Risk Structures:
An Approach to Risk Awareness in Robots

Mario Gleirscher
University of York, UK

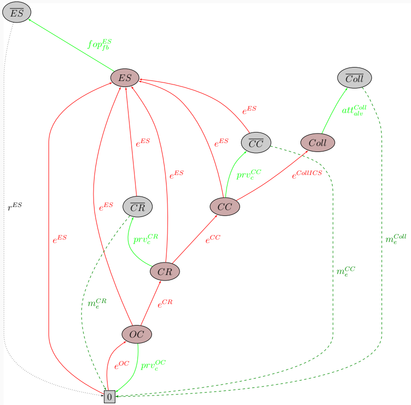
July 10, 2019

Toulouse, FR

Risk Awareness in Autonomous Robots

Why? How?

Risk Structure



Work in progress!

- **Challenge:**
  Autonomous risk handling
  State of the art:
  Design of local handlers
  Problem:
  Design of strategic handlers?
- **Approach:**
  Risk Structure =
  Risk handler
  in specific situation
  for partial hazard profile
- **Vision:**
  Risk-aware behaviour
  in all situations
  for complete hazard profile

Background and Motivation

Running Example: Risk-aware Autonomous Vehicle

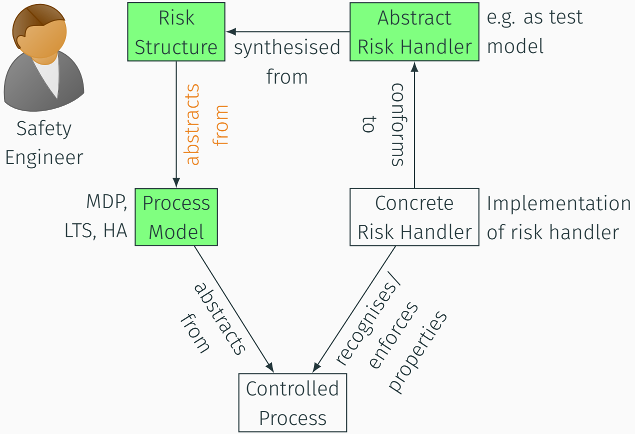
- Plant Modelling: From Dynamical to Situational
- Risk Identification and Assessment

Risk Structures

- Risk Factors and Spaces
- Risk Space Reduction: Factor Dependencies
- Situation Decomposition/Planning: Mitigation Orders

Summary

Background and Motivation



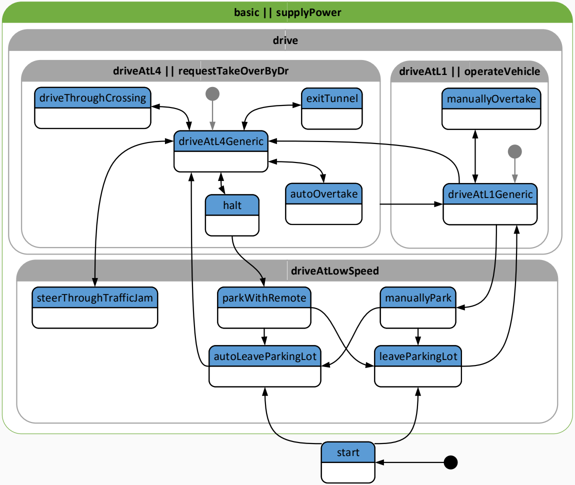
RQ: How to design risk-aware robots?

RQ: How to build a risk handler for all situations/hazards?

Running Example: Risk-aware Autonomous Vehicle

Example: Situational Perspective of Urban Driving

Mode model of Ego's driving activity:



Hazard Profile:

```
HazardModel for "drive"
{
   OC alias "on occupied
         course"
      ;
   CR alias "increased
         collision risk"
      ;
   CC alias "on collision
          course"
      ;
   ICS alias "inevitable
         collision state"
      ;
   Coll  alias "actual
         collision"
      ;
   ES alias "perception
         system fault"
      ;
}
```

Risk factors

defined in YAP

Example: Risk Identification/Assessment Result: YAP script

Knowledge sources for risk/hazard identification, e.g.

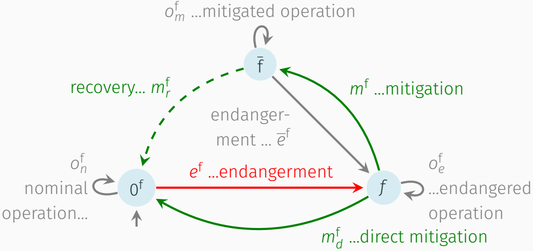
- accident reports
- domain experts
- situation/activity model
- local dynamics model
- control system architecture
- control software

Analysis techniques with focus on

- hazard identification/classification FHA, PHL, ...
- causal reasoning Bowties, ETA, FME(C)A, (D)FTA, ...
- process/scenario analysis BA, HazOp, LOPA, STPA, ...

Risk Structures

Risk Factors (Basic Phase Models of Hazards)


o^f_m ...mitigated operation
$\bar{f}$
recovery... m^f_r
m^f ...mitigation
endanger- ment ... $\bar{e}^f$
o^f_n nominal operation...
0^f
e^f ...endangerment
f
o^f_e ...endangered operation
m^f_d ...direct mitigation

Phase order $\preceq_f$: reflexive transitive closure of $f \preceq_f 0^f, f \preceq_f \bar{f}$

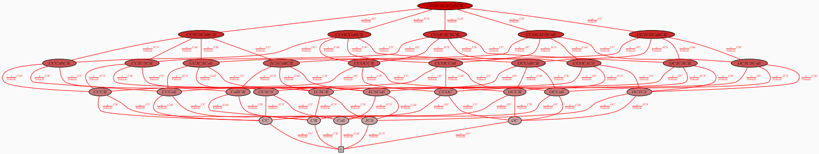
Severity interval for f: $[l, u) \in \mathbb{R}^2$

From Risk Structures to Active Safety Monitors

- Combine and activate all factors

$$\|^{f\in F} f$$

with $F = \{OC, CR, CC, ICS, Coll, ES\}$



Dependencies between Risk Factors (Examples)

causes: activation of f_1 is **propagated** to activation of f_2
to model *forward causal chains*
e.g. inevitable coll. state (ICS) **causes** actual (Coll)ision

requires: activation of f_1 **requires** prior activation of f_2,
to model *backward causal chains*
e.g. coll. course (CC) **requires** increased coll. risk (CR)

excludes: activation of f_1 **invalidates** activation of f_2,
to express *analytical focus*
e.g. coll. course (CC) **excludes** increased coll. risk (CR)

RAV Example: Mitigation Orders

Assessment of mitigations:

- **fully comparable** inclusive mitigation order:

  $$\langle OC 0^{CR} 0^{CC} 0^{ICS} 0^{Coll} 0^{ES} \rangle \preceq_{\mathrm{m}} \langle 0^{OC} 0^{CR} 0^{CC} 0^{ICS} 0^{Coll} 0^{ES} \rangle$$

  $\preceq_{\mathrm{m}}$ reads “more dangerous or riskier than”
- **partially comparable** inclusive mitigation order

  $$\langle OC 0^{CR} 0^{CC} 0^{ICS} 0^{Coll} 0^{ES} \rangle \precsim_{\mathrm{m}} \langle ? \overline{CR} 0^{CC} 0^{ICS} 0^{Coll} 0^{ES} \rangle$$

  where $? = OC$ or $? = 0^{OC}$ and $OC \preceq_{\mathrm{f}} 0^{OC}$, but $0^{CR} \npreceq_{\mathrm{f}} \overline{CR}$
- **strong** mitigation order

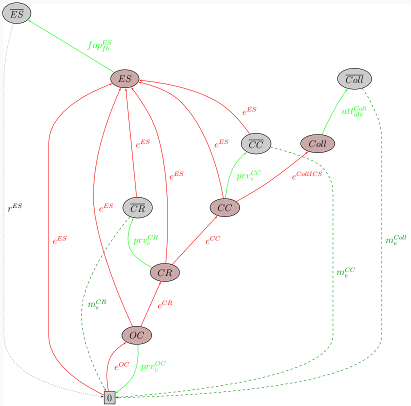
  $$\langle 0^{OC} 0^{CR} 0^{CC} 0^{ICS} Coll\overline{ES} \rangle \leqslant_{\mathrm{m}} \langle 0^{OC} 0^{CR} 0^{CC} 0^{ICS} \overline{CollES} \rangle$$

Summary

Risk Awareness in Autonomous Robots

Why? How?

Risk Structure



Work in progress!

- **Challenge:**
  Autonomous risk handling
  State of the art:
  Design of local handlers
  Problem:
  Design of strategic handlers?
- **Approach:**
  Risk Structure =
  Risk handler
  in specific situation
  for partial hazard profile
- **Vision:**
  Risk-aware behaviour
  in all situations
  for complete hazard profile