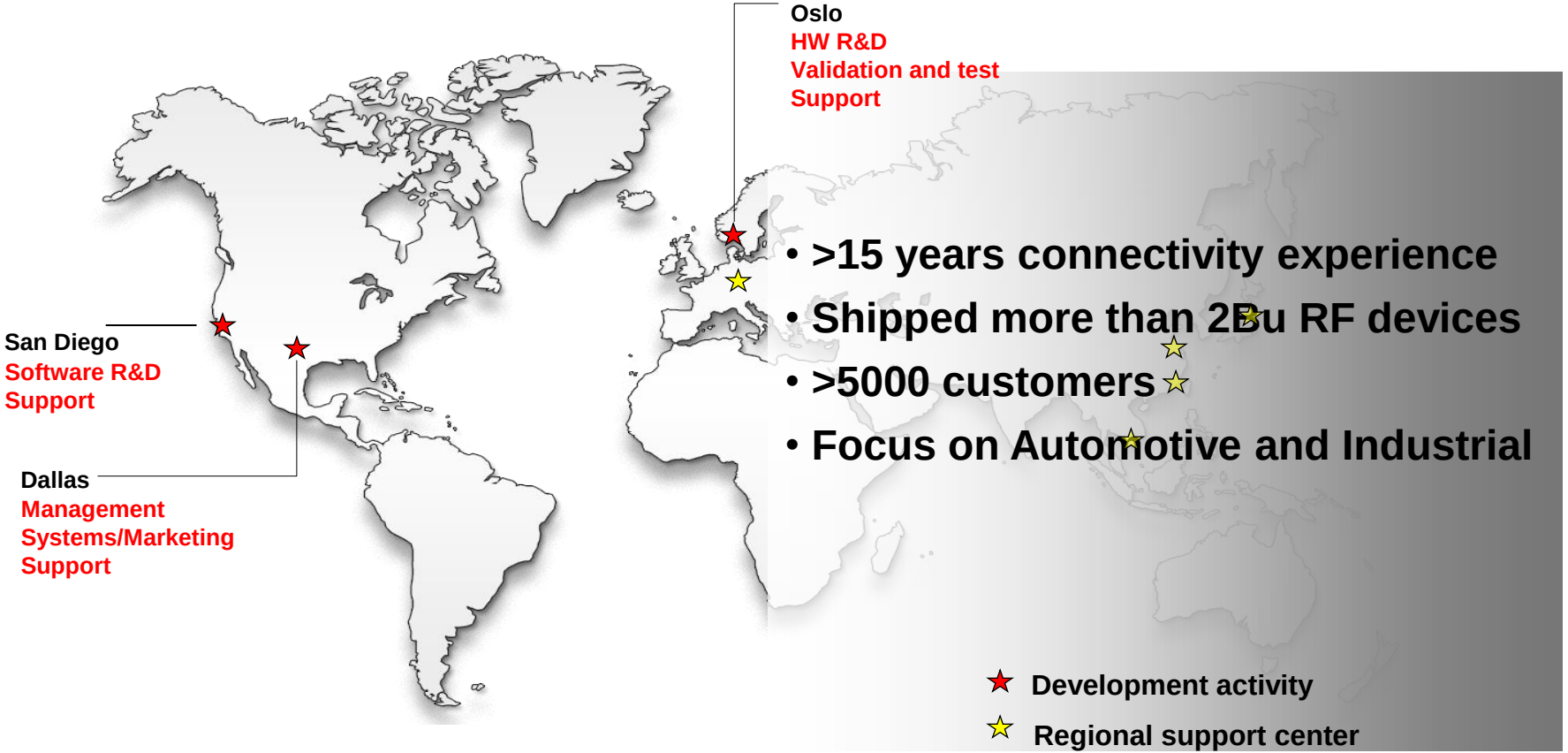
TI BLE for Automotive

Car Access – Relay attack, PEPS, Phone as a Key

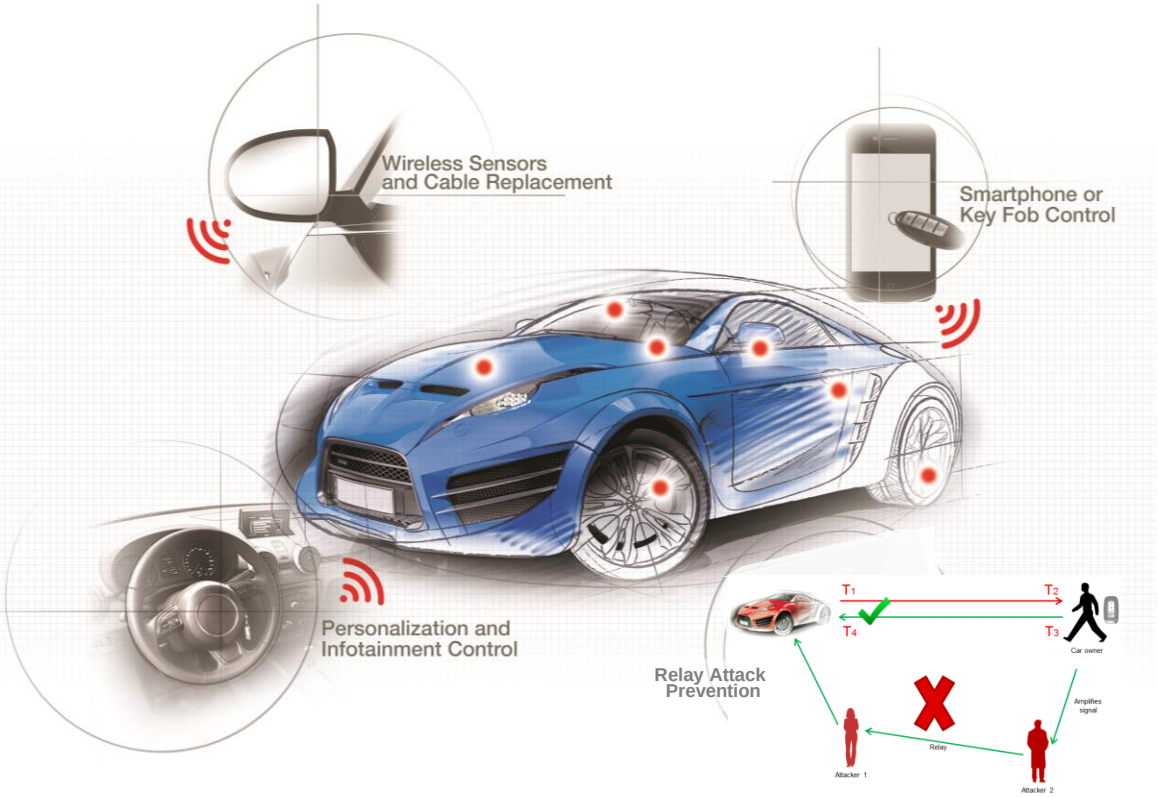
Bluetooth®

Gary Lin
MGTS

Low Power RF WW BLE organization



Why BLE for Automotive Applications?



- **One** system, **multiple** use cases
  - Phone as Key
  - PEPS, RKE
  - Relay Attack Prevention for PEPs
  - Cable Replacement
- Interoperability with smartphones and wearables (smart watch)
- Low power for long battery life and small size on car module
- Enables a cost effective solution for many emerging applications

Security Features for Bluetooth

- Strong encryption
  - Securely encrypting data transmitted between two devices is done by sharing a secret key of up to 128 bits using Advanced Encryption Standard (AES) in CCM mode.
- Secure key exchange:
  - In Bluetooth 4.2 Elliptic Curve Diffie-Hellman (ECDH) key agreement protocol was introduced with the LE Secure Connections pairing feature. ECDH allows two new parties to establish a secret key known to them only without sharing it over the air
- BLE Advertisements Privacy
  - To avoid scanning devices from tracking an advertiser Bluetooth peripherals regularly change their BD address used. This address can be resolved with identity resolving key (IRK) shared via an encrypted connected
- More Information SimpleLink™ BLE Security white paper: SWPB016

Why TI BLE for Automotive?

Portfolio

- Lowest power consumption
- BT5 ready – long range
- Wettable flanks package
- Grade 2 temp (105C)
- 4. generation connectivity

Innovation

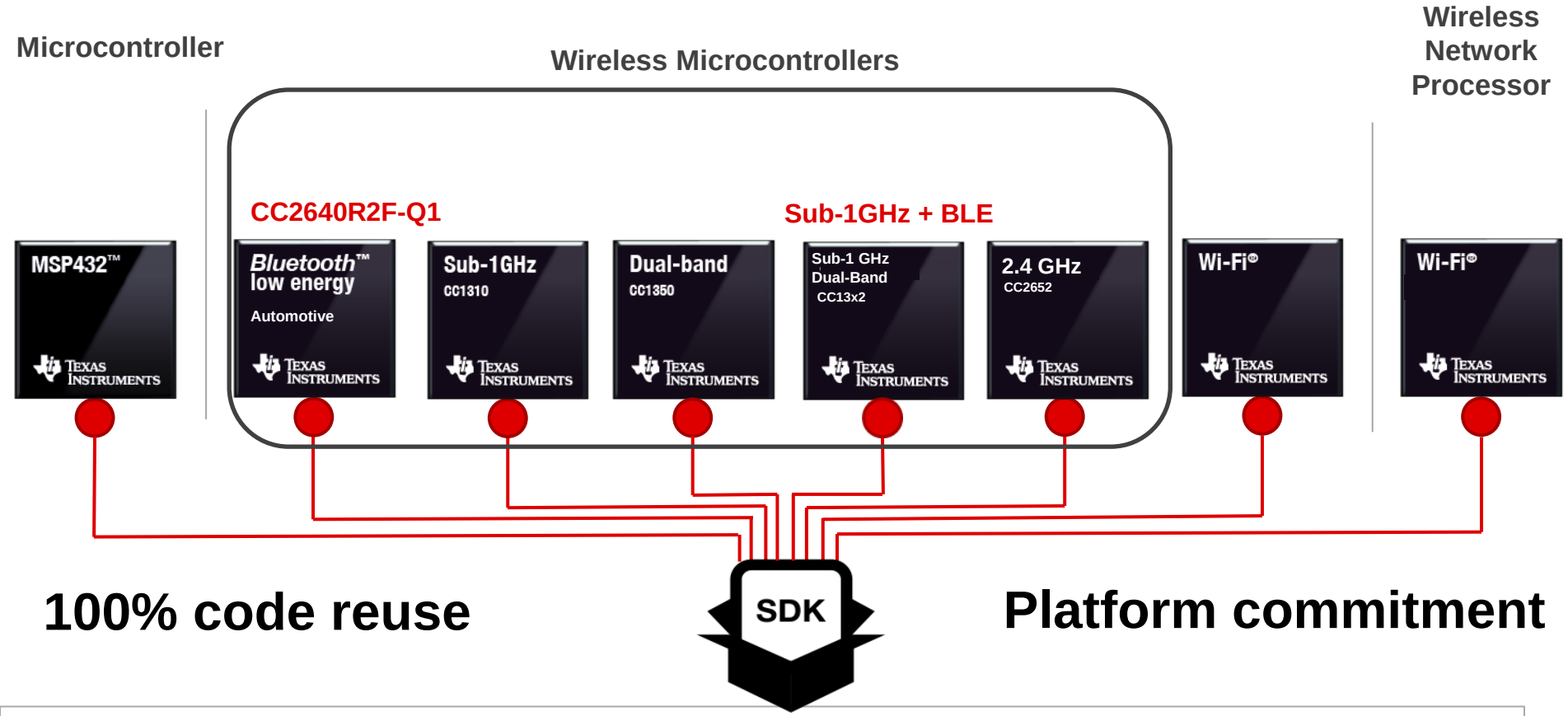
- SW defined radio - flexible future proof architecture
- First with BLE, First with BT5.0
- Real-time Locationing System (RTLS) platform
  1. RSSI w/ connection monitor
  2. Angle of Arrival (AoA)
  3. Time of Flight (ToF)
- Phone as a key (PaaK) using Angle of Arrival

Commitment

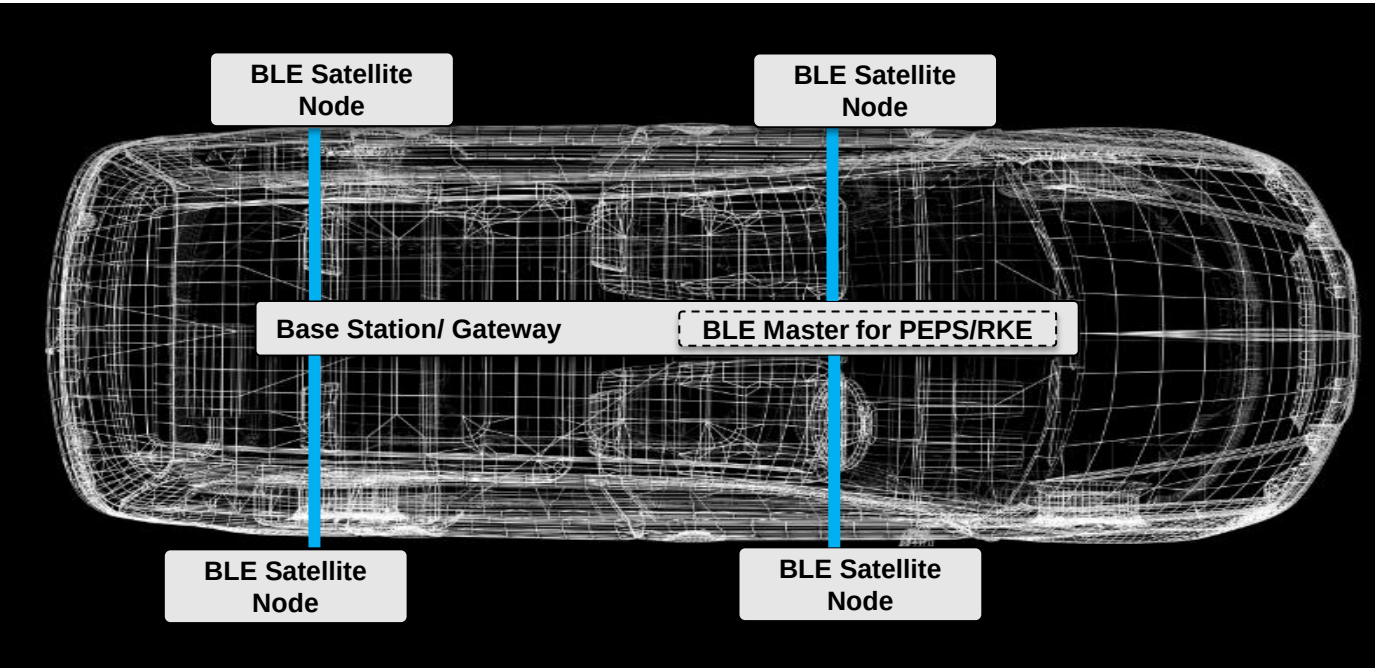
- 8 years BLE experience
- Most robust BLE SW
- Quality and reliability – going beyond AEC-Q100
- Superior customer support

Long Term Investment in SimpleLink wireless platform for Automotive

SimpleLink™ MCU platform Industrial/Automotive



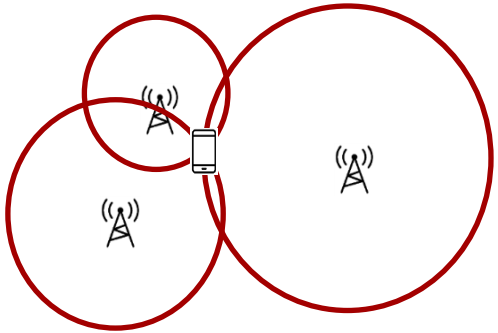
System Overview of BLE in Automotive



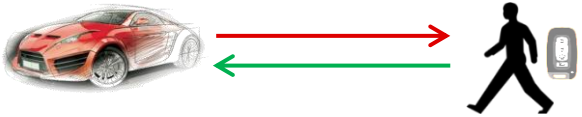
- BLE to enable Relay Attack Prevention, PEPS, PaaK
- 4+ nodes gives better robustness and accuracy
- TI provides a localization solution
  - RSSI with Connection Monitor
  - Angle of Arrival
  - Time of Flight

Real Time Locationing System (RTLS)
TI's solution for Localization

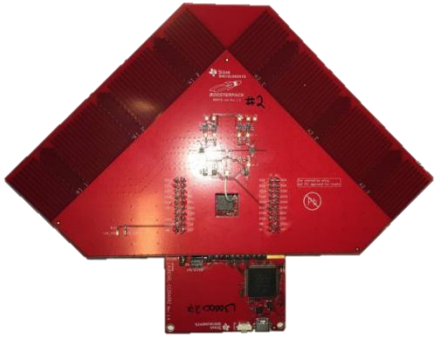
RSSI with Connection Monitor



Time of Flight (ToF)



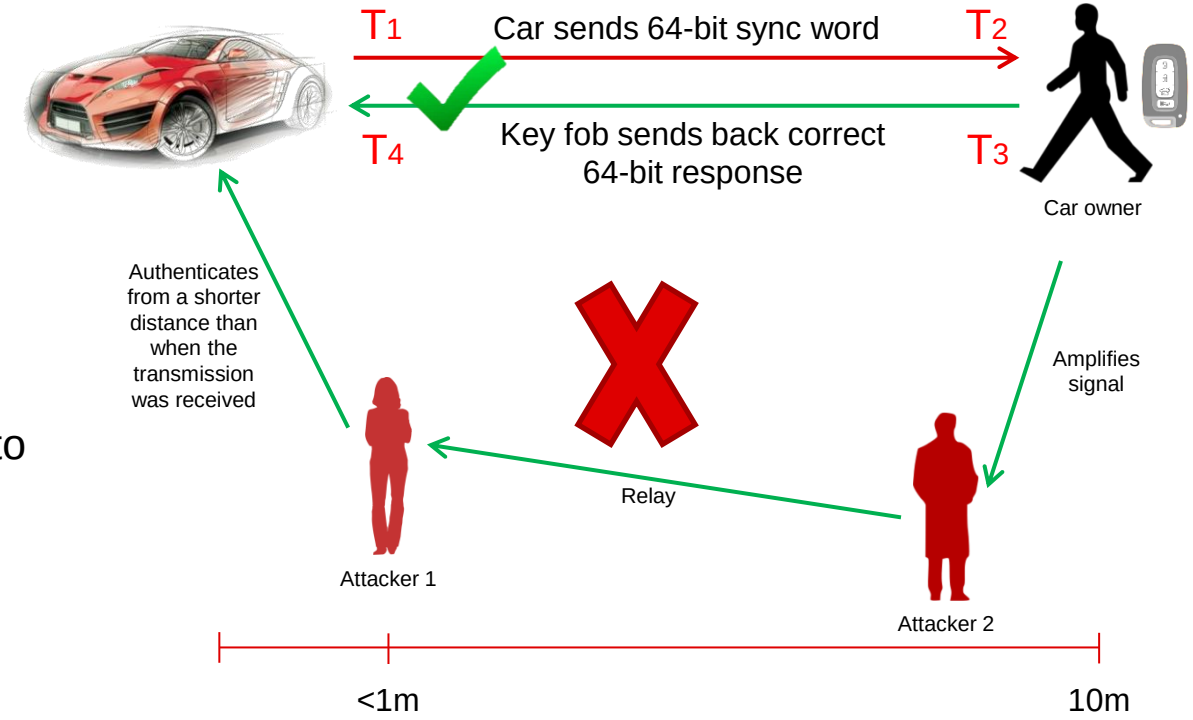
Angle of Arrival (AoA)



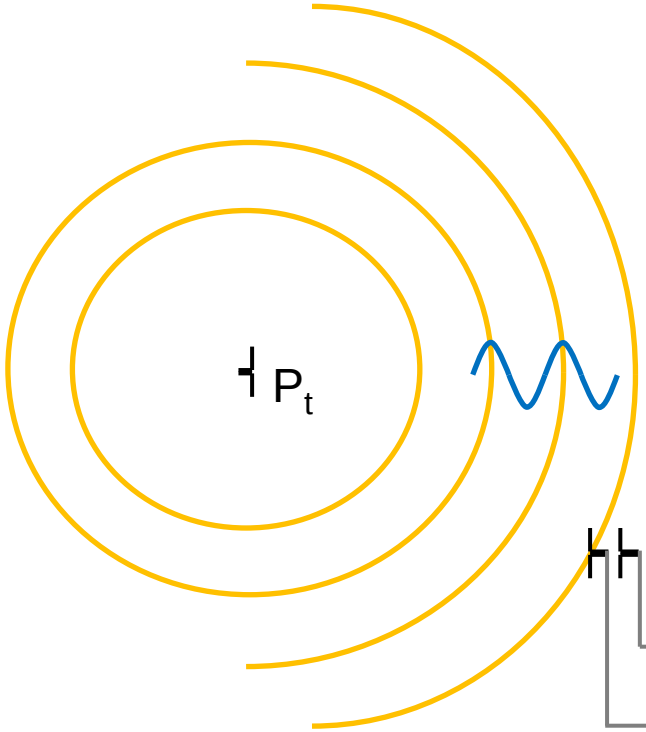
Relay Attack Prevention: Time-of-Flight (ToF)

- Provides “relay attack” protection in BLE-based key fobs

- Features
  - Ranging with <2m accuracy
  - Custom packets exchanged between devices
  - “Secure distance bounding scheme can be implemented to detect relayed signals
  - Turnaround time for key fob

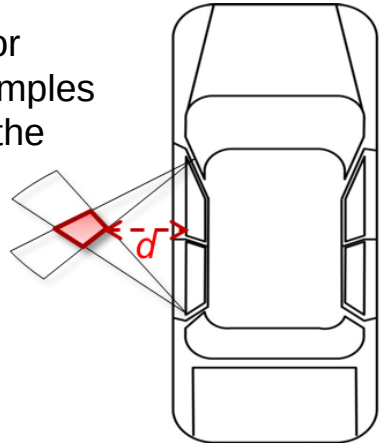


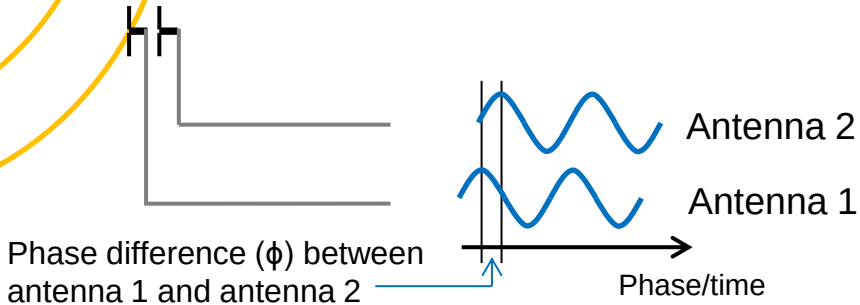
Localization: Angle of Arrival (AoA)



When two antennas are placed at a given distance apart from each other, their received RF signals will have a phase difference that is proportional to the difference between their respective distances from the transmitter.

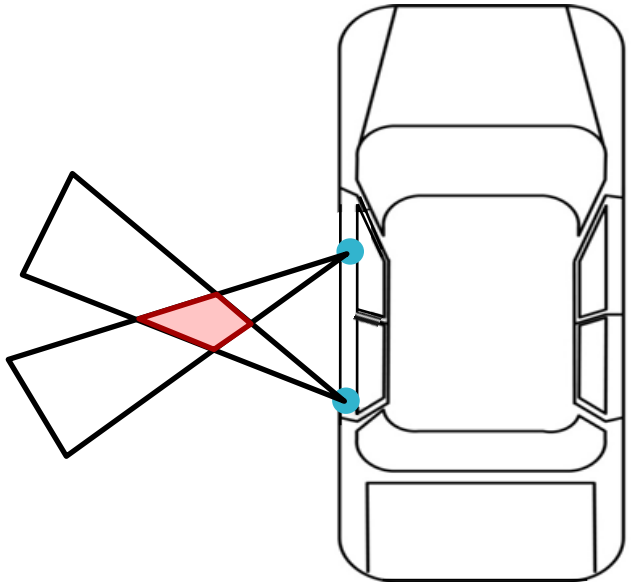
The CC2640R2F-Q1 can utilize its superior flexibility to capture and store I- and Q samples from the incoming RF packets to analyze the phase of the incoming RF carrier wave



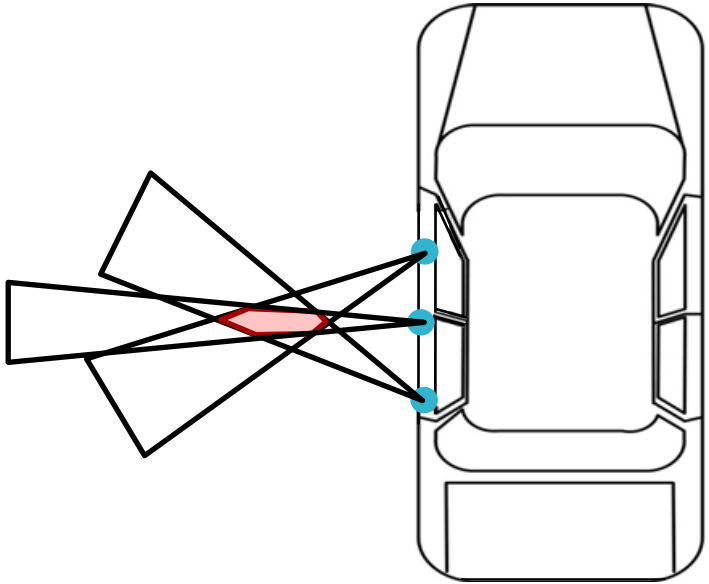


Localization: AoA with Multiple Nodes

Two BLE Nodes



Three BLE Nodes



Adding additional BLE nodes enable:

- Robustness
- More accuracy
- Use existing Smartphones

(coverage example)

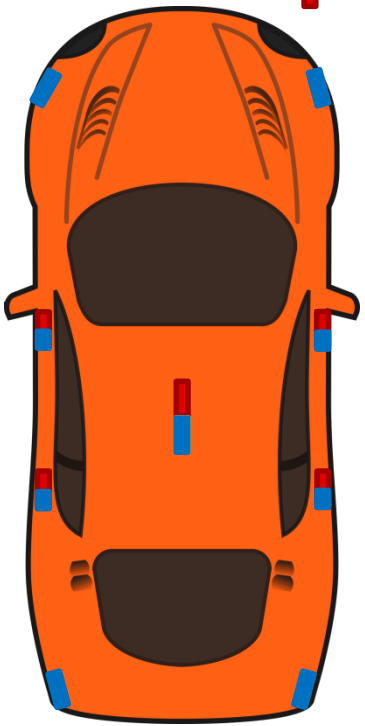
Extending today's car access system

LF + UHF

LF + BLE + UHF

LF + BLE + UHF

BLE + LF(optional)



LF LF + BLE BLE UHF Unsecure Secure

Today:
Key fob position determined by LF, response by UHF

PEPS Relay Attack protection:
TI BLE with ToF solution added for relay attack protection (CC2640R2F-Q1 added)

Phone as a key without HW changes:
BLE used for Smart Phone connectivity

Add Angle of Arrival antennas:
BLE used to locate Smart Phone and key fob

CC2640R2F-Q1 Automotive Wireless MCU

http://www.ti.com/product/cc2640r2f-q1

Features and Benefits

- **AEC-Q100 automotive qualified**
- **Most integrated wireless MCU –** Design versatility and single-chip SoC
- **Lowest power consumption** - ~6mA radio RX/TX and low sleep current for increased battery life
- **Longest range –** 101 dB link budget for increased range and reliability
- **Grade 2 Temperature Rating (-40°C to +105°C)** – Use in areas where elevated temperatures are common
- **Wettable flanks package –** Enables faster and lower cost production line inspection

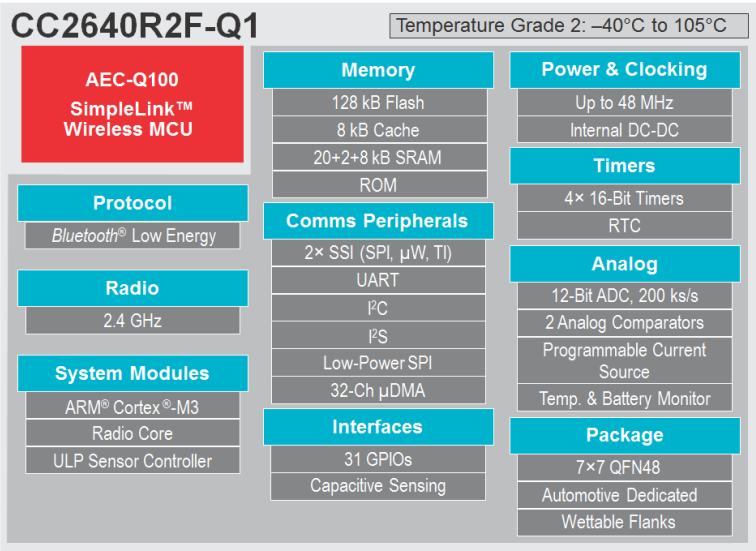
Software and Tools

- **Software Development Kit, including royalty free Stack**
- **BT v4.2 support with qualified Adopted Profiles (BLE 3.x)**
- **SmartRF Studio & TI iOS/Android Multitool**
- **Sensor Controller Studio**

Hardware Development Kits

CC2650 SensorTag

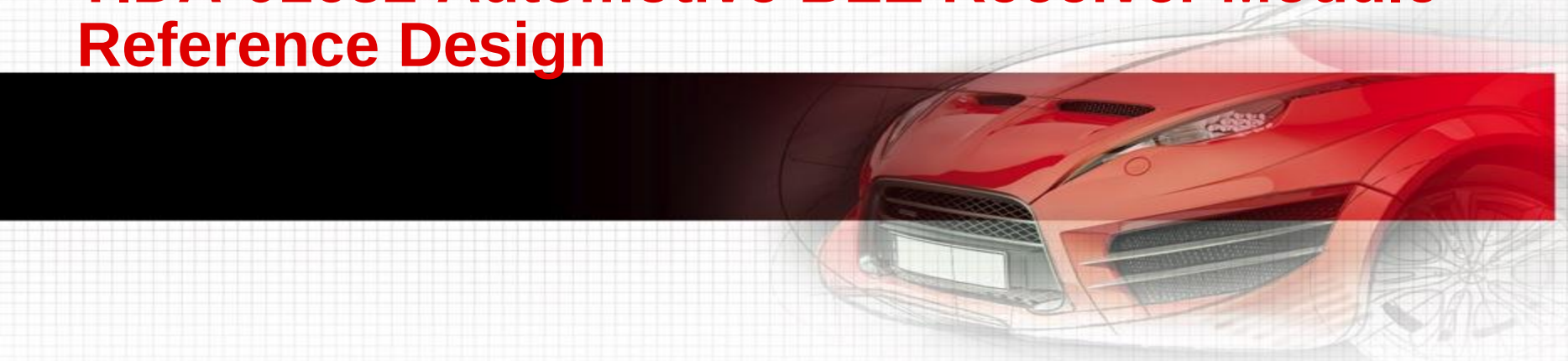
CC2640R2F LaunchPad



Example Applications

- **Car Access (RKE, PKE, PEPS)**
- **Car sharing**
- **Piloted parking**
- **Cable replacement and remote control**
- **Proximity sensing**
- **Interior lighting control**
- **Wireless On-Board Diagnostics**
- **Power seats with memory**

TIDA-01632 Automotive BLE Receiver Module Reference Design



TIDA-01632 Automotive BLE PEPS Satellite Node Reference Design

Design Features

Single master module & multi-slave modules that communicate via LIN:

- Master Module:
  - Usually located in BCM, Gateway, or Telematics Module
  - LIN Master + Wide VIN 3.3V LDO + BLE MCU master
  - Master module connects to phone & shares connection info
- Satellite (Slave) Module:
  - Multiple slave modules to detect RSSI and Angle or Arrival
  - RF MUX for switching between 2 co-linear PCB antennas
  - LIN Slave + Wide VIN LDO + BLE MCU
  - Slaves monitor BLE communication without connecting to phone

Applications

Car Access Passive Entry Passive Start (PEPS) Systems

Design Benefits

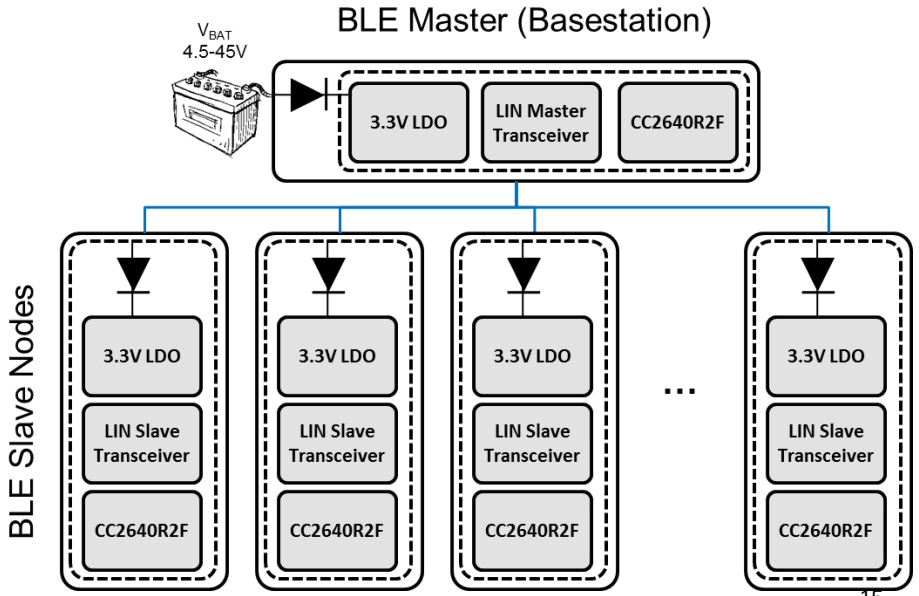
- Able to survive load dump voltages up to 45V
- Able to handle input voltages down to 4.5V
- Low power sleep mode with wake over LIN: < 25µA @ 14 V Supply
- Able to sense three proximity ranges
  - Driver approaching – where puddle & interior lights turn on
  - Driver within 2 meters – typically when doors unlock
  - Driver and phone inside car – driver able to turn on car

Tools & Resources

- **TIDA-01632 Tools Folder**
- **Design Guide**
- **Design Files:** SCH, BOM, Gerbers
- **BEL > Security Systems > PEPS**

Device Datasheets:

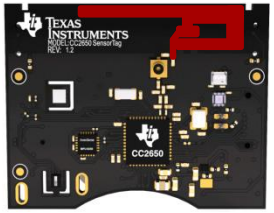
- CC2640R2F-Q1
- TLIN1029-Q1
- TPS7B82-Q1

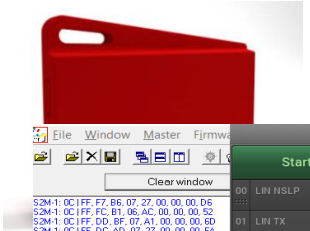


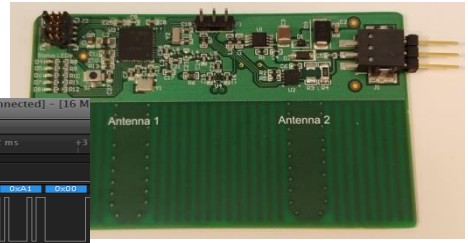
TIDA-01632 Demo

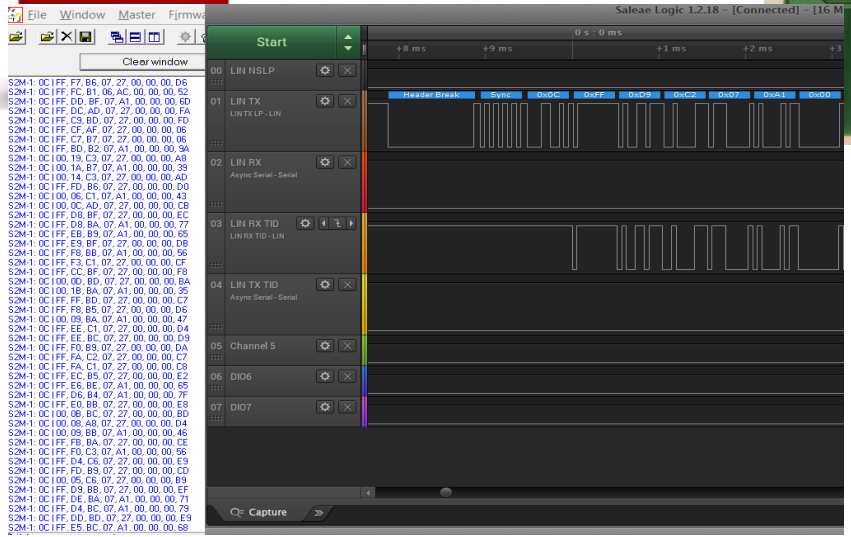
SensorTag – “Key Fob with CC2640R2F”

TIDA-01632 E1









Sharing Data via LIN

Key Takeaways

- **Why BLE in Automotive**
  - Low cost, low power smartphone connectivity
  - BLE can solve Relay Attack
  - One system, multiple use cases (Relay Attack Prevention, Phone as Key, PEPS, RKE, Cable Replacement)
- **Why TI BLE**
  - Long term Experience and Commitment to SimpleLink Automotive platform
  - TI Automotive quality, including ASPICE compliance software
  - Software Innovation (BT5 Long Range, ToF, AoA and more coming)
- **Resources**
  - AoA demo video
  - RTLS SimpleLink Academy Training

Q&A