Towards Specifying for a Trustworthy UAV Flight Control System with Evolving Functionality

University of Bristol[1] | Bristol Robotics Laboratory[2] | University of Southampton[3]

Dhaminda B. Abeywickrama[1,2], Sergio Araujo-Estrada[1,3], Alvin Wilby[3], Kerstin Eder[1], Shane Windsor[1]

dhaminda.abeywickrama@bristol.ac.uk

S.Araujo-Estrada@soton.ac.uk

UKRI Engineering and Physical Sciences Research Council

UKRI Trustworthy Autonomous Systems Hub

Specification Challenge

How do you specify a UAV should deal with situations beyond the limits of its training?

- **Performance measures** of a **UAV classical flight controller** (e.g. PID)
- Ensure control system: stable; disturbance attenuation; smooth and rapid responses to set-point changes; state-state accuracy; and robust
- Very little works comply standards like **DO-178C**, **DO-331** [e.g. Hochstrasser et al., 2018; Grant et al., 2019]
  - No work explores **machine learning (ML)**

Application

Fig. 1: UAV delivering a parcel [UAS traffic management].

Parcel Delivery:

- Complex and uncertain flight conditions (e.g. wind gradients), highly dynamic and uncertain airspace (e.g. other UAVs)
- Investigate UAV flight **control strategies** and **ML** that allow to adapt to changes to parameters of the UAV and environment
- Total mass up to 25kg

Review of Existing Standards

- **Software Considerations in Airborne Systems & Equipment Certification (DO-178C):**
  - Criticality levels of software
  - High-level & low-level software requirements
  - Software derived requirements
  - Traceability
- **Model-Based Development & Verification Supplement to DO-178C & DO-278A (DO-331)**
- **EUROCAE ED 279, NATO STANAG 4671, ARP4761, DO-254**
- **CAP722: Unmanned Aircraft System Operations in UK Airspace – Guidance**
- **CAP722A: Unmanned Aircraft System Operations in UK Airspace – Operating Safety Cases**

Method Explored: AMLAS

Assurance of Machine Learning for use in Autonomous Systems [AMLAS Guidance 1.1]

- **Assurance:** justified confidence or certainty in a system's capabilities, including safety
- **Safety case:** a justification supported by evidence, that the system is safe to operate in its context
  - **Goal Structured Notation**
- **Guidance** on how to systematically integrate **safety assurance** into the development of ML components
- **Outcome:** explicit & structured **safety case**
  - Set of **argument patterns**, and the underlying assurance activities instantiated to develop ML safety cases
- Assurance activities performed in **parallel** to the development of ML component
- **Iterative**

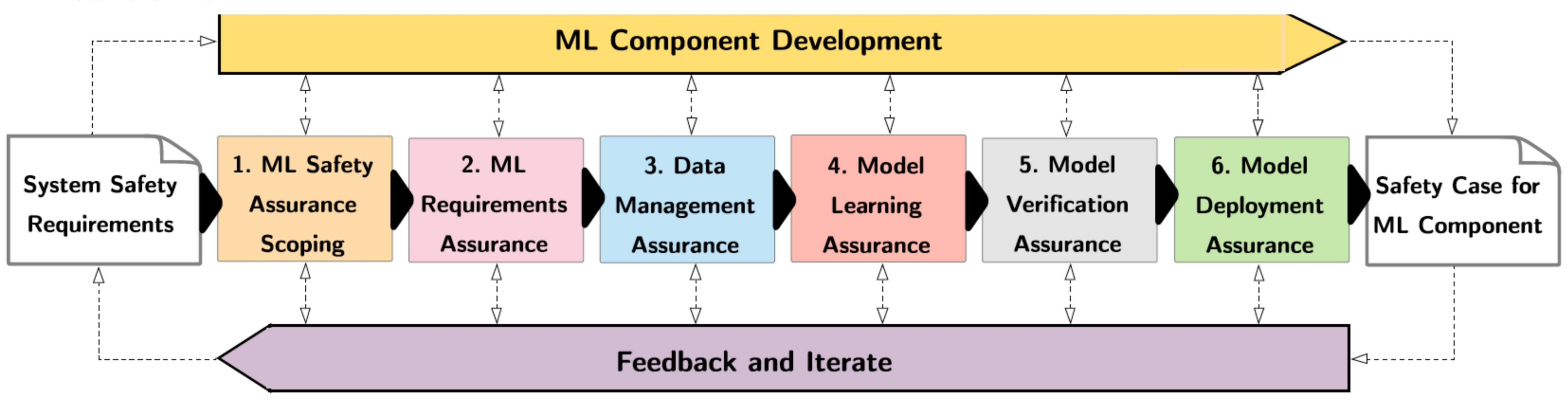
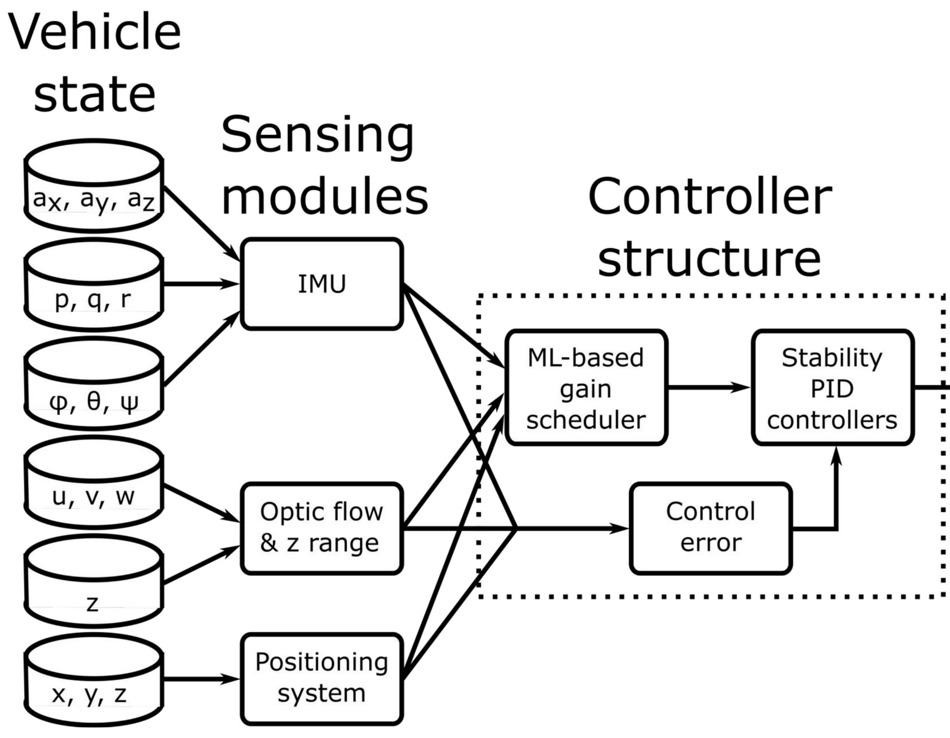


Fig. 2: AMLAS process [AMLAS Guidance 1.1].

- **Our Approach**:
  - Safety Case for **ML component** using AMLAS, and **safety-critical components** using standards like DO-178C, DO-331

System Description



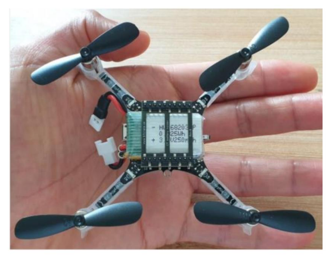


Fig. 3: System architecture for case study example using Crazyflie.

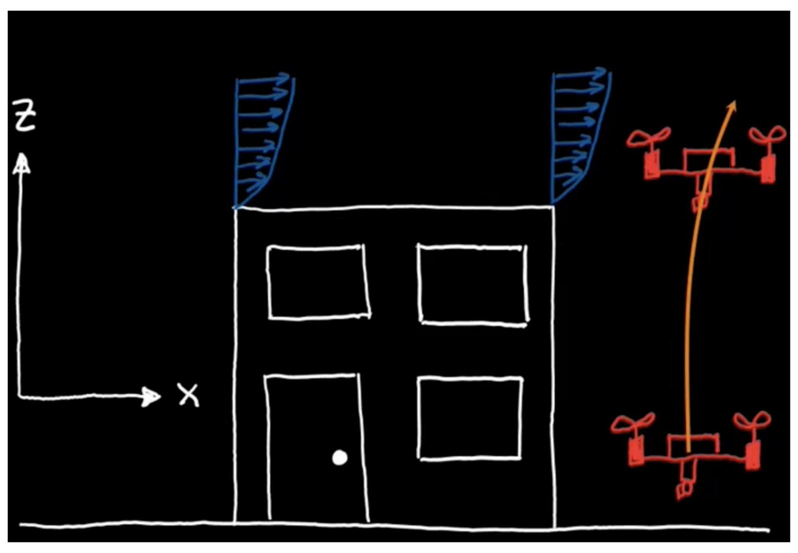
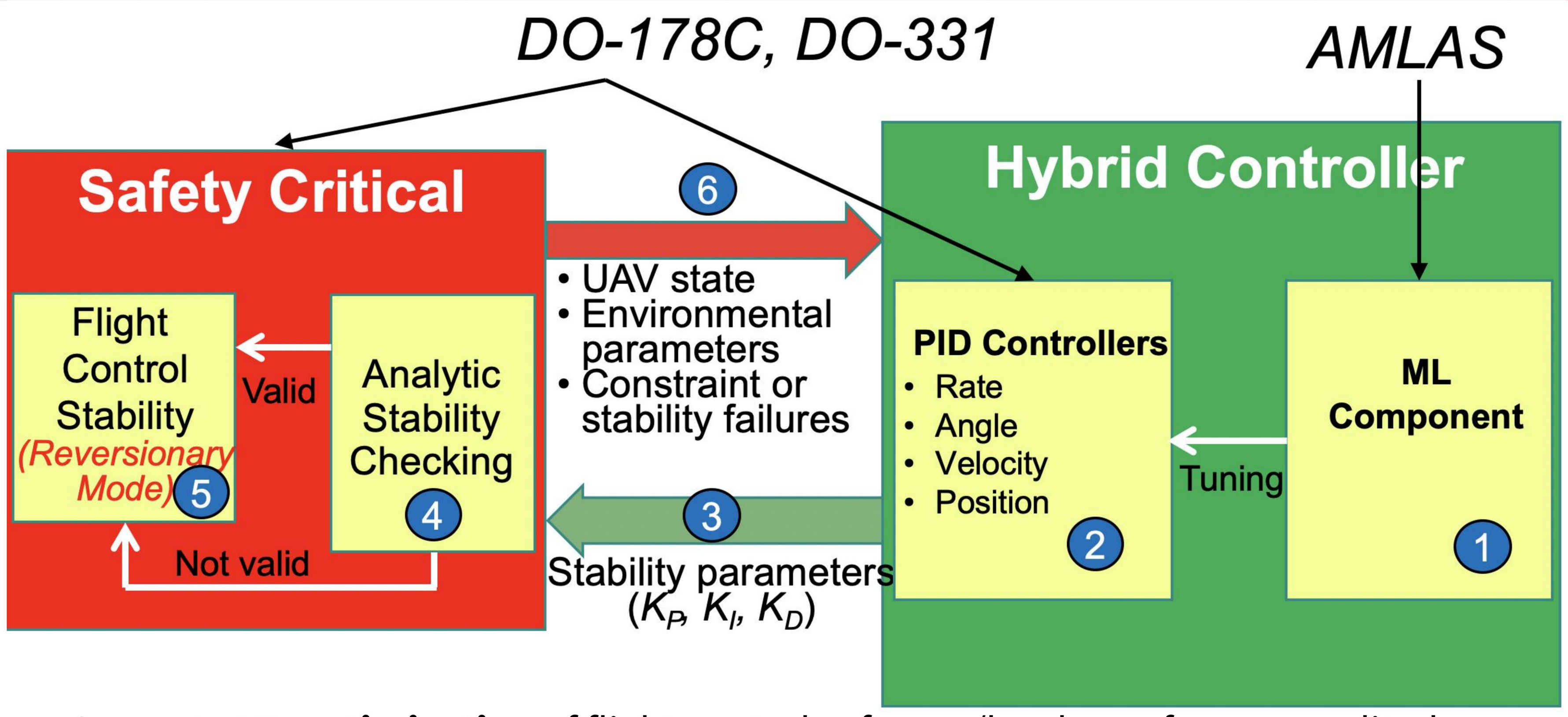


Fig. 4: Initial example: Vertical take-off and landing.

Architecture



- Separate **ML optimization** of flight control software/hardware from accredited **safety-critical** stability software/hardware, with **supervisory functions** to guarantee overall system safety.

ML Safety & Data Requirements

Performance Requirements:
RQ1: ML component *shall* ensure a maximum altitude of 120m (400 feet) during vertical take-off and landing of the UAV
RQ2: ML component *shall* ensure a maximum lateral displacement of 2 X diagonal distance between rotors of the UAV
Robustness Requirements:
RQ3: ML component *shall* perform as required in different wind levels (1–5*)* experienced during vertical take-off and landing of the UAV
RQ4: ML component *shall* perform as required in different turbulence levels (low, high) experienced during flight of the UAV
Data Requirements for Relevance, Completeness, Accuracy & Balance:
RQ5: All data samples *shall* represent vertical take-off and landing phases of the flight
RQ6: All data samples *shall* represent various ranges of wind conditions
RQ7: The data samples *shall* include sufficient range of wind speeds within the scope of the operational domain
RQ8: The data samples *shall* include sufficient range of wind turbulence levels within the scope of the operational domain
RQ9: All gain values produced in the data samples *shall* be correctly labelled to produce stable system
RQ10: The data *shall* have a uniform distribution of samples

Next Steps

- Specify a concrete **safety case** for ML component using AMLAS and safety-critical components using standards like DO-178C & DO-331
- Perform **model learning**, **verification** and **deployment** assurance activities for the ML component
- Explore other **non-functional** requirements as **first-class** objects for trustworthiness
- Explore **ethical** & **regulatory** challenges

Any suggestions and opportunities for collaborations are welcome. Please contact us.

UKRI TAS NODE IN FUNCTIONALITY

University of Bristol | brl Bristol Robotics Laboratory | University of Southampton