

ConfuSense: Sensor Reconfiguration Attacks for Stealthy UAV Manipulation

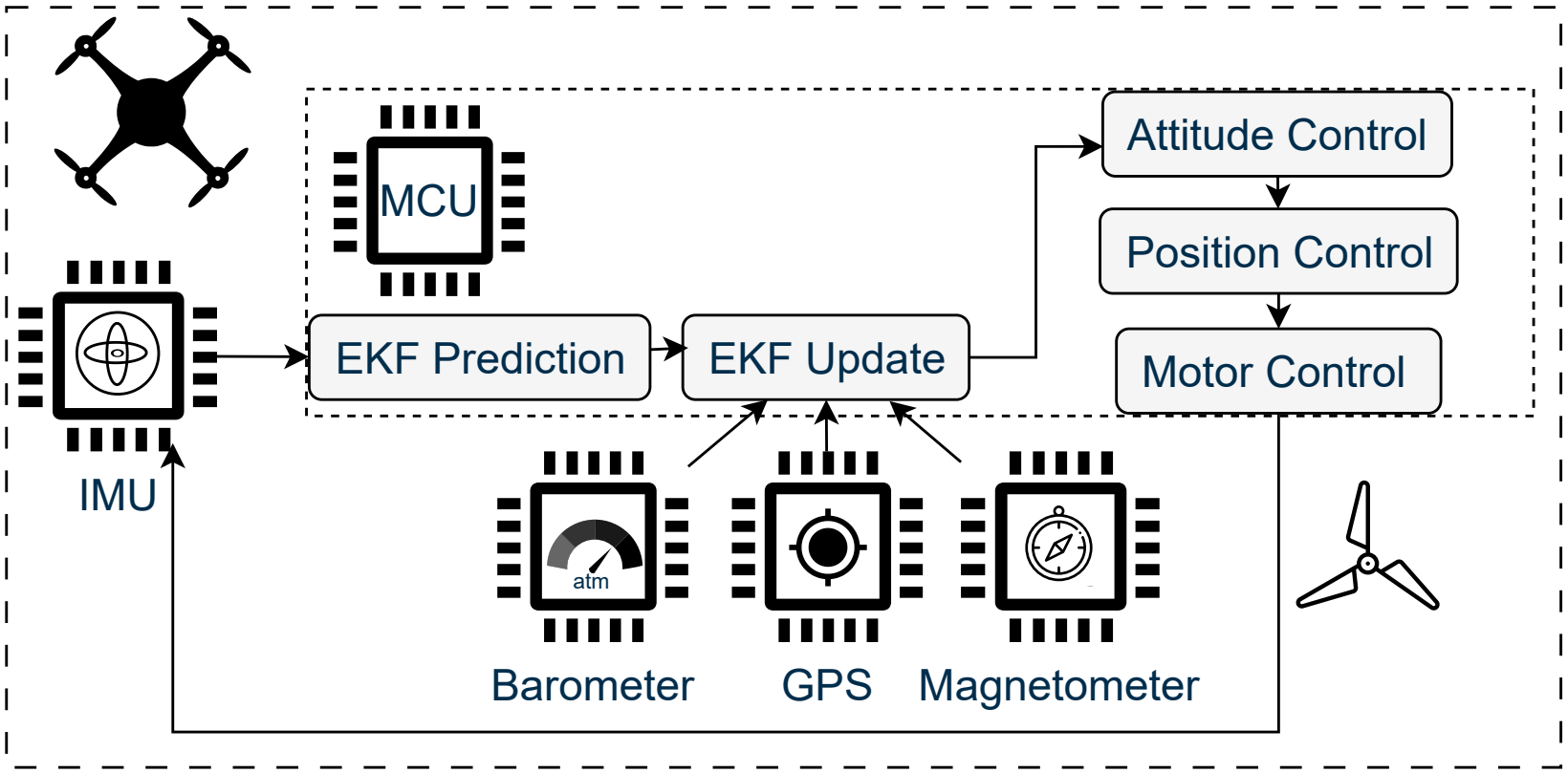
USENIX Symposium on Vehicle Security and Privacy 2025

Alessandro Erba, John H. Castellanos, Sahil Sihag, Saman Zonouz, Nils Ole Tippenhauer

alessandro.erba@kit.edu

11 August 2025

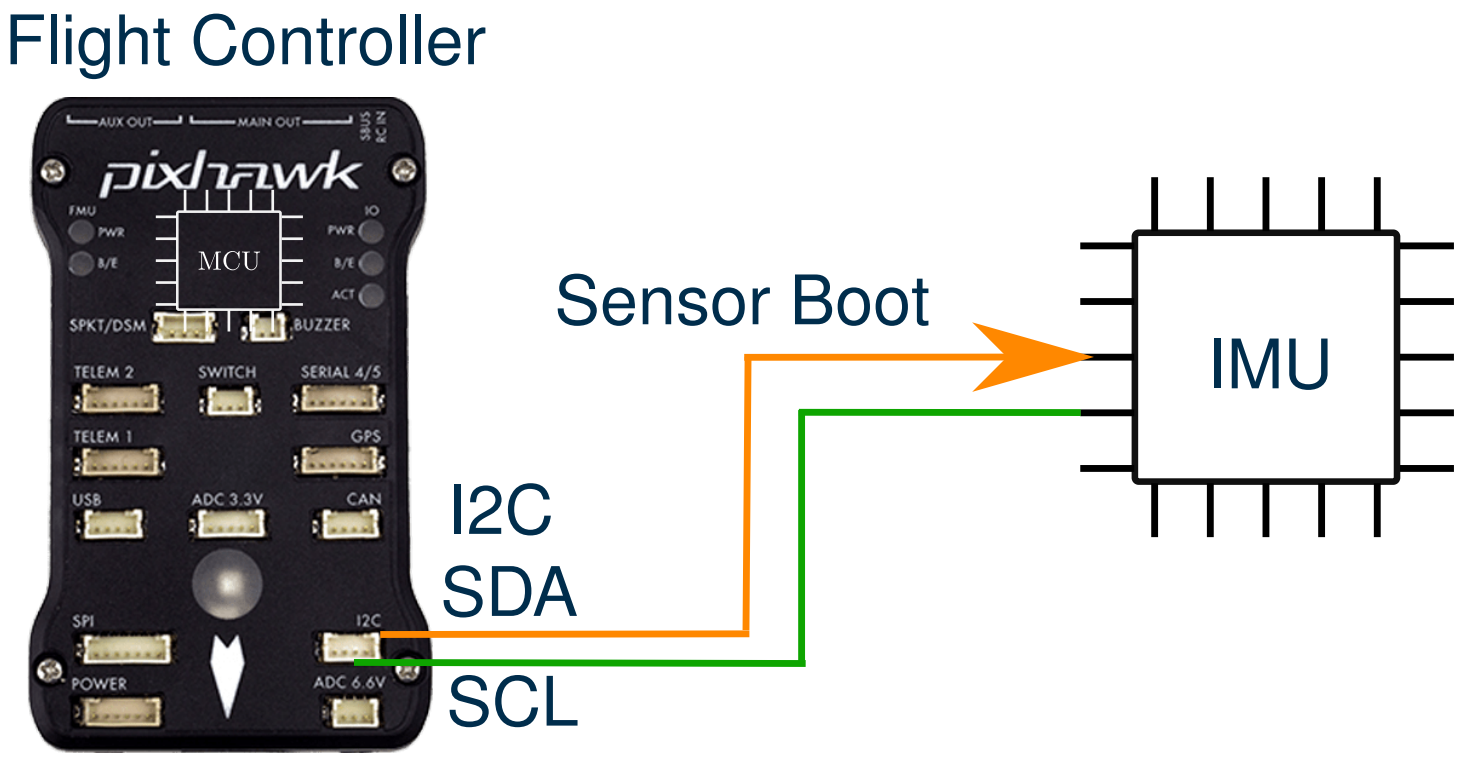
Introduction



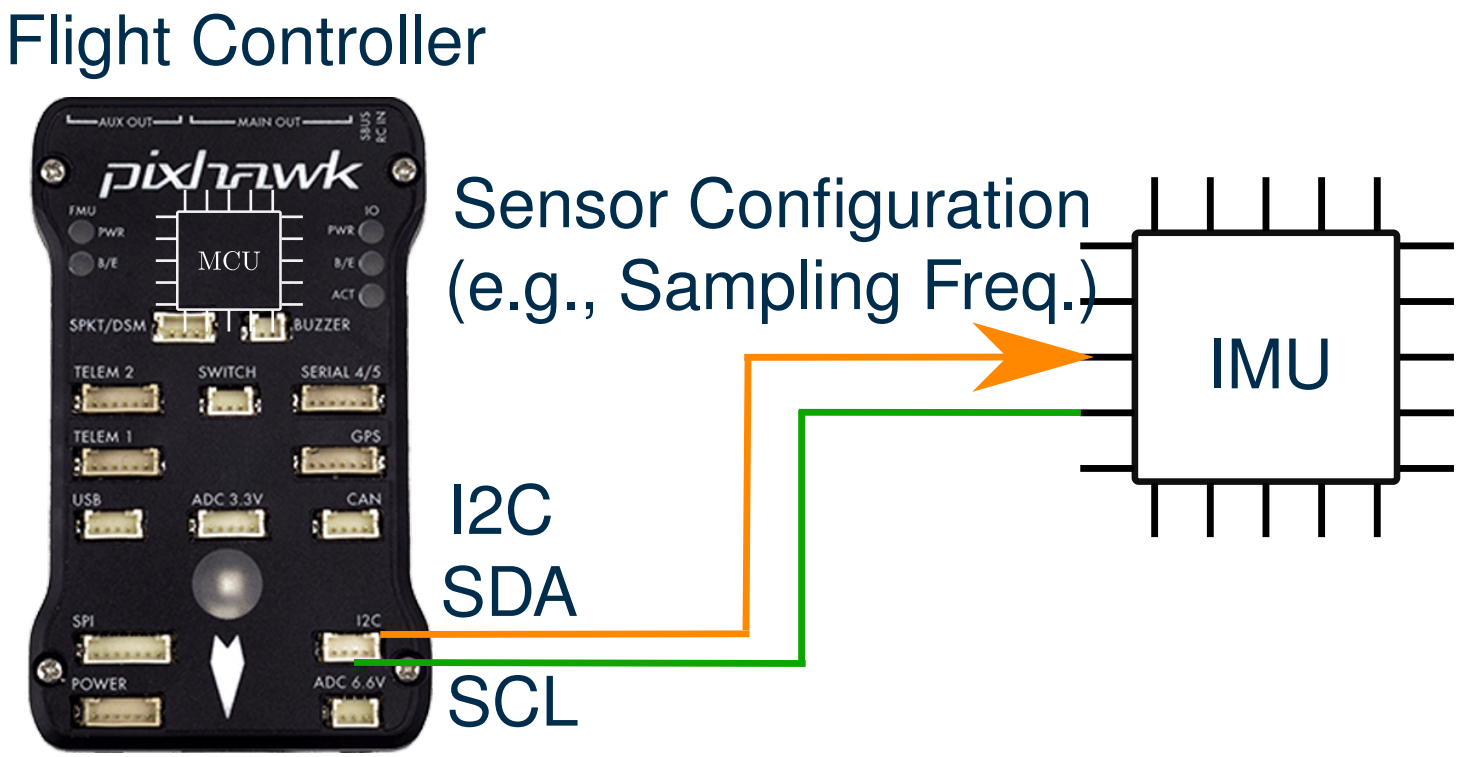
Motivation

Attack Type	Does not require active spoofing	Does not require sensor corruption	Single injection	Persistent Out of Range
GPS, SEC'22 Sathaye et al. 2022	○	●	○	○
IEMI, NDSS'23 Jang et al. 2023	●	○	○	○
Acoustic, NDSS'15 Son et al. 2015	●	○	○	○
Acoustic, NDSS'23 Jeong et al. 2023	●	○	○	○
ConfuSense	●	●	●	●

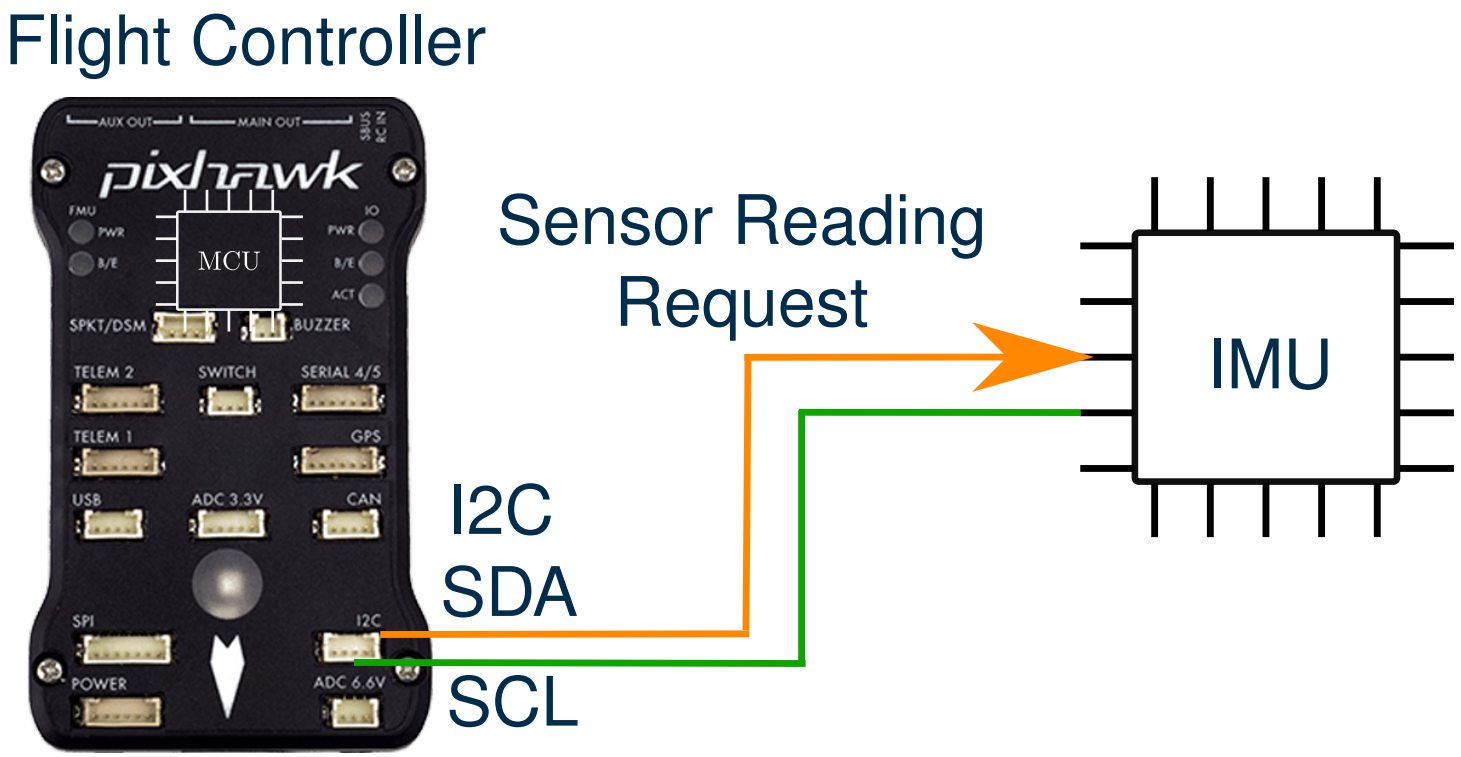
Sensor Configuration



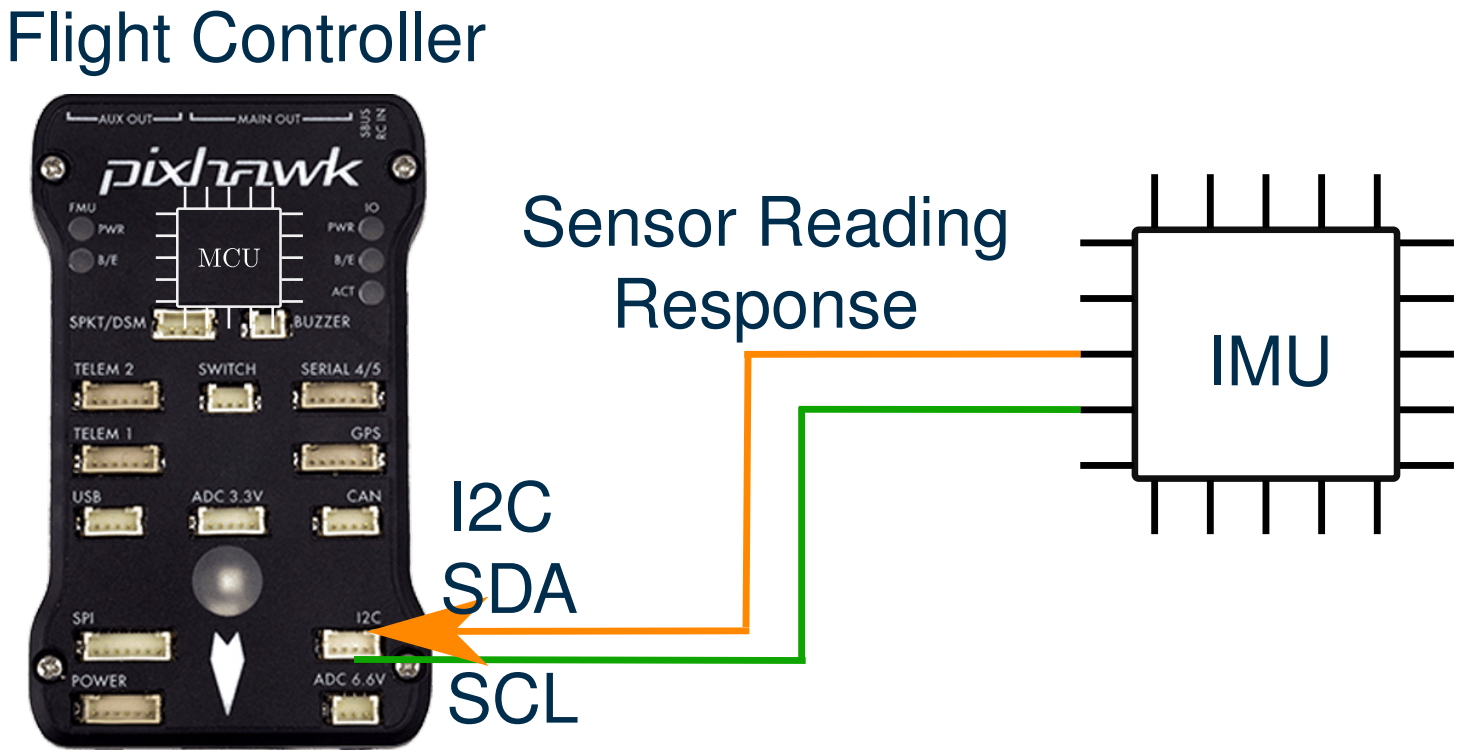
Sensor Configuration



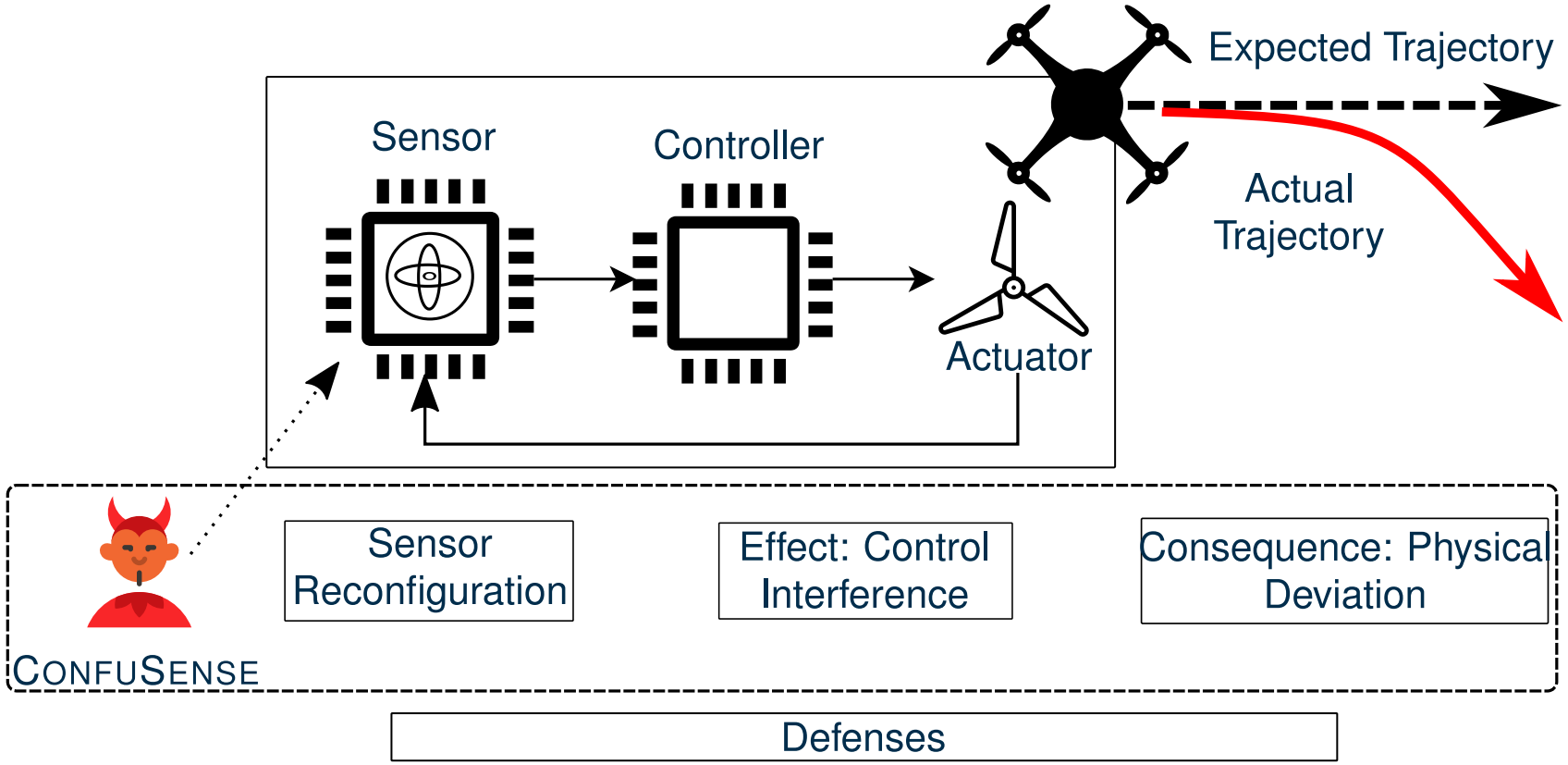
Sensor Configuration



Sensor Configuration



ConfuSense: Overview



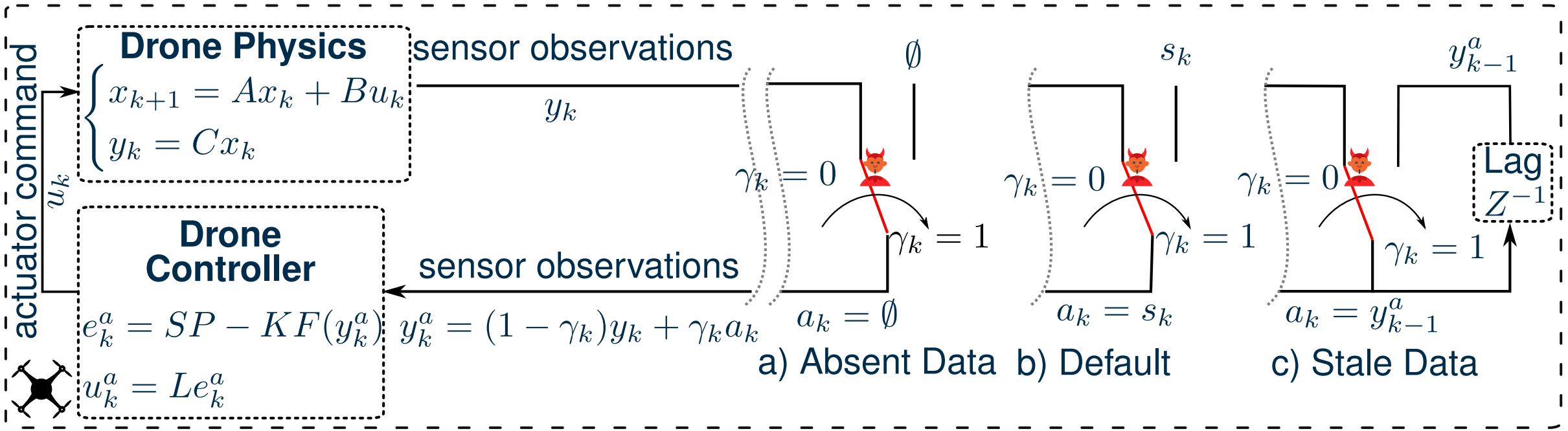
ConfuSense: Sensor Reconfiguration

We identify two target configurations for ConfuSense

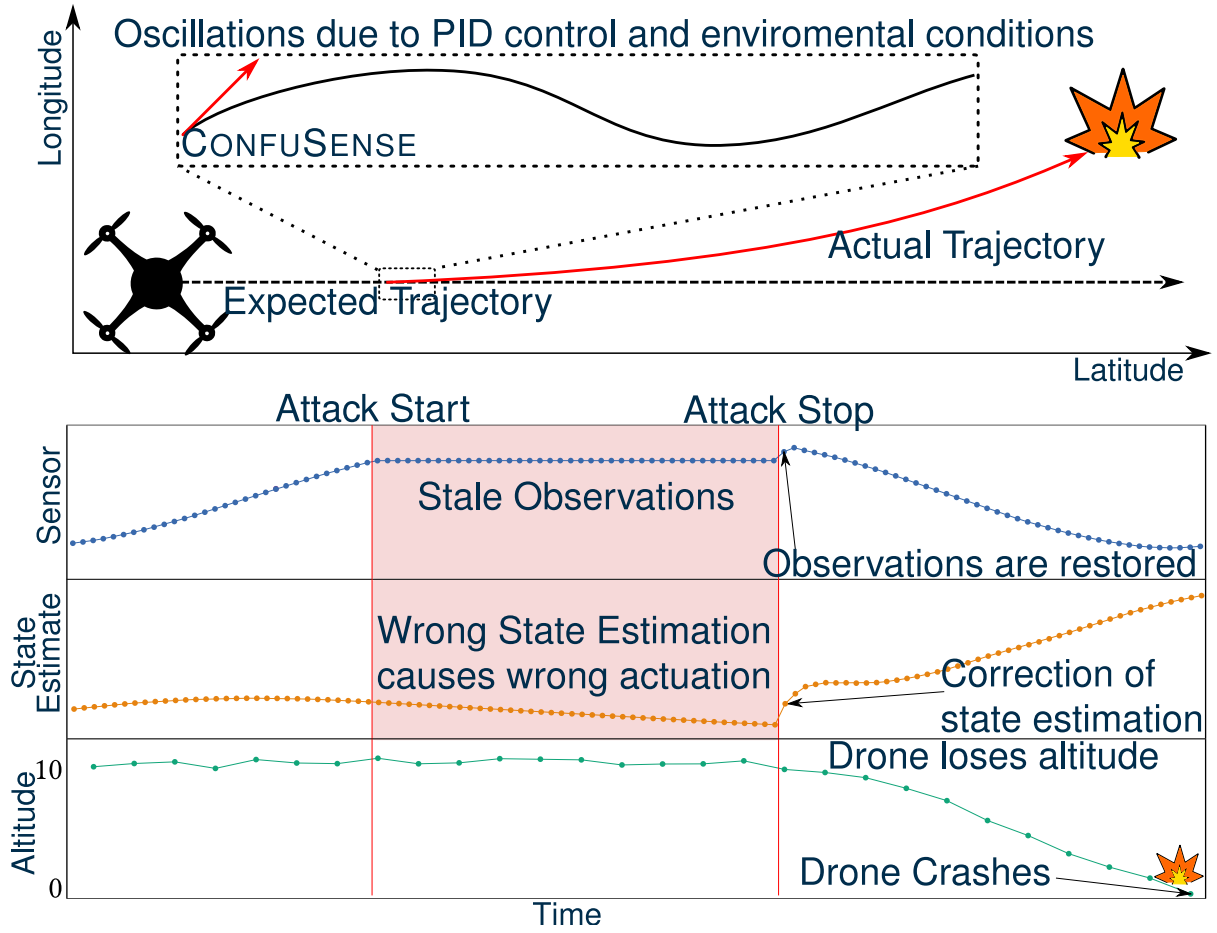
Sensor Power-Save (Suspend)

Sensor Frequency Change

CONFUSENSE: Effect



ConfuSense: Consequence

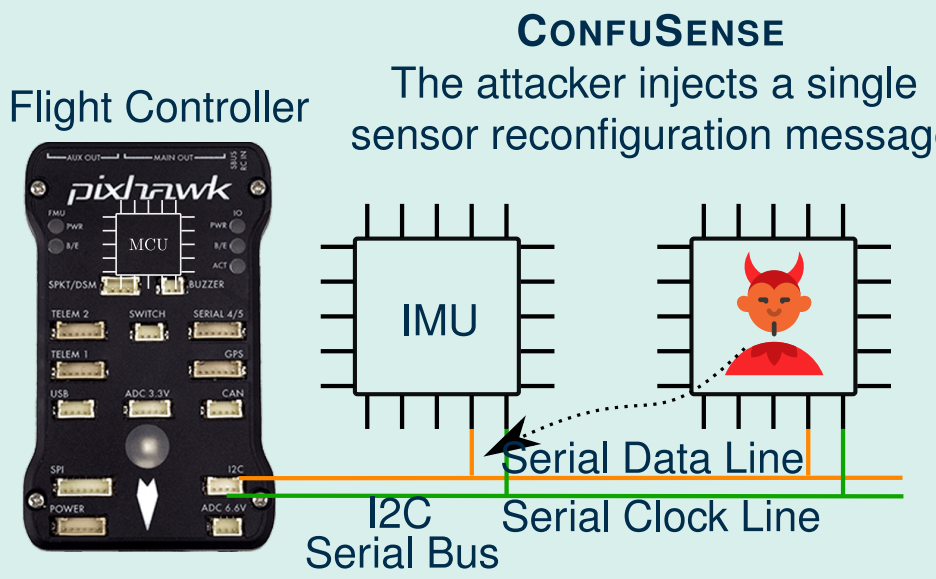


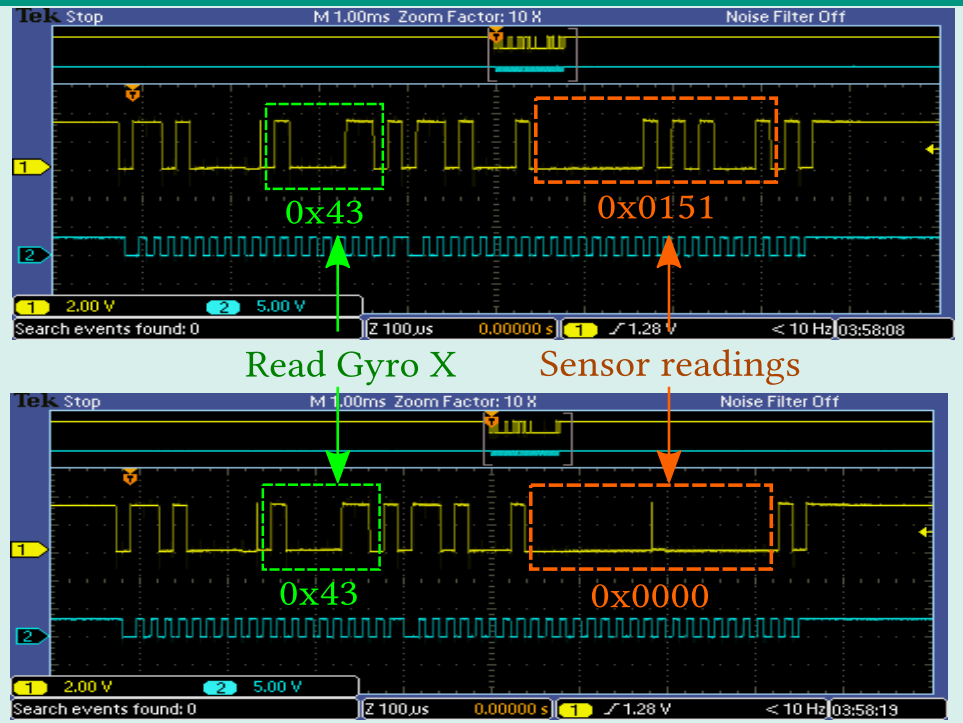
Case Study

RQ1 How can ConfuSense be practically launched on modern flight controllers?

We set up a testbed with an MPU6050 sensor and a Raspberry PI as the controller.

Local sensor reconfiguration



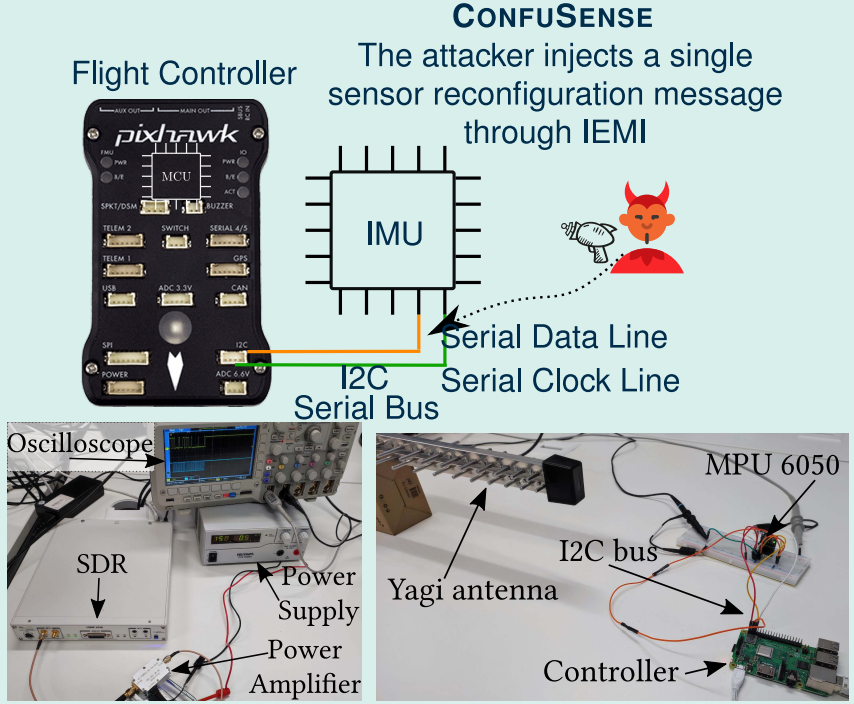


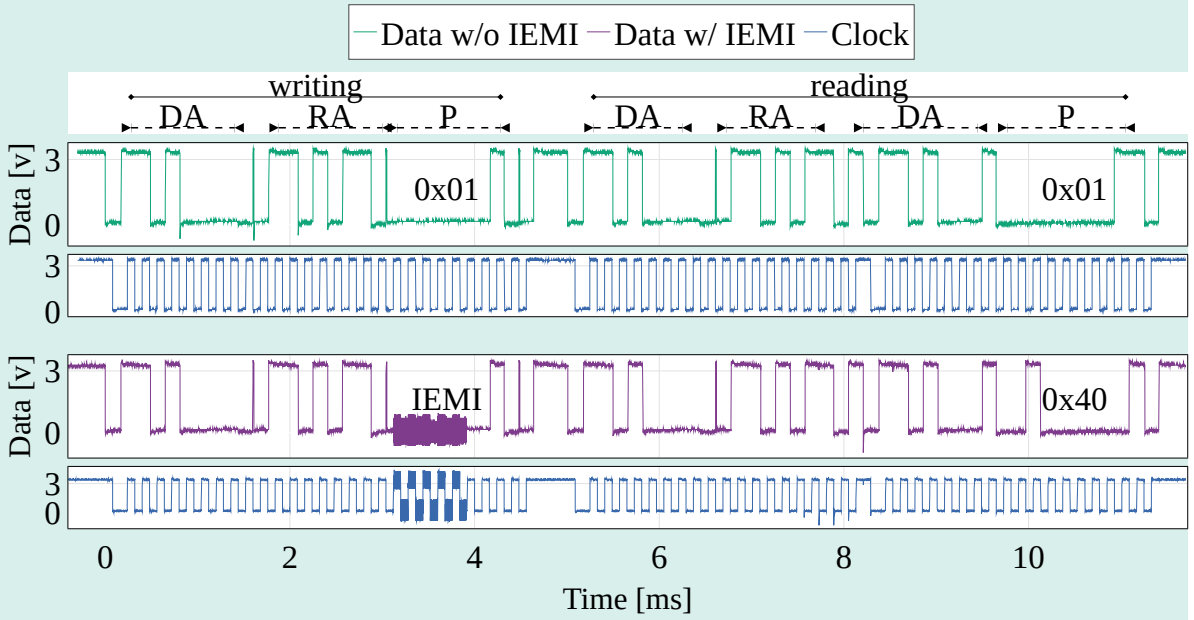
Case Study

RQ1 How can ConfuSense be practically launched on modern flight controllers?

We set up a testbed with an MPU6050 sensor and a Raspberry PI as the controller.

Remote Sensor Reconfiguration



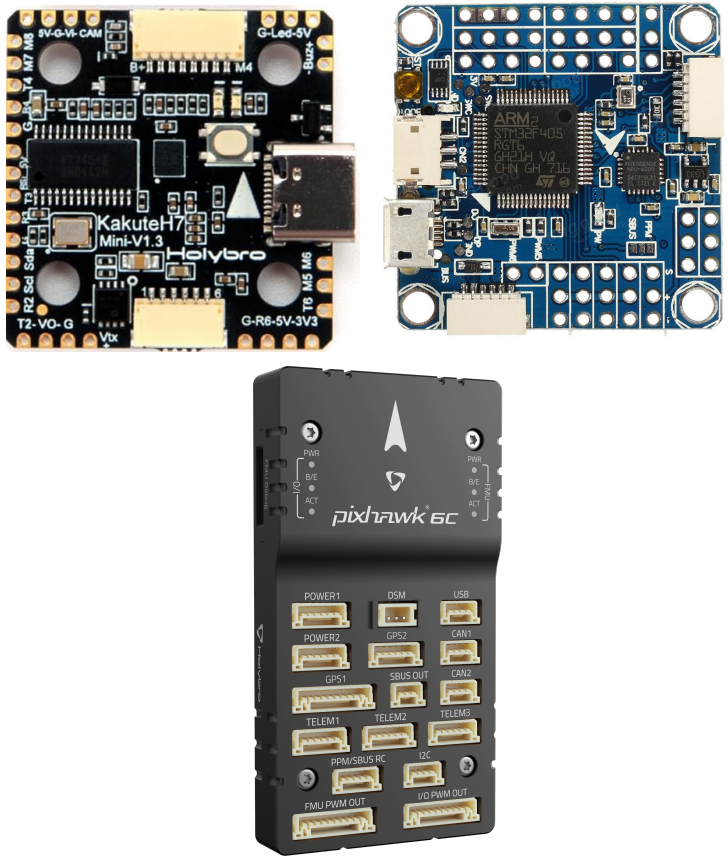


Observed Effect

RQ2 Which interactions between an IMU and the control program are observed?

We test ConfuSense on Ardupilot with three flight controllers:

- Kakute H7 Mini: BMI270 IMU
- Pixhawk 6C: BMI055 IMU and ICM-42688-P IMU
- Omnibus F4: MPU6000 IMU

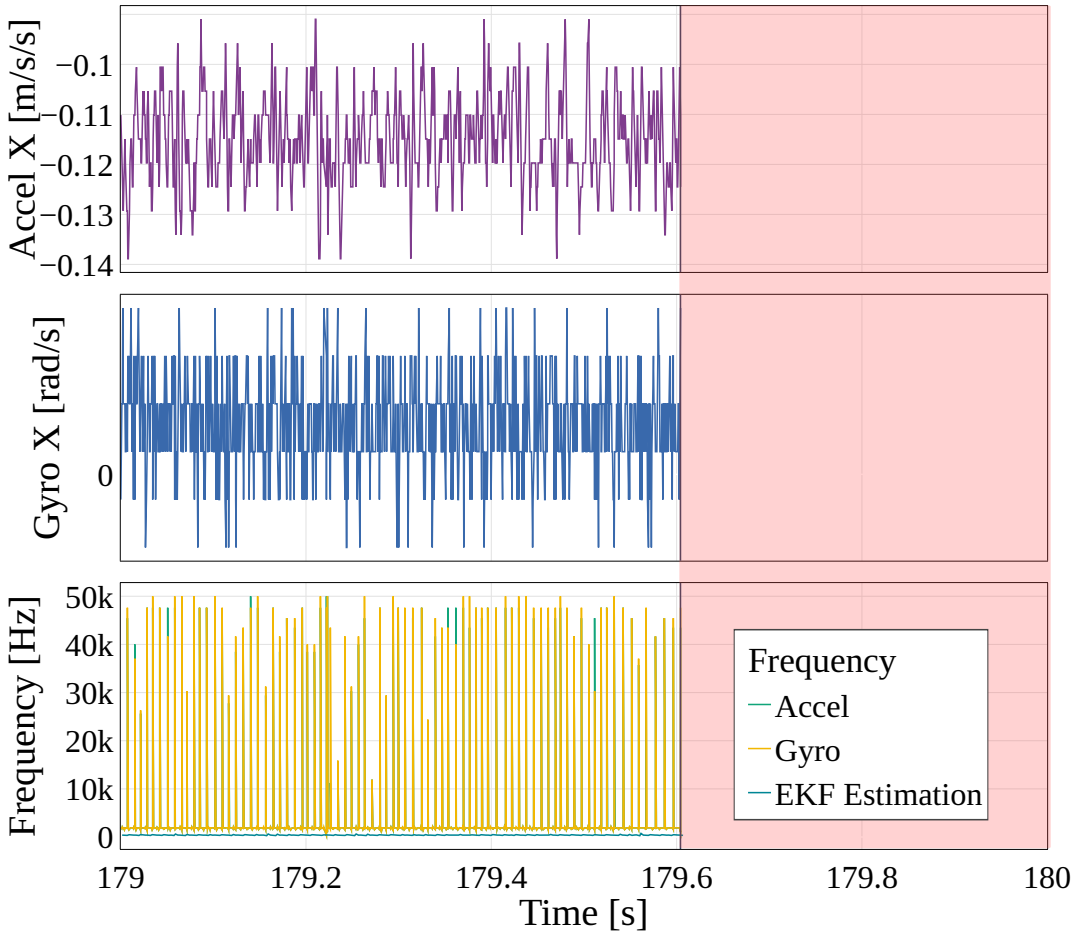


Observed Effect: Results Suspend

RQ2 Which interactions between an IMU and the control program are observed?

IMU Model	Accelerometer Behavior	Gyroscope Behavior
BMI055	Absent Data	Default
BMI270	Default	Default
ICM-42688-P	Absent Data	Absent Data
MPU6000	Default	Default

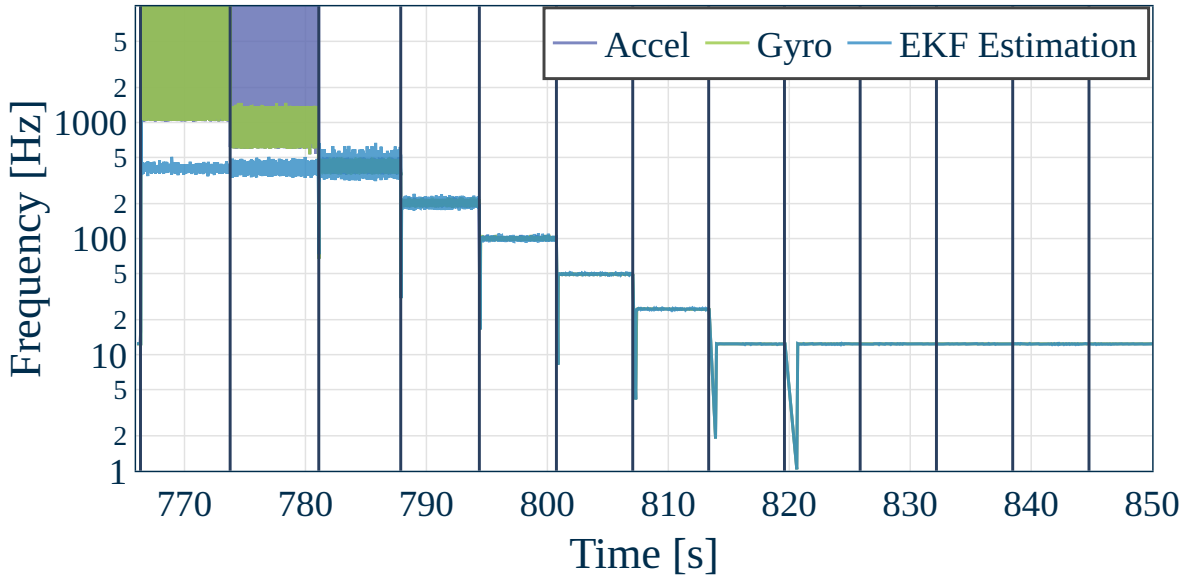
Sensor suspension can induce Absent Data and Default data, which can lead to incorrect EKF Estimation or halt it.



Observed Effect: Results Frequency

RQ2 Which interactions between an IMU and the control program are observed?

Frequency reduction induces the Stale Data Behavior and delays the EKF Estimation



Consequence

RQ3 What is the impact of the proposed ConfuSense on UAVs?

	ConfuSense 1 second				Time to Detect		Time to Crash	
	Undetected		Detected (failsafe)					
	%crash	%compl.	%crash	%land	μ(s)	σ	μ(s)	σ
Stale	0.00	0.00	0.00	100.00	4.99	1.80	N.A.	N.A.
Default	0.00	0.00	100.00	0.00	1.22	0.00	4.56	0.00
Absent	**100.00**	0.00	0.00	0.00	N.A.	N.A.	4.22	0.01

Consequence

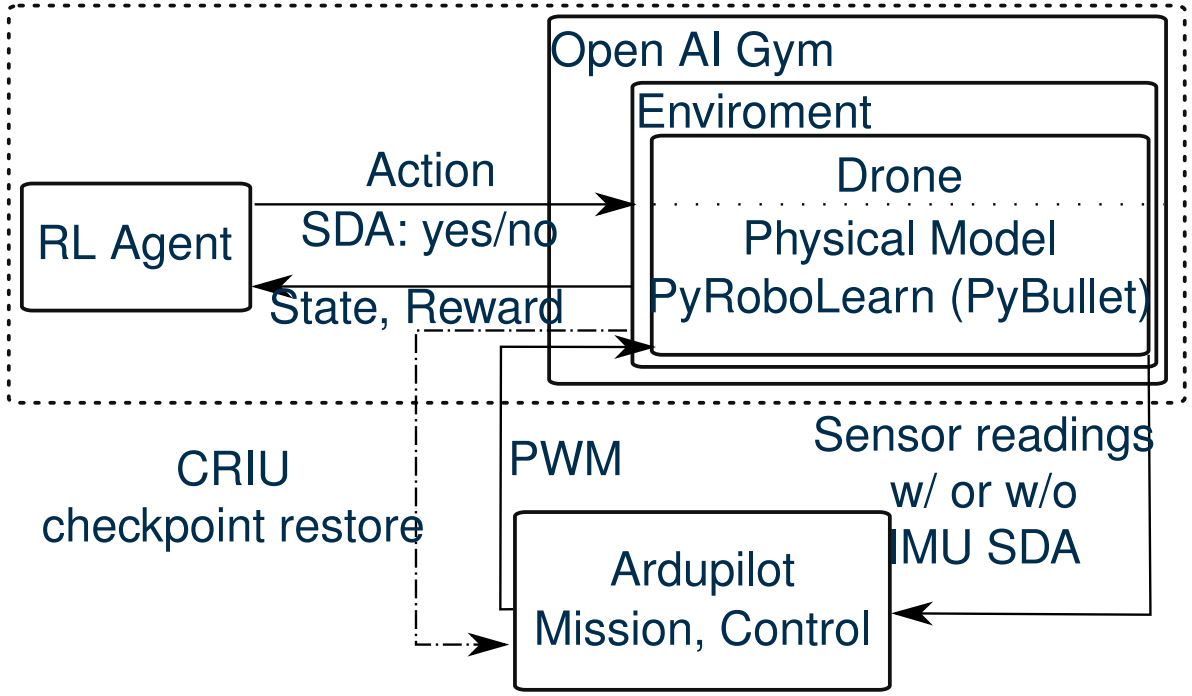
RQ3 What is the impact of the proposed ConfuSense on UAVs?

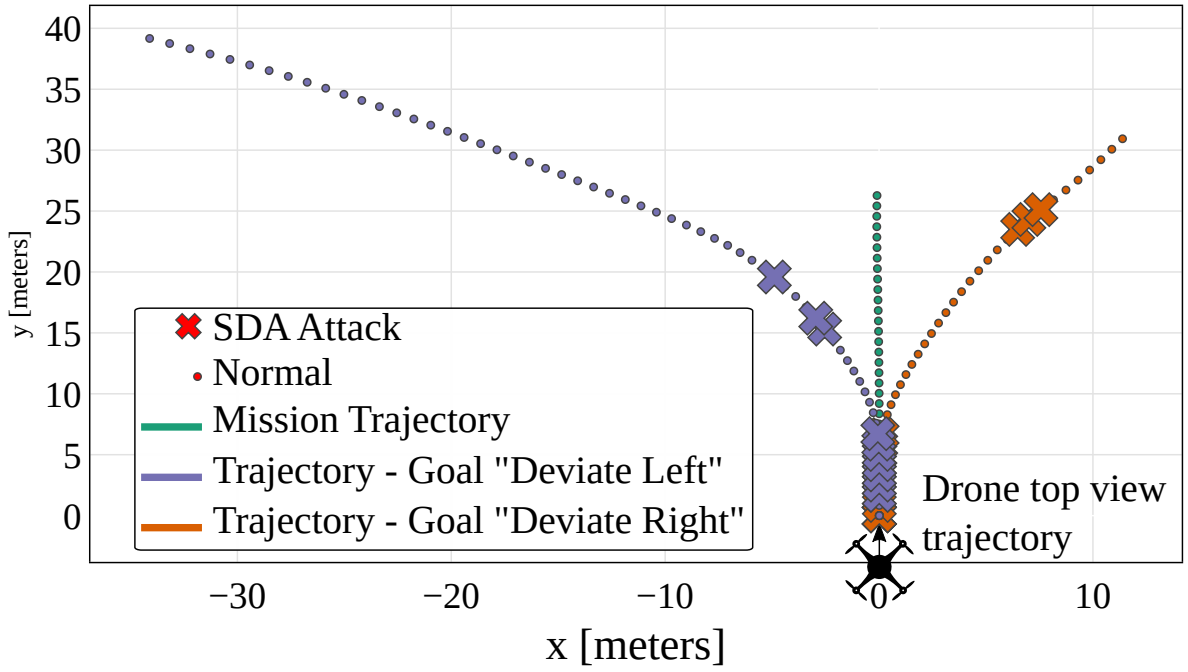
	ConfuSense 1 second				Time to Detect		Time to Crash	
	Undetected		Detected (failsafe)					
	%crash	%compl.	%crash	%land	μ(s)	σ	μ(s)	σ
Stale	0.00	0.00	0.00	100.00	4.99	1.80	N.A.	N.A.
Default	0.00	0.00	100.00	0.00	1.22	0.00	4.56	0.00
Absent	**100.00**	0.00	0.00	0.00	N.A.	N.A.	4.22	0.01

	Induced trajectory deviation					
	x		y		z	
	μ(m)	σ	μ(m)	σ	μ(m)	σ
Stale	16.7	15.8	7.6	7.9	1.2	1.2
Default	4.3	0.2	39.7	0.0	4.9	0.0
Absent	57.8	0.4	**138.1**	0.0	53.1	0.0

Controllability: Attack Synthesis

RQ4: How can UAVs be adversarially controlled via ConfuSense?





Detection

RQ5: Is ConfuSense detected by State-of-the-Art detectors for UAVs?

Attack Detection

We evaluate ConfuSense against M2MON Khan et al. 2021:

- Suspend Attack: accuracy drops from 1 to 0
- Frequency attack: delay detection, 128 missing observations when the IMU frequency drops from 1600 Hz to 12.5 Hz

Detection

RQ5: Is ConfuSense detected by State-of-the-Art detectors for UAVs?

Attack Detection

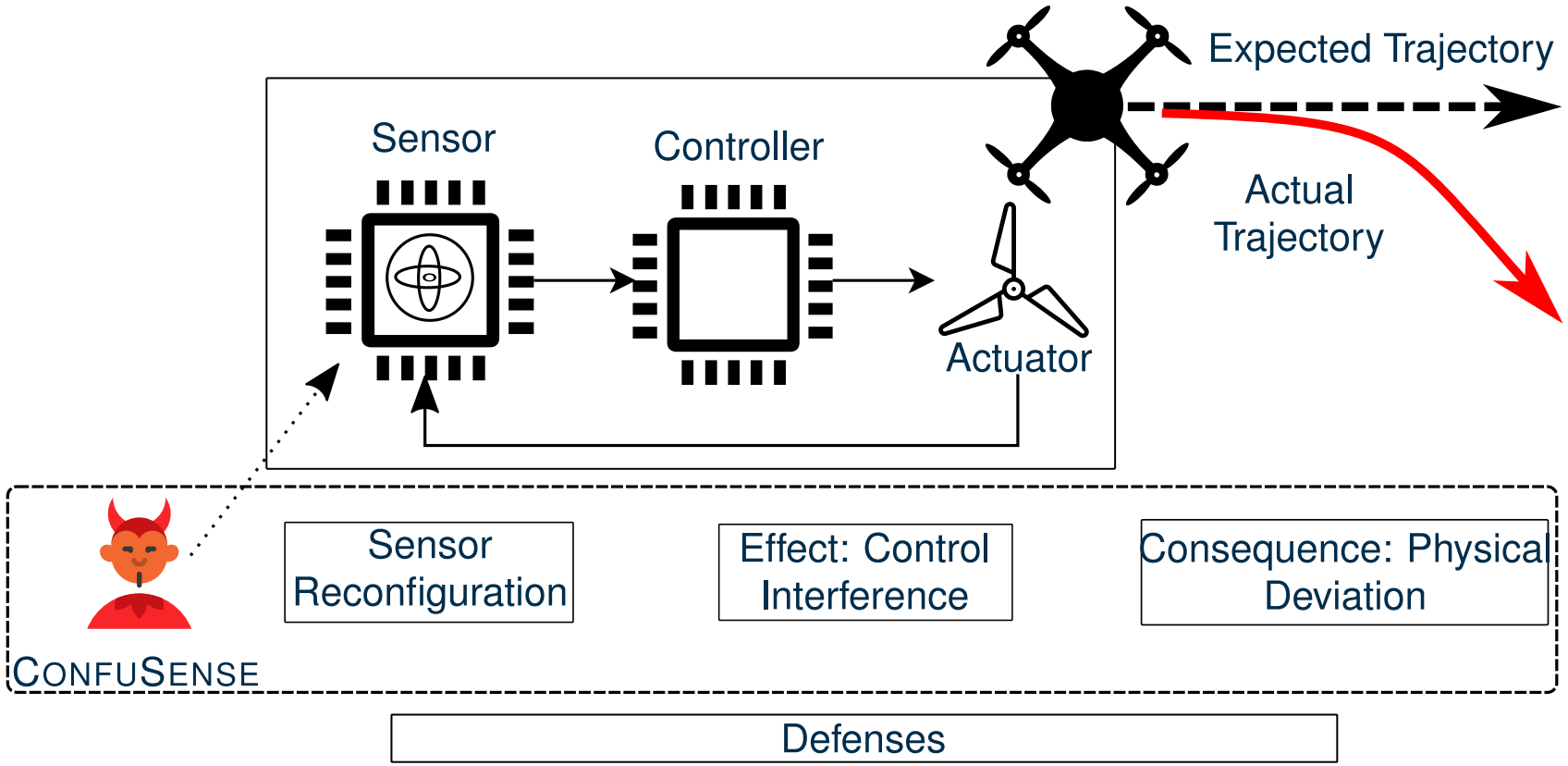
We evaluate ConfuSense against M2MON Khan et al. 2021:

- Suspend Attack: accuracy drops from 1 to 0
- Frequency attack: delay detection, 128 missing observations when the IMU frequency drops from 1600 Hz to 12.5 Hz

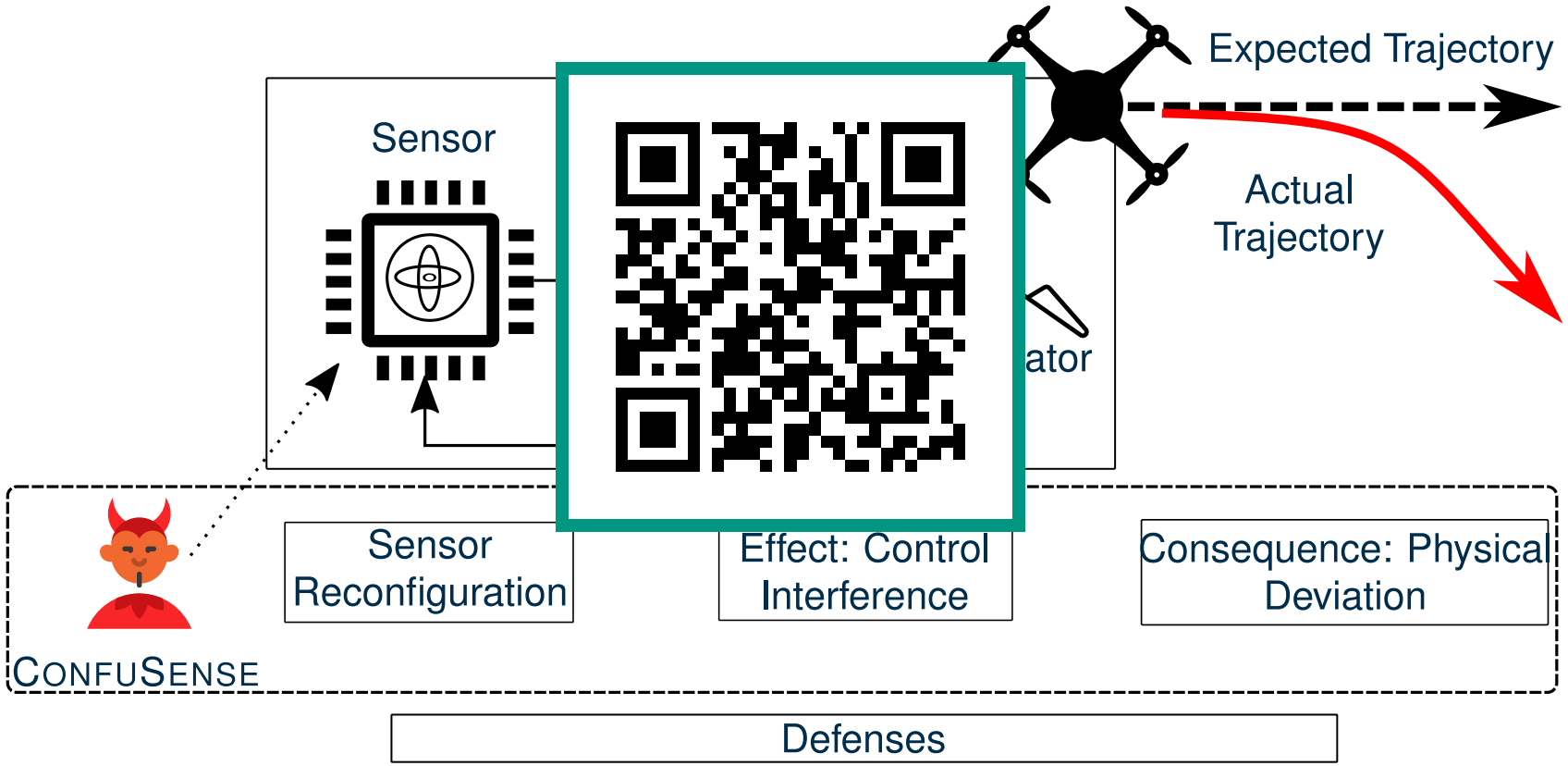
Mitigation

- Chip-level Mitigation
- Software-level Mitigation
- Proactive Solutions
  - Hardware Supply Chain Security
  - IEMI Defenses

Conclusion


Expected Trajectory
Actual Trajectory
Sensor
Controller
Actuator
Sensor Reconfiguration
Effect: Control Interference
Consequence: Physical Deviation
ConfuSense
Defenses

Conclusion


Expected Trajectory
Actual Trajectory
Sensor
ator
Sensor Reconfiguration
Effect: Control Interference
Consequence: Physical Deviation
ConfuSense
Defenses

Conclusion



Thank you — Questions?
alessandro.erba@kit.edu

Bibliography

[1] Joonha Jang et al. “Paralyzing Drones via EMI Signal Injection on Sensory Communication Channels”. In: *Proc. Network and Distributed System Security Symposium (NDSS)*. 2023.

[2] Jinseob Jeong et al. “Un-Rocking Drones: Foundations of Acoustic Injection Attacks and Recovery Thereof”. In: *Proc. Network and Distributed System Security Symposium (NDSS)*. 2023.

[3] Arslan Khan et al. “M2MON: Building an MMIO-based Security Reference Monitor for Unmanned Vehicles.”. In: *Proc. of the USENIX Security Symposium*. USENIX Association, Aug. 2021.

[4] Harshad Sathaye et al. “An Experimental Study of GPS Spoofing and Takeover Attacks on UAVs”. In: *Proc. of the USENIX Security Symposium*. USENIX Association, Aug. 2022. ISBN: 978-1-939133-31-1. URL: https://www.usenix.org/conference/usenixsecurity22/presentation/sathaye.

[5] Yunmok Son et al. “Rocking Drones with Intentional Sound Noise on Gyroscopic Sensors”. In: *Proc. of the USENIX Security Symposium*. Washington, D.C.: USENIX Association, Aug. 2015. ISBN: 978-1-939133-11-3. URL: https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/son.