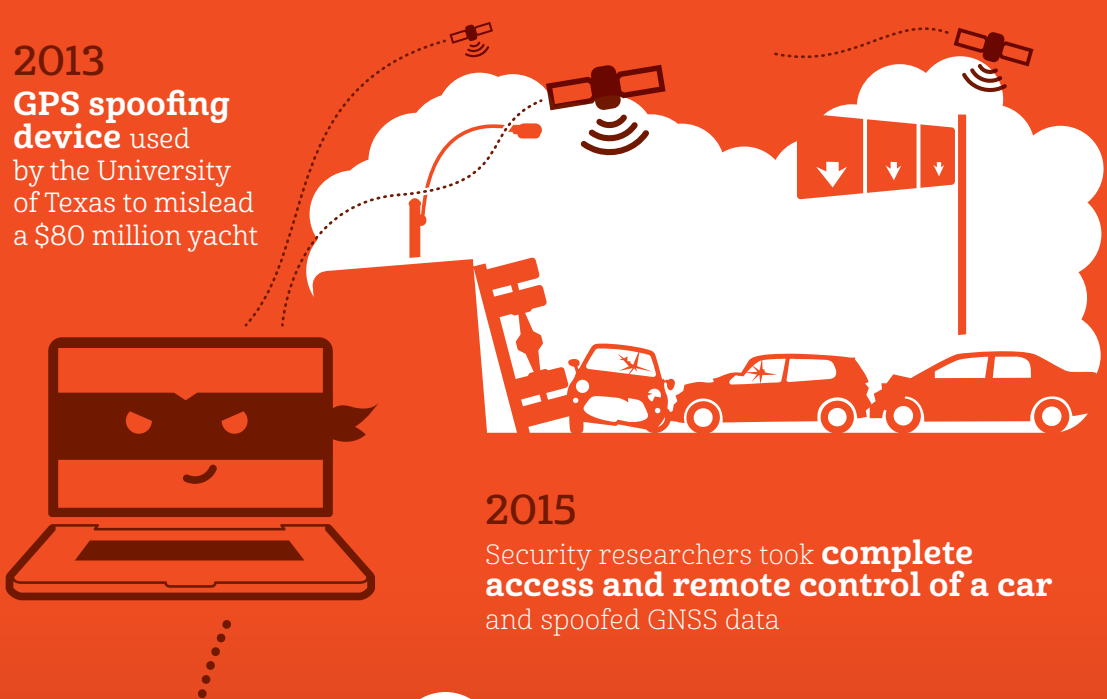
An innovative solution **against** GNSS attacks

FOSTER ITS

First Secured, Trusted and Resilient GNSS Receiver for ITS applications

2013
GPS spoofing device used by the University of Texas to mislead a $80 million yacht



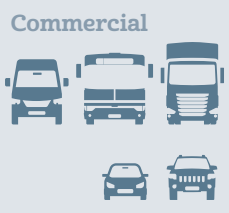
2015
Security researchers took **complete access and remote control of a car** and spoofed GNSS data

2015
Open source GPS constellation simulator available

2015
Availability of Low cost RF open hardware able to run a GNSS simulator in real-time

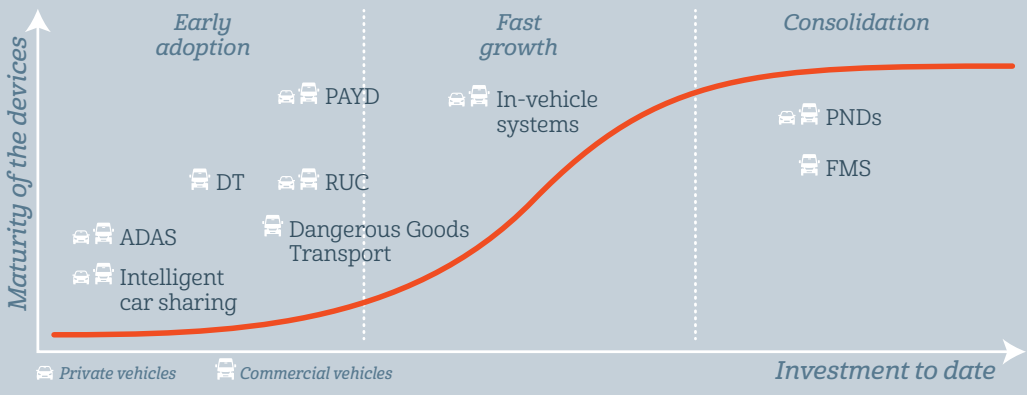
IT and GNSS Security
A critical concern for ITS

Number of vehicles in 2015 (in million)



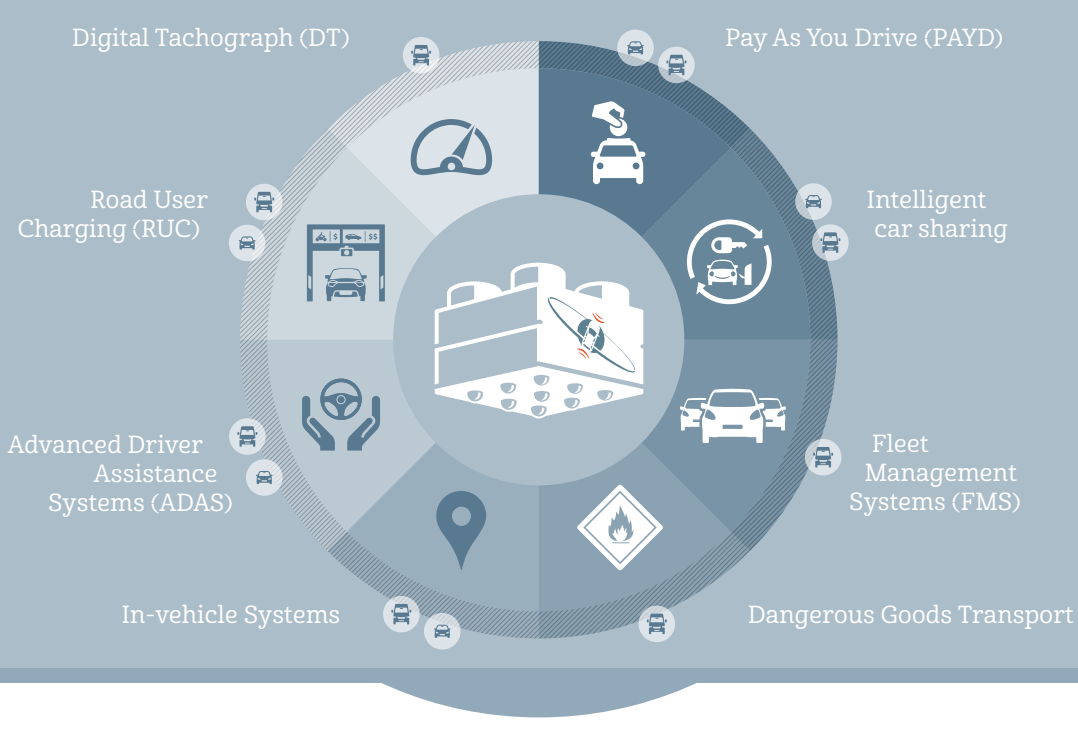
	EU	World
Commercial	39	445
Private	247	907

Current level of maturity of GNSS devices

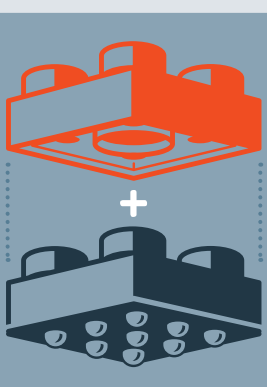


Applications

Private vehicles
Commercial vehicles



FOSTER ITS



Two-in-One device: GNSS + Secure MCU

- ▹ GNSS replay, spoofing and meaconing attack mitigation
- ▹ GNSS interference and jamming detection
- ▹ Attack identification
- ▹ Galileo OS authentication capability
- ▹ Dead Reckoning
- ▹ Ciphered or/and signed data delivery
- ▹ Additional IT security services
- ▹ Tamper resistant
- ▹ Automotive grade and common criteria compliance

Embeds STMicroelectronics ST33 GIM2 & TESEO III
Inputs:
Odometer/CAN bus/antenna
Outputs:
Serial, ISO7816, CAN bus

Products Range

Availability

2016 — First Samples
2017 — First product

Contact

INFO@FOSTERITS.EU

FOSTER ITS

Created, designed and developed by FDC and ST life.augmented

Certification process enabled by NavCert

Integrated and full-scale tested by NOVACOM services

Test and Validation in cooperation with the EC JRC GNSS LAB

INFO@FOSTERITS.EU

European Global Navigation Satellite Systems Agency

HORIZON 2020

This project has received funding from the European GNSS Agency under the European Union's Horizon 2020 research and innovation programme under grant agreement No 641492.