ACCELERATING TECHNOLOGY TRENDS

Secure Connections for a Smarter World

Everything Secure and Safe

Potential savings to economy up to half trillion dollars

Security

Everything Connected

1B+ additional consumers online, 30B+ connected devices

Connectivity

Everything Smart

40B+ devices with intelligence shipped

Processing

Source: Euromonitor; Gartner; ARM Holdings; UBS; Center for Strategic and International Studies; McAfee, NXP analysis, International Telecommunications Union
NXP BUSINESSES

Security & Connectivity
Best-in-class security, contactless performance and the most complete solutions to produce unmatched mobile and IoT solutions

Automotive
Sensor and processing technology driving all aspects of the secure connected cars of today and the autonomous cars of tomorrow

Digital Networking
High-performance multicore solutions that transport, analyze and secure data from the edge of the network to the cloud

Standard Products
Leading supplier for all major automotive, identification, wireless infrastructure, industrial, mobile, lighting, consumer and computing manufacturers

RF
Solutions spanning the wireless infrastructure, broadcast, medical, mobile radio, military, aviation, cooking and industrial markets
Hyper-connectivity is Changing Our World Forever

CONVENIENCE
SECURITY
MOBILITY
INDUSTRIAL AUTOMATION
ENERGY EFFICIENCY
HEALTH

*Source: World Economic Forum
http://www.weforum.org/issues/hyperconnected-world
SEMICONDUCTORS ENABLING SYSTEM SECURITY

- eGoverment
- Mobile Commerce
- Brand Protection
- Banking
- Smart Mobility
- Cyber Security
TODAY: 90% OF AUTO INNOVATION VIA ELECTRONICS

NXP IS #1

#1 INFOTAINMENT
TUNERS
SOFTWARE-DEFINED DIGITAL RADIO
MULTIMEDIA PROCESSORS
SOUND SYSTEM DSPs & AMPLIFIERS
NFC BT PAIRING
WIRELESS POWER CHARGING
POWER MANAGEMENT

STANDARD PRODUCTS
LOGIC
POWER
DISCRETES

#1 VEHICLE NETWORKING
CAN/LIN/ FLEXRAY
ETHERNET
CENTRAL GATEWAY CONTROLLER
SECURITY

#1 BODY
MICROCONTROLLERS
POSITION/ ANGLE SENSORS
SYSTEM BASIS CHIPS

#1 SAFETY
MICROCONTROLLERS AIRBAG
ANALOG AIRBAG
MICROCONTROLLERS BRAKING
ANALOG BRAKING
SENSORS BRAKING
TIRE PRESSURE MONITORING

#1 SECURE CAR ACCESS
IMMOBILIZER/ SECURITY
REMOTE KEYLESS ENTRY
PASSIVE KEYLESS ENTRY/ GO
BI-DIRECTIONAL KEYS
NFC
ULTRA WIDE BAND

#1 Auto Analog/ RF

#1 Auto MCU (ex JPN)

#1 Auto Merchant MEMS Sensors
TOMORROW: ENABLING THE SECURE CONNECTED CAR

Secure Connected, Self-Driving Cars will Save >1,3M Road fatalities globally

NXP Offers Complete Secure ADAS System....

SENSE
Radar Vision
Secure V2X

THINK
Processing
Sensor Fusion
Security

ACT
Powertrain
Chassis
Braking

BIG DATA
Digital Networking Infrastructure
Security

...including Big Data Infrastructure

Surround View
Blind Spot Detection
Rear Collision Warning
Park Assist
Surround View
Cross Traffic Alert
Traffic Sign Recognition
Emergency Braking
Pedestrian Detection
Collision Avoidance
Lane Departure Warning
Adaptive Cruise Control
Security
Secure Network
Secure Network
Secure Network
Secure Network

EXTERNAL USE
ADAS: FROM SENSORY DATA TO KNOWLEDGE

ADAS – INFORMING ⇒ SITUATIONAL AWARENESS ⇒ HIGHLY AUTOMATED VEHICLES (HAD) ⇒

INTELLIGENT FUNCTIONS

<table>
<thead>
<tr>
<th>PERCEPTION</th>
<th>Safe Secure Reliable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Front &amp; Corner Radar</td>
<td></td>
</tr>
<tr>
<td>Mono/ Stereo Vision</td>
<td></td>
</tr>
<tr>
<td>Secure V2X</td>
<td></td>
</tr>
<tr>
<td>SCP220x</td>
<td></td>
</tr>
<tr>
<td>S32R2/3x</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>COMPREHENSION</th>
<th>Safe Secure Reliable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safe DAS Processing</td>
<td></td>
</tr>
<tr>
<td>Sensor Fusion/ 360°</td>
<td></td>
</tr>
<tr>
<td>Sense Grid Mapping</td>
<td></td>
</tr>
<tr>
<td>S32V234</td>
<td></td>
</tr>
<tr>
<td>S32V244</td>
<td></td>
</tr>
<tr>
<td>S32R4x</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PREDICTION</th>
<th>Path Optimization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intelligent Vehicles</td>
<td></td>
</tr>
<tr>
<td>S32A 25x</td>
<td></td>
</tr>
</tbody>
</table>
Applications Trends, Safety Context and Technical Advancements

**Assist**
- NCAP 2016: Lane detect, pedestrian detection, ACC
- Automotive safety (ASIL B) as driver is active
- Classic machine learning for mono front view/ rear view
- 2D/3D Surround View

**Co-Pilot**
- Active steering, emergency braking, HW platoon and self-park
- Automotive safety (ASIL B - C) with security
- Optical flow, sensor fusion and sophisticated classifiers

**Automate**
- 360° sensing; 3D high-accuracy environmental model
- Fully automated vehicle and fail operational system
- Deep learning and advanced machine vision with integrated V2X

Increasing complexity, increasing safety
The “Language” of Intelligent Vehicles

Assist
- Aut. cruise ctrl
- Lane det./ keep
- Blind spot det.
- Road sign rec.

Partially Automated
- Smart Sensor and Fusion
- Co-Pilot Mode
- Dependability
- Park assist
- EBA
- Highway platoons
- ACC with steer

Fully Automated or Autonomous
- Independent Decision ⇒ Full Automation
- Driverless
- Fail Operational
- Commercial autonomous vehicles (drones-big vehicle)
- Driverless public transport
- ACC with steer
ADAS – Real-Time Network of Sensors, Processors and Actuators

**SENSE**

- Radar
- Camera
- Lidar
- Ultrasonic

**THINK**

- V2X

**ACT**

- Instrument cluster
- Vehicle Control:
  - Engine
  - Transmission
  - Brake
  - Steering
  - Airbag
  - Suspension

- Line of Sight
- Non-Line of Sight
- Vehicle State

- Ethernet / CAN

- NXP Portfolio
"Intelligent vehicles are a set of agents which integrate multi-sensor fusion-based environment perception, modeling, localization and map building, path planning, decision making and motion control."

Prof. Cheng - 2011
Processing resources need to be dynamically managed to execute \textit{probabilistic} and \textit{deterministic} functions... Within the same vehicle context.
Automated Drive – Prototyping Platform

1. Rapid prototype platform
2. Performance analysis tool
3. Optimization of acceleration SW
4. Abstract and virtualize (MILS, processing affinity)
‘Blue Box’ Prototyping Platform: 2015-17

- Very high **performance** multicore SoC - 72,000 DMIPS, 64 GFLOPS
- Multiprotocol networking acceleration
- Hardware support for virtualization/separation of real-time and non-real-time functions
- Secure Boot, Secure Debug, Anti-Tamper

- Scalable & **SAFE** Multicore SoC - ~10,000 DMIPS, 40 GMACS
- SW: Automotive and safe quality
- Secure boot, secure debug, anti-tamper
Infotainment & Driver Assistance

Car Infotainment

**Car Radio / TV**
Application: AM/FM, Digital Radio / TV, Audio
Key Product: Dirana, Hero, Atomic (AM/FM)
Cayman, Saturn (Digital Radio / TV)
Mercury (AM/FM/DR - hybrid)
Technology: RFCMOS 1-chip integration
SDR-based multi-standard reception, C065 & C040

**Audio Amplifiers**
Application: Audio Headunit & Sound System
New use cases: engine sound
Key Product: BAP3 / TDF853x (new gen. Class-D)
TDF859x / 8530 (Class-D)
TDF854x (Class-AB)
Technology: Full-digital incl. low-latency ADC, ABCD9

Driver Assistance

**Car-2-X Comm.**
Application: Car-2-car/infrastructure comm., DSRC
Key Product: Mars (DSP)
Wisa (RF transceiver)
SmartMX2 (security)
Technology: RFCMOS 1-chip integration
SDR-based multi-standard reception, C065 & C040

**Radar**
Application: Short / mid / long-range radar
Key Product: Dolphin (digital radar front-end)
Orca (radar 1-chip)
Technology: RFCMOS 1-chip integration, C040
CONNECTED CAR – WHY A HACKER’S TARGET?

Easy Access
- Fully Connected Car
- External & internal interfaces
- Wired & wireless interfaces

Prevent unauthorized Access

High Vulnerability
- Increasing number of nodes
- More advanced features
- X-by-Wire

Increase Safety

Valuable Data
- Collection of data/info
- Storage of data
- Diagnostic functions

Protect Privacy

Smart Car Access
In-Vehicle Network
Cloud Connection
Car2X
Consumer Device Integration
ENTRY POINT: WIRELESS CAR INTERFACES

Wireless interfaces allow for remote attacks:

- More anonymous $\rightarrow$ less risk for the attacker
- More people can attempt $\rightarrow$ lower (avg.) cost
- More cars can be affected $\rightarrow$ larger benefits

Easier and scalable, so likelihood is high!

**Physical Attacks Lead to Remote Attacks**
CHALLENGE: VEHICLE NETWORK ARCHITECTURE

Time

Network Architecture

Protection Level

Full Network is exposed to Attacks

Gateway controls Access to sub Networks

Domain Gateways control Access to Domain Networks
We need to prevent that keys can leak out!

> Physical (tamper-resistant) protection of the keys

FROM PHYSICAL TO REMOTE ATTACK

Example: remote software update
SECURITY BY DESIGN
Prerequisite for all applications in the connected world

- UNOBTRUSIVE
- ADDING VALUE
- REVIEWED
- STATE OF THE ART
- LAYERED
- SECURITY BY DESIGN
- UPGRADABLE
- DECENTRALIZED

SECURITY BY DESIGN
Prerequisite for all applications in the connected world
SOLUTIONS PREVENTING SECURITY ATTACKS

Example: Secure Connected Car

- Secure Car Access
- Secure Telematics
- Securing V2X Communications
- Securing Car Entertainment
- Trust Provisioning for System Security
Secure Car Access: Applications

Immobilizer:
- Car theft protection

Remote Keyless Entry (RKE):
- Car theft protection
- Remote car door lock and unlock

Passive Keyless Entry (PKE):
- Car Theft protection
- Remote car door lock and unlock
- Passive keyless entry
- Passive Start

Smart Car Management:
- Car key communication for:
  - Remote start
  - Car finder
  - Alarm Systems
  - Tire pressure information
  - Fuel level / Charging state
  - Door lock status

Connected Keyless Entry:
- Car Access via NFC enabled phones/wearables
- NFC key advantage: secure transport of keys
- Alternative: Car access via phone using BLE and key fob as ‘Gateway’

Car-key communication for:
- Remote start
- Car finder
- Alarm Systems
- Tire pressure information
- Fuel level / Charging state
- Door lock status

Car- key communication for:
- Remote start
- Car finder
- Alarm Systems
- Tire pressure information
- Fuel level / Charging state
- Door lock status
Secure Car Access: How does it work?

**Immobilizer**
Authentication for Engine Start

1. LF Challenge
2. LF Response

**Remote Keyless Entry**
Authentication for Car Entry

RF signal (rolling code) (on Button press)
Immo/RKE function included*

**Passive Keyless Entry**
Hands free Authentication

1. LF Wake-Up/Challenge
2. RF Response
Immo/RKE function included*

**Smart Car Management**
2 way RF for convenience & robustness

RF data Exchange
Up to 500m

**Connected Keyless Entry**
Access via NFC enabled phones

RF data Exchange
Up to 10cm

*Immo/RKE function included*
Security:
Was the message not modified?
Did it really originate from car A?
Can I trust car A?
Car and message authentication required to prevent traffic disruption or impersonation

Privacy:
Can others track me while driving?
High degree of anonymity (identity hiding) required to prevent tracking
SECURING V2X COMMUNICATIONS
Message authentication via digital signatures … with very high performance requirements

- Digital signature
  - For authentication (sender identity, content integrity)
  - And non-repudiation (no plausible deniability)
- Based on
  - Hash function → unique identifier for message
  - Public-key crypto: two keys, one is private (secret), other public (non-secret)
- ETSI (EU) and IEEE (US) standards mandate ECDSA
  - RSA signatures too long (bandwidth limitation)
  - Comparable security strength: RSA 3072b ~ ECC 256b ~ AES 128b
- Performance requirements
  - Up to 1000 messages per second for signature verification
SECURING CAR ENTERTAINMENT
Conditional Access for Subscribed Services

- Flexible approach for key ladder usage via embedded CA application
- All (intermediate) keys remain in private Trusted Environment
- Secure root of trust key storage mechanism in place
Leadership Security – i.MX Hardware Enablement

Secure Storage
- In-line encryption (memory)
- Manufacturing protection
- Authenticated debug & field returns
- Run-time integrity
- Trust zone

Secure S/W Execution
- Secure Storage
- Zeroizable RAM
- Root of trust

Identity Management
- Cryptographic Acceleration
- Symmetric and asymmetric accl.
- Random number generator

Secure Data Communications
- Attack Protection
- Active tamper detection (Physical)
- DPA protection (side channel)

Secure Network Access
- Secure S/W Execution
- Resource domain control
- System memory protection unit
- On-the-fly decryption (code)

Policies & Certifications
TRUST PROVISIONING FOR SYSTEM SECURITY

- Not impacted by key management

Service Provider → Trusted Service Manager

Data/App

Manufacturing

Secure communication

Initial Security Module key

Dealer

OEMs
SECURE TELEMATICS

Enabling Privacy and Fraud Protection

- CAN
- USB
- UART
- GPIO
- SIM
- ADC
- PCM
- Microphone
- Loudspeaker
- Baseband Microprocessor
- Memory
- GSM
- RF PA
- Antenna
- 2nd Antenna
- GPS
- Active GPS Antenna
- Passive GPS Antenna
- NFC
- NFC Antenna
- RTC Battery
- Main Battery
- Charger
Semiconductors as Enabling Technology for Secure Connections in a Smarter World

Approach
- Security and Privacy BY DESIGN
- TAMPER RESISTANT components
- RELIABLE KEY MANAGEMENT schemes
- PROVEN & CERTIFIED solutions

Handshake of Government, Industry, Public
Definition and consistent exertion of “security & privacy by design” principles, transparency and need-to-know principle
- The Human in the Center
- Secure Identities and Consumer Trust driving the IoT Market
READY NOW TO SUPPORT YOU TO ACHIEVE SUCCESS

SECURE CONNECTIONS
FOR A SMARTER WORLD

©2015 NXP Semiconductors