This thesis is focused on formal verification of cyber-physical systems. Cyber-physical systems (CPSs), such as computer-controlled cars, airplanes or robots play an increasingly crucial role in our daily lives. They are systems that we bet our lives on, so they need to be safe. However, ensuring that CPSs are safe is an intellectual challenge due to their intricate interactions of complex control software with physical behavior. Formal verification techniques, such as theorem proving, can provide strong guarantees for these systems by returning proofs that safety is preserved throughout the continuously infinite space of their possible behaviors.

We provide the first formal verification of distributed car control; the first formal verification of distributed, flyable, collision avoidance protocols for aircraft; and an exploration of control choices within a well-defined safety envelope. Each of these systems presents new verification challenges and required new techniques for proving safety. However, we identify a unifying hurdle for each case study: it is difficult to compare hybrid systems, even when their behaviors are very similar.

We introduce differential refinement logic (dRL), a logic with first-class support for refinement relations on hybrid systems, and a proof calculus for verifying such relations. dRL simultaneously solves several seemingly different challenges common in theorem proving for hybrid systems: abstracting implementation-specific designs, maintaining a modular proof structure, breaking systems into parts, and leveraging iterative system design.

Differential refinement logic extends an existing specification and verification language for hybrid systems (differential dynamic logic, dL) by adding a refinement relation to directly compare hybrid systems. This thesis will give a syntax, semantics, and proof calculus for dRL.