Risk Structures: Concepts, Purpose, and the Causality Problem

Mario Gleirscher
University of York, UK

June 26, 2019

Shonan, JP

Part I

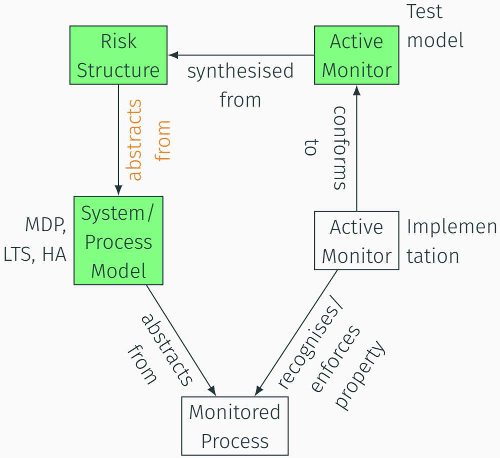
Risk-aware Systems: Abstraction by Example

Example: Air-traffic Collision Avoidance System (TCAS)

Example: Safe Autonomous Vehicle (SAV)

Risk Mitigation / Intervention / Enforcement

Approach: Active safety monitors, enforcement monitors

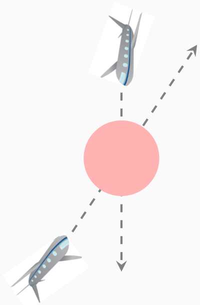


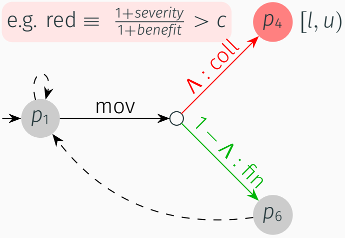
RQ: How to build a mitigation monitor? / Which model to use? / Which abstraction? / What do we need to verify?

Example: Air-traffic Collision Avoidance System (TCAS)

Example: Traffic Collision Avoidance System (TCAS)

Process Model P



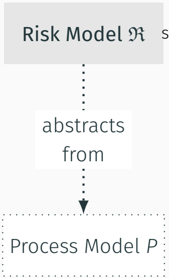


e.g. red $\equiv \frac{1+severity}{1+benefit} > c$

Example: Traffic Collision Avoidance System (TCAS)

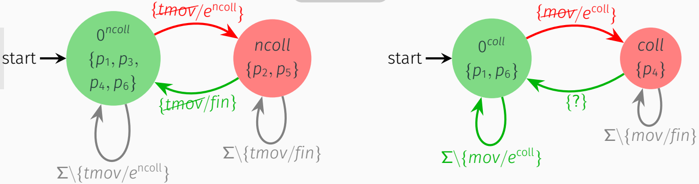
2 Risk Factors

before



near-collision

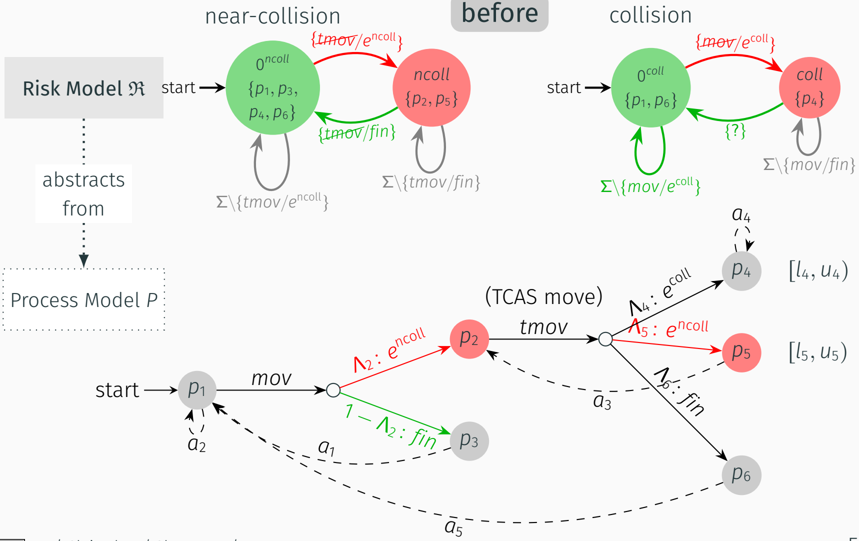
collision



Example: Traffic Collision Avoidance System (TCAS)

2 Risk Factors

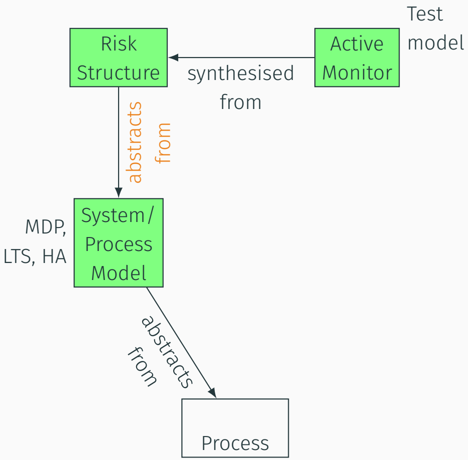
before



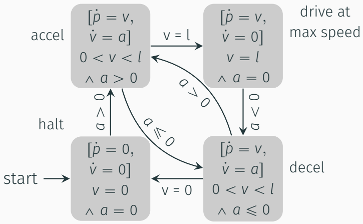
Example: Safe Autonomous Vehicle (SAV)

Risk Mitigation / Intervention / Enforcement

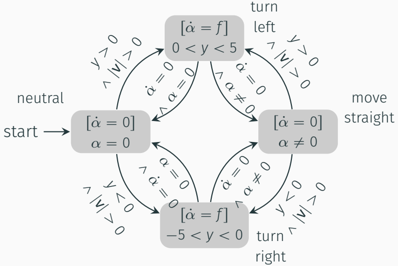
Approach: Active safety monitors, enforcement monitors



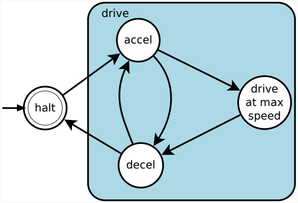
SAV: Low Level Vehicle Dynamics



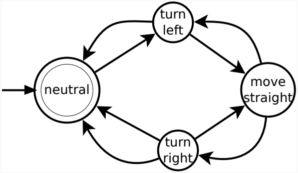
$\|$



Longitudinal dynamics *LoD*



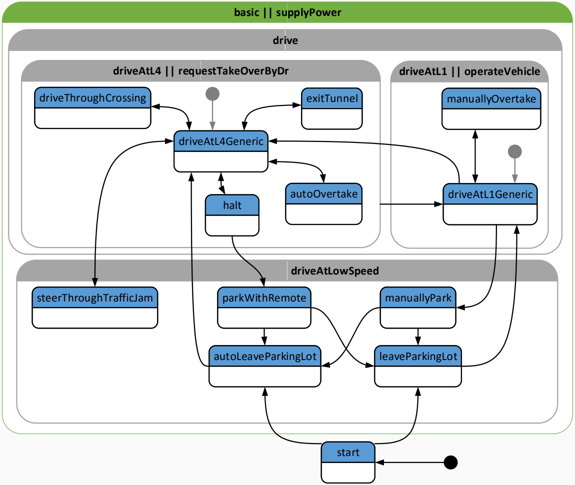
Lateral dynamics *LaD*
(relative to route segment)



Overall low-level dynamics: *drive* || *LaD*

SAV: Situational Perspective of Urban Driving

Mode model of the driving activity:



Integration with low level dynamics:

In each mode, verify contract:

$inv \wedge pre \Rightarrow wp(drive \parallel LaD, inv \wedge post)$

SAV: Risk Identification and Assessment

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

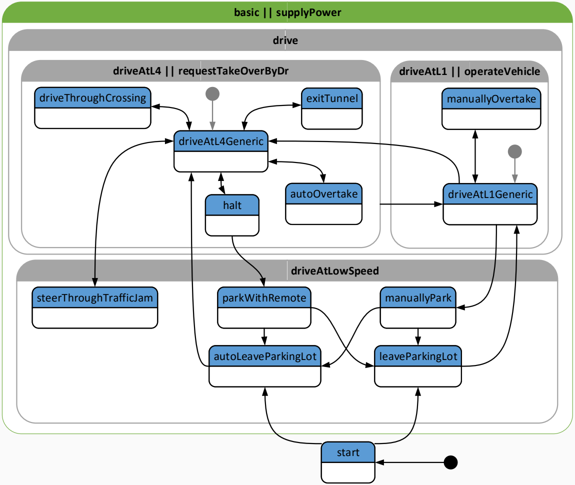
- accident reports
- domain experts
- situation/activity model
- local dynamics model
- control system architecture
- control software

Analysis techniques, e.g.

- hazard identification: FHA, PHL, …
- process/scenario analysis: HazOp, LOPA, BA, STPA, …
- causal reasoning: ETA, FMEA, FTA, Bowties, …

SAV: Situational Perspective of Urban Driving

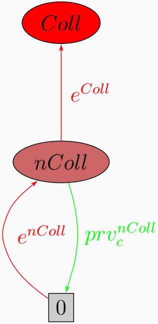
Mode model of the driving activity:



Risk factors (YAP script):

```
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 Structures: Tool Support and Recent Publications



```
OperationalSituation "generic" {}

ControlLoop "Robot" for "generic" {
  emgBr alias "Emergency Brake";
}

HazardModel for "generic" {
  nColl alias "near-collision"
     mitigatedBy (PREVENT_CRASH.emgBr)
     direct;
  Coll  alias "collision"
     requires (nColl)
     mishap;
}
```

From Hazard Analysis to Hazard Mitigation Planning: The Automated Driving Case

Mario Gleirscher and Stefan Kugele

Technische Universität München, Munich, Germany
{mario.gleirscher,stefan.kugele}@tum.de

Abstract. Vehicle safety depends on (a) the range of identified hazards and (b) the operational situations for which mitigations of these hazards are acceptably decreasing risk. Moreover, with an increasing degree of autonomy, risk ownership is likely to increase for vendors towards regulatory certification. Hence, highly automated vehicles have to be equipped with verified controllers capable of reliably identifying and mitigating hazards in all possible operational situations. To this end, available methods for the design and verification of automated vehicle controllers have to be supported by models for hazard analysis and mitigation.

Run-Time Risk Mitigation in Automated Vehicles: A Model for Studying Preparatory Steps

Mario Gleirscher

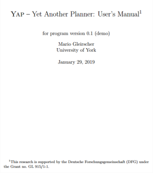
Faculty of Informatics
Technical University of Munich
Munich, Germany
mario.gleirscher@tum.de

8.4 Strukturen für die Gefahrenerkennung und -behandlung in autonomen Maschinen

Dr. Mario Gleirscher
Department of Computer Science, University of York und Fakultät für Informatik, Technische Universität München

2 Hintergrund

2.1 Allgemeine Grundlagen


YAP – Yet Another Planner: User's Manual[1]

for program version 0.1 (demo)

Mario Gleirscher
University of York

January 29, 2019

RISK STRUCTURES: TOWARDS ENGINEERING RISK-AWARE AUTONOMOUS SYSTEMS

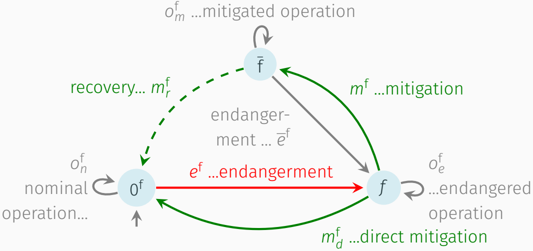
A PREPRINT

Mario Gleirscher
Computer Science Department, University of York, York, UK

April 25, 2019

arXiv:submit/2663380 [cs.SE] 23 Apr 2019

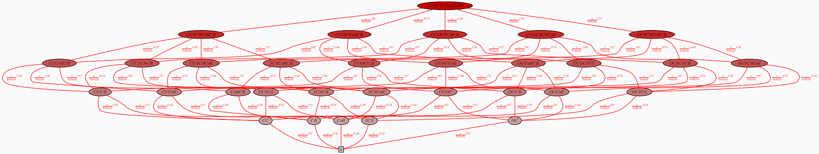
Risk Factors (Basic Phase Model)



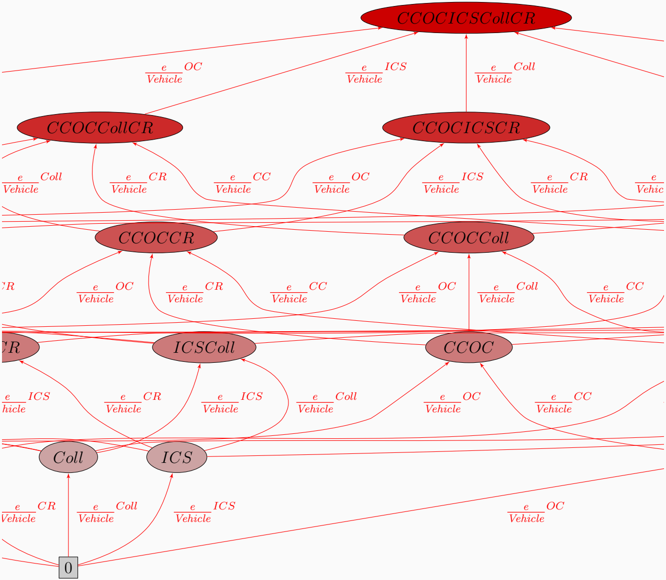
Purposes:

- Modelling primitive for risk space exploration
- Semantics of basic events in DFTs or DFRTs
- Synthesis of local enforcement monitors

SAV: Situational Risk Space



SAV: Situational Risk Space (zoomed)



Causality

(Lewis 1973)

Definition (Counterfactual Conditional)

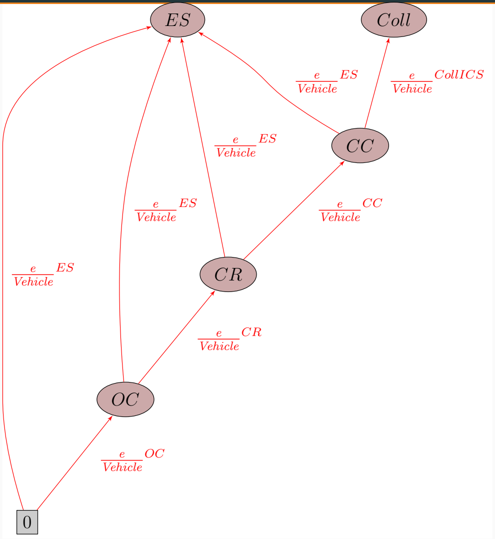
$A \,\Box\!\!\rightarrow C$ is nonvacuously true iff C holds at all the closest A-worlds.

What are the closest A-worlds?

SAV: Risk Identification and Assessment

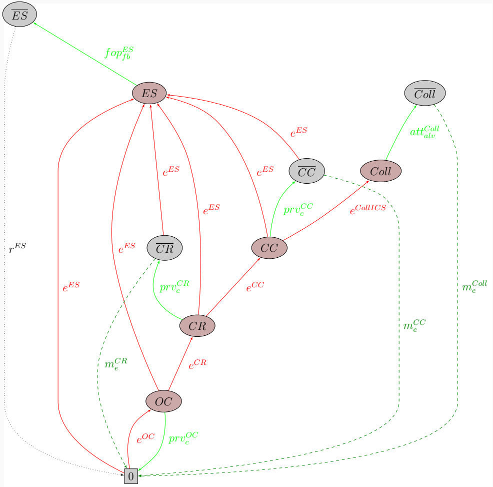
```
OperationalSituation "drive"
{
   include "envPerc";
}

ControlLoop "Vehicle" for "drive"
{
   replan alias "Slow-down || re-plan
         route";
   brake  alias "Standard brake";
   swerve alias "Short-term circumvention
          of obstacle";
   EB     alias "Emergency brake";
   accel  alias "Accelerate";
   airbag alias "Front airbag";
}

HazardModel for "drive"
{
   OC alias "on occupied course"
      mitigatedBy (PREVENT_CRASH.replan)
      direct
      ;
   CR alias "increased collision risk"
      requires (OC)
      deniesMit (OC)
      excludes (OC)
      mitigatedBy (PREVENT_CRASH.EB)
      ;
   CC alias "on collision course"
      requires (CR)
      deniesMit (CR,OC)
      excludes (CR,OC)
      mitigatedBy (PREVENT_CRASH.swerve)
      ;
   ICS alias "inevitable collision state"
      requires (CC)
      excludes (CC,CR,OC)
      causes (Coll)
      mitigatedBy (PREVENT_CRASH.EB)
      ;
   Coll  alias "actual collision"
      requires (ICS)
      excludes (CC,CR,OC,ICS,ES)
      mitigatedBy (ALLEVIATE.airbag)
      mishap
      ;
   ES alias "perception system fault"
      excludes (CC,CR,OC,ICS)
      deniesMit (OC,CC)
      ;
}
```

SAV: Situational Risk Space



Approach: LOPA/BA to create chain of possible interventions

SAV: Situational Risk Space

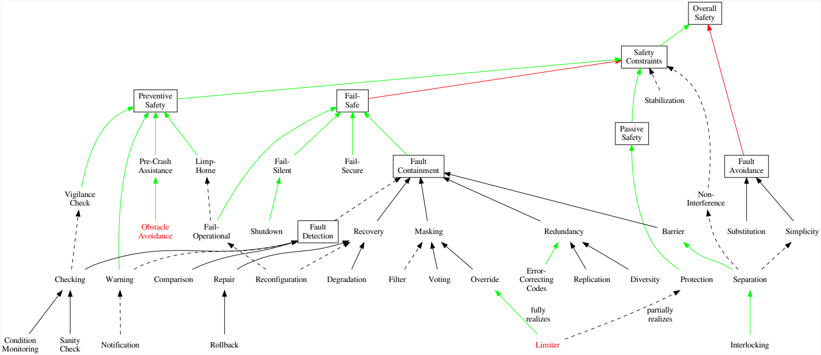


Approach: LOPA/BA to create chain of possible interventions

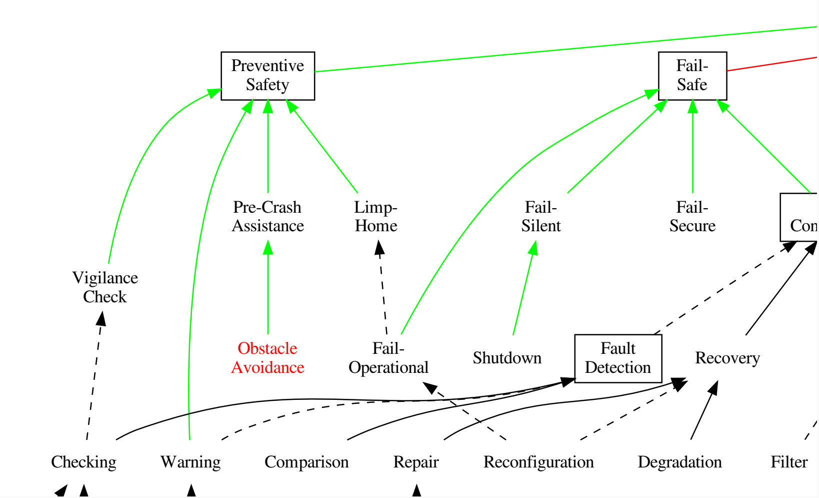
Layered intervention pattern for SAV **obstacle avoidance**

Nice side-effect: Use pattern as enhanced phase model for similar risk factors

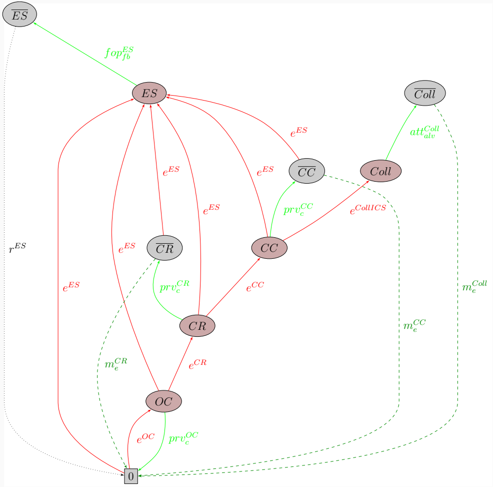
Taxonomy of Mitigations



Taxonomy of Mitigations



SAV: Situational Risk Space (Monitor Candidate)



Approach: LOPA/BA to create chain of possible interventions

= Specification of a valid safe system

expected order violated → lack of *observability*, *incomplete* monitor, context *mismatch*?

Risk Structures: Templates for Causal Reasoning

A risk structure $\mathfrak{R}$ is *valid* iff for

$$s, s', s'', s''' \in R(F), \quad s''' \in Mishaps, \quad e, m, e' \in \Sigma^*$$

$$\forall s, s''' \in R(F), t \in \mathfrak{R}\, \exists s', s'' \in R(F), m \in \Sigma^* : t = eme' \wedge$$

$$\begin{tikzcd} \mathrm{s} \arrow[r, "\mathrm{e}"] & \mathrm{s'} \arrow[r, "\mathrm{m}"] & \mathrm{s''} \arrow[r, "\mathrm{e'}"] & \mathrm{s'''} \end{tikzcd}$$

Definition (Mitigation from Counterfactual Perspective)

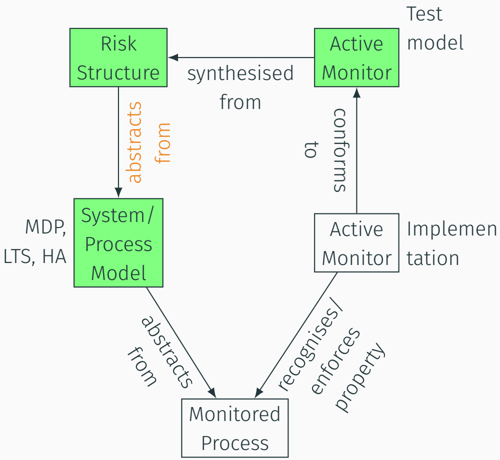
m is mitigation of cause $c \neq s''$ of a mishap s''' iff e' gets unlikely. (s'', e' form the counterfactual.)

Proof obligations for each t: Check that, from s,

1. s'' is actual *cause* of s''',
2. s' is *recognisable*,
3. from s', *m reduces s''*.

Risk Mitigation / Intervention / Enforcement

Approach: Active safety monitors, enforcement monitors


Test model
Risk Structure
synthesised from
Active Monitor
abstracts from
conforms to
MDP, LTS, HA
System/ Process Model
Active Monitor
Implementation
abstracts from
recognises/ enforces property
Monitored Process