SAFE AND SECURE MOBILITY

Keys to Making Level-3 Autonomous Drive Safe and Secure

JENS HINRICHSEN
SVP & General Manager
Business Line Advanced Automotive Analog
AGENDA

- ✔ Automotive Market
- ✔ 5 Domains
- ✔ Functional Safety
- ✔ Security
INDUSTRY MEGA TRENDS
AN INCREDIBLE OPPORTUNITY

CONNECTIVITY
AUTONOMY
ELECTRIFICATION

SAFE AND SECURE MOBILITY
MORE THAN TRIPLING THE SEMI VALUE PER CAR
NXP IS GLOBAL #1
WITH SECURE END-TO-END HARDWARE AND SOFTWARE SOLUTIONS

TECHNOLOGY LEADERSHIP

10% POWER
24% MCU/MPU
18% OTHER
15% SENSORS
32% ANALOG

APPLICATIONS FOCUS

#1 Auto Analog / RF / DSP
#1 Auto Microcontrollers (ex. Japan)
#1 Merchant Auto MEMS Sensors
#1 Car Infotainment
#1 Secure Car Access
#1 Body & In-Vehicle Networking
#1 Safety
#1 Powertrain
Innovation Leader ADAS
Innovation Leader Security

#1 IN AUTO SEMICONDUCTORS

14% IFX
10% REN
7% TXN
8% STM
51% OTHERS

EXTERNAL USE | 3
AGENDA

- Automotive Market
- 5 Domains
- Functional Safety
- Security
TOMORROW’S VEHICLES: SELF-DRIVING, CONNECTED ROBOTS

Level-3 autonomous drive will save >1,3M road fatalities globally

NXP offers safe and secure ADAS solutions….

SENSE
- Radar
- Vision
- Secure V2X

THINK
- Processing
- Sensor Fusion
- Security

ACT
- Powertrain
- Chassis
- Braking

BIG DATA
- Digital Networking
- Infrastructure
- Security

…including Big Data Infrastructure
NXP LEADS DOMAIN BASED VEHICLE ARCHITECTURES

Connectivity

Driver Replacement

Powertrain & Vehicle Dynamics

Body & Comfort

Driver Experience

Networks & Gateways
COMPLETE SOLUTIONS
FASTER TIME TO MARKET
FULL SCALABILITY

NXP LEADS DOMAIN BASED VEHICLE ARCHITECTURES

Connectivity
Driver Replacement
Powertrain & Vehicle Dynamics
Body & Comfort
Driver Experience

SENSE
V2X
Broadcast Radio
Cellular
WIFI, BT, GNSS, NFC
Smart Car Access

THINK
Radar
Camera
Lidar

ACT
Motion & Pressure
Speed
Ultrasound
TPMS

Fusion
Powertrain Domain Controller

Powertrain & Vehicle Dynamics
Engine
Transmission
Brake
Battery Cell Management
Steering

Body Domain Controller

Infotainment

Smart Light
Access, Door Ctrl
eCockpit
Amplifiers

EXTERNAL USE | 7
FUTURE NETWORKS DRIVE FUTURE ARCHITECTURES

**Traditional**

- Flat hierarchy
  - Separate ECUs w/ custom MPUs
  - Point to Point connections
  - Limited Security
  - Low bandwidth data transfer
  - System cost reduction

**Domain Computing**

- Domains separated by gateway
  - Ethernet backbone
  - Preprocessing reduces data transfer
  - Separation of concern for complex networks (HW & SW)
  - Upgradeability and SW scalability

**Centralized Computing**

- Central server hosts >1 domain
  - Cost
  - Fewer ECUs
  - Flexible use of compute power
  - Large bandwidth for data transfer
  - SW virtualization and hypervisor
ADVANCED SYSTEM FUNCTIONALITY: DRIVEN BY DEMAND FOR ACCIDENT-FREE AUTOMATED VEHICLES

1. **Assisted Driving**
   - Security: Risk of Cyber Security Attacks, Increased Connectivity
   - Drastic Power Increase: High Power Efficiency

2. **Co-Pilot Driving**
   - Fast Network: High Speed, High Bandwidth

3. **Automated Driving**
   - Functional Safety: Fail Safe, Fail Silent, Fail Operational, Fault Tolerant
   - Controlled Latencies: No Delay, Controlled Priorities
   - Very High Computing Power: Blue Box

Connecting Points:
- Security
- Drastic Power Increase
- Fast Network
- Functional Safety
- Controlled Latencies
- Very High Computing Power
AGENDA

- Automotive Market
- 5 Domains
- Functional Safety
- Security
SAFETY VERSUS SECURITY

Functional Safety looks at unintentional hazards
*Predictable and regular*

Security looks at intentional hazards
*Unpredictable and irregular*

Standard passive safety systems today
*Active safety becoming more pervasive tomorrow*
WHY FUNCTIONAL SAFETY IS IMPORTANT FOR AUTOMOTIVE

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

Standardization – platform consolidation and system harmonization

Trends – autonomous driving, electric vehicles

Legal – question of responsibility
WHAT IS DRIVING FUNCTIONAL SAFETY TODAY?

Level 0-2
Human driver performs part of the dynamic driving task

Level 3-5
Automated driving system performs the entire dynamic driving task

Needs more performance and towards fail operational safety (Beyond ASIL D as defined by ISO 26262)

SAE standard J3016

HUMAN DRIVER MONITORS DRIVING ENVIRONMENT

AUTOMATED DRIVING SYSTEM MONITORS DRIVING ENVIRONMENT

0 1 2 3 4 5
No Automation Driver Assistance Partial Automation Conditional Automation High Automation Full Automation
SENSOR FUSION AND HIGHLY AUTOMATED DRIVING

**SENSE**
- Ultrasonic: S12
- Lidar: S32V
- Radar: S32R
- Camera: S32V
- V2X: i.MX
- Acceleration, Rotation: PPC
- Speed: S12

**THINK**
- Level 2 & 3 Automated Driving
- Level 4
  - Data Fusion: Combines sensor objects in one map
  - Relation Assessment: Assess situation
  - Decision: Predict and decide for action

**ACT**
- Instrument cluster
- Infotainment
- Vehicle control:
  - Engine control
  - Transmission
  - Brake
  - Steering
  - Airbag
  - Suspension

**Sensor processing creates data object**

**Learning:** Bluebox Development System
SO WHAT DOES FUNCTIONAL SAFETY ACTUALLY MEAN?

- Prevents risks of electronic system malfunctions
- Measures failures, mitigates impact, predicts effects
- Industry-defined standard: ISO 26262 for EE systems
QUANTIFY A RISK: AUTOMOTIVE SAFETY INTEGRITY LEVEL (ASIL) DEFINITION

Severity

How much harm is done?

Exposure

How often is it likely to happen?

Controllability

Can the hazard be controlled?

Severity | Exposure | Controllability
---|---|---
LIGHT | E1→E4 | QM
SEVERE | E1→E4 | QM→A
FATAL | E1→E4 | QM→B

(QM: “quality managed” → no requirements from standard applied explicitly)
LEADING THE INDUSTRY TOWARDS ZERO ACCIDENTS

2016
Fail Safe
High Failure
DETECTION

2018
Fail Silent
Flexible Failure
REACTION

2020
Fail Operational
Intelligent Failure
RECONFIGURATION

2030
High Dependability
Advanced Failure
PREDICTION

SAFETY
SECURITY
EXAMPLES OF A SYSTEM DREADED EVENT AND ASIL LEVELS

<table>
<thead>
<tr>
<th>ADAS Sensor</th>
<th>Battery Management</th>
<th>Power Steering</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phantom detection</td>
<td>Fire</td>
<td>Auto steering, lock, loss</td>
</tr>
<tr>
<td>ASIL B</td>
<td>ASIL C</td>
<td>ASIL D</td>
</tr>
</tbody>
</table>
NXP’S SAFE ASSURE PROGRAM

• Simplify customer experience
• Optimize customer R&D efficiency
• Reduce risk of harm
• Safety starts with quality
NXP FUNCTIONAL SAFETY SYSTEM SOLUTIONS

SAFE
ASSURE™ by NXP

POWERTRAIN
ELECTRIFICATION

VEHICLE NETWORKING

BODY

ADAS/RADAR:
SENSOR FUSION

SECURE CAR ACCESS

INFOTAINMENT

CHASSIS

SAFETY
An example of how to design with Functional Safety

The 2\textsuperscript{nd} Generation Functional Safety-SBC integrates a Fail Safe State Machine:

- Physical & electrical independance (ASILD)
- Power Management Monitoring Unit (UV/OV)
- I/O Monitoring Unit
- Watchdog
AGENDA

- Automotive Market
- 5 Domains
- Functional Safety
- Security
SECURITY FOUNDATION FOR THE CONNECTED CAR

- Protect privacy
- Prevent unauthorized access
- Increase safety
AUTOMOTIVE SECURITY – WAY FORWARD

APPLY BEST PRACTICES:
• Security-by-design & Privacy-by-Design (as opposed to being an afterthought)
• Lifecycle Management (incl. FOTA)

Essential element: Defense-in-Depth approach
• Multiple layers of protection, at different levels in the system
• To mitigate the risk of one component of the defense being compromised or circumvented
NXP OFFERS MOST SCALABLE AUTO CYBERSECURITY SOLUTION

NXP #1 Automotive Hardware Security

4-Layer security solution

1. Secure wireless interfaces – HW crypto
2. Secure gateway – separation of concerns
3. Secure in-vehicle network communication
4. Secure application processing
CORE SECURITY PRINCIPLES

Secure External Interfaces
Secure M2M authentication, secure key storage

Secure Domain Isolation
Domain isolation, firewall/filter, centralized intrusion detection (IDS)

Secure Internal Communication
Message authentication, CAN ID killer, distributed intrusion detection

Secure Software Execution
Secure boot, run time integrity, Over-the-Air updates

All essential elements for any architecture and implementation
CONCLUSION

Today’s traditional view of Automotive is converging towards Safe & Secure Mobility.

The trend towards autonomous driving is significantly increasing the compute power within the future cars.

To increase the trust of highly automated systems, Functional Safety & Security become essential elements of the self-driving car.

Functional Safety looks at unintentional hazards, while Security looks at intended hazards.

Both elements must become an integral part of the car’s electronics architecture.

NXP offers a scalable auto cybersecurity solution and high performance functional safety systems to make the autonomous car a reality.