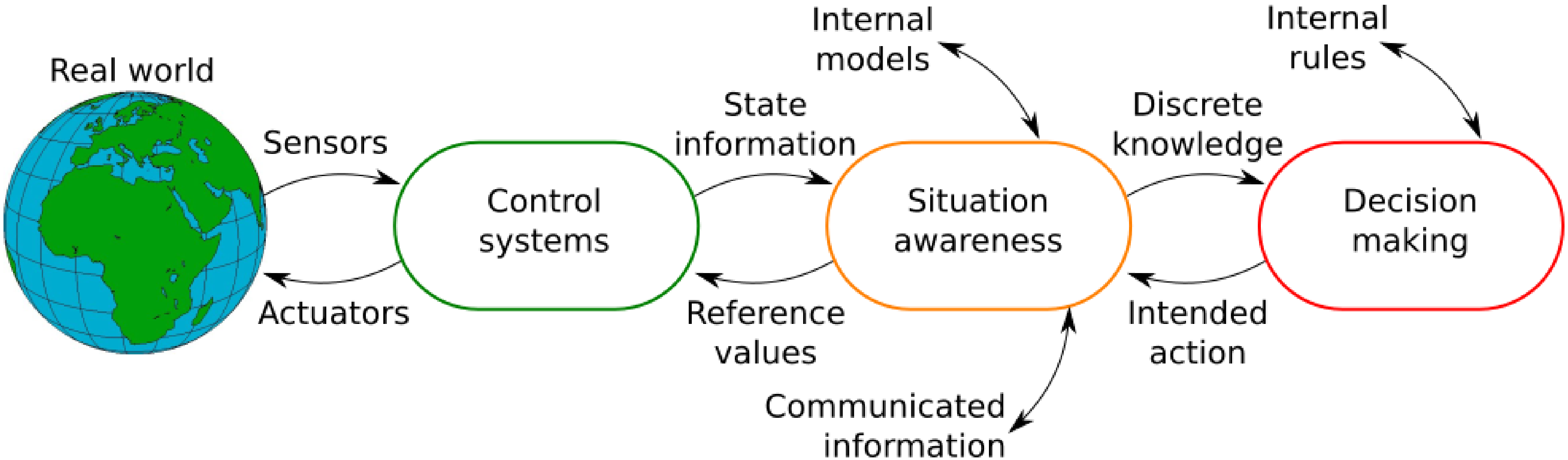
Safety standards for autonomous drones

Owen McAree

University of Sheffield

Anatomy of autonomy

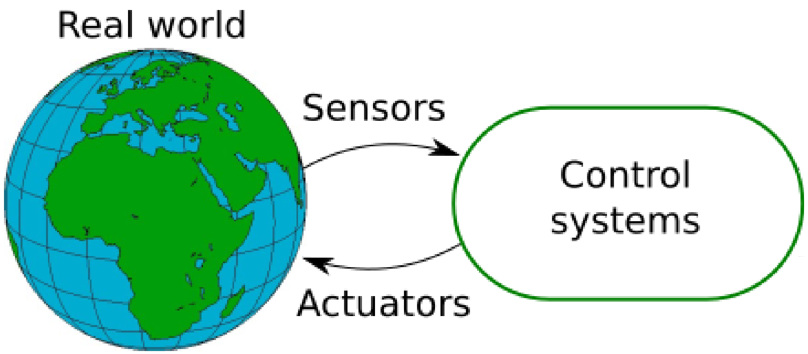
- Rational agent



Adapted from Dennis, Louise A., et al. "Practical verification of decision-making in agent -based autonomous systems." Automated Software Engineering 23.3 (2016): 305-359.

The University Of Sheffield.

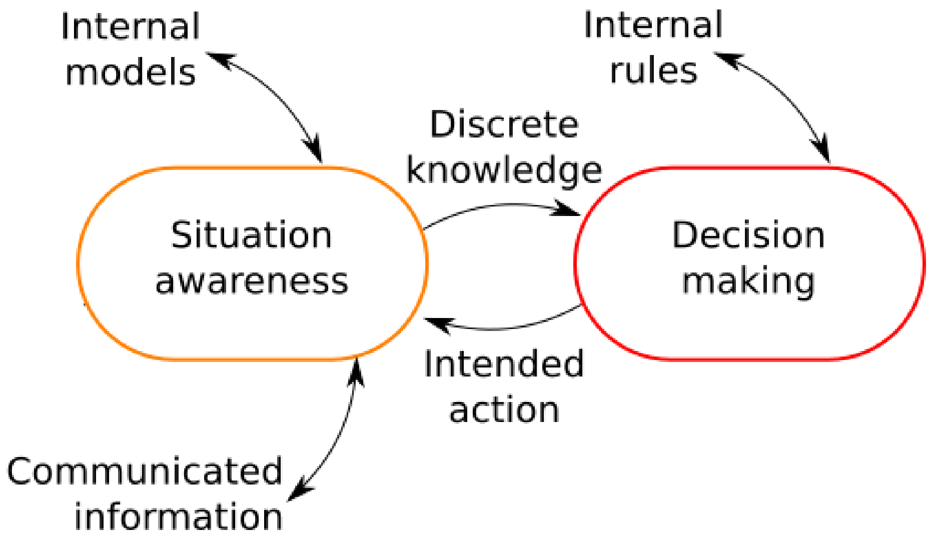
Control systems assessment



- Limited system architectures
- Well understood failure modes, leading to well quantified performance requirements
  - Stability, Robustness, Fault tolerance, etc…
- Straightforward to verify mathematically
- Relatively straightforward to test

Assessment of autonomy

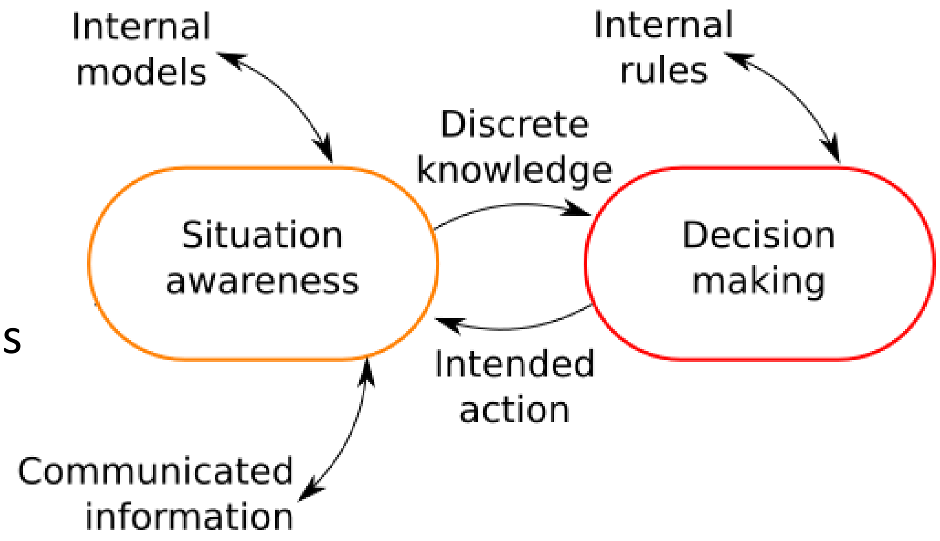
- Large number of potential configurations
  - Logic based, Reactive, BDI, SNN, DNN, etc…
- Open questions
  - What are the failure modes?
  - What are the performance requirements?
  - How do we verify the performance?
  - How do we ensure coverage in testing?



The University Of Sheffield.

Potential solutions

- Apply formal verification methods wherever possible
  - Provides absolute guarantees
- Apply stochastic verification otherwise
  - Provides probabilistic guarantees
- Requires stochastic modelling of all components, including real world and control systems
- Requires probabilistic performance requirements



The University Of Sheffield.