Secure UAV Operation in the U-Space using IEEE 802.11p

Available technologies for UAV-ID, Secure geo-fencing, Detect & Avoid and **D2X**
Securing identity and communication of UAVs to safeguard citiziens

Extract

Jacques Kruse Brandao
Advocacy Partner Secure Digital Identity

CEPT Workshop on Spectrum for Drones / UAS
29.-30.05.2018

NXP SECURE CONNECTIONS FOR A SMARTER WORLD

AGENDA

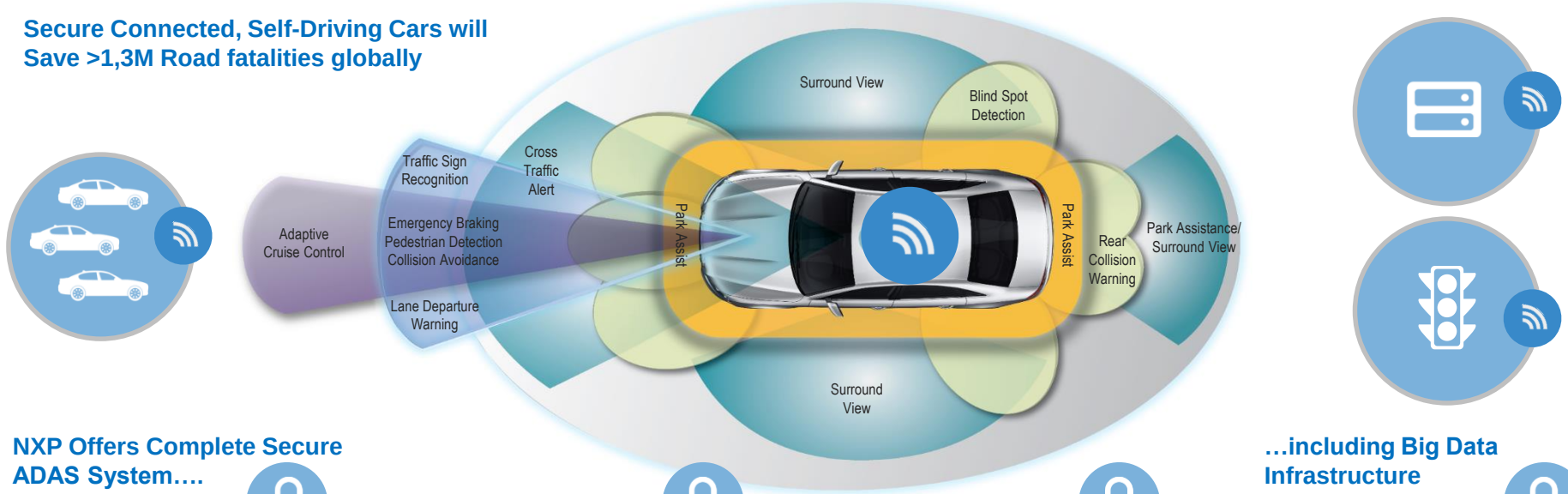
Why is NXP involved in UAV Solutions?

Secure UAV Operation in the U-Space - Visualization of UAVs in UTM

1. Secure Upload of Geo-fencing Data
2. Drone2Drone & Drone2X Communication / Collision Avoidance for Drones
3. Authentication for Operation
4. Restricted Access to defined flight areas
5. Identification of UAV (eID), Pilot, Insurance, Mission

ENABLING THE SECURE CONNECTED CAR

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



NXP Offers Complete Secure ADAS System….

SENSE	Secure Network	THINK	Secure Network	ACT
Radar Vision Secure V2X		Processing Sensor Fusion Security		Powertrain Chassis Braking

…including Big Data Infrastructure

BIG DATA
Digital Networking Infrastructure Security

SECURE UAV OPERATION IN THE U-SPACE

- Current UAV's are manually operated.
  - Manual operation requires **visual line of sight** (VLOS) and relies on the operator knowledge of all aviation rules to for example **avoid no-flying zones** (eg airports)
  - Therefore for commercial use, **the pilot must have a valid pilot's license** (article)
  - Mainly Command and Control operations

- UAV **automation** is key to
  - Enable applications which require flying **beyond** VLOS.
  - Remove the requirements for a pilot's license.

- UAV automation requires flawless technologies for:
  -> UAV-ID / Secure UAV
  -> Pilot / Mission
  -> Geo-fencing
  -> Sense and Avoid
  -> Secure D2D and D2X Communication

AUTONOMY & UTM VISIBILITY

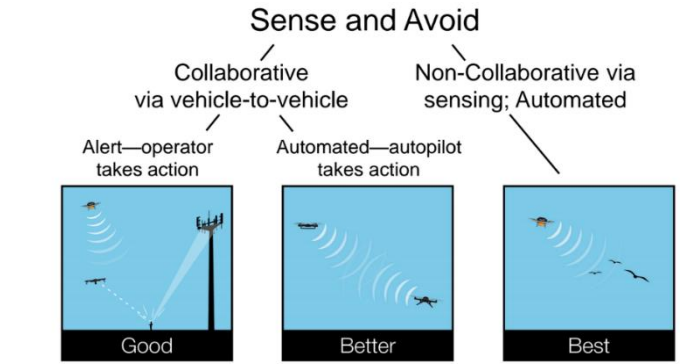
Sense and avoid technologies

Drone2Drone & Drone2X communication
Collision avoidance for drones

Automated Sense and Avoid: Various technologies like ADS-B/ Radar/ Lidar/ Camera are available

1. High amount of UAVs will saturate the channel and make it unreliable
2. Might interfere with regular aviation
3. Cost is a major driver for this technology as ideally every DIY UAV should be equipped with this

FAA encourages at least 3 types of communication technology redundancy



ADS-B / Flarm alike LTE/ Drone2X | **Drone2Drone** | **Radar Lidar\Camera**

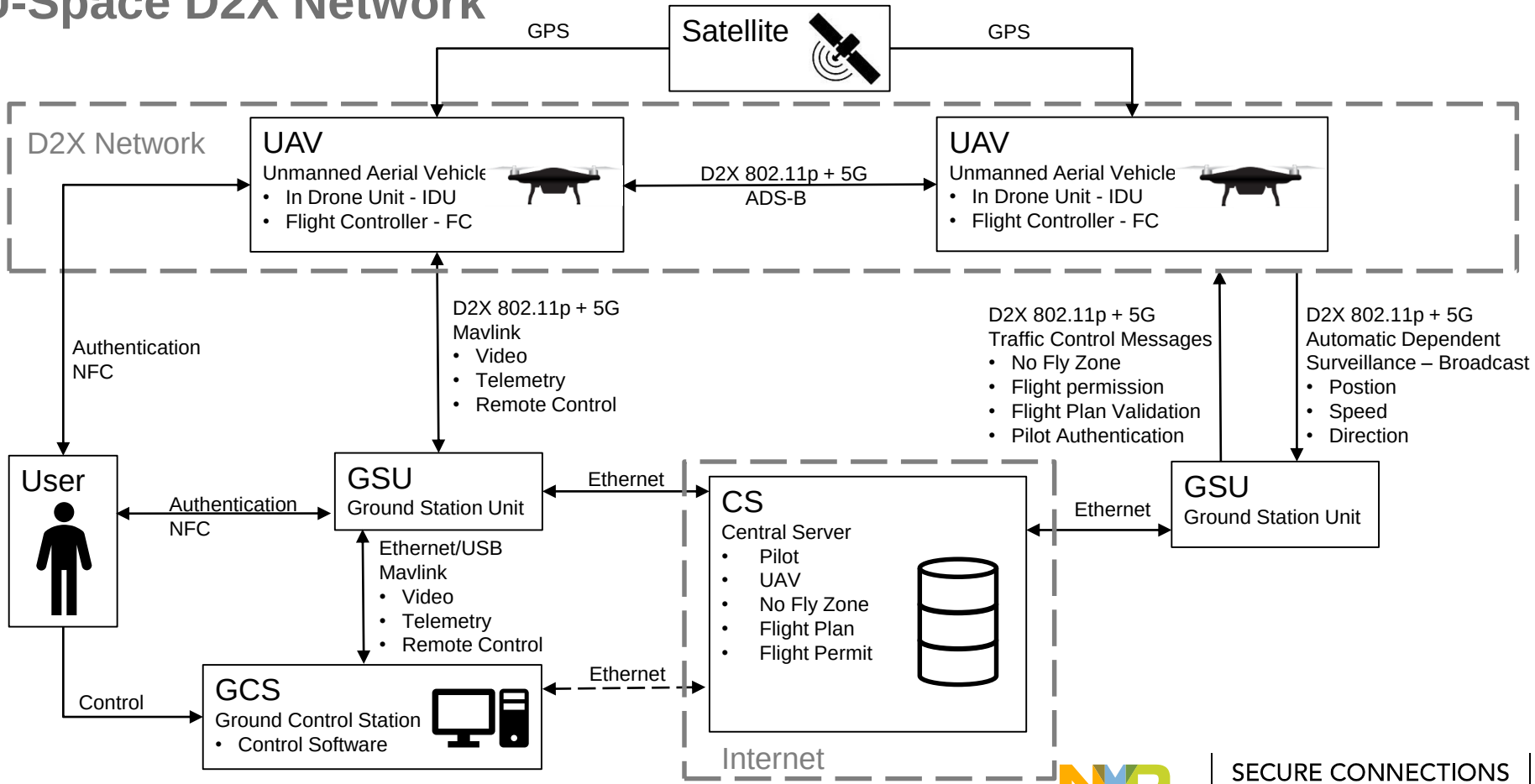
→ Required: Fast Track to Innovation Funding programs for further R&D & Testing Co-creation projects between operators, industry, research and aviation authorities

D2D and D2I Communication

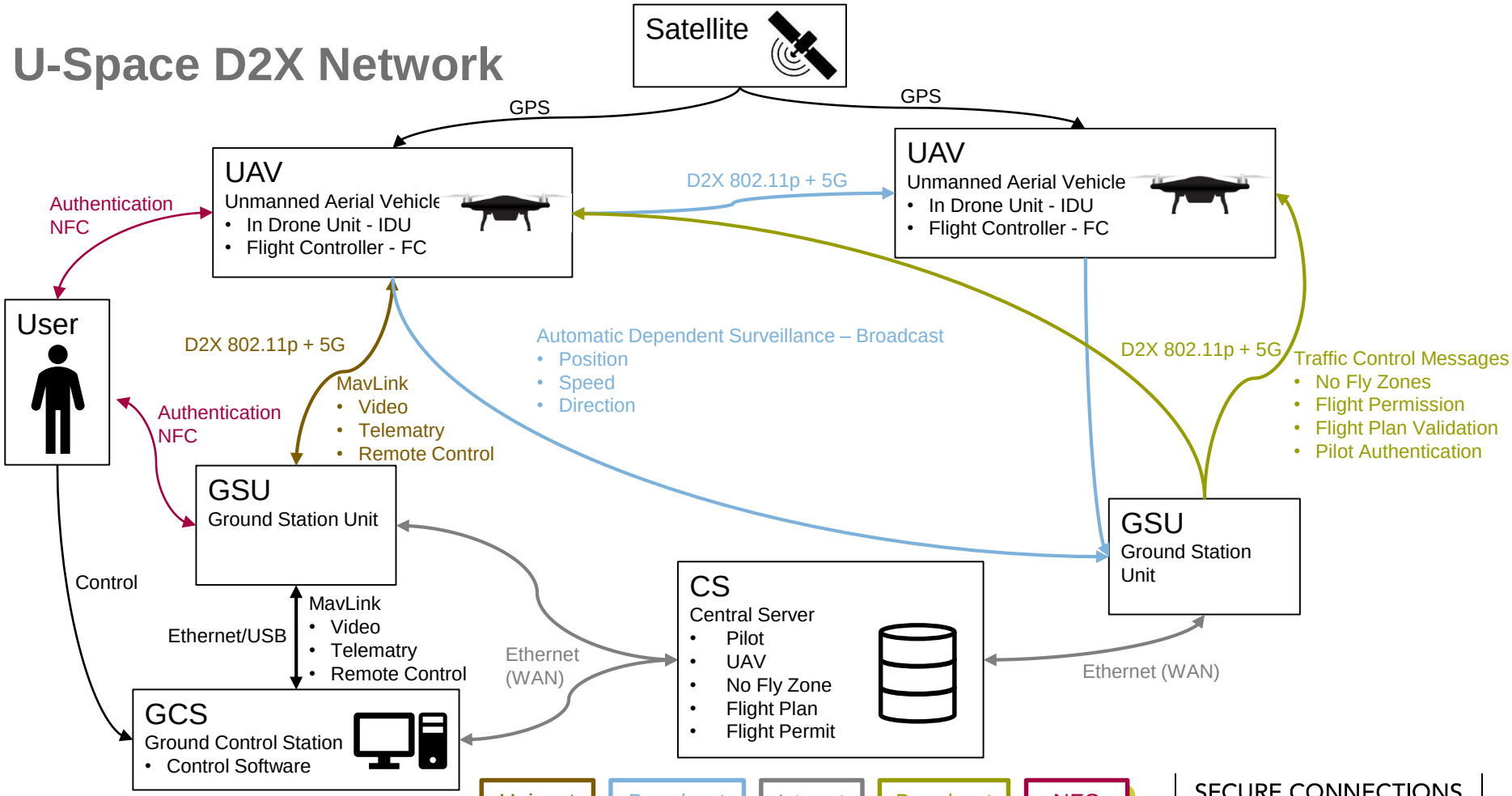
802.11p + 5G for Drones

- **RELIABLE Communication**
- **REAL TIME Video transmission** (avoiding unauthorized access)
- **SECURE Remote Control** of the drone (avoiding unauthorized access)
  - Low latency
- **Drone to Person communication**
  - “Selfie Drone” follows me at specified altitude & distance and makes movies of me while I am windsurfing etc.
- **OVER THE AIR UPDATES**
  - Secure OTA firmware update
  - Secure OTA configuration update
- **Proper authentication of the drone** to local authorities via secure D2X & SMX
  - avoid that drones are used by terrorists at a public events/ in cities to carry explosives.
  - UseCase: Drone authenticates itself as authorized flying object – otherwise a sniper has to take it out of the sky.
- **MULTIPLE Drone2X Communication** at once (allowing teams of drones to operate together – shooting movies / police inspection / maintenance work)
- **Super light weight “Anti Collision Transponder”** via Drone2Drone communication (existing transponders have a weight >10 Kg)
- **Complete hardware security solution** for message authentication and anonymity/tracking prevention
  - Data encryption based on keys stored in secure element
- **Best receiver sensitivity** also for
  - Non-Line-of-Sight and Mobility conditions
  - line of sight range >1km
  - support differential speeds up to 500km/h

U-Space D2X Network



U-Space D2X Network



NXP proposal for UAS (drone) applications of 11p technology

- **Technology of IEEE802.11p is very suitable**
  - Long distance, low latency, mobility tolerance etc.
- **Drone-to-car messages could be transmitted at 5.9 GHz ITS channels**,
  but co-existence study with existing C2X applications must be performed in advance due to UAS (as they are expected in getting part of the road traffic and therefore need to be integrated into related safety applications)
- **Drone dedicated communications not related to Drone-to-car messages should use different frequency bands**
  - Currently no band perfect match, frequency regulation may need to be adapted
  - Alternatives to 5.9 GHz as used in automotive IEEE802.11p:
    - **5.150-5.250 GHz** reserved for, but unused by the aeronautical community? *)
    - 5.150-5.350 GHz RLAN: indoor use only (plus limitation as in next entry)
    - 5.470-5.725 GHz RLAN: 'aeronautical mobile service' explicitly excluded **)
    - 5.725-5.875 GHz ISM/SRD allowed but at maximum 25 mW

- *: ref ECC/DEC/(04)08, consideration d (page 4)
- **: definition 'aeronautical mobile service' unclear; specific service or includes UAS (generic DFS-mobility issue driven)?

Requirements to autonomous mobility

Resumée: Pre-requisite for controlled use of UAVs needs respect towards

- Safety functionality of UAV (using D2D and D&A)
- Identification of each UAV
- latest and correct geo-fencing data

is the safe-guard of

- **Authentication** of UAVs (UAV-ID)
- **Data integrity** (flight data, geofencing data)
- **Confidentiality**
- **Encryption** of the transmission channels

by **certified** standards.

Only with **trust**, **transparency** and the **same legal framework** for all market participants there will be planning reliability for a prosperous future of the UAV market with safe flights.

Summary NXP Technology for UAV

Summary NXP Technologies for UAV

Secure UAVs can be fully powered by NXP

click https://www.youtube.com/watch?v=xLfMEuMjAZE&feature=youtu.be

Summary NXP Technologies for UAV

UAVs can be fully powered by NXP

Flight Controller
- Secure Microcontrollers
- Sensors
- Secure Autopilot SW

Sense and avoid
- Secure Drone2X
- RADAR
- Sensor Fusion

Future drone generation

Rotors
- Microcontrollers
- Motor control SW
- Power MOSFET

Remote control
- Secure microcontroller
- Charger
- Video streaming

Registration/activation
- Secure ID
- NFC
- BTLE

Future drone generation

Battery
- Power MOSFET
- Smart Charging
- Wall plug adapter
- TVS protection

Interfaces
- HDMI ESD protection
- USB, CAN ESD protection

NXP Information on UAV/Drones

- UAV Website → www.nxp.com/uav
- UAV Solutions video → https://youtu.be/xLfMEuMjAZE
- UAV Registration Authorization -> https://nxp-rfid.com/electronic-registration-authorization/
- UAV Flight Permission -> https://youtu.be/Um9pe8zbWXE
- UAV Whitepaper ‚SECURING THE FUTURE OF UAVS' -> www.nxp.com/uav or please ask
- EENews on **Applying V2X technology to drones**
  http://www.eenewsautomotive.com/design-center/applying-v2x-technology-drones-0

  + D2X whitepaper full version
- International Journal of Network Security & Its Applications:
  Performance of Vehicle-to-Vehicle Communication using IEEE 802.11p in Vehicular Ad-hoc Network Environment
- TicTac Drone → https://youtu.be/pr6LDSe_DMI

Thank you!
Shape the future, Lead the Dialogue, Get involved.

SECURE CONNECTIONS
FOR A SMARTER WORLD

www.nxp.com/uav
Contact: Jacques Kruse Brandao, jacques.kruse-brandao@nxp.com