Safety and Security in the Car of the Future

Luis Basto
Feb 11, 2020
Agenda
Intro
Safe and Secure Mobility
Security is critical for connected vehicles
4+1 Automotive Security Framework
Safety & Security Go Together
Standards and Best Practices
Q&A
Some terms use in automotive electronics

- CAN bus – Controller Area Network
- DSRC – Dedicated short range communication (802.11p)
- V2X – V2V, V2I (vehicle-vehicle, vehicle to whatever)
- ADAS – Advanced Driver Assist System
- ASIL – Automotive Safety Integrity Level
- LIDAR – Light Detection and Ranging
- IVI – In vehicle infotainment
- EPS – electronic power steering
- ESP – electronic stability program
- ISO -26262 Functional Safety Standard
Safe and Secure Mobility
More than tripling the semi value per car – today’s standard car at $380
Autonomy

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
<th>Price (vs Level 0)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>No Automation</td>
<td>$0</td>
</tr>
<tr>
<td>1</td>
<td>Driver Assistance</td>
<td>$50</td>
</tr>
<tr>
<td>2</td>
<td>Partial Automation</td>
<td>$100</td>
</tr>
<tr>
<td>3</td>
<td>Conditional Automation</td>
<td>$400</td>
</tr>
<tr>
<td>4</td>
<td>High Automation</td>
<td>$600</td>
</tr>
<tr>
<td>5</td>
<td>Full Automation</td>
<td>$700</td>
</tr>
</tbody>
</table>

- Level 0-2 Human Driver: Performs part of dynamic driving task, Monitors environment
- Level 3-5 Automated Driving System: Performs entire dynamic driving task, Monitors environment

Source: Strategy Analystics; IHS; Evercore; ABI Research; NXP
Electrification

- **Pure Electric Vehicle**: $+450
- **Range Extended Electric Vehicle**: $+425
- **Plug-in Hybrid**: $+400
- **Full Hybrid**: $+350
- **Mild Hybrid**: $+200

Semi-Content per Car Increase (TAM) vs Level 0

Source: Strategy Analytics; IHS; Evercore; ABI Research; NXP
## Connectivity

<table>
<thead>
<tr>
<th>Level</th>
<th>Connectivity Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>C0</td>
<td>No Connectivity</td>
</tr>
<tr>
<td>C1</td>
<td>Analog Radio</td>
</tr>
<tr>
<td></td>
<td>AM/FM, WiFi, BT</td>
</tr>
<tr>
<td>C2</td>
<td>+ Connectivity</td>
</tr>
<tr>
<td></td>
<td>2G/3G AM/FM, WiFi, BT</td>
</tr>
<tr>
<td>C3</td>
<td>+ Digital Radio, 4G</td>
</tr>
<tr>
<td></td>
<td>AM/FM, Digital, 4G</td>
</tr>
<tr>
<td>C4</td>
<td>+ 4G-LTE Advanced, V2X Security</td>
</tr>
<tr>
<td></td>
<td>AM/FM, Digital, 4G-LTE, WiFi, BT</td>
</tr>
<tr>
<td>C5</td>
<td>Fully Connected Car</td>
</tr>
<tr>
<td></td>
<td>AM/FM, Digital, 4G-LTE, WiFi, BT</td>
</tr>
</tbody>
</table>

*Source: Strategy Analytics; IHS; Evercore; ABI Research; NXP*
Automotive
Solutions for Safe and Secure Mobility

Value Proposition

Solution portfolio
The most complete system solutions for fastest time to market and scalability

Innovation power
In-house high performance processing, security and mobile eco-system capabilities

Automotive safety & reliability
Zero defect quality
Leading with security and functional safety
Safety & Security
Did you Know?

- **>50 Vehicle hacks**
  - published since 2015

- **1.4 M Vehicles recalled**
  - in the largest incident to date

**Why hacking?**

- **Valuable data** attracts hackers
- Car-generated data may become a 750 B$ market by 2030

**Security is a MUST-HAVE for connected & autonomous vehicles**
Did you Know?

>50
Vehicle hacks published since 2015

1.4 M
Vehicles recalled in the largest incident to date

Why hacking?
Valuable data attracts hackers
Car-generated data may become a 750 B$ market by 2030

Why is it possible?
High system complexity implies high vulnerability
Up to 150 ECUs per car, up to 200 M lines of software code

SECURITY IS A MUST-HAVE FOR CONNECTED & AUTONOMOUS VEHICLES
Today's Vehicle contains greater than **200 million** lines of code.

- MODERN HIGH END CAR
- facebook
- Windows Vista
- Large Hadron Collider
- Boeing 787
- Android
- Chrome
- Linux
- Kernal 2.6.0
- Mars Curiosity Rover
- Hubble Space Telescope
- Space Shuttle

The car today contains more software than any other embedded system and most compute applications.

Source: choice.com.au
Did you Know?

- **>50** Vehicle hacks published since 2015
- **1.4 M** Vehicles recalled in the largest incident to date

**Why hacking?**
- Valuable data attracts hackers
- Car-generated data may become a 750 B$ market by 2030

**Why is it possible?**
- High system complexity implies high vulnerability
- Up to 150 ECUs per car, up to 200 M lines of software code

**Why now?**
- Wireless interfaces enable scalable attacks
- 250 M connected vehicles on the road in 2020

SECURITY IS A **MUST-HAVE** FOR CONNECTED & AUTONOMOUS VEHICLES
Cybersecurity Threats in Automotive

**Local Attacks**

- Tampering the odometer
  - [Odometer Fraud Facts](https://www.nhtsa.gov/equipment/odometer-fraud)

- Engine tuning
  - Workshop around the corner, or in your garage

**Remote Attacks**

- Vehicle theft by relay attack
  - [Remote hack of an unaltered car (July 2015)](https://www.youtube.com/watch?v=MK0SrxBC1xs)

- Ransom for a drive
  - [Remote hack of an unaltered car (July 2015)](https://www.youtube.com/watch?v=8pfcngJLq0)

- VDI Conference on IT Security for Vehicles (Berlin / July 2017)
  - [Remote hack of an unaltered car (July 2015)](https://www.youtube.com/watch?v=M0xSrBC1xs)
What is at Risk and who is Affected?

<table>
<thead>
<tr>
<th>IMPACT</th>
<th>Car Users</th>
<th>Car Owners</th>
<th>Insurers</th>
<th>OEM &amp; Suppliers</th>
<th>Service Providers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Safety</strong></td>
<td>Injuries</td>
<td>Damage</td>
<td></td>
<td>Claims, brand damage</td>
<td></td>
</tr>
<tr>
<td><strong>Financial</strong></td>
<td>Vehicle theft</td>
<td>Insurance claims</td>
<td>IP theft</td>
<td>Loss of income (fraud, DoS, …)</td>
<td></td>
</tr>
<tr>
<td><strong>Privacy</strong></td>
<td>Loss of personal data (PII)</td>
<td></td>
<td>Claims, brand damage</td>
<td>Claims, brand damage</td>
<td></td>
</tr>
</tbody>
</table>
Layer 1 - Secure Interface

Layer 1: Secure Interface
Secure M2M authentication, secure key storage

- TCU
- OBD
- SE
- ADAS
- Braking
- Powertrain
- IVI
- Cluster
- Body
Layer 2 – Secure Gateway

Layer 2: Secure Gateway
Domain isolation, firewall/filter, centralized intrusion detection (IDS)
Layer 3 – Secure Network

Layer 3: Secure Network
Message authentication, CAN ID killer, distributed intrusion detection (IDS)
Layer 4 – Secure Processing

Layer 4: Secure Processing
Secure boot, run time integrity, OTA updates
Layer 4 – Secure Processing

+ Secure car access – remote lock/unlock, immobilizer, car access via NFC, etc.
Safety & Security Go Together

#1 Objective: no functional **hazards** on mission-critical ECUs → Protects people

Only possible, if:
- System availability **ensured**
- Information received / processed **trustworthy**
→ Protects against loss
Functional Safety & Security – System-Level Concerns

IC-LEVEL SAFETY & SECURITY SOLUTIONS + SAFE & SECURE DOMAIN ARCHITECTURES = SAFE AND SECURE MOBILITY

• Resource isolation
• On-die monitoring
• Integrity & authenticity checks

• Domain isolation
• Firewalls
• Network intrusion detection

• Fail operational
• Resilient against cyber attacks
<table>
<thead>
<tr>
<th>Domain</th>
<th>Application</th>
<th>Hazardous Event (example)</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active safety</td>
<td>Central Fusion</td>
<td>Inadvertent hard braking during driving</td>
<td>D</td>
</tr>
<tr>
<td>Passive Safety</td>
<td>AIRBAG</td>
<td>Inadvertent deployment during driving</td>
<td>D</td>
</tr>
<tr>
<td>Chassis</td>
<td>EPS</td>
<td>Self steer during driving</td>
<td>D</td>
</tr>
<tr>
<td></td>
<td>Stability control</td>
<td>One wheel lock during driving</td>
<td>D</td>
</tr>
<tr>
<td></td>
<td>ABS</td>
<td>One wheel lock during hard braking</td>
<td>C</td>
</tr>
<tr>
<td>HEV/EV</td>
<td>Motor control</td>
<td>Sudden Torque Up/Down</td>
<td>C</td>
</tr>
<tr>
<td>Power Train</td>
<td>Transmission</td>
<td>Speed down on express way</td>
<td>C</td>
</tr>
<tr>
<td></td>
<td>Engine control</td>
<td>Decreasing of engine torque</td>
<td>B</td>
</tr>
<tr>
<td>Body</td>
<td>Brake Lamp</td>
<td>No brake lighting during braking</td>
<td>B</td>
</tr>
</tbody>
</table>

ASIL Level Examples For Different Solutions

ADAS/ RADAR: SAFE CENTRAL COMPUTE
SECURE CAR ACCESS
POWERTRAIN ELECTRIFICATION
SAFETY

VEHICLE NETWORKING
BODY
CHASSIS
NXP
### 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 Automotive Security Solutions

Automotive ICs with... on-chip security subsystems

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

Security Controller (SECO)
- High performance
- Media content protection

Security Engine (SEC)
- High performance
- Versatile feature set

Security Controller (SECO)
- Ease-of-use
- Cost-optimized

Security companions

- Security Element (SE)
  - Tamper-resistant secure system ideal for M2M authentication (e.g. V2X)

Function-specific secure ICs

- Secure CAN Transceiver (TJA115x)
  - For enhanced IDS & IPS

- Secure Ethernet Switch (SJA1110)
  - Network frame analysis (L2/L3/L4)

- Secure Car Access ICs
  - For advanced RKE / PKE solutions

- V2X DSRC Baseband (SAF5x00)
  - Ultra-fast ECDSA verifications
Standards and Best Practices

NXP is an active member of Auto-ISAC

- A key forum and network for automotive cybersecurity
- Enables leveraging industry know-how & best practices
- And sharing intelligence on threats & vulnerabilities

We also participate in standards development; e.g.:

- ISO/SAE 21434
- SAE TEVEES18 (J3061, J3101, …)
- AUTOSAR WP-X-SEC
- IEEE 1609 WAVE, ETSI TC ITS
- Car Connectivity Consortium (CCC) – Digital Key Specification
- ISO/SAE 21434 (Road Vehicles – Cybersecurity Engineering, 2020)
- Making Safe & Secure Mobility a Reality

Solution Portfolio

The most complete system solutions for fastest time to market and scalability.

Innovation Power

In-house high performance processing, security and mobile eco-system capabilities.

Safe & Secure

Zero defect methodology. Leading with security and functional safety.