Can Robots Ever Be Safe?

The multitude of possible applications of mobile and autonomous robots fascinates us all. When it comes to the realisation of all this potential, a limiting factor is the need to provide evidence of safety. The practice in development of robotic systems is not compatible with the modern outlook of applications. We are designing platform-independent notations for modelling and simulation. Their formal underpinning supports generation of reliable and concrete evidence of safety, and model-based development via property-preserving transformations. Early analysis reduces costs and traceability ensures maintainability.

Challenges

- Practical notations to model the environment
- Automatic generation of simulations
- Reasoning about collections
- Tractable approach to dealing with time and probability
- Heterogeneous semantic models: continuous, probabilistic, reactive

Modelling

- Eclipse plug-in supporting both graphical and textual specification notation.
- State-machine based notation with facilities to specify behaviour and data operations, as well as time properties and the environment.

Simulation

- High-level domain specific language
- Platform independent

Object-Oriented Simulation

- RoboCalc (a Calculus for Software Engineering of Mobile and Autonomous Robots)

Analysis

- Model-checking: FDR, UPPAAL, PRISM
- Theorem proving: rich semantics in Isabelle/UTP

Platform-specific implementation

- V-REP
- ARGoS
- Enki

Deployment

- RoboCalc Eclipse plug-in

Controller example