Autonomous Systems: Specification and Verification

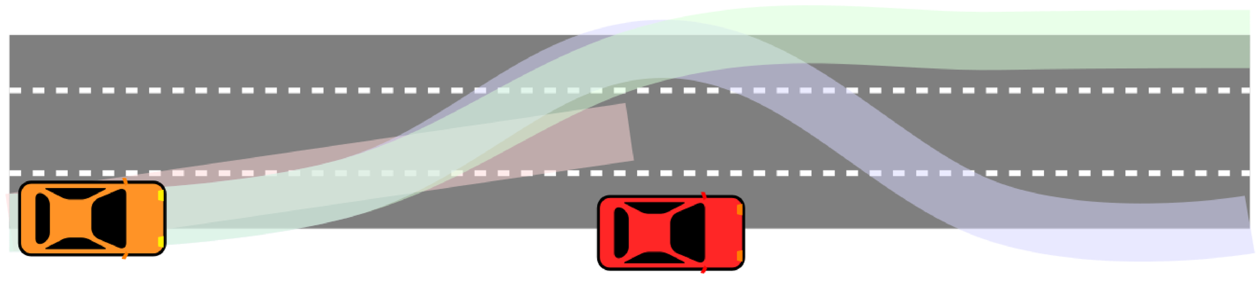
Lancaster University
School of Computing and Communications

Andrew Sogokon (a.sogokon@lancaster.ac.uk)
Prof Neeraj Suri (PI)

Engineering and Physical Sciences Research Council
UKRI Trustworthy Autonomous Systems Hub

Specifications for Autonomous Systems

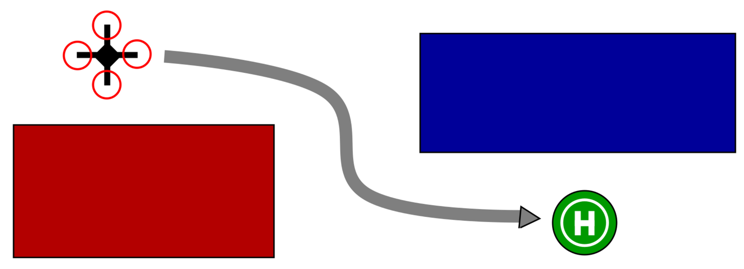
- Specifications are descriptions of what a system should (or should not) do.
- A large source of specifications for AS comes from ***regulations*** (e.g. the *Highway Code* for terrestrial vehicles, or the *Rules of the Air* for aerial vehicles).
- Regulations written in natural language (e.g. English prose) can be imprecise and subject to various interpretations.
- E.g. "*When changing the lane to the left lane during overtaking, no following road user shall be **endangered***" (Rizaldi et al., 2017).



Formal Specifications

- **A formal model** of the system provides a precise description of the dynamics.
- **A formal specification** can be *verified* against a formal model.
- Mission specifications can often be stated in formal logic (such as various **temporal logics**) and can incorporate safety and liveness requirements:
  - $\Box_{[0,\infty)}$ **dist**(*ownship*, *intruder*) $\geq d_{min}$ (collision avoidance)

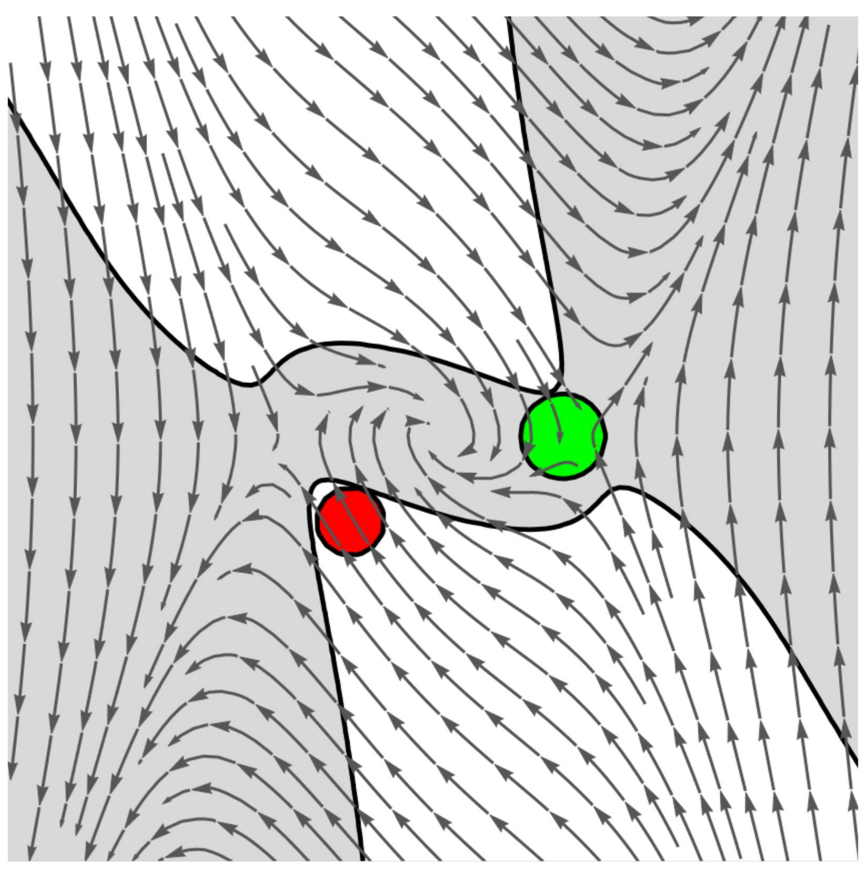
  - $(\Diamond_{[0,T]}\, Target) \wedge (\Box_{[0,T]}\, Safe)$ (reach-avoid)



Safety Specification and Verification

Safety Specifications

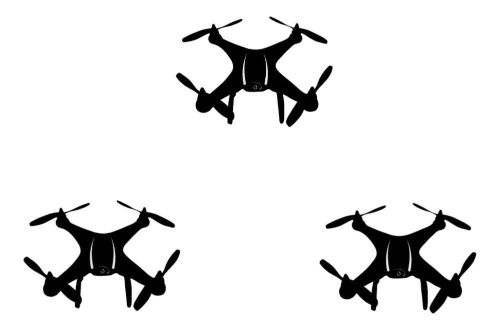
- A **safety specification** for a given system requires two elements:
  - 1 - A description of the possible initial states from which the system may begin its operation.
  - 2 – A description of undesirable (i.e. unsafe) states into which the system must never transition.

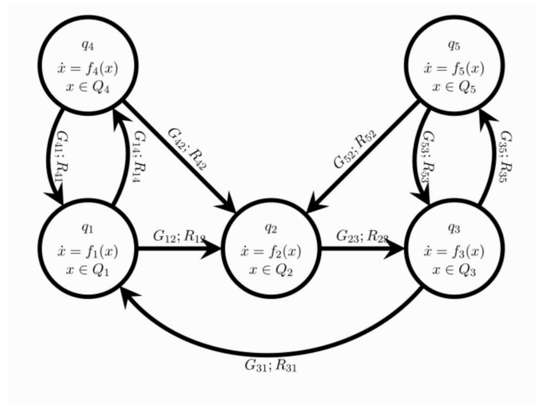


- **Safety verification** is concerned with proving a safety specification, i.e. rigorously demonstrating that a system may never transition into any of the unsafe states provided that it starts operating from one of the specified initial states.

Cyber-Physical Autonomous Systems

- Systems that interact with a physical environment are *cyber-physical systems* (***CPS***).
- Continuous dynamics in CPS is usually described using ***differential equations***.



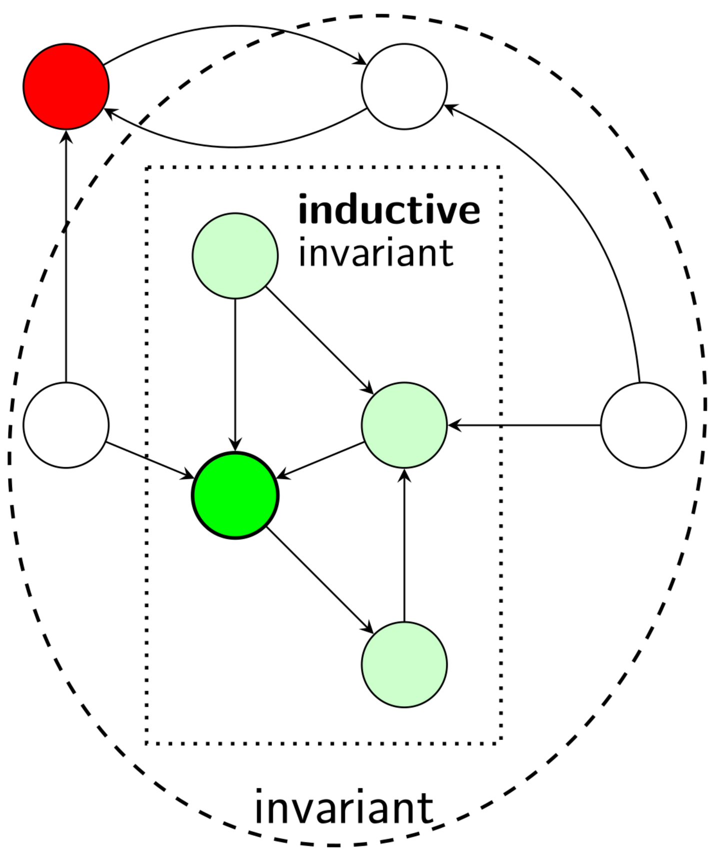


- Formal models of CPS involve **real numbers** and formal verification **requires real arithmetic**. ℝ

Formal Modelling and Verification in TLA+

Temporal Logic of Actions

- Lamport's Temporal Logic of Actions was designed to enable formal modelling and verification of concurrent systems. It enjoys excellent tool support in the form of the **TLA+ Toolbox** and has been successfully applied in industry.
- Formally proving safety specifications of discrete transition systems is typically done by finding an appropriate **invariant**.

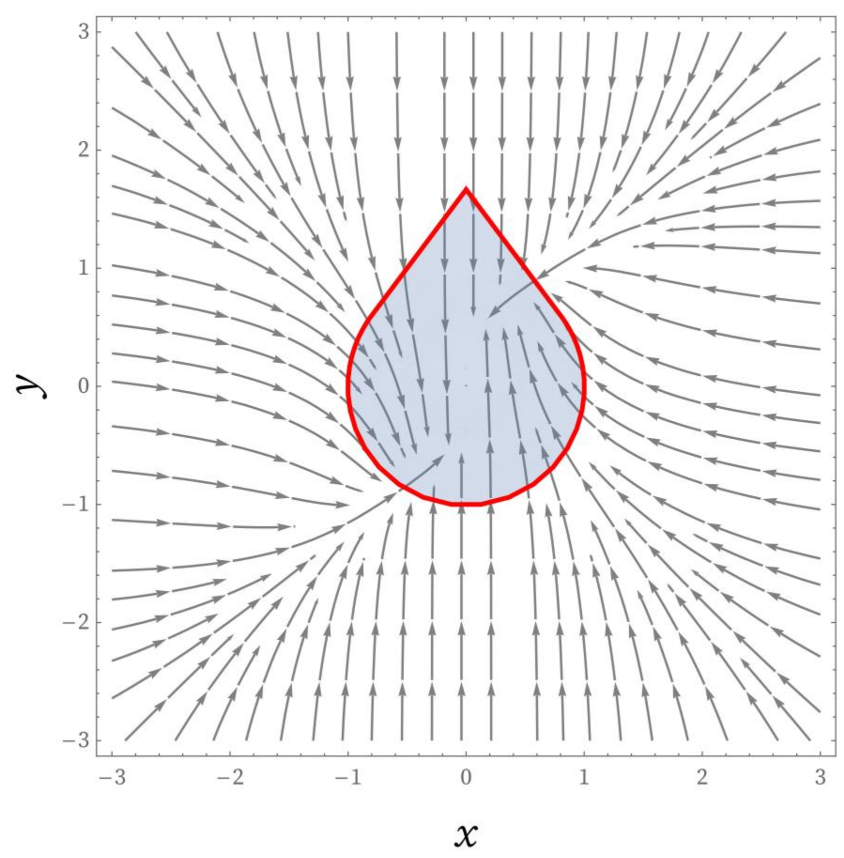


Inductive Invariants

- An **invariant** is a set of states that:
  - It includes all the initial states (as described in the safety specification).
  - It does not include any of the unsafe states.
  - The unsafe states are not reachable from the initial states.

  An invariant is **inductive** if there are no transitions out of the invariant.

- A corresponding notion to an inductive invariant in continuous systems is that of a **positively invariant set / continuous invariant** .
- Recent work in computer science has established that it is **decidable** to check whether a set is positively invariant (provided it is described using polynomial functions). *This requires real arithmetic*.
- This result makes it possible to perform safety verification without having to solve the ODEs.



Automating Real Arithmetic in TLA+

- **TLA+** supports real numbers (which are required for modelling and verifying CPS, especially in checking continuous invariants).
- However, the proof system currently lacks support for automatic proofs of first-order real arithmetic sentences (e.g. $\forall\, x, y \in \mathbb{R}.\ 2x^2 + (xy - y)^2 \geq -1$) .
- The **TLA+ Proof Manager (TLAPM)** has now been extended to support nonlinear real arithmetic (O. V. Gunasekera et al.) – a step towards safety verification of CPS using TLA+.