AVACS*
Automatic Verification and Analysis of Complex Systems
Lessons Learned

Werner Damm
AVACS coordinator

*www.avacs.org
Transregional Collaborative Research Center
funded by the German Science Foundation SFB-TR 14
1.1.2004 – 31.12.2015 total funding ≈30 Mill €

CARL VON OSSIETZKY universität OLDENBURG

UNIVERSITÄT DES SAARLANDES

ALBERT-LUDWIGS UNIVERSITÄT FREIBURG

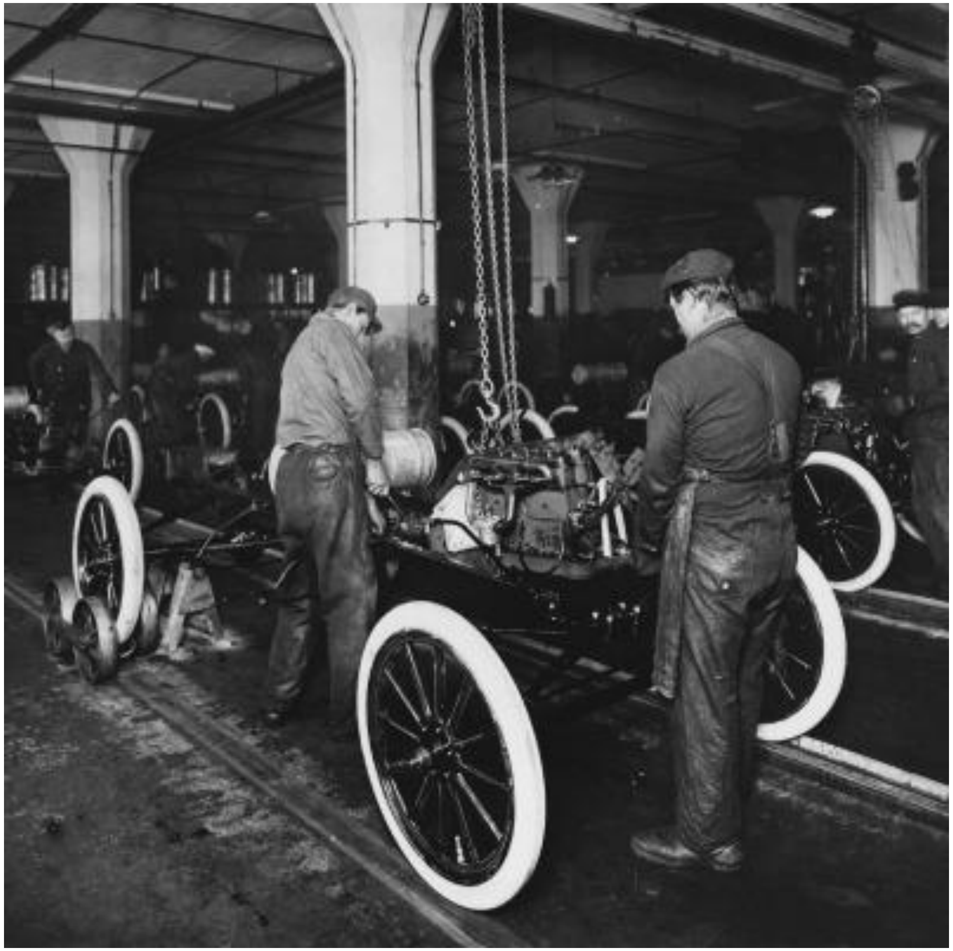
Structure of Presentation

- Complex Systems – and the AVACS vision
- Selected Highlights
- Lessons Learned
- Impact

Complex Systems

how the landscape changed

Those were the days, my friend, …



from http://mashable.com/2015/01/05/car-tech-ces

well, not quite

from http://mashable.com/2015/01/05/car-tech-ces

Connected and Smart Cars

In the coming decade,

your auto may well be just another component of a fully connected consumer experience.

Optimizing their own performance and maintenance

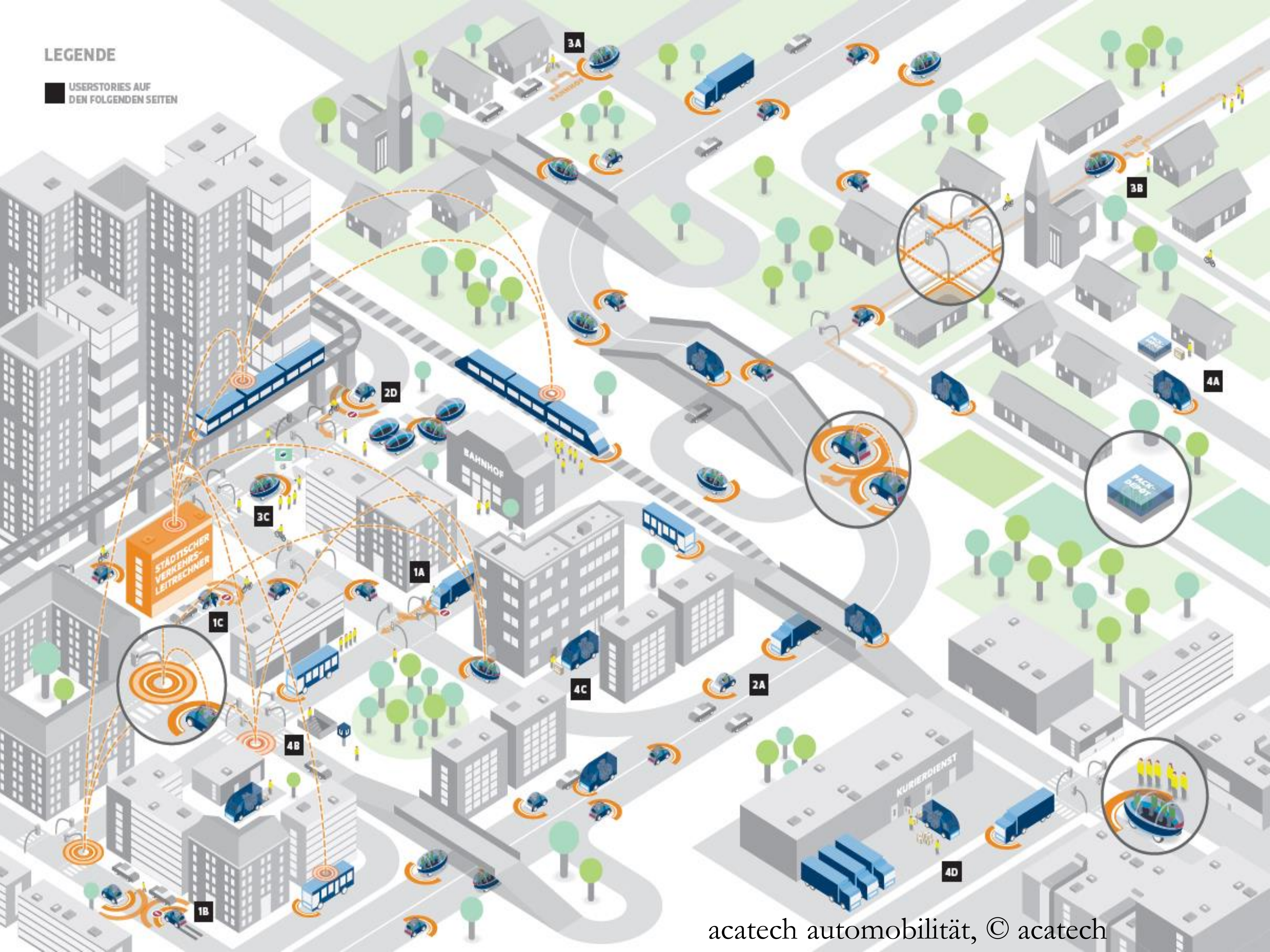
is one thing,

but the potential to move into a realm

where cars navigate, brake, avoid collisions and hazards on their own

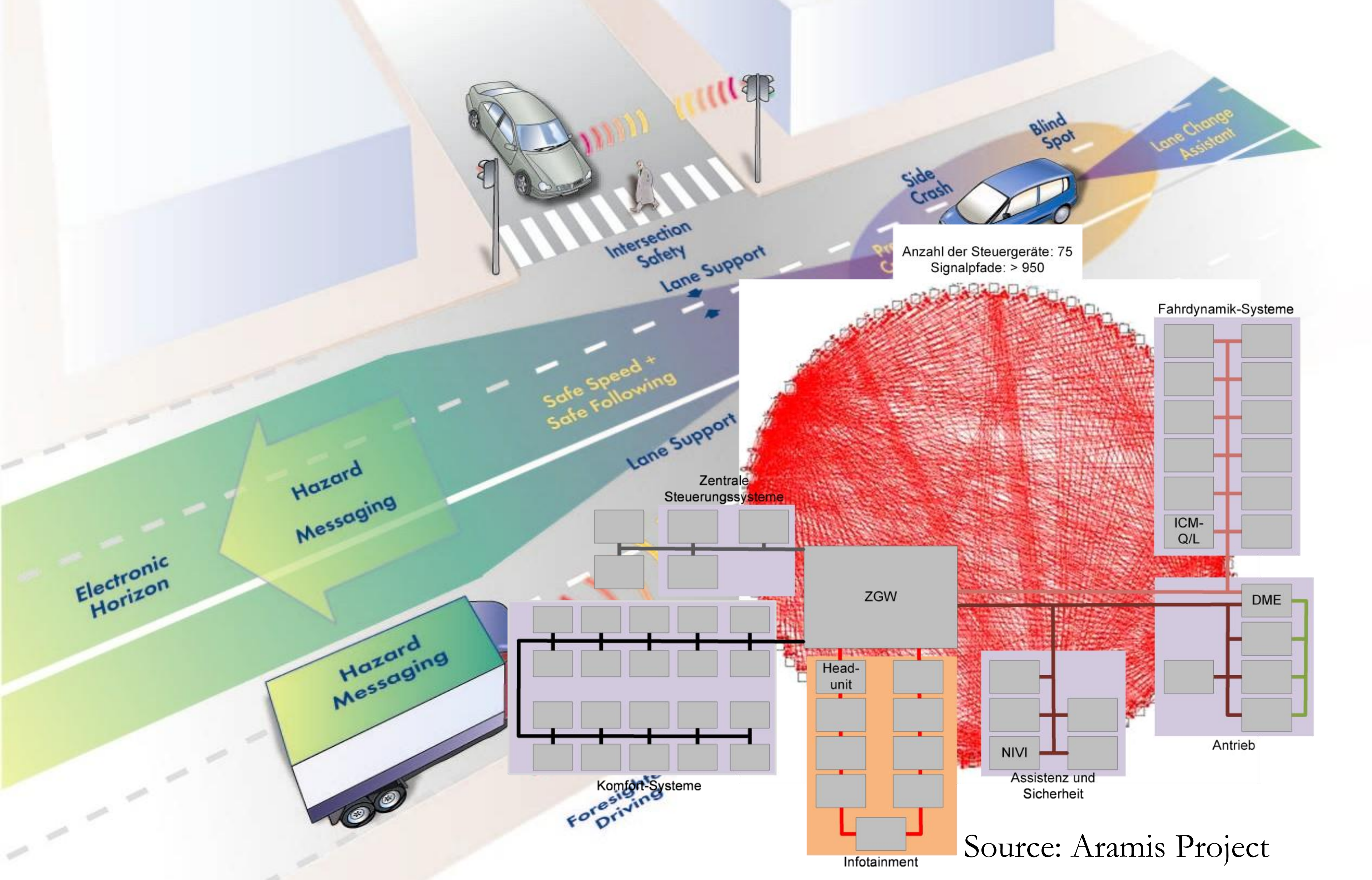
-- basically become autonomous on a number of levels -- is no longer a subject for science fiction alone.

quoted from http://mashable.com/2015/01/05/car-tech-ces



acatech automobilität, © acatech

Complex Systems



Source: Aramis Project

The Application Context

- Complex Embedded Systems are key enablers for safe flight and safe ground transportation
- Exponential growth in system complexity is a challenge for quality assurance
- AVACS contributes to meeting forthcoming requirements of pertinent safety standards on use of formal analysis methods
- Methods and tools cover large class of "cyber physical systems" seen to be highly relevant for addressing societal challenges (health, security, green mobility, …)

CARL VON OSSIETZKY universität OLDENBURG

UNIVERSITÄT DES SAARLANDES

ALBERT-LUDWIGS UNIVERSITÄT FREIBURG

The AVACS Vision

To Cover the Model- and Requirement Space of Complex Safety Critical Systems

with Automatic Verification Methods

Giving Mathematical Evidence
of Compliance of Models

To Dependability, Coordination, Control
and Real-Time Requirements

Verified wireless safety-critical hard real-time design

"The wireless bike brake demonstrator" [IEEE WoWMoM11]

- Hard real-time
- Wireless
- Safety-critical

- Verified with AVACS S2 technology.
- Built.
- Works.
- modestchecker.net

ALBERT-LUDWIGS
UNIVERSITÄT FREIBURG

UNIVERSITÄT DES SAARLANDES

Selected Highlights

Themes

1. Exploiting robustness
2. Causality based reasoning
3. Finding sufficiently precise abstractions
4. Finding Precise abstractions
6. Compositional Reasoning and Decomposition
7. Solver Technologies

Exploiting Robustness I: Drifting Clocks in TA

Can small drifts in clocks cause a safe TA to become unsafe? In general, yes

Can we efficiently analyse, whether TA can become unsafe when small drifts are allowed?

- Definition of robust reachability: a reachability property is considered to be "robustly (in-)valid" iff it does not change its validity for some small relative drift between clocks.
- Main result: under identified conditions (exact) reachability analysis as done by UPPAAL proves that system is even epsilon robustly valid, if clocks are re-synchronized regularly, thus bounding the maximal drift by epsilon

M. Swaminathan, M. Fränzle, and J.-P. Katoen,
The Surprising Robustness of (Closed) Timed Automata against Clock-Drift,
IFIP TCS, IFIP(273) (Springer, 2008) 537–55

Robust constraint solving for non-linear constraints

- Decision procedures for robust satisfaction for arithmetic SMT formulae involving large Boolean combinations of linear, polynomial, and transcendental constraints (HySAT II, iSAT 2, iSAT 3)
- first practical solver for SMT over such theories based on a tight integration of SAT solving techniques with interval-based arithmetic constraint solving

Martin Fränzle, Christian Herde, Stefan Ratschan, Tobias Schubert, and Tino Teige
Efficient solving of large non-linear arithmetic constraint systems with complex boolean structure.
Journal on Satisfiability, Boolean Modeling and Computation –
Special Issue on SAT/CP Integration, 1:209-236, 2007

- avoids non-termination by enforcing epsilon progress in interval splitting and resumption with smaller epsilon if results are inconclusive
- extended to untinterpreted First-order relational logic with non-linear constraints: SUP(NLA) is sound and complete for robust satisfaction

Andreas Eggers, Evgeny Kruglov, Stefan Kupferschmid, Karsten Scheibler,
Tino Teige and Christoph Weidenbach: Superposition Modulo Non-linear Arithmetic.
In Frontiers of Combining Systems, 8th International Symposium,
FroCoS 2011, LNCS 6989, 2011.

Exploiting Robustness II: Hybrid Automata

- Most verification problems for hybrid systems are undecidable
- We developed a theory that circumvents undecidability by providing verification algorithms that provably terminate for all robust problem instances, but need not necessarily terminate for non-robust problem instances.
- A problem instance x is robust iff the given property holds not only for x itself, but also when x is perturbed a little bit.

Exploiting Robustness II: Hybrid Automata

- Since, in practice, well-designed hybrid systems are usually robust, this implies that the algorithms terminate for the cases occurring in practice

Results

- Guaranteed Termination in the Verification of LTL Properties of Non-linear Robust Discrete Time Hybrid Systems
- Safety Verification of Non-linear Hybrid Systems is Quasi-decidable.

Werner Damm, Guilherme Pinto and Stefan Ratschan:
Guaranteed Termination in the Verification of LTL Properties of Non-linear Robust Discrete Time Hybrid Systems.
International Journal of Foundations of Computer Science (IJFCS) 18(1), 63--86, 2007.

Stefan Ratschan: Safety Verification of Non-linear Hybrid Systems is Quasi-decidable. Formal Methods in System Design 44(19, 71--90}, 2014.

Causality Based Analysis

Synthesis of Winning Strategies for Petri Games

- Games with causal memory modelled by Petri games with n system players, 1 environment player, local safety objective
- Intuitively, whenever players synchronise, they exchange all their past observations
- Winning strategy exists only if arena allows to synchronize sufficiently often
- solving takes only single-exponential time, compared with
  - general undecidabilty for Pnueli-Rosner game model,
  - nonelementary complexity for trees of Zielonka automata.
- Tool Adam automatically synthesizes distributed systems with > 30 processes.

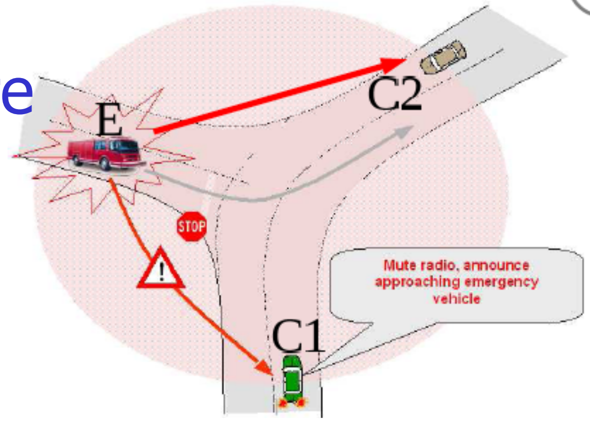
B. Finkbeiner and E. -R. Olderog. Petri Games: Synthesis of Distributed Systems with Causal Memory, GandALF 2014, EPTCS 161: 217-230, 2014

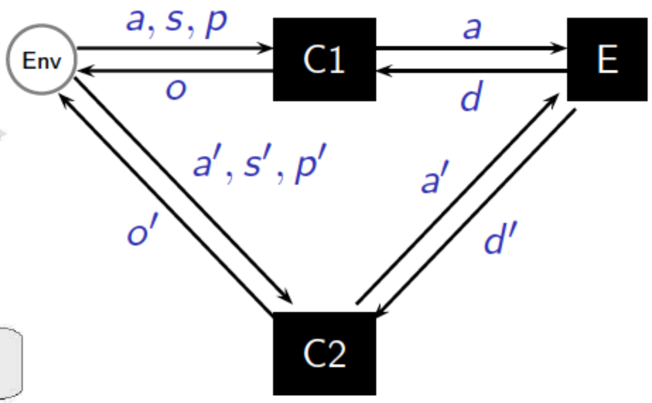
B. Finkbeiner, M. Gieseking, and E.-R. Olderog.Adam: Causality-Based Synthesis of Distributed Systems, CAV 2015, LNCS 9206, 433-439, Springer, 2015

Coordination Logic: who needs to know what

- Distributed synthesis is problem is undecidable for this architecture
- But for “Warn the driver of C1 iff he is on collision course” no need to know setting of switches in Car 2
- Coordination logic allows to say under what assumption on knowledge do I ask for realizability
- Decidable logic
- Synthesis procedure

a: User setting: active
s: User setting: speaker
p: User setting: display
o: output
d: data transmission



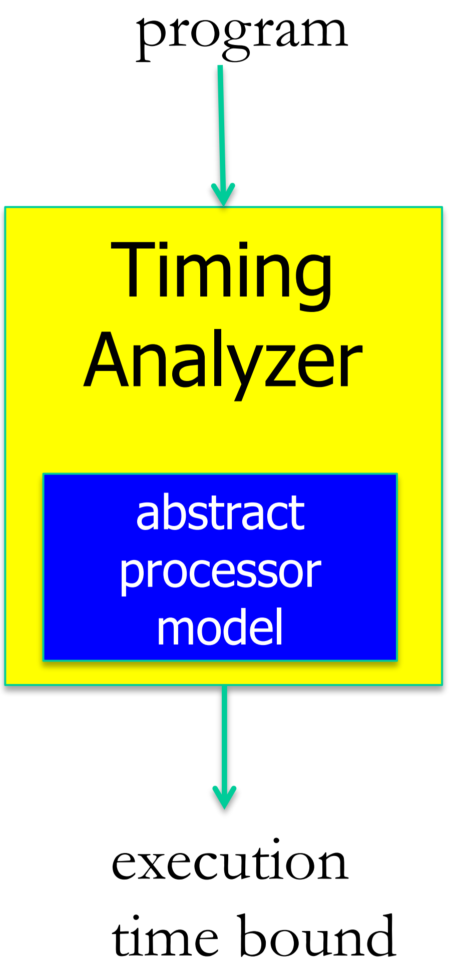


Does the Emergency Vehicle (E) have a strategy such that the Car (C) can warn the driver if and only if they are on a collision course?

$$⅃a\,\exists d.\,⅃s,p\,\exists o.\,\varphi(a,d,s,p,o)\wedge$$
$$⅃a'\,\exists d'.\,⅃s',p'\,\exists o'.\,\varphi(a',d',s',p',o')$$

Finding Sufficiently Precise Abstractions

For Worst Case Timing Analysis: Predictability



- first quantitative, analytical results for the predictability of replacement policies
- first compact abstract domain pipelines

efficiency

predictability

- caches – first clarified notion, R07, RGBW07
- pipelines – first compact abstract domain, HRW15

precision

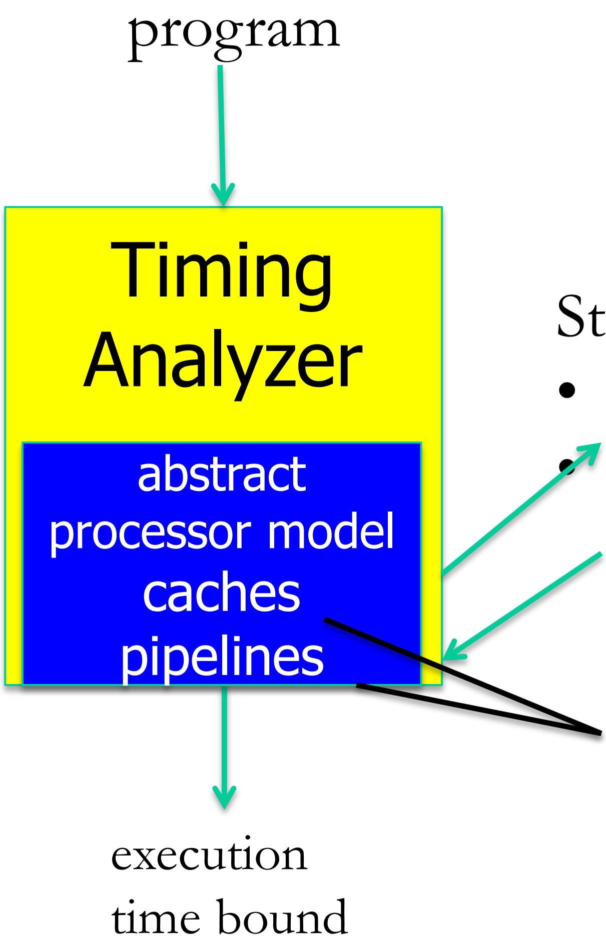
heavily influenced the design of the Kalray MMP 256

CARL VON OSSIETZKY universität OLDENBURG

ALBERT-LUDWIGS UNIVERSITÄT FREIBURG

UNIVERSITÄT DES SAARLANDES

For Worst Case Timing Analysis


program

Timing Analyzer

abstract processor model caches pipelines

execution time bound

Strengthening cache analysis:

- relational cache analysis, HG11
- cache analysis for FIFO, PLRU, GR09, GR10

learning cache architectures, AR13

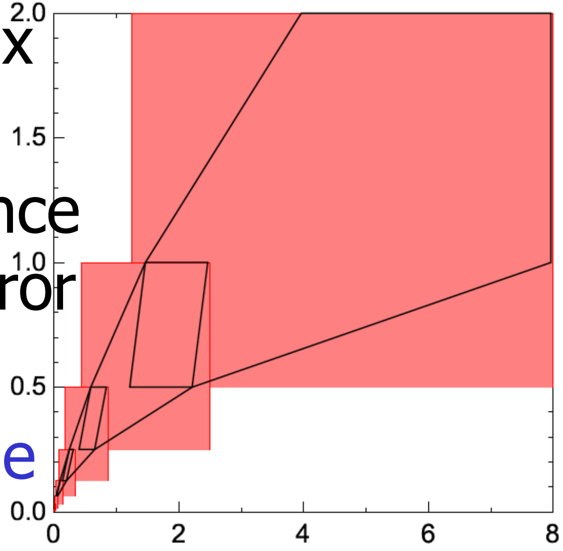
extension to multi-core architectures, JHH15

Compositional analysis

Bogomolov, Donze, Frehse, Grosu, Johnson, Ladan, Podelski & Wehrle. CAV 2012, SPIN 2013.

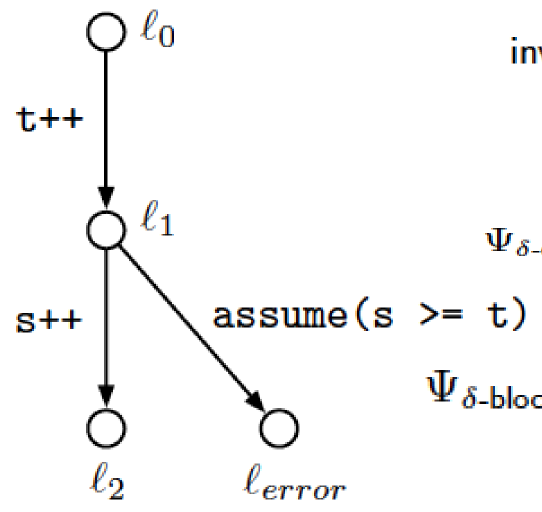
Abstraction Based Guided Search for Hybrid Systems

- The support function of a closed and bounded continuous set $\mathcal{S} \subseteq \mathbb{R}^n$ with respect to a direction vector $\ell \in \mathbb{R}^n$ is $\rho(\ell, \mathcal{S}) = \max_{x \in \mathcal{S}} \ell \cdot x$. The number of direction vectors („a template") determines the precision in approximating $\mathcal{S} = \bigcap_{\ell \in \mathbb{R}^n} \{x \mid \ell \cdot x \leq \rho(\ell, \mathcal{S})\}$
- For a given safety property and hybrid system with linear dynamics in each location, we compute an abstraction by coarsening the over-approximation SpaceEx computes in its reachability analysis.
- The abstraction is used to derive the distance in number of transitions to the symbolic error state.
- This distance is then guiding SpaceEx in the concrete search.



Through Synthesizing Counters: Proofs that Count

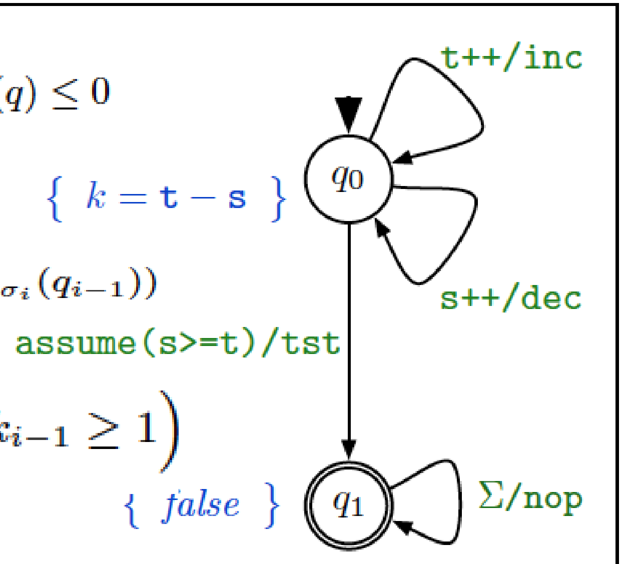
- Synthesis of Annotated Counter Automata employing UF(NLA) constraint solving yields a relatively complete proof method for pre/post specifications of multi-threaded programs with linear arithmetic



$$\mathsf{inv}(q) \triangleq \left(\sum_{i=1}^{|X|} C_{x_i}(q)\cdot x_i\right) + C_{\mathtt{k}}(q)\cdot \mathtt{k} + C_1(q) \le 0$$

$$\Psi_{\delta\text{-counter}} \triangleq k_0 \ge 0 \wedge \bigwedge_{i=1}^{|\tau|} k_i = k_{i-1} + \mathsf{incr}(\alpha_{\sigma_i}(q_{i-1}))$$

$$\Psi_{\delta\text{-block}} \triangleq \bigwedge_{i=1}^{|\tau|} \left(\alpha_{\sigma_i}(q_{i-1}) \in \{\mathsf{dec},\mathsf{tst}\} \Rightarrow k_{i-1} \ge 1\right)$$



$$\Psi_{\mathsf{final}} \triangleq (\forall \mathtt{k}, X)(\mathsf{inv}(q_{|\tau|}) \wedge \mathtt{k} \ge k_{\mathit{final}} \Rightarrow \psi_{\mathsf{post}})$$

$$\Psi_{\mathsf{init}} \triangleq (\forall \mathtt{k}, X)(\psi_{\mathsf{pre}} \Rightarrow \mathsf{inv}(q_0))$$

unbounded number of threads

safety property: never in error state

Azadeh Farzan, Zachary Kincaid, Andreas Podelski:
Proofs that count. POPL 2014

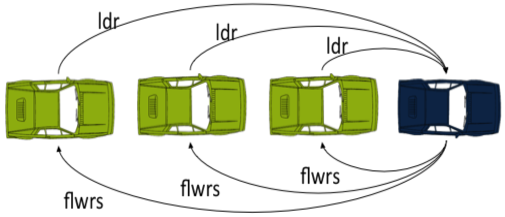
Azadeh Farzan, Zachary Kincaid, Andreas Podelski:
Proof Spaces for Unbounded Parallelism.
(POPL 2015)

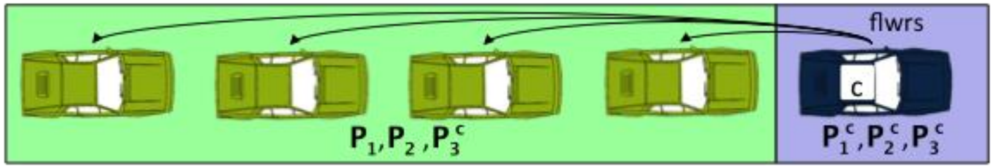
Through Synthesizing Predicate Automata

- A finitely generated proof space for a concurrent program P is generated from a finite set of basic Hoare triples by closing this under sequencing, symmetry and conjunction
- Thm: for each P there is a finitely generated proof space s.t. for any trace τ violating its pre/post spec {true} τ {false} is an element of the proof space
- A predicate automata generalizes Alternating automata to first order logic with uninterpreted relational symbols
- The paper constructs for each proof space H for P a predicate automata A(H) s.t. A(H) accepts exactly the traces tau s.t. {true} τ {false} εH
- This yields a semi-decision procedure, which terminates for the special case of modular programs

Through Symbolic Shape Analysis

- First approach that integrates shape analysis into a CEGAR loop
- First verification method based on shape analysis
- Uses symbolic reasoning to compute abstraction
- Abstraction is adapted to the verification problem by automatically introducing new node predicates

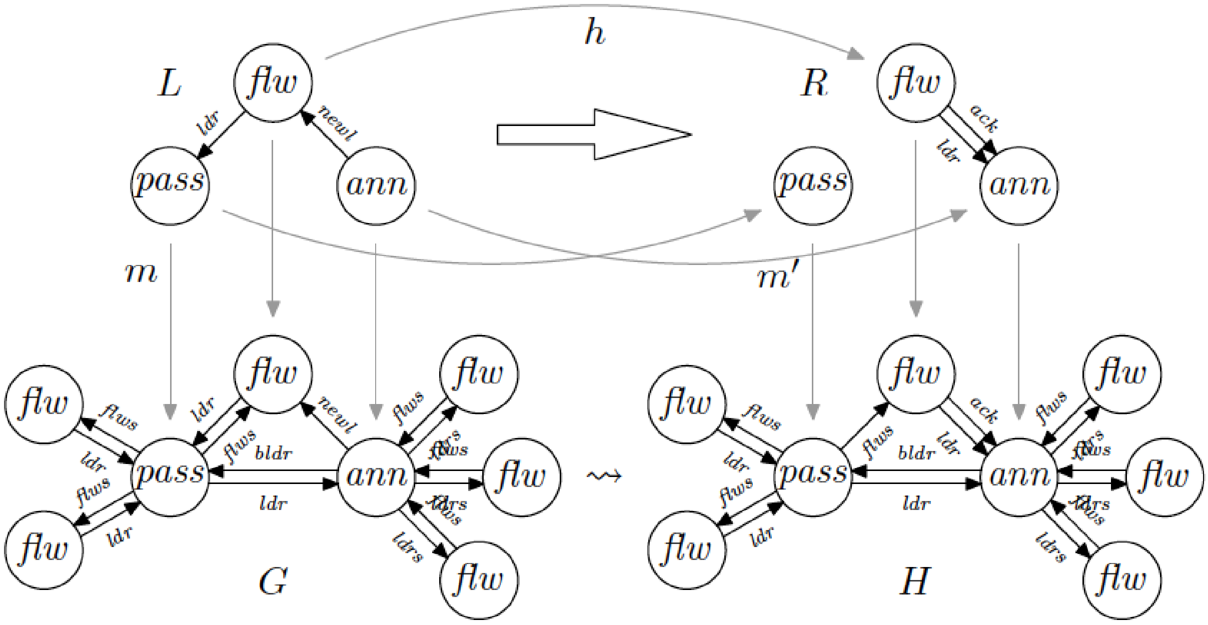




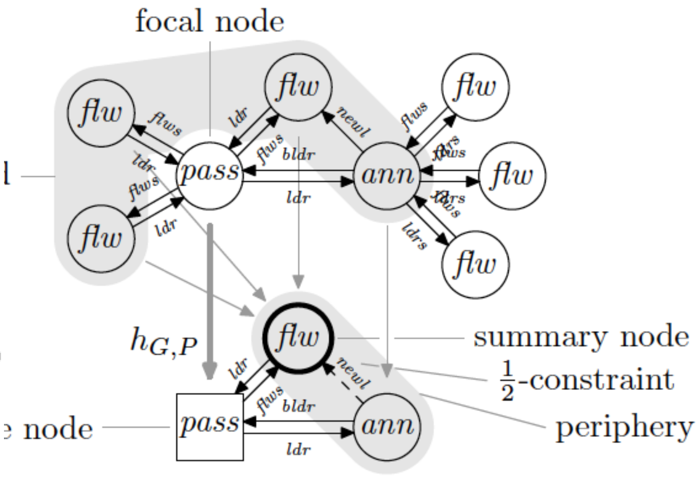
Andreas Podelski and Thomas Wies. Counterexample-guided focus. POPL 2010
Andreas Podelski and Thomas Wies. Boolean heaps. SAS 2005

universität OLDENBURG
UNIVERSITÄT DES SAARLANDES
ALBERT-LUDWIGS
UNIVERSITÄT FREIBURG

Through Abstract Interpretation of Graph Grammars



[Backes and Reineke, 2015] Peter Backes, Jan Reineke: Analysis of Infinite-State Graph Transformation Systems by Cluster Abstraction. VMCAI 2015



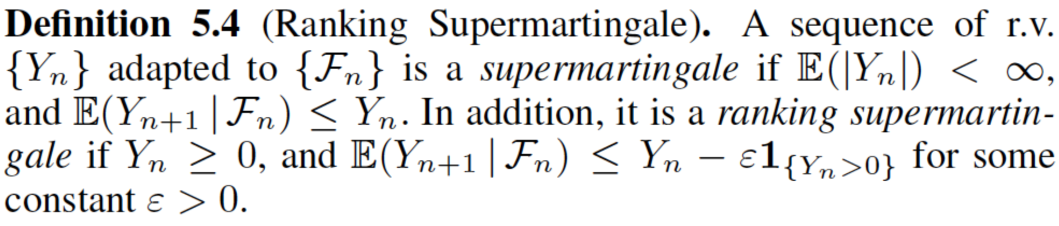
- Models distributed systems with message passing and dynamic process creation through graph grammars
- Uses abstract interpretation to compute a finite overapproximation of the set of reachable graphs

Abstractions for Time-Bounded Rewards

- Markov Automata combine nondeterminism with probabilistic behaviour and continuous stochastic timing
- Markov Reward Automata allow to analyse time-bounded accumulated rewards *e.g.* „What is the maximal expected cost the system causes within 10 hours of operation?"
- abstracted into a two-player stochastic reward game, which keeps the nondeterminism present in the concrete system separate from the nondeterminism introduced by abstraction
- This allows to compute safe upper and lower bounds on the minimal and maximal reward value of the original system. If too poor, then refine.

Bettina Braitling, Luis María Ferrer Fioriti, Hassan Hatefi, Ralf Wimmer, Holger Hermanns, and Bernd Becker. Abstraction-based computation of reward measures for Markov automata. VMCAI 2015, LNCS 8931, 172-189

Through Automatic Synthesis of Ranking Functions



Definition 5.4 (Ranking Supermartingale)**.** A sequence of r.v. $\{Y_n\}$ adapted to $\{\mathcal{F}_n\}$ is a *supermartingale* if $\mathbb{E}(|Y_n|) < \infty$, and $\mathbb{E}(Y_{n+1} \mid \mathcal{F}_n) \leq Y_n$. In addition, it is a *ranking supermartingale* if $Y_n \geq 0$, and $\mathbb{E}(Y_{n+1} \mid \mathcal{F}_n) \leq Y_n - \varepsilon \mathbf{1}_{\{Y_n > 0\}}$ for some constant $\varepsilon > 0$.

- *A compositional rule for proving probabilistic termination:*

- Find ranking function for inner loop.

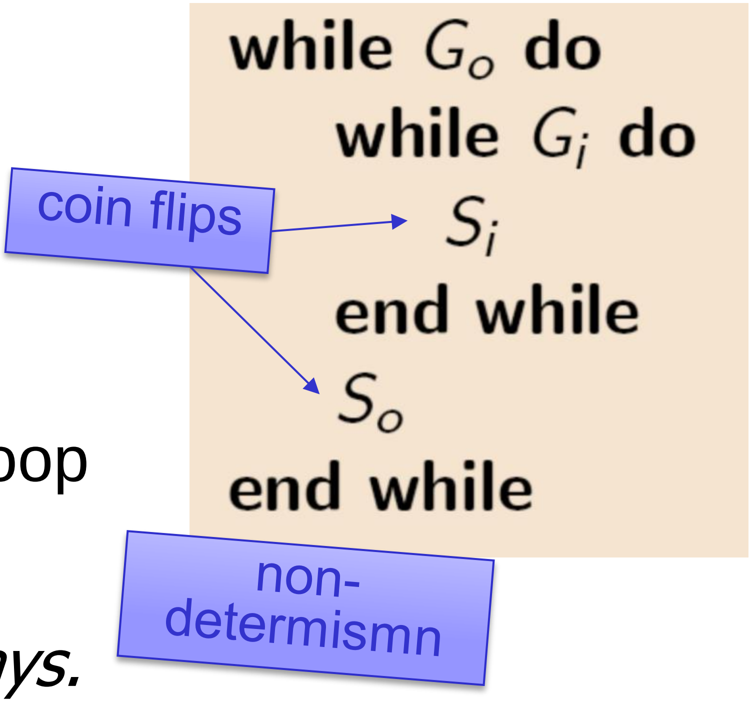
  ↑ Lyapunov

- Find ranking function for outer loop.

  ↑ Lyapunov

- Show that ranking function for outer loop does not increase in inner loop.

  ↑ in expectation



```
while $G_o$ do
    while $G_i$ do
        $S_i$
    end while
    $S_o$
end while
```

coin flips

non-determismn

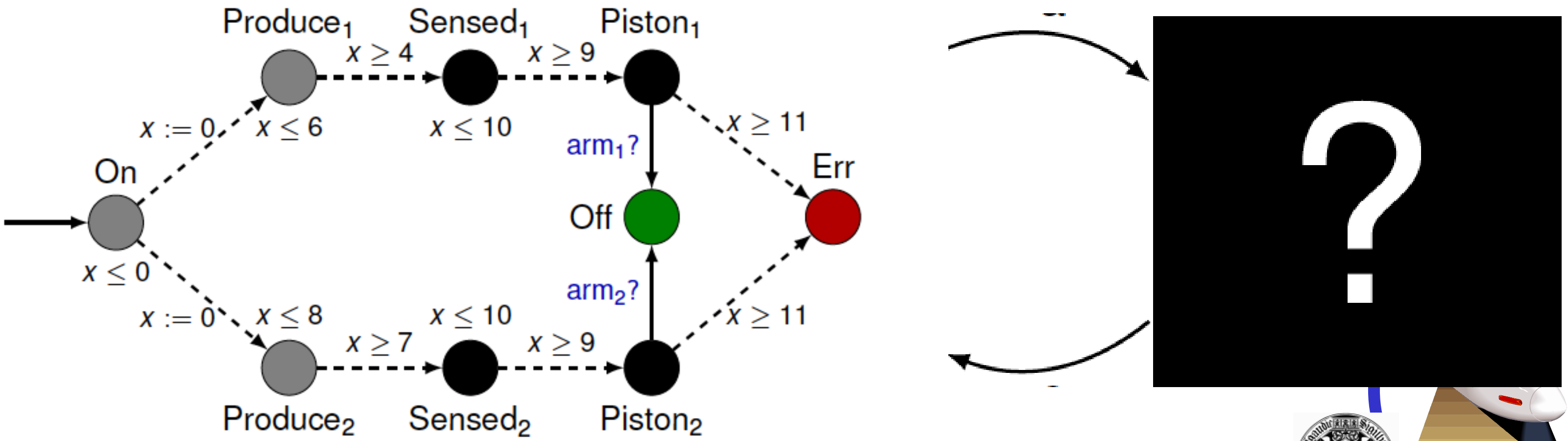
- *Looks good. But unsound in many ways.*
- *We made it sound and complete for non-deterministic probabalistic programs using martingale theory solving a long-standing open problem*

Probabilistic Termination:
Soundness, Completeness, and Compositionality
Luis Maria Ferrer Fioriti, Holger Hermanns
POPL 2015

Finding Precise abstractions

Through synthesizing observation predicates

- Want to synthesize TA controller avoiding bad states of plants in spite of partial observability of plant
- Learn relevant observations (what type of box, when and how to remove box) by finding winning strategies in abstract game based on current set of observations
- use CEGAR to generate new observations eliminating spurious non-winning strategies, yielding precise abstraction

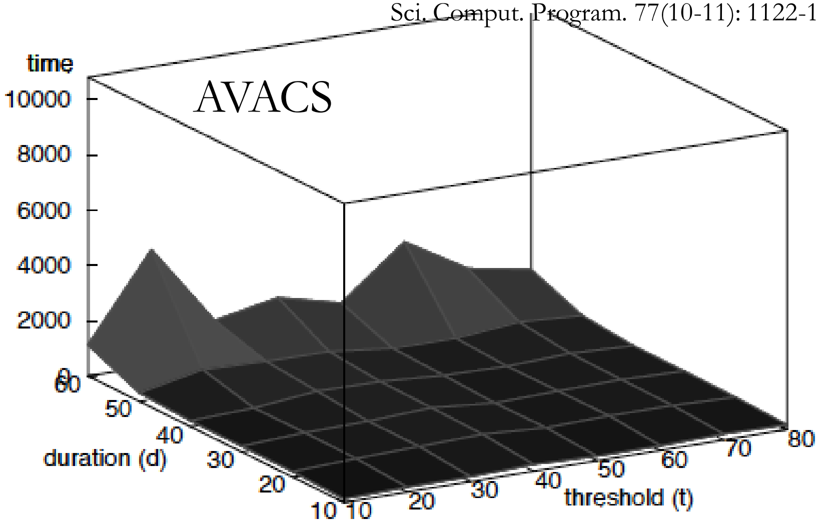


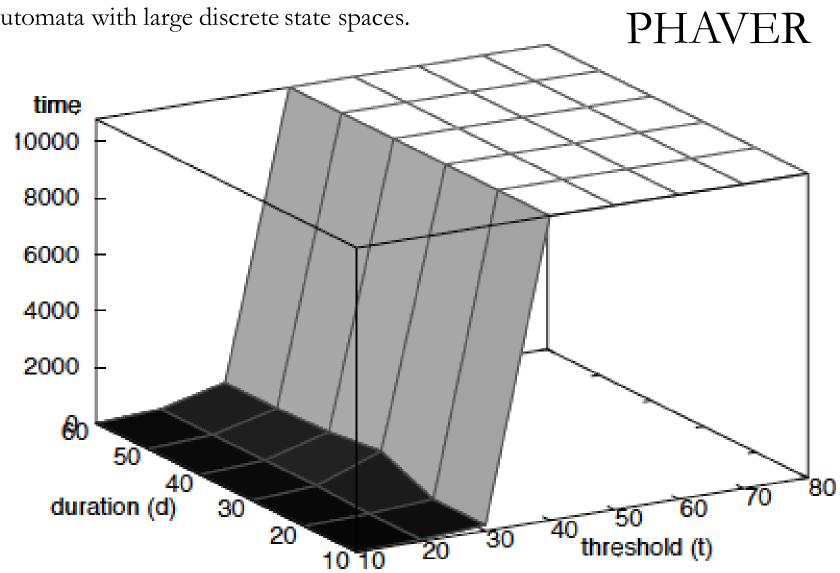
Rayna Dimitrova and Bernd Finkbeiner. **Counterexample-guided synthesis of observation predicates.** *, FORMATS 2012, London, UK, September 18-20, 2012. LNCS* 7595 107-122. Springer, 2012.

Through on-the-fly generation of precise predicate abstraction

- We have developed fully symbolic verification methods for hybrid systems providing precise abstractions for the verification of safety properties of Linear Hybrid Automata, allowing for the first time to deal at the same time with large discrete state spaces and continuous evolutions
- relevant predicates to achieve preciseness are computed on the fly

Werner Damm, Henning Dierks, Stefan Disch, Willem Hagemann,
Florian Pigorsch, Christoph Scholl, Uwe Waldmann, Boris Wirtz:
Exact and fully symbolic verification of linear hybrid automata with large discrete state spaces.
Sci. Comput. Program. 77(10-11): 1122-1150 (2012)





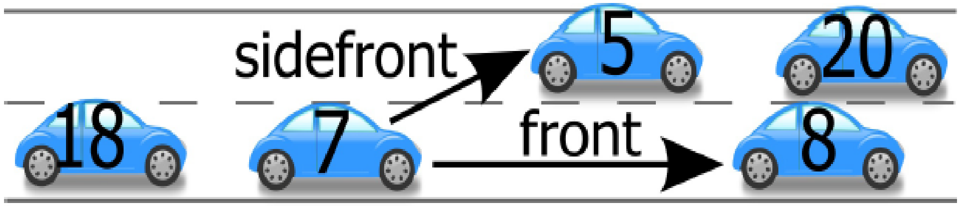
Through Locality Based Reasoning

V. Sofronie-Stokkermans. Hierarchical Reasoning and Model Generation
for the Verification of Parametric Hybrid Systems.
CADE-24, LNCS 7898: 360-376, Springer, 2013

- We have developed a completely new line of reasoning about safety properties of hybrid systems based on reduction to showing satisfiability of formula in so-called local theory extensions of decidable fragments of first order logic

Werner Damm, Carsten Ihlemann, and Viorica Sofronie-Stokkermans.
PTIME parametric verification of safety properties for reasonable linear hybrid automata.
Mathematics in Computer Science 5(4), 469-479, 2011

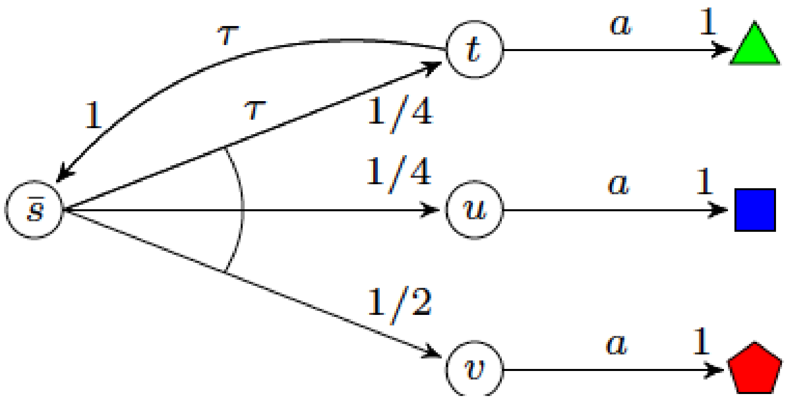
- Applied to parametric verification of safety properties of LHA: identified conditions under which this is in NP
- Applied to model of cooperating vehicles, where decisions are taking only on sensing location of vehicles in the neighborhood: gives precise reduction of collision freedom to analyzing only scenarios with finitely many cars in the neighborhood of the ego car

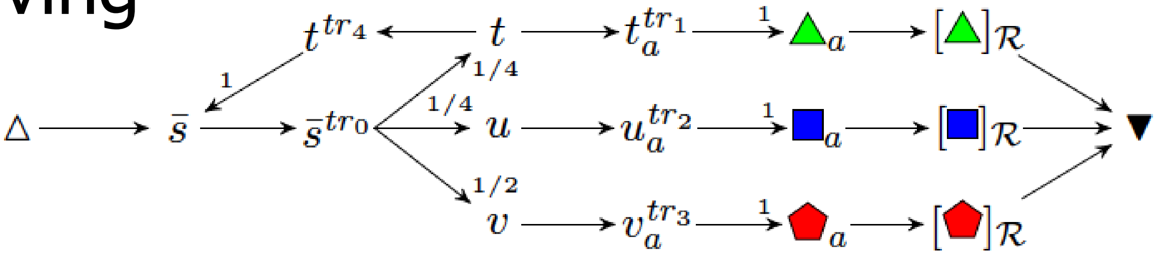


Werner Damm, Matthias Horbach and Viorica Sofronie-Stokkermans
“Decidability of Verification of Safety Properties of
Spatial Families of Linear Hybrid Automata”, FroCoS, LNAI 9322 2015

Through precise reduction to LP problem: Deciding Probabilistic Automata Weak Bisimulation in Polynomial Time

- Transforms PA into flowgraph – not semantic preserving, but mismatch can be recovered in LP solving maxflow by adding constraints
- solves 10 yr old open problem





$$f_{\triangle,\bar{s}} = 1 \qquad f_{[\blacktriangle]_{\mathcal{R}},\blacktriangledown} = 1/16 \qquad f_{[\blacksquare]_{\mathcal{R}},\blacktriangledown} = 5/16$$

$$f_{[\text{⬟}]_{\mathcal{R}},\blacktriangledown} = 10/16 \qquad f_{\bar{s},\bar{s}^{tr_0}} - f_{\bar{s}^{tr_0},t} - f_{\bar{s}^{tr_0},u} - f_{\bar{s}^{tr_0},v} = 0 \qquad f_{\triangle,\bar{s}} + f_{t^{tr_4},\bar{s}} - f_{\bar{s},\bar{s}^{tr_0}} = 0$$

$$f_{\bar{s}^{tr_0},t} - f_{t,t_a^{tr_1}} - f_{t,t^{tr_4}} = 0 \qquad f_{\bar{s}^{tr_0},u} - f_{u,u_a^{tr_2}} = 0 \qquad f_{\bar{s}^{tr_0},v} - f_{v,v_a^{tr_3}} = 0$$

$$f_{t,t_a^{tr_1}} - f_{t_a^{tr_1},\blacktriangle_a} = 0 \qquad f_{u,u_a^{tr_2}} - f_{u_a^{tr_2},\blacksquare_a} = 0 \qquad f_{v,v_a^{tr_3}} - f_{v_a^{tr_3},\text{⬟}_a} = 0$$

$$f_{t,t^{tr_4}} - f_{t^{tr_4},\bar{s}} = 0 \qquad f_{t_a^{tr_1},\blacktriangle_a} - f_{\blacktriangle_a,[\blacktriangle]_{\mathcal{R}}} = 0 \qquad f_{u_a^{tr_2},\blacksquare_a} - f_{\blacksquare_a,[\blacksquare]_{\mathcal{R}}} = 0$$

$$f_{v_a^{tr_3},\text{⬟}_a} - f_{\text{⬟}_a,[\text{⬟}]_{\mathcal{R}}} = 0 \qquad f_{\blacktriangle_a,[\blacktriangle]_{\mathcal{R}}} - f_{[\blacktriangle]_{\mathcal{R}},\blacktriangledown} = 0 \qquad f_{\blacksquare_a,[\blacksquare]_{\mathcal{R}}} - f_{[\blacksquare]_{\mathcal{R}},\blacktriangledown} = 0$$

$$f_{\text{⬟}_a,[\text{⬟}]_{\mathcal{R}}} - f_{[\text{⬟}]_{\mathcal{R}},\blacktriangledown} = 0 \qquad f_{\bar{s}^{tr_0},t} - 1/4 f_{\bar{s},\bar{s}^{tr_0}} = 0 \qquad f_{\bar{s}^{tr_0},u} - 1/4 f_{\bar{s},\bar{s}^{tr_0}} = 0$$

$$f_{\bar{s}^{tr_0},v} - 1/2 f_{\bar{s},\bar{s}^{tr_0}} = 0 \qquad f_{t_a^{tr_1},\blacktriangle_a} - 1 f_{t,t_a^{tr_1}} = 0 \qquad f_{u_a^{tr_2},\blacksquare_a} - 1 f_{u,u_a^{tr_2}} = 0$$

$$f_{v_a^{tr_3},\text{⬟}_a} - 1 f_{v,v_a^{tr_3}} = 0 \qquad f_{t^{tr_4},\bar{s}} - 1 f_{t,t^{tr_4}} = 0$$

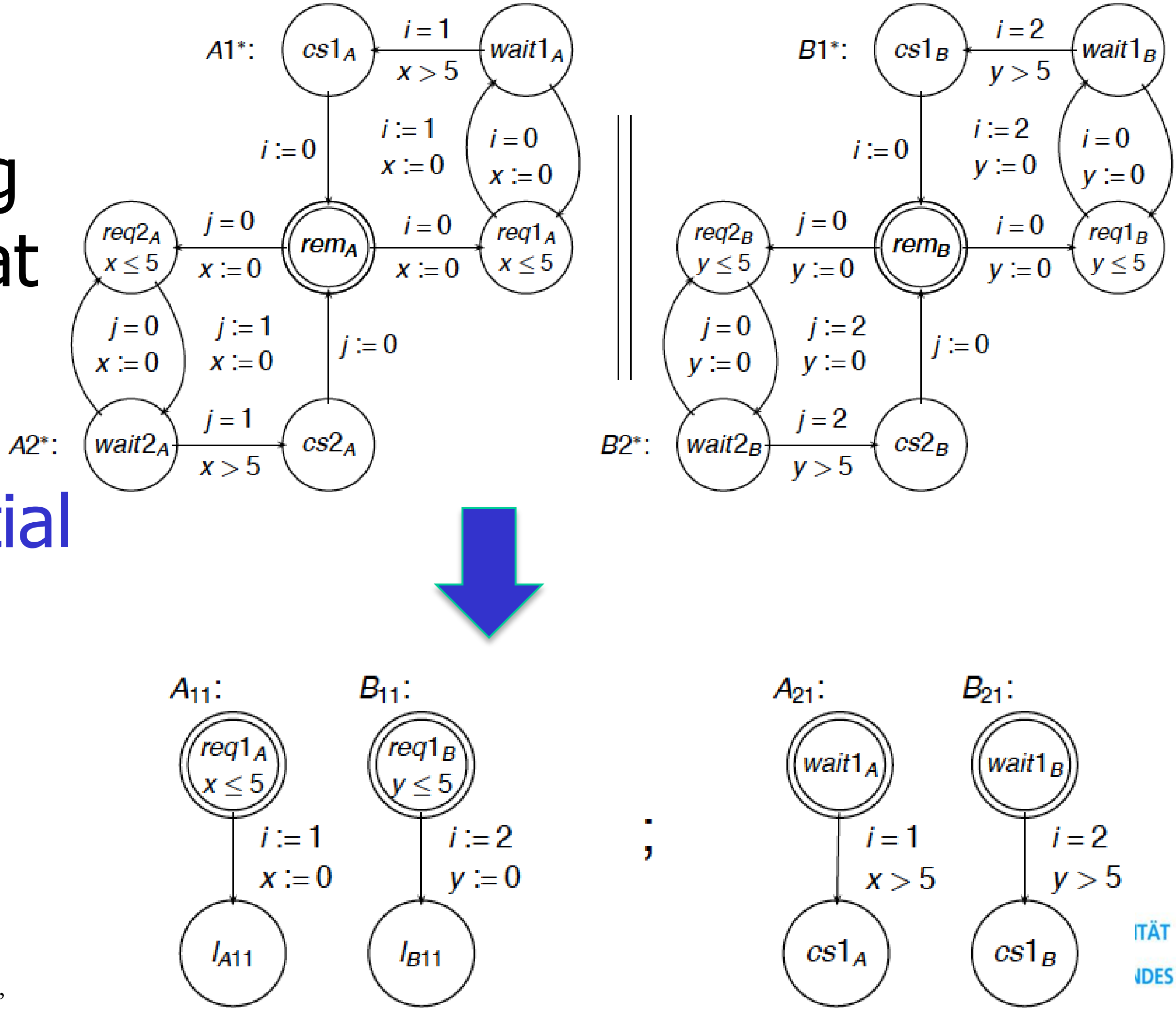
Holger Hermanns, Andrea Turrini:
Deciding Probabilistic Automata Weak Bisimulation
in Polynomial Time. FSTTCS 2012: 435-447

Compositional Reasoning and Decomposition

Through Transformations for extended TA

Never together in $cs1_A$ and $cs1_B$ or in $cs2_A$ and $cs2_B$

- isolate conditions which enable property-preserving transformations that replace parallel composition by variants of sequential composition and eliminate loops.
- eases automatic analysis



E.-R. Olderog, M. Swaminathan,
Structural Transformations for Data-Enriched Real-Time-Systems,
Formal Aspects of Computing 27 (2015) 727-750

Werner Damm and Bernd Finkbeiner.
Automatic compositional synthesis of distributed systems.
FM 2014, LNCS 8442, p. 179-193., 2014.

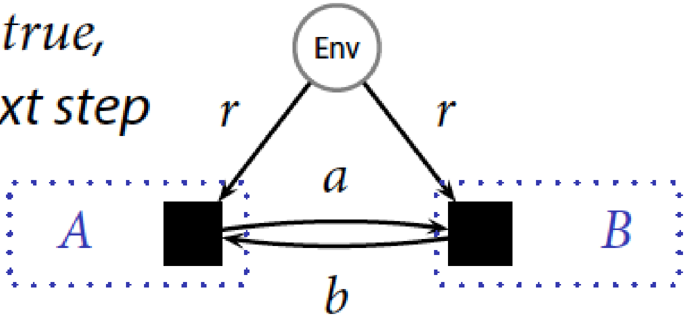
Compositional Controller Synthesis

- A strategy is remorse-free dominant for LTL formula Φ iff it fails to achieve Φ only in situations where any other strategy would fail to achieve Φ. We call Φ admissable if there is a remorse-free dominant strategy for Φ
- The distributed synthesis problem for admissable Φ is decidable in double exponential time. The composition of remorse-free dominant strategies for A and B yields a remorse-free strategy for A||B.
- We can compute the weakest environment assumption of a remorse-free dominant strategy under which the strategy is winning.

whenever r is true, set a in the next step

$\varphi = \mathsf{G}(r \rightarrow \mathsf{X}(a \wedge b))$ is admissible in A

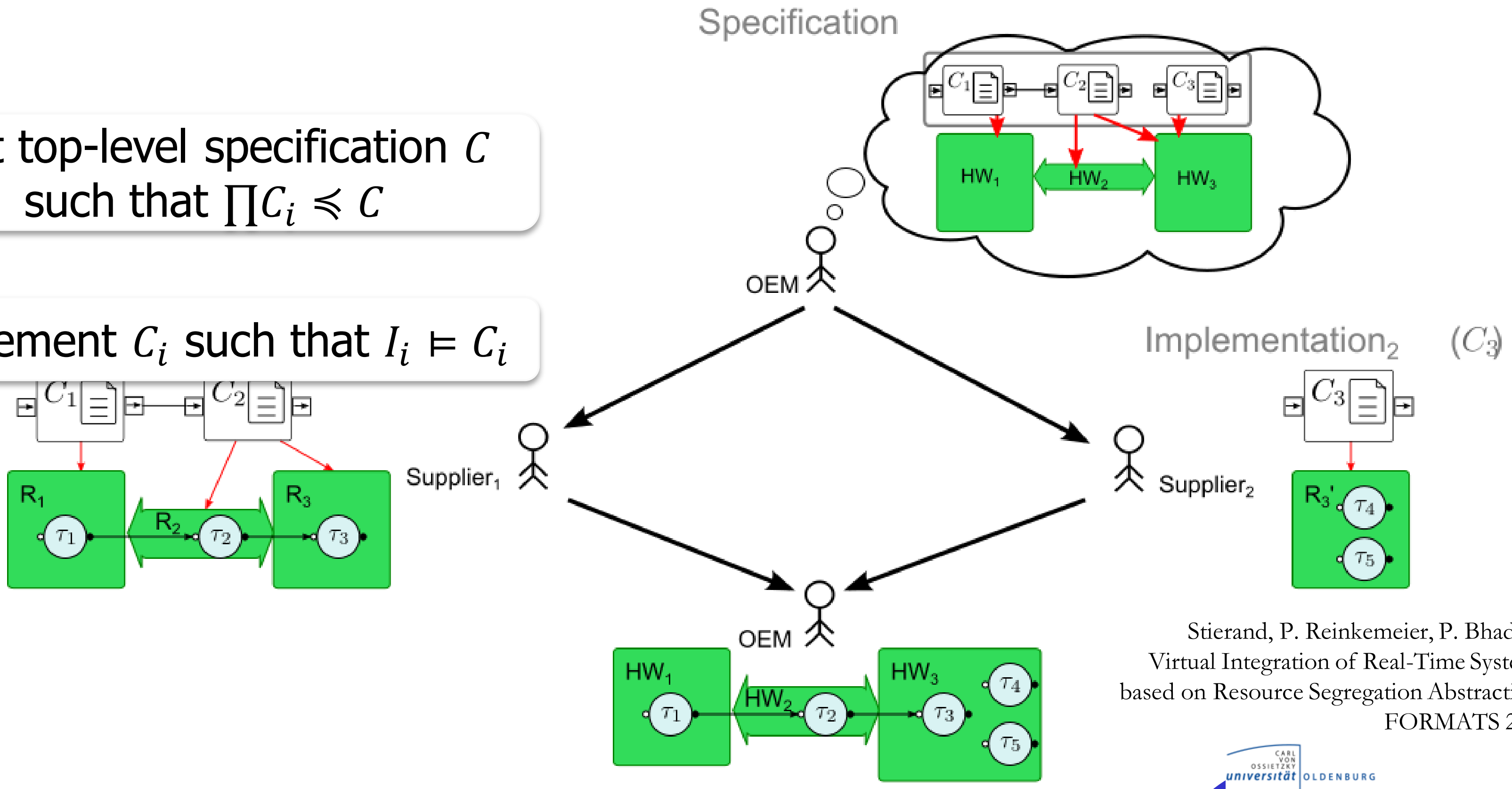
$w(A, \varphi) = \mathsf{G}(r \rightarrow \mathsf{X}b)$



Compositional Reasoning on Resource Usage

Split top-level specification C such that $\prod C_i \preccurlyeq C$

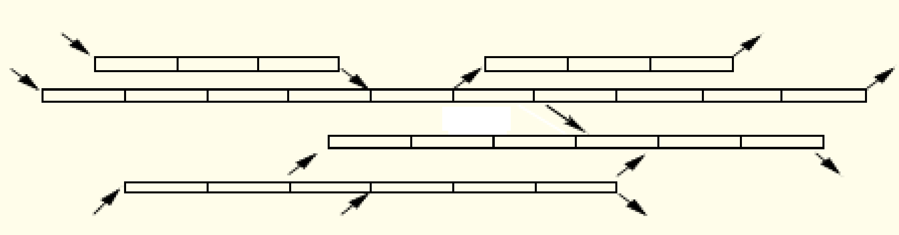
Implement C_i such that $I_i \vDash C_i$



Stierand, P. Reinkemeier, P. Bhaduri:
Virtual Integration of Real-Time Systems
based on Resource Segregation Abstraction.
FORMATS 2014

Define/derive "segregation properties" B_i characterizing usage of (virtual) architecture resources. It holds: $\prod B_i \vDash \neg\emptyset \Rightarrow \prod I_i \vDash \prod C_i$

Parametric verification of networks of TA with complex types



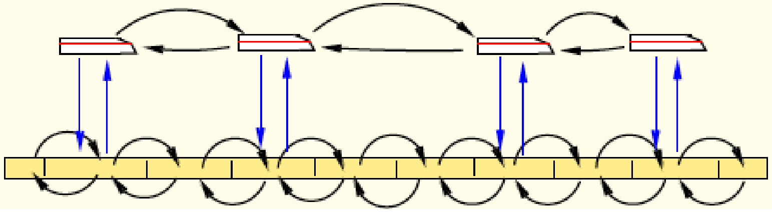
- Decompose the system in trajectories (linear rail tracks; may overlap)
- Prove safety for trajectories with incoming/outgoing trains
- Conclude that for control rules in which trains have sufficient freedom (and if trains are assigned unique priorities) safety of all trajectories implies safety of the whole system

Data structures:

- 2-sorted pointers

p_1: trains

p_2: segments

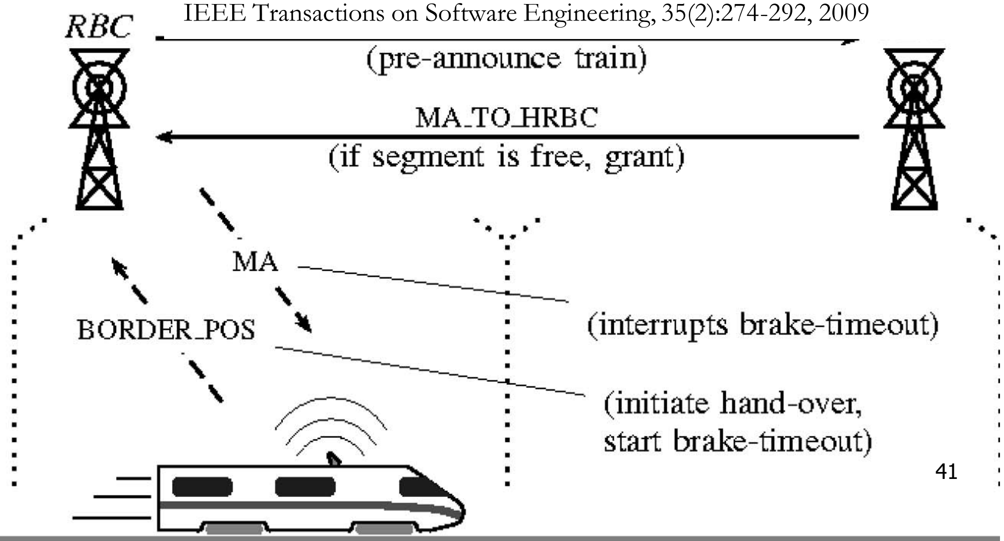


J. Faber, C. Ihlemann, S. Jacobs, and V. Sofronie- Stokkermans.
Automatic Verification of Parametric Specifications with Complex Topologies.
Proceedings of IFM 2010, LNCS 6396: 152-167, Springer, 2010.

Decomposition of Dependability Analysis for enriched Statecharts

- Enrich Statemate with capability to capture failures and their probability distributions
- to analyse questions such as “The probability to hit a safety-critical system configuration within a mission time of 3 hours is at most 0.01.”

E. Böde, M. Herbstritt, H. Hermanns, S. Johr, T. Peikenkamp, R. Pulungan, J. Rakow, R. Wimmer, and B. Becker. Compositional dependability evaluation for statemate. IEEE Transactions on Software Engineering, 35(2):274-292, 2009


RBC
(pre-announce train)
MA_TO_HRBC
(if segment is free, grant)
MA
BORDER_POS
(interrupts brake-timeout)
(initiate hand-over, start brake-timeout)

Decomposition result allows to seperate concerns

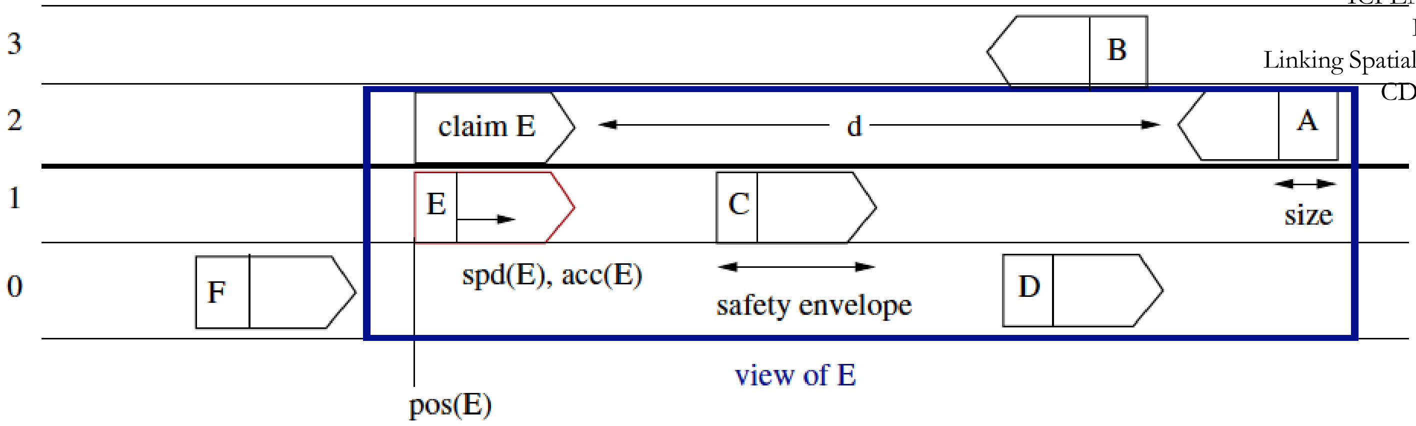
- reducing the enormous state space complexity of application modelling through a fully symbolic branching bi-simulation algorithm
- using a compositional algorithm for deriving uniform continous time Markov Decision processes reflecting transition delays and failure distributions
- performing time bounded dependability analysis on the reduced model

- We managed to avoid state spaces in the order of 10^{40} and instead only need to handle models of up to 10^5 states and 10^6 transitions.

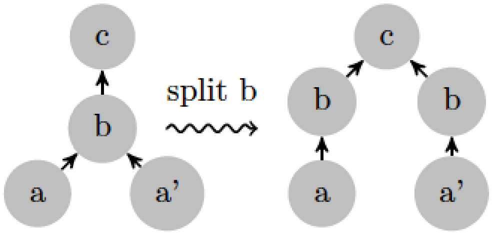
Decompose Spatial and Dynamic Reasoning

- Proving safety (collision freedom) of cars with lane-change maneuvers is a hybrid system verification problem:
- car dynamics + car controllers + assumptions |= safety
- Noticing that collision freedom is a spatial property, we developed a spatial approach to proving safety using spatial logic + abstract controllers.
- The relation to car dynamics is established by linking predicates.

M. Hilscher, S. Linker, E.-R. Olderog, and A.P. Ravn.
An Abstract Model for Proving Safety of Multi-Lane Traffic Manoeuvres,
ICFEM 2011, LNCS 6991, 404-419, Springer, 2011.
E.-R. Olderog, A.P. Ravn, and R. Wisniewski.
Linking Spatial and Dynamic Models for Traffic Maneuvers,
CDC 2015, 8 pp., IEEE, to appear in Dec. 2015.



Decomposition of Stability Proofs



- We use graph-based reasoning todecompose hybrid automata into subgraphs, for which we then solve semidefinite optimization problems to obtain local Lyapunov functions.
  - search for cycles that are connected to the rest of the graph by exactly one vertex
  - Generate a sub-proof for the cycle and thereby obtain Lyapunov function candidates for the "border mode."
  - Replace the cycle by a new mode which has the set of Lyapunov function candidates attached
  - If no such cycle exists, then select a single vertex and split it into one vertex for each pair of incoming and outgoing edges. After splitting, restart
- Integrated into toolset integrated multiple approaches for stability verifcation of hybrid systems

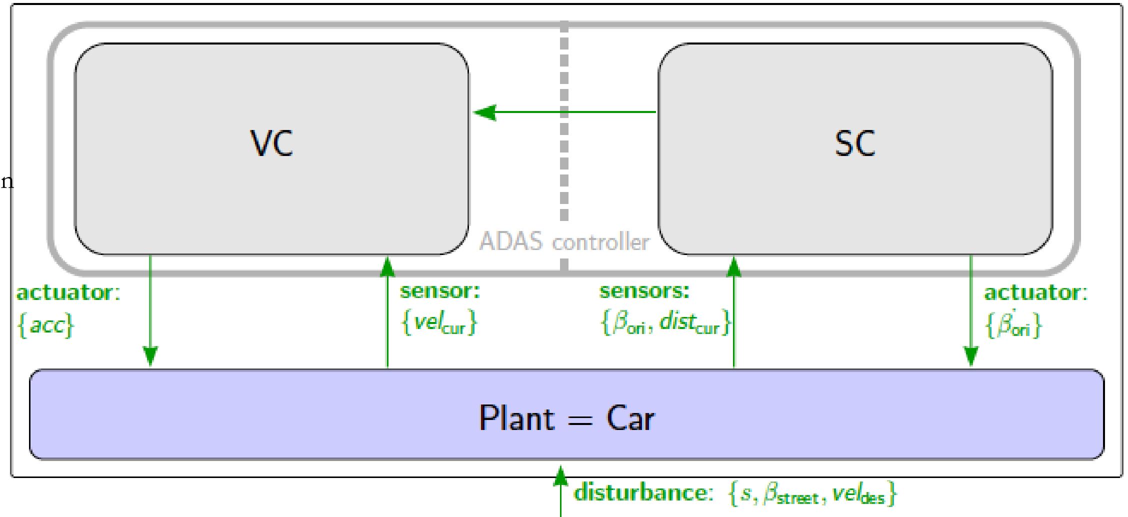
Decompositional Construction of Lyapunov
Functions for Hybrid Systems
Jens Oehlerking and Oliver Theel
HSCC 2009

Stabhyli – A Tool for Automatic Stability Verification of
Non-Linear Hybrid Systems
Eike Möhlmann and Oliver Theel
HSCC 201

Compositional Verification of Hybrid Automata

- We have developed a compositional assume-guarantee approach for the verification of safety and stability properties of hybrid systems with evolutions given by linear differential systems of equations.
- We have developed automated tool support combining synthesis of Lyapunov functions, symbolic orthogonal projections, and SMT solving for discharging verification conditions in compositional reasoning

Werner Damm, Eike Möhlmann, and Astrid Rakow.
Component based design of hybrid systems: A case study on concurrency and coupling
HSCC'14, 145-150. ACM, 2014.
Werner Damm, Henning Dierks, Jens Oehlerking, and Amir Pnueli.
Towards component based design of hybrid systems: Safety and stability. In
Time for Verification: Essays in Memory of Amir Pnueli,
LNCS 6200, 96-143. 2010
Willem Hagemann, Eike Möhlmann, and Astrid Rakow.
Verifying a PI controller using soapbox and stabhyli: Experiences on establishing properties for a steering controller.
In 1st International Workshop on Applied Verification for Continuous and Hybrid Systems, April 2014
Willem Hagemann, Eike Möhlmann, and Oliver Theel.
Hybrid tools for hybrid systems: Proving stability and safety at once,
FORMATS 2015, 222-239, LNCS 9268



VC
SC
ADAS controller
actuator: $\{acc\}$
sensor: $\{vel_{cur}\}$
sensors: $\{\beta_{ori}, dist_{cur}\}$
actuator: $\{\dot{\beta}_{ori}\}$
Plant = Car
disturbance: $\{s, \beta_{street}, vel_{des}\}$

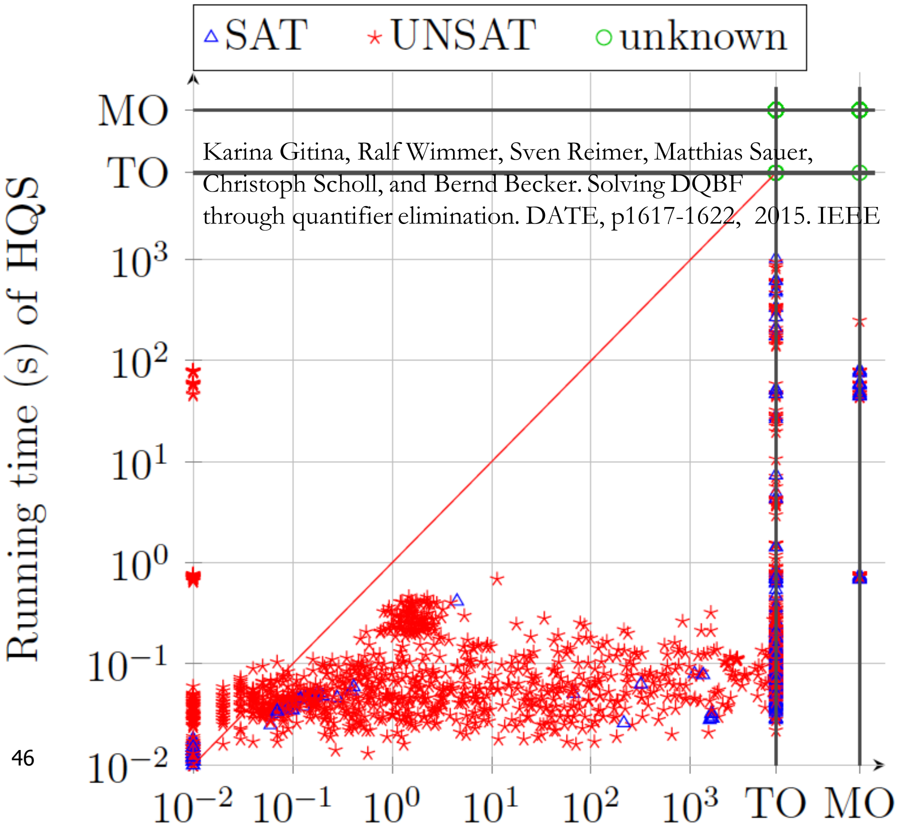
Solver technology

Solving dependency quantified Boolean formula

$$\forall x_1 \forall x_2 \ldots \forall x_n \exists y_1 (D_{y_1}) \exists y_2 (D_{y_2}) \ldots \exists y_m (D_{y_m}) : \varphi.$$

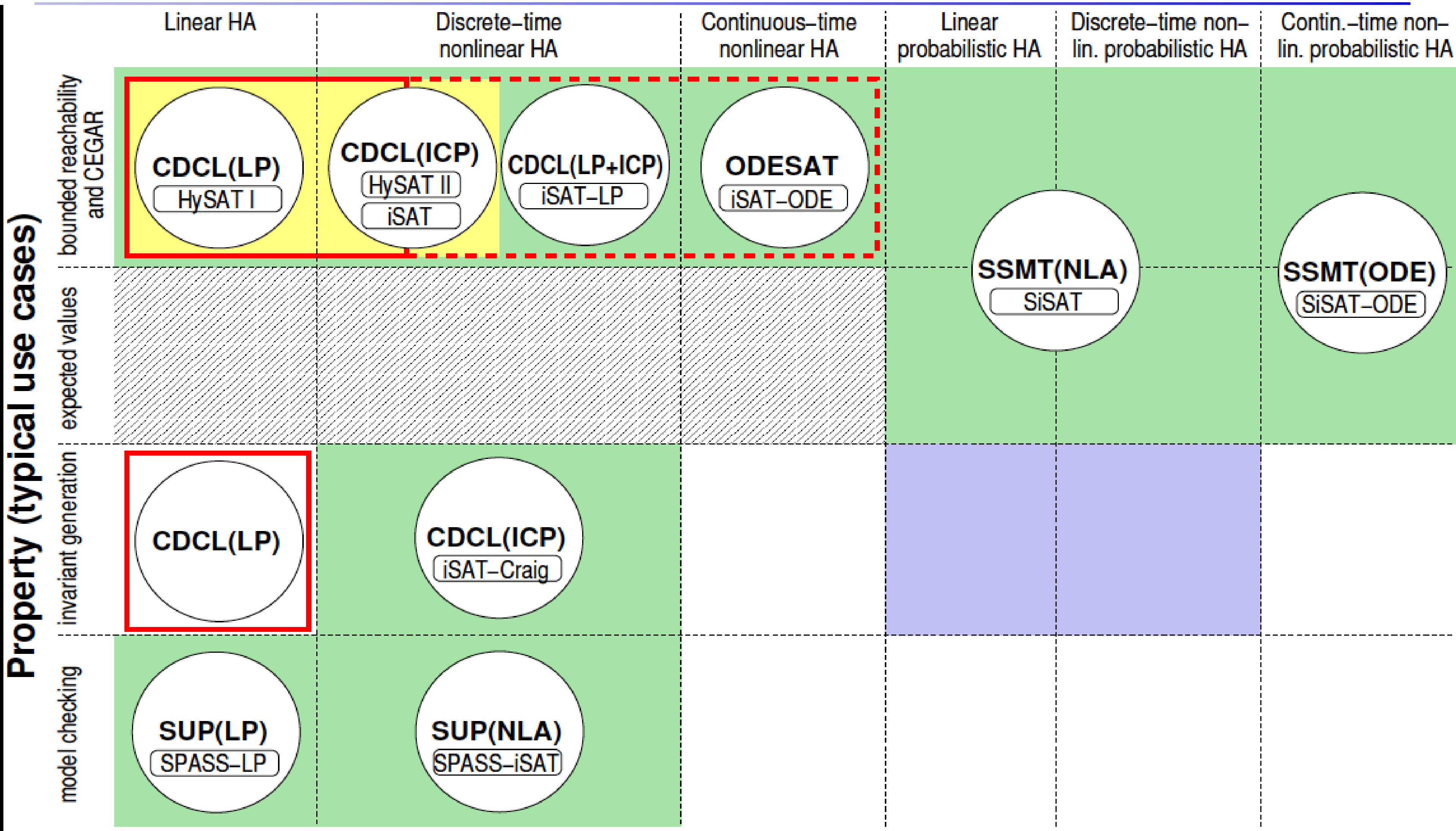
- strictly more expressive than QBF, as needed in designs with multiple black boxes: can give detailed description of which variable depends on which black-box
- reduction to QBF by eliminating variables which destroy linear order and many more tricks, AIG based QBF

- drastically outperforms only other available DQBF solver



Karina Gitina, Ralf Wimmer, Sven Reimer, Matthias Sauer, Christoph Scholl, and Bernd Becker. Solving DQBF through quantifier elimination. DATE, p1617-1622, 2015. IEEE

Solver Technologies for Hybrid Automa



Property (typical use cases)	Linear HA	Discrete-time nonlinear HA		Continuous-time nonlinear HA	Linear probabilistic HA	Discrete-time non-lin. probabilistic HA	Contin.-time non-lin. probabilistic HA
bounded reachability and CEGAR	CDCL(LP) HySAT I	CDCL(ICP) HySAT II iSAT	CDCL(LP+ICP) iSAT-LP	ODESAT iSAT-ODE	SSMT(NLA) SiSAT		SSMT(ODE) SiSAT-ODE
expected values	▨	▨	▨	▨			
invariant generation	CDCL(LP)	CDCL(ICP) iSAT-Craig					
model checking	SUP(LP) SPASS-LP	SUP(NLA) SPASS-iSAT					

2007: 🟨 **AVACS H1/2** 🟥 **Competitors** **2011/15:** 🟩 / 🟪 **AVACS H1/2** ⬚ **Competitors**

Solver Techniques for Probabilistic Systems

- First approach to define and efficiently compute interpolants for SSAT problems (with applications to modelchecking safety and region stability in Markov Decision processes)

- We invented the notion of stochastic satisfiability modulo theories (SSMT) and the corresponding SiSAT solving algorithm, which provide a symbolic method for the reachability analysis of probabilistic hybrid systems.

Tino Teige and Martin Fränzle: Generalized Craig Interpolation for Stochastic Boolean Satisfiability Problems with Applications to Probabilistic State Reachability and Region Stability, Logical Methods in Computer Science 8(2)), 1-32, 2012.

M. Fränzle, H. Hermanns, and T. Teige. Stochastic satisfiability modulo theory:
A novel technique for the analysis of probabilistic hybrid systems, Proceedings HSCC'08, LNCS 4981, 2008

Tino Teige, Andreas Eggers, and Martin Fränzle.
Constraint-based analysis of concurrent probabilistic hybrid systems:
An application to networked automation systems. Nonlinear Analysis: Hybrid Systems, 5(2):343-366, 2011

Solver Techniques for non-linear arithmetic

- see exploiting robustness (iSAT, SUP(NAP))
- Finding Craig Interpolants for non-linear arithmetic using iSAT allows model-checking of safety properties of hybrid automata with non-linear dynamics
- Establishing lower bounds for safety properties of probabilistic Hybrid Automata by reduction to SSMT solving
- Extended methods for finding Craig Interpolants to SSMT allowing modelchecking of PHA

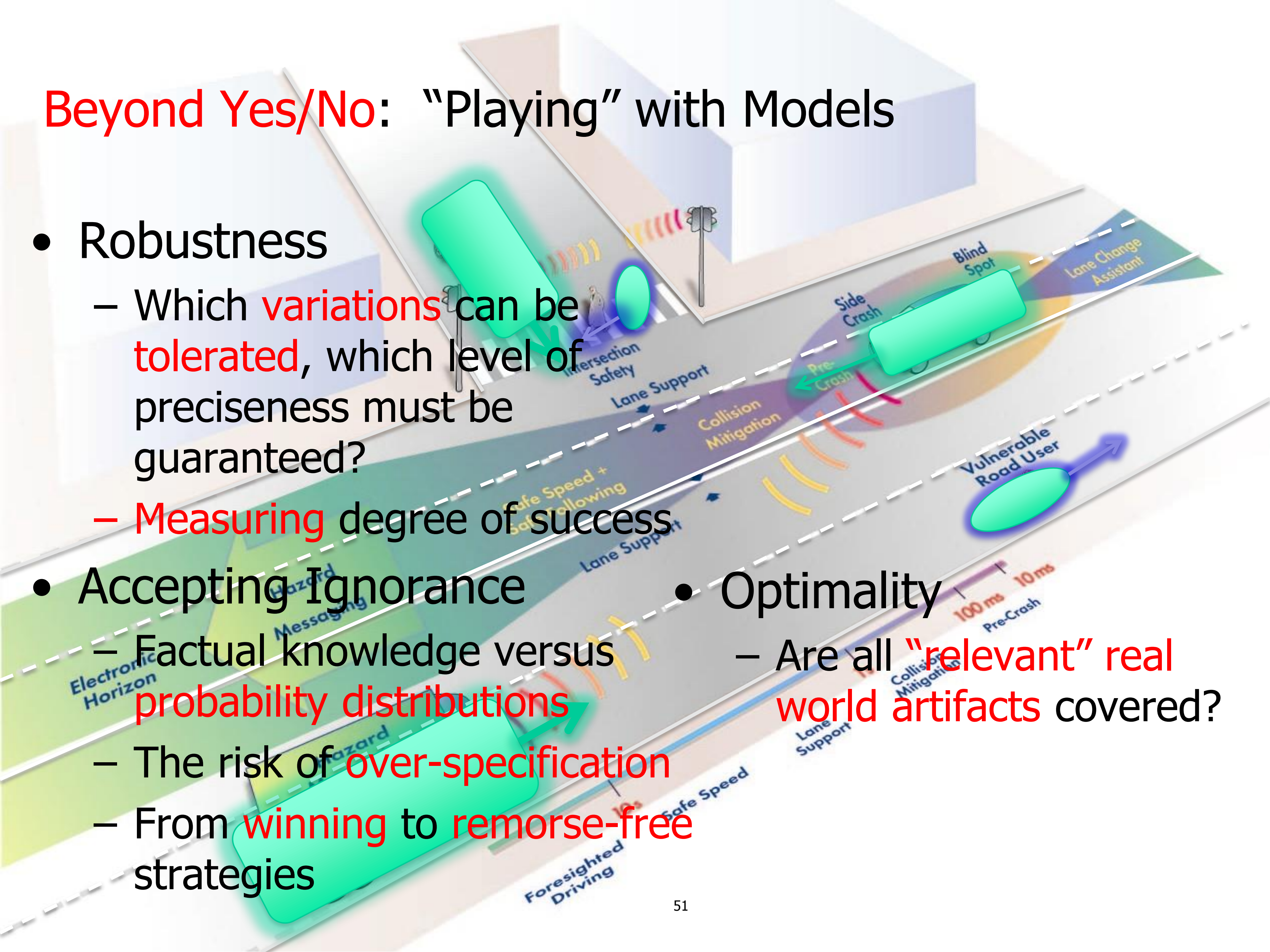
Stefan Kupferschmid and Bernd Becker: Craig Interpolation in the Presence of Non-linear Constraints, in Formal Modeling and Analysis of Timed Systems, 9th International Conference, FORMATS 2011, Aaalborg, Denmark, September 21-23, 2011, LNCS, 2011

Tino Teige, Andreas Eggers, and Martin Fränzle.
Constraint-based analysis of concurrent probabilistic hybrid systems:
An application to networked automation systems.
Nonlinear Analysis: Hybrid Systems, 5(2):343-366, 2011.

Yang Gao and Martin FrÃ¤nzle. A Solving Procedure for
Stochastic Satisfiability Modulo Theories with Continuous Domain.
InProc. QEST 2015, Madrid, Spain. LNCS 9259, Springer, September 2015.

Lessons Learned

Beyond Yes/No: “Playing” with Models



- Robustness
  - Which variations can be tolerated, which level of preciseness must be guaranteed?
  - Measuring degree of success
- Accepting Ignorance
  - Factual knowledge versus probability distributions
  - The risk of over-specification
  - From winning to remorse-free strategies
- Optimality
  - Are all “relevant” real world artifacts covered?

Beyond Yes/No: “Playing” with Models

- Don´t take a model as God-given!
  - Sensitivity analysis: will slightly twisted model change verification result?
  - Can “slightly twisted” model reduce complexity of verification problem?
  - Will a statistical view or a metric view provide more relevant insights?

- Examples
  - Quasi decidability result for robust hybrid systems
  - Metric temporal logics measuring distance from truth
  - Parametric verification for sensitivity analysis of sensor precision
  - Probabilistic timed reachability analysis for completing a maneuver
  - Extending the world model

Design Meets Verification

- Investigate interplay between system design and system analyzability
  - Exploit deep insight into analysis algorithms to provide guidelines for system model easing system analysis
  - Guidelines establish invariants by construction. Those can be exploited in optimizing analysis algorithms

- Examples
  - Let the compiler guarantee invariance properties regarding resource usages
  - “reasonable LHA” are analyzable in polynomial time
  - design patterns, such as architectural patterns guaranteeing invariants on system interactions supporting compositional reasoning
  - Design for robustness

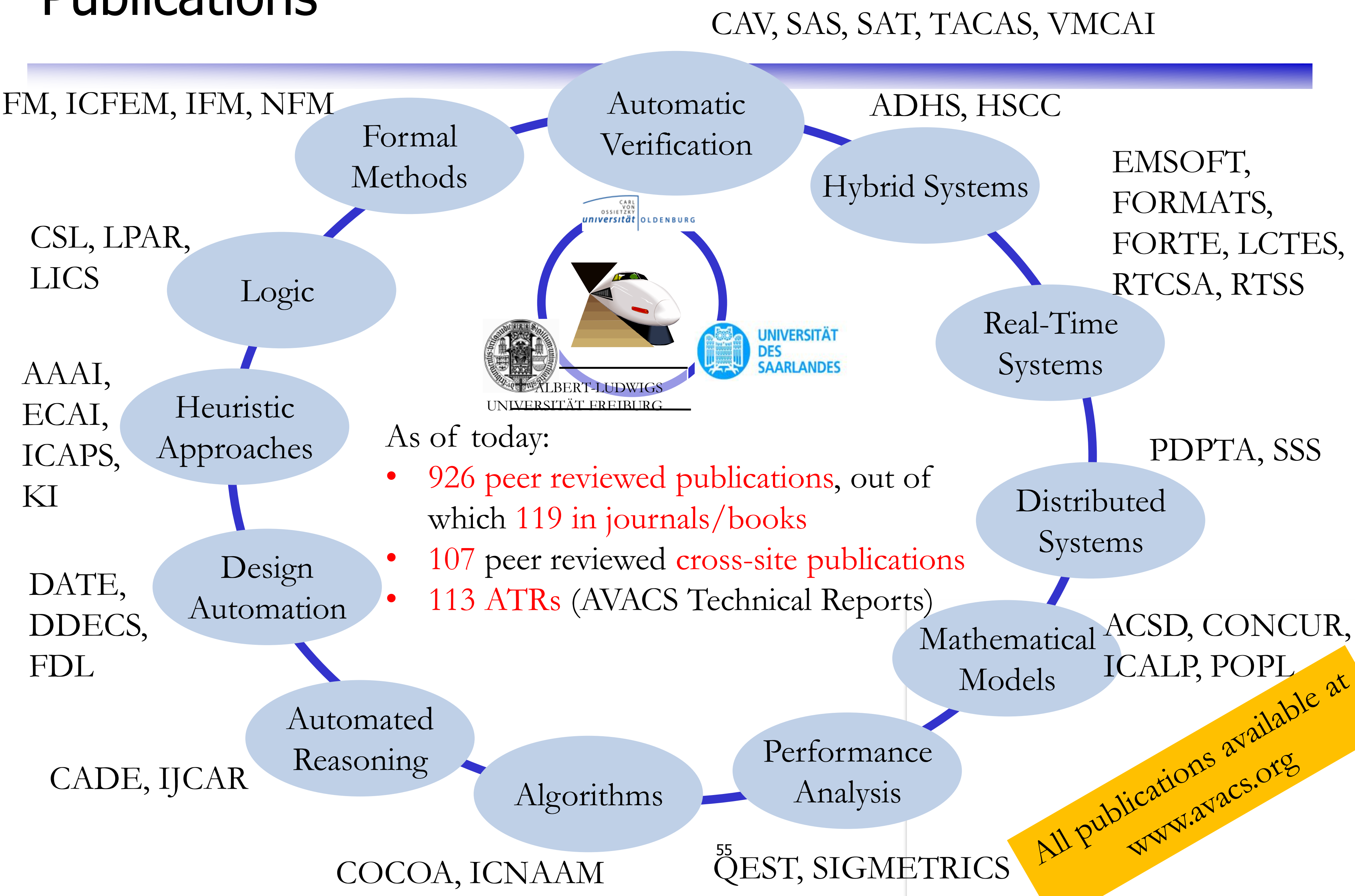
CARL VON OSSIETZKY universität OLDENBURG

ALBERT-LUDWIGS UNIVERSITÄT FREIBURG

UNIVERSITÄT DES SAARLANDES

Impact

Publications



Automatic Verification: CAV, SAS, SAT, TACAS, VMCAI

Hybrid Systems: ADHS, HSCC

Real-Time Systems: EMSOFT, FORMATS, FORTE, LCTES, RTCSA, RTSS

Distributed Systems: PDPTA, SSS

Mathematical Models: ACSD, CONCUR, ICALP, POPL

Performance Analysis: QEST, SIGMETRICS

Algorithms: COCOA, ICNAAM

Automated Reasoning: CADE, IJCAR

Design Automation: DATE, DDECS, FDL

Heuristic Approaches: AAAI, ECAI, ICAPS, KI

Logic: CSL, LPAR, LICS

Formal Methods: FM, ICFEM, IFM, NFM

Carl von Ossietzky Universität Oldenburg

Universität des Saarlandes

Albert-Ludwigs Universität Freiburg

As of today:

- 926 peer reviewed publications, out of which 119 in journals/books
- 107 peer reviewed cross-site publications
- 113 ATRs (AVACS Technical Reports)

All publications available at www.avacs.org

Increasing Automation - www.avacs.org/tools

Model checker / solver for ...

HySAT-I, HySAT-II, iSAT/iSAT-3, iSAT(ODE), SiSAT, SiSAT-SMC, SUP(T), fomc , HyFold , Stabhyli, HYFOLD,

... hybrid systems

Geobound, INFAMY, Modest Toolset, PARAM, PASS, SiSAT, SiSAT-SMC, SHAVE, ProHVer

... probabilistic systems

SLAB, Ultimate Automizer, rtana2, rtana_DS, Mcta, SpaceEx, fsmtMC, INFAMY, Modest Toolset, PARAM, SHAVE, ProHVer, HYFOLD

... hard & soft real-time systems

Systems

ADAM, Unbeast, Synthia

Synthesis Tools

Theorem prover...

Keymaera, SUP(T)

... for hybrid systems

CARL VON OSSIETZKY universität OLDENBURG
ALBERT-LUDWIGS-UNIVERSITÄT FREIBURG
UNIVERSITÄT DES SAARLANDES

Modeling

ASTRA, sigref

Model reduction

Syspect, APHzip

Graphical specification tools

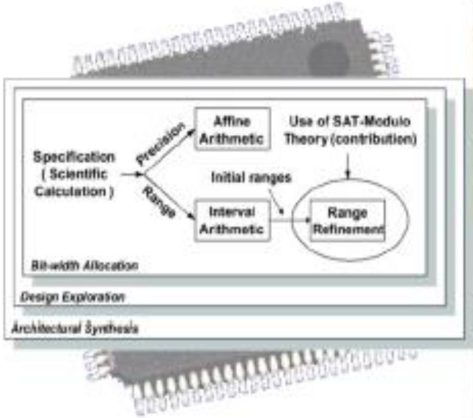
Basics

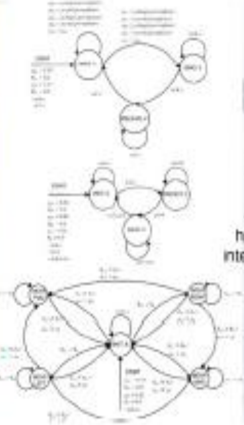
H-PILot, SmtInterpol, Arctor, chi, SSPRATTUS, MyND, QMiraXT, PaQuBE, AIGsolve, HQS, bunsat, FlowSim, HySAT-I, HySAT-II, iSAT/iSAT-3, iSAT(ODE), SiSAT, SiSAT-SMC, SUP(T), H-PILoT , soapbox , HAHA (Hierarchical Analysis of Hybrid Automata)

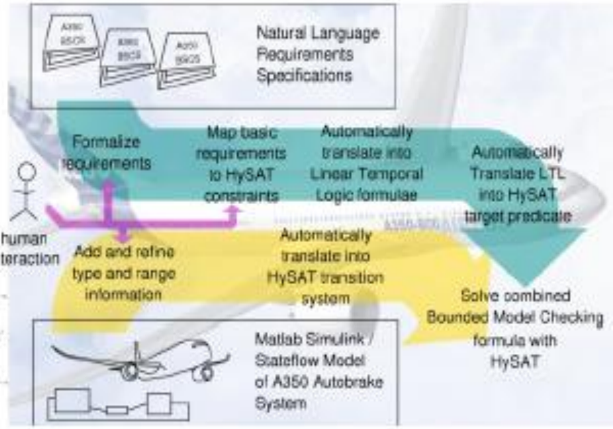
Core algorithms

LinAIG and many more

Data structures for symbolic state representation

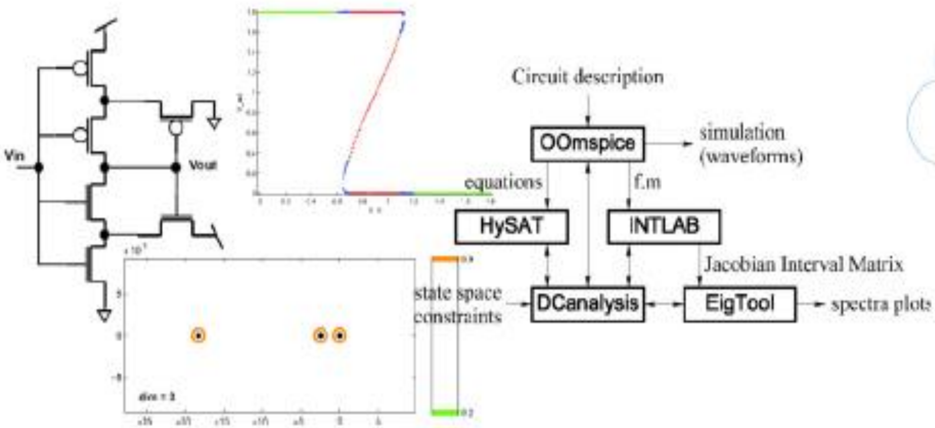


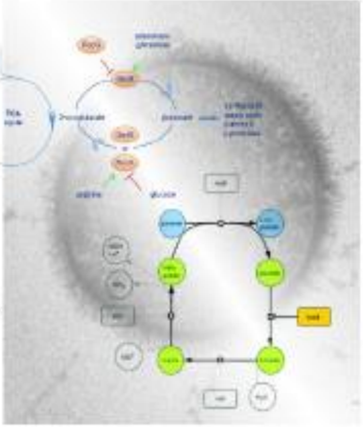


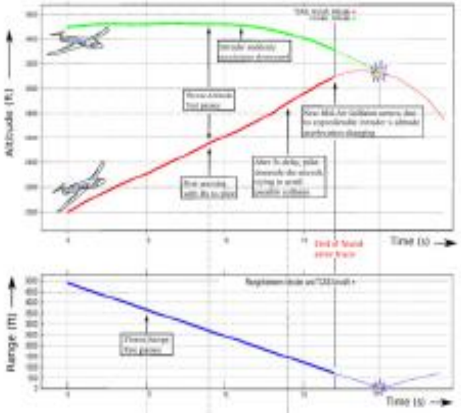


External use of iSAT algorithm

- Automatic bit-width allocation for FPGAs (McMaster University, Hamilton, ON, Canada)
- Online(!) safety verification of a learning air-hockey robot (Italian Inst. of Technology & University of Genova, Italy)
- Integration into the engineering of the Airbus A350 autobrake system (Airbus UK & Edinburgh U, UK)
- Identification of equilibrium points in analog DC circuits (University of British Columbia, Vancouver, Canada)
- Automatic hypothesis finding for cell mutations (Göttingen University, Germany)
- Validation of airborne collision avoidance systems (Lincoln Laboratory, M.I.T., USA)







TP1 DeCoDe: Accurate Dead Code Detection in Embedded C Code

- Transfers H1/2's arithmetic constraint solving techniques to industrial practice,
  - extending iSAT with constraint propagation & Craig interpolation reflecting IEEE 754 number formats
  - in order to automatically solve reachability problems in floating-point dominated embedded C code
  - by means of BMC, inductive verification, and CEGAR
- Automatic detection of dynamically unreachable code enhances interpretation of test coverage figures, helps to improve code, ...
- Partners: BTC ES AG (Oldenburg), Sick AG (Waldkirch), Oldenburg University, University of Freiburg

universität OLDENBURG

ALBERT-LUDWIGS UNIVERSITÄT FREIBURG

UNIVERSITÄT DES SAARLANDES

Through industrial research projects/cooperation

- Examples at Oldenburg
  - MOVES – power grid stability analysis
  - Crystal – consistency and completeness analysis of requirements
  - Pegasus – statistical model checking in analysis of autonomous driving
  - SAVE – ISO 26262 compliant safety analysis of automotive applications
- Examples at Freiburg
  - BMWi project Kontiplan
  - HW/SW Co-verification in safety relevant sensor applications
  - safe system initialization
  - Verification and Test in the Presence of Unknowns
- Examples at Saarbrücken
  - Improvements of Saarbrücken's timing-analysis technology have been and will be integrated into AbsInt's timing-analysis tools
  - Insights into the timing-predictability of architectures have led to the design of the Kalray many-core architecture MMPA

"In jedem Anfang wohnt ein Zauber inne‟

Andreas Podelski
nach Herrmann Hesse

CARL VON OSSIETZKY universität OLDENBURG

ALBERT-LUDWIGS
UNIVERSITÄT FREIBURG

UNIVERSITÄT
DES
SAARLANDES