Enabling Formal Safety Verification of Cyber-Physical Systems in TLA+

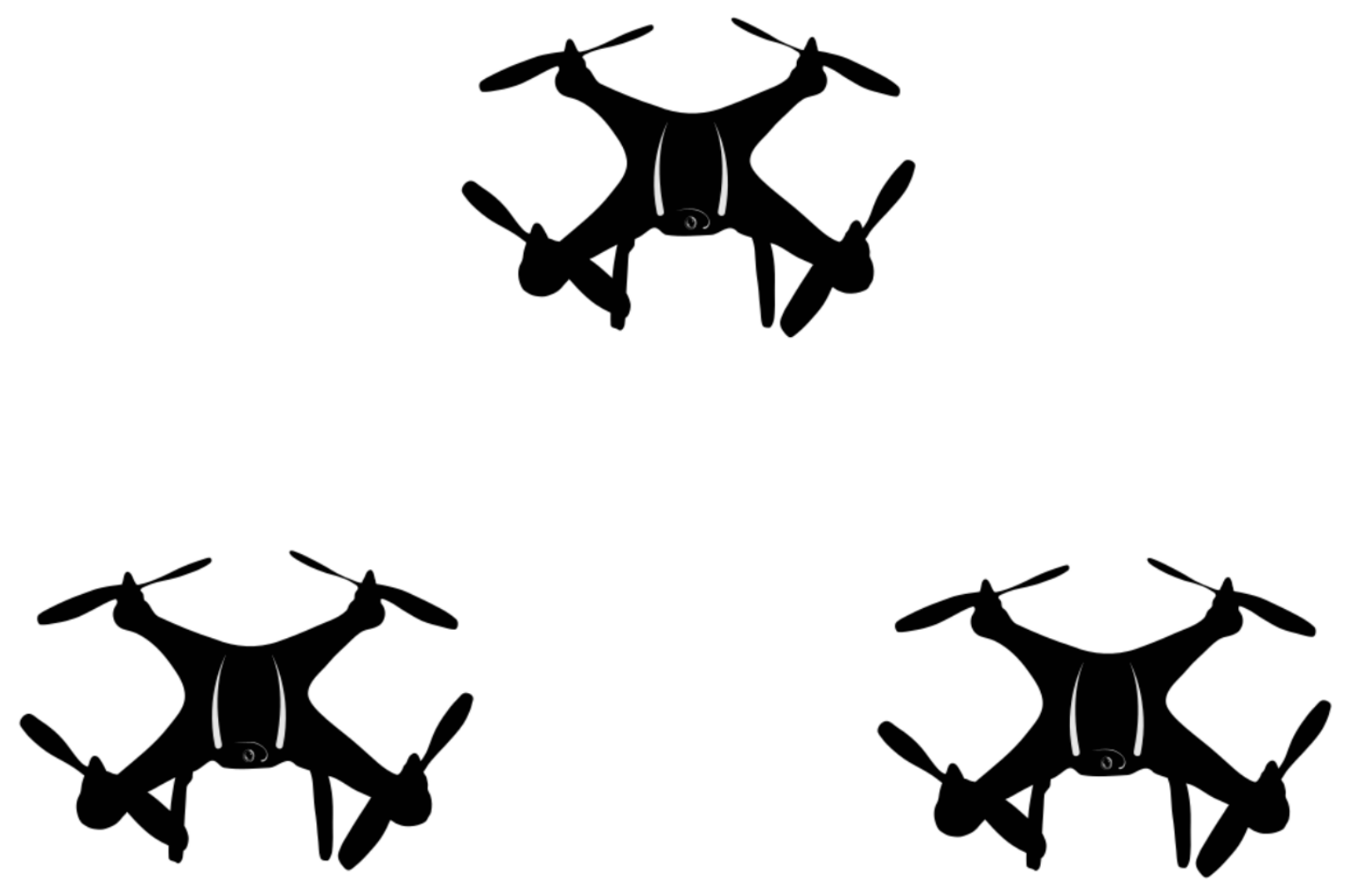
Lancaster University

Researcher: Dr. Andrew Sogokon
Investigator: Prof. Neeraj Suri

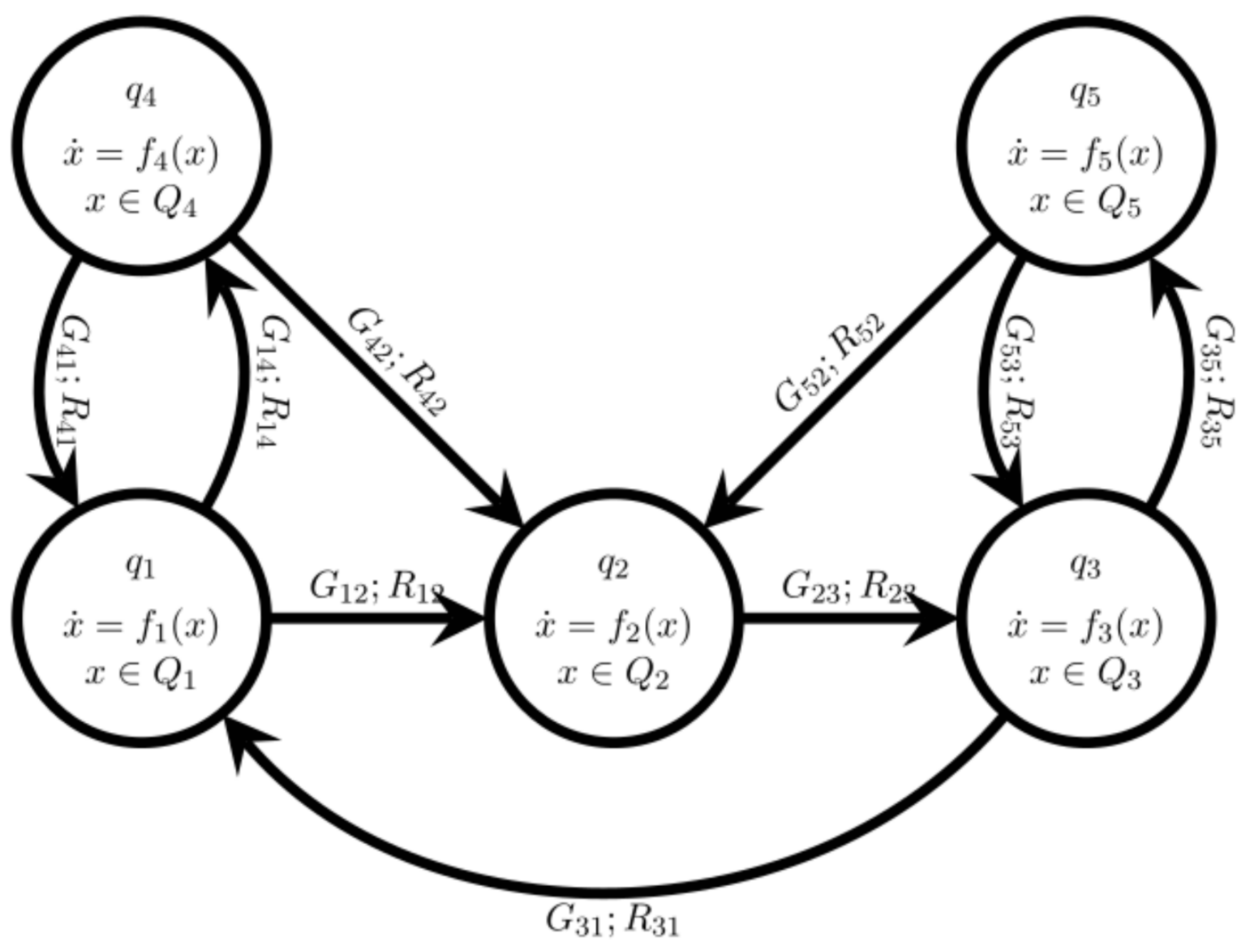
Safety-Critical Cyber-Physical Systems

Cyber-Physical Systems

- Cyber-Physical Systems (**CPS**) combine discrete and continuous behaviour.
- Examples include digital computer systems that operate in a continuous physical environment.
- Some CPS are **safety-critical** which means that failures can result in catastrophic consequences.
- Examples of safety requirements for CPSs include *collision avoidance* between autonomous vehicles in the aerial as well as the terrestrial domain.



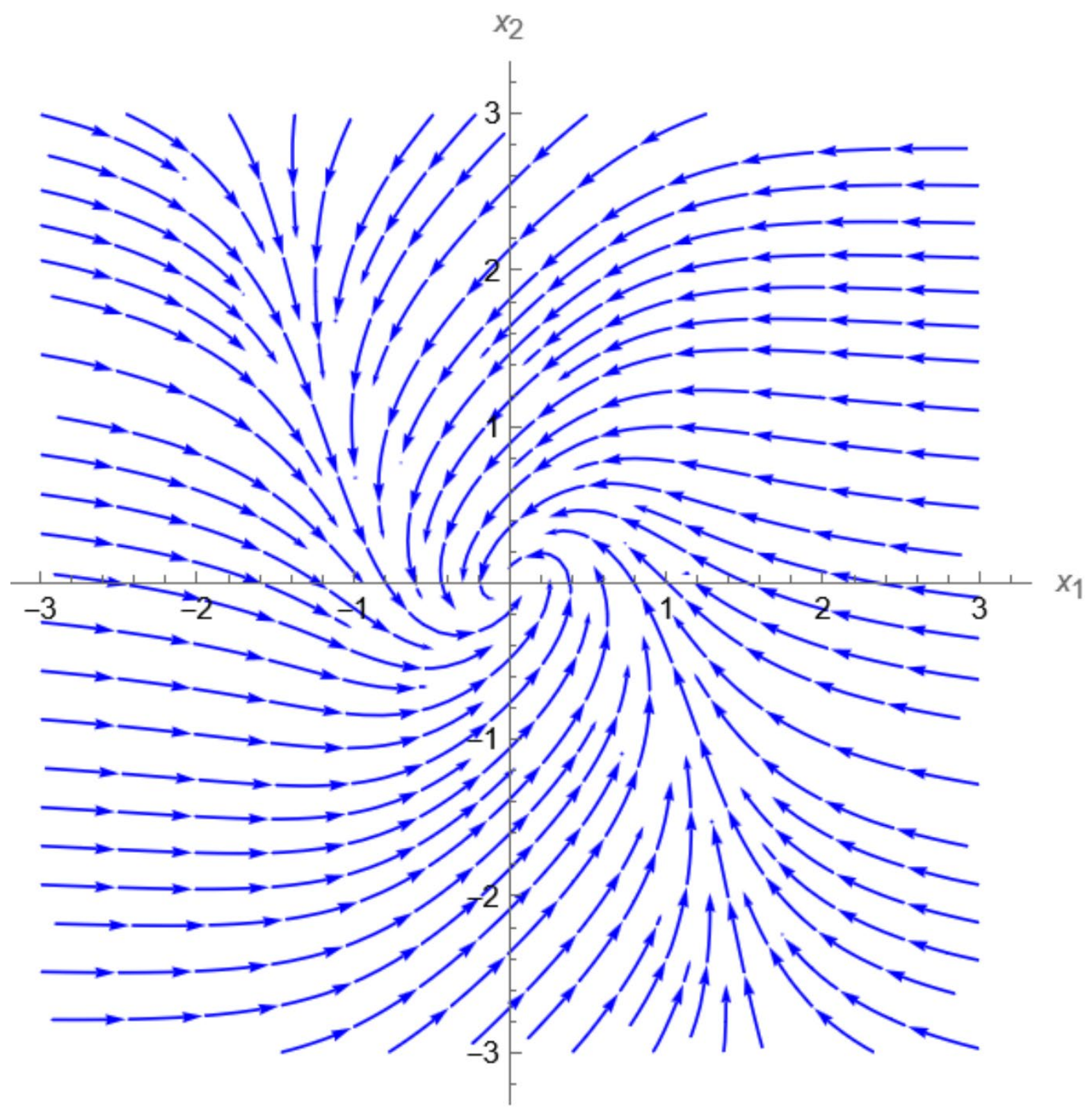
Formal Models of CPS



- Cyber-Physical Systems can be represented formally, e.g. using operational models such as hybrid automata or hybrid programs.
- A formal model of a CPS provides a mathematically precise description of the system that can be rigorously analysed.
- For **safety-critical** CPS it is important to ensure that the system adheres to its safety specification (e.g. avoids collisions at all times).
- A formal model of a CPS can (in some cases) be checked against a formal safety specification (typically stated using a formal logic). If successful, the safety of the model can be rigorously established.

Continuous Dynamics of CPS

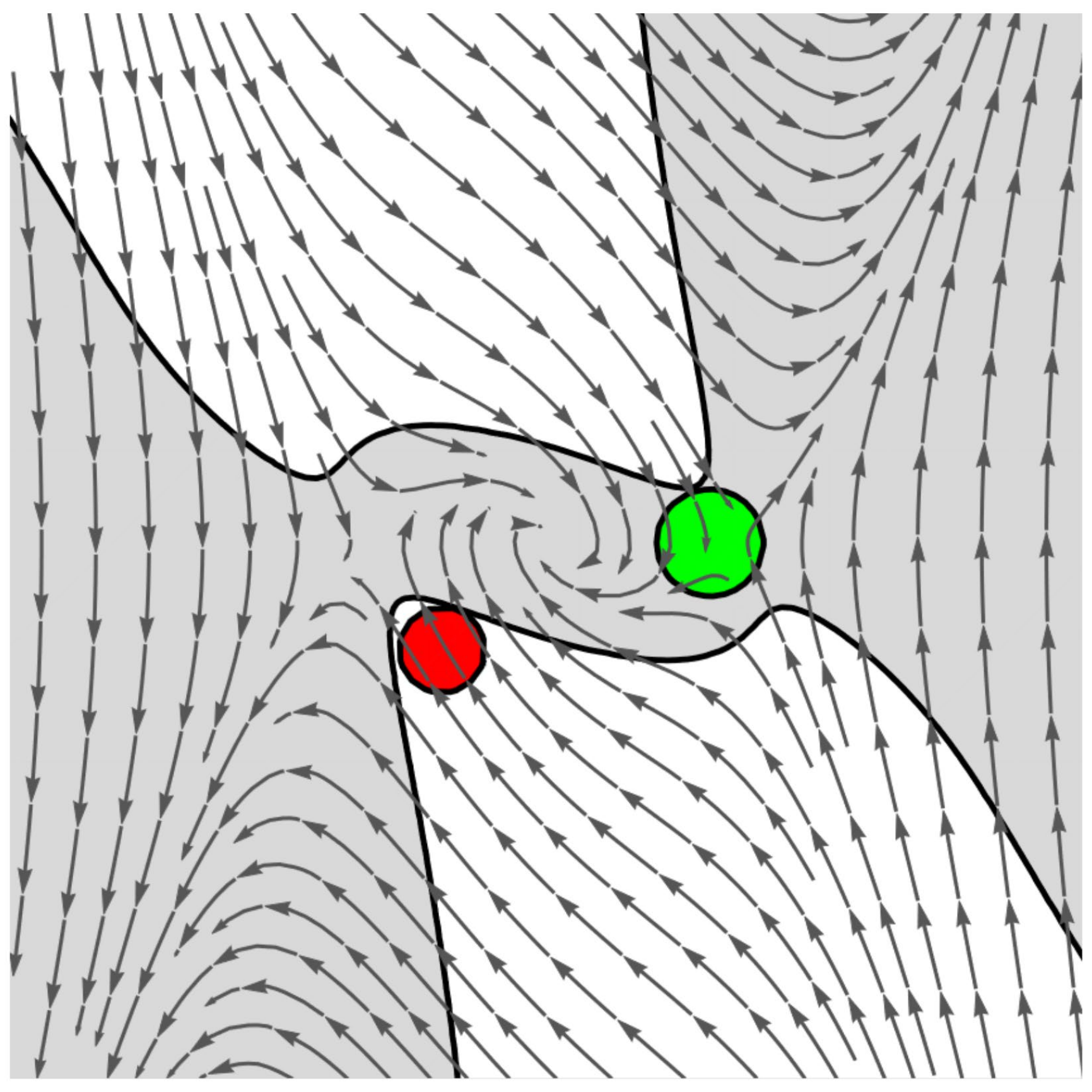
- Continuous behaviour in CPS is usually governed by systems of ordinary differential equations (ODEs).
- Geometrically, a system of ODEs corresponds to a vector field defined on n-dimensional Euclidean space (where n is the dimension of the system).
- Solving ODEs is usually not possible analytically.
- Non-linear ODEs are particularly difficult to analyse.



Safety Specifications for Continuous Systems

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.

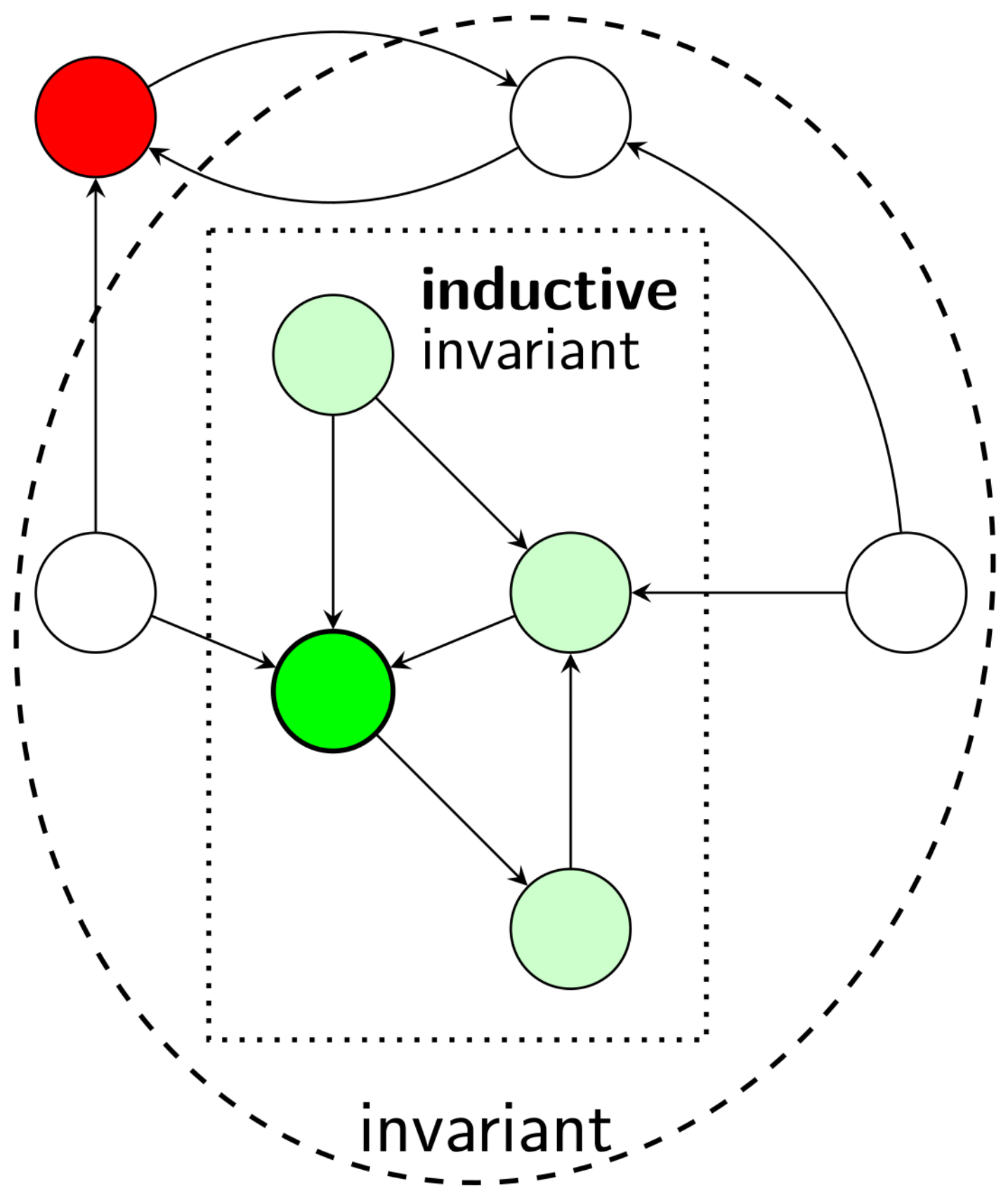


- **Safety verification** is concerned with proving a safety specification, i.e. rigorously demonstrating that a system may never transition into any of the unsafe states provided that it starts operating from one of the specified initial states.

Formal 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**.



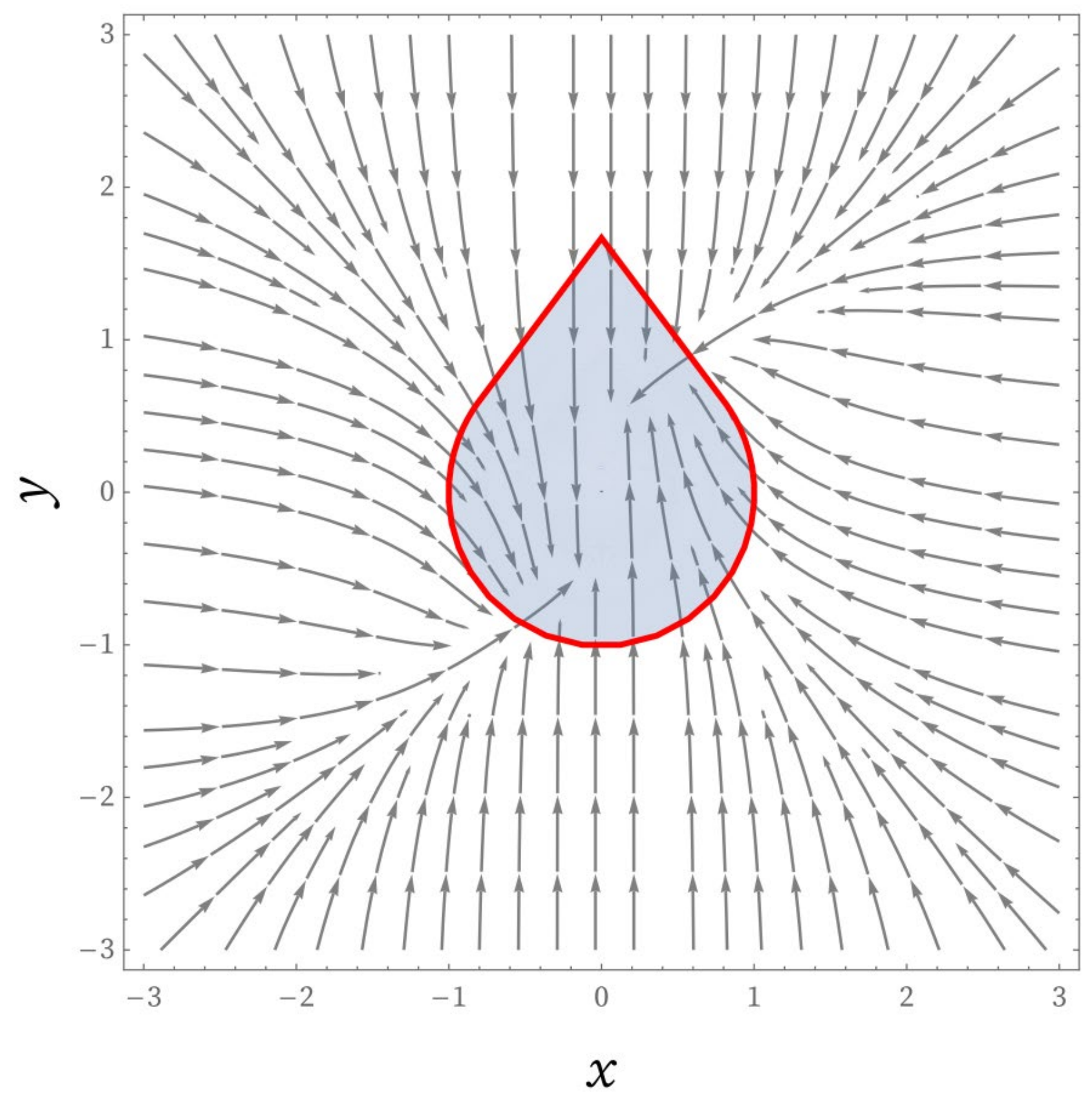
Inductive Invariants

- 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.

Checking Continuous Inductive Invariants

- A corresponding notion to an inductive invariant in continuous systems is that of a **positively invariant set**.
- There is a rich theory and powerful results about positively invariant sets in dynamical systems.
- More 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 result makes it possible to perform safety verification without having to solve the ODEs.
- Adding support for checking continuous invariants would greatly facilitate CPS verification in the TLA formal framework.



This work is supported by the Engineering and Physical Sciences Research Council [grant number: EP/V026763/1]