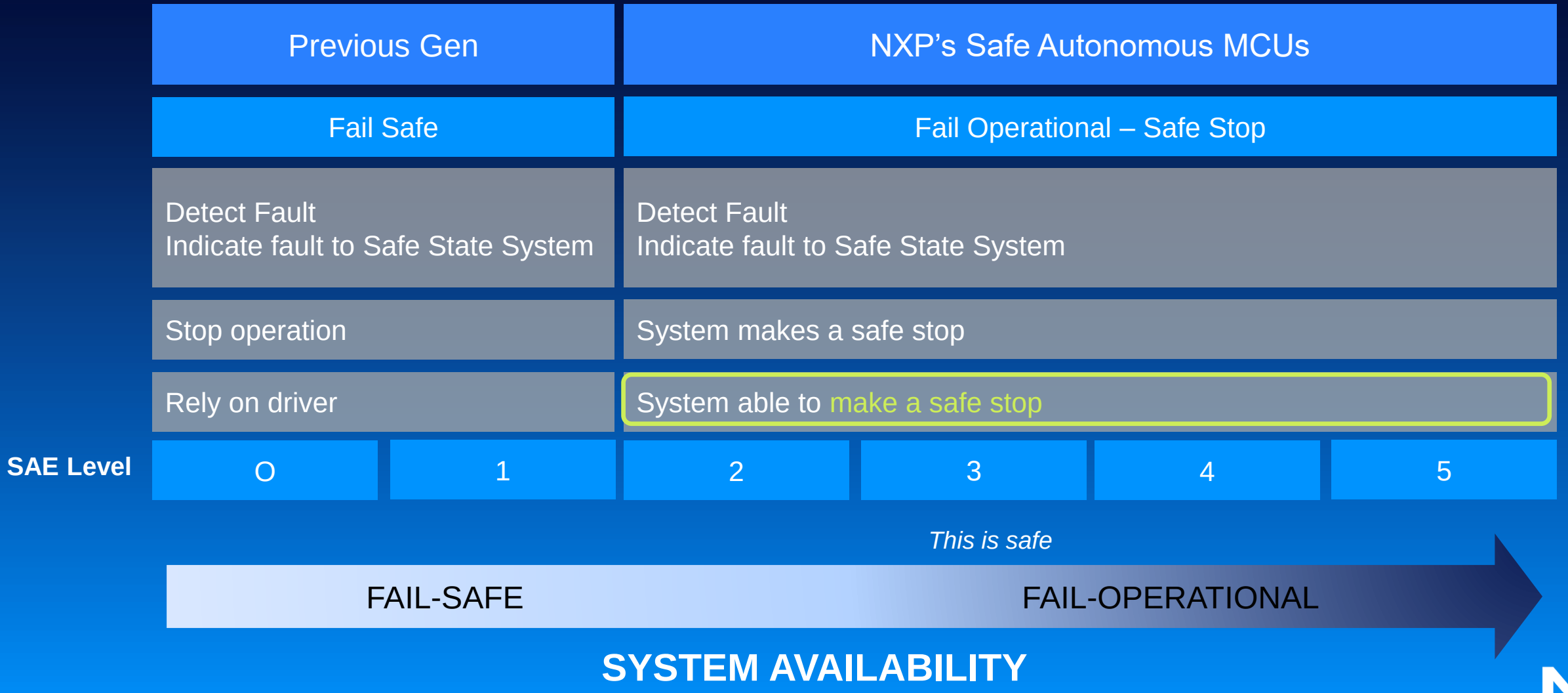
	Previous Gen		Current Gen		Next Gen	
	Fail Safe		Safety & Availability		Fail Operational	
	Detect Fault Indicate fault to Safe State System		Detect Fault Indicate fault to Safe State System and recover		Detect Fault Indicate fault to Safe State the System	
	Stop operation		Continue operation Continue degraded Stop operation		Sufficient vehicle level redundancy to continue full operation	
	Rely on driver		Partially rely on driver		No reliance on driver	
SAE Level	O	1	2	3	4	5

Driver needs to be in the loop for this to be safe

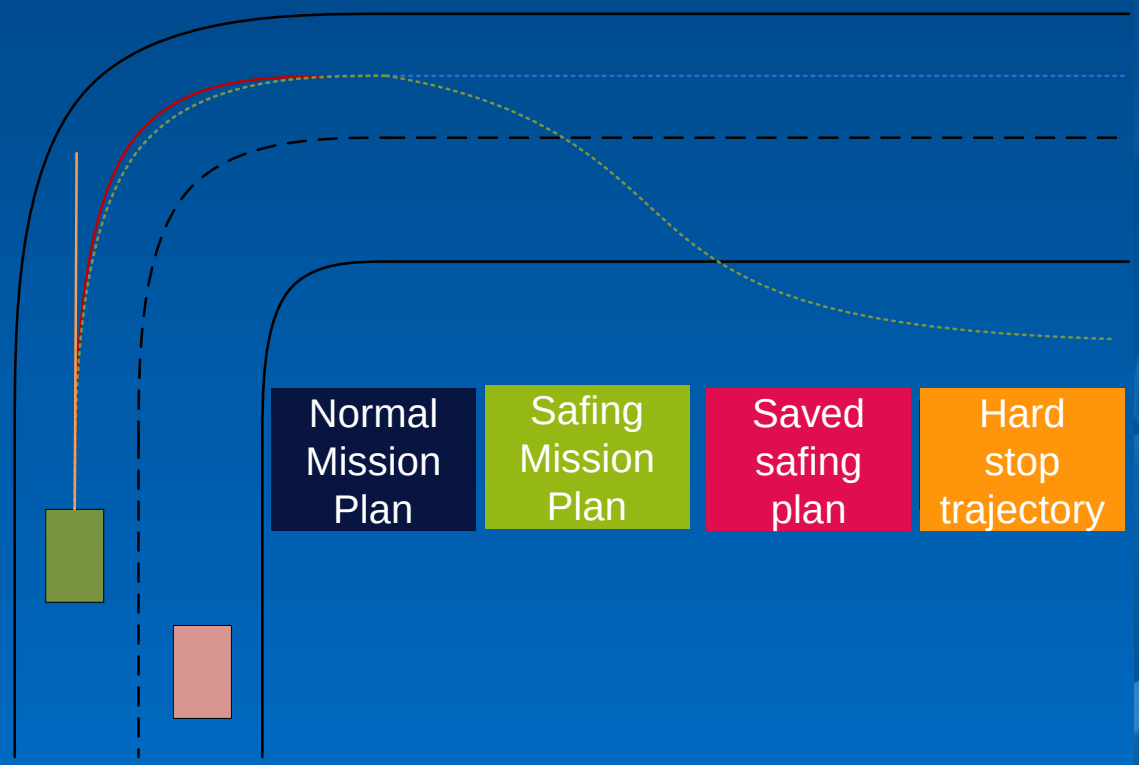
FAIL-SAFE DEGRADED MODE FAIL-OPERATIONAL

SYSTEM AVAILABILITY

Safety Concept Evolution – Safe Autonomous, NXP Approach



Basic Vehicle Plans



Normal Mission Plan

Driving mission towards a final destination/goal

Saving Mission Plan

Short-duration mission towards a safe stop

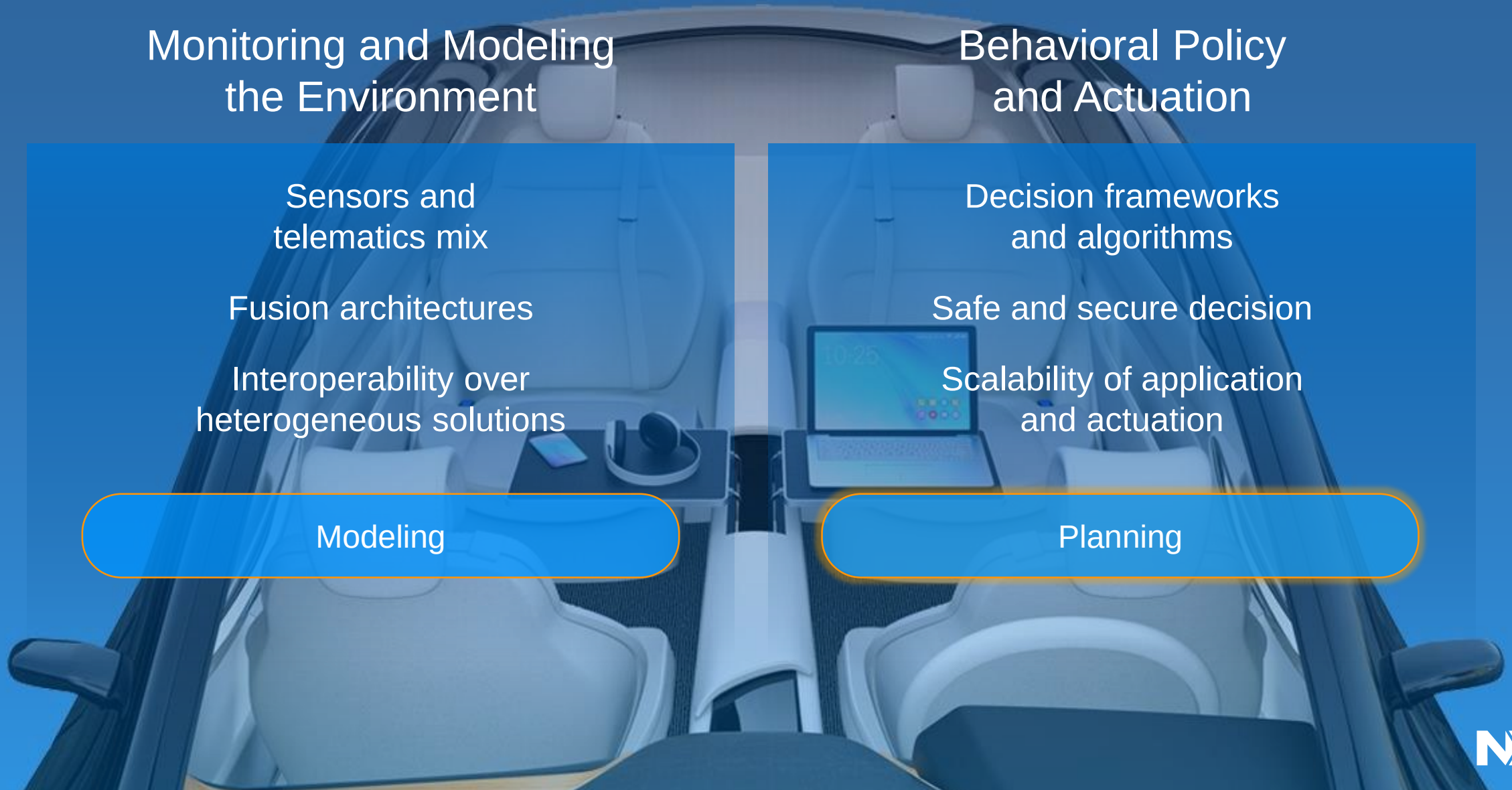
In-Lane Stop

Stopping plan within lane

Hard Stop Trajectory

Apply hard brake and maintain steering

Autonomous Driving at a High Level



Monitoring and Modeling the Environment

Sensors and telematics mix

Fusion architectures

Interoperability over heterogeneous solutions

Modeling

Behavioral Policy and Actuation

Decision frameworks and algorithms

Safe and secure decision

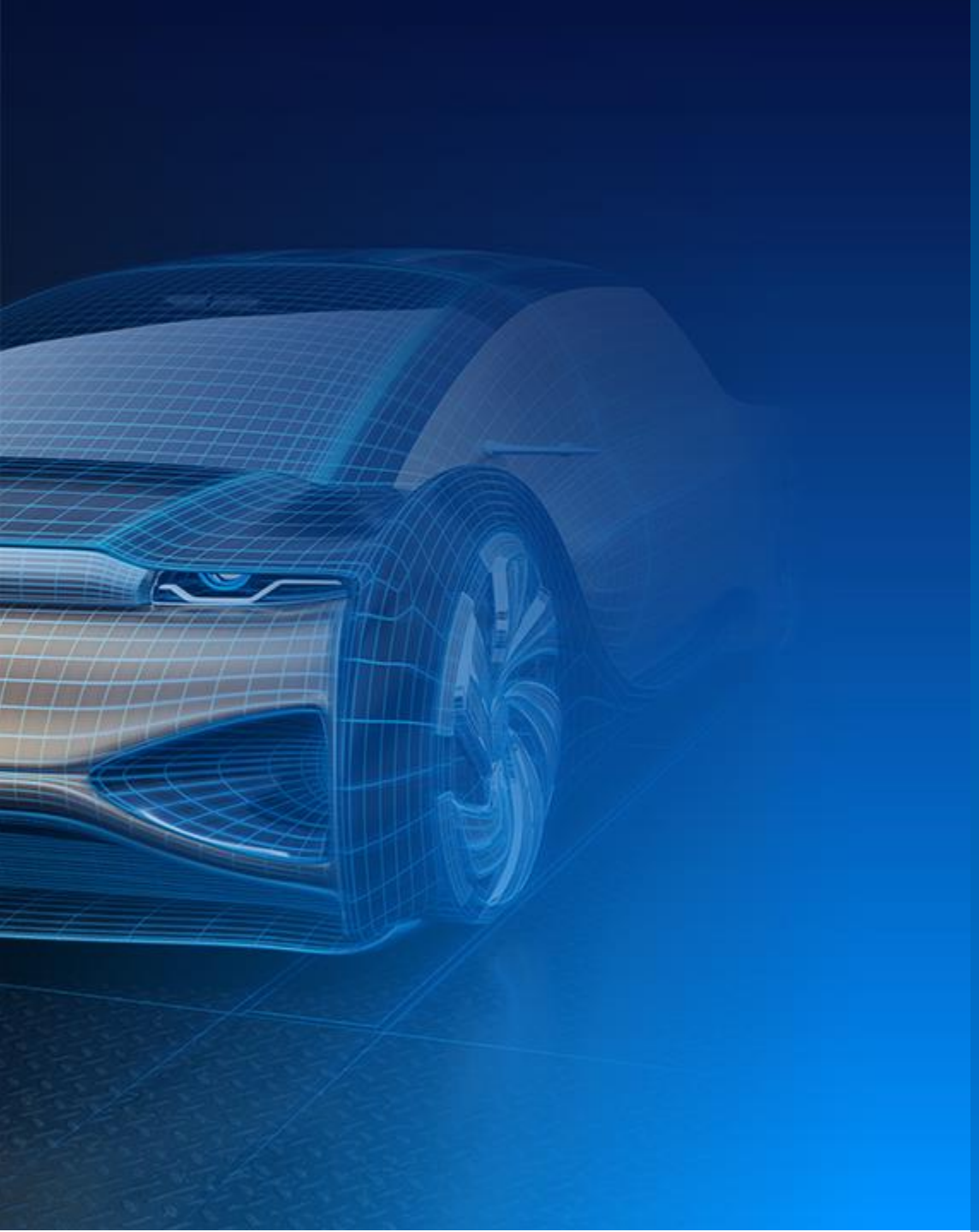
Scalability of application and actuation

Planning

Autonomous Driving Approaches

- Purely AI-based implementation
- Redundancy distributed
- Mission saving plans distributed
- Safety achieved by complex crosschecking

- AI-based functions
- Deterministic functions for saving
- B-channel for mission saving only
- Safety achieved ASIL-D deterministic checker



Autonomous Driving Challenges

Modeling

Feasibility of End-to-End solutions

- Large black-box approach not conducive to safety
- Unified compute architecture not scalable for evolving heterogeneous compute model

Use of Unsupervised Learning

- Can it simplify the learning process?
- Can it speed up AD adoption? Will it be safe?

Where does Sensor Fusion take place

- How does this impact connectivity and BW across the vehicle

Autonomous Driving Challenges

Planning

Is ML-based path planning safe?

- Can AI be guaranteed to detect free space and safe trajectory planning (yet?)

How much test time/distance is necessary to ensure automated driving is safe?

- 1 Million/Billion/Trillion km/miles driven, how much of real driven miles, how much simulated

Is a Fail Stop acceptable?

- Psychological trauma of a hard stop in the middle lane of a busy highway,

Autonomous Driving Progress

Automotive application specific training data sets
- Pedestrians and bicycles, not dog breeds

Sensors; higher capability, more robust, less cost
- Imaging radar, smart cameras, solid state LiDAR

HPC and larger storage
- Increased server compute capacity as well as decreased cost of storage enabling faster training and more training data generation.

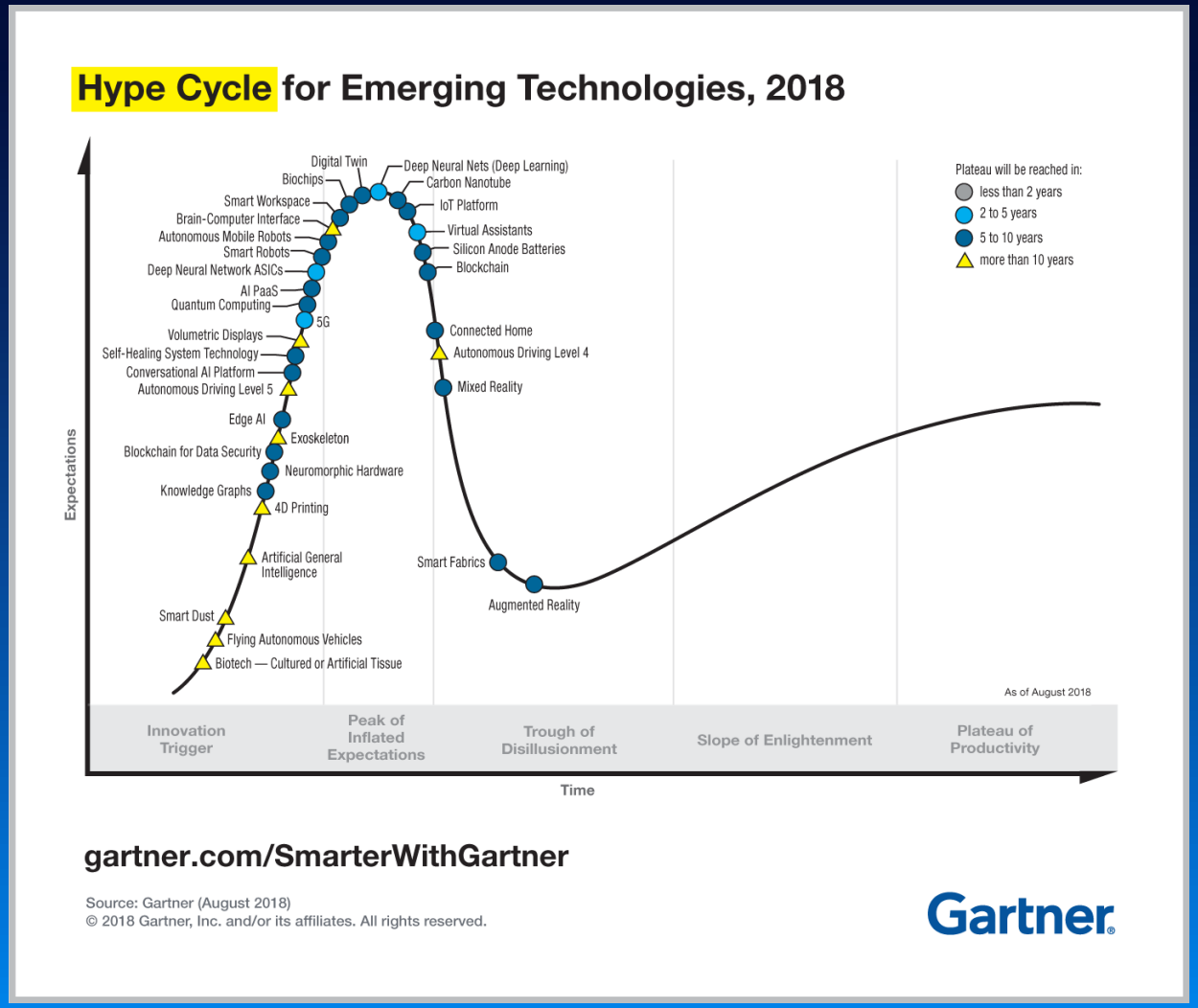
Sophisticated driving scenario simulators
- Driving simulation SW with physics based scene and environment rendering built for AD development

Higher edge compute performance
- NXP solutions enabling embedded AI at 100x higher power efficiency compared to current deployed test AVs.

When will Fully Autonomous Cars be Available

- Uber accident in May 2018 was turning point of peak
- Autonomous Driving Level 4 on down slope >10 years
- Autonomous driving level 5 pm initial up slope >10 years

…But its all about matching use case to technology capability



Source: Gartner, 2018

Different Innovation Strategies
EVOLUTION AND REVOLUTION

Revolutional

Evolutional

Safe, Secure
Mobility

ACCELERATE AND WIN
IN BOTH WORLDS

Semiconductors – Foundation for Safe & Secure Mobility

Better senses –
Complementary, accurate, full surround

Safety and Security by Design

Zero Congestion

Zero Accidents

Zero Emissions


NXP
SECURE CONNECTIONS
FOR A SMARTER WORLD