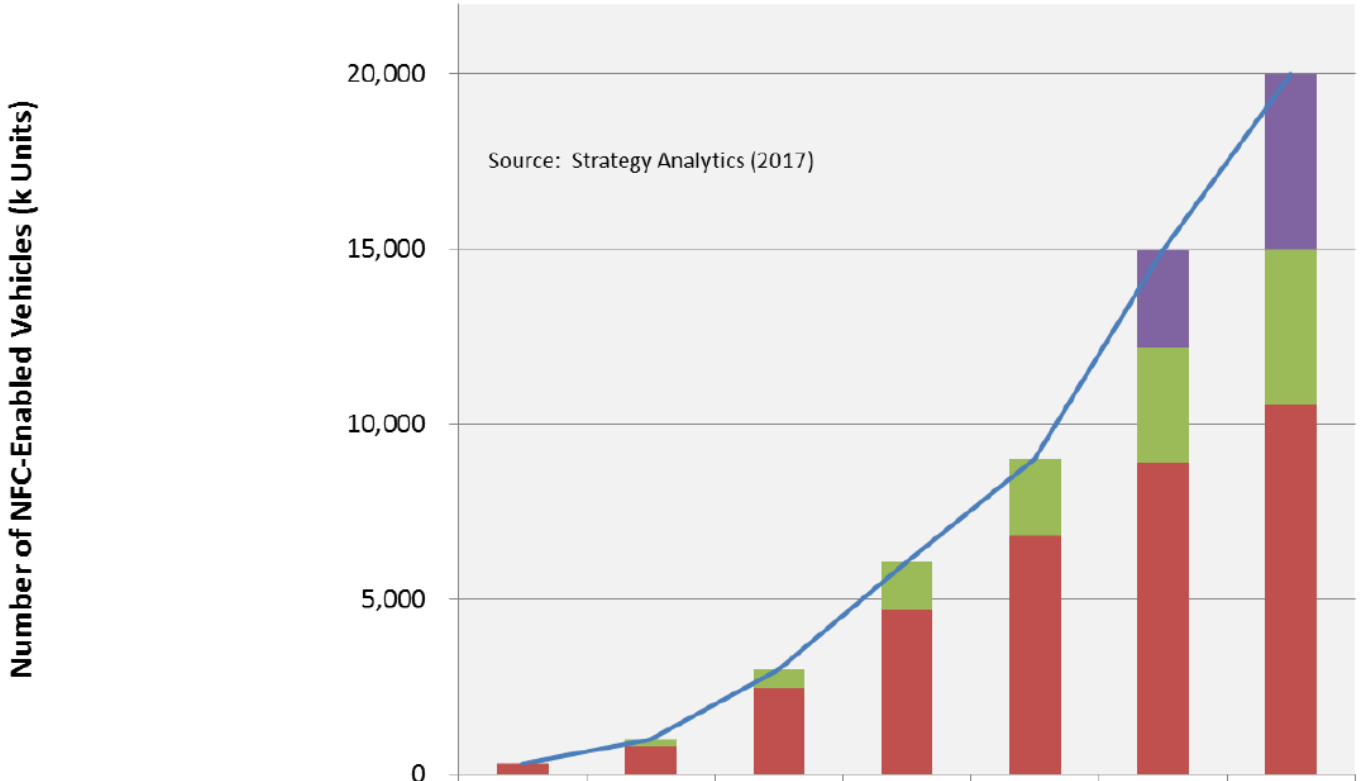
NFC in Automotive

Rock Feng
ST MMY Technical Marketing
Dec 2019

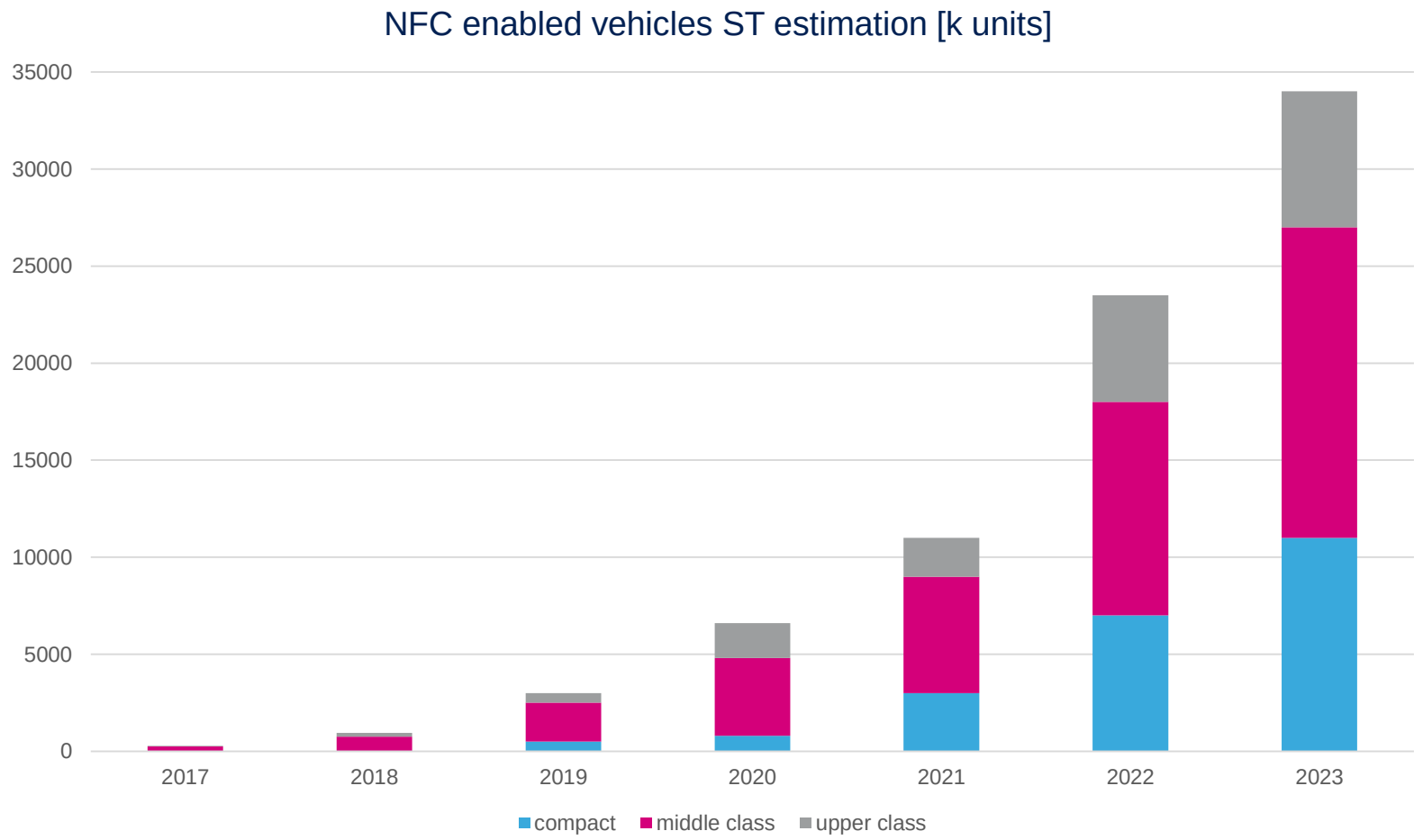
life.augmented

NFC Automotive Market Analysts



	2017	2018	2019	2020	2021	2022	2023
Non-Premium Compacts	0	0	0	0	0	2,760	5,000
Non-Premium Mid/SUV Segment	0	209	533	1,373	2,184	3,295	4,443
Premium Sector	300	791	2,467	4,677	6,816	8,895	10,557
Total	300	1,000	3,000	6,050	9,000	14,950	20,000

NFC Automotive Market ST Estimates



x2 for middle console & door

Cars with NFC Doorlock

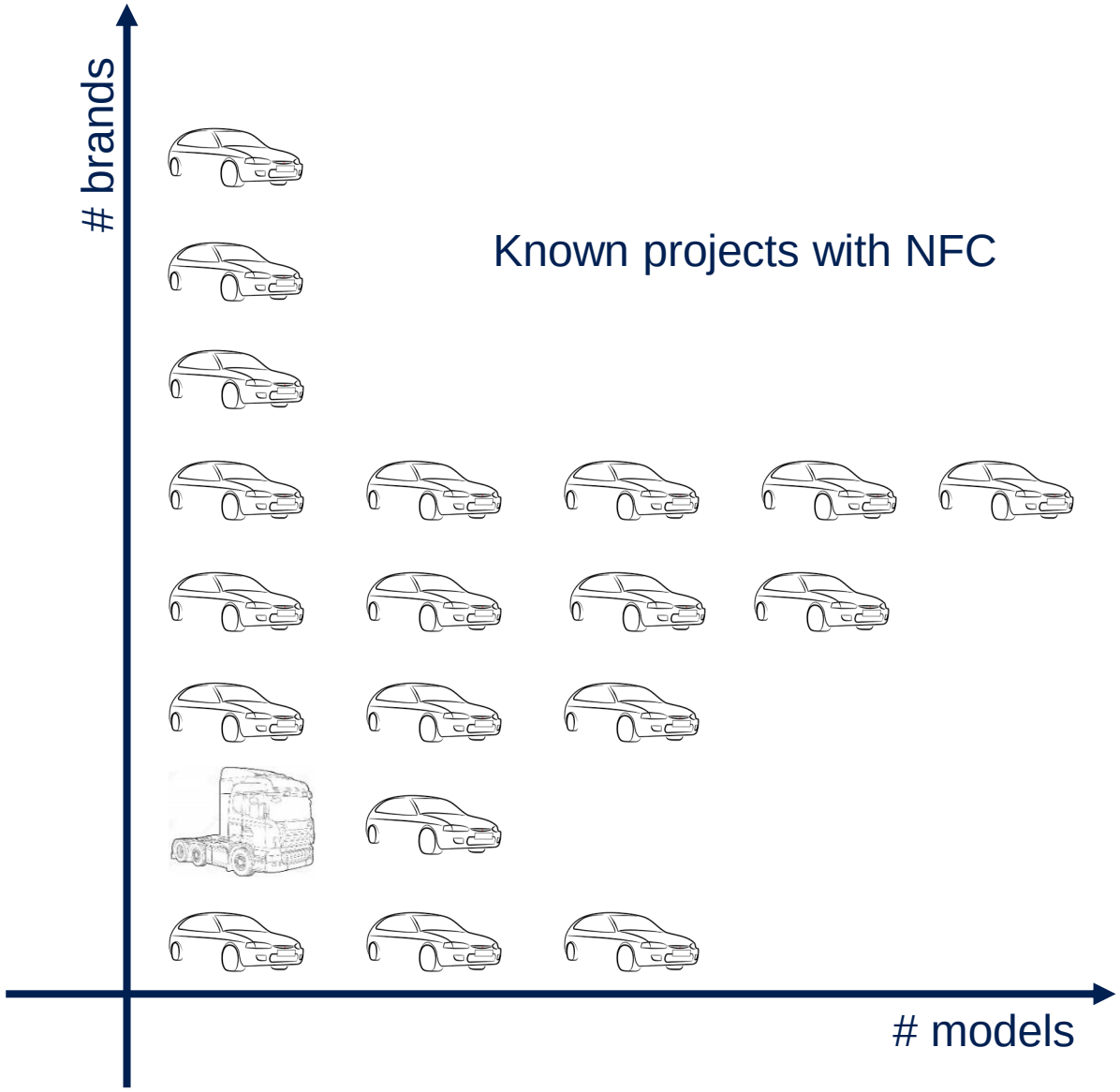
Audi A8

Tesla Model 3

BMW Drive Now

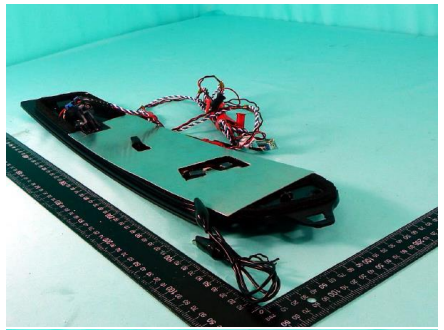
Mercedes e-class

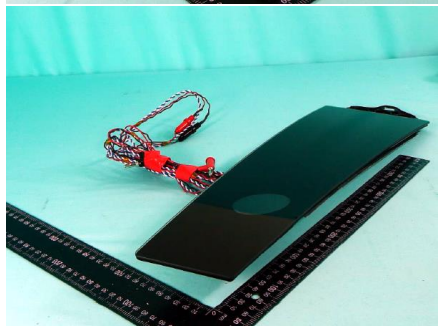
Cars on the market with NFC

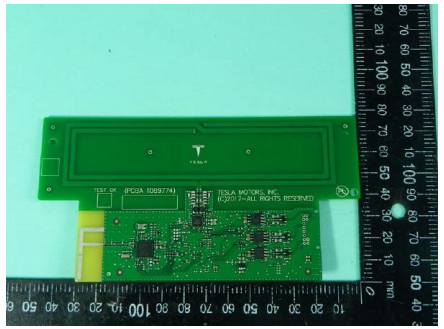


life.augmented

From FCC







Audi connect Schlüssel

Mit dem Audi connect Schlüssel digitalisiert Audi den herkömmlichen Fahrzeugschlüssel und transferiert ihn in das Smartphone. Das mobile Gerät dient zum Öffnen, Schließen und Starten des Autos. Die Kommunikation zwischen Fahrzeug und Smartphone erfolgt per Near Field Communication (NFC). Diese Technologie bezeichnet einen Standard, bei dem Daten über kurze Strecken per Funk übertragen werden. Zum Entriegeln des Autos hält der Fahrer das Smartphone nah vor den Griff der Fahrertür, der eine NFC-Antenne birgt. Zum Motorstart legt er es in die Audi phone box, die ebenfalls mit einer NFC-Antenne ausgestattet ist.

Die hochsensiblen Daten des digitalen Schlüssels müssen im Smartphone gegen Auslesen, Duplikation und Manipulation geschützt sein. Dafür wird der Audi connect Schlüssel in einer sicheren Speicher- und Ausführungsumgebung im Smartphone, entweder auf der SIM-Karte oder unmittelbar im Gerät, abgelegt. Dieses sogenannte Secure Element ist direkt per Single Wire Protocol (SWP) an die NFC-Antenne angebunden – ein weiterer Sicherheitsvorteil, da das Betriebssystem des Smartphones nicht in die Kommunikation zwischen Auto und Smartphone eingebunden ist.

Kunden können zukünftig over-the-Air bis zu 15 Schlüssel weitergeben, etwa an Familienmitglieder, Freunde oder Kollegen. Das Auto erkennt den Besitzer schon beim Öffnen und lädt verschiedenste Einstellungen aus seinem individuellen Profil – von der Sitzposition über die Klimatisierung bis zur Navigation. Die 1:1-Beziehung zwischen Schlüssel und Fahrzeug löst sich ebenfalls auf, da das Smartphone die Schlüssel für mehrere Fahrzeuge vorhalten kann. Für Situationen, in denen der Fahrer den Audi connect Schlüssel kurzfristig weitergeben muss, das Smartphone aber nicht aus der Hand geben will, liegt die Audi connect Schlüsselkarte im Scheckkartenformat im Auto bereit. Sie kann vom Fahrer aktiviert und zum Beispiel beim Valet Parking oder im Pannenfall weitergegeben werden.

Der Audi connect Schlüssel ist jederzeit einsatzbereit, selbst wenn der Akku des Smartphones leer sein sollte (abhängig vom jeweiligen Modell), weil der NFC-Chip die benötigte Energie vom elektromagnetischen Feld der Gegenstelle bezieht.

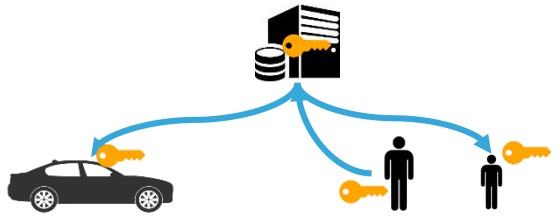
Automotive NFC Key Drivers

Keyless GO hacked

Keyless GO systems are not secure anymore.
Industry considers NFC as a safe replacement.

Key Managment solved

E-call (a safty feature) 3G/LTE uplink mandatory for all cars starting 2018.



Key cost reduction

A NFC Keycard with cryptography costs <<1$
A Keyfob replacement costs 120~800$
=> considerable cost reduction also for initial production costs on both car & key side.

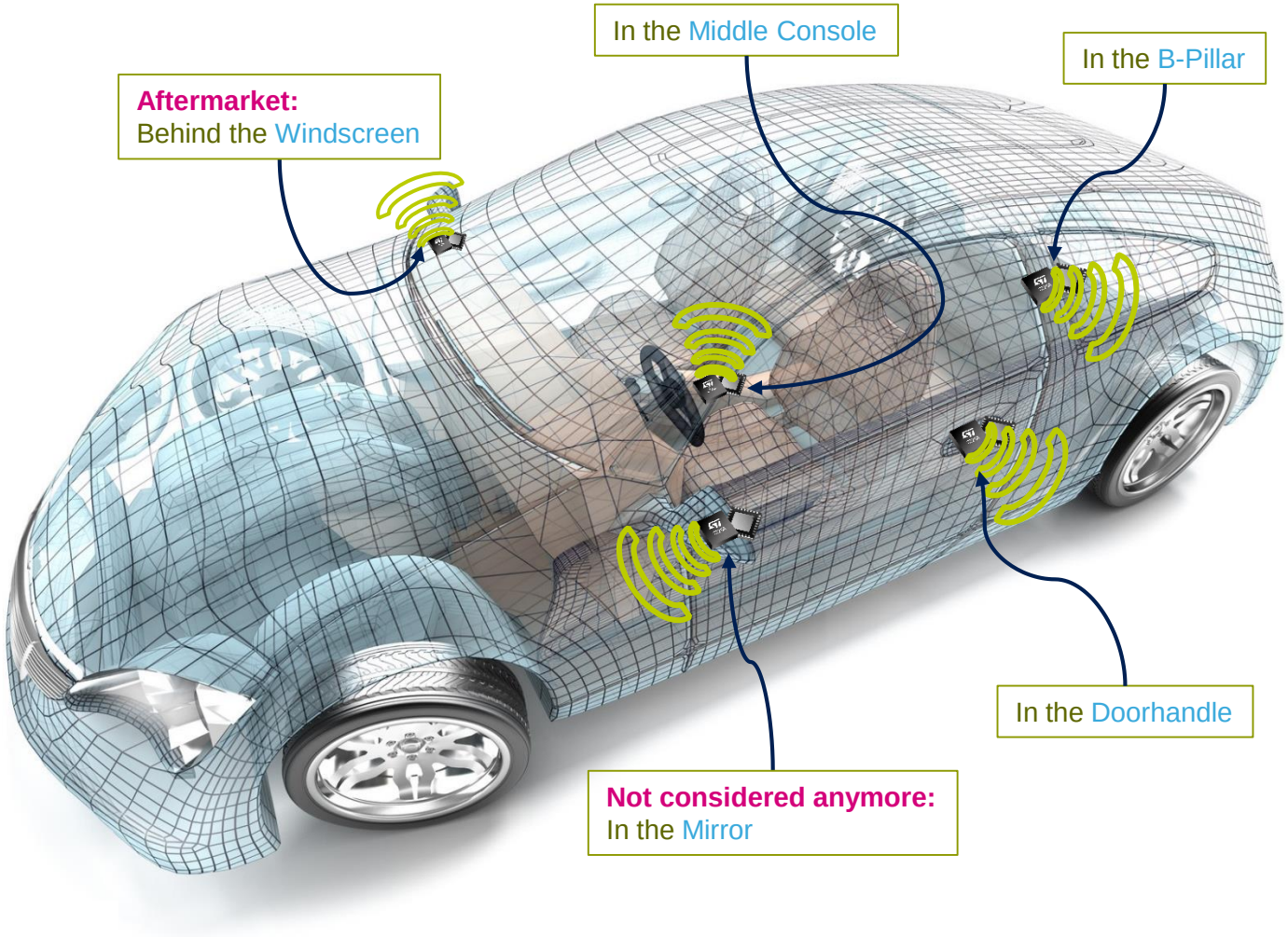
TESLA Model 3 + iPhone Wallet

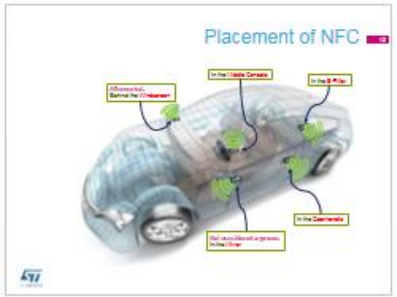
TESLA seems to have the same effect on the automotive market like APPLE had on the phone market.

Full ST Solution

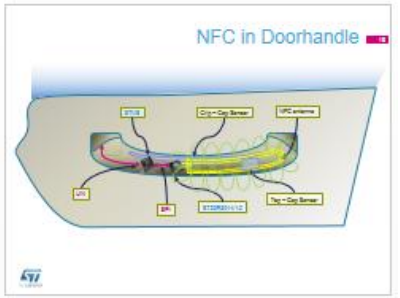
Full ST Solution

Automotive Applications

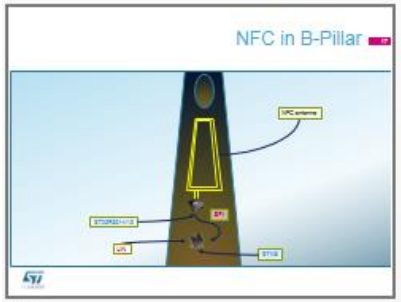




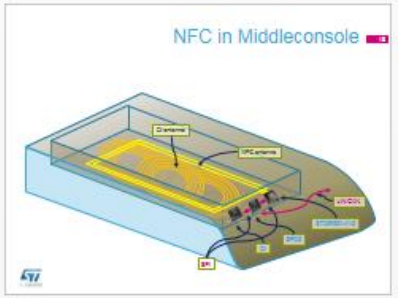
15



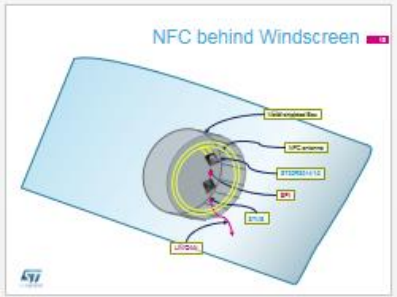
16



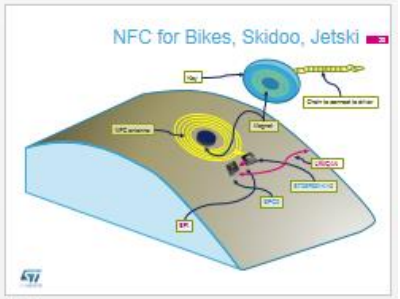
17



18



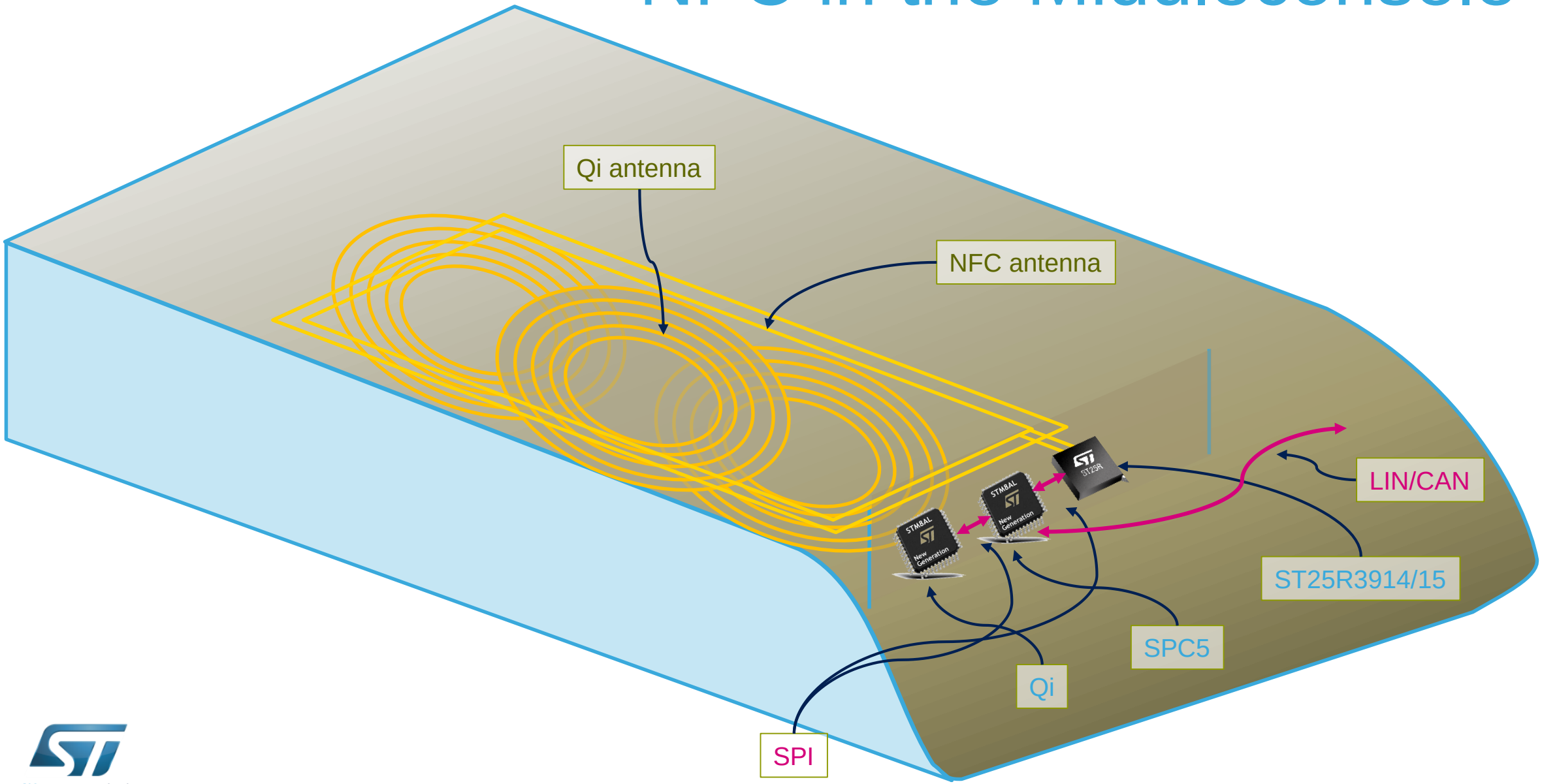
19



20

life.augmented

NFC in the Middleconsole

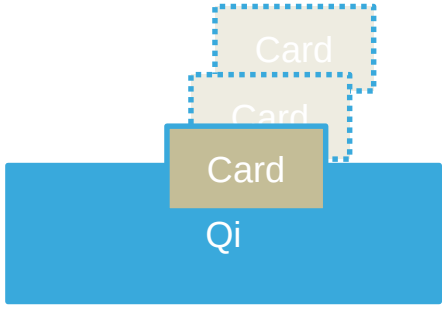


life.augmented

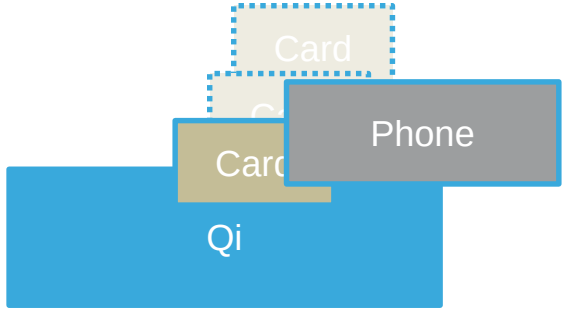
Requirements for NFC Card Protection

Protect cards against damage by Qi charger

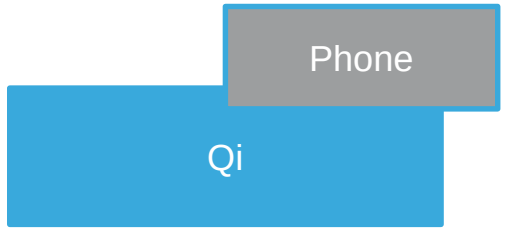
Usecase 1:
One or more Card(s):
Do not Charge



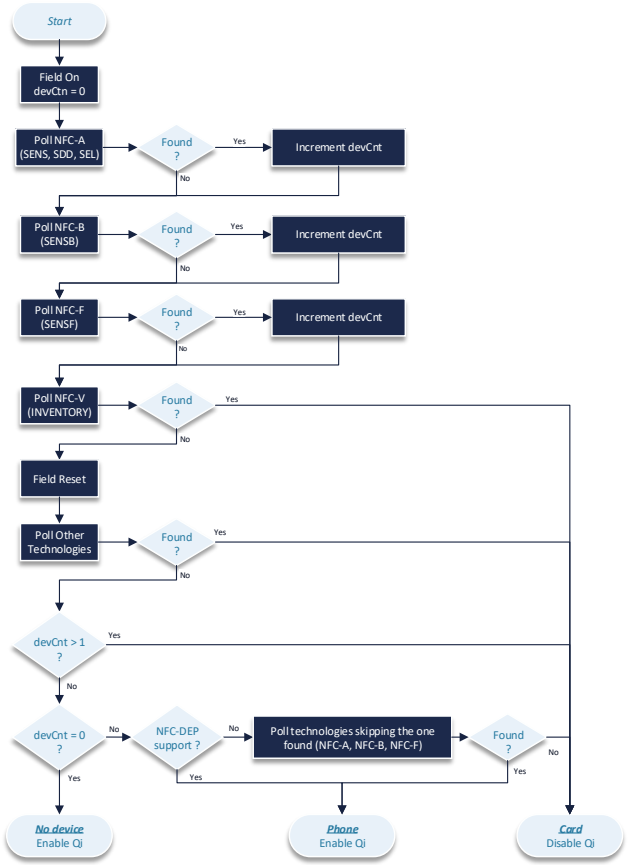
Usecase 2:
One or more Card(s) + Phone
Do not Charge



Usecase 3:
Phone:
Charge



NFC for Qi Protection Algorithm



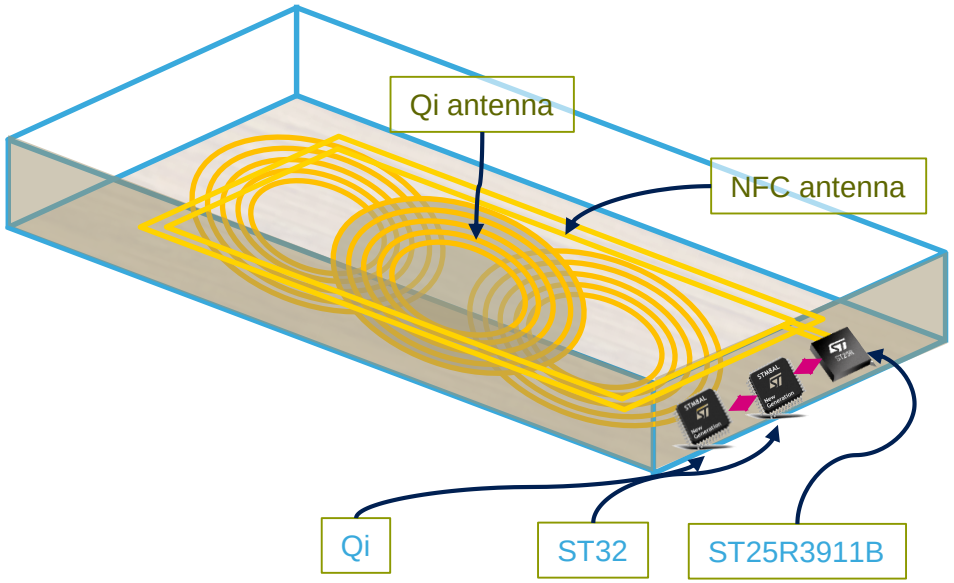
ST offers a sophisticated Algorithm to detect a card inside the charging field.

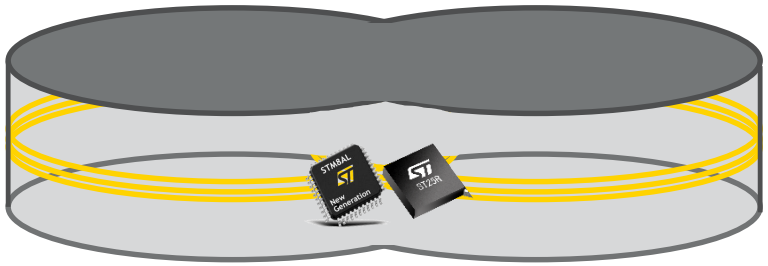
Device(s)	Qi Charger
None	Enabled
Phone(s) (NFC Off)	Enabled
Phone (NFC On)	Enabled
Phone(s) in CE mode only	Enabled*
Several Phones (NFC On)	Disabled
Card	Disabled
Several Cards	Disabled
Phone(s) + Card(s)	Disabled

* If the phone device employs card emulation in multiple technologies

life.augmented

NFC for Qi





Benefits:

- Automatic antenna tuning
  - Compensates for metal environment, eg. Coins placed on the charger, or charger placed on metal table.
  - Compensates for build variances, placement of the NFC antenna.
- High output power
  - Enough margin to offer a good user experience also in combination with Qi charging and other antennas offering a very robust system.

Usecase:

- Protection of NFC cards (eg. Credit card) from Qi field.
- Secure Wifi/BT Pairing
- Data transfer, configuration of Qi charger.

life.augmented

Requirements

Large operating volume

A approaching NFC card must be detected before entering the Qi charging field. The bigger the volume of the NFC field the greater the area of protection.

ST25R offers highest output power combined with automatic antenna tuning.

Short reaction time and good singulation of cards

The entry function continuously checks for cards. The time window for detection must be low to ensure best protection.

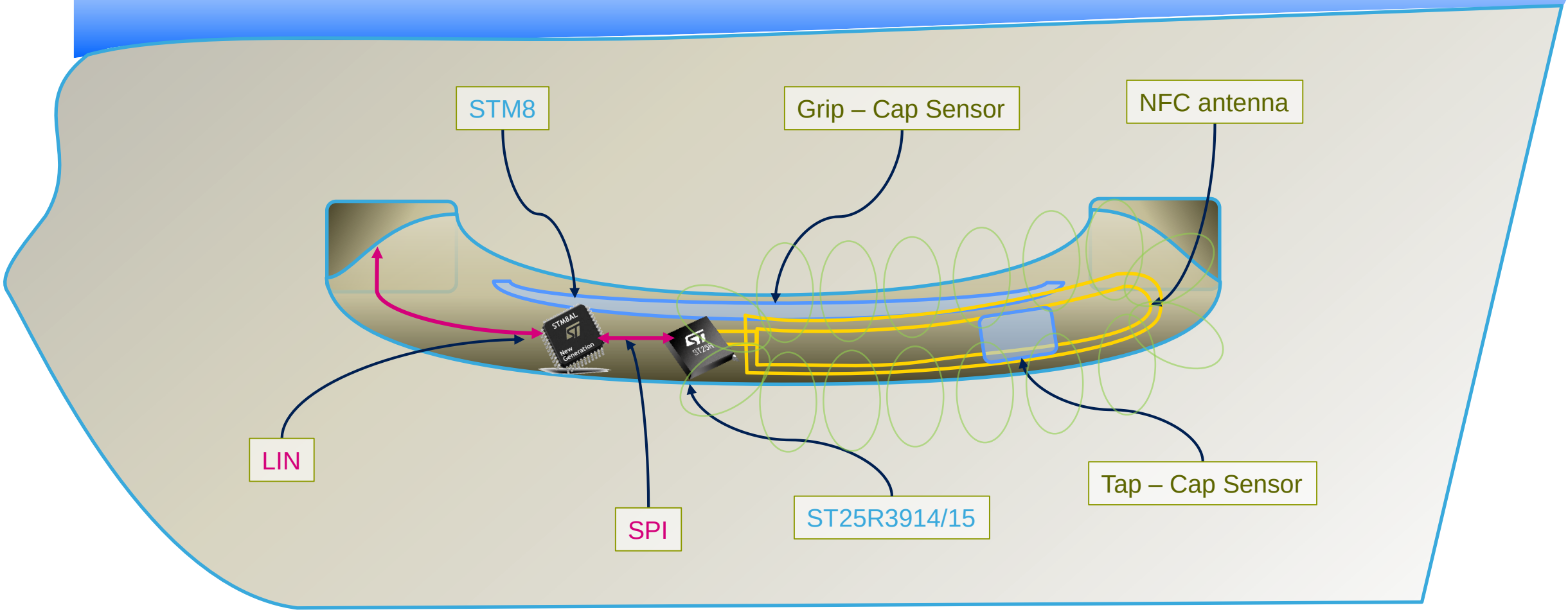
A card together with a phone should be detected.

Interoperability

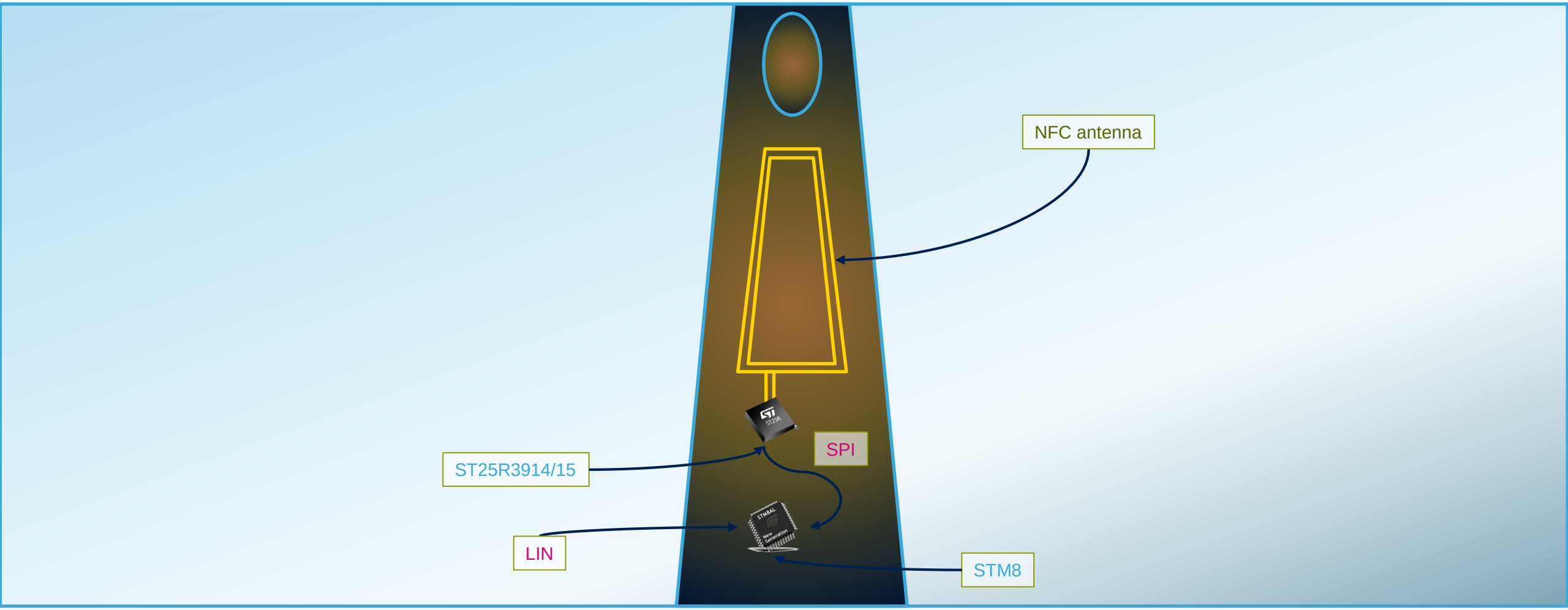
NFC communication should work while charging to detect also incoming cards. No retries or different placement required.

ST25R offers excellent compatibility with NFC devices and offers robust TX & RX to continue NFC detection while charging.

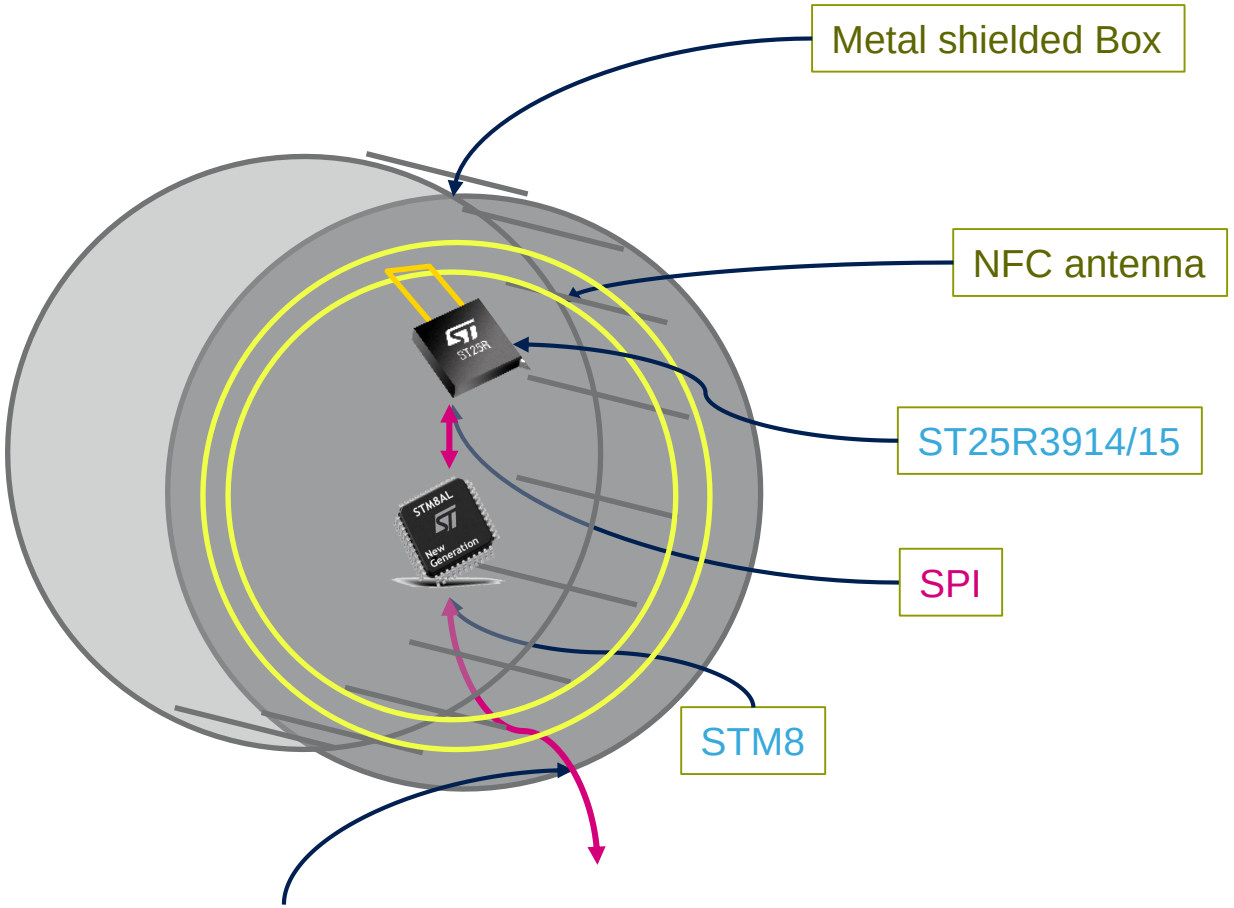
NFC in Doorhandle



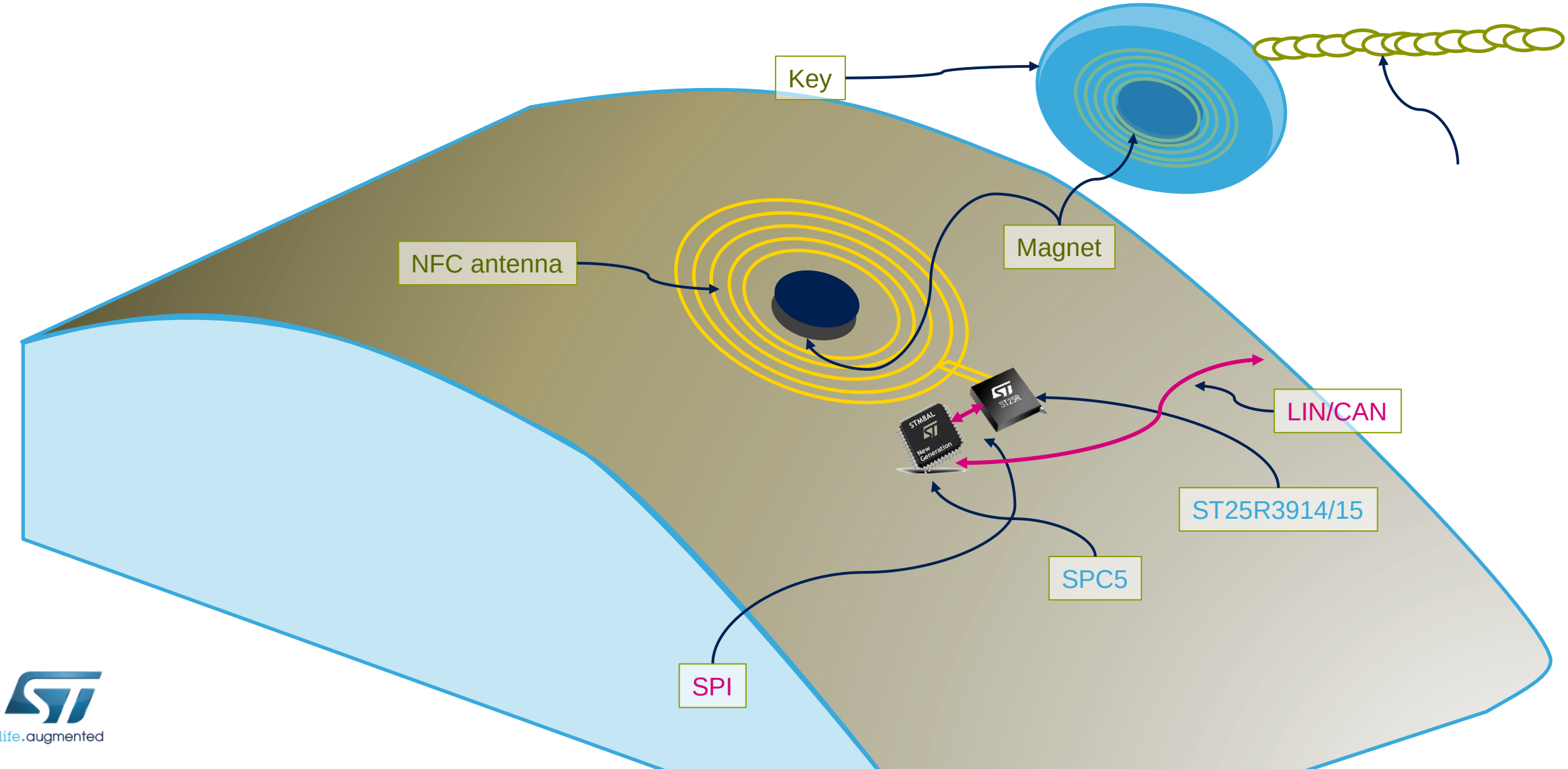
NFC in B-Pillar



NFC Behind Windscreen



NFC for Bikes, Skidoo, Jetski



life.augmented

NFC for Automotive

Car access & start

Convenient access to the car, start and distribution of keys online to a NFC enabled phone

Personal Settings & secure pairing

Just sit in, and the entire cockpit will fit the driver wish
Your NFC phone will take care of secure pairing!

Diagnostics

No physical connection is anymore required for car diagnostics, which helps on safety

life.augmented

Use Case I/II

Car rental, fleets, sharing

- In car payment (eg. Rental, or electric charge)
- No waiting to get or drop the key
- Cheap replacement for lost keys
- Drop car anywhere (there is no physical key, or a cheap one)
- Book the car on-the-go by touching it with card/phone
- Check for the driver license/ Passport
- User settings stored
- Easy extension of a rental period
- Disabling the key remotely
- NFC for secure BT/Wifi pairing (eg. Everyday the key is changed)
- Car can be adjusted to customer request, eg =>
  - Navigation yes/no
  - Change of horsepower

Use Case II/II

Home/family, Industrial use

- In Car payment for electric charge
- Set time limits for driving
- Cheap key replacement
- Disabling the key remotely
- Share keys with friends, family
- Identify with ID card or license
- User settings stored
- Use cheap & time limited NFC key for eg. Valet parking

- BT pairing via NFC
- Push/Pull GPS coordinates
- Configuration in post-production
- Diagnostic and statistics

Automotive Requirements

Large operating volume

Door handles are in metal environment and allow space for small antennas only; There is a influence of metalized windscreens if placed behind those.

Coins, pencil and other metallic objects as well as wireless chargers are detuning the antenna in the middle console.

ST25R3914/15 offers highest output power combined with automatic antenna tuning.

Short interaction time

The entry function continuously checks for cards. The time window for interaction must be low to ensure best user experience.
ST25R3914/15 offers low power wakeup functionality combining capacitive & inductive sensors.

Wide Interoperability

Communication should work immediately. No retries or different placement required.

ST25R3914/15 offers excellent P2P compatibility with NFC devices

ST25R HF Readers Overview

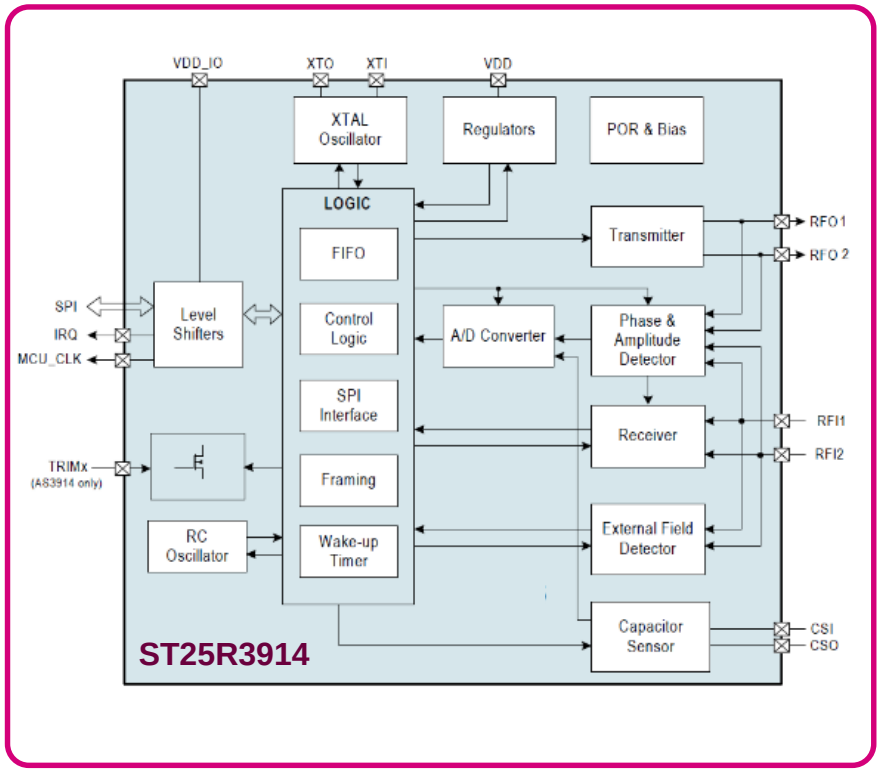
	ST25R3910	ST25R3911B	ST25R3912	ST25R3913	ST25R3914	ST25R3915
Description	Mid-Range Reader	High-Perf Reader & NFC initiator suited for Payment / Passport applications			High-Perf Reader & NFC initiator suited for Automotive	
Reader/Writer mode	ISO14443A/B ISO15693 & FeliCa by Transparent mode	ISO14443A/B ISO15693 FeliCa			ISO14443A/B ISO15693 FeliCa	
Card emulation mode	-	-			-	
P2P mode	-	Yes			Yes	
RF speed	848kbps	6.8Mbps (VHBR)	848kbps		848kbps	
Market certification	- -	Payment : EMVco, PBOC, mini-pay			Automotive: AECQ100	
Advanced features	AAT, Ind wake-up	AAT, DPO, Cap & Ind wake-up	DPO, Ind wake-up	AAT, DPO, Ind wake-up	AAT, DPO, Cap & Ind wake-up	DPO, Cap & Ind wake-up
Interface	SPI 6Mbps	SPI 6Mbps			SPI 6Mbps	
Power supply	2.4V - 3.6V	2.4V – 5.5V			2.4V – 5.5V	
Output power	0.7W	1.4W	1.0W		1.0W	
Temperature range	-40°C to +85°C	-40°C to +125°C				
Package	32-pin QFN (5x5mm)	32-pin QFN (5x5 mm) / Wafer	32-pin QFN (5x5 mm) / WLCSP	32-pin QFN (5x5 mm)	32-pin QFN [WF Q1 2018] (5x5 mm)	

P2P: Peer to Peer mode
VHBR: Very High Baud Rate
AAT: Automotatic Antenna TuningDPO: Dynamic Power Output
Cap & Ind wake-up: Capacitive and Inductive wake-up

life.augmented

ST25R3914-15 NFC / RFID Reader

- High Power Automotive solution



WF QFN32

- Use cases
  - Ideal for **Automotive** applications
    - keyless entry and start and driver authentification
  - Data transfer, pairing, in car payment
- Key features
  - NFC forum compatibility (no passive target)
  - **AEC Q100** certified with **wetable Flank** QFN package
  - 1W output power at 5V
  - Capacitive / Inductive Wake up
  - Antenna Auto Tuning (3914 only)
  - -40°C to **125°C** temperature range
- Key benefits
  - No external power amplifier required
  - Low power operation & Standby
  - Reliable performance even in metallic environment
  - Faster design times
  - Easy-to-use evaluation / development kits
  - Reference designs, application notes

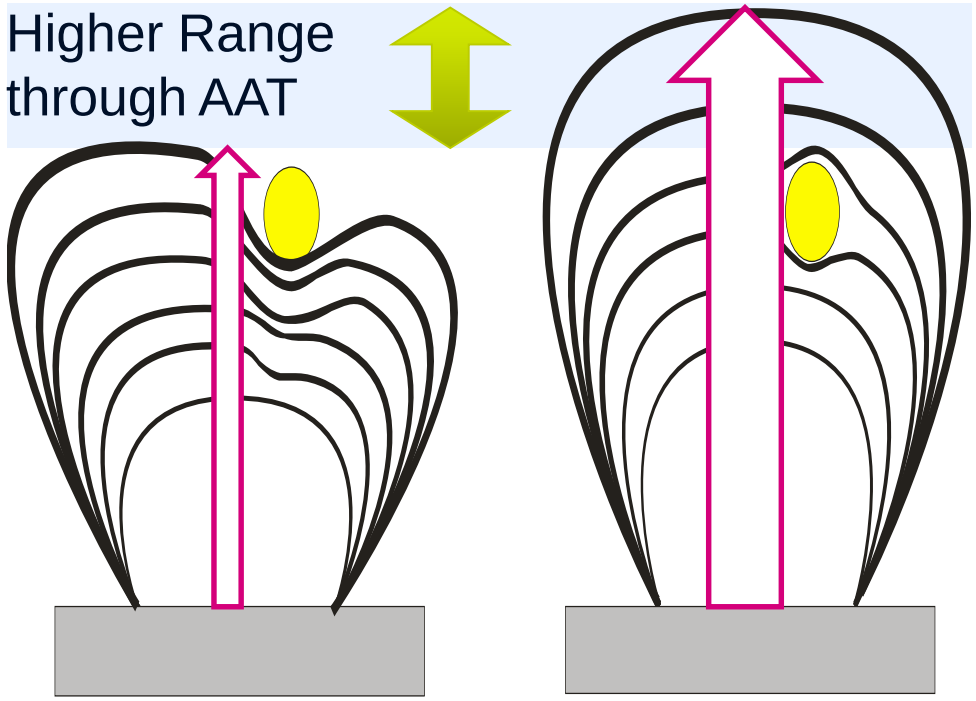
life.augmented

Key Features

life.augmented

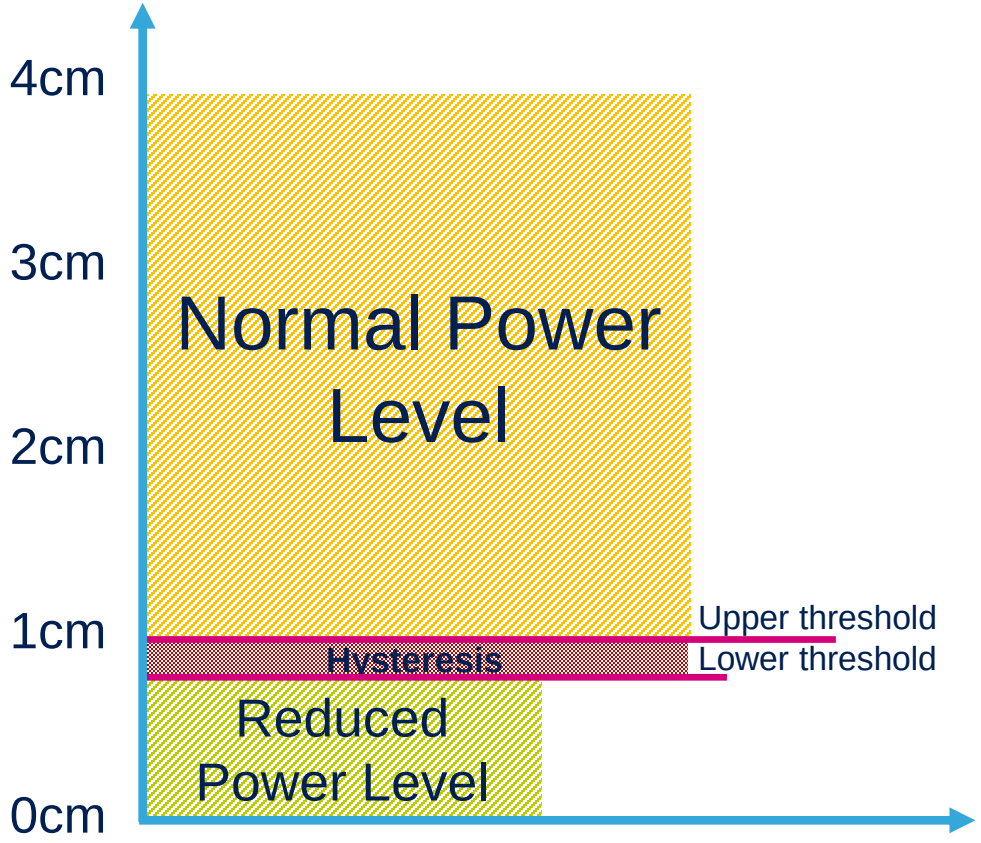
Automatic Antenna Tuning

- AAT increases Range & Field strength
  - AAT increases the range of an HF reader in bad environmental conditions and sustains maximum output power to the field with best efficiency
- AAT compensated for environment
  - Automatic antenna tuning analyses the phase shift of the antenna and retunes automatically
- AAT reduces production cost
  - The antenna can be tuned with an automatic procedure during production to fine adjust the design to different housings.
- Multiple Tag placement
  - Multiple tags in the field can be compensated to transfer a maximum of power for each.



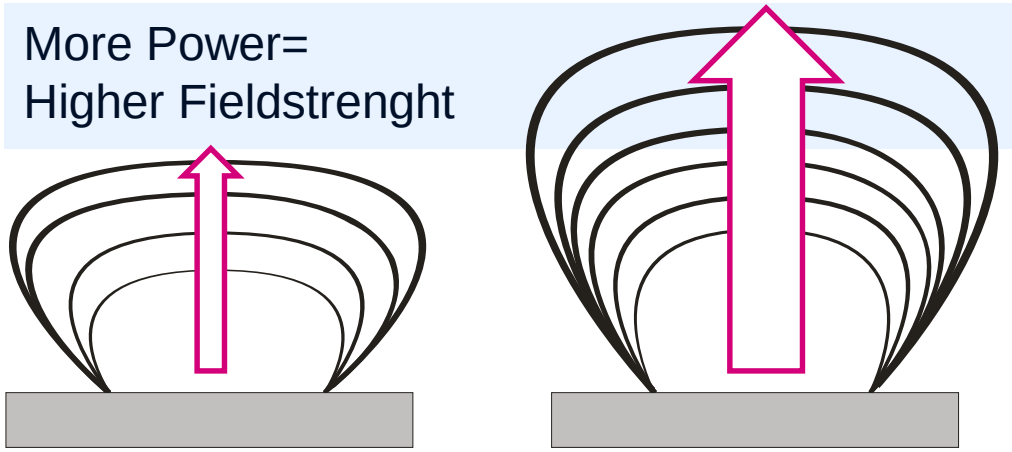
Dynamic Power, Gain & Squelch

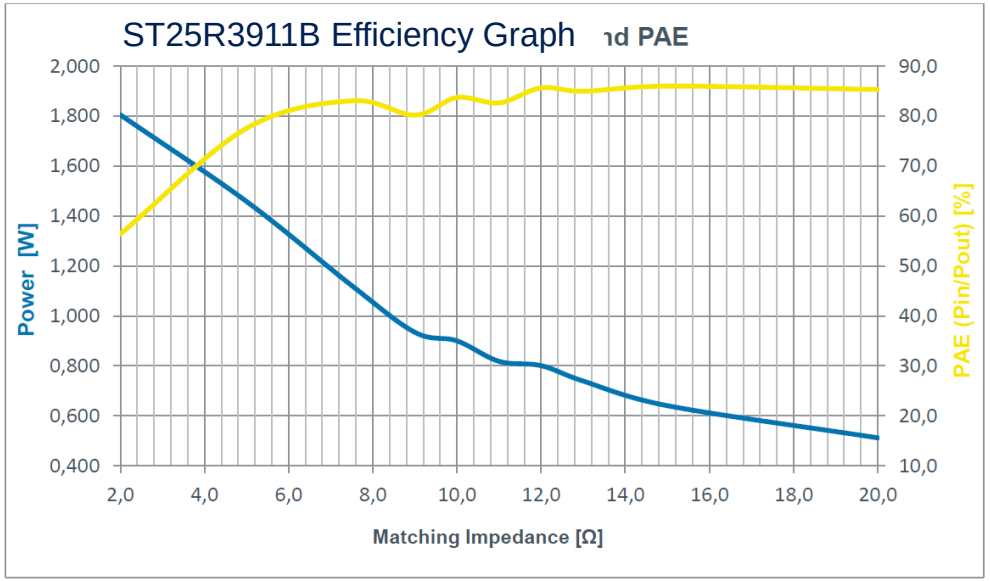
- Achieve min/max power limits easier
  - The ST25R series allows to adjust the output power dynamically via Dynamic Power Control
- Optimal performance from weak to strong card response
  - ST25R series allows to adopt to different power level of card responses via Active Gain Control
- Improved noise immunity
  - Squelch feature allows to scale the signal level to have improved immunity against noise



Highest Output Power & Efficiency

- No external Booster required for **POS**
  - The ST25R3911B includes low impedance drivers capable of generating **>1.4W** of output power
  - **EMVco certification** easily possible without external boosters
- Maximum transferred Power
  - “Slave” devices like interface tags are able to harvest far more energy for batteryless devices
  - Ideal for sophisticated **NextGen Gaming** platforms
- Ideal for Challenging Environment
  - The ST25R series is able to operate in metal encapsulation like **doorlocks**

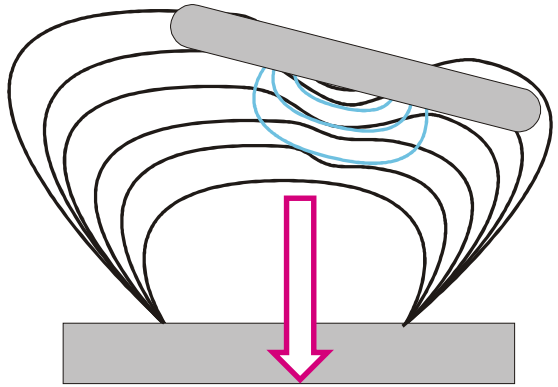


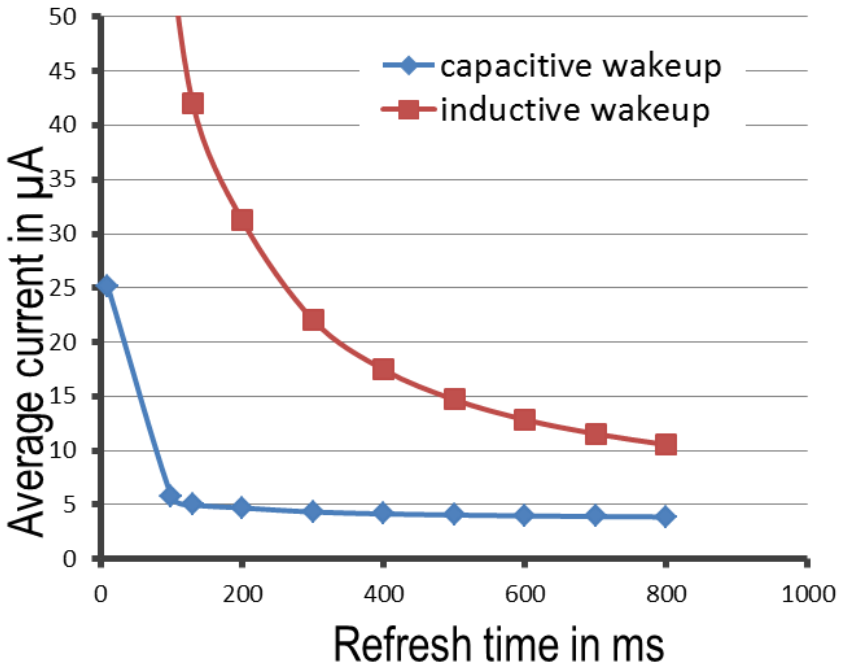


life.augmented

Low Power Wake up

- Internal wakeup circuitry
  - The ST25R series includes a fully programmable wakeup scheme. All relevant parameters like cycle time & sensitivity can be programmed.
  - No MCU required to run the wakeup; Capacitive & Inductive wakeup can be serially combined in for sophisticated wakeup scripts
- Capactive wakeup
  - ST25R series with this feature can detect capacitive changes. Eg. the approach of a hand.
- Inductive wakeup
  - The inductive wakeup is dedicated to detect approaching cards only





ST25R Series Benefits

- The ST25R family is an integrated reader IC for contactless applications with several benefits:
  - Outstanding analog performance
    - No external amplifier to achieve high field strength required
    - Automatic antenna tuning
    - Lowest power wakeup
    - Excellent P2P compatibility
  - Fastest time to market
    - reduced time to market at our customers significantly
  - Proven solution
    - The ST25R family is a market proven solution used in the consumer and automotive space.
    - Ensures best customer experience
  - Full integration into the STM32 library

Relay Attack

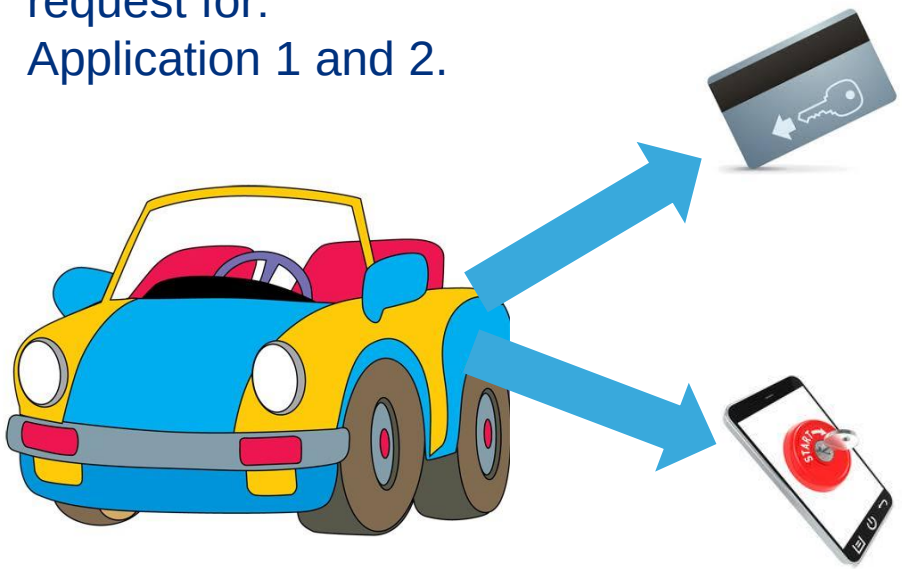
life.augmented

Benefits of NFC Vs. Relay Attack

- NFC is a short range technology. A relay attack using a mobile phone will only work on distances ~2cm. A longer range attack would require big antennas as the distance is defined by transmitter & receiver antenna size. => walking around with a 50cm antenna while having a read range of ~50cm is NOT convenient.
- If multiple NFC cards are in the pocket, it is already tricky to read out the correct card. And nowadays you will find ~3 credit cards in the pockets.
- Considering above a relay attack done on NFC is not very likely and if done with a mobile phone the card can be already considered stolen.
- Even so ST25R3911B can implement following countermeasures.

Relay Attack Countermeasures

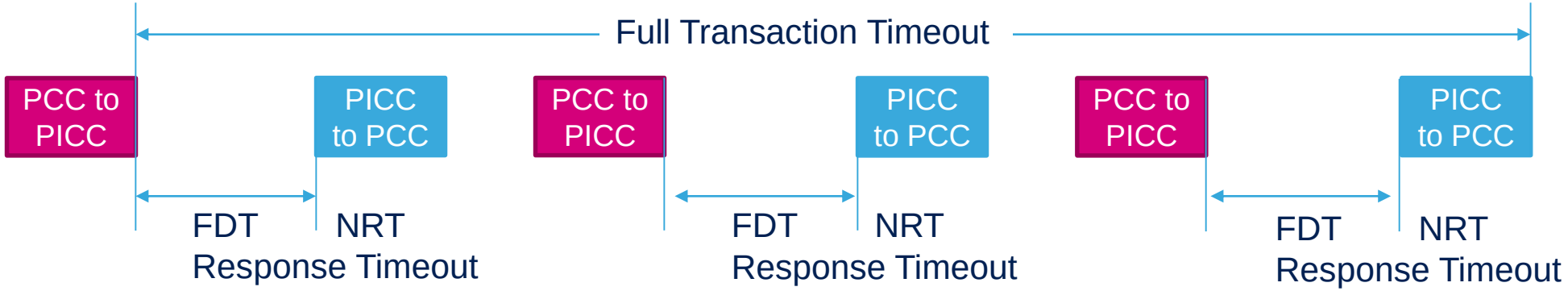
Cardoor polls and starts request for:
Application 1 and 2.



Application 1: Must be a card:
Reduce card response time to known limits of the used card. Restricts usage of cards.
Fingerprint Cards?

Application 2: Must be a phone:
Card response timer cannot be constrained, but fingerprint sensor on the phone will give best security.

Relay Attack



- According to NFC Forum reader MUST accept a response delay of up to 5s but a card SHOULD response within 77ms.
  => This can be shortened below those standards against relay attacks and captured by internal NRT

- Full transaction time can be monitored on top for enhanced security.

Table 40. No-Response Timer Register 1(1)

Bit	Name	Default	Function	Comments
7	nrt15	0	No-Response timer definition MSB bits Defined in steps of 64/fc (4.72 µs). Range from 0 to 309 ms If bit nrt_step in *General Purpose and No-Response Timer Control Register* is set the step is changed to 4096/fc	Defines timeout after end of Tx. In case this timeout expires without detecting a response a No-Response interrupt is sent. In NFC mode the No-Response timer is started only when external field is detected. In the NFCIP-1 active communication mode the No-Response timer is automatically started when the transmitter is turned off after the message has been sent All 0: No-Response timer is not started. No-Response timer is reset and restarted with Start No-Response Timer direct command.
6	nrt14	0		
5	nrt13	0		
4	nrt12	0		
3	nrt11	0		
2	nrt10	0		
1	nrt9	0		
0	nrt8	0		

1. Default setting takes place at power-up and after Set Default command.

life.augmented

Automotive Processors
with Built-In Security

Advanced secure microprocessors
protect connected cars

TELEMACO 3P

Telemaco3P

- Secure Elements (ST33) and embedded Flash microcontrollers (SPC5).

- HIS SHE/SHE+ Service Set with extensions for PKC (SHE_EXT)
- Cryptographic Functions Accelerators
- Symmetric keys: MP AES
- Public keys: RSA, ECC
- Hash: MD5, SHA1, SHA2, SHA3
- True Random Number Generator


life.augmented