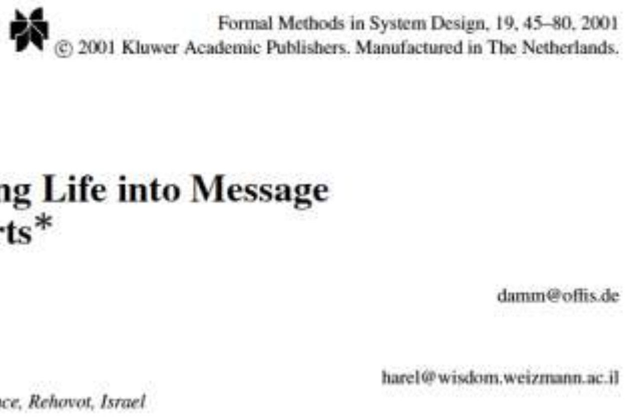
# On the no´s and must´s in system design

**Werner Damm**

**joint work with Bernd Finkbeiner, Universität des Saarlandes, and Astrid Rakow, Carl von Ossietzky Universität Oldenburg**

# Thanks, David!



Formal Methods in System Design, 19, 45–80, 2001
© 2001 Kluwer Academic Publishers. Manufactured in The Netherlands.

**LSCs: Breathing Life into Message Sequence Charts***

WERNER DAMM damm@offis.de
*OFFIS, Oldenburg, Germany*

DAVID HAREL harel@wisdom.weizmann.ac.il
*The Weizmann Institute of Science, Rehovot, Israel*

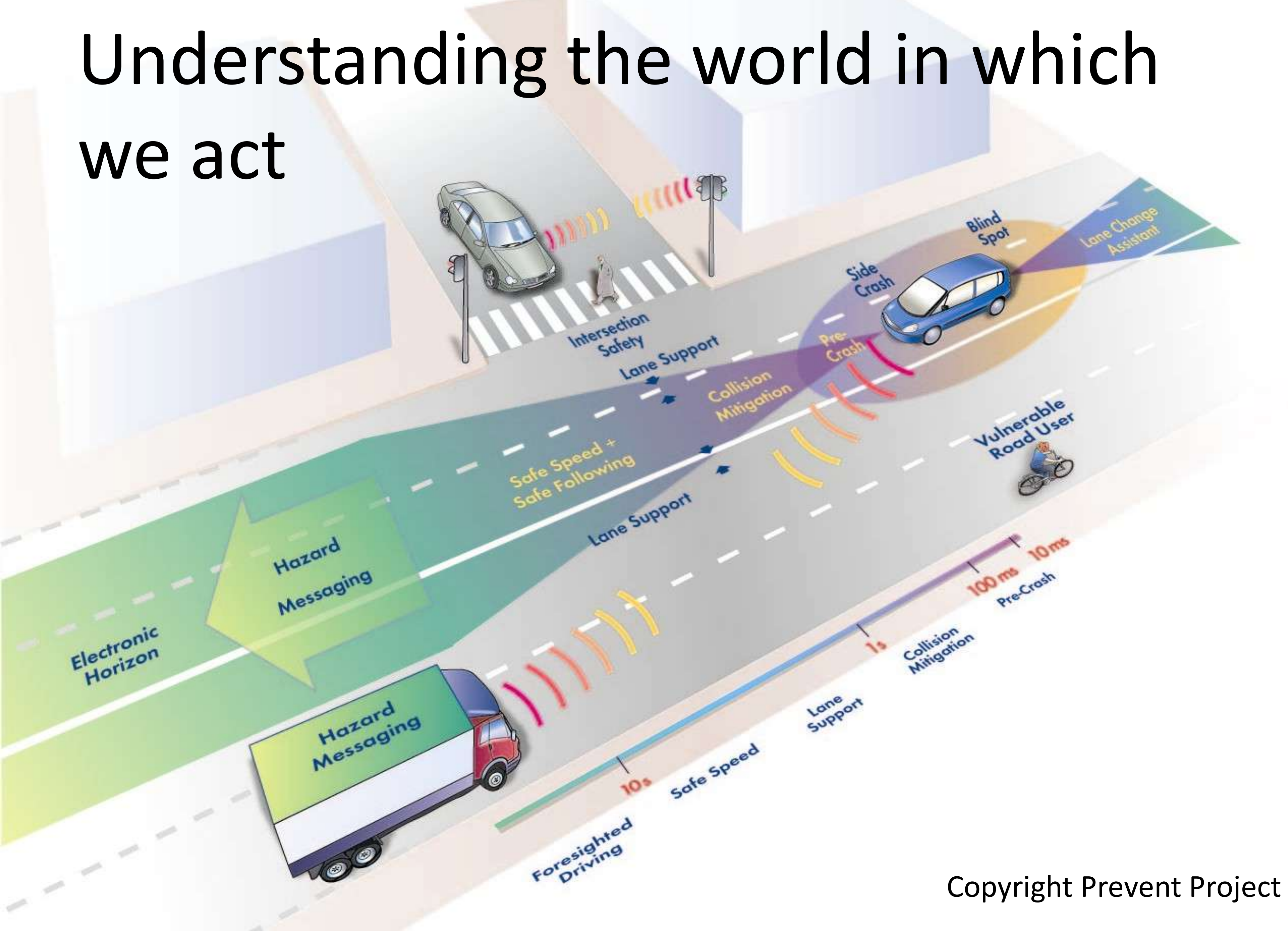
- "… Mandatory conditions (that is, hot ones), together with other hot elements, make it possible to specify *forbidden scenarios,* i.e., ones that the system is not allowed to exhibit. This is extremely important and allows the behavioral specifier to say early on which are the "yes-stories" that the system adheres to and which are the "no-stories" that it must not adhere to.

# Structure of Presentation

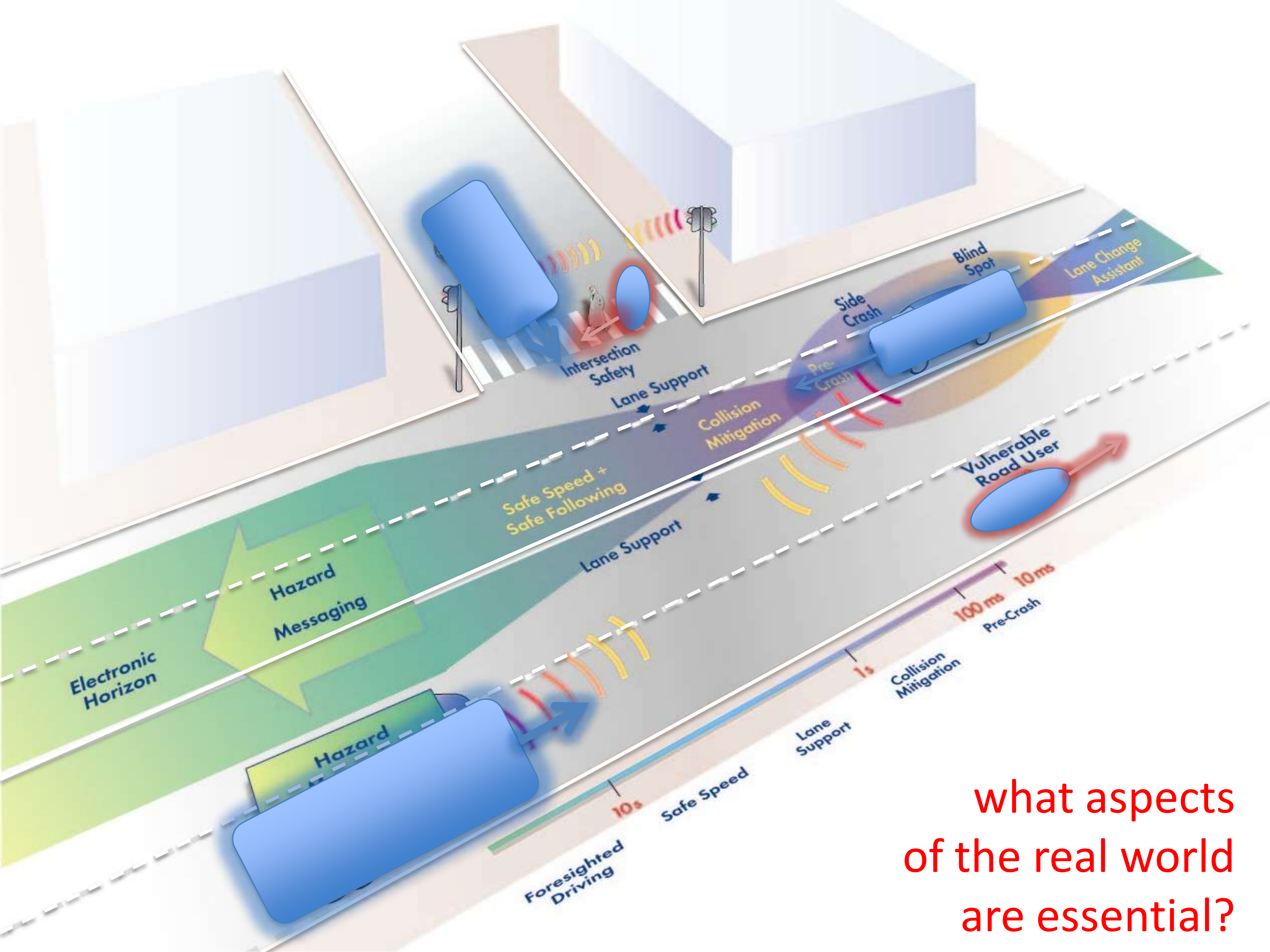
- Motivation
- Optimal World Models
- Compositional Synthesis and Weakest Assumptions
- Strong and Weak Assumptions
- An industrial vision
- Conclusion

# MOTIVATION

# Understanding the world in which we act



Copyright Prevent Project



what aspects
of the real world
are essential?

The discrepancy between the real world and what the aircraft perceives as real decide over life and death

14.09.1993 -
Aircraft thought it was still airborne, because only two tons weight lasted on the wheels due to a strong side wind and the landing maneuver. The computer did not allow braking.
*The plane ran over the runway into a rampart.*

# THE SYSTEM ENGINEERING CHALLENGE

Given

a (physical) system S under development

what real-world aspects

could potentially impact S

in a way that endanger its proper functioning?

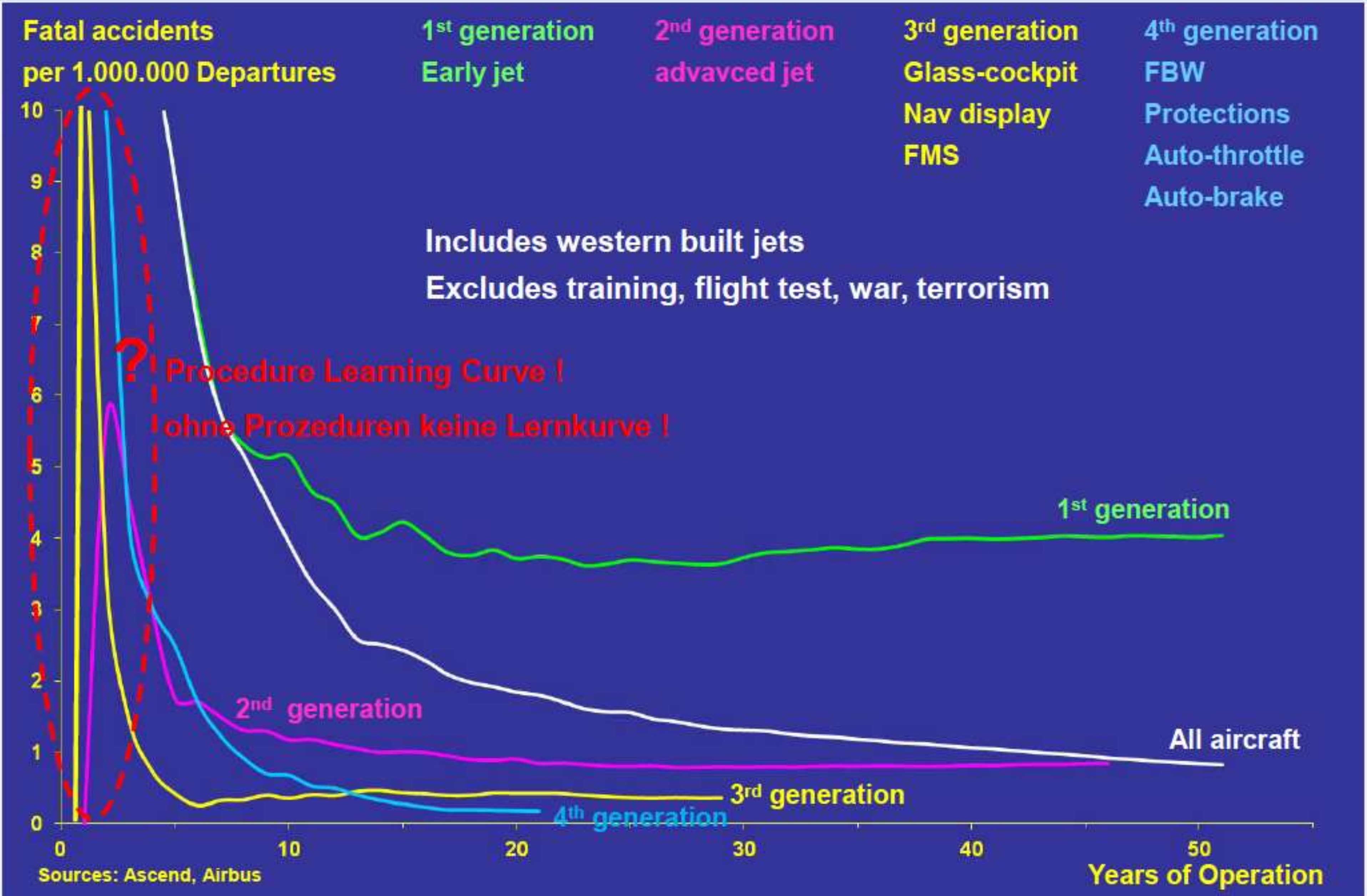
# Questions

- are all “relevant” real-world artifacts part of my world model?
- can the system observe all “relevant” real-world artifacts?
- can we characterize (formally) the notion of “relevance”?
- is there a notion of optimal world models?
- can we characterize the environments, into which our system can be safely deployed?

# Industrial Practice: learning processes

- Company XY
  - all flight incidents are analyzed
  - to identify the process step in which the potential for an incident should have been detected
  - existing models are extended to allow the prediction of such potential incidents
  - measures protecting against such hazards are integrated into the design (and aircrafts)
  - safety processes are used to demonstrate resilience against root cause for such hazards

# Fatal Accident Rate since Entry Into Service – valid through 2010



Includes western built jets

Excludes training, flight test, war, terrorism

Procedure Learning Curve !

ohne Prozeduren keine Lernkurve !

Sources: Ascend, Airbus

# Why we should be concerned

- Even in aerospace learning curve approach fails with introduction of new a/c generation
- Increasing degrees of automation in driving necessitates rigorous measures for qualification / certification of employed world models

# Structure of Presentation

- What is “relevant”: a theoretical approach
- Compositional Controller Design
- On no´s and must´s in system design
- Industrial Deployment
- Conclusion

# WHAT IS RELEVANT? A THEORETICAL APPROACH

# World Models I

- Let $V_S$ be a finite set of *system variables*
  - modeling actions under the system's control, such as the setting of actuators
- $\boldsymbol{V_E}$ be an **arbitrary** set of *environment variables*,
  - in the context of control theory corresponding to the variables of the plant model
- Environment variables are partitioned into disjoint sets of
  - *disturbances* $\boldsymbol{V_D}$

    modeling *uncontrollable environment observations*, and
  - *controllable environment variables* $V_C$

    modeling phenomena in the environment which can be influenced by the system through the system variables

# World Models II

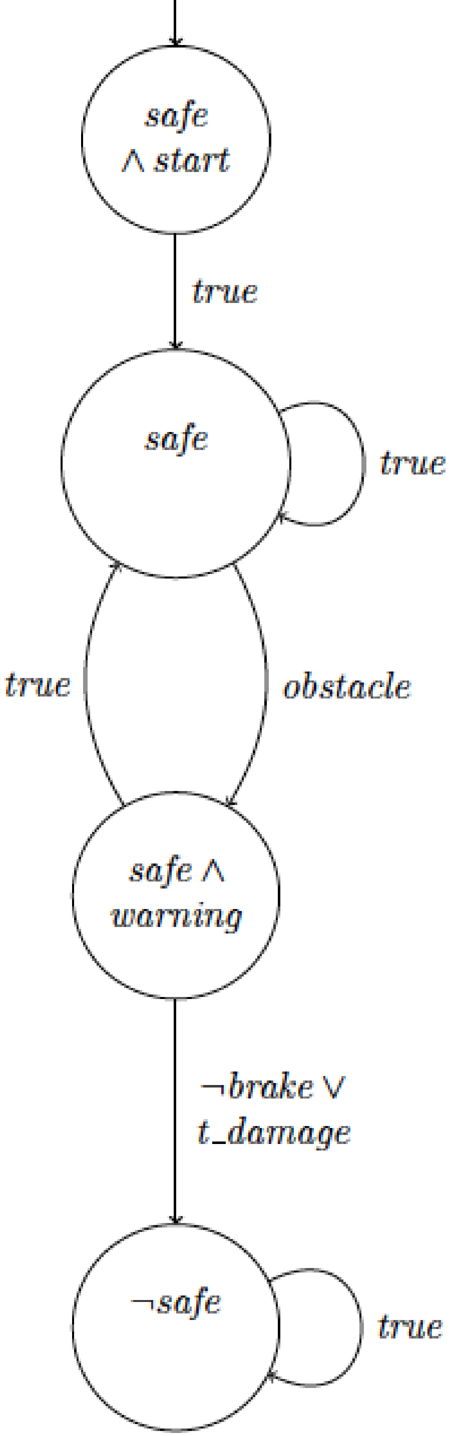
- restrict only a finite subset $V_E \subseteq \boldsymbol{V}_E$ called the *perimeter* of the world model
- assign *arbitrary* valuations to the environment variables outside the perimeter of the model
- We assume finitely typed variables, wlog of type boolean

# World Models III

A *world model* is a tupel

$$M = (V_E, N, n_0, E, L_N, L_E)$$

- $V_E \subseteq \mathbf{V}_E$ is the *perimeter* of the world model
- $N$ is a possibly infinite set of *nodes*, $E \subseteq N \times N$
- $L_N : N \rightarrow P(P(V_C))$ assigns sets of valuations of controllable variables which agree on the variables within the perimeter of the model (intuitively: state of the plant)
- $L_E : E \rightarrow P(P(V_S \cup \mathbf{V}_D))$ defines for each edge sets of system moves and disturbances (which agree on the variables within the perimeter of the model)



# A simple world model

... for an ADAS to maintain **safe distance to objects ahead** on same lane (cars, cargo, ...), two lane hwys,

*secondary objective* **avoid braking**

disturbances

appearance of an obstacle

tire-burst

controllable actions

brake

states

safe: the distance to the object ahead of the ego car is greater than some constant

warning: an obstacle has been detected ahead of the ego car

The world model explains how the plant state changes depending on disturbances and controllable actions

# From yes/no to: could we do better?

- No world model will ever be complete
- Hence no formal verification of a cyber physical system can “guarantee” safety (e.g. no crash)

We *“measure” the benefit of extending a world model W*

to include a new real world artifact  a

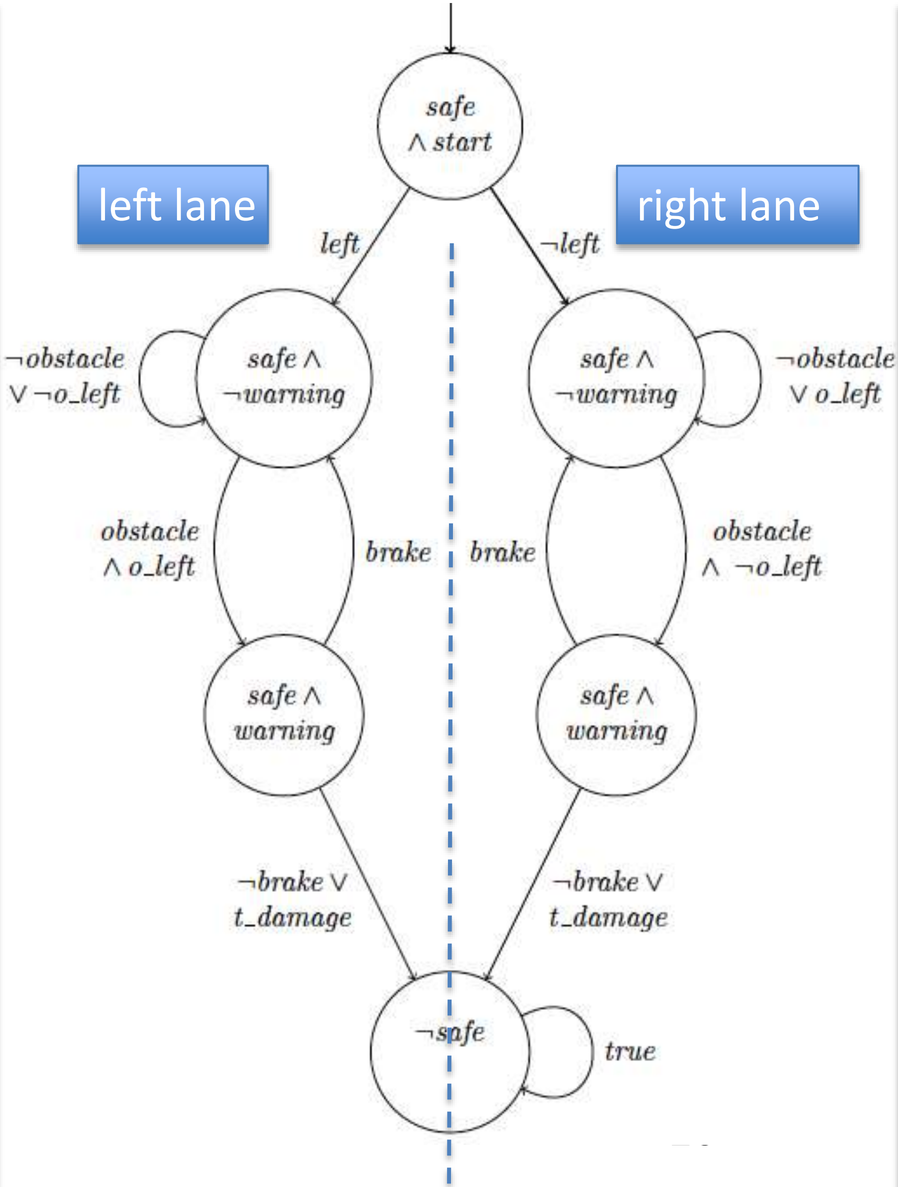
by comparing the strategic capabilities of W and W∪{a}:

**Does the richer world model allow to define strategies,**

**which, in comparable environment moves,**

***allow more often to achieve the systems objective*?**

# A richer world model



disturbances

appearance of an obstacle

o_left: on left lane

tire-burst

controllable actions

brake

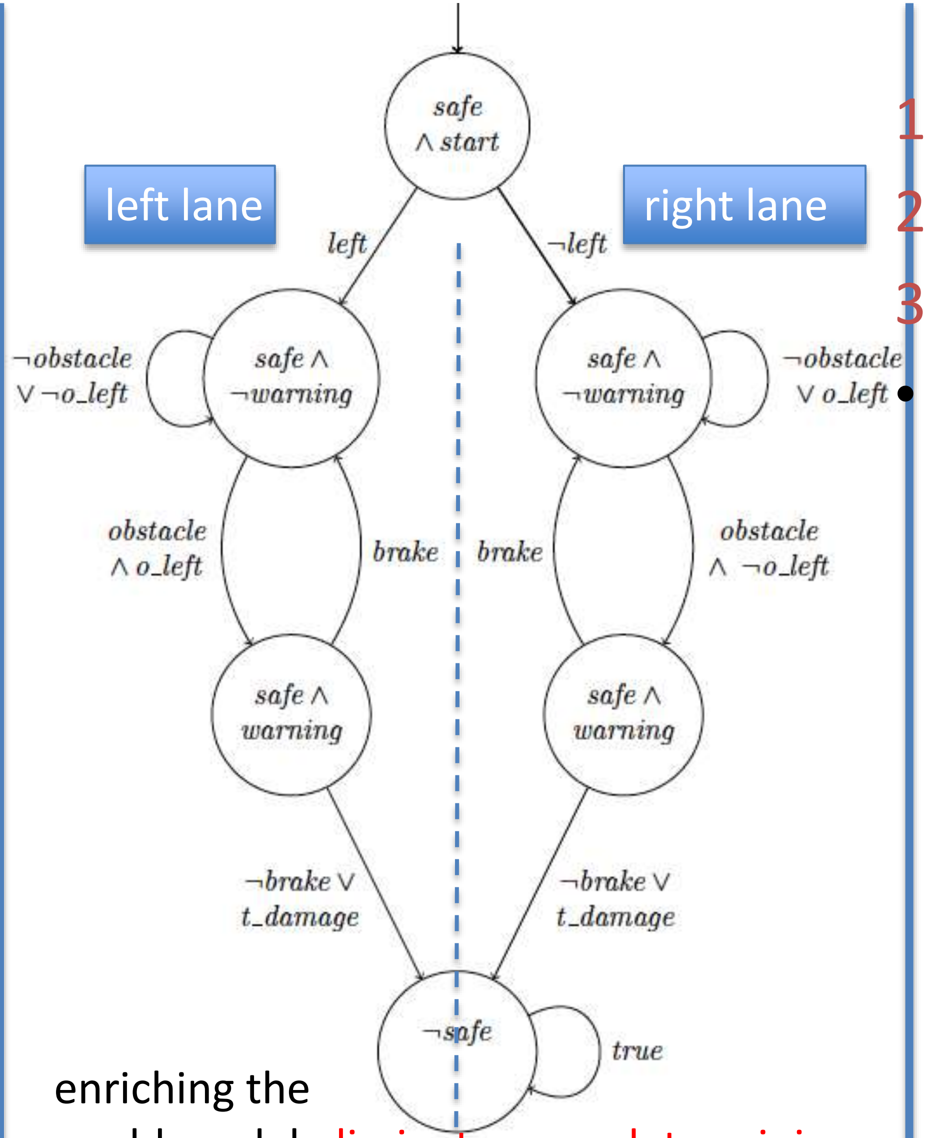
left: take left lane

states

safe: the distance to the object ahead of the ego car is greater than some constant

warning: an obstacle has been detected ahead of the ego car

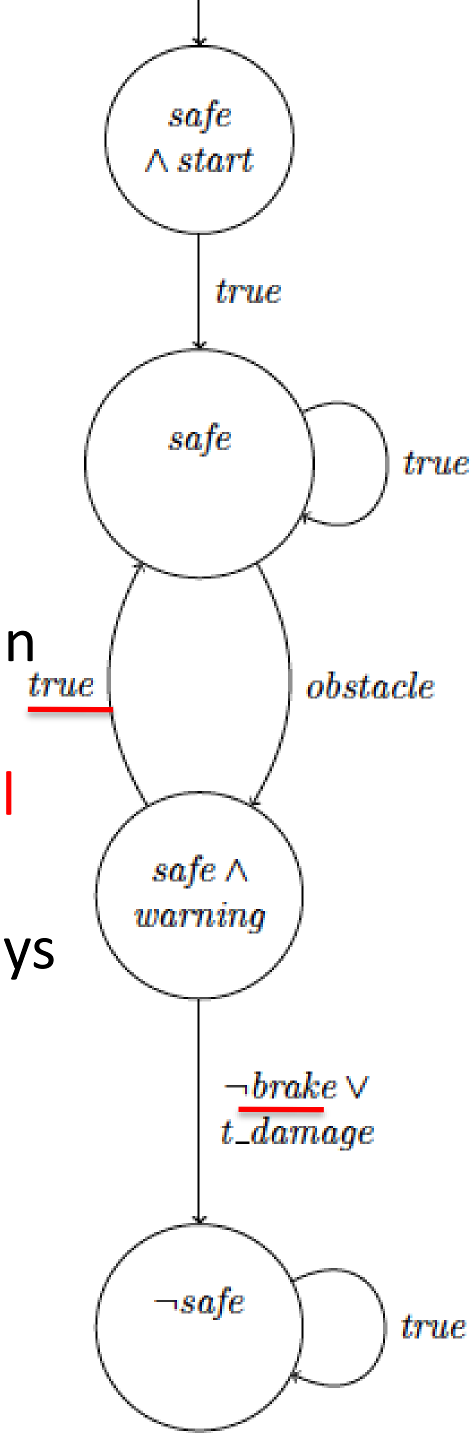
# Beyond YES/NO



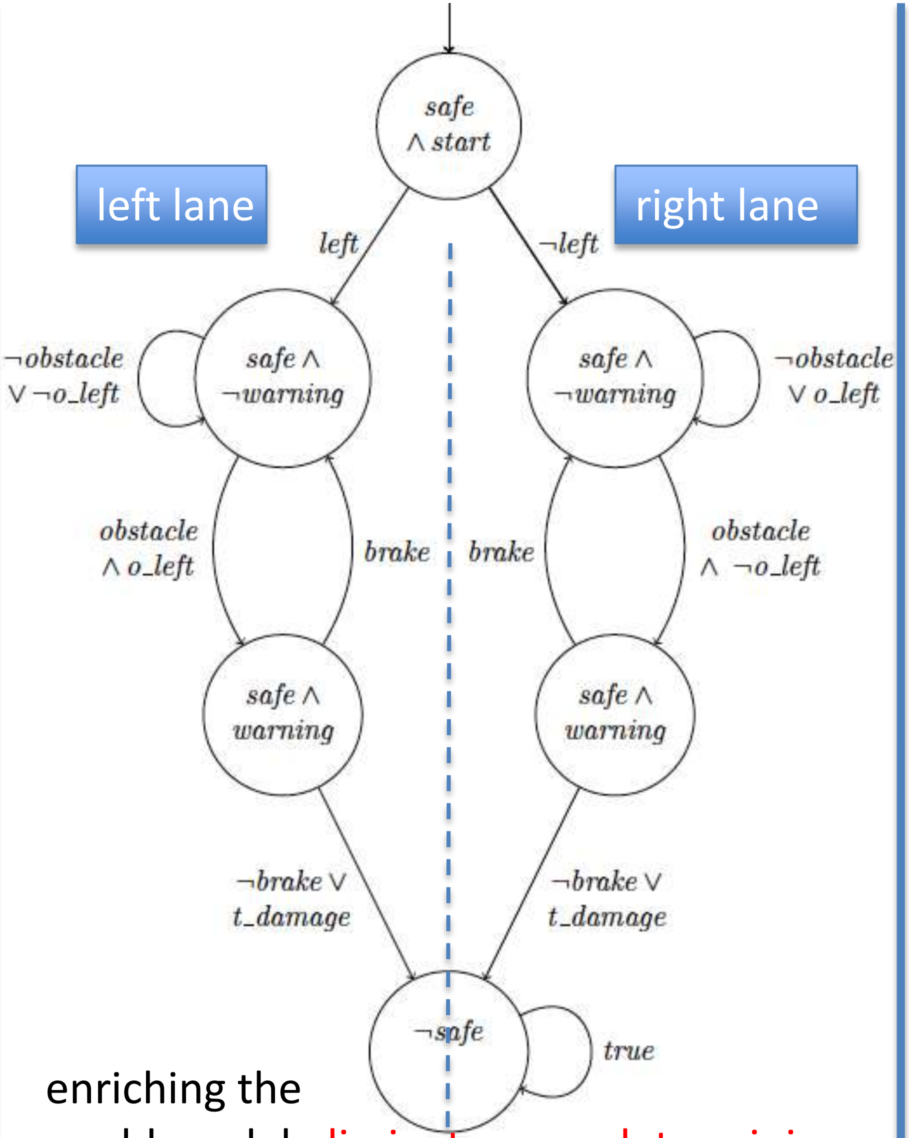
enriching the world model eliminates non-determinism

1. Never brake
2. Brake iff warning
3. Brake always

- all strategies fail in both models to always achieve all objectives: tire damage can always cause system to become unsafe



# Comparing strategies: remorse-free dominance



enriching the world model eliminates non-determinism

$s_1$ Never brake

$s_2$ Brake iff warning

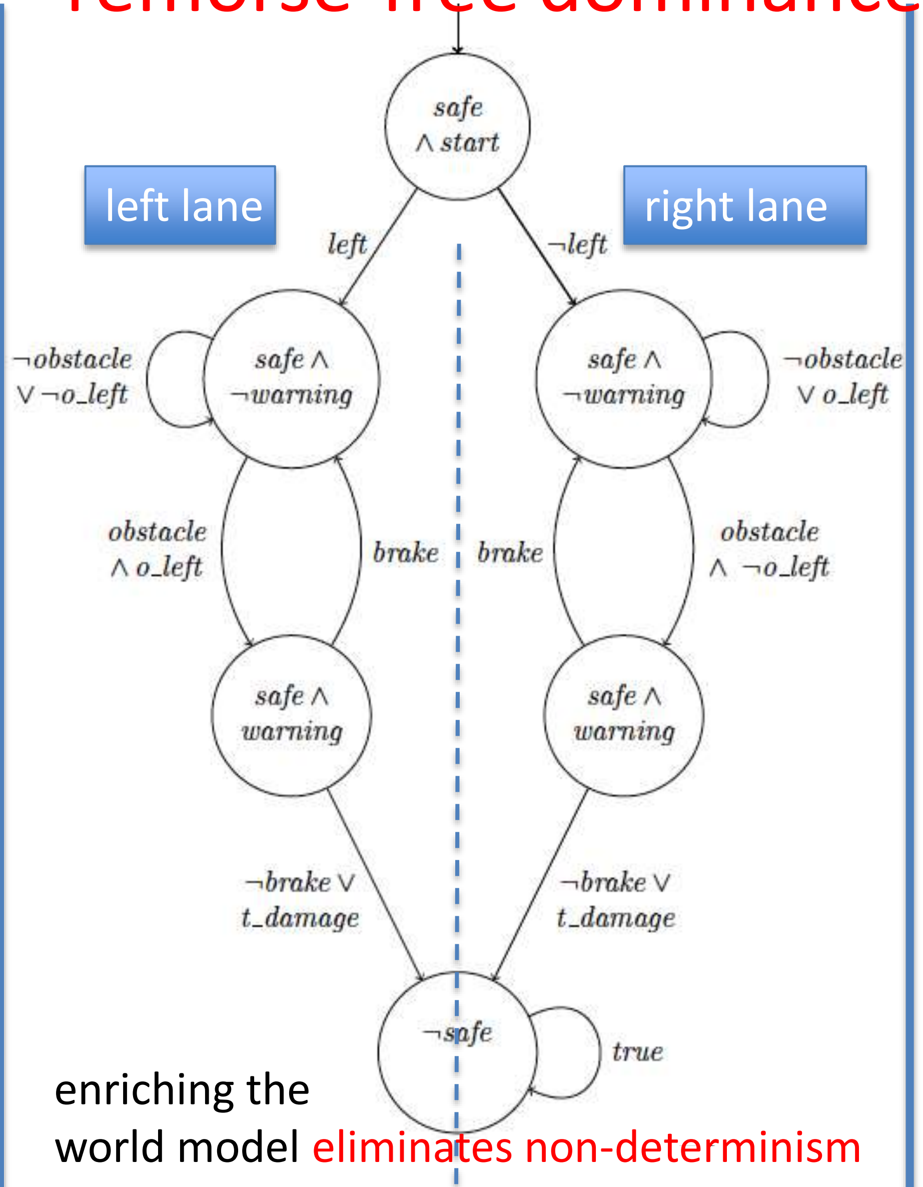
$s_3$ Brake always

- compare strategies wrt remorse: *could I "have done better"* = achieved higher priority objectives

*in "comparable situations"* = same sequence of disturbances

- $s_2$ dominates $s_3$:
  - whenever $s_3$ achieves up to prio_x in some sequence of disturbances, so will $s_2$
  - but $s_2$ avoids (unnecessary) braking in safe state with no warning

# Comparing strategies: remorse-free dominance



enriching the
world model eliminates non-determinism

$s_1$ Never brake

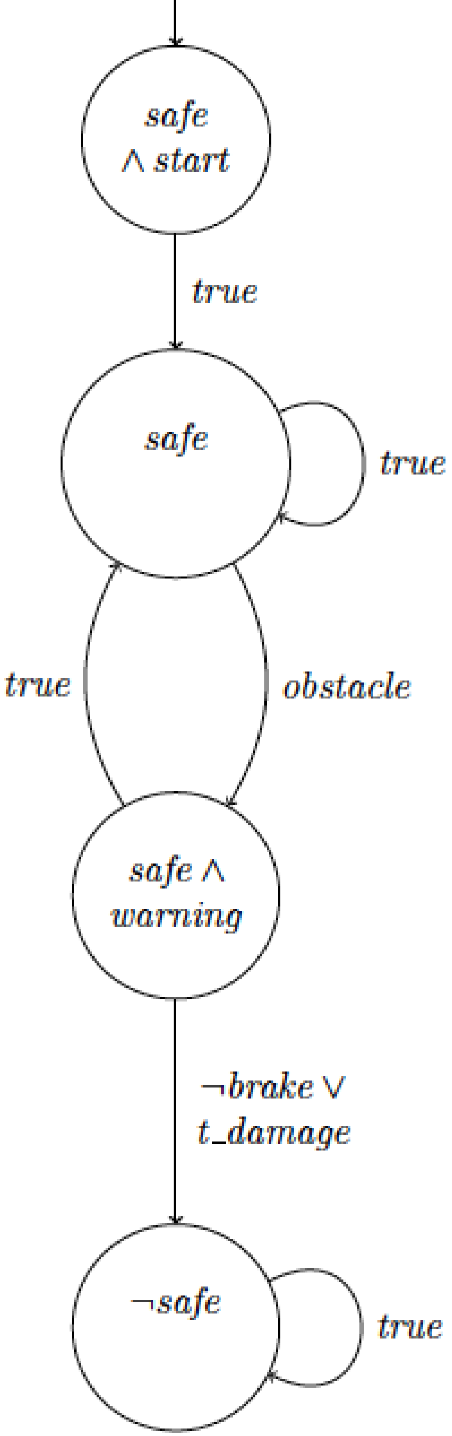
$s_2$ Brake iff warning

$s_3$ Brake always

- compare strategies wrt remorse: *could I "have done better"* = achieved higher priority objectives

*in "comparable situations"* = same sequence of disturbances

- $s_2$ dominates $s_1$:
  - whenever $s_1$ achieves up to prio_x in some sequence of disturbances, so will $s_2$
  - but $s_1$ can cause crash in sequences of disturbances where $s_2$ will remain safe



$s_1$ Never brake

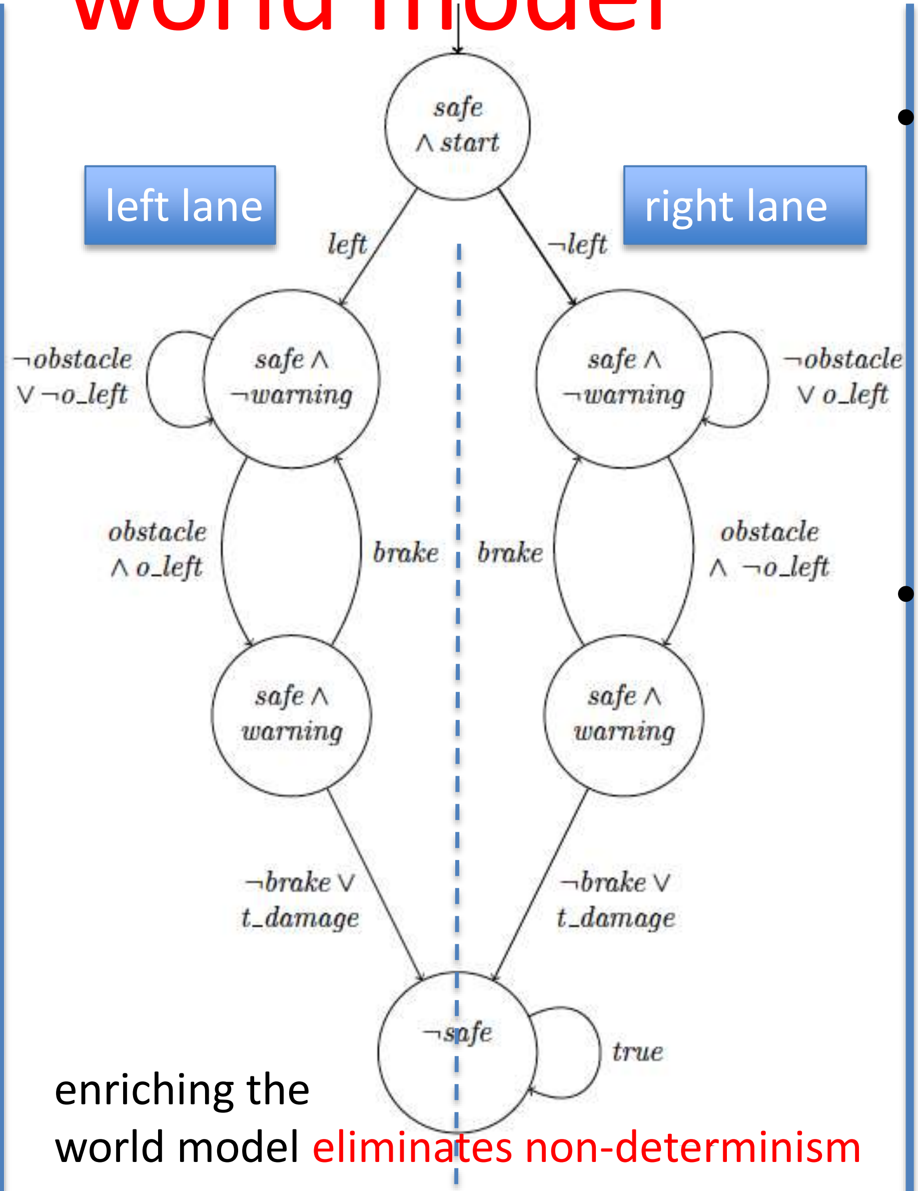
$s_2$ Brake iff warning

$s_3$ Brake always

- $s_3$ is not dominant, because it brakes even in the middle safe state, where there is no danger for safety (hence braking is causing remorse because both $s_2$ and $s_1$ avoid this)
- $s_1$ does not dominate $s_2$ , because it does not avoid crashes in sequences of disturbances, where this is avoided by $s_2$
- $s_2$ does not dominate $s_1$, because for some sequence of disturbances braking is not necessary to avoid crash (if obstacle is on other lane)

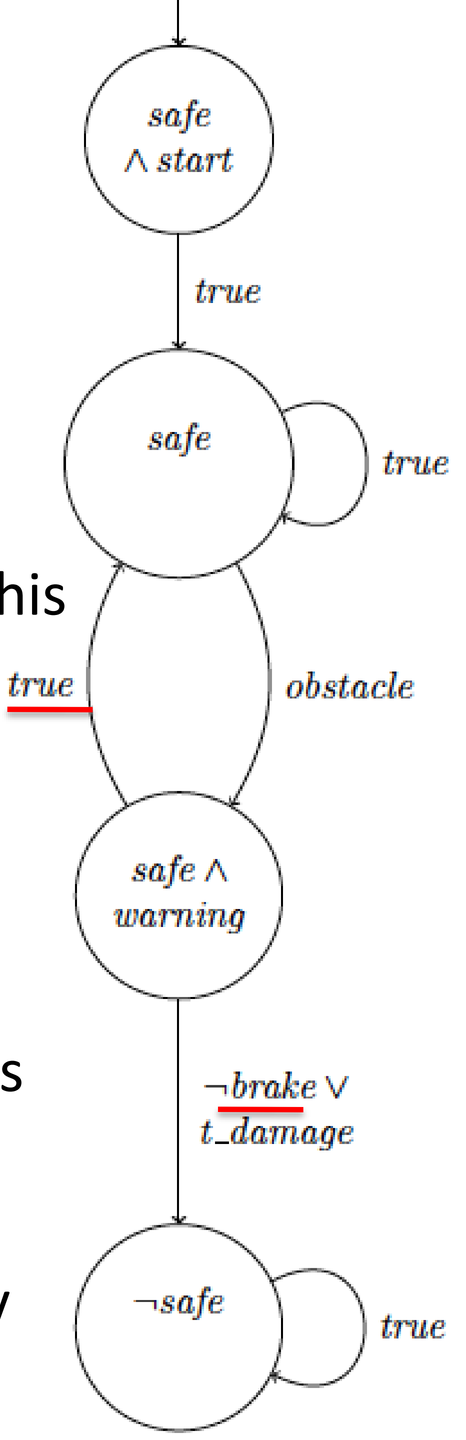
The simple world model does not permit a dominant strategy

# It paid to enrich the world model



enriching the world model eliminates non-determinism

- In the refined model, there is a “best in class” strategy: picking this will never cause remorse
- The simple model does not contain sufficiently many real world artifacts so as to allow construction of a dominant strategy



# Optimal world models

- Intuitively, given a fixed set of prioritized objectives, only a subset of all real world artifacts are required to define the "best possible strategy" for these objectives

A world model W is optimal
if it allows do define a ("best") strategy
which not only dominates all other strategies in W,
but also those definable in all refinements of W

# Optimal world models

A world model W is optimal
if it allows do define a ("best") strategy
which not only dominates all other strategies in W,
but also those definable in all refinements of W

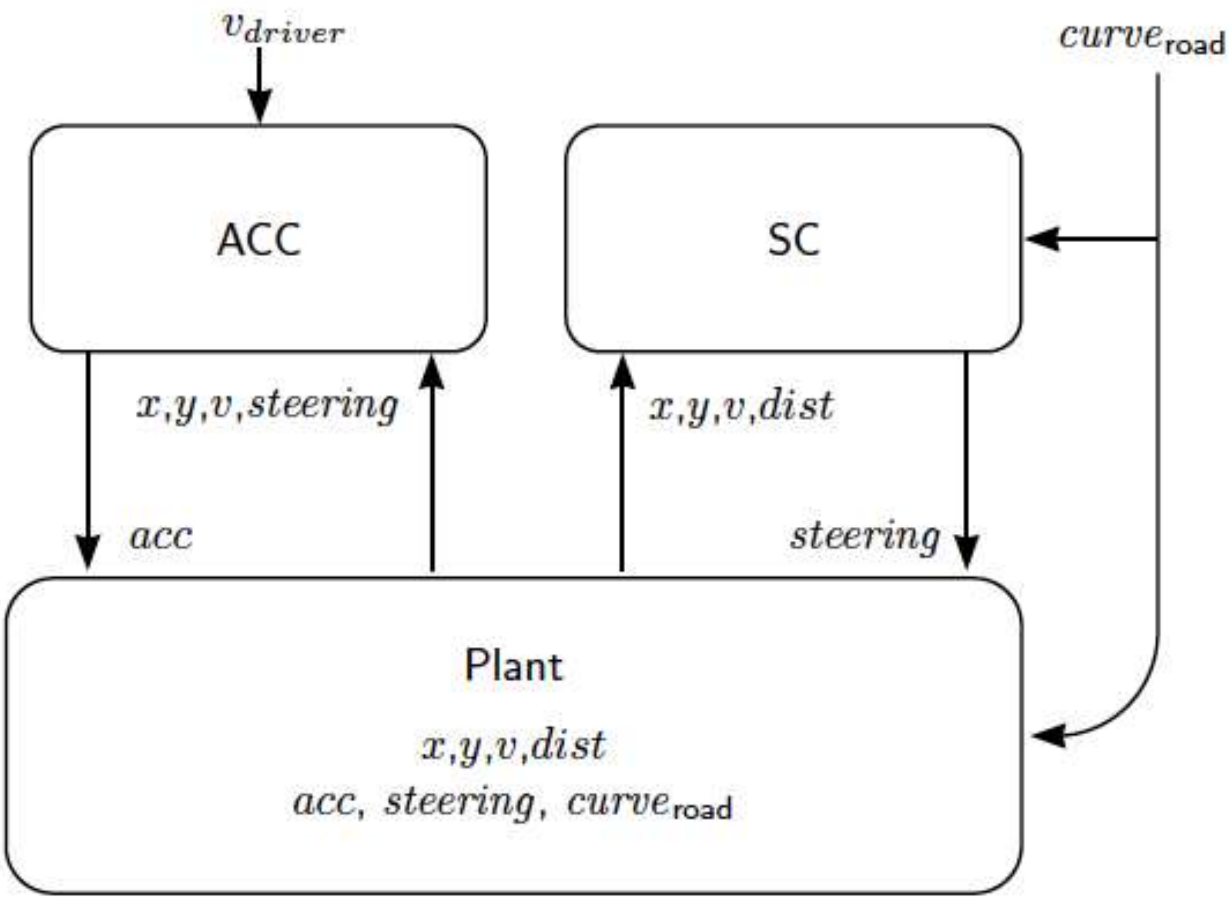
Theorem

Let W be a world model, ϕ an objective specification given as prioritized list of LTL formula

(1) We can automatically check whether W is optimal for ϕ
(2) If true, we can automatically synthesize a „best" strategy

# CONTRACT BASED CONTROLLER DESIGN

# A running Example



# Control objectives

1. top priority: maintain stability of the car

$$\varphi_{global} = \Box((\mu \cdot g)^2 - (\frac{v^2}{r})^2 \geq acc^2)$$

2a. keep car on lane

$$\varphi_{SC_{high}} = \Box(|dist| \leq 0.5 \cdot width_{lane})$$

2b. approximately achieve driver selected speed

$$\varphi_{ACC_{high}} = \forall \hat{v} : \Box((\uparrow_{v_{req}} \wedge \Box_{\leq t_{\Delta}} \hat{v} = v_{req}) \Rightarrow$$
$$(\Diamond_{\leq t_{\Delta}}((v \;\; is \;\; v_{req} \pm x\%) \mathsf{U} (\uparrow_{v_{req}} \wedge (v_{req} \neq \hat{v}))))$$

3a. follow center of lane

$$\varphi_{SC_{low}} = \Box(|dist| \leq 0.2 \cdot width_{lane})$$

3b. follow driver selected speed almost exactly

# Contract Based Design

- Given an objective specification
- under which assumptions on the environment will the system be able to meet its objectives (up to priority n)
- contract: pair of assumptions, objective spec (for each priority)

# Contract Based Design

Examples

- assumptions of the combined ACC-SC relate to the interaction with the driver in choosing a desired speed, and to the evolution of the street (e.g. curvature of the next road segment).
- assumptions of the ACC controller additionally relate to uncontrolled plant actuators, such as the actuators of the lanekeeping controller, SC.

# Admissable objective specifications

- We provide automatic methods adressing these for *admissable* specifications
- An objective specification is called *admissible wrt world model M* if it possesses a remorse-free dominant strategy
- Intuitively, a specification is admissible as long as we do not require a process to “guess” variables it cannot see or to “predict” future inputs.

# Example

- The objective specification

  $$\varphi_{ACC} = \langle \varphi_{global}, \varphi_{ACC_{high}}, \varphi_{ACC_{low}} \rangle$$

  is not admissible, because no strategy can predict the future settings of steering control

  - s hopes for non-interference of SC, and achieves $\varphi_{ACC_{low}}$ when no interference
  - s´ bets on interference, and gives up $\varphi_{ACC_{low}}$
  - s and s´ are incomparable

# Weakest Environment Assumptions

Given

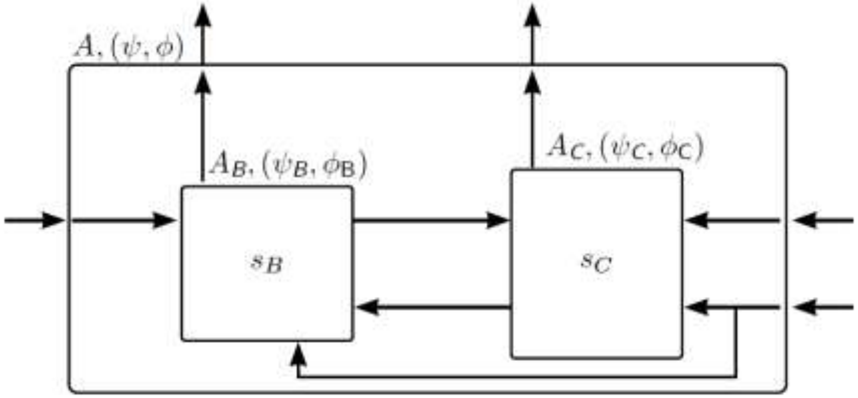
- an objective specification $\phi_A$ admissible for A together with its static interface

we can effectively compute

- a remorse-free dominant strategy s(A, $\phi_A$)
- a (weakest) environment assumption w(A, $\phi_A$)

s.t. s(A, $\phi_A$) is winning for $\phi_A$ iff the environment of A satisfies w(A, $\phi_A$)

# Incremental Design



- Assume A is to be realized by using C already meeting subset $\phi_C$ of A´s objectives $\phi_A$
- *Can we find a specification $\phi_B$ of subsystem B, s.t. when put together with C,*

  *any implementation of $\phi_B$ will jointly meet $\phi_A$ whenever the assumptions derived in B's contracts and assumptions of C relating to the environment of A are met?*

# Incremental Design Theorem

- Given
  - an objective specification $\phi_A$ admissible for A together with its static interface and subsystems B, C, with their interfaces and their interconnection structure,
  - a subset $\phi_C$ of $\phi_A$ admissible for C
  - a remorse-free dominant strategy $s_C$ realizing $\phi_C$ under assumptions $\psi_C$.

# Incremental Design Theorem

Let $\phi_B = \text{Rem}(\phi_C, \phi_A) \wedge \psi_C$ be admissable for B

Then

for any remorse-free dominant strategy $s_B$ realizing $\phi_B$

$s_C$⍰$s_B$ is remorse-free dominant for A and $\phi_A$

# ON NO´S AND MUST´S IN SYSTEM DESIGN

# introducing modalities

- **Strong** assumptions characterize allowed design context
  - – If component´s environment does not meet strong assumption, product liability does not apply
- **Weak** assumption define a subspace of the allowed design context
  - – Example: different conformance levels
  - – Example: different degradation levels

# Example I (autonomous driving)

- highly autonomous driving requires sufficient levels of coherency between relevant real world objects and digital world model used by car
- weak assumptions characterize conditions on environment (light, road surface) and health state of complete sensor chain under which this functionality is available
- strong assumptions state that when autonomous driving is allowed to be active: health state of complete sensor chain is ok, and no dangerous environment conditions prevail

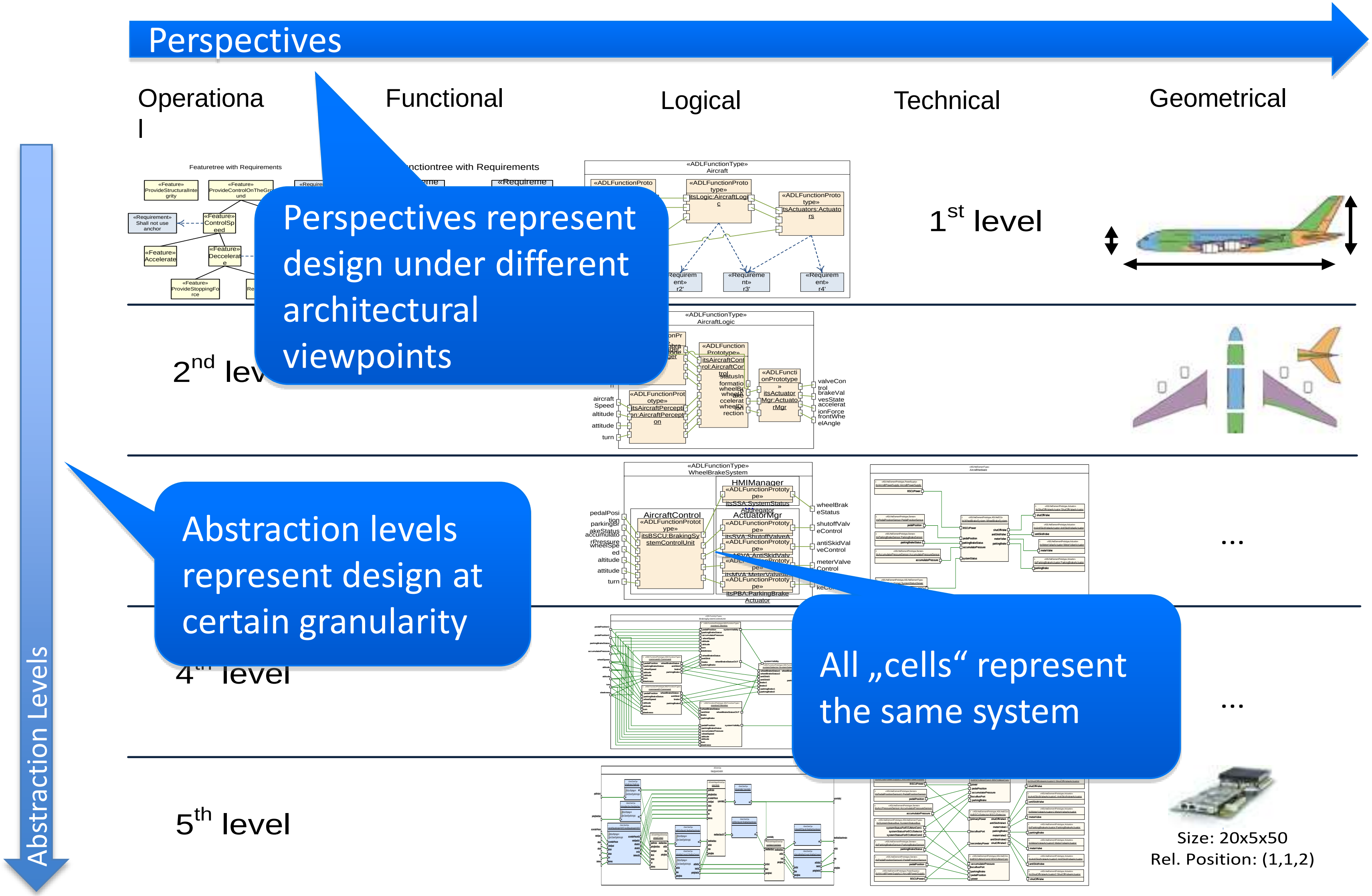
# Example II (safety)

- when using world models incorporating failure modes and failures, the methods discussed allow to automatically derive failure hypothesis under which the system is guaranteed not to reach top-level hazards
- strong assumptions characterize e.g. requirements on allowed component failure types induced from overall safety assurance levels

# weak and strong assumptions

- Weak assumptions can in principle be generated automatically using approach of previous sections, but will most likely be derived manually, using adaptations of methods like fault-tree analysis to general system design
- It is a separate design step to then selectively derive from these the required strong assumptions

# A Systems Engineering Meta-Model



Perspectives

Operational

Functional

Logical

Technical

Geometrical

Abstraction Levels

1st level

2nd lev

4th level

5th level

…

…

Size: 20x5x50
Rel. Position: (1,1,2)

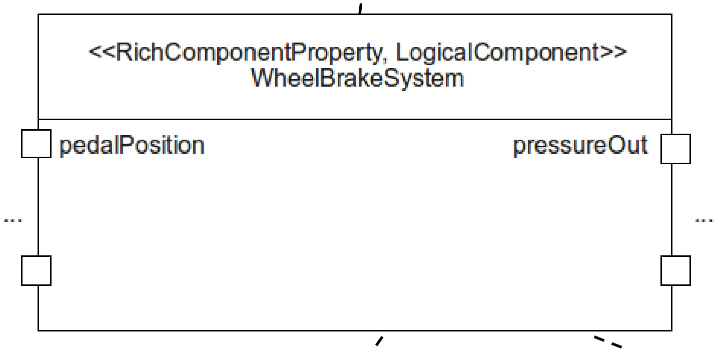
Perspectives represent design under different architectural viewpoints

Abstraction levels represent design at certain granularity

All „cells“ represent the same system

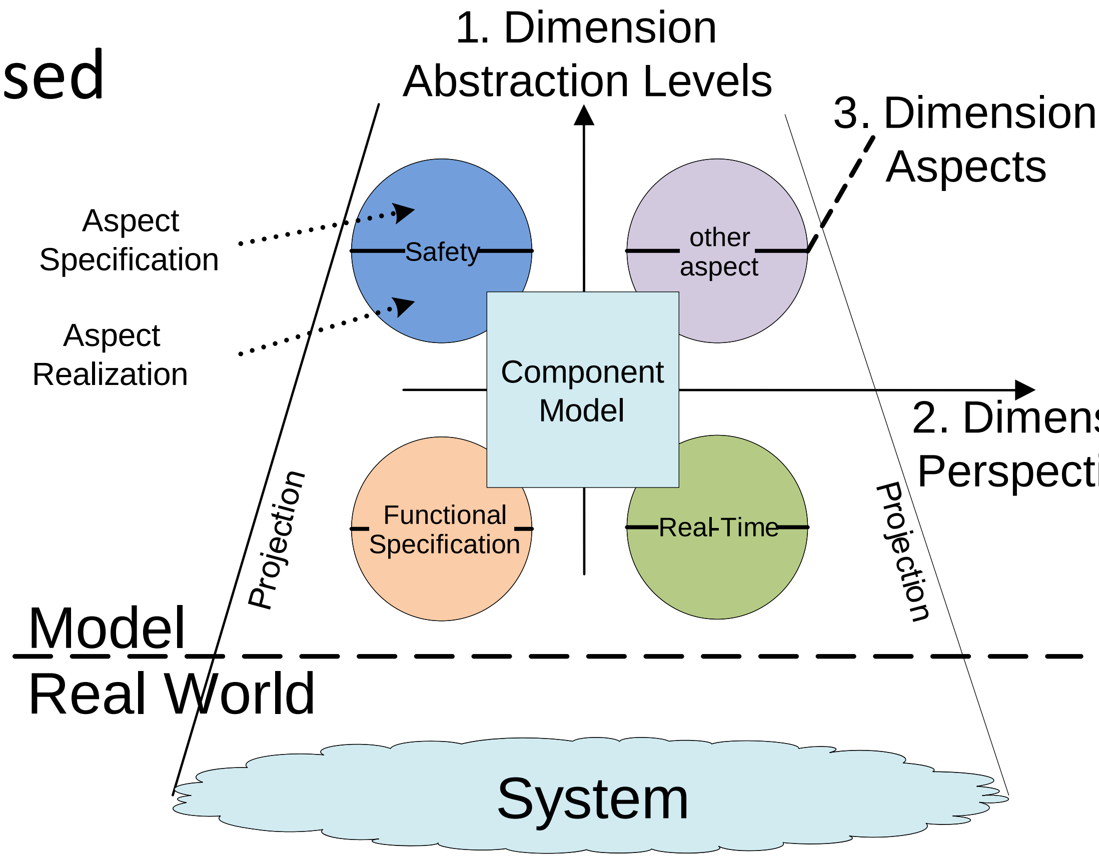
# Multi-aspect contract based specifications

Loss of all wheel braking during landing or Rejected Take Off shall be less than $5*10^{-7}$ per flight

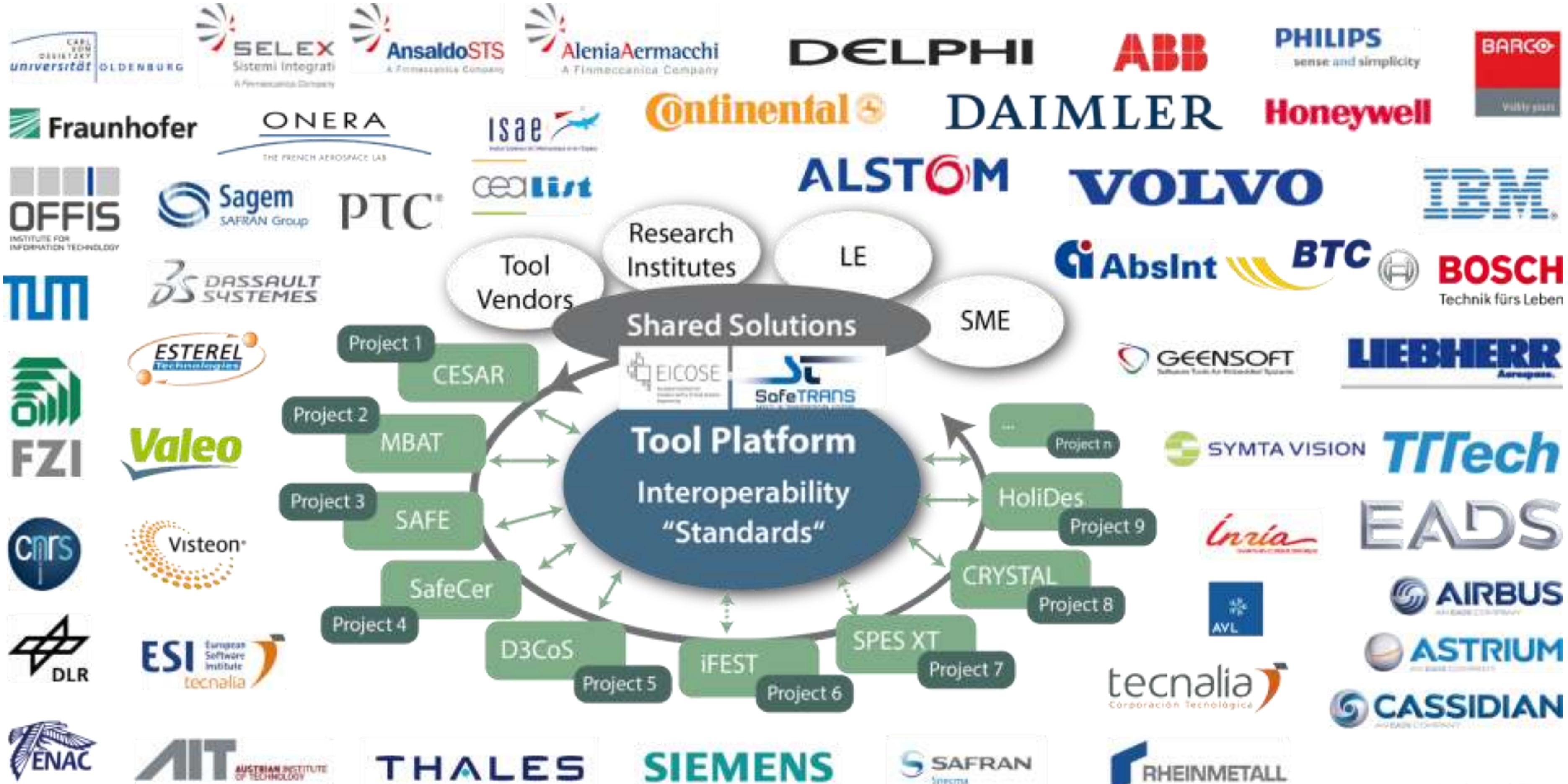


The pilot shall be allowed to override the autobrake function

When brake pedal is pressed, pressure to wheels should be supplied within 10ms



# An Innovation Eco-System for Critical Systems Engineering



Tool Vendors

Research Institutes

LE

SME

Shared Solutions

Tool Platform

Interoperability "Standards"

Project 1 CESAR

Project 2 MBAT

Project 3 SAFE

Project 4 SafeCer

Project 5 D3CoS

Project 6 iFEST

Project 7 SPES XT

Project 8 CRYSTAL

Project 9 HoliDes

Project n …

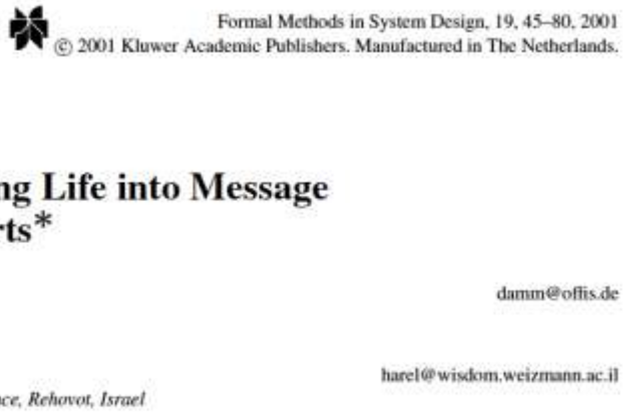
Graphic: SafeTRANS

# CONCLUSION

# Such modalities have already been introduced in live sequence charts

- strong assumptions correspond to hot conditions in live sequence charts: violation leads to abortion

- weak assumptions correspond to cold conditions in live sequence charts: they allow to consider different cases



Formal Methods in System Design, 19, 45–80, 2001
© 2001 Kluwer Academic Publishers. Manufactured in The Netherlands.

**LSCs: Breathing Life into Message Sequence Charts***

WERNER DAMM damm@offis.de
*OFFIS, Oldenburg, Germany*

DAVID HAREL harel@wisdom.weizmann.ac.il
*The Weizmann Institute of Science, Rehovot, Israel*

# Foundational Contributions

- the identification of a class of *admissible linear time temporal logic formula* for which the distributed controller synthesis problem is decidable (in double exponential time);
- the capability to effectively derive a weakest assumption on the environment of a system under which a global specification ϕ given as admissible LTL formula is realizable
- the capability to effectively synthesize an *optimal strategy* realizing ϕ, in the sense that if ϕ fails to realize the global specification, than also any other strategy would fail to realize the global specification

# Industrial Impact

- The contract based approach to systems engineering is increasingly seen as a key enabler to drastically reduce development time
- Product level tools supporting the methodology are now available on the market
- Key element in the current large scale European Initiative on building a reference platform for critical systems engineering

# Selected References

- Werner Damm, Eike Möhlmann, Astrid Rakow, *Component Based Design of Hybrid Systems: A Case Study on Concurrency and Coupling*, accepted for publication at 17th International Conference on Hybrid Systems: Computation and Control (HSCC 2014), Berlin, April 2014
- Werner Damm, Bernd Finkbeiner, *Automatic Compositional Synthesis of Distributed Systems*, accepted for publication at the 19th International Symposium on Formal Methods, Singapur, May 2014
- Alberto Sangiovanni-Vincentelli, Werner Damm, Roberto Passerone. *Taming Dr. Frankenstein: Contract-Based Design for Cyber-Physical Systems*. European Journal of Control, 18 (3):217-238, 2012
- Werner Damm and Bernd Finkbeiner. *Does it pay to extend the perimeter of a world model?* In Michael Butler and Wolfram Schulte, editors, Proceedings of the 17th International Symposium on Formal Methods, Lecture Notes in Computer Science, pages 12--26, June 2011.
- W. Damm, H. Hungar, B. Josko, T. Peikenkamp, I. Stierand: *Using Contract-based Component Specifications for Virtual Integration Testing and Architecture Design*. In Jim Kobylecky, editors, Proc. Design, Automation Test in Europe Conference Exhibition (DATE 2011: 1023-1028), pages 1--6, 2011
- Werner Damm, Henning Dierks, Jens Oehlerking, and Amir Pnueli. *Towards component based design of hybrid systems: Safety and stability.* In Zohar Manna and Doron Peled, editors, Time for Verification: Essays in Memory of Amir Pnueli, volume 6200 of Lecture Notes in Computer Science (LNCS), pages 96-143, 2010.
- W. Damm, B. Josko, T. Peikenkamp: *Contract based ISO CD 26262 safety analysis.* In: Proc.SAE World Congress and Exhibition, 2009.

# Relevant Projects

- Foundations
  - SFB TR AVACS “Automatic Verification and Analysis of Complex Systems”, www.avacs.org
- Industrial
  - Speeds http://www.speeds.eu.com/
  - Danse http://www.danse-ip.eu/home/
  - CESAR http://www.cesarproject.eu/
  - MBAT http://www.mbat-artemis.eu/home/
  - Crystal http://www.crystal-artemis.eu/
  - SPES XT http://spes2020.informatik.tu-muenchen.de/spes_xt-home.html