86th IFIP WG 10.4 Meeting, June 2024

Unmanned Aerial Vehicles (UAVs) and Airspace Safety

Naghmeh Ivaki

FACULDADE DE CIÊNCIAS E TECNOLOGIA UNIVERSIDADE D COIMBRA

CISUC

Autonomous Vehicles

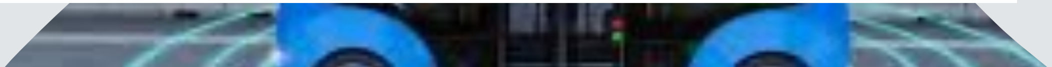

SEVENTY-FOURTH YEAR

SCIENTIFIC AMERICAN

THE WEEKLY JOURNAL OF PRACTICAL INFORMATION

VOLUME CXVIII. NUMBER 1 | NEW YORK, JANUARY 5, 1918 | 15 CENTS A COPY $4.00 A YEAR

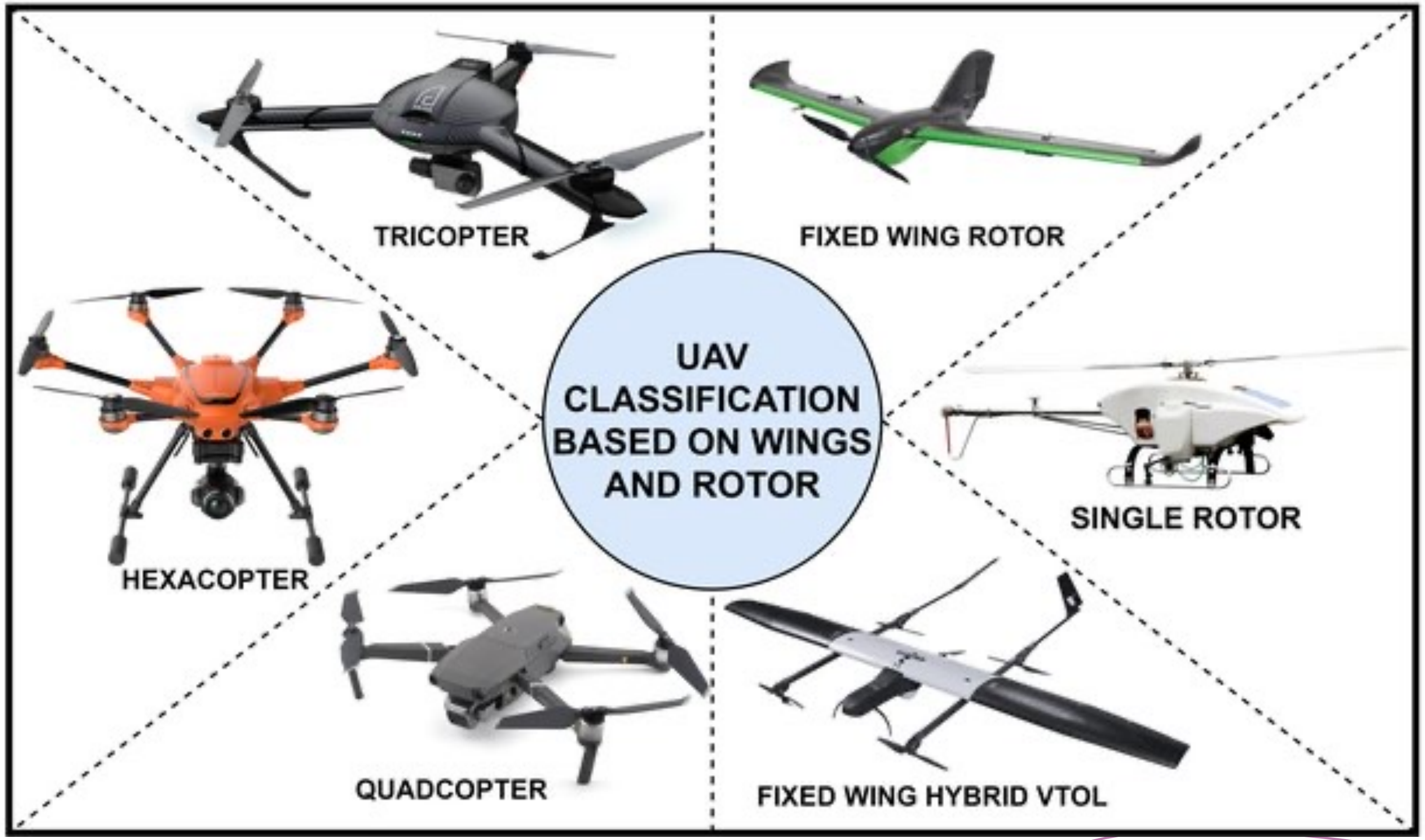
The motorist's dream: a car that is controlled by a set of push buttons



What is a UAV?

- An ***unmanned aerial vehicle (UAV)***, commonly known as a **drone**, is an aircraft **without any human pilot or crew on board**

Classification of UAV based on Wings and Rotors



UAVs Characteristics

- Flexible in movement
- Mechanically Simple
- Cheep

Applications of UAV

Agriculture

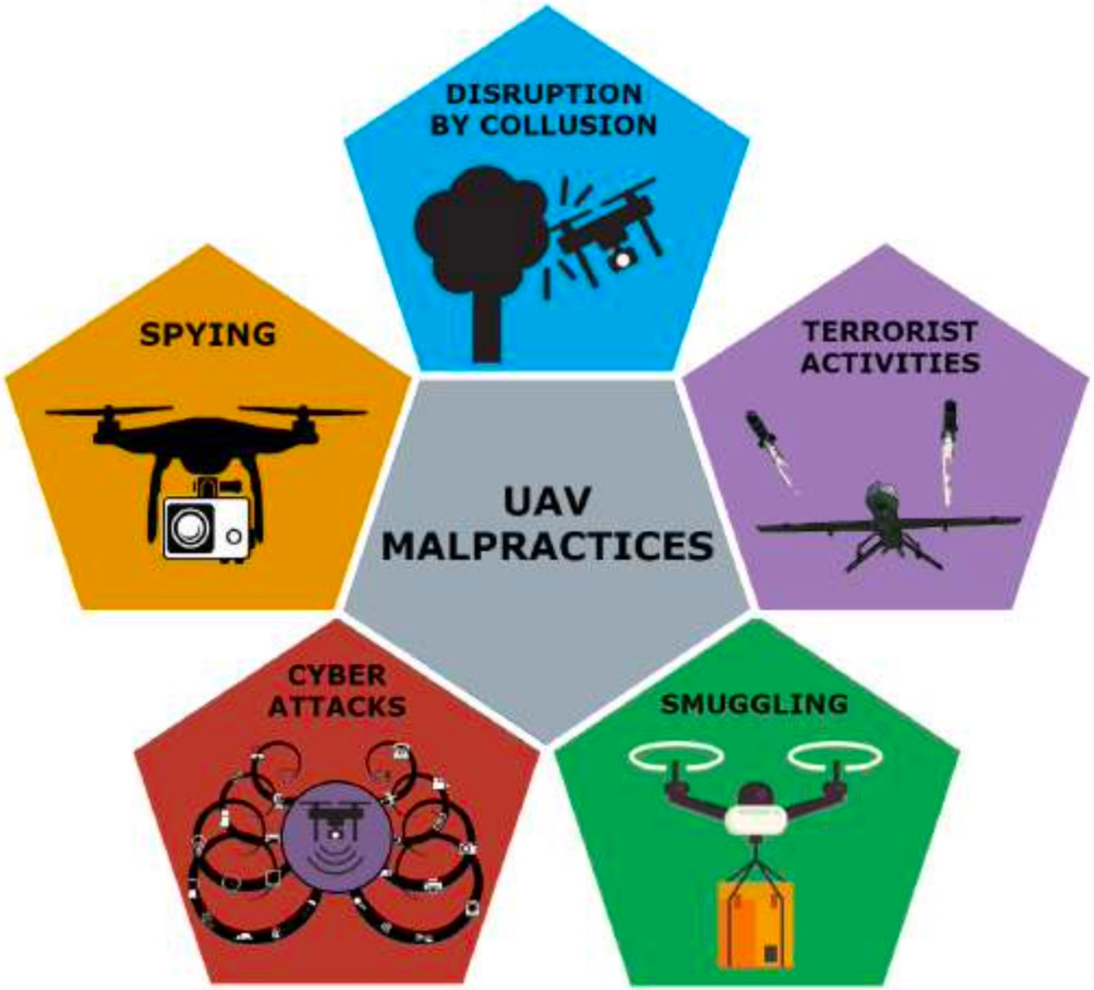
Taxi

Delivery

security surveillance

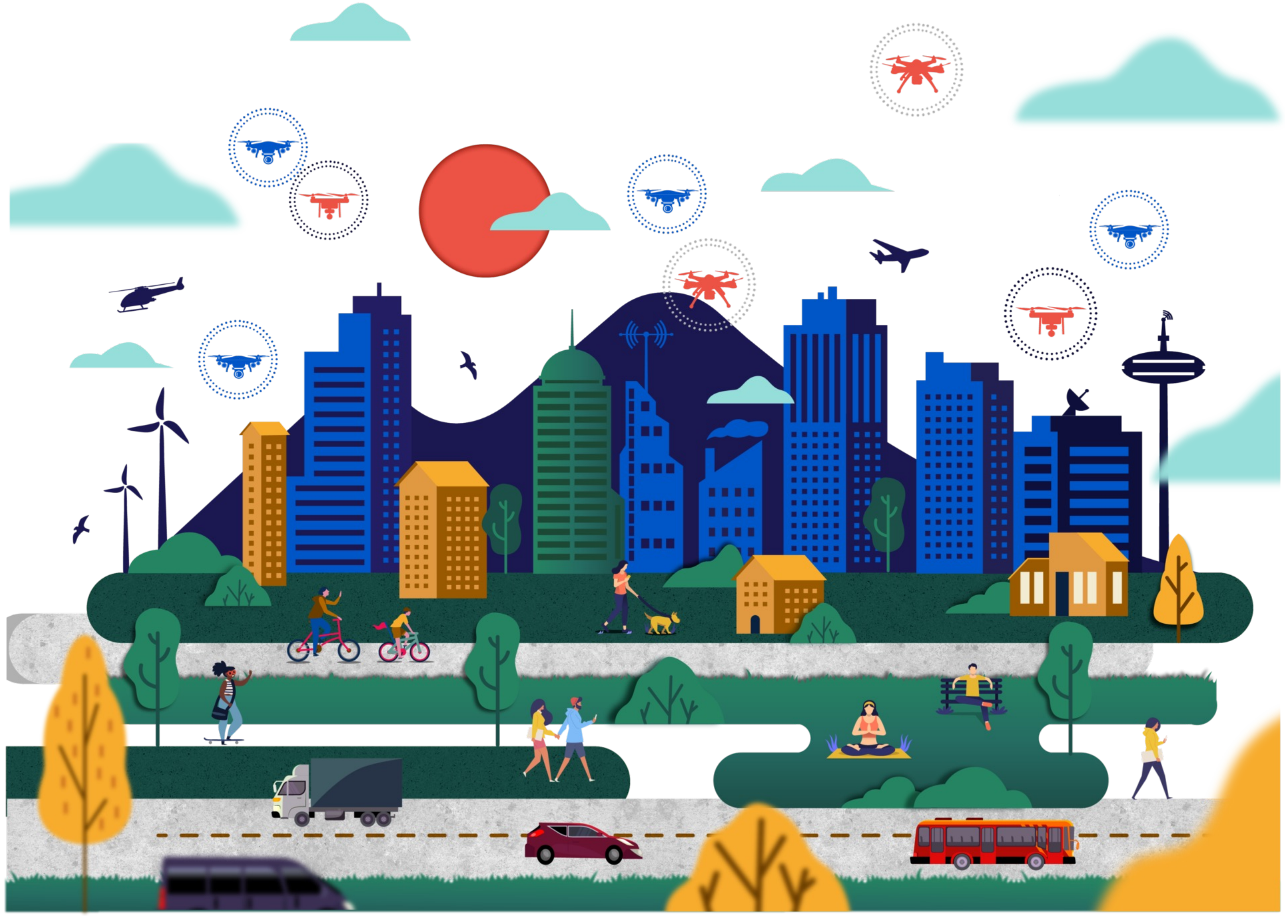
Photography and Filming

UAV Malpractices



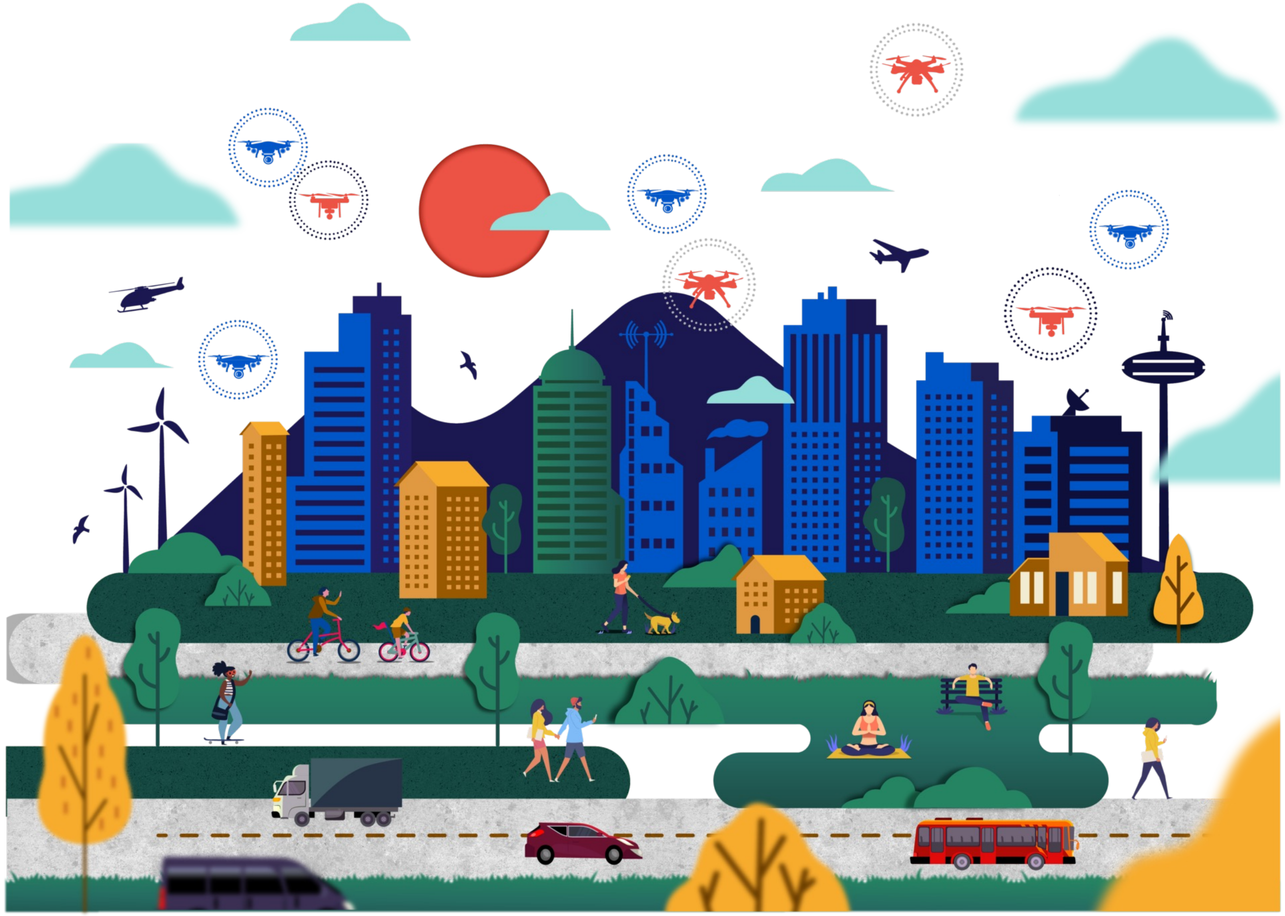
Future of UAVs

According to SESAR (European Union's Digital Sky technology pillar) **400,000 drones** will be flying over **European airspace** by **2035**



Main Challenges

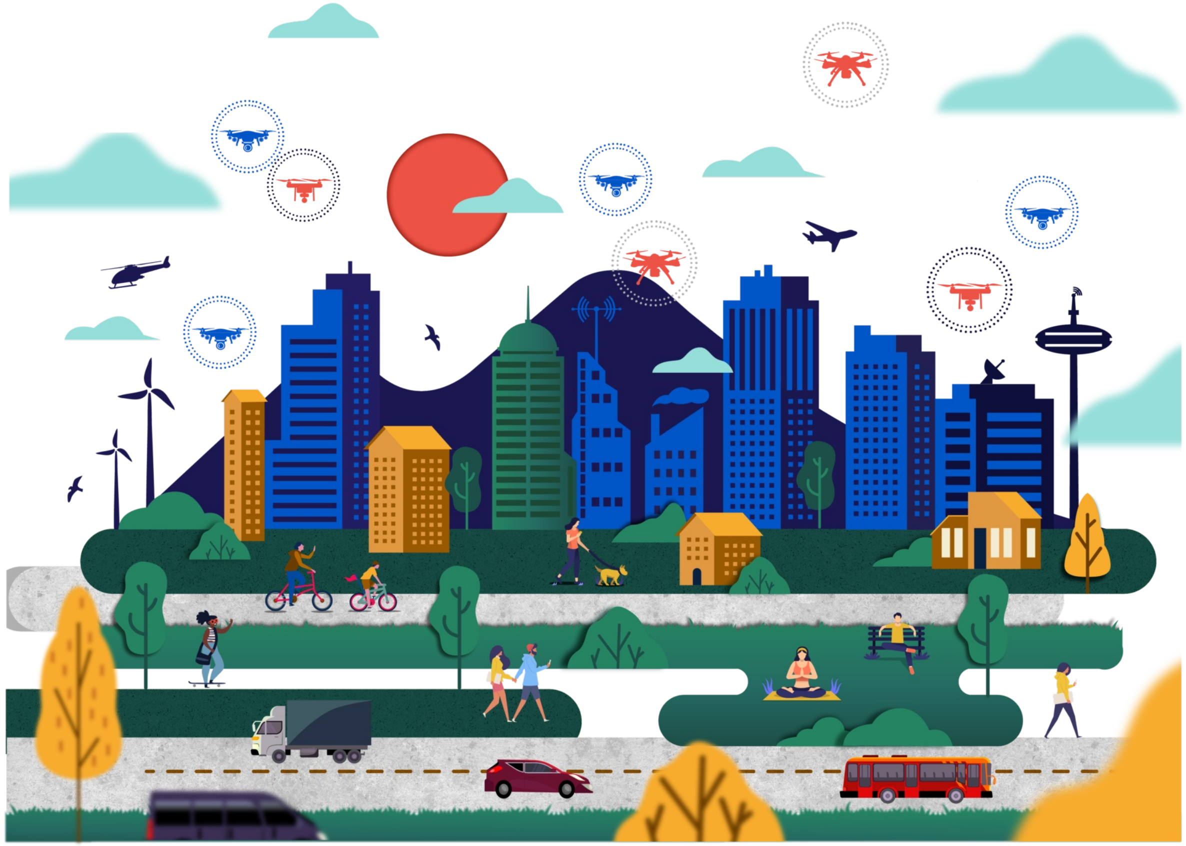
- High Density
  - High probability of collision
- High Target Level of Safety
  - Highly risky environment (urban air space)
- Use of AI in AVs
  - V&V of AI safety
- Low budget



Need for Air traffic control

Other Challenges with UAVs in Urban Air

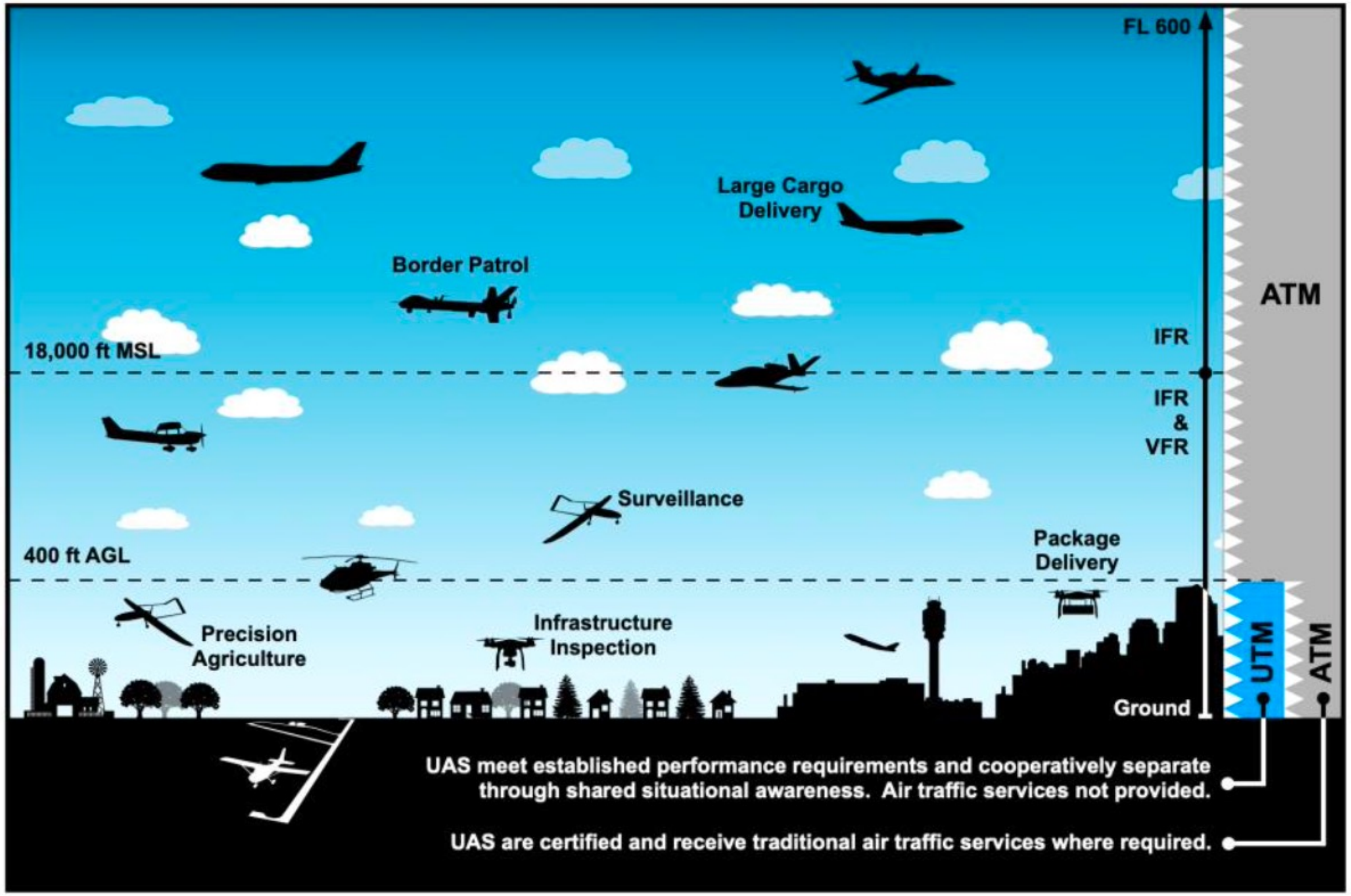
- Violation of public privacy
- Noises
- Social Acceptance
- Mission Priority (e.g., emergency services)



Need for Unmanned Aircraft System (UAS) Traffic Management (UTM)

- A **conceptual framework** for UTM was first conceived by NASA in **2013**
- The Federation Aviation Administration (FAA) and NASA formed a **UTM Research Transition Team** (RTT) in **2016** to jointly undertake the development and eventual implementation of UTM

Operational context of UTM services



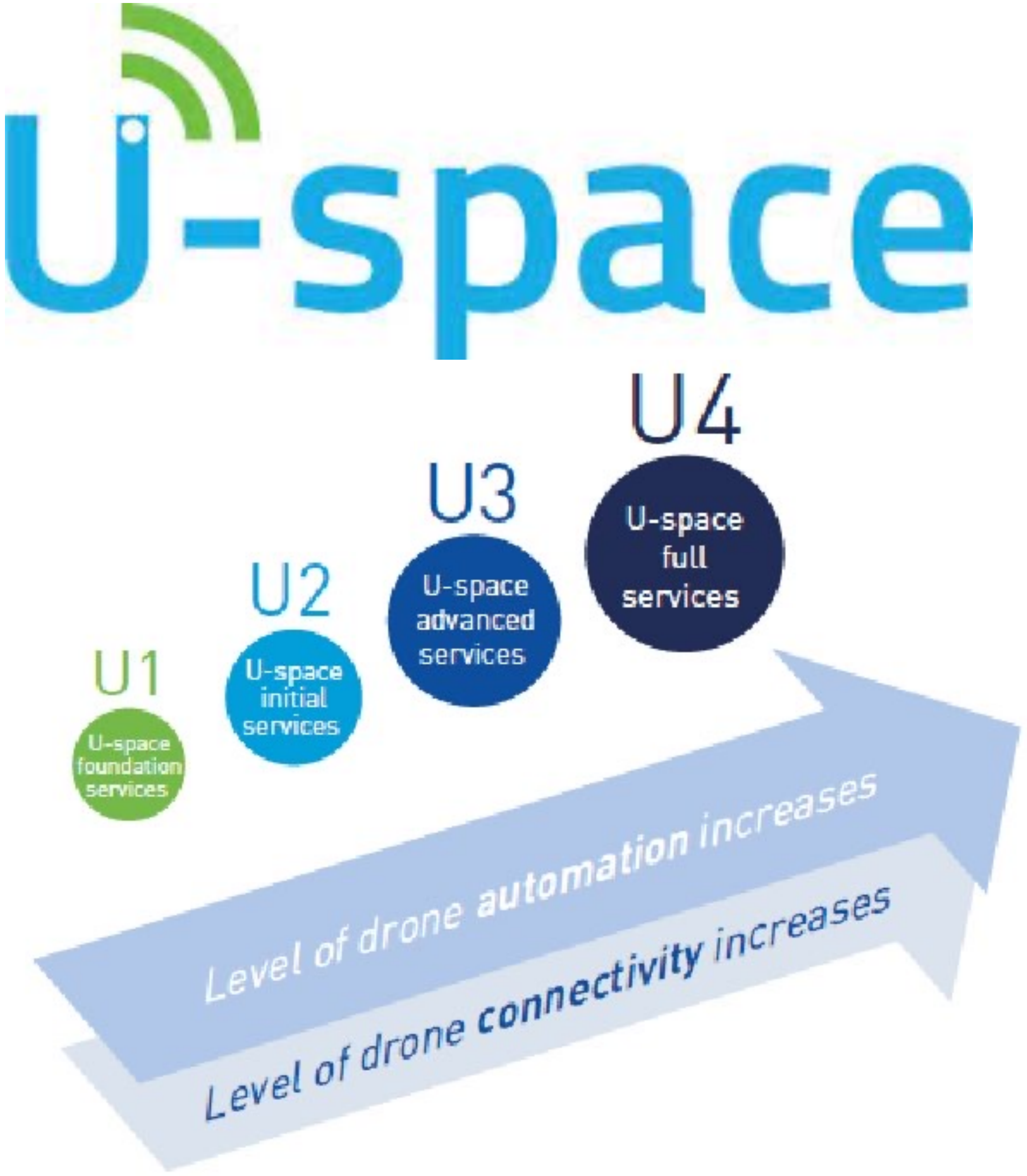
UTM: is the manner in which the FAA (Federal Aviation Administration) will **support operations for UAS operating in low altitude airspace**

U-space

- What is U-space?
  - U-Space is the UTM system in Europe

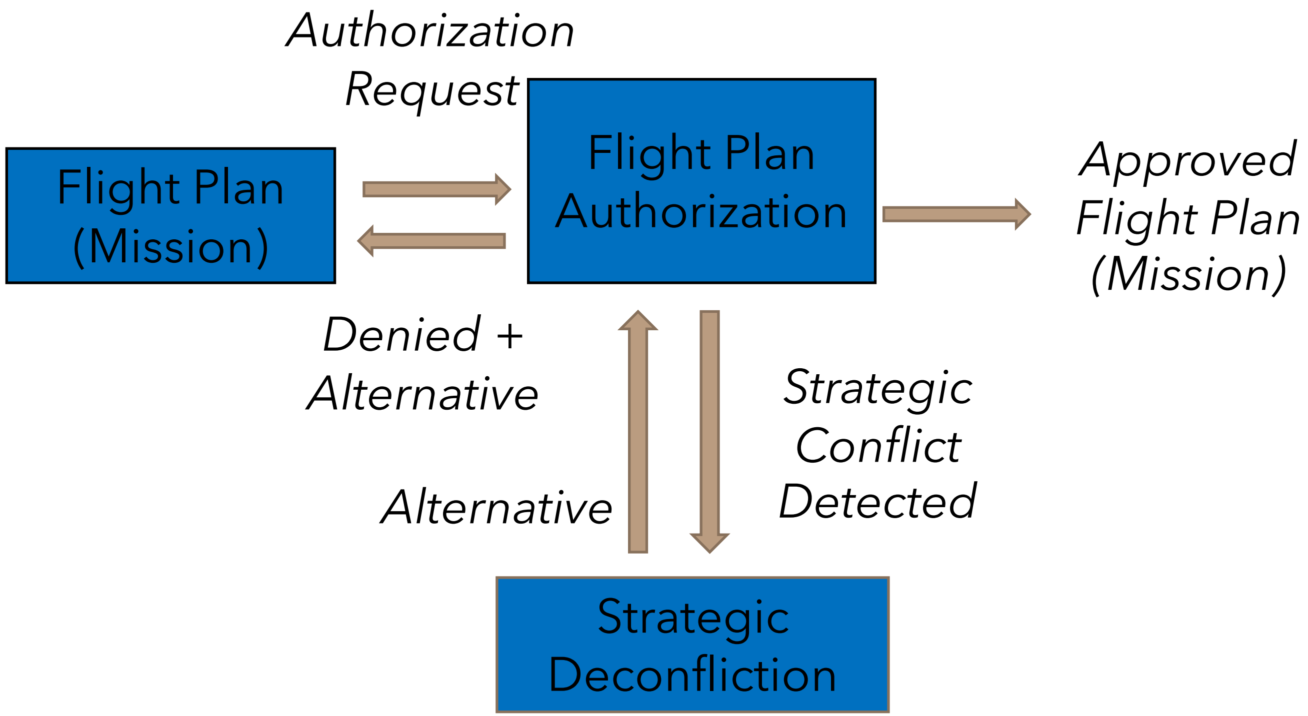
"A set of new services and specific procedures designed to support **safe**, **efficient** and **secure** access to airspace for large numbers of drones"

U-Space Blueprint



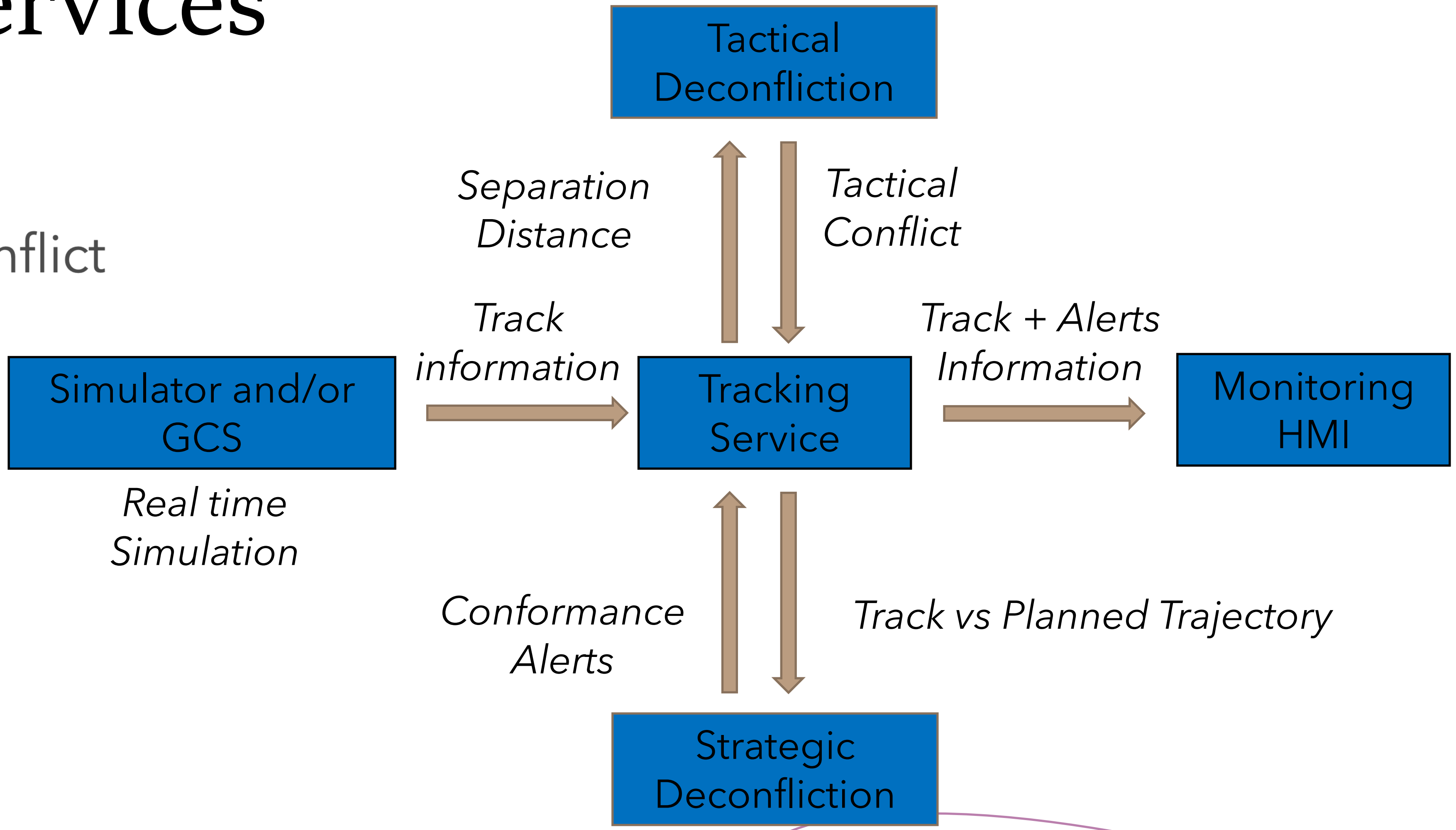
U-space services

- Strategic Phase
  - E.g., Pre-flight Conflict Detection



U-space services

- Tactical Phase
  - E.g., In flight Conflict Detection

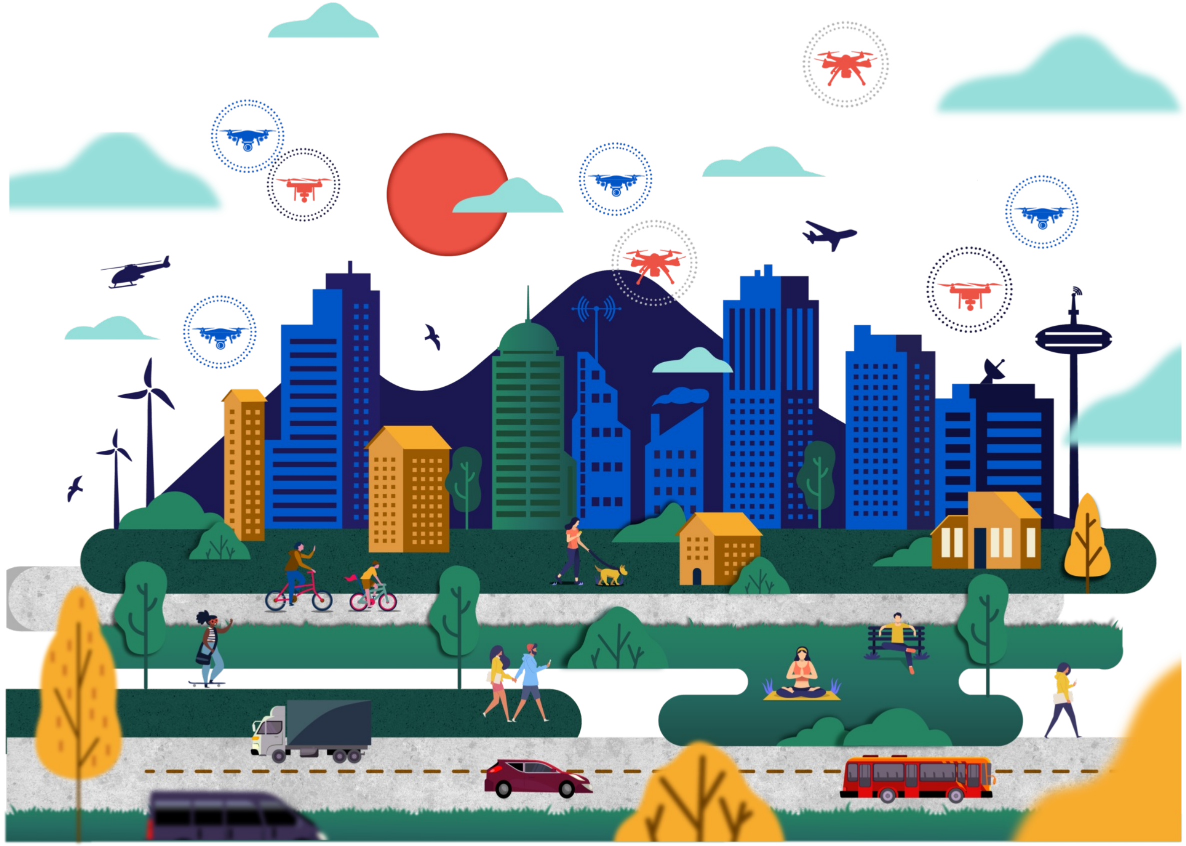


BUBBLES Project

https://bubbles-project.eu/

Our Objective in BUBBLES

Validate U-space separation minima in **abnormal** and **faulty** conditions



Communication Failures

Internal Communication
between Sensors and GPS
with Flight Controller

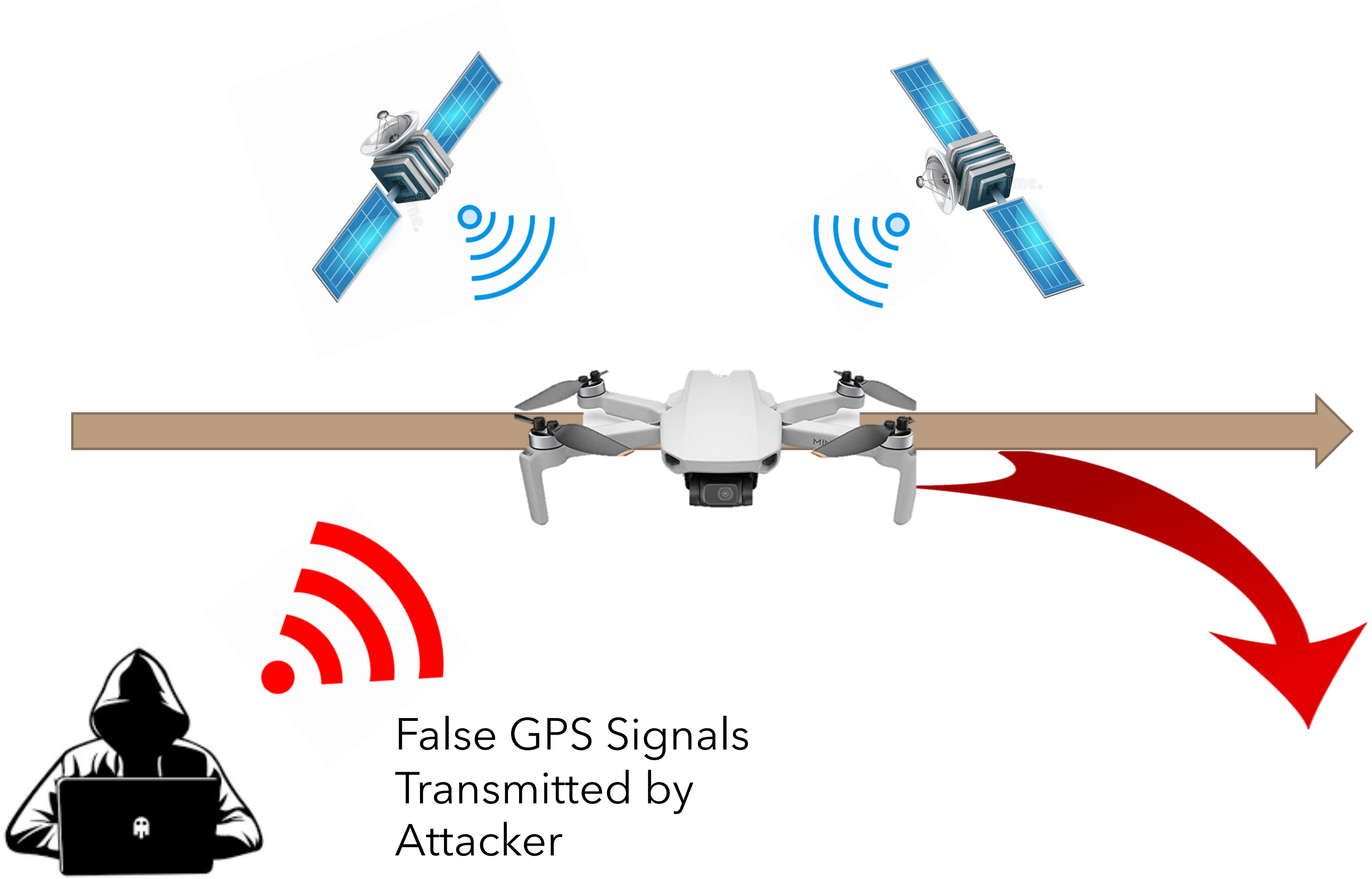
Communication between
UAV and ground
controller/pilot

Communication between
UAV and tracking service

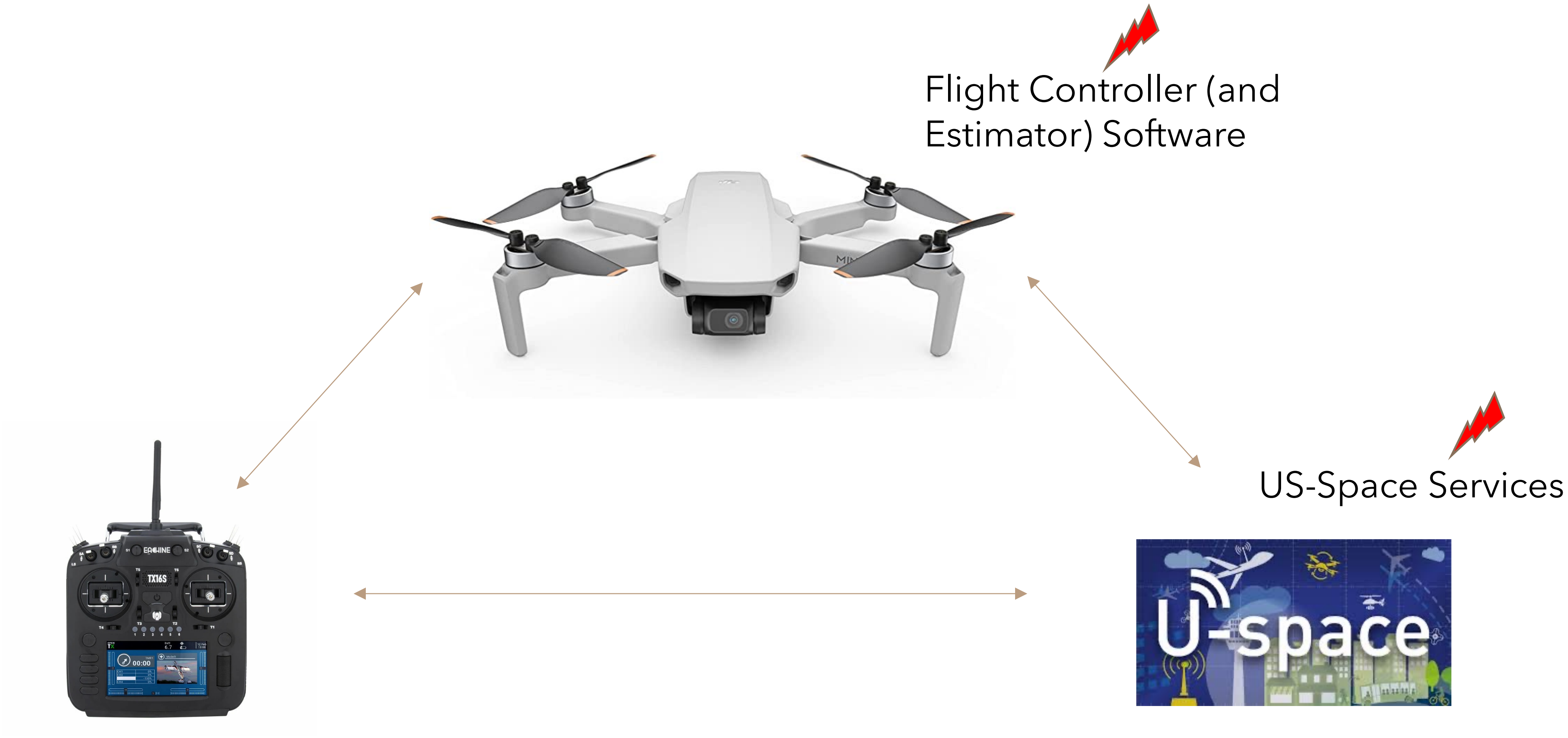
Communication between
tracking service and ground
controller/pilot

Tracking Services

Security Attacks



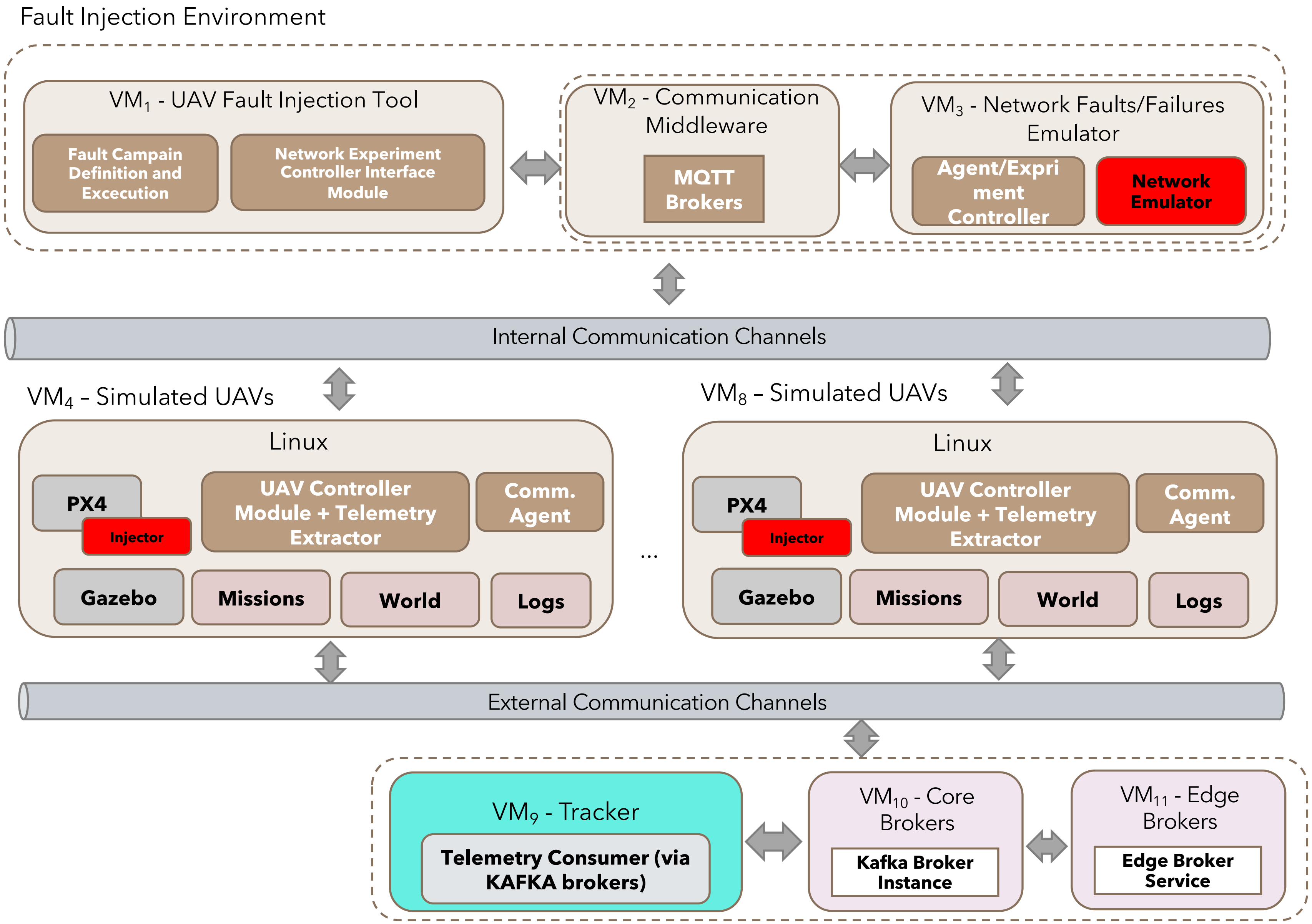
Software component/service failures



Artificial Intelligence (AI) failures

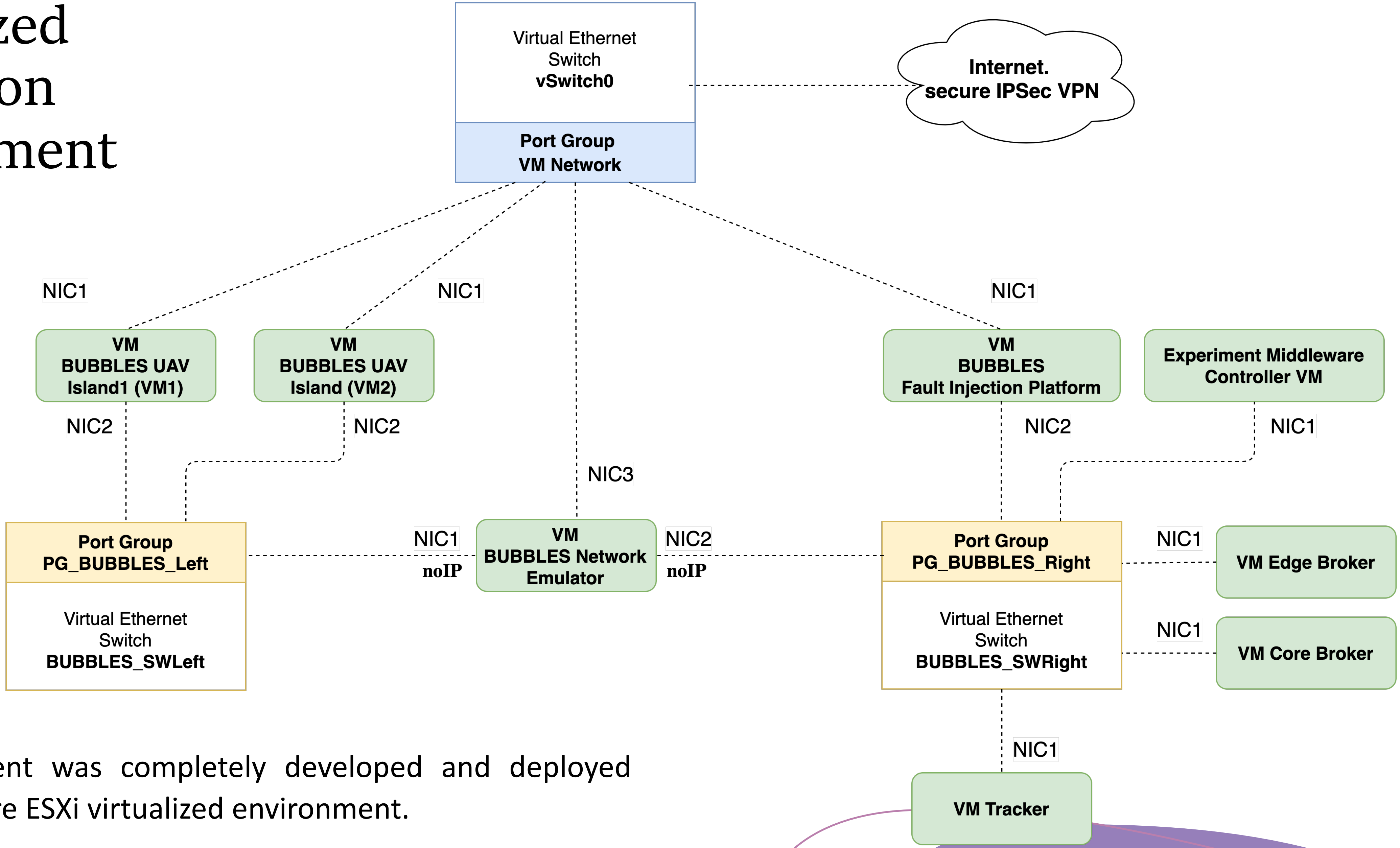
Erroneous Decision made by
AI used in Autonomous Drones

Erroneous Decision made by
AI used in US-Space Services



Evaluation Platform – Logical view

Virtualized evaluation environment



This environment was completely developed and deployed within a VMware ESXi virtualized environment.

Fault model for GPS

Fault type	Test cases	Duration
Fixed Valid values	A set of fixed values, each time one of these fixed values is injected during the fault injection campaign. (100 values at this stage)	2sec, 5sec, 10sec, 30sec
Fixed Invalid values	A set of fixed values, each time one of these fixed values is injected during the fault injection campaign. (10 values at this stage)	2sec, 5sec, 10sec, 30sec
Delayed values	Does not need user's input value	2sec, 5sec, 10sec, 30sec
Freeze values	Does not need user's input value	2sec, 5sec, 10sec, 30sec
Random value	Does not need user's input value	2sec, 5sec, 10sec, 30sec
Min value	Does not need user's input value	2sec, 5sec, 10sec, 30sec
Max Value	Does not need user's input value	2sec, 5sec, 10sec, 30sec

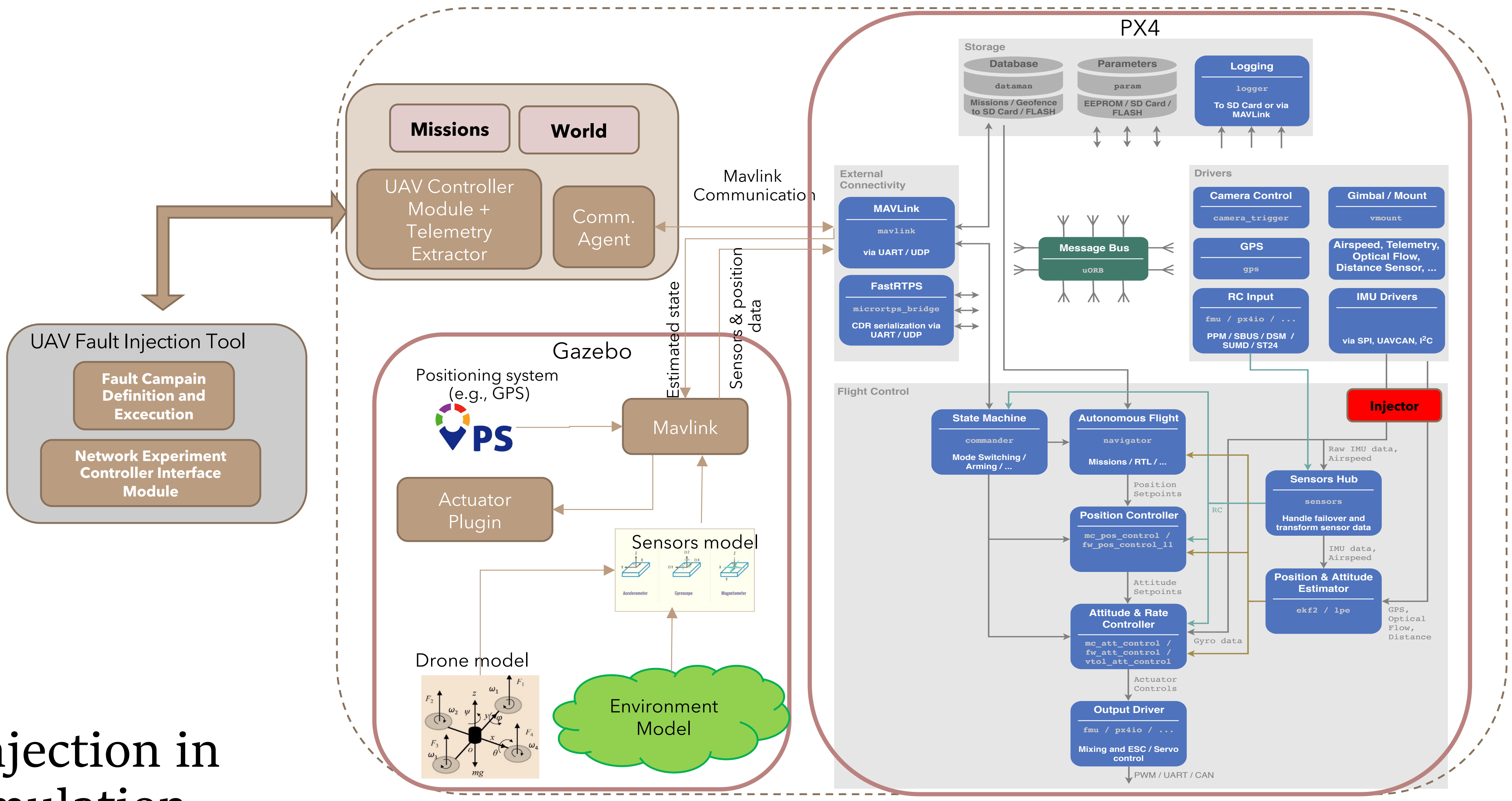
Fault Model for **GPS**

Fault type	Test cases	Duration
Random Longitude	Does not need user's input value	2sec, 5sec, 10sec, 30sec
Random Latitude	Does not need user's input value	2sec, 5sec, 10sec, 30sec
Random Position	Does not need user's input value	2sec, 5sec, 10sec, 30sec
GPS delay	Does not need user's input value	2sec, 5sec, 10sec, 30sec
Force landing	Does not need user's input value	2sec, 5sec, 10sec, 30sec
Hijack with a second UAV	Does not need user's input value	2sec, 5sec, 10sec, 30sec
Hijack with attacker's specified position	Does not need user's input value.	2sec, 5sec, 10sec, 30sec

Fault Model for **IMU Sensors**

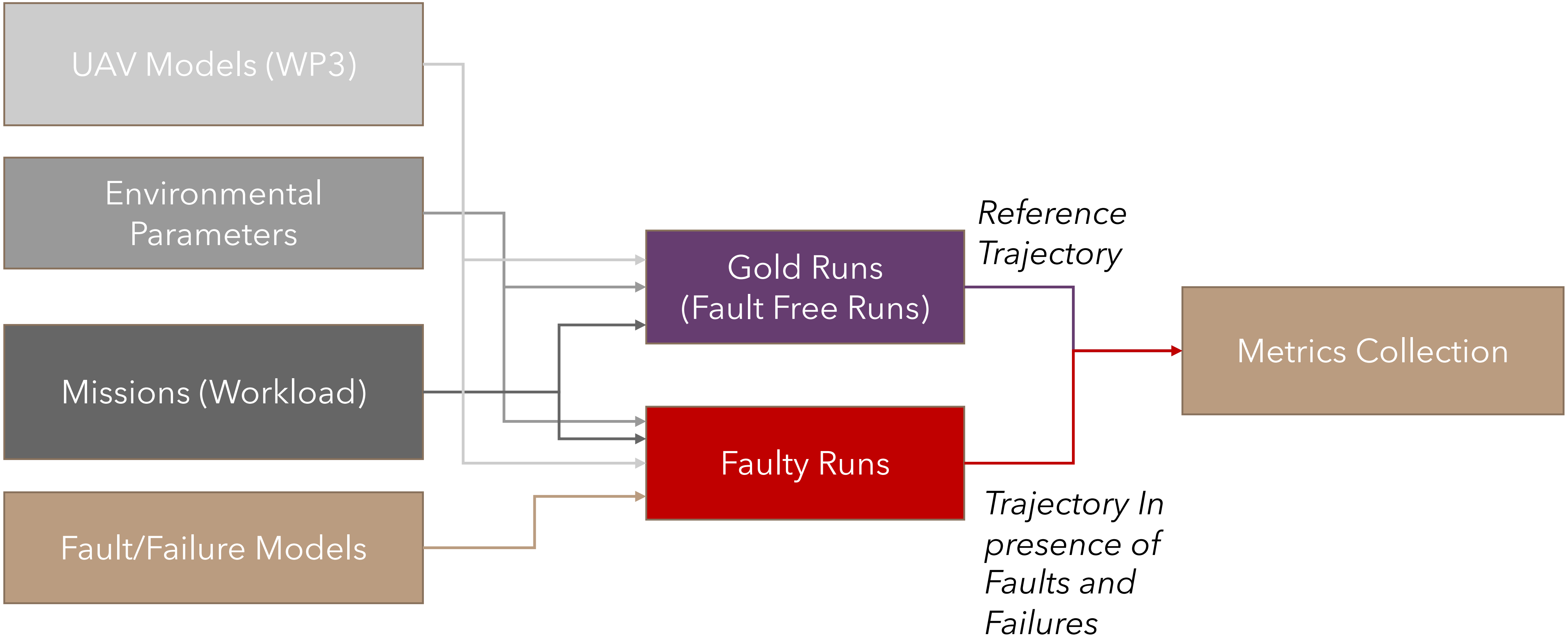
- Accelerometer
- Gyrometer

Fault	Description	Can be represented by	References
Instability	This fault is caused by random values and can be due to factors like radiation or temperature	Random values	[19], [20], [21], [22]
Bias error	This fault is caused by noise and can happen due to factors like old sensors or temperature	Noise	[19], [22], [23], [24]
Gyro drift	This fault is a constant error in measurement and can be caused by factors like old sensors, noise, or bias due to temperature	Noise	[19], [20], [25], [26]
Acc drift	This fault is a constant error in measurement and can be caused by factors like old sensors, noise, or bias due to temperature	Noise	[19], [20], [27], [28]
Constant output	This fault is caused by a lag in updating and getting the same frozen values constantly	Freeze values	[19]
Damaged IMU	This fault occurs when the IMU has been damaged due to old age or external factors, causing failure in all IMU sensors	No updates / zeros	[29], [30]
Gyro failure	This fault occurs when the gyro sensor has been damaged or has failed	No updates / zeros	[30], [31], [32], [33]
Acc failure	This fault occurs when the acc sensor has been damaged or has failed	No updates / zeros	[30], [31], [34]
Acoustic attack	This fault occurs when the drone is attacked by powerful broadband pulsed or Continuous Wave (CW) acoustic energy, or by narrowband CW. It can cause the drone to lose control and crash	Random values	[35], [36]
False data injection	This fault occurs when fake series of data are injected	Fixed values	[37], [38], [39]
Physical isolation	This fault occurs when one or all sensors are attacked to stop responding	No updates / zeros	[40]
Hardware trojan	This fault occurs when the electronic hardware is modified (e.g., tampering with the hardware circuit, resizing the logic gate, etc.)	Fixed values	[41]
Malicious software	This fault occurs when the Ground Control Station and the Flight Controller are prone to malicious software. It can lead to the loss of sensitive data and control of the operated UAV system	Zeros / Random Values	[35]
OS system attack	This fault occurs when potential attacks against civilian or military missions happen through the Flight Controller's system software	Min/Max/Fixed values	[42]



Fault injection in UAV simulation environments

General Assessment Process



Analysis of the Results

- Two sets of analysis:
  - Analysis of the **impact of fault on one single mission** by comparing the gold run trajectory of the mission with the faulty trajectory.
  - Analysis of the **impact of fault on one scenario** (with several missions) by comparing the **number of conflicts and conflict rate** of the gold run scenario with the faulty scenario.

Analysis of the impact on a single mission

- The faults may affect on the following aspect of a mission:
  - **Completion of the mission**
  - **Duration of the mission**
  - **Trajectory of the mission** (Violation form separation minima)
- Failure models:
  - **No effect**: the mission is finished, and the injected fault had no effect on the above aspects
  - **Minor effect – No safety Violation**: the mission is finished but it took more time than gold run trajectory/deviated from the reference trajectory but **still inside the volume.**
  - **Critical effect – Safety Violation**: the mission is finished but it is deviated from the reference trajectory and **went outside of the volume**.
  - **Drastical effect - Safety Violation**: the mission did not finish (Failsafes is activated (minimal safety violation), abrupt landing or crash (safety violation), Lost control of UAV (safety violation)) → **(it would be outside the scope of the TLS defined for mid air collisions)**

Analysis of the impact on one Scenario

When comparing the gold run trajectories of a scenario with the faulty trajectories, we can look at:

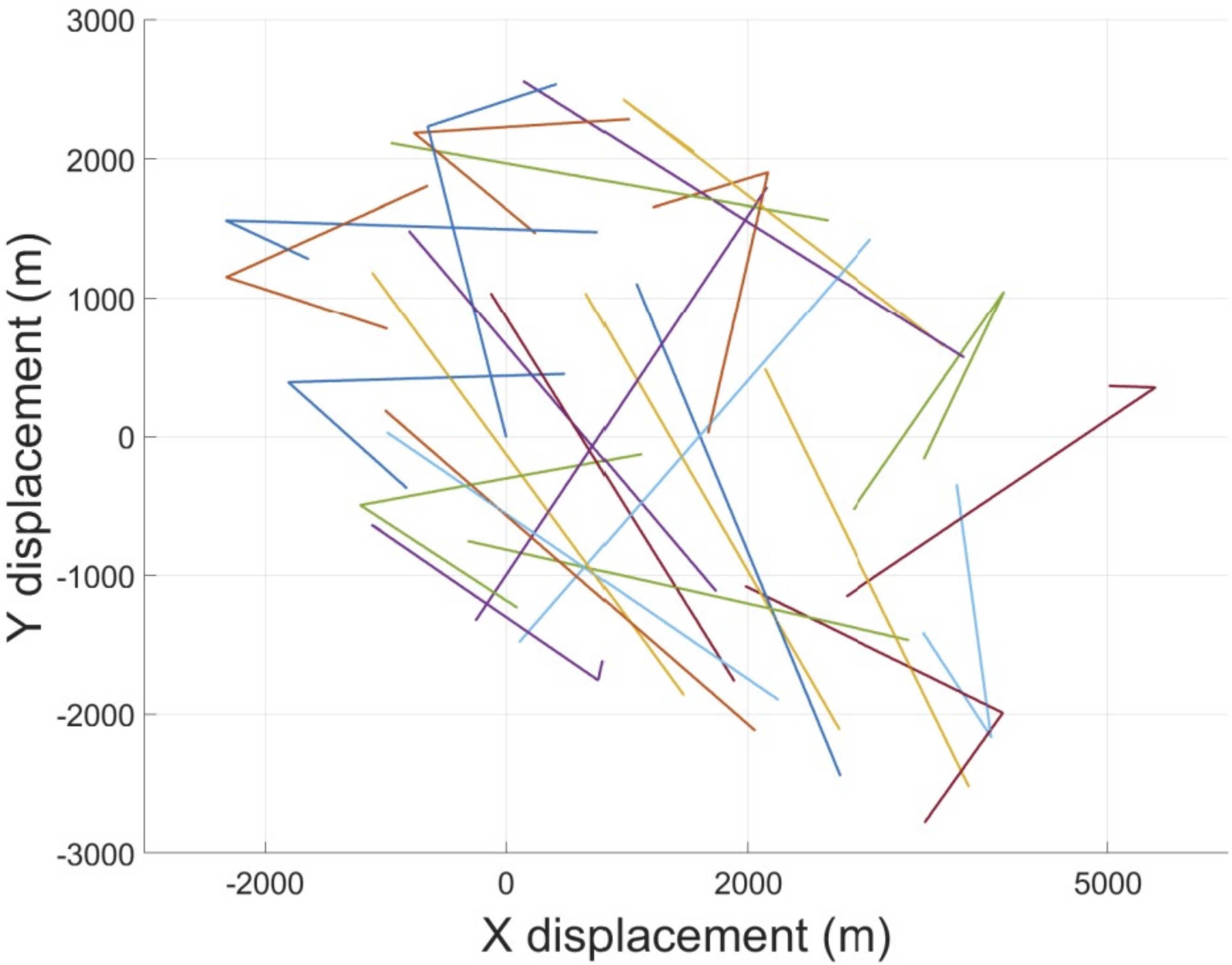
- **Occurrence of collision**
- **Number of conflicts**
- **Conflict rate**
- **Total duration of conflicts**

- Accordingly, the Failure Models can be defined as follows:
  - **No Effect -** no changes in the above aspects
  - **Visible Effect - Impact on the target level of safety** : the number of conflicts increases/conflict rate increases (the effect on TLS depends on the magnitude of the increase in the conflict rate; need to define boundaries)
  - **Critical Effect - Impact on the target level of safety** : When a collision occur (impact on the target level of safety)

Example: Scenarios and Missions

- Valencia, Spain
- High density
  - 28 drones
  - 25 km2 area
- 1 hour scenario

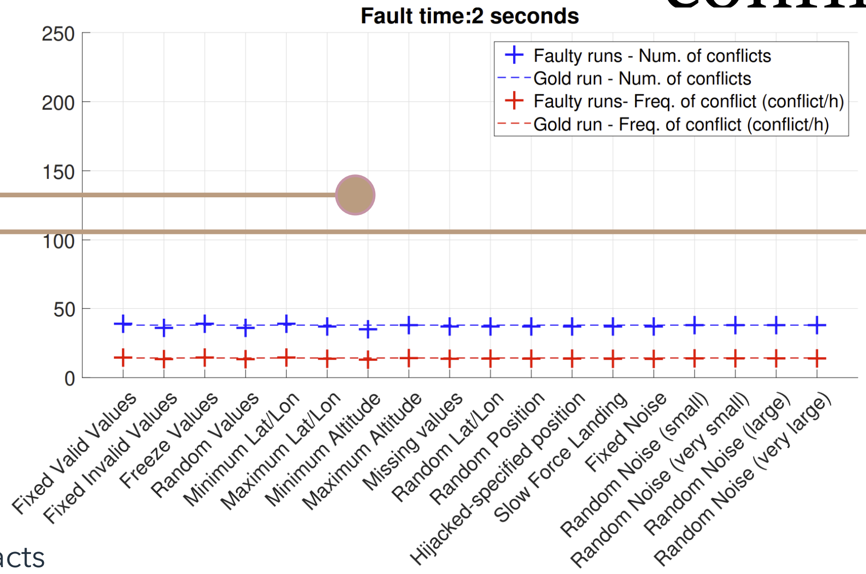
- Gold Runs
- Faulty runs
  - 4 Durations:
    - 2 seconds
    - 5 seconds
    - 10 seconds
    - 30 seconds

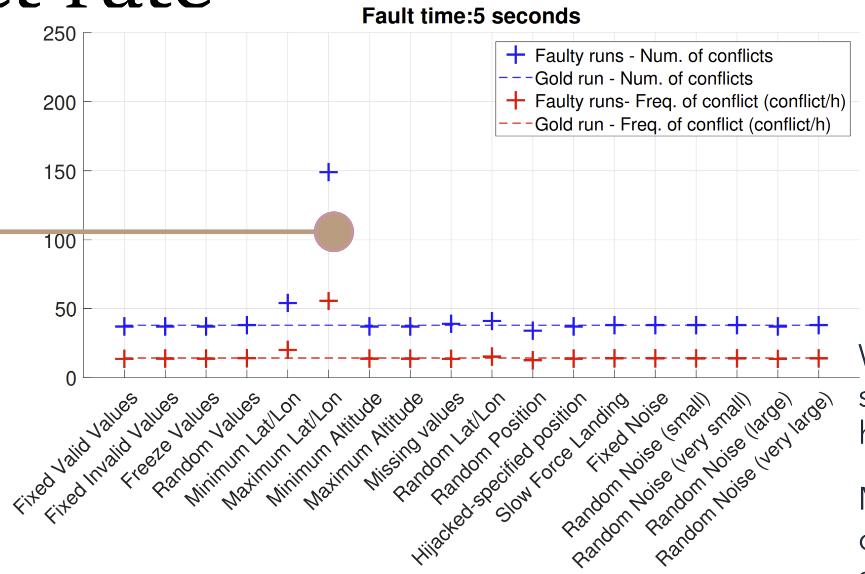


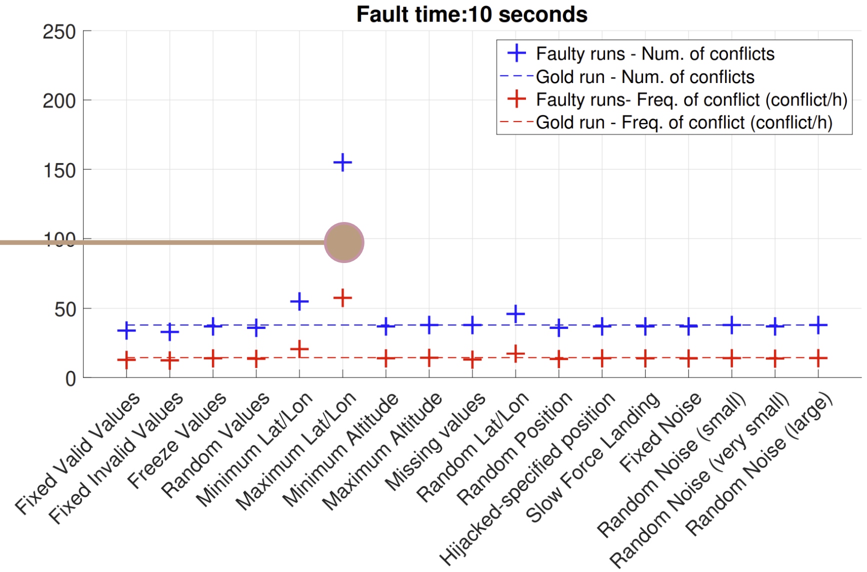
Results for GPS Faults - Impact on conflict rate

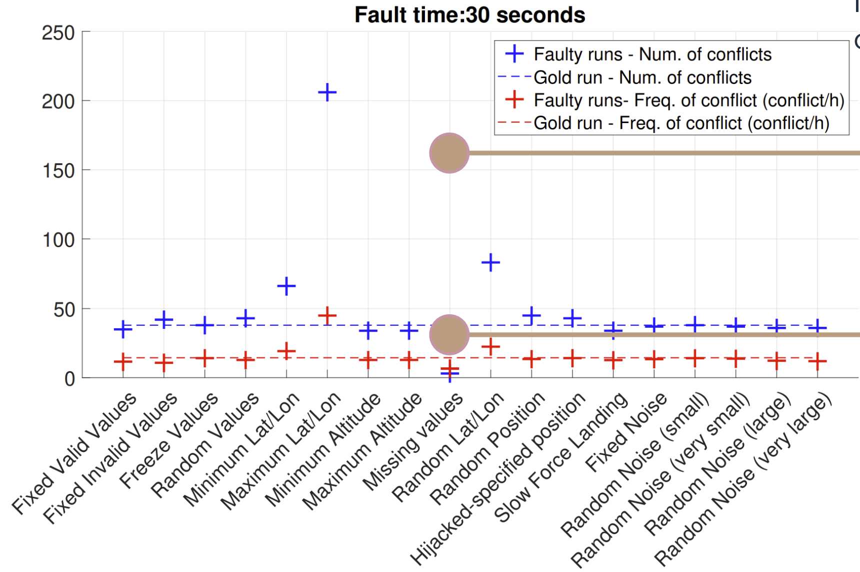
When injected for 2 seconds The difference between the faulty and golden run are negligible (kalman filter absorbs the effect of short duration failures).

Max and Min values impacts more than others









When injected for 30 seconds, all faults show higher impact

Missing GPS value caused the drone to activate failsafe and land, so we have low conflict rate

Are UAVs Flight Controller Reliable?

- Findings:
  - For **small faults** (e.g., Fixed Small Noise or Freeze Values), **EKF** is efficient and can tolerate/compensate the faults
  - **For bigger anomalies** (e.g., Invalid Values or Random Values) in the GPS data, **EKF is not effective at all**
  - For GPS faults **lasting 30 seconds or more**, we observed a noticeable effect
    - This represents a clear **vulnerability** since GPS can be subject of cyber attacks such as spoofing.

Results with of IMU Faults

- In general **IMU** is **more critical** than GPS

Injection Duration	Inner Bubble Violations (#)	Outer Bubble Violations (#)	↓ Missions Completed (%)	Duration (sec)	Distance (km)
Gold Run	0	0	100%	491.26	3.65
2 seconds	18.30	17.81	20%	188.87	0.98
5 seconds	20.16	16.79	15.23%	146.07	0.81
10 seconds	20.97	19.16	11.42%	151.90	0.69
30 seconds	24.47	21.65	10.47%	154.70	0.75

Most missions are failed

Results of IMU Fault Injection

Injection Type	Inner Bubble Violations (#)	Outer Bubble Violations (#)	↓ Missions Completed (%)	Duration (sec)	Distance (km)
Gold Run	0	0	100%	491.26	3.65
Acc Zeros	23.36	17.5	67.5%	338.67	2.45
Acc Noise	25.23	13.48	60%	306.11	2.22
Acc Freeze	23.40	15.82	42.5%	244.09	1.80
Acc Random	20.13	16.34	5%	110.76	0.55
Acc Min	20.57	24.25	5%	137.18	0.51
Acc Max	41.32	35.32	2.5%	103.35	0.73
Acc Fixed Value	40.30	36.51	2.5%	103.99	0.75
Gyro Zeros	18.88	18.15	40%	223.21	1.20
Gyro Fixed Value	17.51	15.90	17.5%	159.57	0.49
Gyro Freeze	19.11	21.5	15%	145.92	0.98
Gyro Noise	16.01	20.67	10%	156.43	0.52
Gyro Random	16.75	16.36	2.5%	169.28	0.47
Gyro Max	16.32	14.13	2.5%	135.50	0.44
Gyro Min	19.73	14.86	0%	104.41	0.47
IMU Max	14.19	17.34	17.5%	212.30	0.46
IMU Zeros	18.17	16.55	2.5%	104.43	0.52
IMU Noise	21.19	17.61	2.5%	143.73	0.48
IMU Random	16	15.03	2.5%	104.66	0.53
IMU Fixed Value	15.67	14.28	2.5%	110.45	0.53
IMU Min	18.63	17.61	0%	155.08	0.46
IMU Freeze	18.03	16.71	0%	98.93	0.46

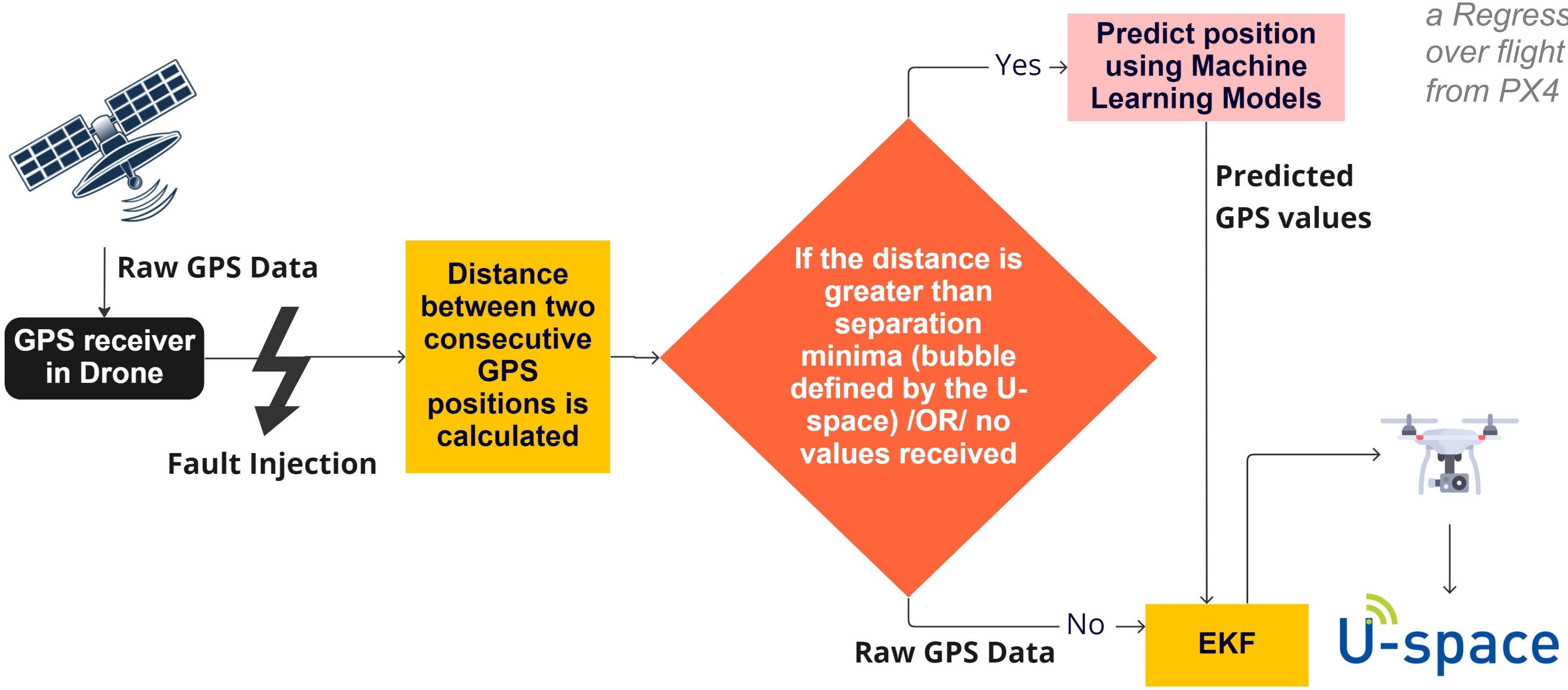
Gyrometer is more critical than Accelerometer

Results of IMU Faults

- Failsafe Activation

Injection Type	Total Missions Failed (%)	Crash (%)	Failsafe (%)
Gold Run	0%	0%	0%
2 seconds	80%	73%	27%
5 seconds	84.77%	73%	27%
10 seconds	88.58%	70%	30%
30 seconds	89.53%	34%	66%
Acc	73.22%	77.2%	22.8%
Gyro	87.5%	63.1%	36.9%
IMU	96.08%	47.2%	52.8%

Can AI help to Tolerate Failures?



a Regression mode built over flight log files collected from PX4 repository

How Can AI help to Tolerate Failures?

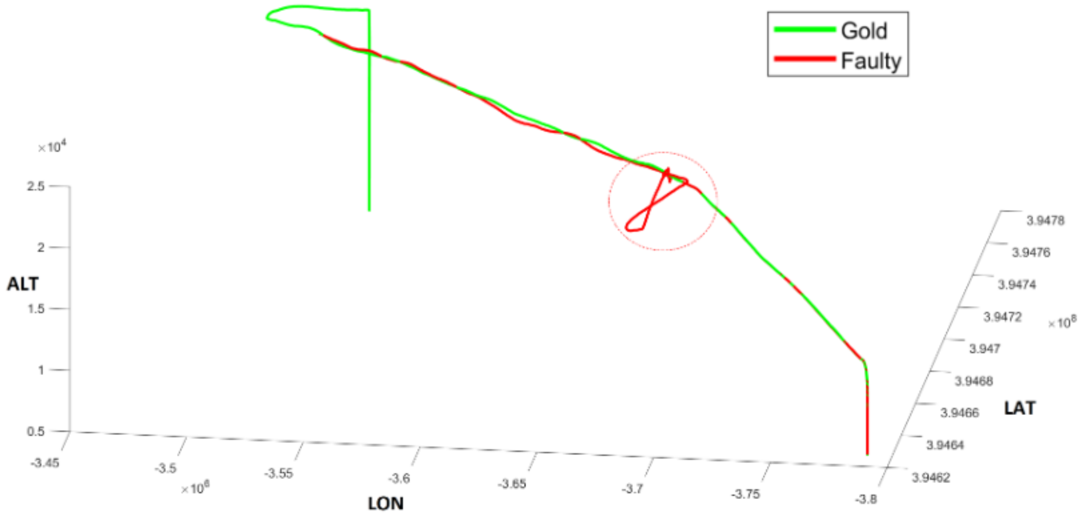


Fig. 6: Trajectory of a UAV in faulty condition, in comparison with the Gold run.

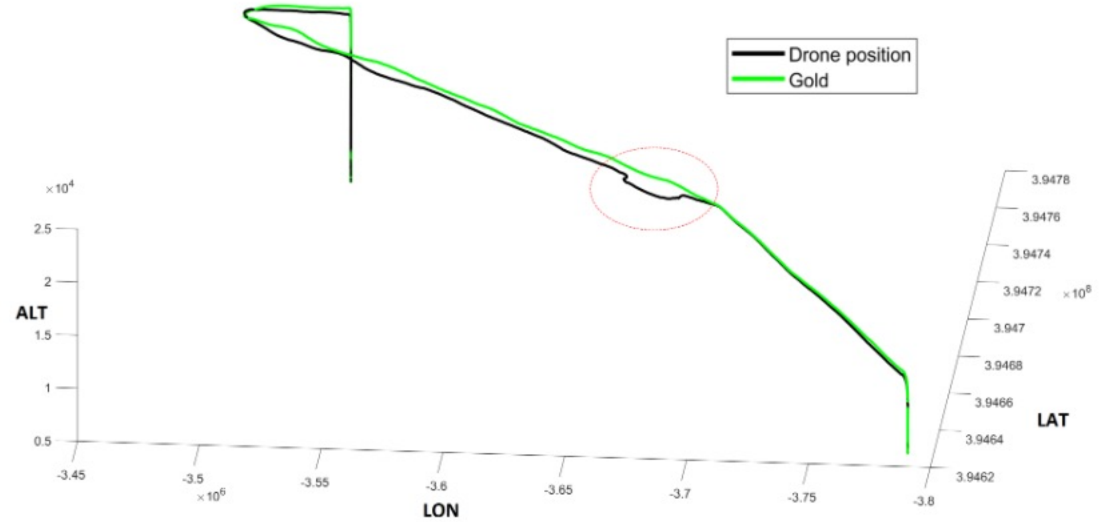


Fig. 7: Trajectory of a UAV with the fault-tolerance mechanism integration in a faulty condition, in comparison with the gold run.

Why AI and not a Physics Model?

$$Position_{current} = Position_{previous} + Speed_{current} * Time$$

$$Speed_{current} = Speed_{previous} + Acceleration_{current} * Time$$

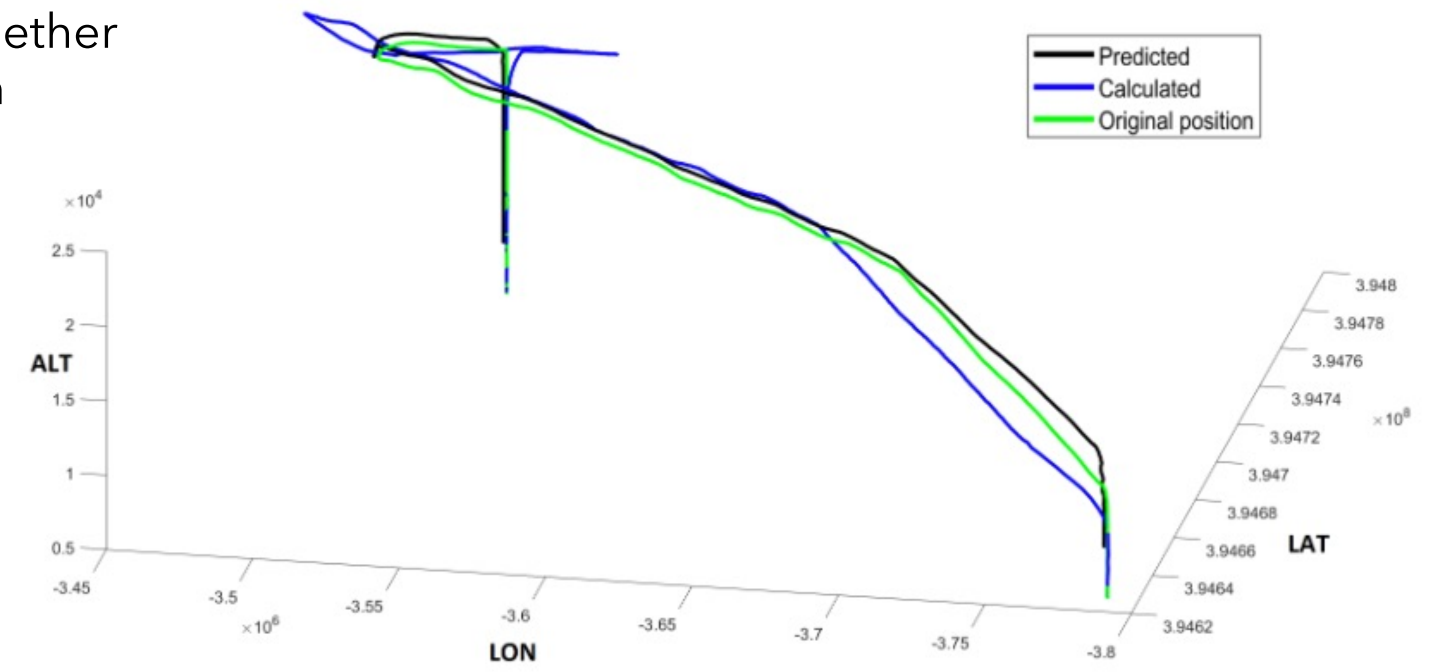
$$Lat_{current} = Lat_{previous} + Speed_Y * Time + \frac{Acceleration_Y * Time^2}{2}$$

$$Lon_{current} = Lon_{previous} + Speed_X * Time + \frac{Acceleration_X * Time^2}{2}$$

$$Alt_{current} = Alt_{previous} + Speed_Z * Time + \frac{Acceleration_Z * Time^2}{2}$$

Why AI and not a Physics Model?

GPS noises and windy whether condition



Physics model outperformed the AI model in the presence of GPS failures

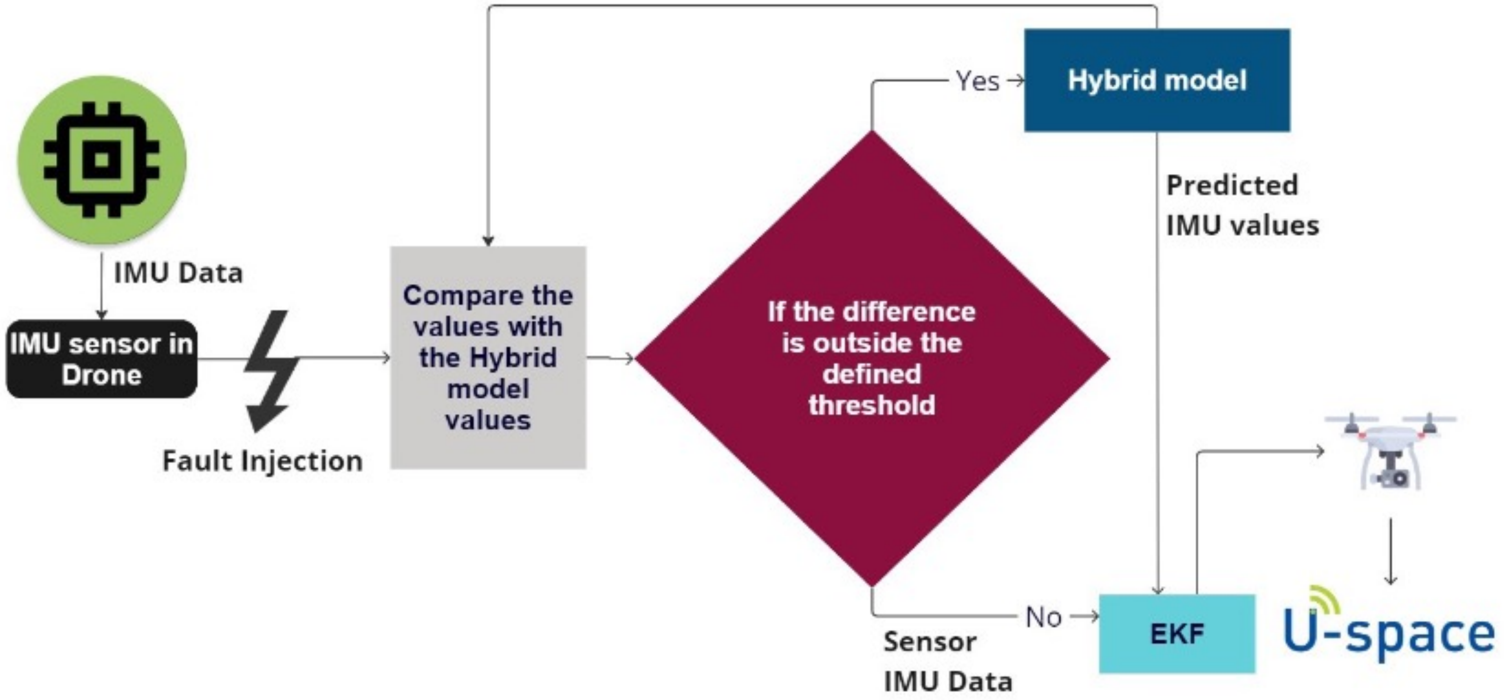
AI and Physics Model for IMU

- AI models for both Accelerometer and Gyrometer
  - Recurrent Neural Network (RNN)
  - Convolutional Neural Network (CNN)
  - Generative Adversarial Network (GAN)
  - Autoencoder
  - Regression
  - Long Short-Term Memory (LSTM) on Regression
  - **LSTM with RNN**

- Physics model
  - Well established models in the literature for both Accelerometer and Gyrometer

Interestingly, **physics model** outperformed the AI model for **accelerometer**
And **AI model** outperformed the physics model for **gyrometer**,

Hybrid Model for IMU fault Tolerance



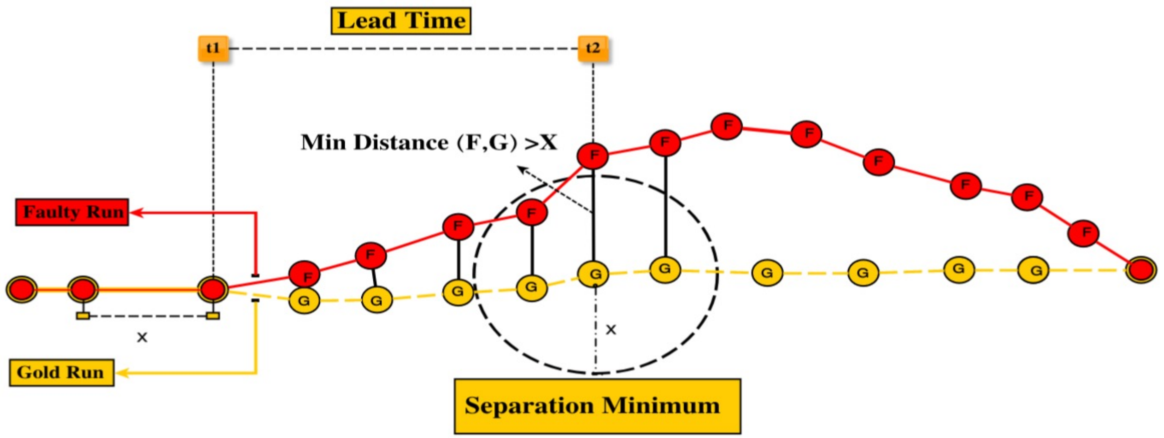
Hybrid Model for IMU fault Tolerance

Type	IBV	OBV	Duration	Distance	Acc Err	Gyro Err	FD Acc	FD Gyro	MD Acc	MD Gyro	Completed
Gold	0.00	0.00	202.34	0.722	0.0000000	0.0000000	-	-	-	-	100%
Small Noise	2.64	0.00	203.98	0.723	0.0000919	0.0002699	-	-	-	-	100%
Small Noise Hybrid	2.40	0.00	203.62	0.723	0.0000913	0.0002834	0.133333	0.740741	78.56	75.19	100%
Medium Noise	13.56	5.00	203.62	0.755	0.0000951	0.0003415	-	-	-	-	80%
Medium Noise Hybrid	2.76	0.00	204.12	0.723	0.0000850	0.0002822	0.000000	0.000000	20.9	15.60	100%
Large Noise	6.03	4.44	158.86	0.524	2.4148614	33.1308037	-	-	-	-	33%
Large Noise Hybrid	0.56	0.00	202.67	0.723	0.0000876	0.0003000	0.001008	0.000544	0.00	0.00	100%

We could complete all the mission successfully

Another Study: Lead Time Analysis

- Failure Prediction
  - Failure: bubble violation
  - Lead time



Category	Fault Type	Average Lead Time	Minimum Injection Duration
Category 1	Maximum Altitude, Minimum Altitude, Force Landing, Hijack By UAVs, and Random Noise.	No Failure	No Failure
Category 2	GPS Failure	5 Seconds	> 5 Seconds
Category 3	Random Value, Zigzag, Invalid Fixed Value Hijack By Fixed Position, Fixed value, Maximum Longitude, and Maximum Latitude.	15 Seconds	> 14 Second
Category 4	Freeze Value, Random Latitude, Minimum Latitude, Minimum Longitude, and Fixed Noise.	44 Seconds	>14 Second

Ongoing Study: U-space Safety Assessment

- Definition and validation of **Safety Metrics**
  - How the metrics should be measures?
    - **Measurement interval**
  - How **sensitive** the metrics are to the influencing factors (environmental or technical, failures or attacks)
  - How effective the metrics are for **Target level of safety**?
    - The correlation of metrics with **Collision rate**


THANK
YOU