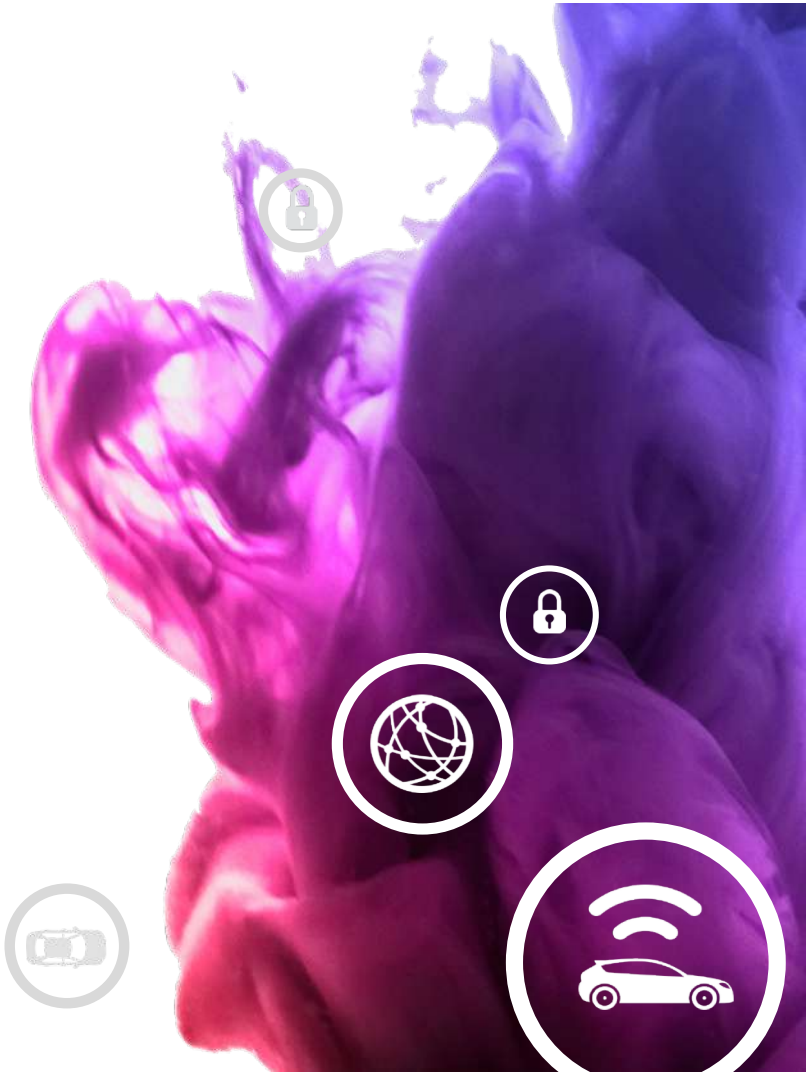
SAFETY AND SECURITY AT THE HEART OF AUTONOMOUS DRIVING

KAMAL KHOURI

NXP AUTOMOTIVE



SECURE CONNECTIONS FOR A SMARTER WORLD

PUBLIC

GLOBAL MEGA TRENDS

AN INCREDIBLE OPPORTUNITY

CONNECTIVITY

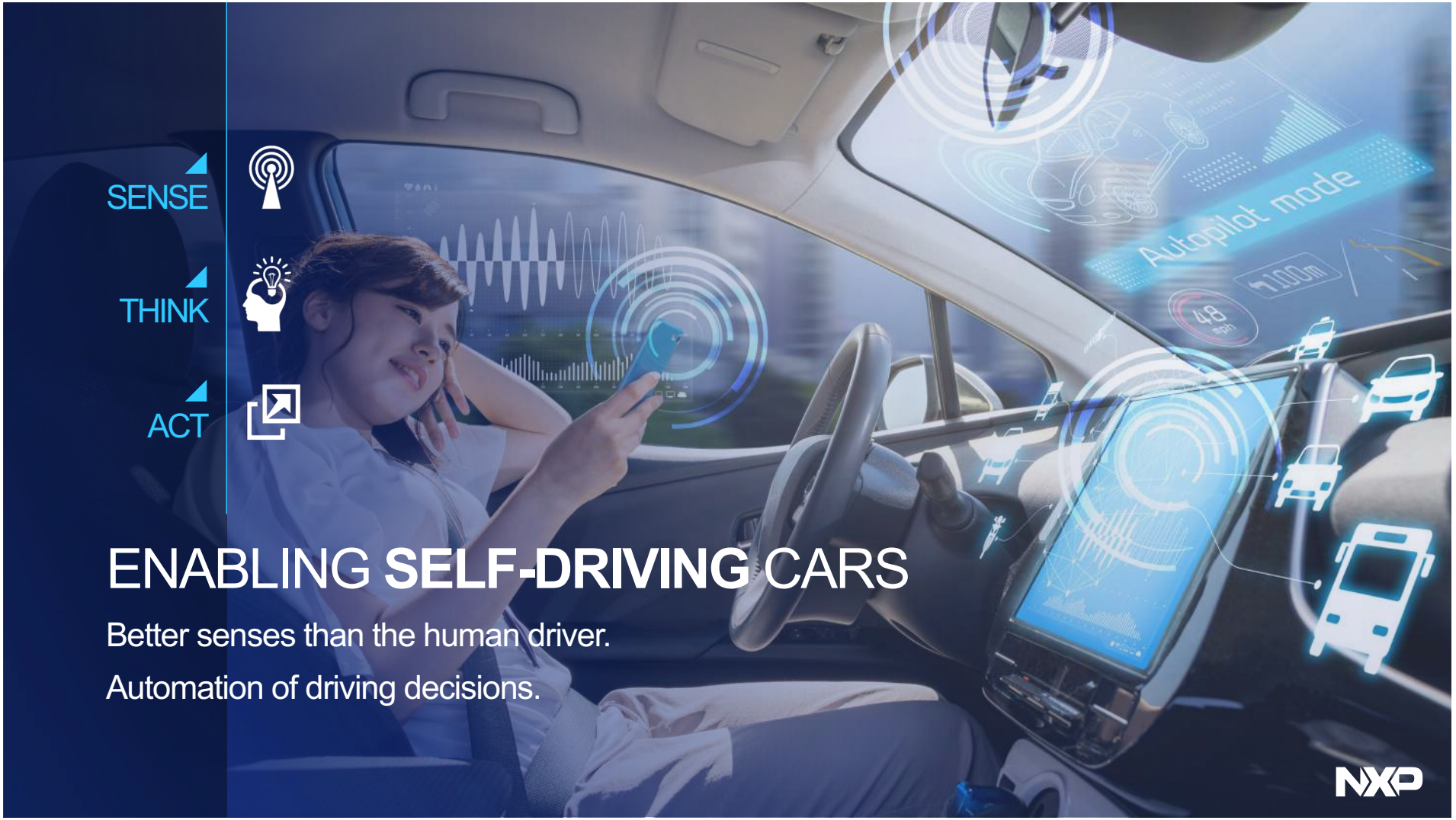
AUTONOMY

ELECTRIFICATION

SAFE AND SECURE MOBILITY

AND AN INCREDIBLE RESPONSIBILITY

1.3
MILLION
Road traffic deaths
occur every year
HIT BY A VEHICLE TRAVELING AT:
35
km/h
9 OUT OF 10
PEDESTRIANS SURVIVE*
HIT BY A VEHICLE TRAVELING AT:
50
km/h
5 OUT OF 10
PEDESTRIANS SURVIVE
HIT BY A VEHICLE TRAVELING AT:
70
km/h
ONLY 1 OUT OF 10
PEDESTRIANS SURVIVES
OUT OF ALL ACCIDENTS GLOBALLY,
90% are caused by
HUMAN ERROR
Source: Seattle's Vision Zero Plan/Documents/Departments/beSuperSafe/VisionZeroPlan, ASIRT.ORG
NXP



ENABLING **SELF-DRIVING** CARS

Better senses than the human driver.

Automation of driving decisions.

NXP

DOMAIN ARCHITECTURE CONSIDERATIONS

SOFTWARE

Dynamic, Partitionable, and Reusable Software Environment

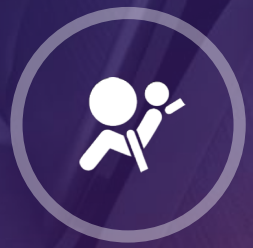
Multi OS, Multi Supplier/Partner, Hypervisor and Virtual Machine Enabled, Full Middleware Support

HARDWARE

High Performance Without Complexity, Scalable/Reusable, Cost Competitive, Power Conscious

SECURITY

Multi-layer, Updatable, Symmetric and Asymmetric Crypto Support, Side Channel Resistance



SAFETY

High Availability and Fault Tolerance (Fail Operational)

Provide Requisite Processes, Support, Silicon, Systems, and Software

SAFETY AND
SECURITY
AT THE HEART OF
AUTONOMOUS
DRIVING
NXP

System Safety

Absence of **unreasonable risk** due to **hazards** caused by **malfunctioning** behavior of electrical or electronic **systems**

Why Safety Is Important For the Automotive Market

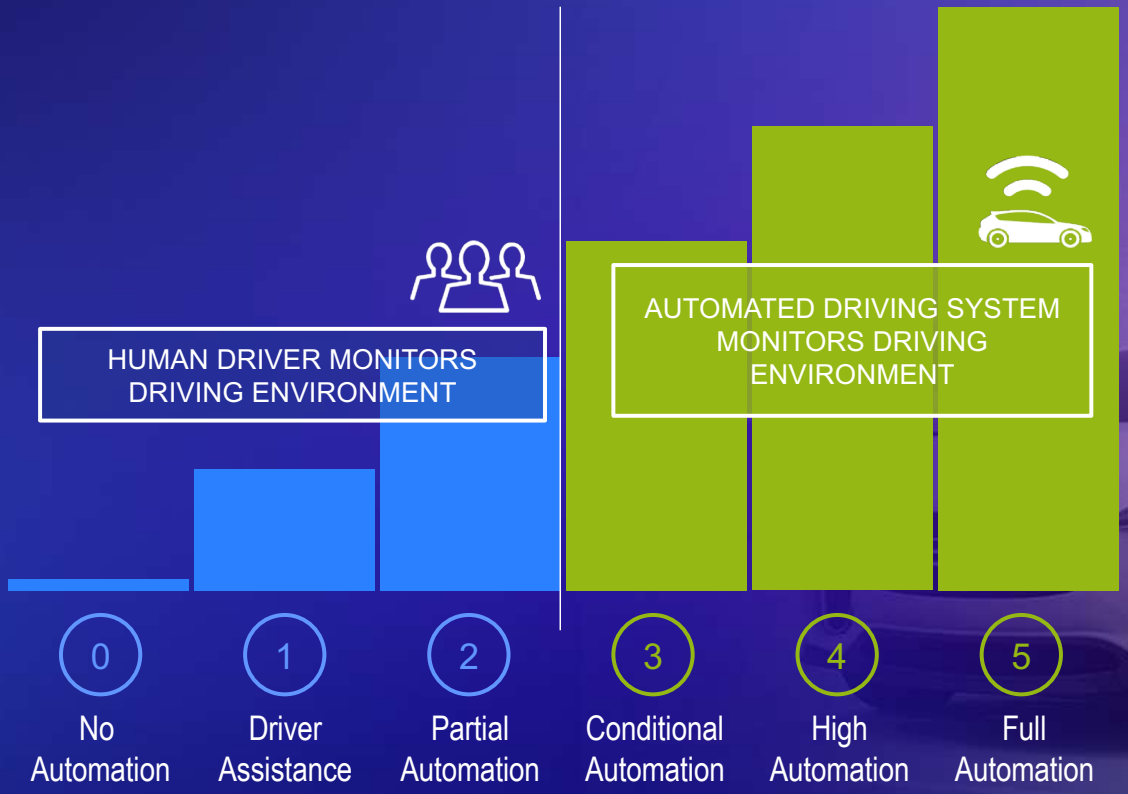
Legal – question of responsibility

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

Standardization – platform consolidation and system harmonization

Trends – autonomous driving, electric vehicles

WHAT IS DRIVING SAFETY TODAY?



SAE standard J3016

RISING COMPUTING AND SAFETY REQUIREMENTS

Probabilistic
- Analyze Scenario
- Make Contextual Decision

Deterministic
- Initiate Safe Measure
- Fail Safe / Operational

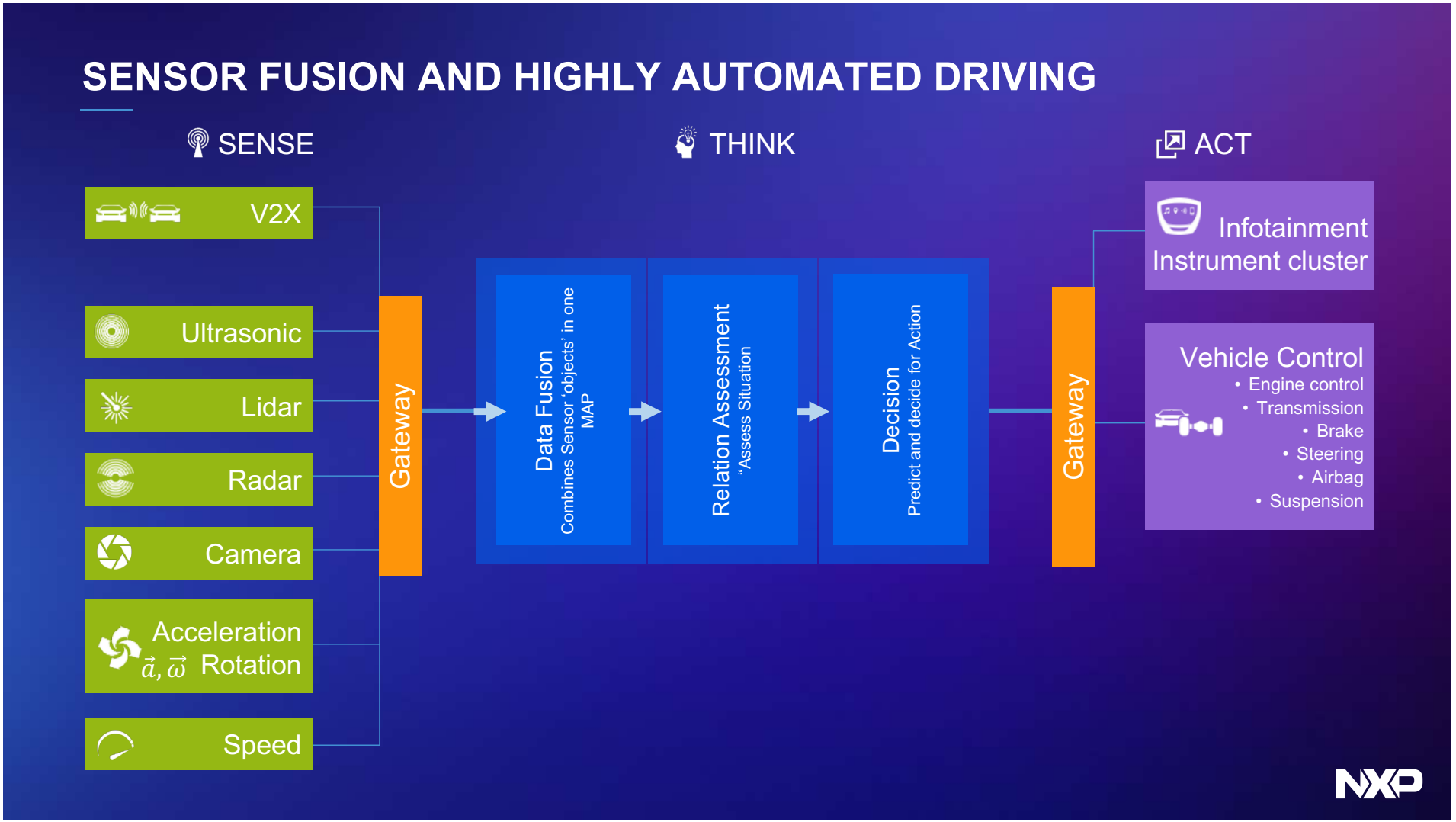
Automated Drive | Co-pilot | Collision Avoidance | Self Parking | Lane Keeping | Collision Warning | Sign View

Super Computing

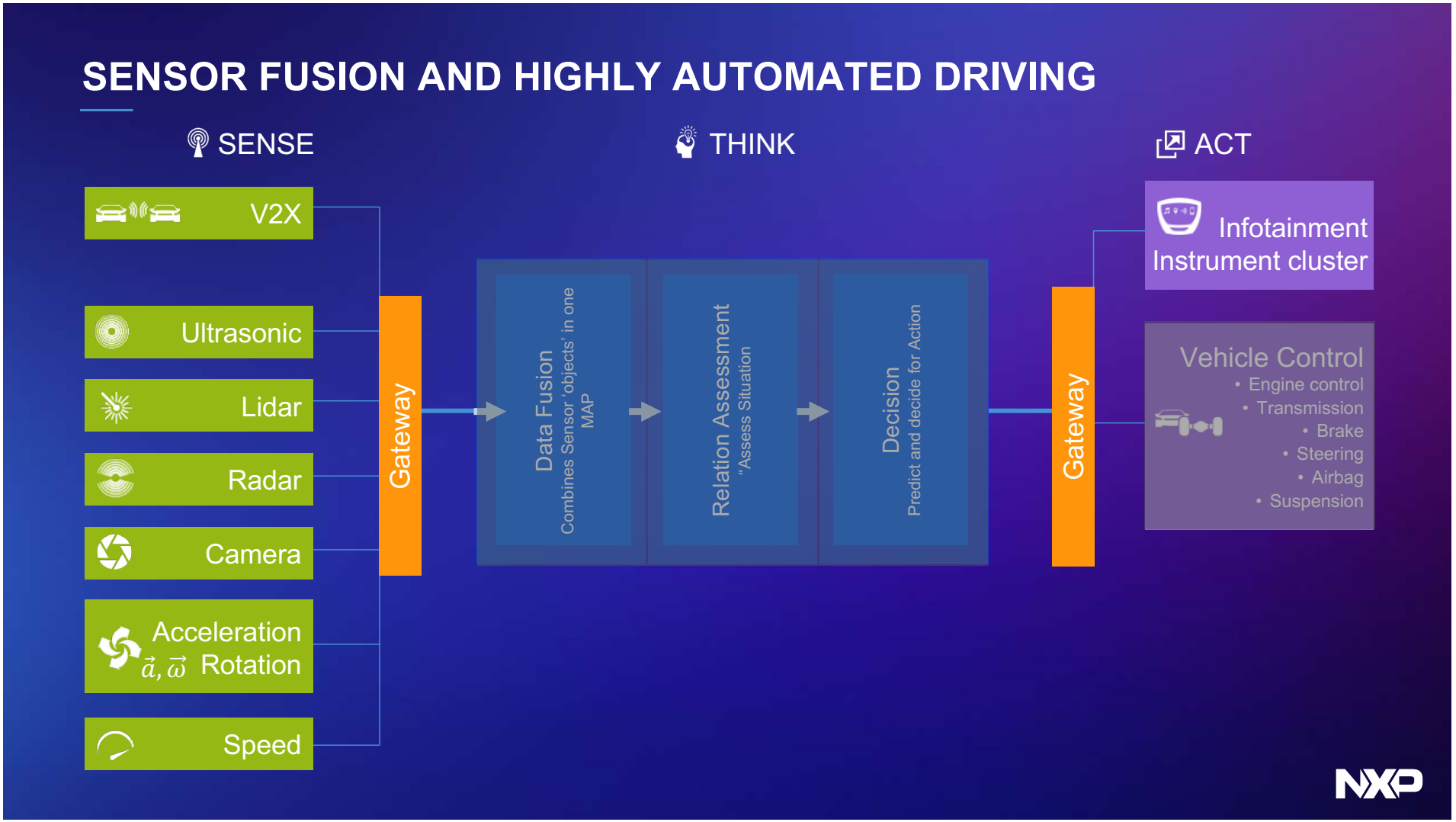
Safe Computing

NXP

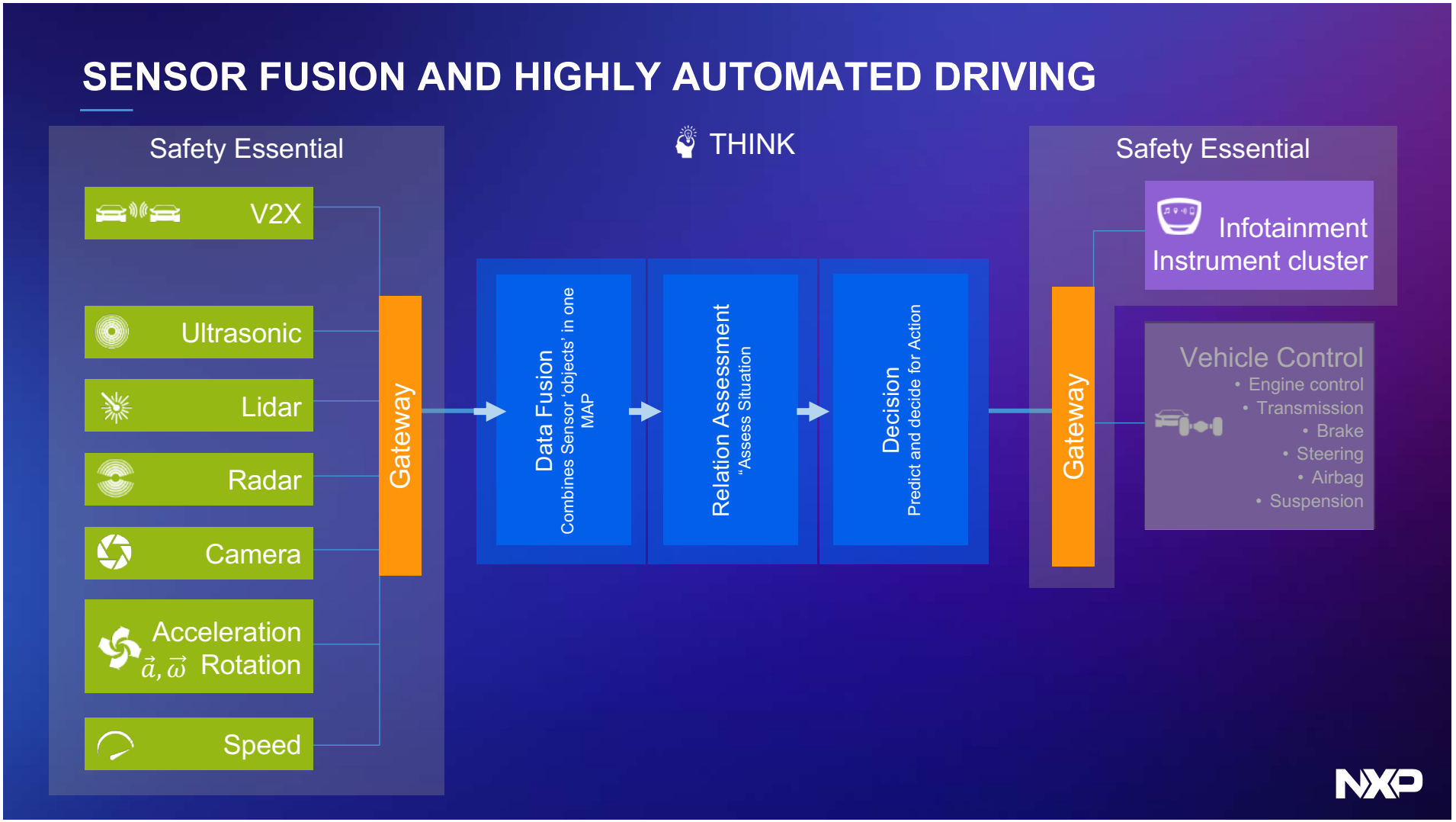
SENSOR FUSION AND HIGHLY AUTOMATED DRIVING



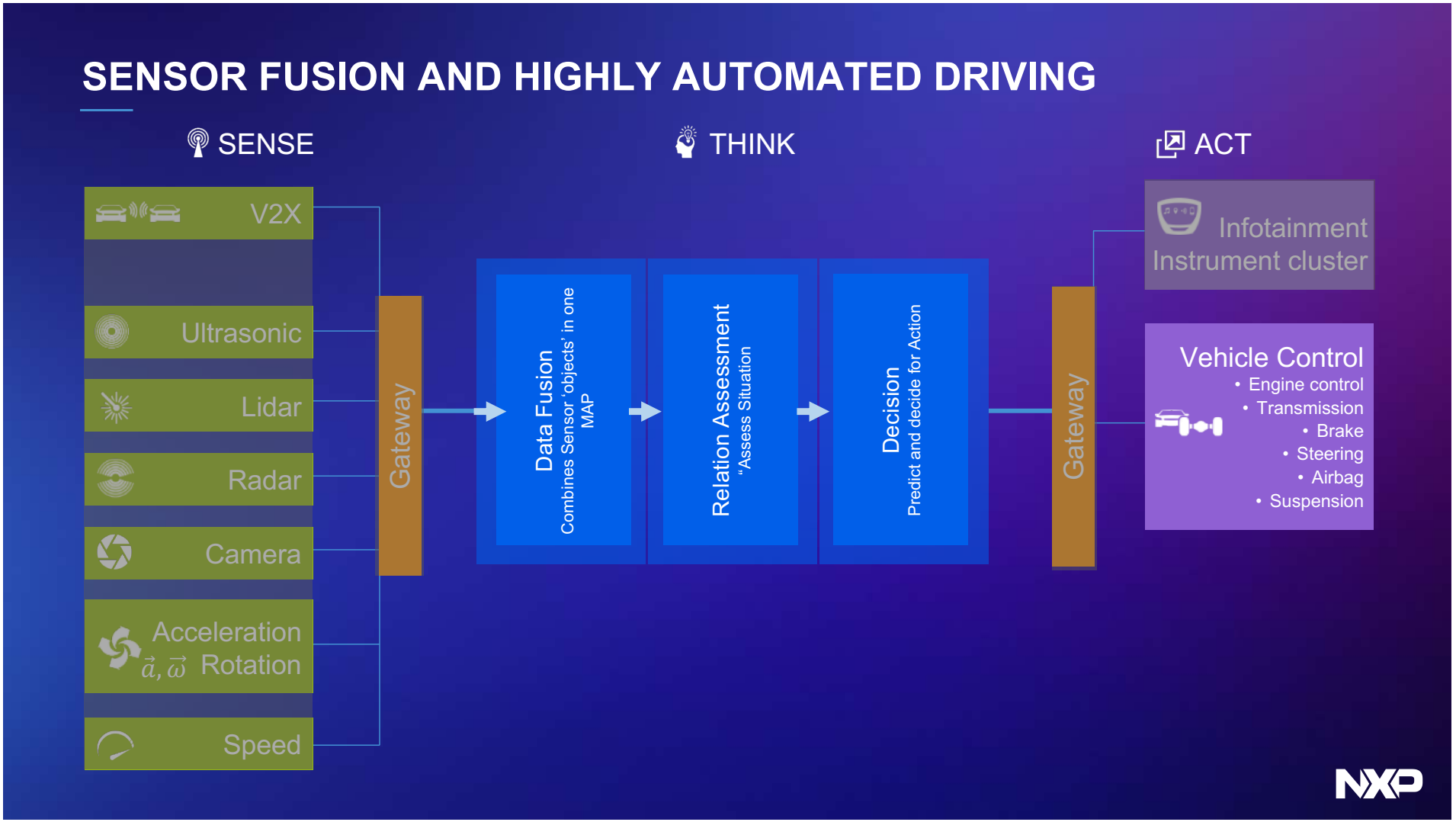
SENSOR FUSION AND HIGHLY AUTOMATED DRIVING



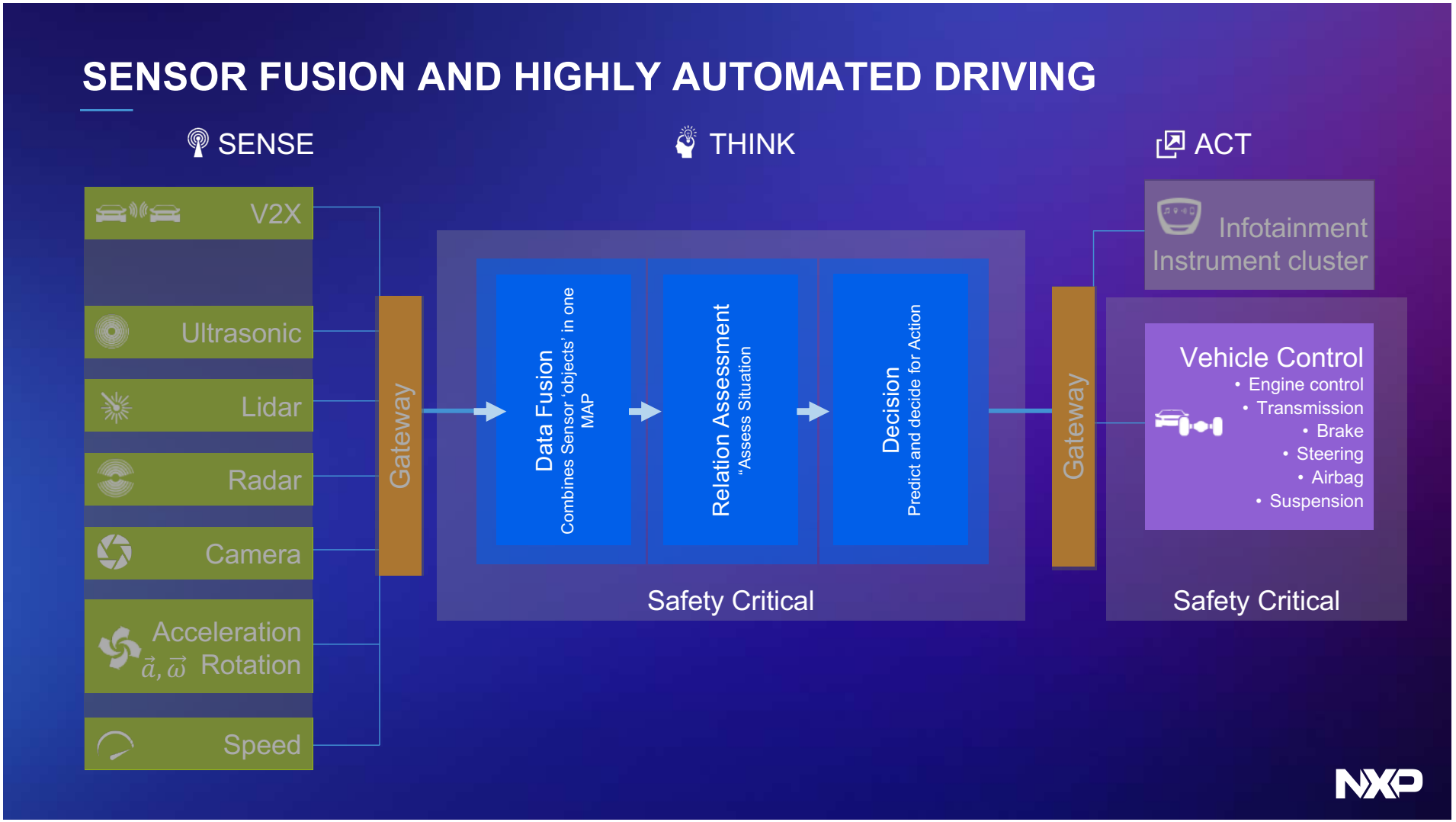
SENSOR FUSION AND HIGHLY AUTOMATED DRIVING



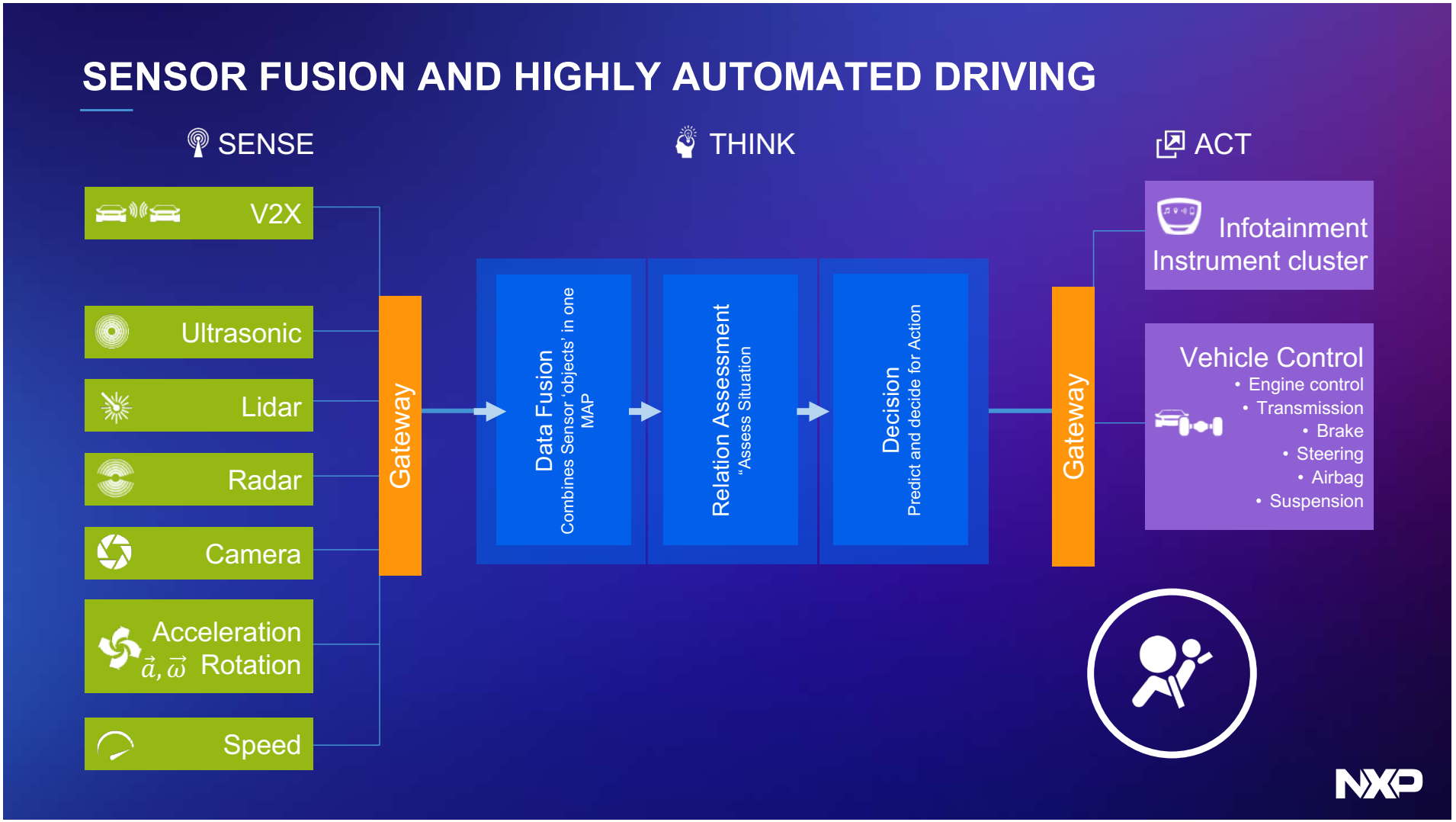
SENSOR FUSION AND HIGHLY AUTOMATED DRIVING



SENSOR FUSION AND HIGHLY AUTOMATED DRIVING



SENSOR FUSION AND HIGHLY AUTOMATED DRIVING

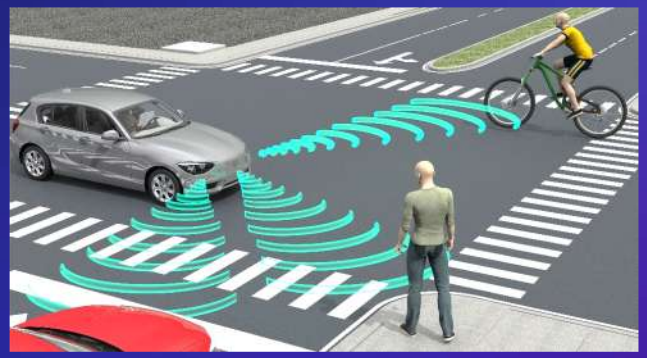


SAFETY AND MACHINE LEARNING (ML): FUNCTIONAL SAFETY

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

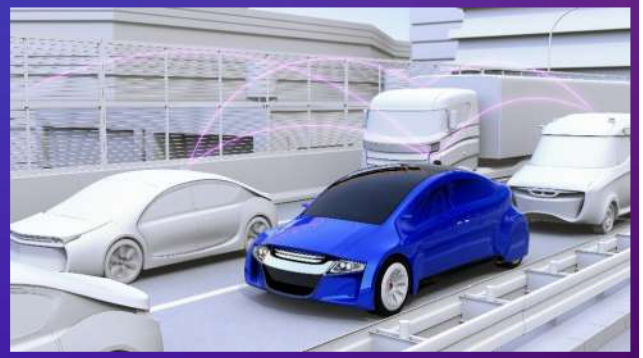
NXP

SAFETY AND MACHINE LEARNING (ML): BEHAVIORAL SAFETY

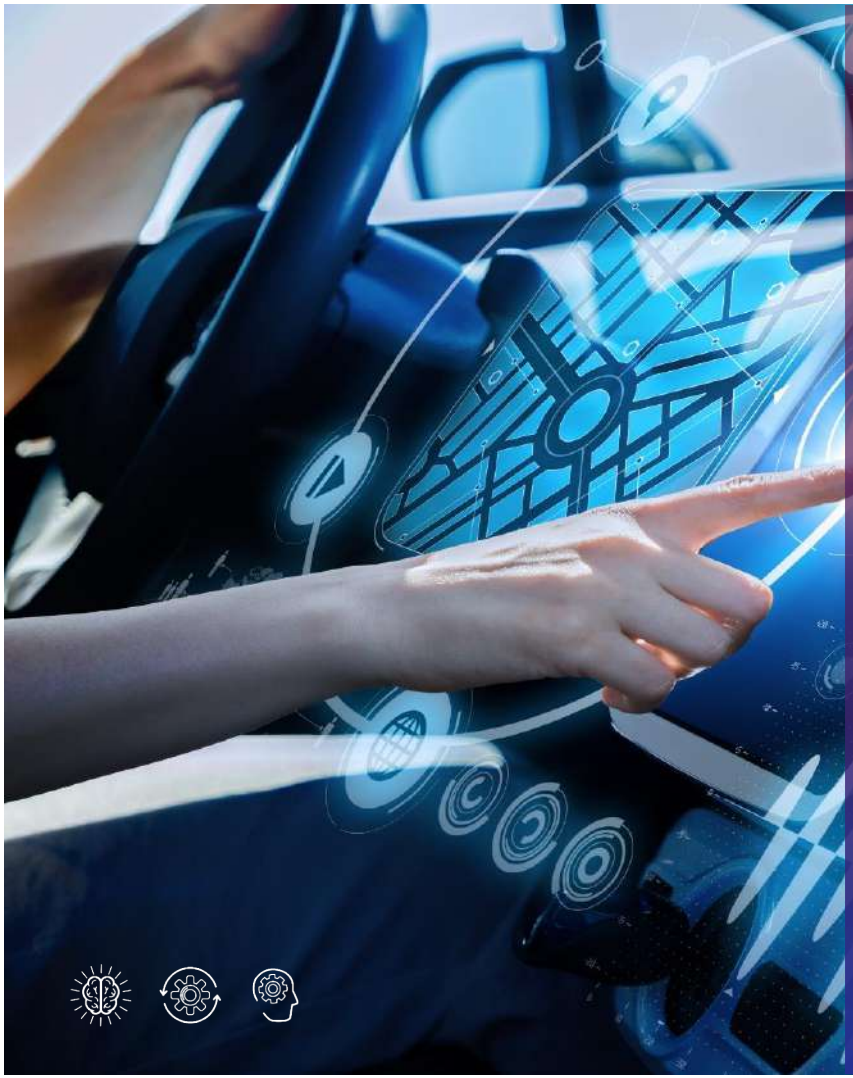


- Learn to interact with non-automated vehicles and pedestrian – Driving Policy
- Predict the behavior of other Agents
- Predict dangerous or safety critical situation
- Follow the rules all the time? Break them in certain circumstance? When?

SAFETY AND MACHINE LEARNING (ML): ENVIRONMENTAL SAFETY



- Understand different driving environments: Highway, Rural, City
- React to levels of environmental threats: Rain vs. Flooding
- Passenger fatigue and emotional state



A few open hot debates

Sense - Think

Are end-to-end solutions really acceptable?

Is Deep learning is the only path?

Edge or Cloud?

What is the role of unsupervised learning?

A few open hot debates

Think - Act

Is reinforcement learning sufficient?

How much data is necessary for automated driving?

When and how can we certify safe decisions?

DID YOU KNOW?

>25

Vehicle hacks
published since 2015

1.4M

Vehicle recalled
in the largest incident to date

Why hacking?

Valuable Data
attracts hackers

Car-generated data may become a USD 750B 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

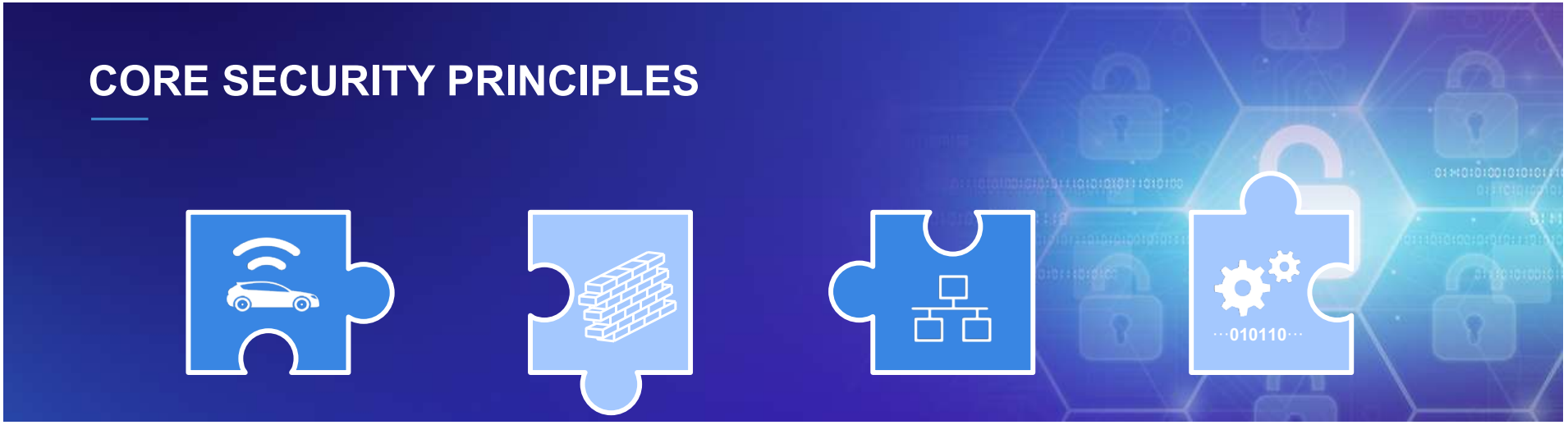
250M connected vehicles on the road in 2020

SECURITY IS A MUST-HAVE FOR CONNECTED & AUTONOMOUS VEHICLES

SECURITY FOUNDATION FOR THE CONNECTED CAR

- Protect privacy
- Prevent unauthorized access
- Increase safety

CORE SECURITY PRINCIPLES



Secure
External Interfaces

Secure
Domain Isolation

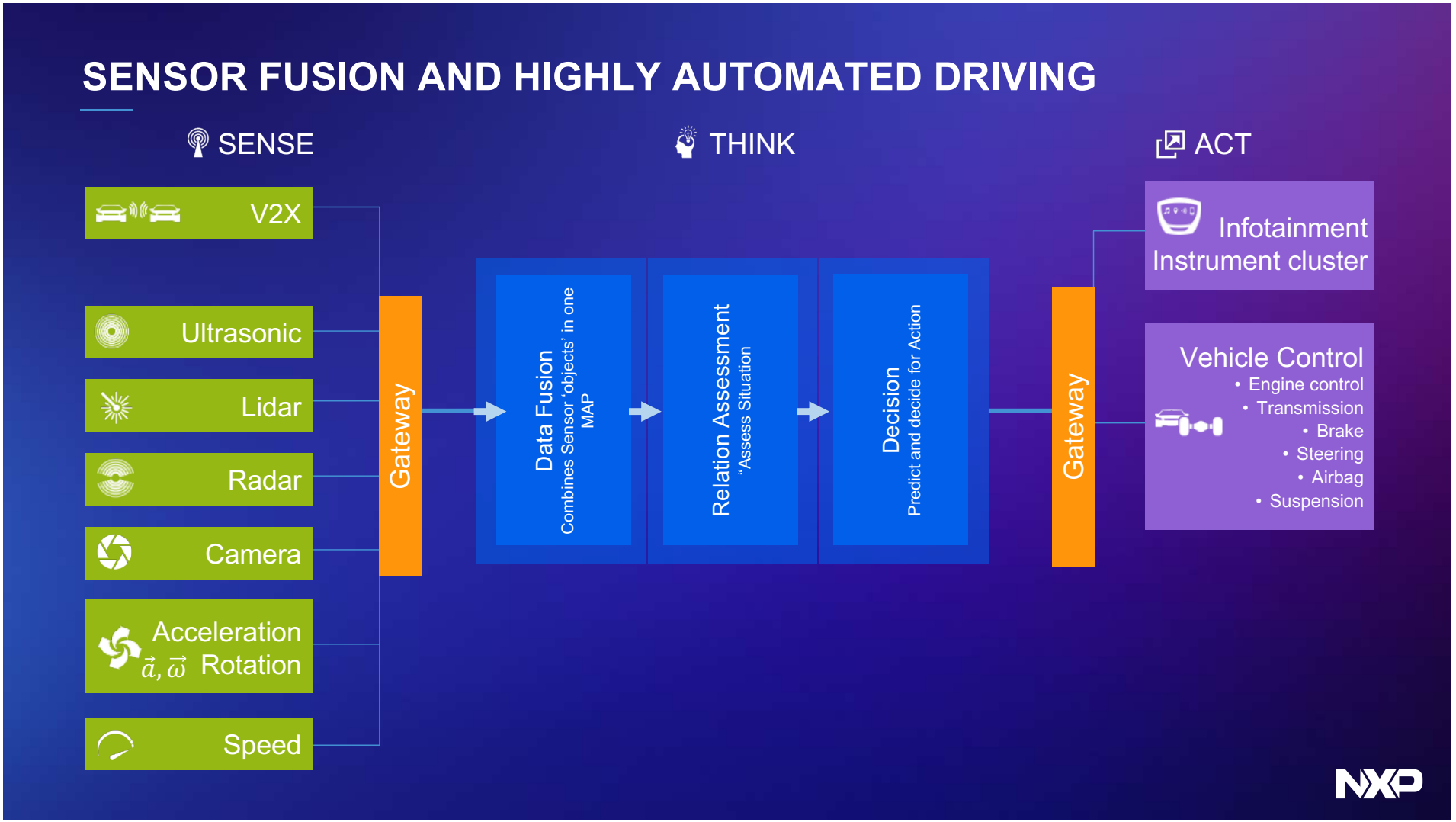
Secure
Internal Communication

Secure
Software Execution

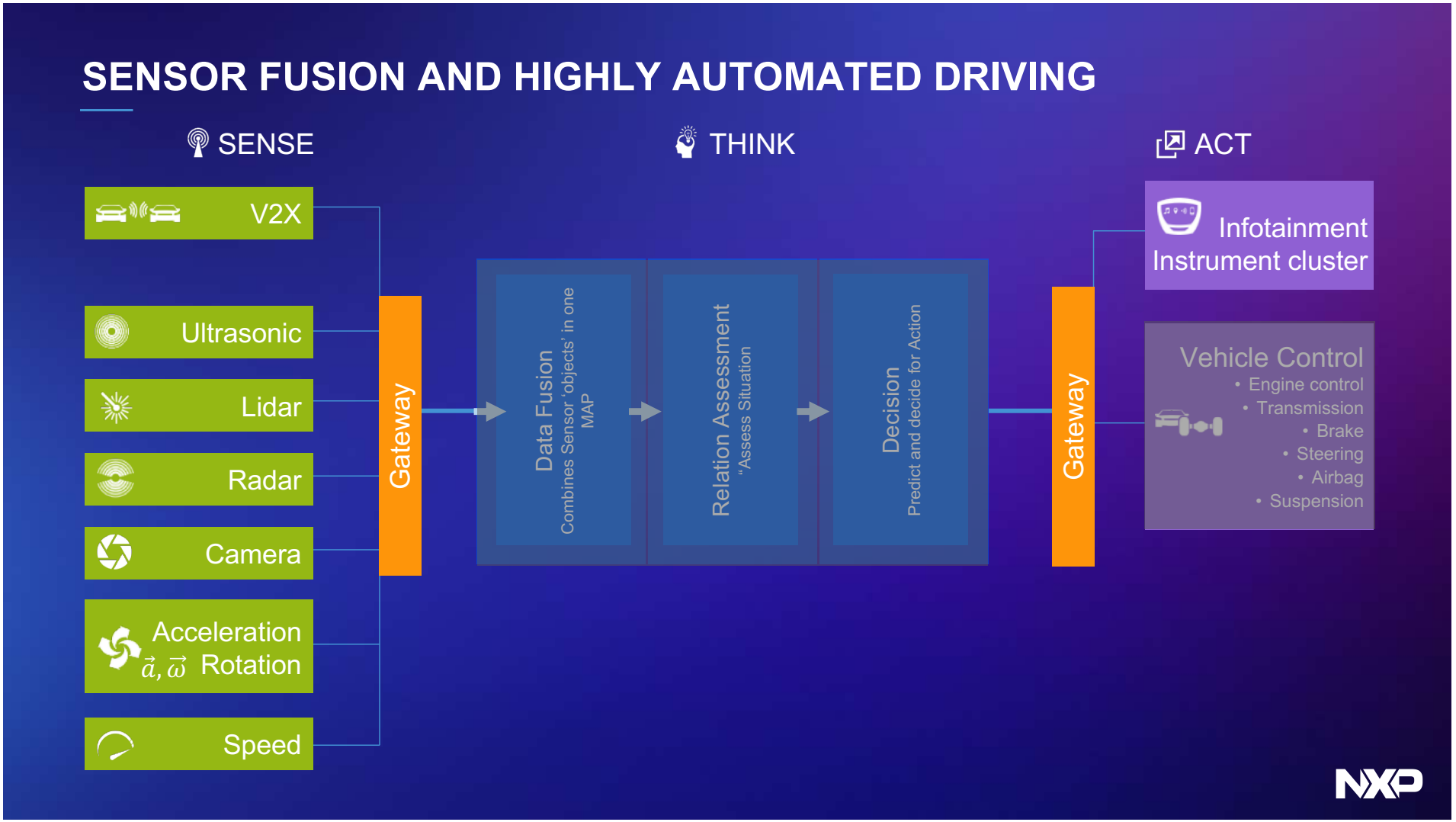
They need to be in place in ***any*** electrical and electronic network

- Regardless of the actual architecture and implementation

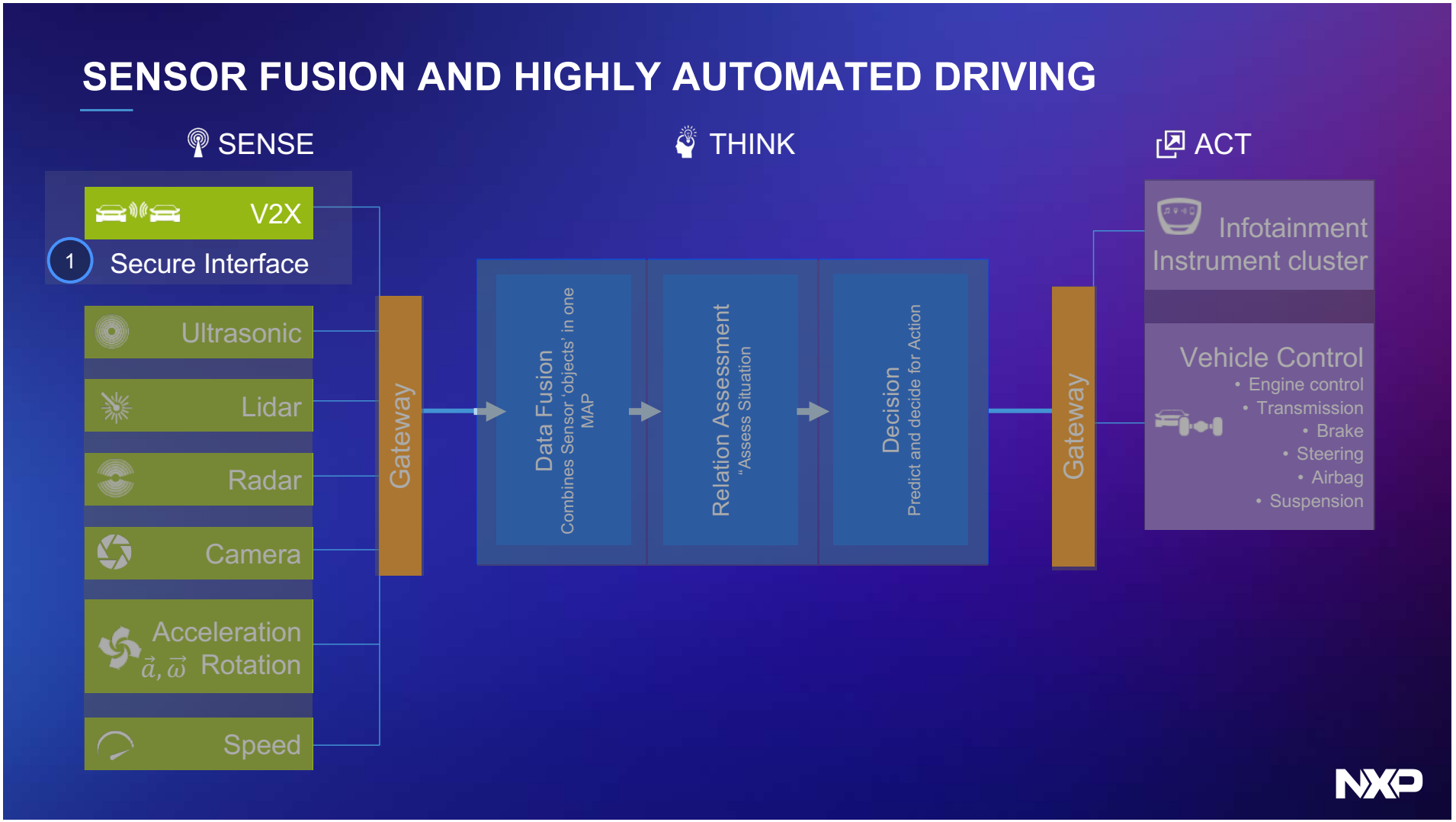
SENSOR FUSION AND HIGHLY AUTOMATED DRIVING



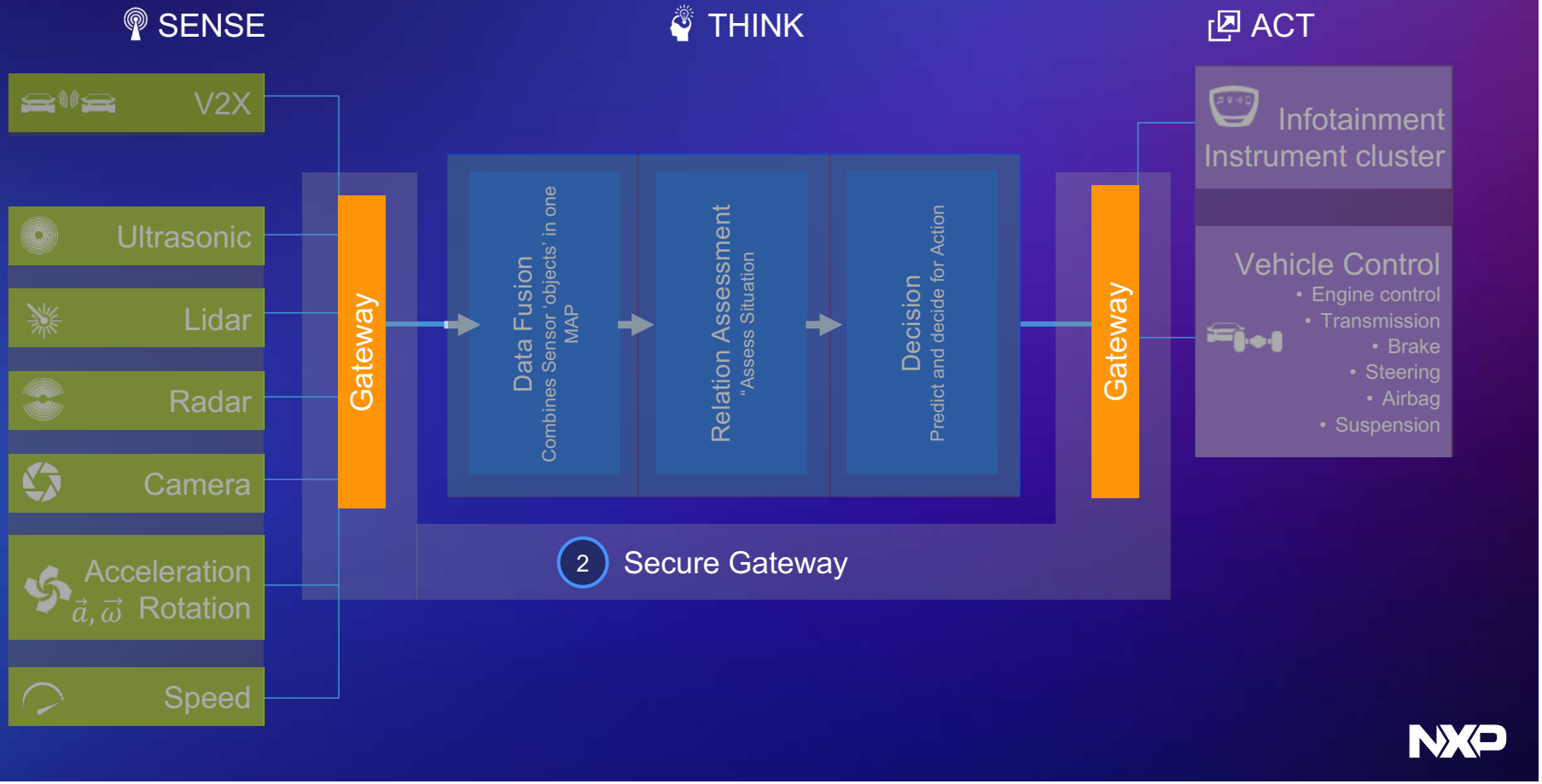
SENSOR FUSION AND HIGHLY AUTOMATED DRIVING



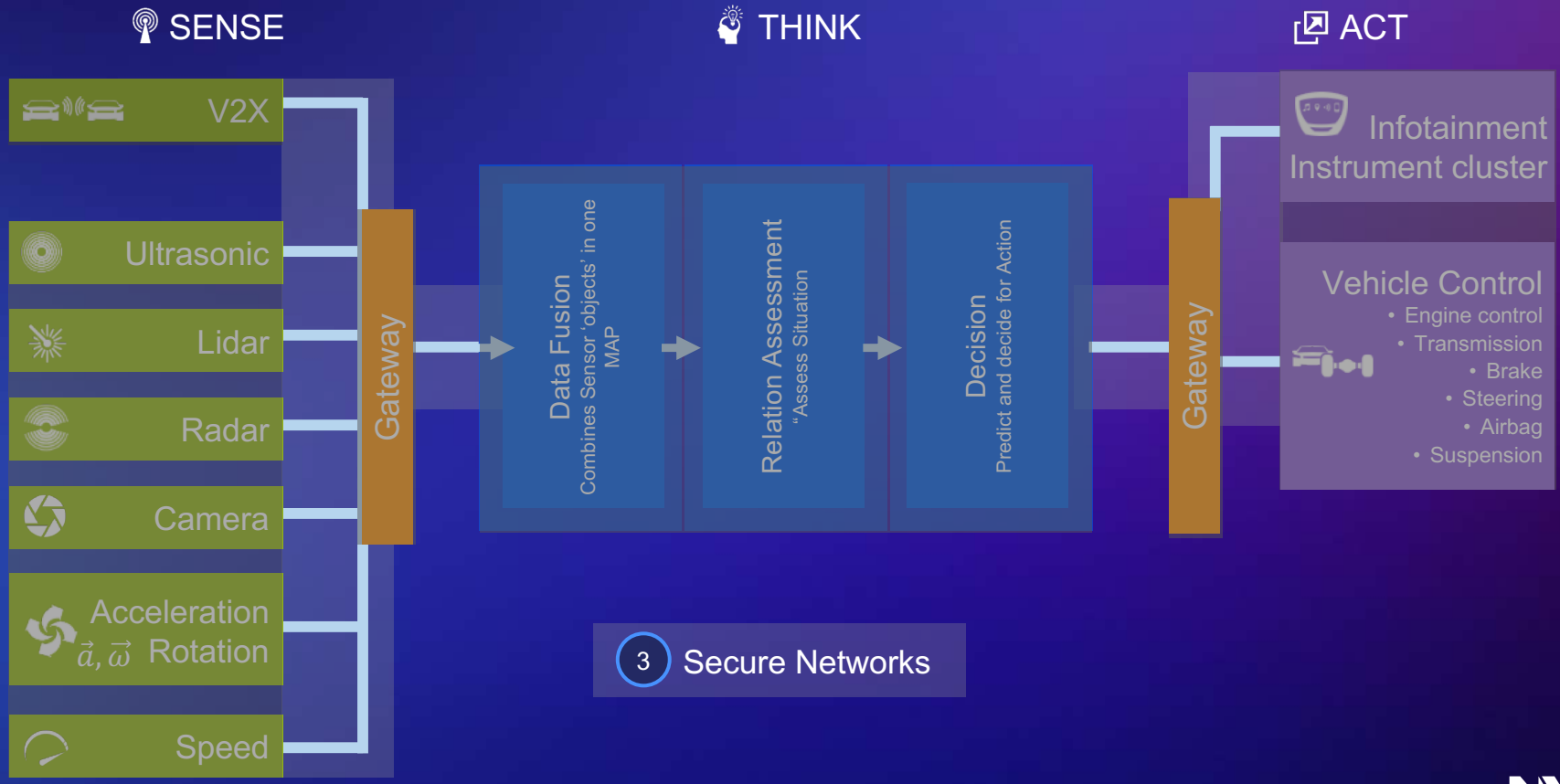
SENSOR FUSION AND HIGHLY AUTOMATED DRIVING



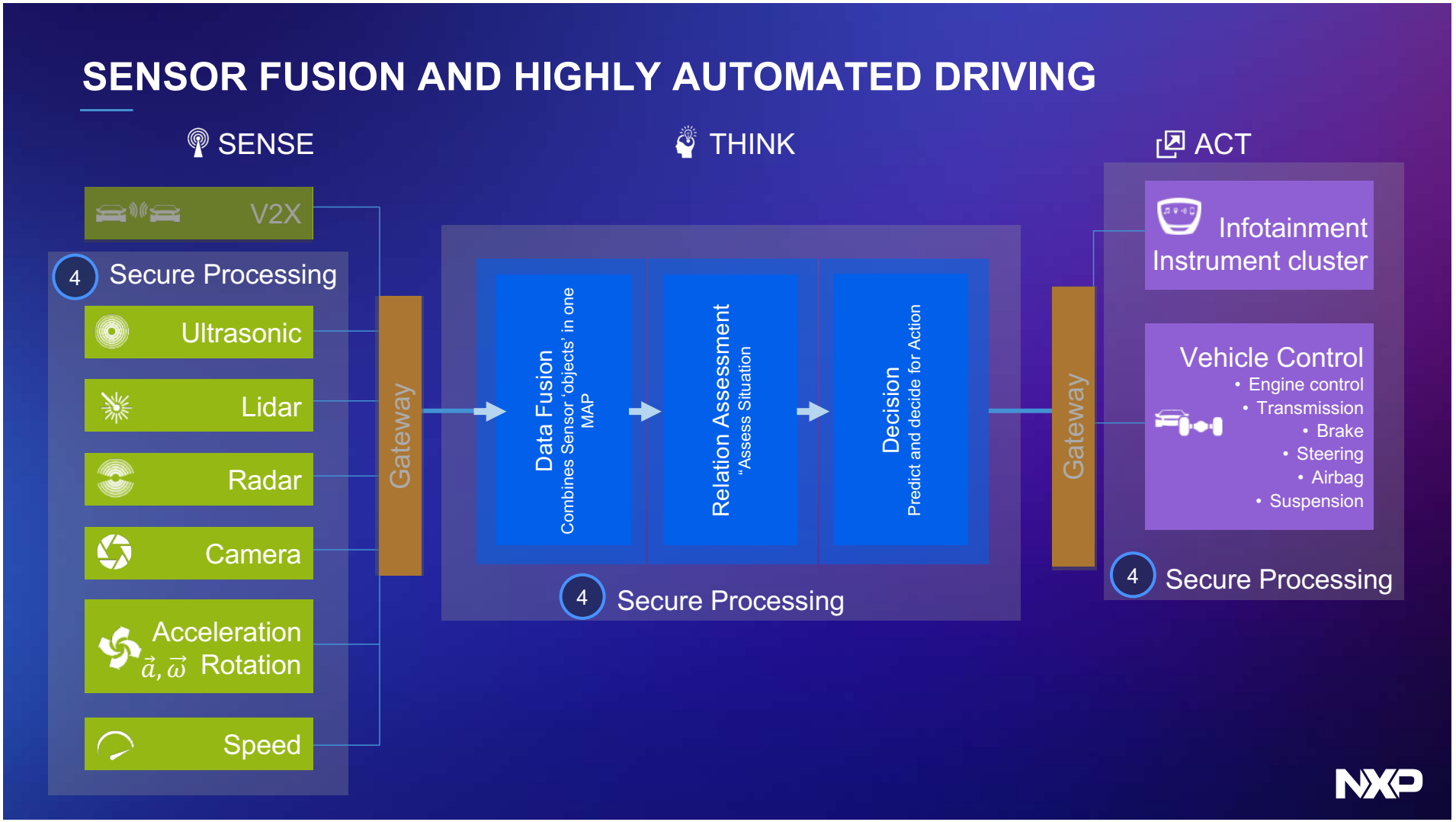
SENSOR FUSION AND HIGHLY AUTOMATED DRIVING

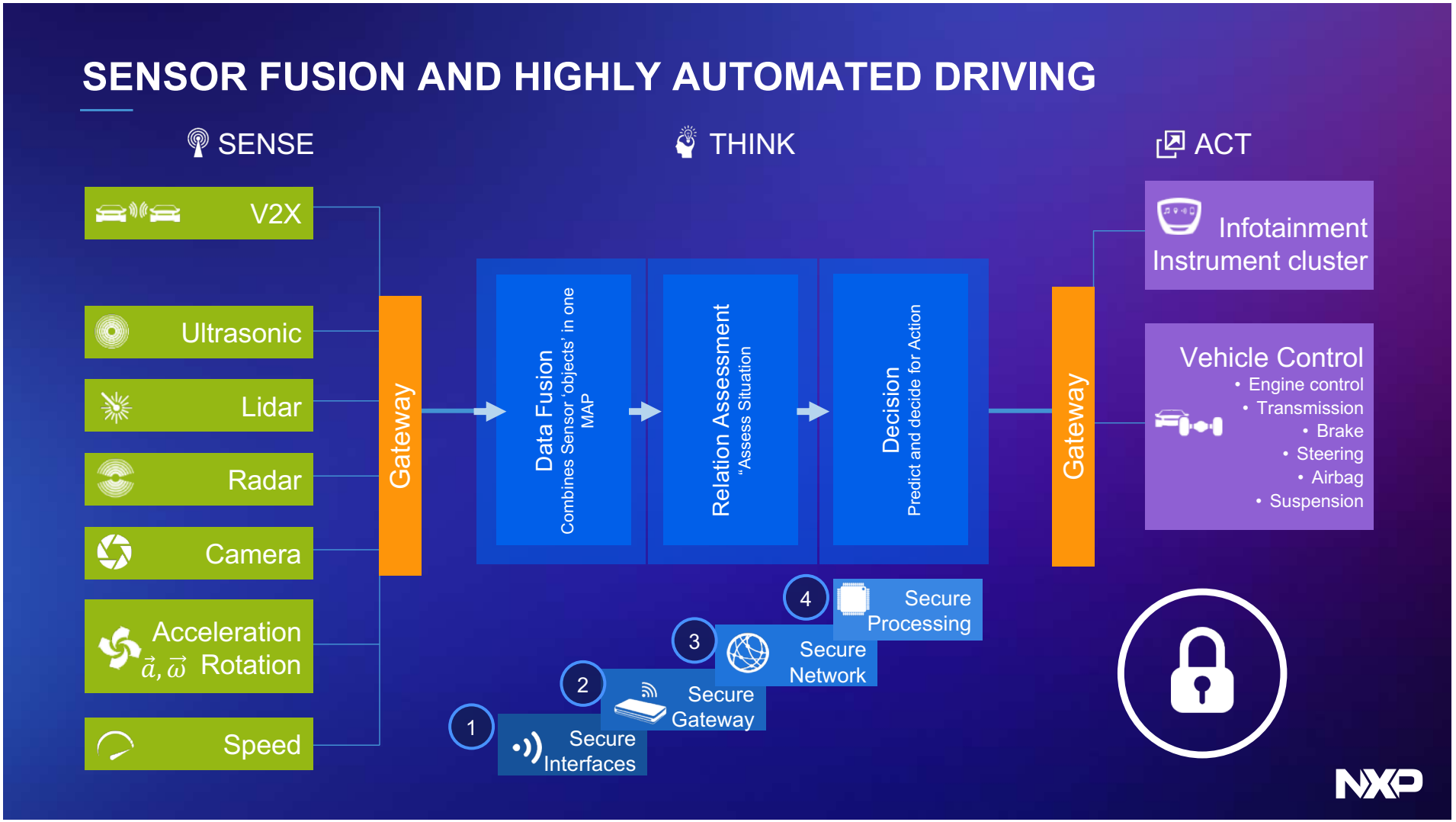


SENSOR FUSION AND HIGHLY AUTOMATED DRIVING



SENSOR FUSION AND HIGHLY AUTOMATED DRIVING




SENSOR FUSION AND HIGHLY AUTOMATED DRIVING
SENSE
THINK
ACT
V2X
Ultrasonic
Lidar
Radar
Camera
Acceleration
$\vec{a}, \vec{\omega}$ Rotation
Speed
Gateway
Data Fusion
Combines Sensor 'objects' in one MAP
Relation Assessment
"Assess Situation
Decision
Predict and decide for Action
Gateway
Infotainment
Instrument cluster
Vehicle Control
• Engine control
• Transmission
• Brake
• Steering
• Airbag
• Suspension
1
Secure Interfaces
2
Secure Gateway
3
Secure Network
4
Secure Processing
NXP

SAFE AND SECURE
MOBILITY
AT THE HEART OF
AUTONOMOUS DRIVING
NXP