Summary of Session 3: Collaborative Robots and Assessment

Safety Rules Synthesis for Run-Time Monitoring of Autonomous Robots in Human Environment

- Independent safety monitor
- Approach is to explore system state space to identify transitions from safe states to catastrophic states
- Concepts of “warning states” (can lead to catastrophic states) and “safety margin” (“distance” between safe and catastrophic states)
- Design system to ensure at least one warning state on every path from a safe state to a catastrophic state
- Safety strategy synthesis: try all possible interventions in all warning states to prevent transitions to catastrophic states
- Handling state explosion: no. of variables not too large, branch and bound state space search
- Approach tested on a real mobile robot with articulated arm, analysis and synthesis took around ½ hour

SAFER-HRC: Safety Analysis through Formal Verification in Human-Robot Collaboration

- Risk-based safety approach using formal verification with first order temporal logic
- Model includes: 1) constraints specifying operator behavior, 2) constraints specifying robot behavior, 3) layout of physical environment
- Identify high-risk hazards, define them with predicates
- Exhaustively explore state space to find executions in which hazardous predicates occur, apply risk reduction measures to eliminate hazardous states identified
- State space construction: tasks are broken down into actions
- Actions have pre-conditions and post-conditions, constraints on action sequencing can be imposed through pre-conditions
- Risk reduction measures modify model, e.g. change layout or add constraints to robot or operator
- Case study - robot and operator collaborate to take work pieces from a bin, move them to a tomb area, and screw them into tomb structure: possible hazards identified and formal analysis detected several executions that resulted in hazards

Original Robot Safety Rules

1. A robot may not injure a human being or, through inaction, allow a human being to come to harm.
2. A robot must obey the orders given it by human beings except where such orders would conflict with Rule 1.
3. A robot must protect its own existence as long as such protection does not conflict with Rule 1 or Rule 2.

Comments and Discussion Items

- We are still a long way from Asimov!
- There is still a large amount of manual effort required for safety model specification and analysis
- State space explosion still seems like a barrier to analysis of more complex systems, e.g. the factory of the future (Industry 4.0)
- SMT solvers could make synthesis-verification loop more efficient
- Neither Asimov nor the presenters considered executions resulting from malicious human actors, which is important moving forward
- Care should be taken with concept of “safety margin” as presented – difficult to apply it as a quantitative measure