Design Tools for Verification

Zhe Hou
Institute for Integrated and Intelligent Systems (IIIS)
Griffith University
“We should be certain what the autonomous system intends to do and how it chooses to go about this.”

--Michael Fisher,
ICRA 2016
Correct-by-construction

Design → Formalise → Formal Model → Verification

Implementation → Refinement
Curry-Howard Correspondence

Types \leftrightarrow Propositions

Programs \leftrightarrow Proofs

Evaluation of Programs \leftrightarrow Simplification of Proofs
GRAVITAS: Goal Reasoning And Verification for Independent Trusted Autonomous Systems
Overall Mission
Simulation