Semiconductor challenges for a “Securely Connected Smart World”

Hans Rijns
CTO - NXP Semiconductors

ISS Europe
Stresa, 25 February 2013
NXP – A European Global Innovator

- Established in 2006 (formerly a division of Royal Philips)
- Net sales: $4.36 billion in 2012
- In > 25 countries in Europe, Asia and US
- Manufacturing in Europe and Asia

Strong Innovation Pipeline:
- Over $550M / year in R&D
- 3,300 engineers
- 11,000 patents
- Focused Mixed-signal portfolio
The Internet of Things will drive the next semiconductor growth wave

Bringing the industry over $400Bn…

…and doubling IP device volumes

**Semiconductor industry revenue**, bn USD

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>50</td>
<td>100</td>
<td>150</td>
<td>200</td>
<td>250</td>
<td>300</td>
<td>350</td>
<td>400</td>
</tr>
</tbody>
</table>

**Connected devices in use**, bn Units

<table>
<thead>
<tr>
<th>Year</th>
<th>2003</th>
<th>2011</th>
<th>2020</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value</td>
<td>1</td>
<td>9-12</td>
<td>50</td>
</tr>
</tbody>
</table>

**Driver**

- Computer
- Smartphone
- M2M

Source: WSTS (extrapolated after 2011), Cisco, BBC, Gartner, GSMA, OECD

(1) Excluding phones, computers,
Urbanization and mega cities drive M2M…

- In 2007 about 50% of our world population lived in Urban environments
- By 2050 this is expected to be around 70-80%
- This drives the need for innovation in Smart Mobility and Smart Energy
…..with numerous related application areas
Evolution of connectivity

Reliability level

- “Lethal”
- “Critical”
- “Comfort”

Dependable systems

Supportive systems

- “On-demand”
- “Always-on”
- “Autonomous”

Networking level

- Stand alone device
  - Single node, no data exchange
- Connected devices
  - Info exchange between single nodes
- Cooperative systems
  - Database & infrastructure supported
- Collaborative systems
  - Dynamic self-controlled systems. Configuration is function of capabilities of the nodes

“Lethal”
“Critical”
“Comfort”

Info exchange between single nodes
Connected World theme raises challenges to the semiconductor industry

- **Wireless; How to…**
  - Enable all wireless data traffic within finite spectrum: cognitive radio
  - Handle all different standards and protocols: Software Defined Radio
  - Ensure only on-demand power usage: duty-cycled radio
  - Receive multiple signals simultaneously: multi-antenna / array systems
  - Ensure ‘lethal-level’ QoS: redundancy, majority voting, prognostics

- **Data integrity**
  - Trusted data, protected privacy and guaranteed secure data transfer: authentication and encryption
  - Counter-act security threats and physical attacks: war fare!

- **System complexity**
  - Concurrent development application functionality and connectivity solutions: value chain partnering
Case 1: Smart Mobility

*Wireless systems view*

- **802.11p**
- **LF, UHF**
- **Cellular**
- **NFC**

Diagram showing various wireless technologies and their applications in smart mobility.
Smart Mobility

*Functional view*

- **Intelligent Traffic Management**
- **Car Entertainment**
- **Car Access & Remote Car Management**
- **In Vehicle Networks**

*Networks:*
- CAN
- FlexRay
- Ethernet
Smart Mobility
Applications & end-user view

*Third party businesses include insurance companies, fleet management, traffic control
Source: SBD, 2012
So by 2022, 20-25% of cars will be connected

Sources: Cisco IBSG, 2011, based on data from U.S. Department of Transportation, iSupply, McKinsey & Company
Intelligent Transport Systems (ITS)

- Car-car and car-Infrastructure communication network
- Traffic/energy management (support systems):
  - Emergency vehicles
  - Speed congestion controls
  - Green light zone
- Safety (dependable systems):
  - Beyond driver line-of-sight; hazardous location & Curve Speed Warning
  - Lane change warning
  - Collision Warning
  - Car as a Sensor
- Supported by dedicated wireless standards
  - ETSI/IEEE, Car2Car Communications Consortium
C2X – Emergency vehicle warning

Courtesy of Cohda Wireless
C2X – Seeing around corners

Courtesy of Cohda Wireless
C2X – Hazard warning

 Courtesy of Cohda Wireless
ITS Challenge 1: Connected car is an open system.....how to ensure security and privacy?

- Avoid car hacking
- Data Security is precondition to safe Car2X comms
- Personal privacy

(H) EV
- Connection to the Grid at charging facilities
- Secure billing & battery swapping

Manipulation
- Easy access to car network via OBD....
  - Engine tuning
  - Unpaid (optional) feature activation
How serious is this security risk in Automotive?

- Trojan Horse in vehicle via MP3 files
- Car access & manipulation via Tire-Pressure Monitoring
- Network access & replay attacks via OBD Interface
- Control over vehicle through e-call Module
- Bluetooth interface access via mobile phone
- Electrical Vehicle Charge - Grid Manipulations
- “War Texting” – car access via SMS hack
- Car tuning via µC Debug Interfaces
- “Counterfeit auto parts flood China’s aftermarket”
Performance & security requirements

- Performance level:
  - broadcast (TX) up to 20 safety messages per second...
  - receive (RX) N times more messages
    - real-life traffic measurements: ≤ 750/s

- Security level:
  - Secret key material (pseudo-identities) involved in signature generation (TX)
  - Only public key material involved in signature verification (RX)

<table>
<thead>
<tr>
<th>Operation</th>
<th>TX</th>
<th>RX</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rate</td>
<td>Signature generation Low: ≤ 20 / s</td>
<td>Signature verification High: 400-1000 / s</td>
</tr>
<tr>
<td>Security level</td>
<td>High: protection of private keys (=car identity)</td>
<td>Modest: only non-secret data</td>
</tr>
</tbody>
</table>

Hello! sign Hello! Hello! verify
Public key exchange (can be part of message)
ITS Challenge 2: Quality of Service wireless links

- Automotive IEEE 802.11p WiFi
  - 5.9 GHz band reserved
  - **Longer ranges** (up to 1000m)
  - **High (relative) speed of vehicles** (Doppler effects)
  - **Low latency** by
    - No frequency scanning
  - **Robust** under automotive harsh conditions
    - Rapid changes in multi-paths reflections
    - Long excess delays to indoor

- Multi-radio: co-existence and concurrency
  - Multiple-standards, multiple frequency bands world-wide
  - Closely spaced structures like shark-fins
  - Simultaneous transmit and receive
Field trial NL consortium SPITS

„Transparent Truck“

Safety Message Success Rate

- 802.11p WiFi
- Conventional WiFi

Higher is better

90%
ITS Challenge 3: .. Collaborative innovation

Innovation combining in-car data, traffic info and dynamic max. speed to improve traffic flow and road safety and to reduce emissions
Case 2: Smart Energy – Home & Building Automation (HABA)

Distributed electricity generation and storage
- Wind Turbine
- Solar Panel
- Hybrid car
- Light
- Appliances

User Interfaces
- Home displays
  - TV, Computer
- In-Home Energy Display
- Home Energy Box

IP network
- Independent service providers

Wide area network
- Utility Data centers

Concentrator
- Communication hub

Neighborhood network
- Home energy display
- Smart metering & sensing devices
- User Interfaces

Home network
- Smart Elec.
- Smart Heat
- Smart Gas
- Smart Water
- Smart Valve
- Smart Breaks
- Sensors
- Temp control

Smart Home Appliances
- Smart Elec.
M2M nodes in Smart Energy - Homes

Functional view

Potential for smart household nodes
Units (based on ‘conventional’ 2010)

<table>
<thead>
<tr>
<th>Category</th>
<th>Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lighting</td>
<td>70-90</td>
</tr>
<tr>
<td>Consumer Electronics</td>
<td>20-30</td>
</tr>
<tr>
<td>Electricity control</td>
<td>30-40</td>
</tr>
<tr>
<td>Climate control</td>
<td>10-15</td>
</tr>
<tr>
<td>Security</td>
<td>~10</td>
</tr>
<tr>
<td>Other</td>
<td>~10</td>
</tr>
<tr>
<td>Total per household</td>
<td>150-200</td>
</tr>
</tbody>
</table>

Source: industry studies, team estimates, web search
M2M nodes in Smart Energy - Buildings

Functional view

Room sensor (Smoke, CO, alarm, ...)

Window sensor

Activity based lighting

Personalized workspaces

Desk sensor (light, T, RH, presence, CO₂, ...)

Micro-climate
M2M nodes in Smart Energy - Homes

Architecture view

High Bandwidth, High Power, High Cost comms

WiFi (+ Ethernet, BT, USB, PLC)

Narrow Band, Low Power, sensing, secure

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Bridge / dongle

Gateway

Tablet

Smartphone

SmartTV

PC

Security Camera

Electricity/ metering

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)

Lighting/ switches

Connected Appliances/Smart Plugs

Remote

802.15.4 / (+PLC)

Climate control/ sensor networks

Home health

Home monitoring (security, fire)
HABA Challenge 1: Security

- Security risks
  - Cyber attacks
  - Stealing / Fraud
  - Privacy

- All network communication should be in Secure Authenticated Channels (SAC)
  - All messages are integrity and confidentiality protected by use of secure elements
  - All components need to be authenticated and be certified tamper resistant
HABA Challenge 2: Wireless sensor nodes

- HABA system characteristics:
  - Comfort: support level
  - Energy control: critical level
  - Security: lethal level

- Power autonomy
  - Low power (<< 100 μW)
  - Duty-cycled operation

- Reliability
  - 15-20 yrs lifetime with open packages
  - ESD protection for exposed die
  - 12-14b accuracy measurement levels for energy metering

- Radio link
  - ~zero power standby, fast wake-up
  - Interferers avoidance:
    • Time Domain - Listening Before Transmit
    • Frequency Domain - Free Channel Selection
HABA Challenge 3: Collaborative innovation

- Secure Elements
- Wired and wireless connectivity solutions
- Environmental sensors
- Dr. Neuhaus
- Secure energy metering
- Building performance monitoring
- Smart Climate control Systems
- Smart Lighting Control
- Ballast Nedam
- Royal HaskoningDHV
- VolkerWessels
- Schneider Electric
- NUS
- TNO
- TU/e
- PRIVA
- belkin
- TCP
- LEEDARSON

Component & standards → Systems → Smart Buildings
Key messages

- Connected devices are the prime volume drivers for next growth phase of the semiconductor industry
  - Leading application area’s are Smart Mobility and Smart Energy

- The need for data security protection and connectivity reliability scales with the system intelligence level – the robustness of our solutions will determine the speed of market adoption

- The vision of Smart Connected Systems can only be realized by collaborative innovations driven by its value chain partners:
  - M2M Semi + infra & data management + end-user application
Thank you!