Invited Academic Keynote

Kim G. Larsen
Aalborg University

AVACS & UPPAAL
12 Years of Interaction

Kim G. Larsen
Aalborg University

AVACS

German Science Foundation, 1.1.04 – 31.12. 15.

AIM (Werner Damm, FM 2015)

- rigorous mathematical verification and analysis of models and realizations of complex safety-critical computerized systems,
- raise the state of the art in verification and analysis from a level, where it is applicable .. to a level allowing comprehensive and holistic verification.

AVACS

German Science Foundation, 1.1.04 – 31.12. 15.

Werner Damm, FM 2015.

Models:

- all types of behaviours
  - nondeterministic, probabilistic, real-time, and hybrid system models, models reflecting the dynamic
- the investigated classes of models cover all system structures
- the investigated classes of time models are expressive enough to cover all layers of the design space
  - physical latencies of vehicles to worst-case execution times of tasks on modern processor architectures

Tools:

- automatic techniques to verify or falsify compliance of models

Methods:

- formal proofs for complete systems from guarantees of subsystems

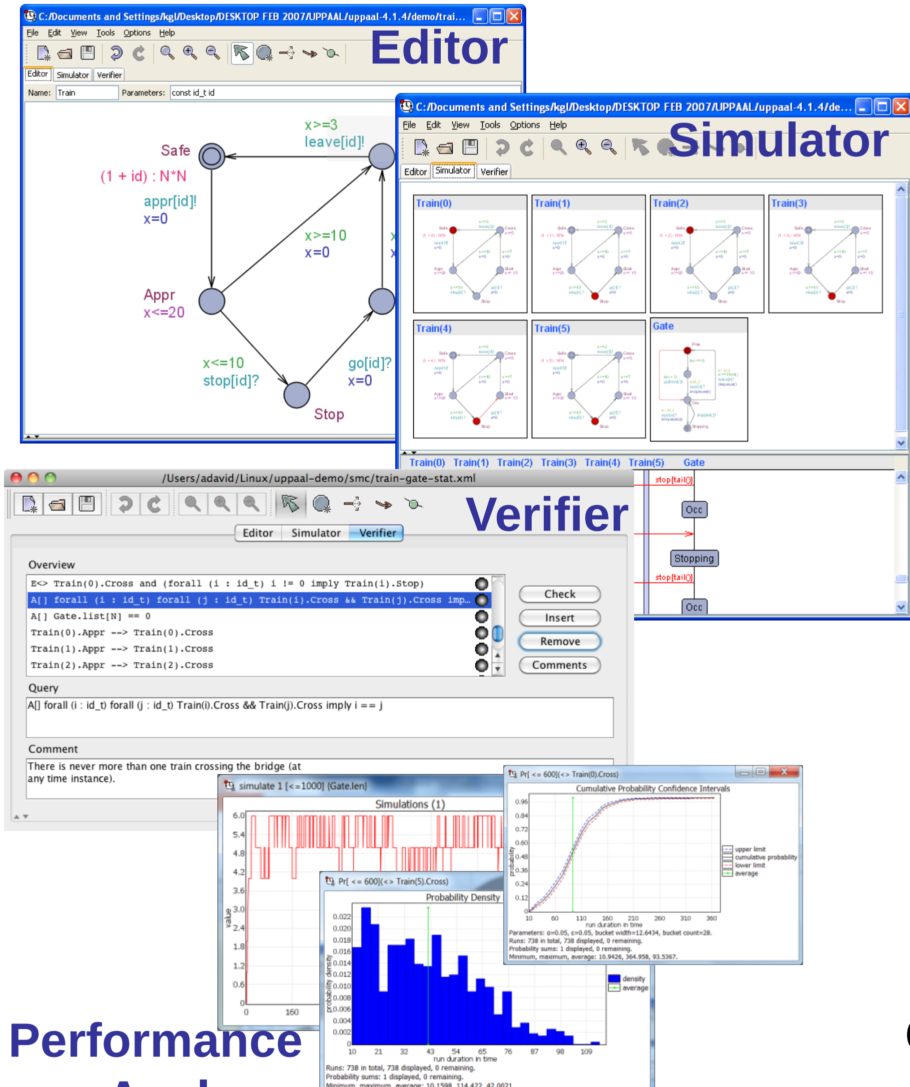
AVACS

German Science Foundation, 1.1.04 – 31.12. 15.

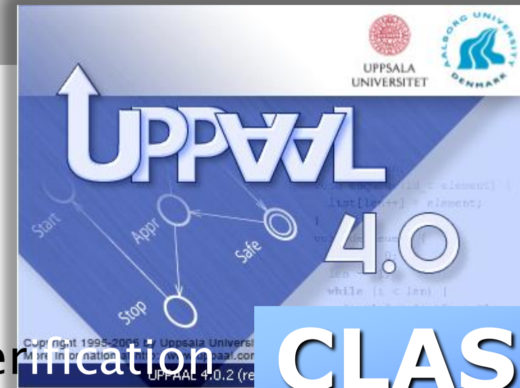
Project Group R Real-Time Systems Coordinator: E. Olderog, CvOU Summary	**Project Group H** Hybrid Systems Coordinator: M. Fränzle Summary	**Project Group S** Coarse Grain System Structure Coordinator: Podelski Summary
R1: Beyond Timed Automata	H1/2: Constraint-based ... S. Ratschan, ASCR	S1: Compositional Approaches to
R2: Timing Analysis and Distribution of Real-Time Tasks Coordinator: Wilhelm, UdS Additional PIs: E. Althaus, MPII W. Damm, CvOU S. Hack, UdS J. Reineke, UdS	H3: Automated Verification of Cooperating Traffic Agents Coordinator: W. Damm, CvOU Additional PIs: E. Althaus, MPII E. Olderog, CvOU C. Scholl, ALU Sofronie-Stokkermanns, MPII U. Waldmann, MPII	S2: Dynamic Communication Systems Coordinator: A. Podelski, ALU Additional PIs: W. Damm, CvOU B. Finkbeiner, UdS H. Hermanns, UdS J: Reineke, UdS C. Weidenbach, MPII
R3: Heuristic Search and Abstract Model Checking Coordinator: B. Nebel, ALU Additional PIs: B. Finkbeiner, UdS A. Podelski, ALU	H4: Automatic Verification of Hybrid System Stability Coordinator: O. Theel, CvOU Additional PIs: M. Fränzle, CvOU H. Hermanns, UdS A. Podelski, ALU V. Wolf, UdS	S3: Formal Verification of Dependability Properties Coordinator: H. Hermanns, UdS Additional PIs: B. Becker, ALU O. Theel, CvOU V. Wolf, UdS

Project Group R Real-Time Systems Coordinator: E. Olderog, CvOU Summary
Project Group H Hybrid Systems Coordinator: M. Fränzle Summary
Project Group S Coarse Grain System Structure Coordinator: Podelski Summary

UPPAAL Tool Suit



Performance Analyses



Verification	CLASSIC
Optimization	CORA
Synthesis	TIGA
Component	ECDAR
Testing	TRON
Performance Analysis	SMC
Optimal Synthesis	STRATEGO

AVACS & UPPAAL

Highlevel view

[PDF] REPORTS - AVACS
www.avacs.org/.../avacs_technical_report_072.pdf ▾ Oversæt denne side
efter BWIST Gezgin - 2011 - Relaterede artikler
AVACS – Automatic Verification and Analysis of Complex Systems ... **Uppaal** is known to be an efficient tool to verify properties of systems in the dense.

[PDF] Download as a PDF
citeseerx.ist.psu.edu/viewdoc/download?doi... ▾ Oversæt denne side
efter B Westphal - 2011 - Relaterede artikler
AVACS – Automatic Verification and Analysis of Complex Systems ... leads-to verification as supported by **Uppaal**, thereby obtain observer based LSC ...

[PDF] Faster than UPPAAL ?
www2.informatik.uni-freiburg.de/.../kupferschmid-et... ▾ Oversæt denne side
efter S Kupferschmid - Citeret af 15 - Relaterede artikler
not even try to compete with **UPPAAL** in this (i.e., **UPPAAL's**) arena. Instead, ... Both case studies are part of the **AVACS** project benchmark suite. The results in ...

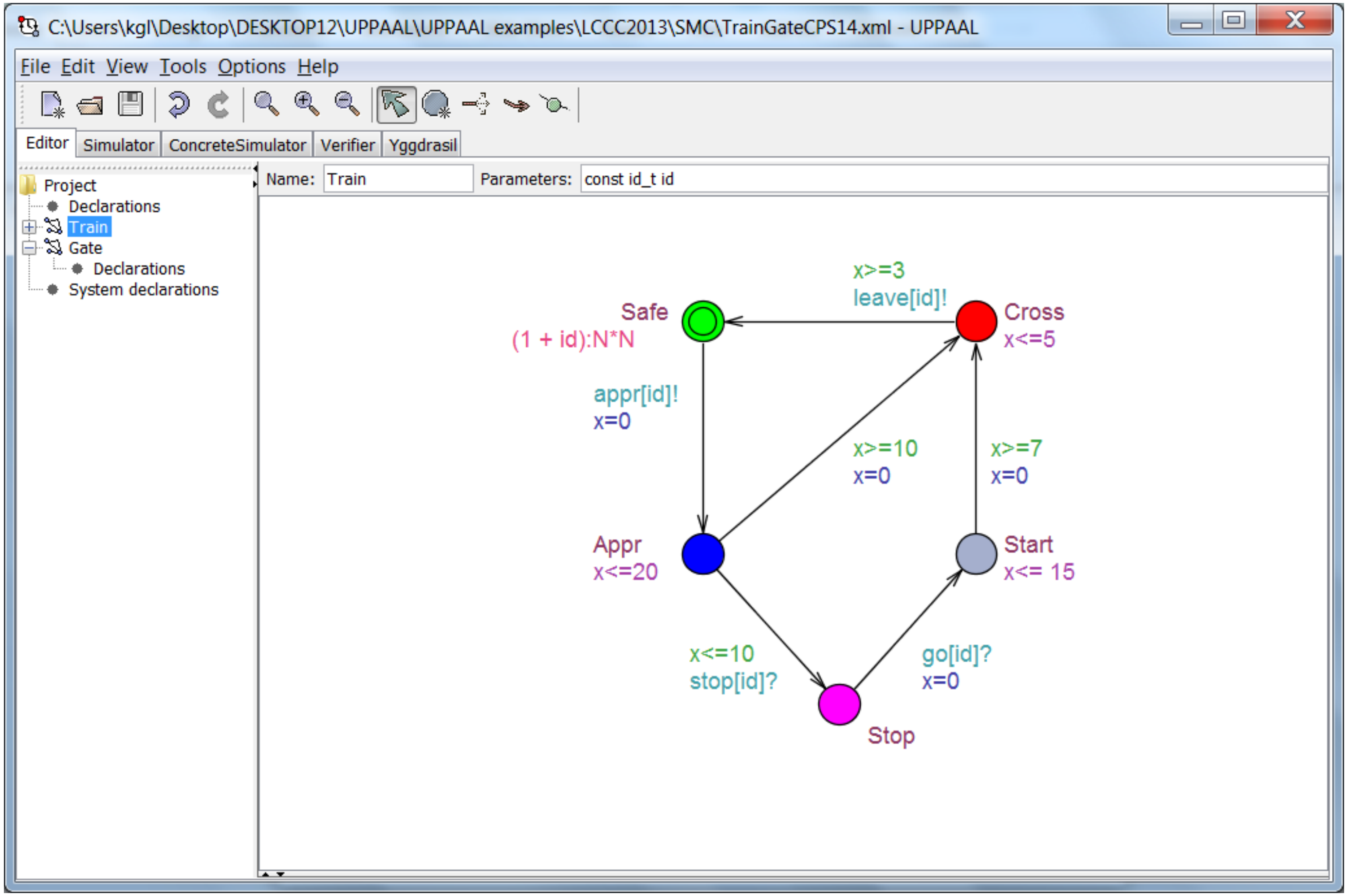
[PDF] mctau: Bridging the Gap between Modest and UPPAAL*
www.modestchecker.net/Link.aspx?id=pub:BDHH12 ▾ Oversæt denne side
We present our Modest-to-**Uppaal** tool chain mctau, which allows both a fully ... SFB/TR 14 **AVACS**, and by the DFG/NWO Bilateral Research Program ROCKS.

mctau: Bridging the Gap between Modest and UPPAAL ...
link.springer.com/.../10.1007%2F978-3-642-31759-... ▾ Oversæt denne side
efter J Bogdoll - 2012 - Citeret af 12 - Relaterede artikler
We present our Modest-to-**Uppaal** tool chain mctau, which allows both a fully ... 295261, by the DFG as part of SFB/TR 14 **AVACS**, and by the DFG/NWO Bilateral ...

Damm
AVACS publications
926

GOOGLE:
AVACS+UPPAAL
1.200

Demo


C:\Users\kgl\Desktop\DESKTOP12\UPPAAL\UPPAAL examples\LCCC2013\SMC\TrainGateCPS14.xml - UPPAAL
File Edit View Tools Options Help
Editor
Simulator
ConcreteSimulator
Verifier
Yggdrasil
Project
Declarations
Train
Gate
Declarations
System declarations
Name: Train
Parameters: const id_t id
x>=3
leave[id]!
Safe
(1 + id):N*N
Cross
x<=5
appr[id]!
x=0
x>=10
x=0
x>=7
x=0
Appr
x<=20
Start
x<= 15
x<=10
stop[id]?
go[id]?
x=0
Stop

AVACS

German Science Foundation, 1.1.04 – 31.12. 15.

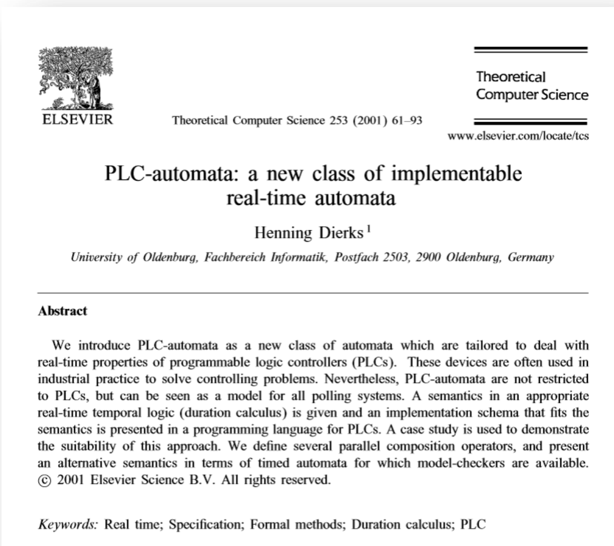
Project Group R Real-Time Systems Coordinator: E. Olderog, CvOU Summary	**Project Group H** Hybrid Systems Coordinator: M. Fränzle Summary	**Project Group S** Coarse Grain System Structure Coordinator: Podelski Summary
R1: Beyond Timed Automata Coordinator: E. Additional PIs: B. Finkbeiner, U M. Fränzle, CvO A. Podelski, ALU V. Sofronie- Sto	H1/2: Constraint-based	S1: Compositional Aproaches to iner, UdS
R2: Timing Anal Distribution of Coordinator: Wi Additional PIs: E. Althaus, MPI W. Damm, CvO S. Hack, UdS J. Reineke, UdS		ication A.
R3: Heuristic Se Abstract Model Coordinator: B. Nebel, ALU Additional PIs: B. Finkbeiner, UdS A. Podelski, ALU	Coordinator: O. Theel, CvOU Additional PIs: M. Fränzle, CvOU H. Hermanns, UdS A. Podelski, ALU V. Wolf, UdS	Coordinator: H. Hermanns, UdS Additional PIs: B. Becker, ALU O. Theel, CvOU V. Wolf, UdS

R1: Beyond Timed Automata
Coordinator: E. Olderog, CvOU
Additional PIs:
B. Finkbeiner, UdS
M. Fränzle, CvOU
A. Podelski, ALU
V. Sofronie- Stokkermans, MPII

R1: Beyond Timed Automata

MobY/PLC

Henning Dierks
Ernst-Rüdieger Olderog



ELSEVIER

Theoretical Computer Science 253 (2001) 61–93

Theoretical Computer Science

www.elsevier.com/locate/tcs

PLC-automata: a new class of implementable real-time automata

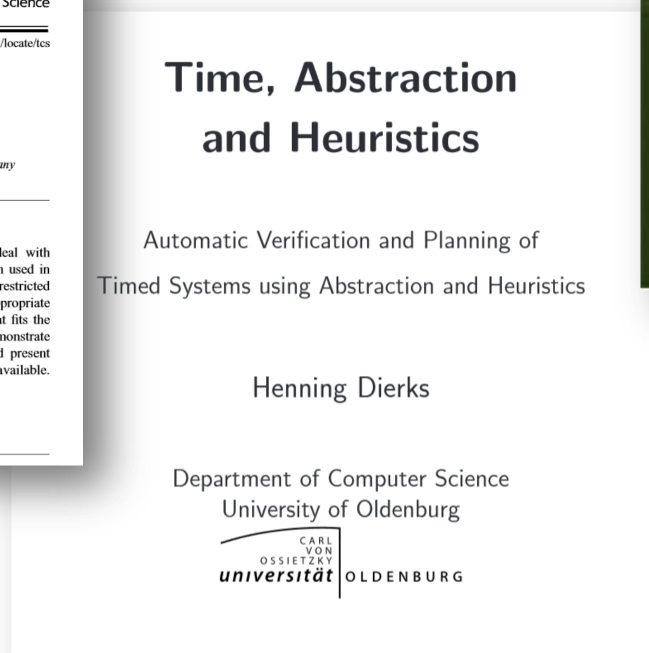
Henning Dierks[1]

University of Oldenburg, Fachbereich Informatik, Postfach 2503, 2900 Oldenburg, Germany

Abstract

We introduce PLC-automata as a new class of automata which are tailored to deal with real-time properties of programmable logic controllers (PLCs). These devices are often used in industrial practice to solve controlling problems. Nevertheless, PLC-automata are not restricted to PLCs, but can be seen as a model for all polling systems. A semantics in an appropriate real-time temporal logic (duration calculus) is given and an implementation schema that fits the semantics is presented in a programming language for PLCs. A case study is used to demonstrate the suitability of this approach. We define several parallel composition operators, and present an alternative semantics in terms of timed automata for which model-checkers are available.

Keywords: Real time; Specification; Formal methods; Duration calculus; PLC



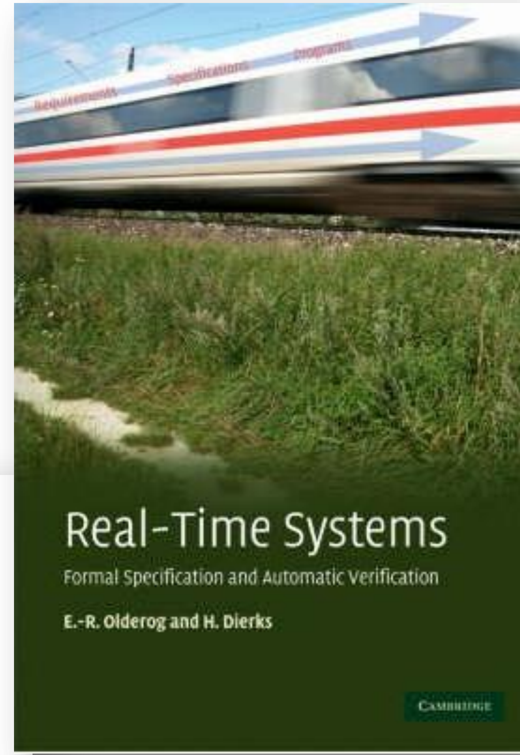
Time, Abstraction and Heuristics

Automatic Verification and Planning of Timed Systems using Abstraction and Heuristics

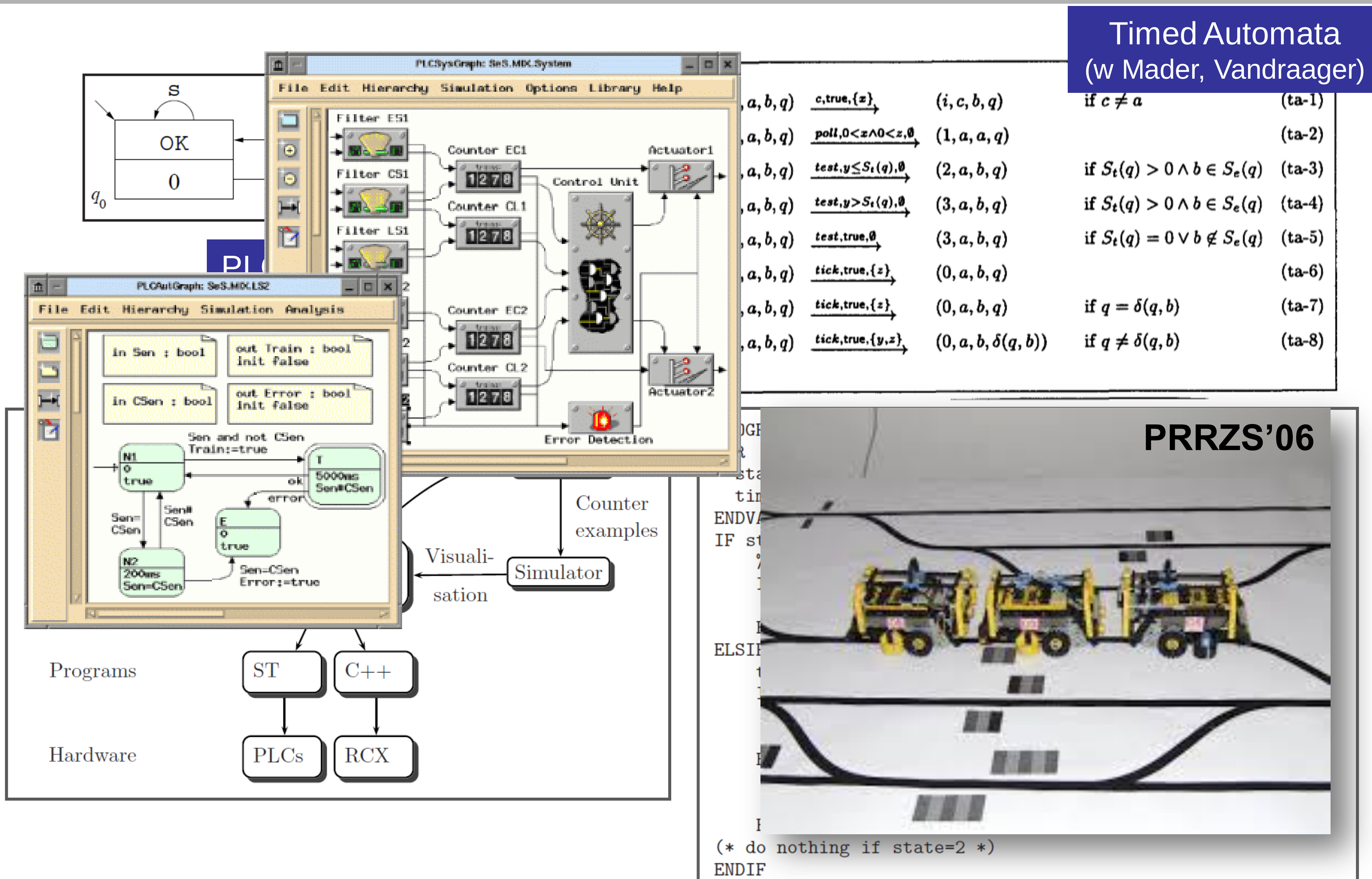
Henning Dierks

Department of Computer Science
University of Oldenburg

CARL VON OSSIETZKY universität OLDENBURG



R1: Beyond Timed Automata



R1: Beyond Timed Automata

Michael Gerke, Rüdiger Ehlers, Bernd Finkbeiner, Hans-Jörg Peter:
Model Checking the FlexRay Physical Layer Protocol.
FMICS'10

Fault-tolerance under error models and hardware assumptions (glitches, jitter)

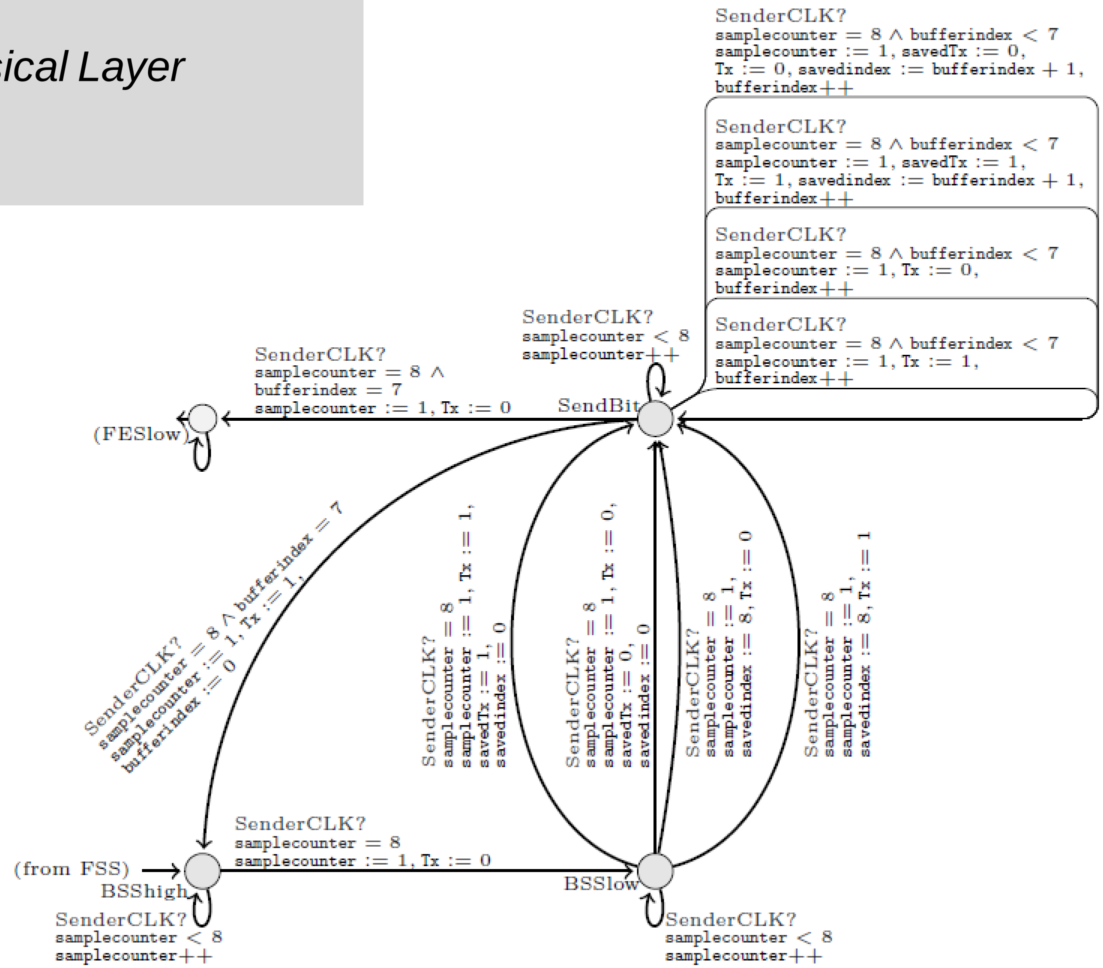


Fig. 4. Model of the transmission of the message bytes.

R1: Beyond Timed Automata

(a) Standard parameter values.

Parameter	Value	Corresponds to
CYCLE	10000	$\frac{1}{80\,MHz} = 12.5\,ns$
DEVIATION	30	$\pm 0.15\,\%$
SETUP	368	$460\,ps$
HOLD	1160	$1450\,ps$
PMIN	12	$15\,ps$
PMAX	1160	$1450\,ps$
ERRDIST	4	1 out of 5

(b) Changed parameter values.

Changed parameter	Tolerable glitches
PMAX − PMIN $\leq$ 6086	1 out of 4
PMAX − PMIN $\leq$ 6086	at most 2
PMAX − PMIN $\leq$ 9616	at most 1
DEVIATION $\leq$ 92	1 out of 4
DEVIATION $\leq$ 92	at most 2
DEVIATION $\leq$ 218	at most 1
DEVIATION $\leq$ 348	none

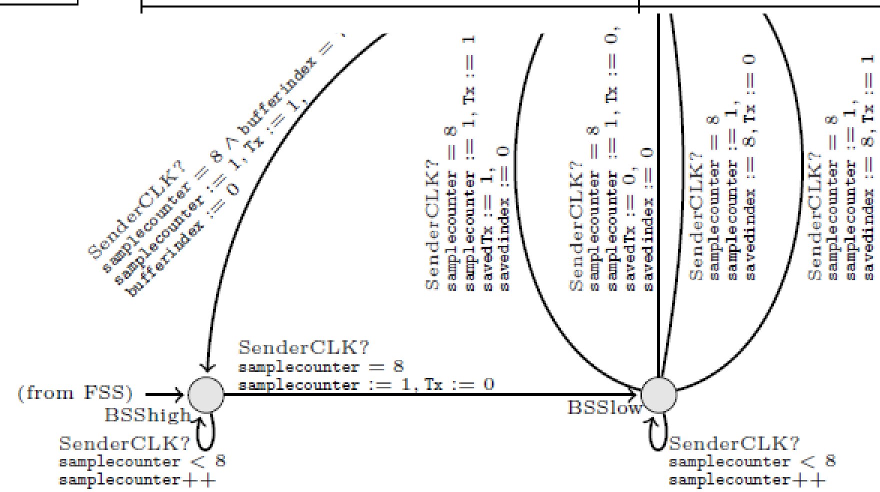
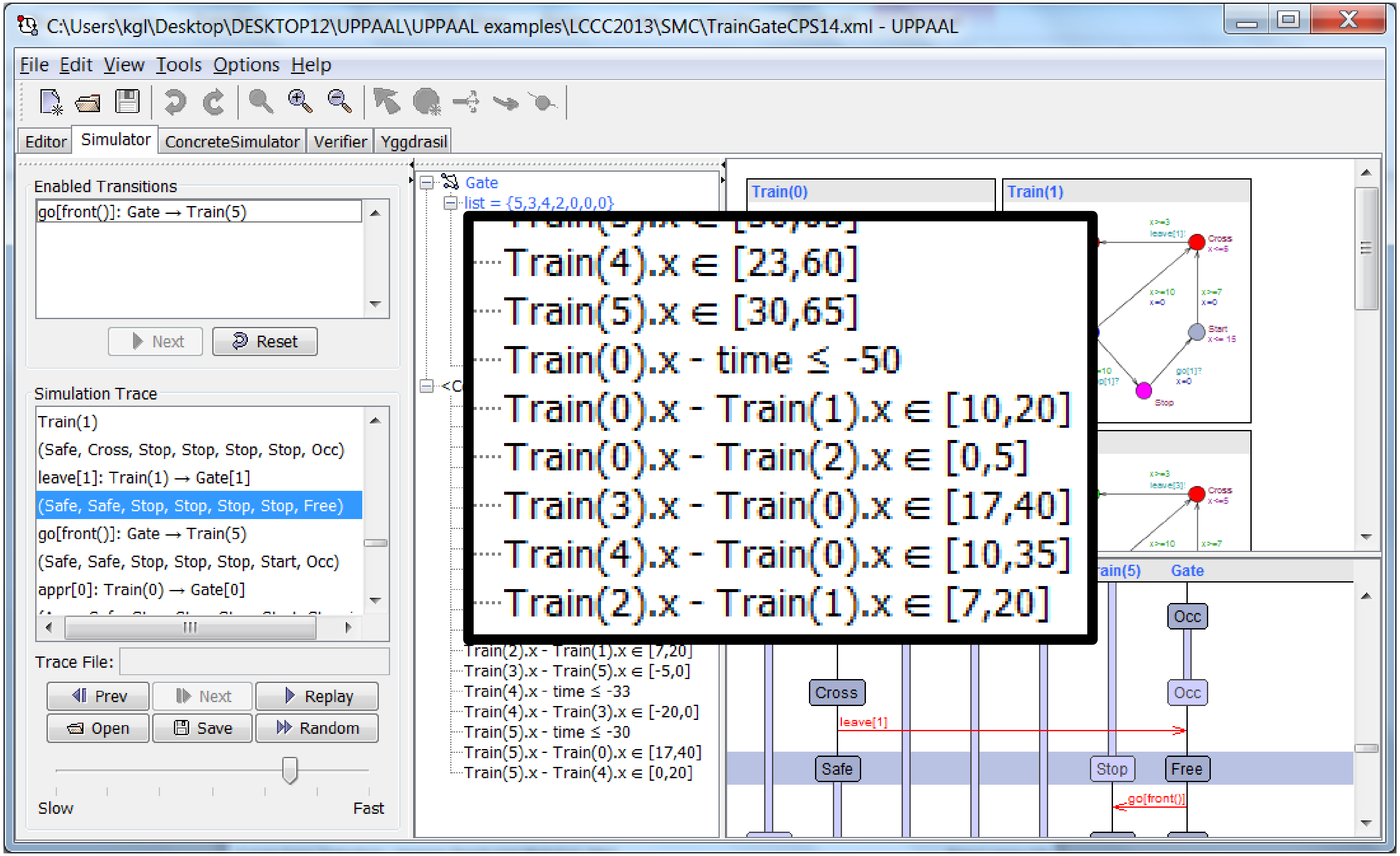


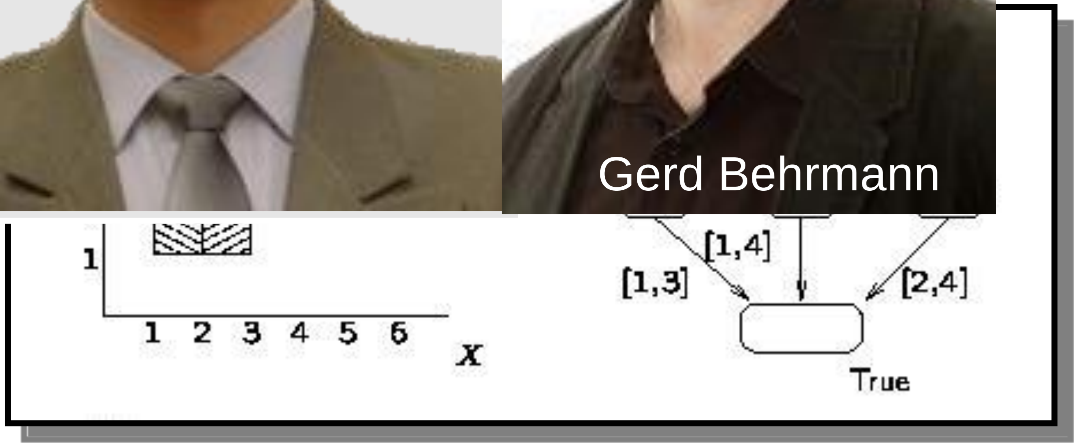
Fig. 4. Model of the transmission of the message bytes.

THE "secret" of UPPAAL



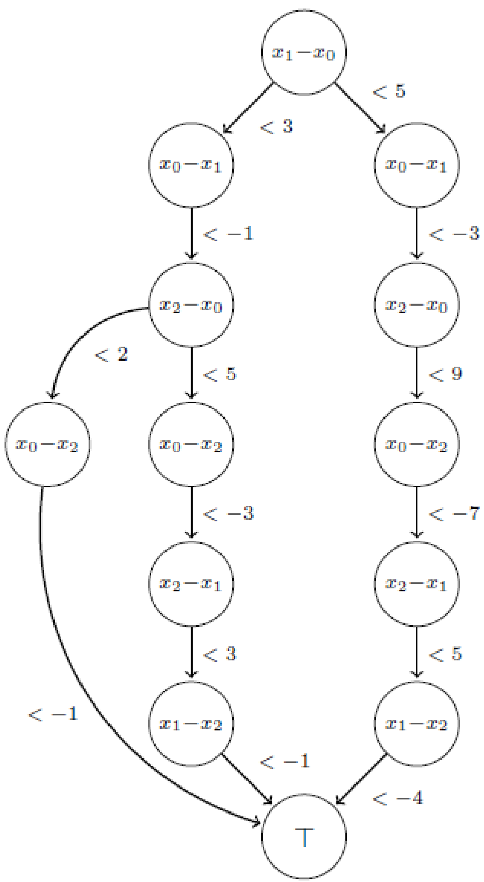
Zones & DBMs
THE "secret" UPPAAL

- DBM package

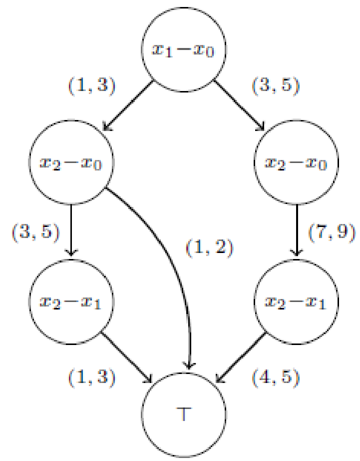


- PW List
  [SPIN03]

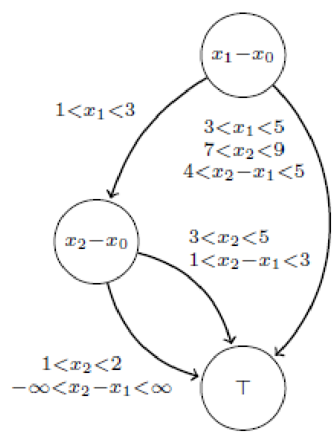
R1: Beyond Timed Automata



(a) CRD



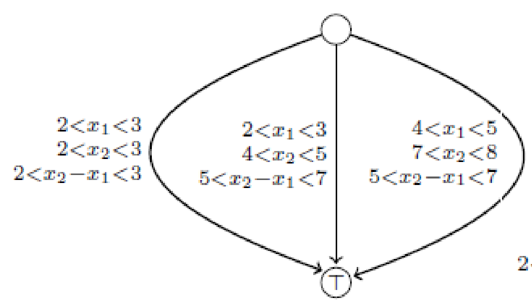
(b) CDD



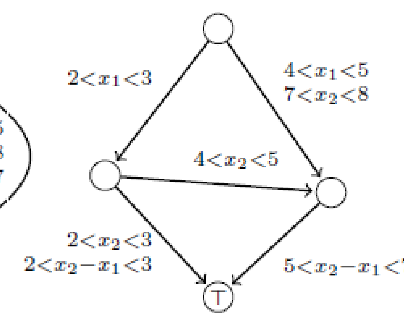
(c) CMD

Rüdiger Ehlers, Daniel Fass, Michael Gerke, Hans-Jörg Peter:

Fully Symbolic Timed Model Checking Using Constraint Matrix Diagrams. RTSS'10



(a) Compact form



(b) Diagram form

Figure 4. Semantically equivalent CMDs.

Performance

		CMD model checker				RED			Uppaal			
Benchmark	Sat	Mode	Steps	Time	Mem	Steps	Time	Mem	Params	States	Time	Mem
GPS 16	No	B/D	49	4	204	49	795	2923	-C	1365519	55	266
GPS 17	No	B/D	52	4	163		MEMOUT		-C -S2	3174448	139	470
GPS 19	No	B/D	58	4	221		MEMOUT		-C -S2	17155714	974	2425
GPS 20	No	B/D	61	5	229		MEMOUT		-S2		MEMOUT	
GPS 22	No	B/D	67	7	284		MEMOUT		-S2		MEMOUT	
GPS 15	Yes	B/D	46	3	146	46	169	1437	-S2	43046719	1612	3640
GPS 16	Yes	B/D	49	4	204	49	820	2923	-S2		MEMOUT	
GPS 17	Yes	B/D	52	4	218		MEMOUT		-S2		MEMOUT	
GPS 22	Yes	B/D	67	6	278		MEMOUT		-S2		MEMOUT	
FlexRay 1	Yes	F/C	987	16	172		MEMOUT		-C -S2	2368799	17	88
FlexRay 33	Yes	F/C	11851	524	577		MEMOUT		-C -S2	182095135	1515	3907
FlexRay 34	Yes	F/C	12191	527	584		MEMOUT		-S2		MEMOUT	
FlexRay 100	Yes	F/C	34599	695	761		MEMOUT		-S2		MEMOUT	
FlexRay 200	Yes	F/C	68551	2599	1299		MEMOUT		-S2		MEMOUT	
FlexRay 262	Yes	F/C	89603	2869	1482		MEMOUT		-S2		MEMOUT	
Fischer 11	No	B/D	6	13	228	6	8540	3472		2525	0	37
Fischer 12	No	B/D	6	28	297		MEMOUT		-C -S2	4521	0	37
Fischer 19	No	B/D	6	2864	3788		MEMOUT		-C	42941	7	130
Fischer 20	No	B/D		MEMOUT			MEMOUT		-C -S2	54341	9	147
Fischer 11	Yes	B/D	13	119	395	5	6693	3470	-C	2730268	112	233
Fischer 12	Yes	B/D	14	308	698		MEMOUT		-C	8936216	450	693
Fischer 13	Yes	B/D	15	1546	1434		MEMOUT		-C	29016288	1789	2262
Fischer 14	Yes	B/D	16	5727	2800		MEMOUT		-S2		MEMOUT	
Fischer 15	Yes	B/D		MEMOUT			MEMOUT		-S2		MEMOUT	
FDDI 40	Yes	B/D	0	63	495	0	72	729	-C	185535	2713	411
FDDI 50	Yes	B/D	0	109	495	0	624	2959	-C		TIMEOUT	
FDDI 75	Yes	B/D	0	360	934		MEMOUT		-C		TIMEOUT	
FDDI 100	Yes	B/D	0	1315	1779		MEMOUT		-S2		TIMEOUT	
Leader 5	No	F/D	30	30	182	30	190	1034		3257	0	37
Leader 6	No	F/D	38	4394	475		MEMOUT		-C -S2	21375	0	37
Leader 7	No	F/D		TIMEOUT			MEMOUT		-C	86645	1	40
Leader 5	Yes	F/D	97	105	209	83	417	1413		7398	0	37
Leader 6	Yes	F/D		TIMEOUT			MEMOUT			42482	1	38
Leader 7	Yes	F/D		TIMEOUT			MEMOUT			227253	4	41

AVACS

German Science Foundation, 1.1.04 – 31.12. 15.

Project Group R Real-Time Systems Coordinator: E. Olderog, CvOU Summary	**Project Group H** Hybrid Systems Coordinator: M. Fränzle Summary	**Project Group S** Coarse Grain System Structure Coordinator: Podelski Summary
R1: Beyond Timed Automata Coordinator: E. Olderog, CvOU Additional PIs: B. Finkbeiner, UdS M. Fränzle, CvOU A. Podel… V. Sofro…	H1/2: Constraint-based Verification for Hybrid Systems Coordinator: M. Fränzle, CvOU Additional PIs: E. Althaus, MPII	S1: Compositional Aproaches to System Verification Coordinator: B. Finkbeiner, UdS Additional PIs: B. Becker, ALU
R2: Timi… Distribut… Coordina… Addition… E. Althau… W. Dam… S. Hack, … J. Reinek…		…ommunication …inator: A. …U …dS …dS … MPII
R3: Heur… Abstract… Coordina…r: B. Nebel, ALU Additional PIs: B. Finkbeiner, UdS A. Podelski, ALU	Coordinator: O. Theel, CvOU Additional PIs: M. Fränzle, CvOU H. Hermanns, UdS A. Podelski, ALU V. Wolf, UdS	…ification of …roperties Coordinator: … Hermanns, UdS Additional PIs: B. Becker, ALU O. Theel, CvOU V. Wolf, UdS

R3: Heuristic Search and Abstract Model Checking

Coordinator: B. Nebel, ALU

Additional PIs:

B. Finkbeiner, UdS

A. Podelski, ALU

R3: Search & Abstraction

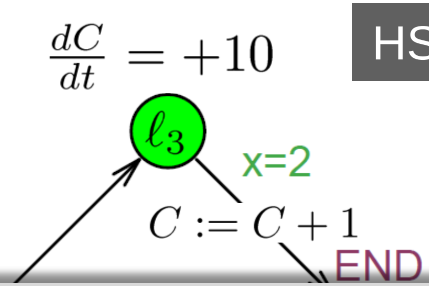
Visiting Aalborg 2001

- H. Dierks. **Heuristic Guided Model-Checking of Real-Time Systems,** NWPT04
- H. Dierks. **Finding Optimal Plans for Domains with Continuous Effects with UPPAAL CORA.** ICAPS05
- K. Larsen: **Optimal and Real-Time Scheduling using UPPAAL.** ICAPS05

Priced Timed Automata

HSCC01, CAV01, TACAS01

Observer variable C:



- [HSCC01,HSCC01]
  Cost-optimal reachability is decidable
  in PSPACE

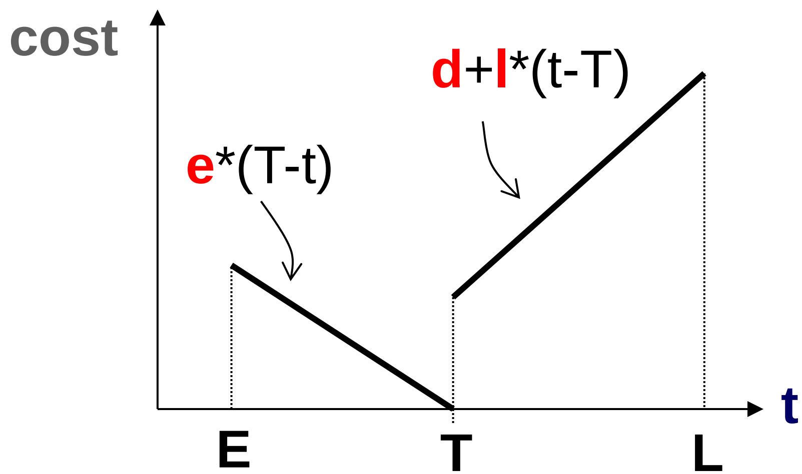
- [CAV01, TACAS01]
  Symbolic A* using Prized zones

$(\ell_0, [0, 0])$ … $\sum C_i = 16.6$

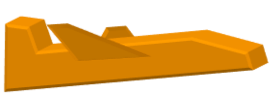
$(\ell_0, [0,0]) \xrightarrow{1.2}_{6.0} (\ell_0, [1.2, 1.2]) \rightarrow_0 (\ell_1, [1.2, 0]) \rightarrow_0$

$(\ell_3, [1.2, 0]) \xrightarrow{0.8}_{8.0} (\ell_3, [2, 0.8]) \rightarrow_1 (\ell_4, [2, 0.8])$ $\sum C_i = 15.0$

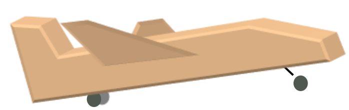
Example: Aircraft Landing

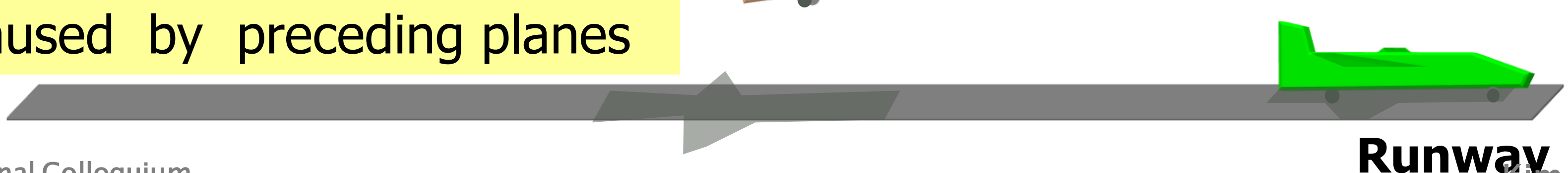


E earliest landing time
T target time
L latest time
e cost rate for being early
l cost rate for being late
d fixed cost for being late

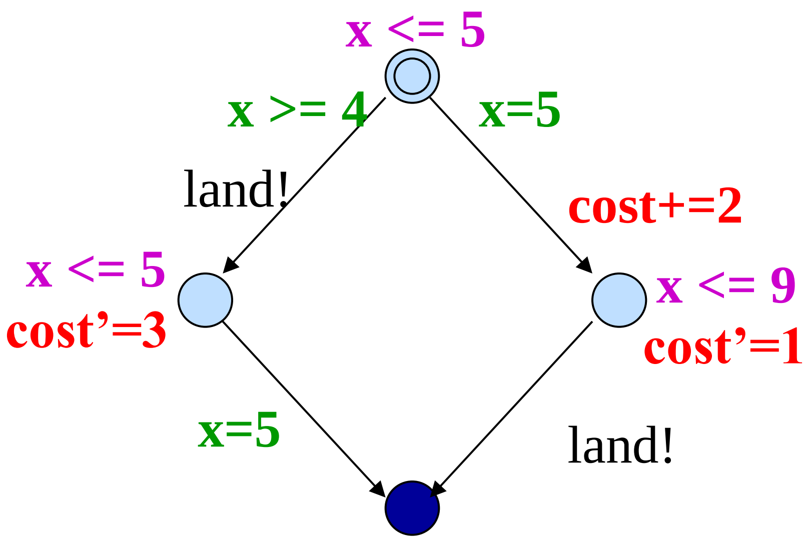


Planes have to keep separation distance to avoid turbulences caused by preceding planes

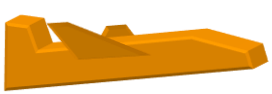




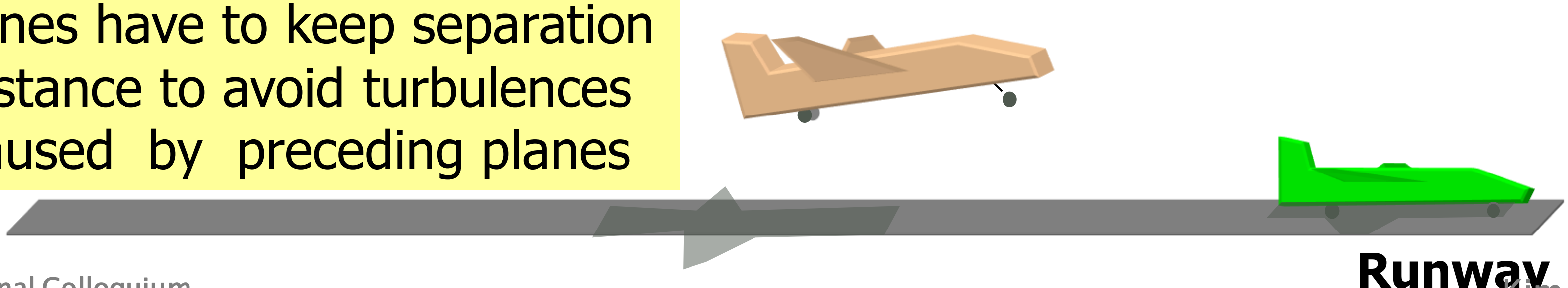
Example: Aircraft Landing



4 earliest landing time
5 target time
9 latest time
3 cost rate for being early
1 cost rate for being late
2 fixed cost for being late



Planes have to keep separation distance to avoid turbulences caused by preceding planes



Aircraft Landing

Source of examples: Baesley et al'2000

	problem instance	1	2	3	4	5	6	7
	number of planes	10	15	20	20	20	30	44
	number of types	2	2	2	2	2	4	2
1	optimal value	700	1480	820	2520	3100	24442	1550
	explored states	481	2149	920	5693	15069	122	662
	cputime (secs)	4.19	25.30	11.05	87.67	220.22	0.60	4.27
2	optimal value	90	210	60	640	650	554	0
	explored states	1218	1797	669	28821	47993	9035	92
	cputime (secs)	17.87	39.92	11.02	755.84	1085.08	123.72	1.06
3	optimal value	0	0	0	130	170	0	N/A
	explored states	24	46	84	207715	189602	62	
	cputime (secs)	0.36	0.70	1.71	14786.19	12461.47	0.68	
4	optimal value	N/A	N/A	N/A	0	0	N/A	N/A
	explored states				65	64		
	cputime (secs)				1.97	1.53		

PDDL3 to UPPAAL Cora

Experimental Results

Translating PDDL$_3$ to PTA

[Dierks VVPS05+]

# planes	# inst	# clocks	costs	time (s)	mem (MB)
3	2	3	0	0.5	5
3	3	4	0	1.9	9
3	4	5	0	9	28
4	2	3	860	0.8	7
4	3	4	860	7.4	29
4	4	5	860	59	168
5	2	3	1540	2.4	16
5	3	4	1540	30	114
5	4	5	out of mem (400MB,97 s)		
6	2	3	180	10.3	56
6	3	4	60	out of mem (96 s)	
6	4	5	out of mem (76 s)		
7	2	3	920	30.8	166
7	3	4	out of mem (66 s)		
8	2	3	1870	out of mem (63 s)	
8	3	4	out of mem (60 s)		
9	2	3	out of mem (55 s)		

UCb

Modeling

```
(define (domai
  (:requiremen
   :conditiona
   :durative-a
  (:types plan
  (:predicates

  (:functions
```

```
(:durative-act
 :duration (<=
 :condition (a

 :effect (and

)
```

UCb

ierks VVPS05]

R3: Search & Abstraction

- Gerd Behrmann, Ed Brinksma, Martijn Hendriks, Angelika Mader: Production Scheduling by Reachability Analysis - A Case Study. IPDPS 2005
- Sebastian Kupferschmid, Jörg Hoffmann, Henning Dierks, and Gerd Behrmann. **Adapting an AI planning heuristic for directed model checking**. SPIN06
- Jürg Hoffmann, Jan-Georg Smaus, Andrey Rybalchenko, Sebastian Kupferschmid, and Andreas Podelski. **Using predicate abstraction to generate heuristic functions in UPPAAL**. MoChArt06
- Sebastian Kupferschmid, Klaus Dräger, Jörg Hoffmann, Bernd Finkbeiner, Henning Dierks, Andreas Podelski, and Gerd Behrmann. **Uppaal/DMC -- abstraction-based heuristics for directed model checking**. TACAS07.

R3: Search & Abstraction

- Henning Dierks,
  Sebastian Kupferschmid, and
  Kim G. Larsen.
  Automatic abstraction refinement for timed automata. FORMATS07
- Sebastian Kupferschmid,
  Martin Wehrle, Bernhard Nebel, a
  nd Andreas Podelski.
  Faster than Uppaal?. CAV2008
- Sebastian Kupferschmid, Jörg Hoffmann, and Kim G. Larsen. **Fast directed model checking via Russian doll abstraction.** TACAS 2008
- **Holger Hermanns, Jan Krcal, Gilles Nies, Marvin Stenger: GOMX 4 – Satelite as a Services. SENSATION 2015**

AVACS

German Science Foundation, 1.1.04 – 31.12. 15.

Project Group R Real-Time Systems Coordinator: E. Olderog, CvOU Summary	**Project Group H** Hybrid Systems Coordinator: M. Fränzle Summary	**Project Group S** Coarse Grain System Structure Coordinator: Podelski Summary
R1: Beyond Timed Automata Coordinator: E. Olderog, CvOU Additional PIs: B. Finkbeiner, UdS M. Fränzle, CvOU A. Podelski, ALU V. Sofronie- Stokker	H1/2: Constraint-based Verification for Hybrid Systems	S1: Compositional Aproaches to System Verification iner, UdS
R2: Timing Analysis Distribution of Real- Coordinator: Wilhelm Additional PIs: E. Althaus, MPII W. Damm, CvOU S. Hack, UdS J. Reineke, UdS		ication A.
R3: Heuristic Search Abstract Model Checking Coordinator: B. Nebel, ALU Additional PIs: B. Finkbeiner, UdS A. Podelski, ALU	Hybrid System Stability Coordinator: O. Theel, CvOU Additional PIs: M. Fränzle, CvOU H. Hermanns, UdS A. Podelski, ALU V. Wolf, UdS	of Dependability Properties Coordinator: H. Hermanns, UdS Additional PIs: B. Becker, ALU O. Theel, CvOU V. Wolf, UdS

R2: Timing Analysis and Distribution of Real-Time Tasks

Coordinator: Wilhelm, UdS

Additional PIs:

E. Althaus, MPII

W. Damm, CvOU

S. Hack, UdS

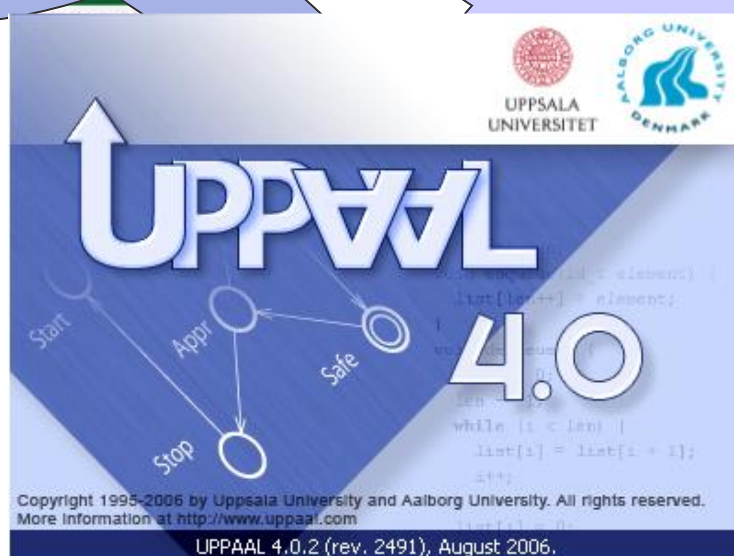
J. Reineke, UdS

R2: Real-Time Tasks

Abstract Interpretation is

Why AI + ILP Is Good for WCET, but MC Is Not, Nor ILP Alone! (CAV03)

Why Model Checking Can Improve WCET Analysis (CAV04)
Alexander Metzner



Herschel-Planck Scientific Mission at ESA


Attitude and Orbit Control Software
TERMA A/S Steen Ulrik Palm, Jan Storbank Pedersen, Poul Hougaard

Blocking & WCRT

ID	Task	Specification			Blocking times			WCRT		
		Period	WCET	Deadline	Terma	UPPAAL	Diff	Terma	UPPAAL	Diff
1	RTEMS_RTC	10.000	0.013	1.000	0.035	0	0.035	0.050	0.013	0.037
2	AswSync_SyncPulseIsr	250.000	0.070	1.000	0.035	0	0.035	0.120	0.083	0.037
3	Hk_SamplerIsr	125.000	0.070	1.000	0.035	0	0.035	0.120	0.070	0.050
4	SwCyc_CycStartIsr	250.000	0.200	1.000	0.035	0	0.035	0.320	0.103	0.217
5	SwCyc_CycEndIsr	250.000	0.100	1.000	0.035	0	0.035	0.220	0.113	0.107
6	Rt1553_Isr	15.625	0.070	1.000	0.035	0	0.035	0.290	0.173	0.117
7	Bc1553_Isr	20.000	0.070	1.000	0.035	0	0.035	0.360	0.243	0.117
8	Spw_Isr	39.000	0.070	2.000	0.035	0	0.035	0.430	0.313	0.117
9	Obdh_Isr	250.000	0.070	2.000	0.035	0	0.035	0.500	0.383	0.117
10	RtSdb_P_1	15.625	0.150	15.625	3.650	0	3.650	4.330	0.533	3.797
11	RtSdb_P_2	125.000	0.400	15.625	3.650	0	3.650	4.870	0.933	3.937
12	RtSdb_P_3	250.000	0.170	15.625	3.650	0	3.650	5.110	1.103	4.007
14	**FdirEvents**	250.000	5.000	230.220	0.720	0	0.720	7.180	5.153	2.027
15	**NominalEvents_1**	250.000	0.720	230.220	0.720	0	0.720	7.900	5.873	2.027
16	**MainCycle**	250.000	0.400	230.220	0.720	0	0.720	8.370	6.273	2.097
17	HkSampler_P_2	125.000	0.500	62.500	3.650	0	3.650	11.960	5.380	6.580
18	HkSampler_P_1	250.000	6.000	62.500	3.650	0	3.650	18.460	11.615	6.845
19	Acb_P	250.000	6.000	50.000	3.650	0	3.650	24.680	6.473	18.207
20	IoCyc_P	250.000	3.000	50.000	3.650	0	3.650	27.820	9.473	18.347
21	**PrimaryF**	250.000	34.050	59.600	5.770	0.966	4.804	65.470	54.115	11.355
22	**RCSControlF**	250.000	4.070	239.600	12.120	0	12.120	76.040	53.994	22.046
23	Obt_P	1000.000	1.100	100.000	9.630	0	9.630	74.720	2.503	72.217
24	Hk_P	250.000	2.750	250.000	1.035	0	1.035	6.800	4.953	1.847
25	StsMon_P	250.000	3.300	125.000	16.070	0.822	15.248	85.050	17.863	67.187
26	TmGen_P	250.000	4.860	250.000	4.260	0	4.260	77.650	9.813	67.837
27	Sgm_P	250.000	4.020	250.000	1.040	0	1.040	18.680	14.796	3.884
28	TcRouter_P	250.000	0.500	250.000	1.035	0	1.035	19.310	11.896	7.414
29	Cmd_P	250.000	14.000	250.000	26.110	1.262	24.848	114.920	94.346	20.574
30	**NominalEvents_2**	250.000	1.780	230.220	12.480	0	12.480	102.760	65.177	37.583
31	**SecondaryF_1**	250.000	20.960	189.600	27.650	0	27.650	141.550	110.666	30.884
32	**SecondaryF_2**	250.000	39.690	230.220	48.450	0	48.450	204.050	154.556	49.494
33	Bkgnd_P	250.000	0.200	250.000	0.000	0	0.000	154.090	15.046	139.044

Marius Micusionis

TERMA Case Follow-Up

ISOLA 2012

[f*WCET, WCET]

limit	f=100%			f=95%		
	states	mem	time	states	mem	ti[illegible]
1	1300	51.2	1.47	485077	[illegible]	[illegible]
2	2522	53.7	2.45	80691[illegible]	[illegible]	[illegible]
4	4981	54.5	4.62	1499700	[illegible]	[illegible].8
8	[illegible]	[illegible]	[illegible]			
16	[illegible]	[illegible]	[illegible]			
∞	1[illegible]	[illegible]	[illegible]			

1 Day

6 Days

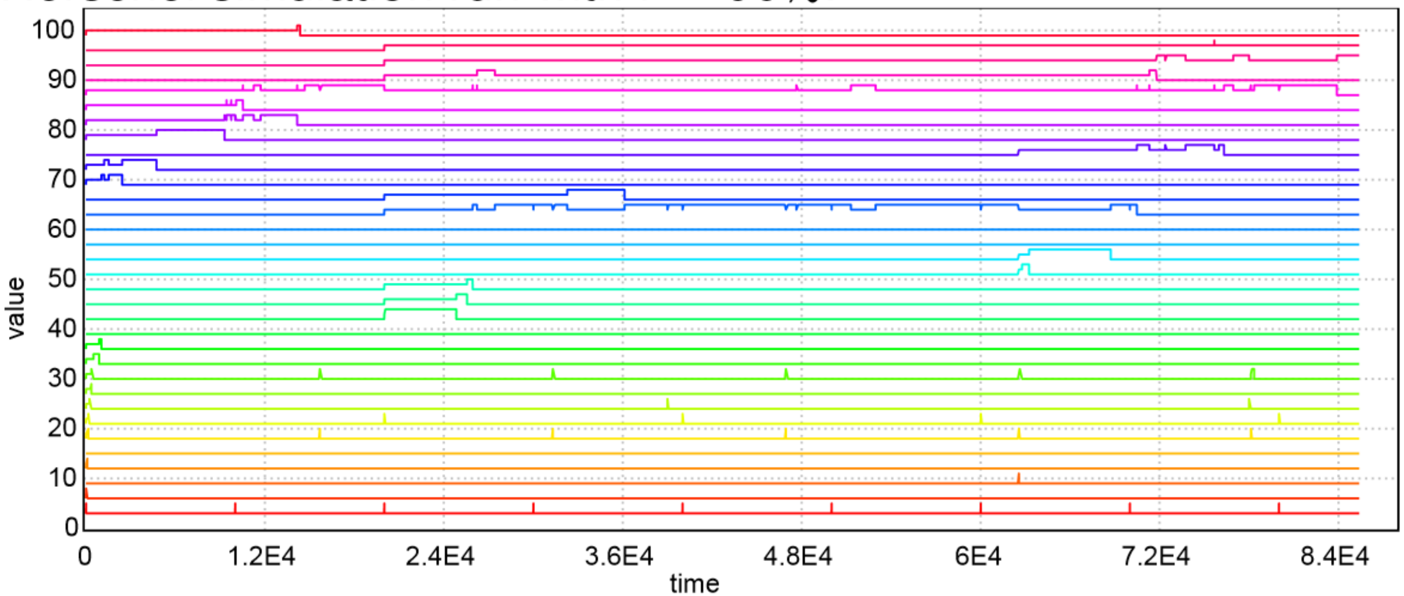
f=90%			f=86%		
states	mem	time, s	states	mem	time
1481162	124.1	4962.[illegible]	3348246	186.9	23986.5
2414679	139.7	7755.[illegible]	5253778	198.7	33299.2
4421630	138.3	13720.[illegible]	9231399	274.6	51176.6
9093562	156.5	3112[illegible].3	18240030	364.6	102932.4
17798572	176.0	601[illegible]4.5	35432003	520.4	158816.7
181869652	1682.2	530604.9	error may be reachable		

TERMA Case – Statistical MC

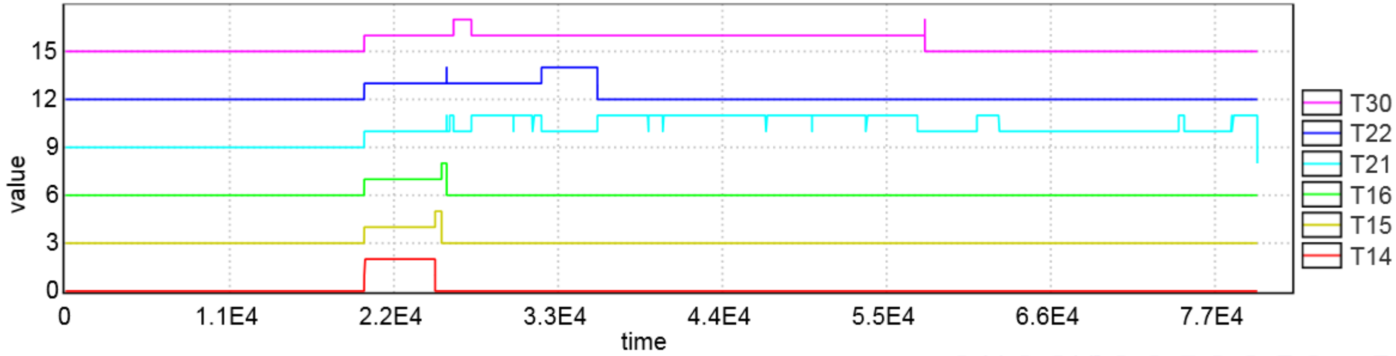
Limit cycles	f %	α	ε	Total traces, #	Error traces #	Error traces Probability	Earliest Error cycle	Earliest Error offset	Verification time
1	0	0.0100	0.005	105967	1928	0.018194	0	79600.0	1:58:06
1	50	0.0100	0.005	105967	753	0.007106	0	79600.0	2:00:52
1	60	0.0100	0.005	105967	13	0.000123	0	79778.3	2:01:18
1	62	0.0005	0.002	1036757	34	0.000033	0	79616.4	19:52:22
160	63	0.0100	0.05	1060	177	0.166981	0	81531.6	2:47:03
160	64	0.0100	0.05	1060	118	0.111321	1	79803.0	2:55:13
160	65	0.0500	0.05	738	57	0.077236	3	79648.0	2:06:55
160	66	0.0100	0.05	1060	60	0.056604	2	82504.0	2:62:44
160	67	0.0100	0.05	1060	26	0.024528	1	79789.0	2:64:20
160	68	0.0100	0.05	1060	3	0.002830	67	81000.0	2:67:08
640	69	0.0100	0.05	1060	8	0.007547	114	80000.0	12:23:00
640	70	0.0100	0.05	1060	3	0.002830	6	88070.0	12:30:49
1280	71	0.0100	0.05	1060	2	0.001887	458	80000.0	25:19:35

TERMA Case – Conclusion

Herschel simulation run with $f = 90\%$:



Herschel deadline violation with $f = 50\%$:



R2: Real-Time Tasks

What is a Timing Anomaly?	2012	WCET 2012	Hansen, Rene Rydhof; Olesen, Mads Chr.
Schedulability Ar Abstractions for Java			
Schedulability of Revisited Using Checking			

Battery-Aware Scheduling of Mixed Criticality Systems	2014	IsoLA 2014	Wognsen, Erik Ramsgaard; Hansen, Rene Rydhof; Larsen, Kim Guldstrand.
Compositional Schedulability Analysis of An Avionics System Using UPPAAL	2014	ICAASE 2014	Boudjadar, Jalil; Larsen, Kim Guldstrand; Kim, Jin Hyun; Nyman, Ulrik.
Degree of Schedulab Criticality Real-time S Probabilistic Sporadi			
Hierarchical Schedul Based on Compositio Uppaal.			
Schedulability and E Multi-core Hierarchic Systems			
Schedulability of Her using statistical mode			
Model Checking Pro Communicating Reso time Systems.			

Adaptive Task Automata with Earliest-Deadline-First Scheduling	2015	AVOCS 2015	David, Alexandre; Hatvani, Leo; Pettersson, Paul; Seceleanu, Cristina.
Flexible Framework for Statistical Schedulability Analysis of Probabilistic Sporadic Tasks	2015	ISORC 2015	Boudjadar, Jalil; David, Alexandre; Kim, Jin Hyun; Larsen, Kim Guldstrand; Mikucionis, Marius; Nyman, Ulrik; Skou, Arne; Lee, Insup; Thi Xuan Phan, Linh
Quantitative Schedulability Analysis of Continuous Probability Tasks in a Hierarchical Context	2015	CBSE'15	Boudjadar, Jalil; David, Alexandre; Kim, Jin Hyun; Larsen, Kim Guldstrand; Mikucionis, Marius; Nyman, Ulrik; Skou, Arne; Lee, Insup; Thi Xuan Phan, Linh.
Widening the Schedulability Hierarchical Scheduling Systems	2015	FACS'14	Boudjadar, Jalil; David, Alexandre; Kim, Jin Hyun; Larsen, Kim Guldstrand; Nyman, Ulrik; Mikučionis, Marius; Skou, Arne.

AVACS

German Science Foundation, 1.1.04 – 31.12. 15.

Project Group R Real-Time Systems Coordinator: E. Olderog, CvOU Summary	**Project Group H** Hybrid Systems Coordinator: M. Fränzle Summary	**Project Group S** Coarse Grain System Structure Coordinator: Podelski Summary
R1: Beyond Tim… Coordinator: E. … Additional PIs: B. Finkbeiner, U… M. Fränzle, CvO… A. Podelski, ALU… V. Sofronie- Sto…	H1/2: Constraint-based … Verification for Hybrid Systems	S1: Compositional Approaches to System Verification
R2: Timing Anal… Distribution of R… Coordinator: Wil… Additional PIs: E. Althaus, MPII W. Damm, CvOU S. Hack, UdS J. Reineke, UdS	… E. Althaus, MPII E. Olderog, CvOU C. Scholl, ALU Sofronie-Stokkermanns, MPII U. Waldmann, MPII	… W. Damm, CvOU B. Finkbeiner, UdS H. Hermanns, UdS J: Reineke, UdS C. Weidenbach, MPII
R3: Heuristic Search and Abstract Model Checking Coordinator: B. Nebel, ALU Additional PIs: B. Finkbeiner, UdS A. Podelski, ALU	H4: Automatic Verification of Hybrid System Stability Coordinator: O. Theel, CvOU Additional PIs: M. Fränzle, CvOU H. Hermanns, UdS A. Podelski, ALU V. Wolf, UdS	S3: Formal Verification of Dependability Properties Coordinator: H. Hermanns, UdS Additional PIs: B. Becker, ALU O. Theel, CvOU V. Wolf, UdS

Project Group H

Hybrid Systems

Coordinator: M. Fränzle

Summary

H: Hybrid Systems

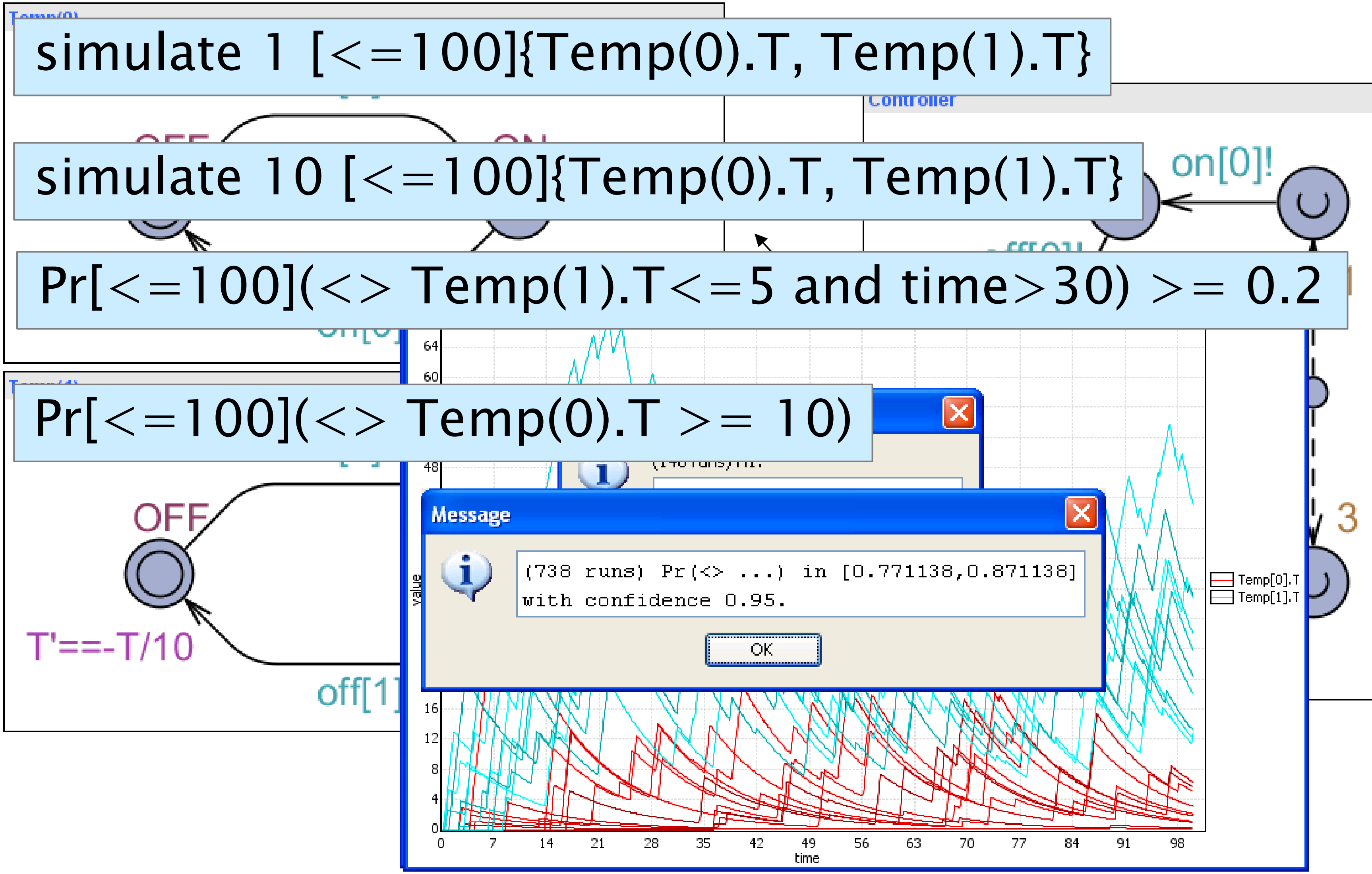
Statistical MC,Stochastic HS

simulate 1 [<=100]{Temp(0).T, Temp(1).T}

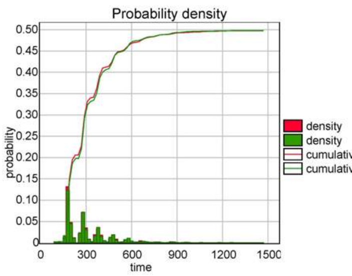
simulate 10 [<=100]{Temp(0).T, Temp(1).T}

Pr[<=100](<> Temp(1).T<=5 and time>30) >= 0.2

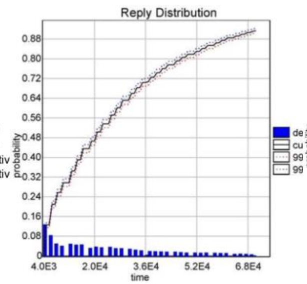
Pr[<=100](<> Temp(0).T >= 10)



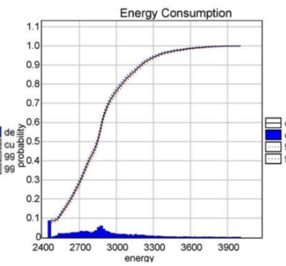
H: Hybrid Systems
Other Case Studies

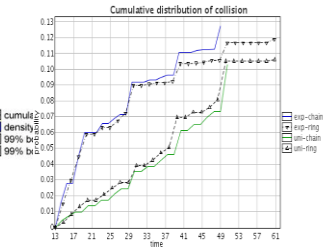


FIREWIRE

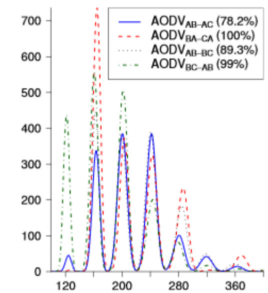


BLUETOOTH

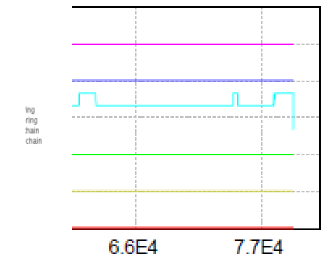




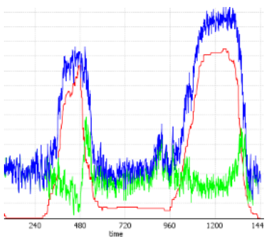
10 node LMAC



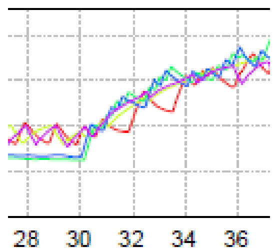
AODV & DYMO



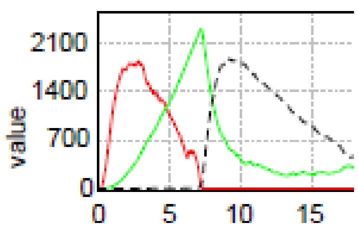
Schedulability Analysis for Mix Cr Sys



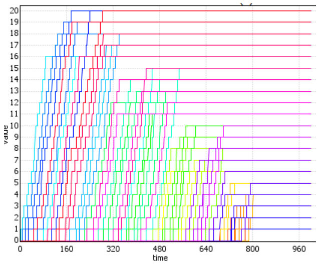
Smart Grid Demand / Response



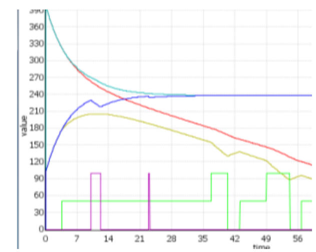
Energy Aware Buildings



Genetic Oscilator (HBS)



Passenger Seating in Aircraft



Battery Scheduling

H3: Automated Verification of Cooperating Traffic Agents
Coordinator: W. Damm, CvOU
Additional PIs:
E. Althaus, MPII
E. Olderog, CvOU
C. Scholl, ALU
Sofronie-Stokkermanns, MPII
U. Waldmann, MPII

04 – 31.12. 15.

...t Group H
...ems
...: M. Fränzle

Project Group S
Coarse Grain System Structure
Coordinator: Podelski
Summary

...traint-based ... for Hybrid Systems
...: M. Fränzle, CvOU
...Is:
...MPII
...LU
..., MPII
...ch, MPII
Associated PIs:
S. Ratschan, ASCR

S1: Compositional Aproaches to System Verification
Coordinator: B. Finkbeiner, UdS

S1: Compositional Aproaches to System Verification
Coordinator: B. Finkbeiner, UdS
Additional PIs:
B. Becker, ALU
B. Nebel, ALU
C. Scholl, ALU

R2: Timing Analysis and Distribution of Real-Time Tasks
Coordinator: Wilhelm, UdS
Additional PIs:
E. Althaus, MPII
W. Damm, CvOU
S. Hack, UdS
J. Reineke, UdS

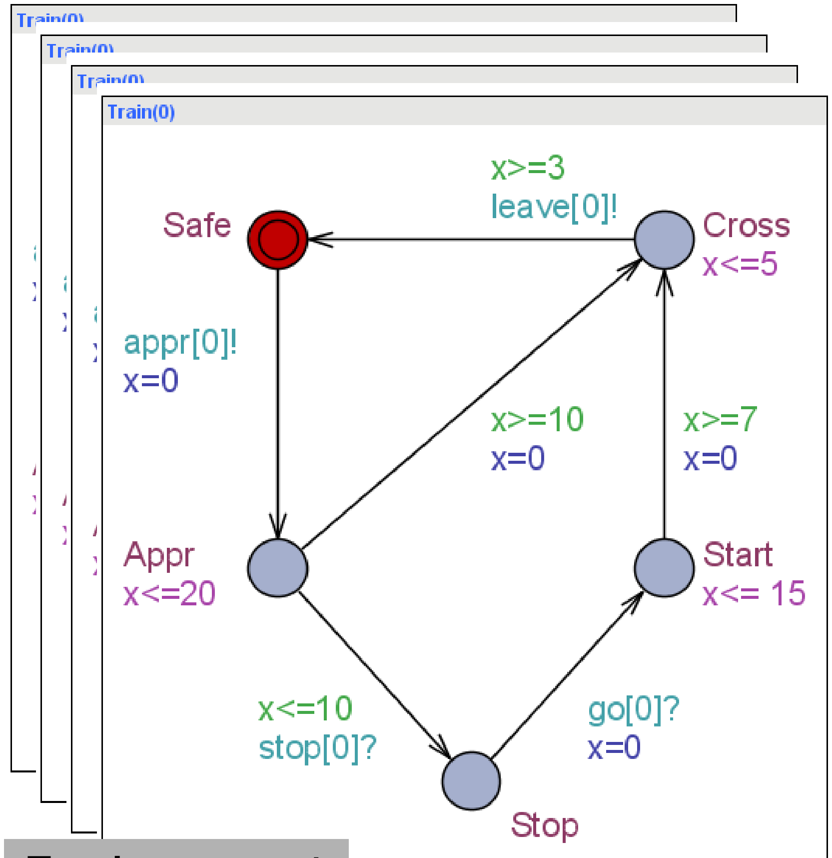
H3: Automated Verificat... Cooperating Traffic Agen...
Coordinator: W. Damm, ...
Additional PIs:
E. Althaus, MPII
E. Olderog, CvOU
C. Scholl, ALU
Sofronie-Stokkermanns, ...
U. Waldmann, MPII

R3: Heuristic Search and Abstract Model Checking
Coordinator: B. Nebel, ALU
Additional PIs:
B. Finkbeiner, UdS
A. Podelski, ALU

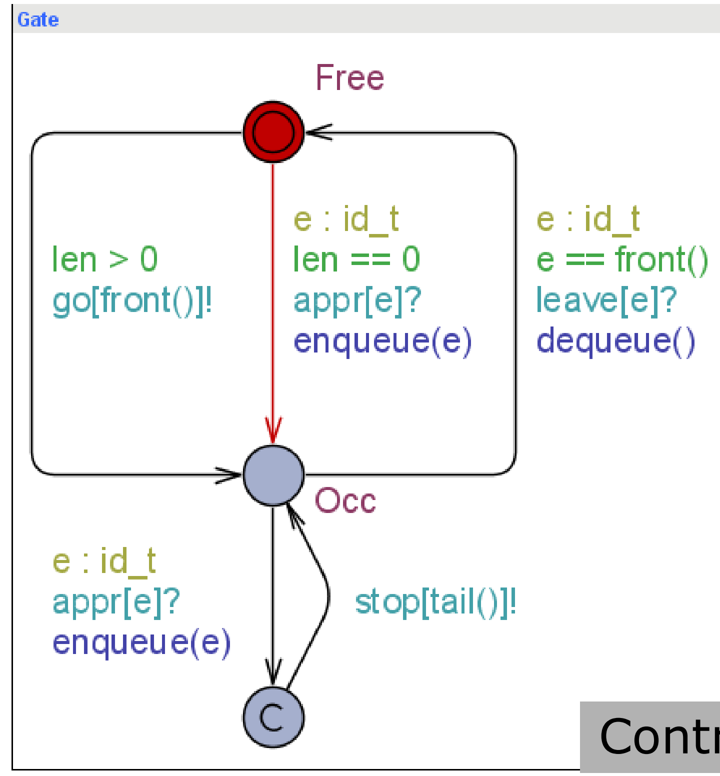
H4: Automatic Verificati... Hybrid System Stability
Coordinator: O. Theel, C...
Additional PIs:
M. Fränzle, CvOU
H. Hermanns, UdS
A. Podelski, ALU
V. Wolf, UdS

Additional PIs:
B. Becker, ALU
O. Theel, CvOU
V. Wolf, UdS

S1 / H3: Compositional Games



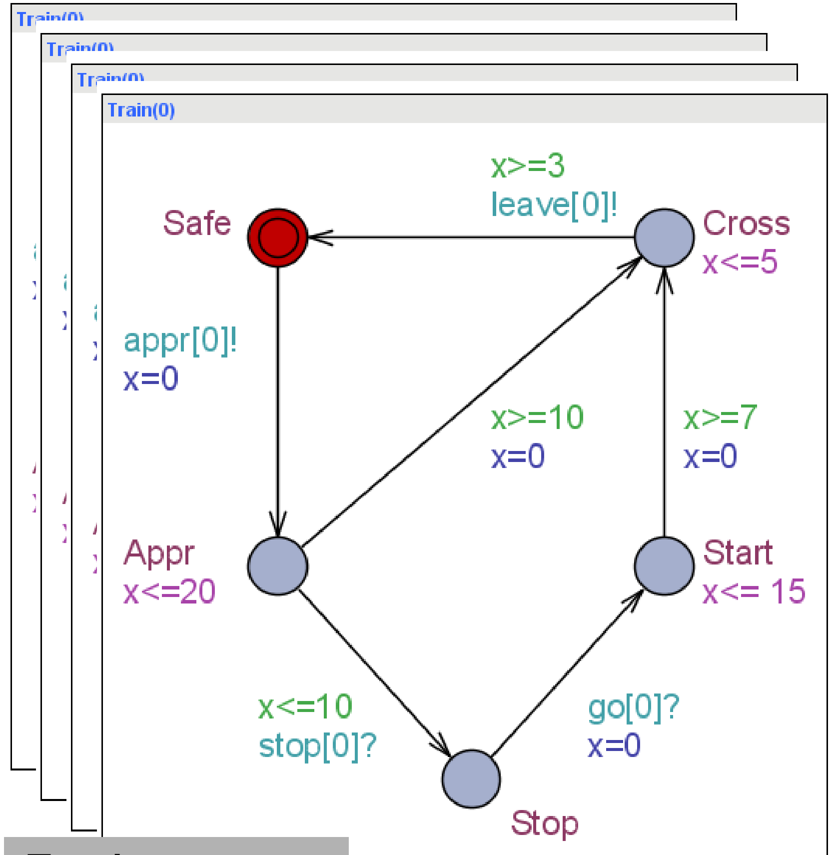
Environment



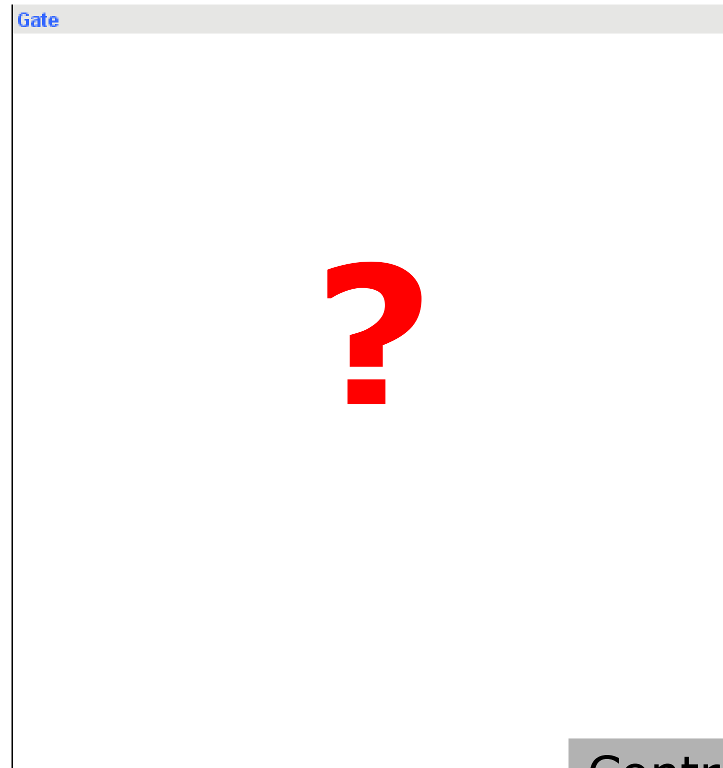
Controller

ϕ: Never two trains at the crossing at the same time

S1/ H3: Compositional Games



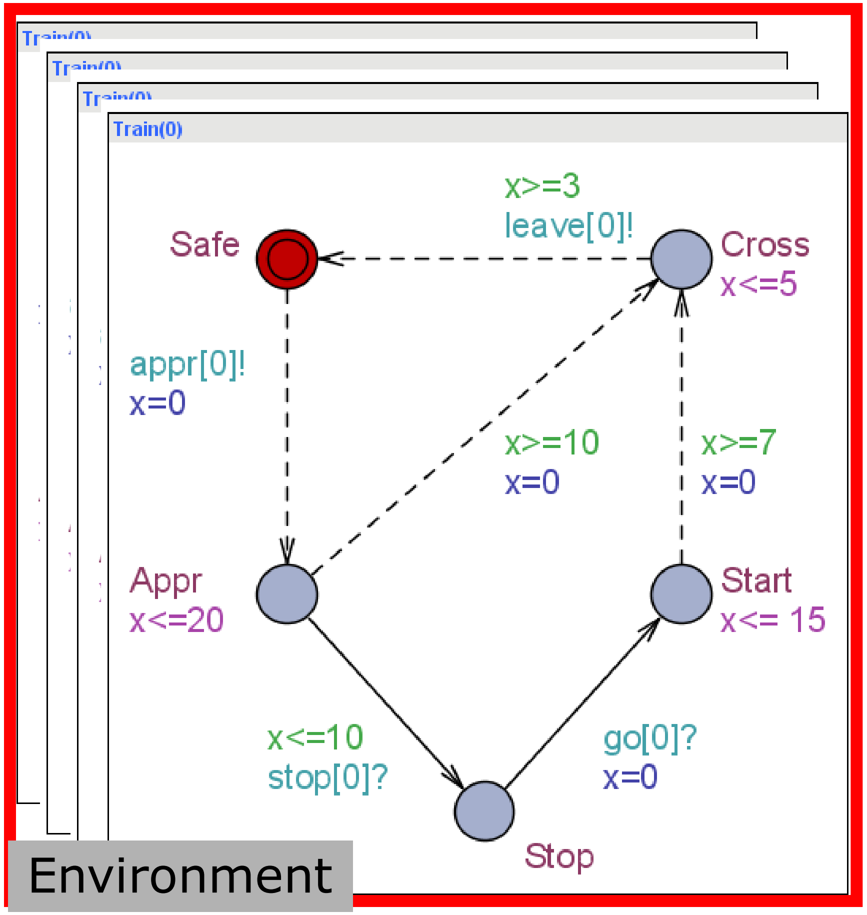
Environment

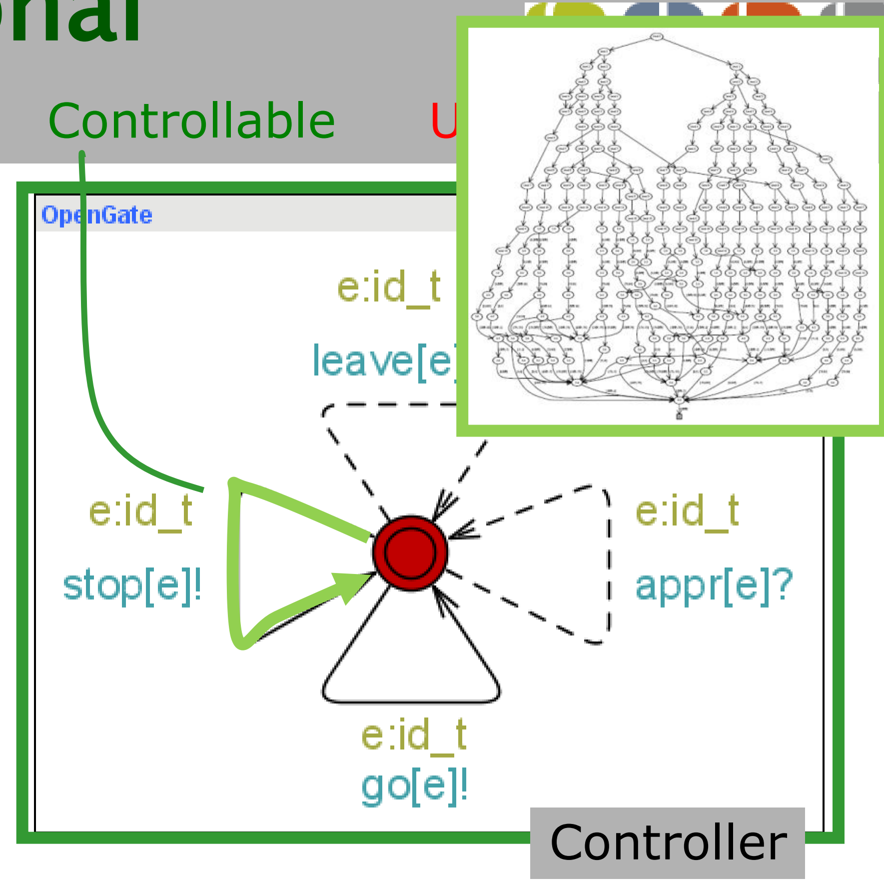


Controller

ϕ: Never two trains at the crossing at the same time

S1 / H3: Compositional Games



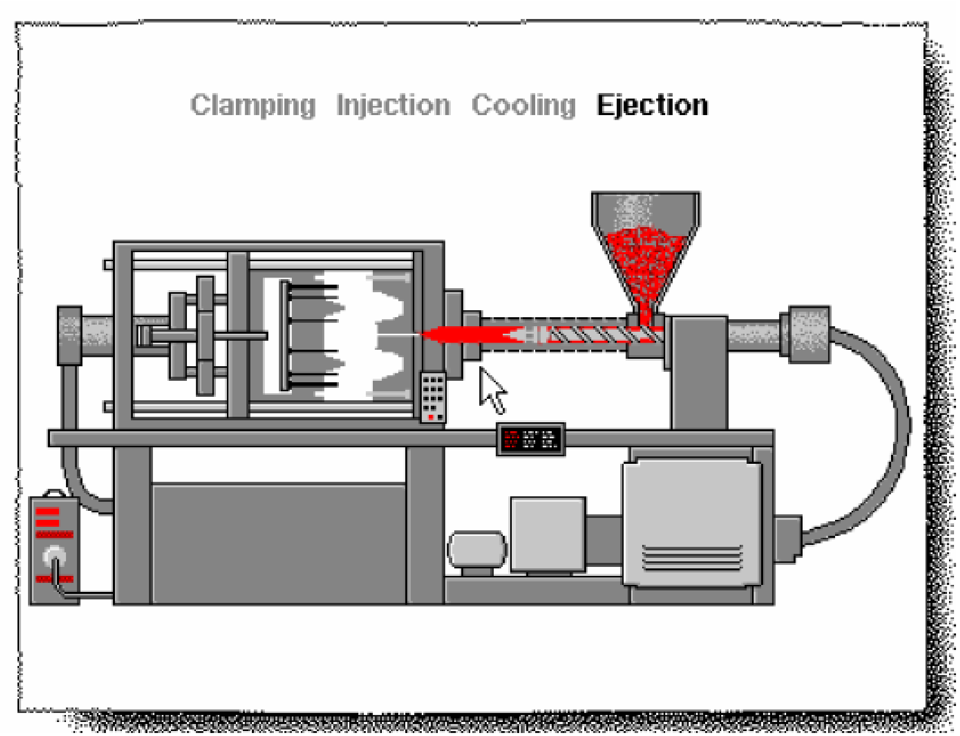


Find strategy for controllable actions st behaviour satisfies ϕ

ϕ: Never two trains at the crossing at the same time

S1 / H3: Compositional Games

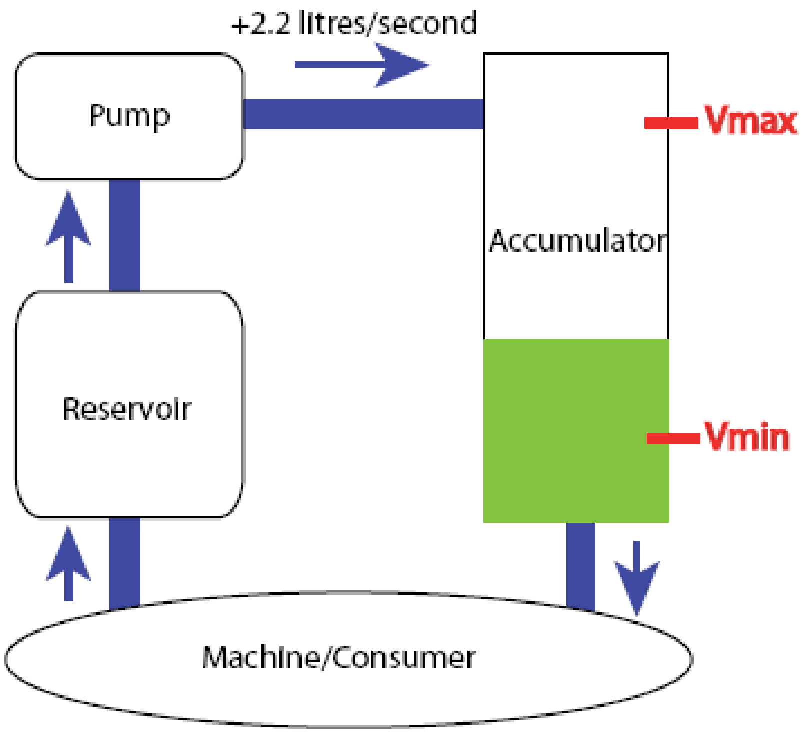
[CJL+09]



HYDAC

- Robust and optimal control
- Tool Chain
  - Synthesis: UPPAAL TIGA
  - Verification: PHAVer
  - Performance: SIMULINK
- 40% improvement of existing solutions..

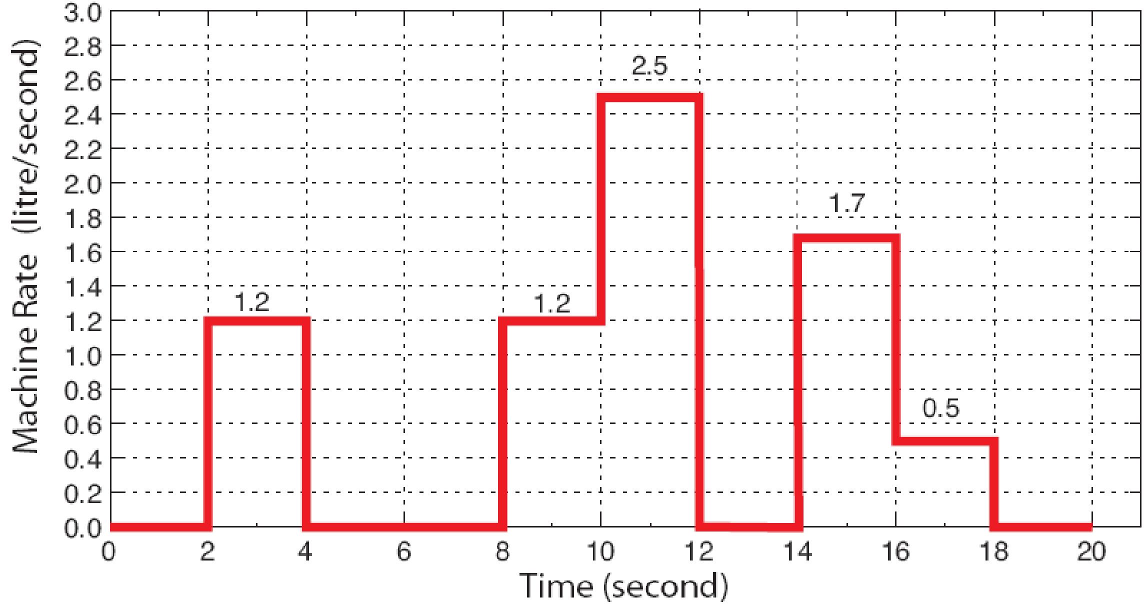
S1/ H3: Compositional Games



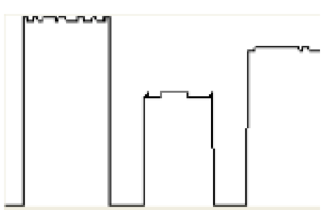
- R1: stay within safe interval [4.9,25.1]
- R2: minimize average/overall oil volume

$$\int_{t=0}^{t=T} v(t)dt \,/\, T$$

S1/ H3: Compositional
Games

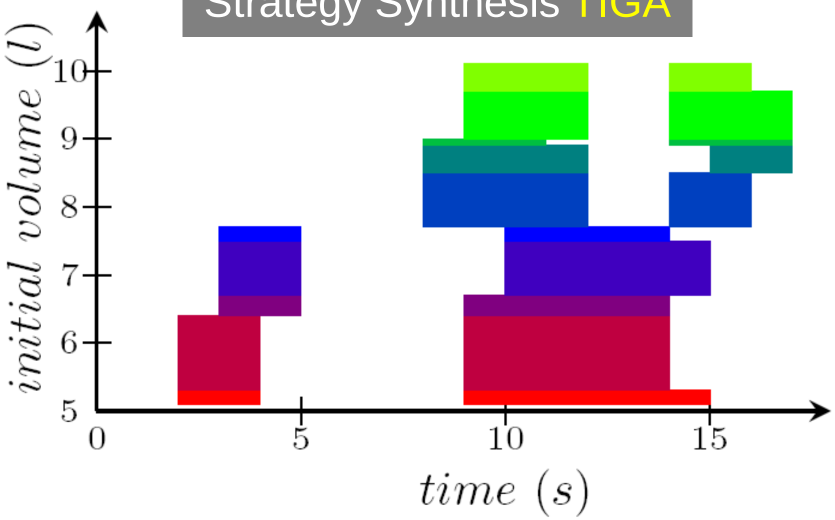


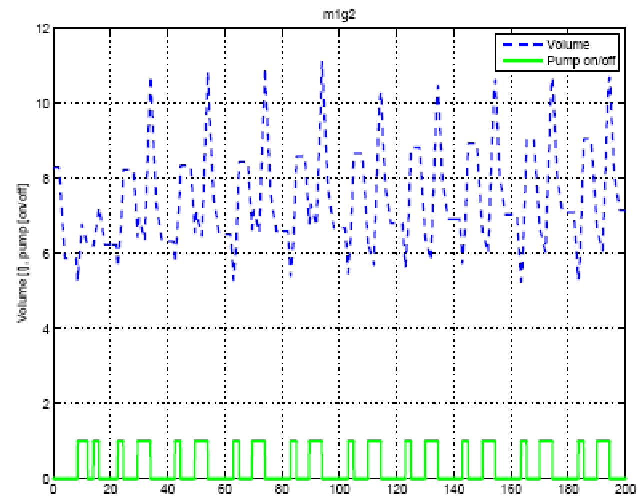
- Infinite cyclic demand to be satisfied by our control strategy.
- P: latency 2 s between state change of pump
- F: noise 0.1 l/s



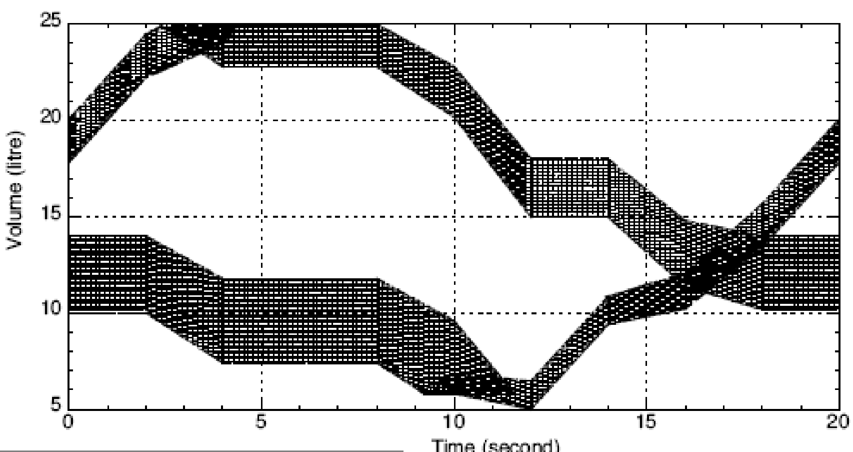
S1/ H3: Compositional Games

Strategy Synthesis TIGA





Performance Evaluation SIMULINK



Verification PHAVER

Guaranteed
Correctness
Robustness

with
40% Improvement

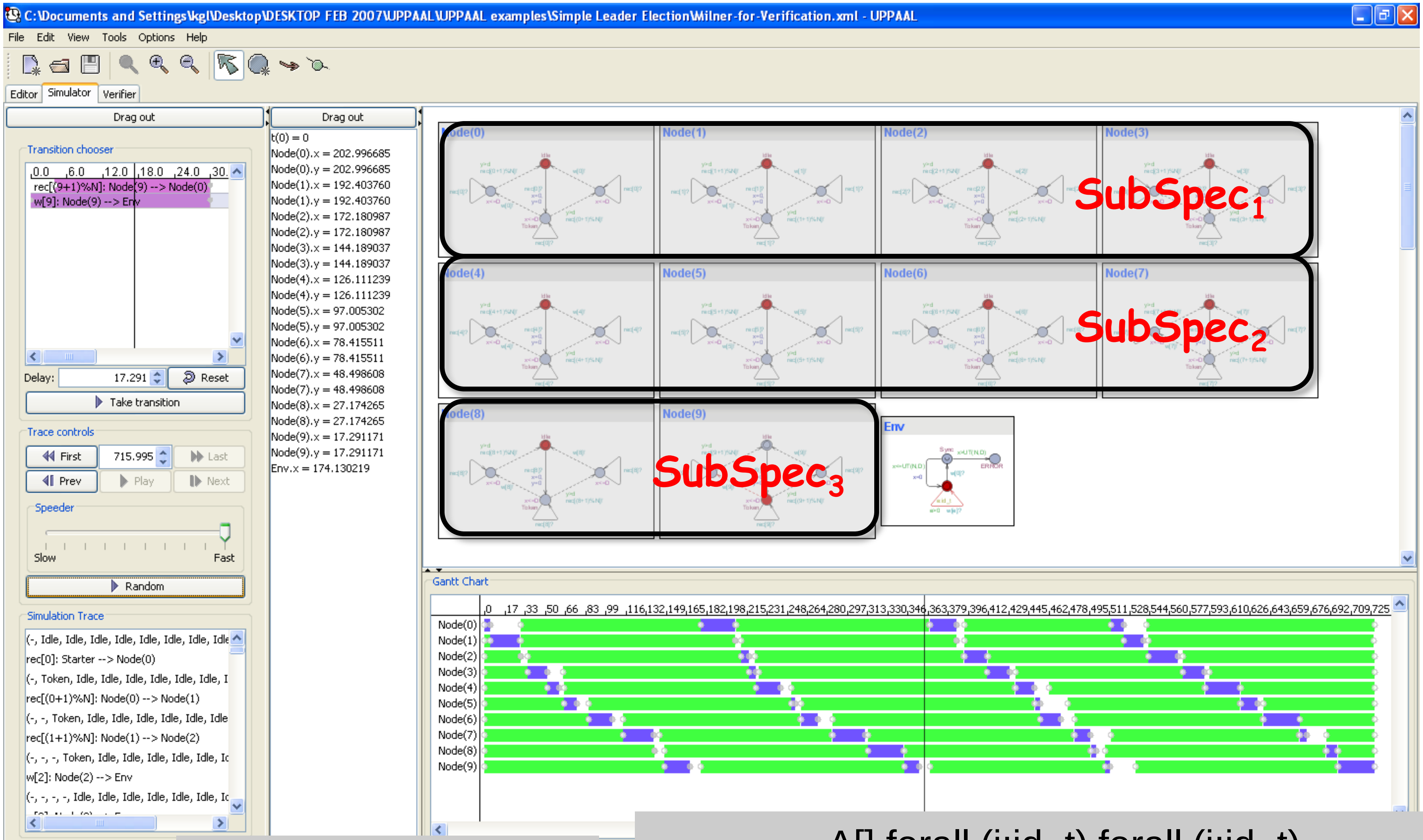
S1/ H3: Compositional
Games

- Hans-Jörg Peter, Robert Mattmüller: **Component-Based Abstraction Refinement for Timed Controller Synthesis.** RTSS 2009: 364-374
- Rüdiger Ehlers, Robert Mattmüller, Hans-Jörg Peter: **Combining Symbolic Representations for Solving Timed Games.** FORMATS 2010: 107-121
- Hans-Jörg Peter, Rüdiger Ehlers, Robert Mattmüller: **Synthia: Verification and Synthesis for Timed Automata.** CAV 2011: 649-655
- Bernd Finkbeiner, Hans-Jörg Peter: Template-Based **Controller Synthesis for Timed Systems.** TACAS 2012: 392-406
- Hans-Jörg Peter, Bernd Finkbeiner: **The Complexity of Bounded Synthesis for Timed Control with Partial Observability.** FORMATS 2012: 204-219

S1 / H3: Compositional

Compositional Verification

ECDAR



A[] not Env.ERROR

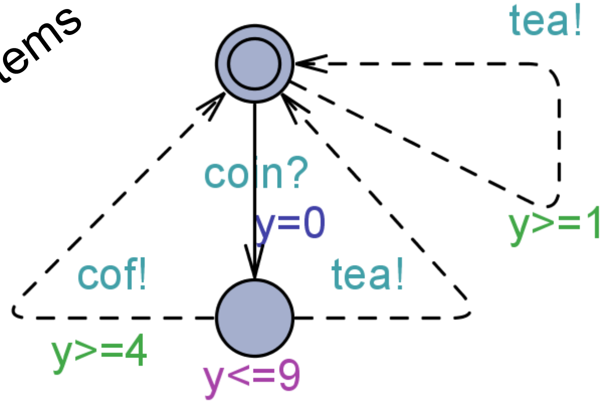
A[] forall (i:id_t) forall (j:id_t)
(Node(i).Token and Node(j).Token imply i==j)

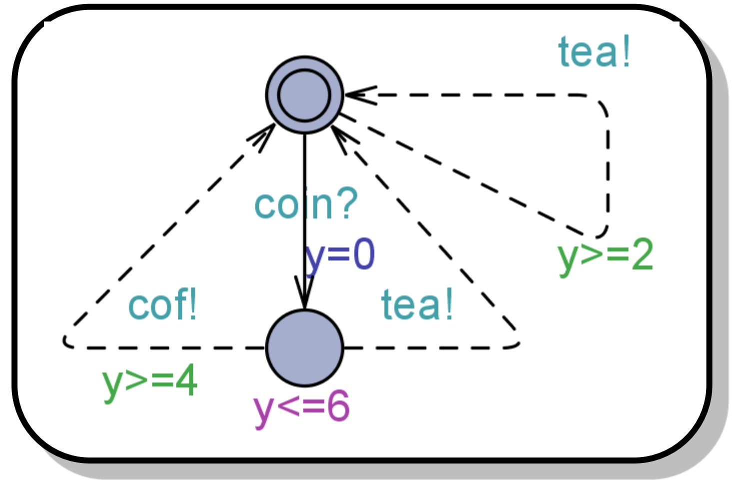
S1/ H3: Compositional

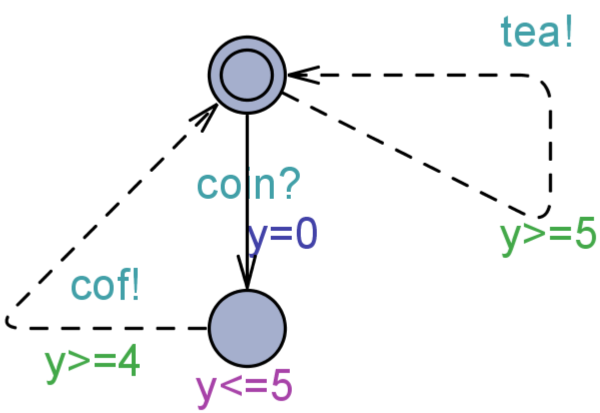
Compositional Verification

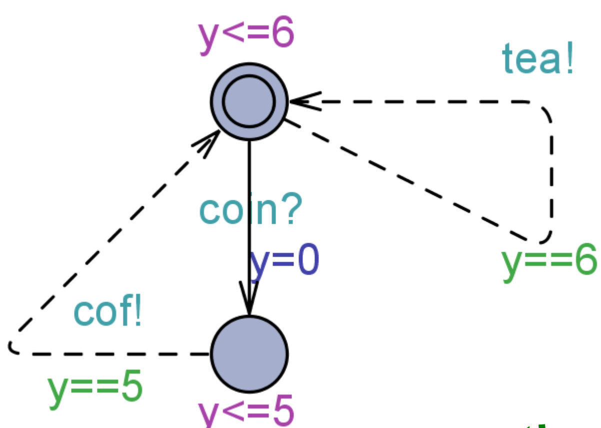
ECDAR

Timed Modal Transition Systems

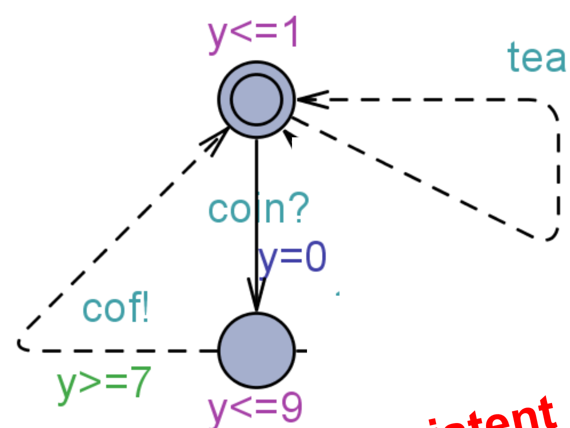








An Implementation



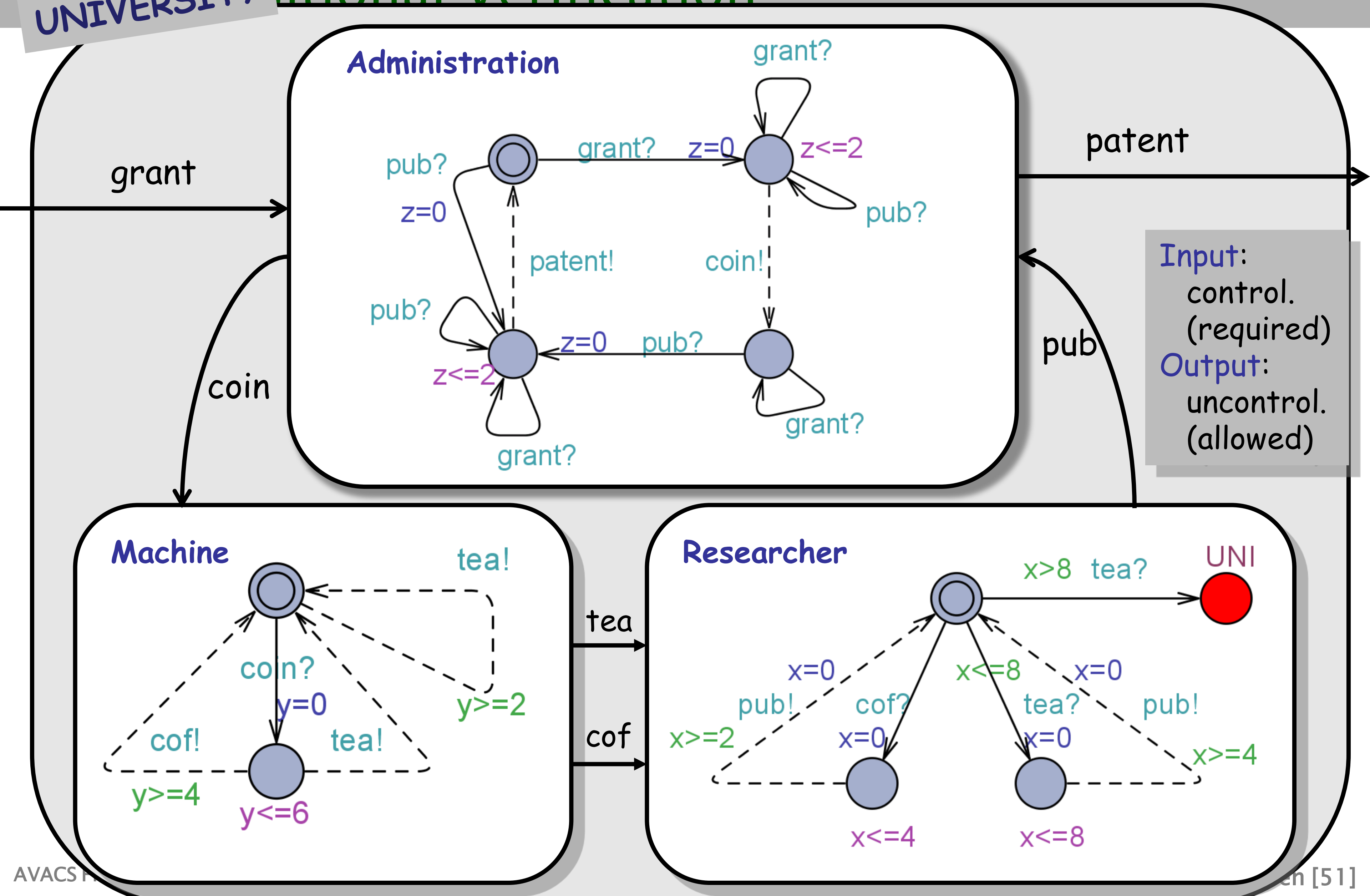
Inconsistent

S1/ H3: Compositional

C… sitional Verification

UNIVERSITY

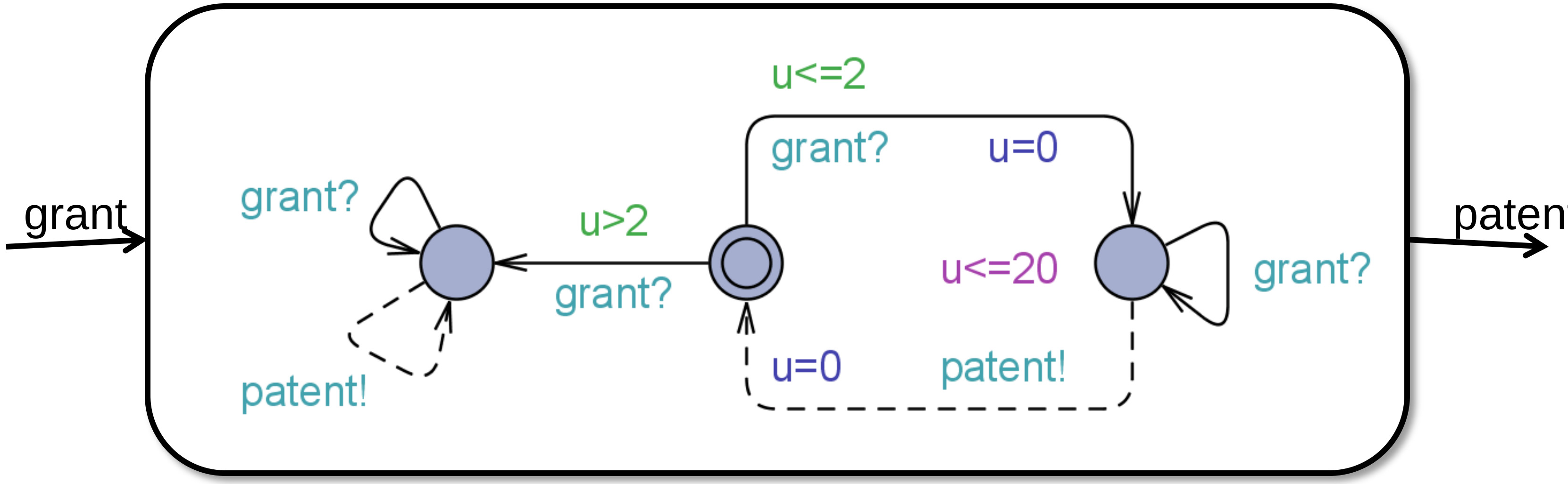
ECDAR

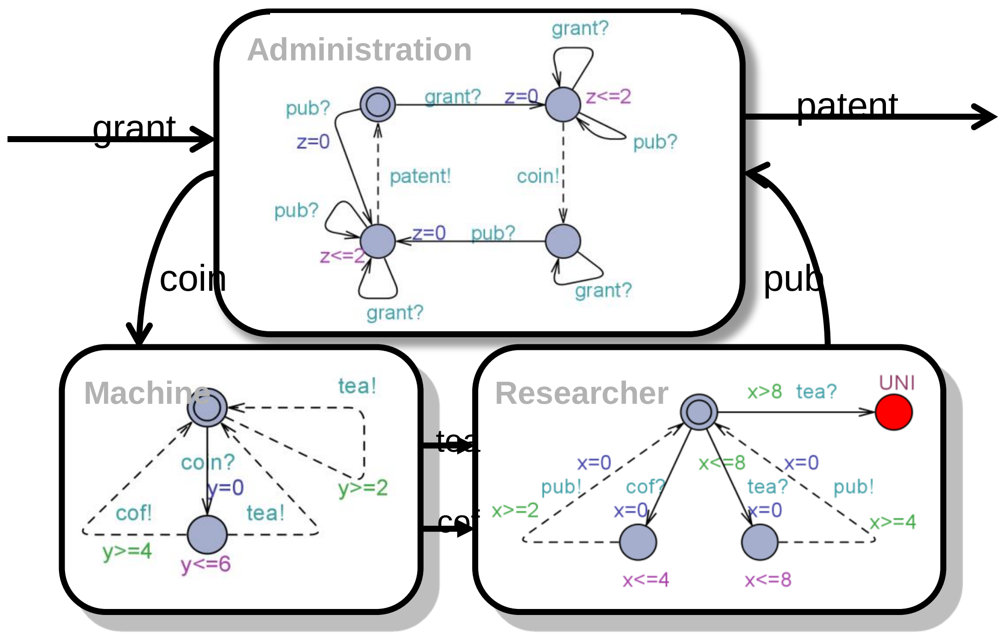


S1/ H3: Compositional

Compositional Verification

ECDAR





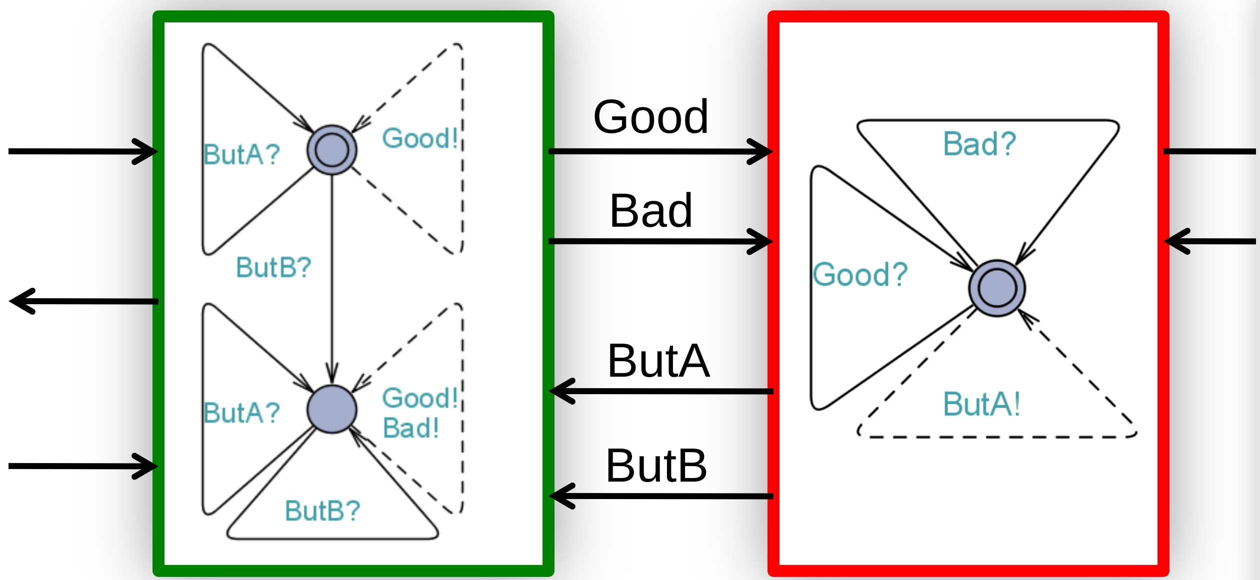
?

S1 / H3: Compositional

Compositional Verification

ECDAR

Guarantee Assumption



Properties

- (A | G) · ¸ (A | A>>G)
- A>>G ¸ G
- A · A') A>>G ¸ A'>> G
- G · G') A>>G · A>>G'

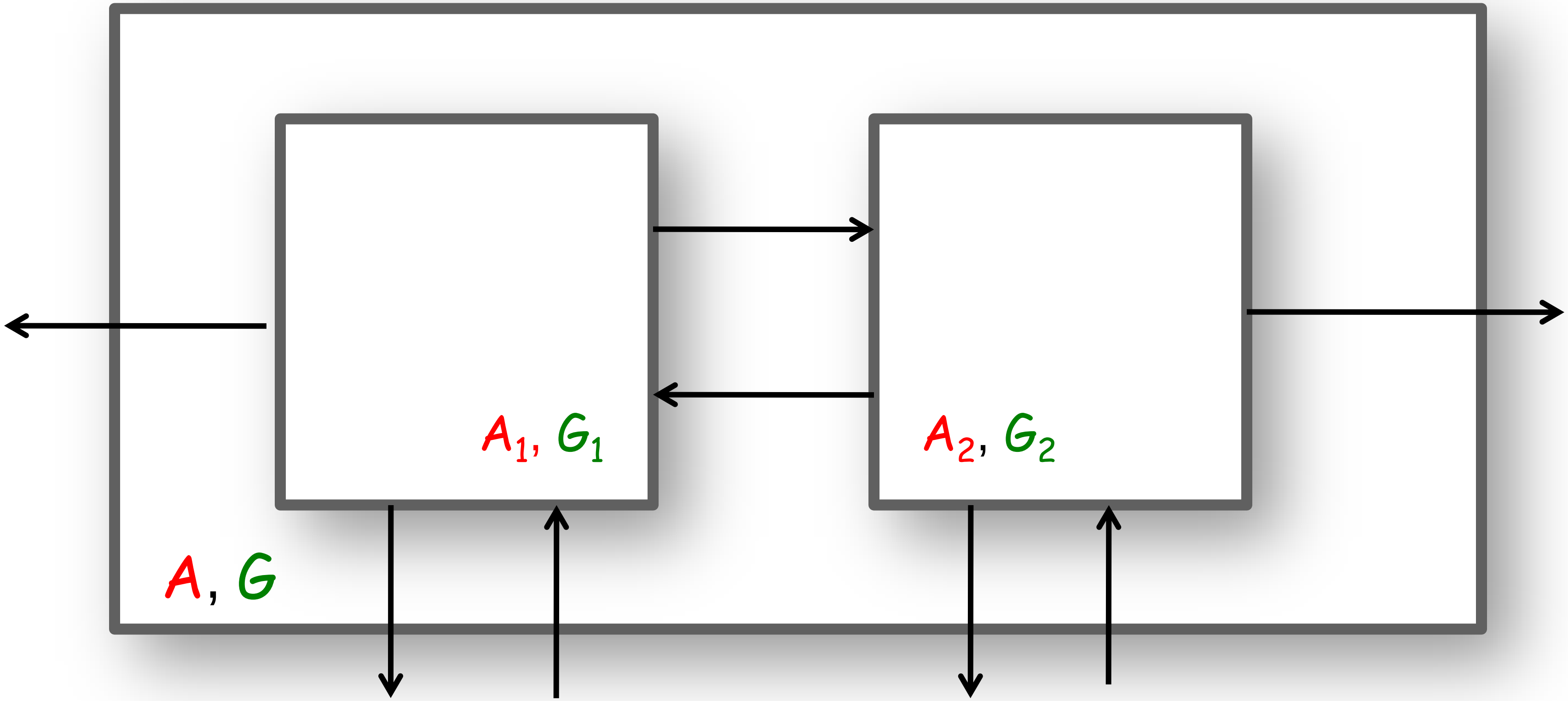
A>>G = (A | G) \ A

Quotient

X · B\A iff (X | A) · B

S1/ H3: Compositional
Compositional Verification

ECDAR



Proof Rule:

$A \gg G$ ⸲ ($A_1 \gg G_1$ | $A_2 \gg G_2$)

FASE'12: Moving from Specifications to Contracts in Component-Based Design

S1/ H3: Compositional

Compositional Verification

Contracts for Systems Design: theory

Albert Benveniste · Benoît Caillaud · Dejan Nickovic · Roberto Passerone · Jean-Baptiste Raclet · Philipp Reinkemeier · Alberto Sangiovanni-Vincentelli · Werner D... Henzinger · Kim Larsen

September 4, 2015

Abstract Recently an approach has be... to all methodologies introduced thus fa... analysis and abstraction/refinement: *co*... obtained in this domain but a unified tre... based design in perspective is missing. ... contracts are precisely defined and char...

... reasoning about safety and stability pro... trollers we examine a case study on a... sistance system for lane keeping and ... thereby target loosely coupled systems ...

Contracts for Systems Design: Methodology and Application

Albert Benveniste · Benoît Caillaud · Dejan Nickovic · Roberto Passerone · Jean-Baptiste Raclet · Philipp Reinkemeier · Alberto Sangiovanni-Vincentelli · Werner Damm · Tom Henzinger · Kim Larsen

September 4, 2015

Abstract Recently, *contract-based design* has been proposed as an "orthogonal" approach that can be applied to all system design methodologies proposed so far to cope with the complexity of system design. Contract-based design provides a rigorous scaffolding for verification, analysis and abstraction/refinement. This paper complements a companion theory paper [11] by further discussing methodological aspects of system design with contracts in perspective and presenting illustrations of the use of the contract methodology in two cases:

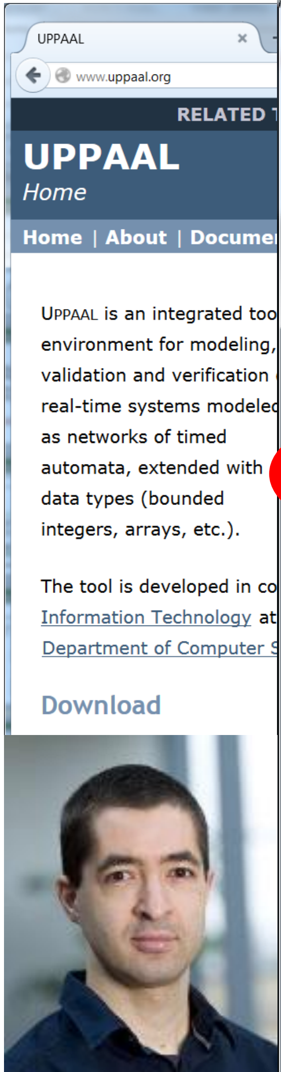
AVACS

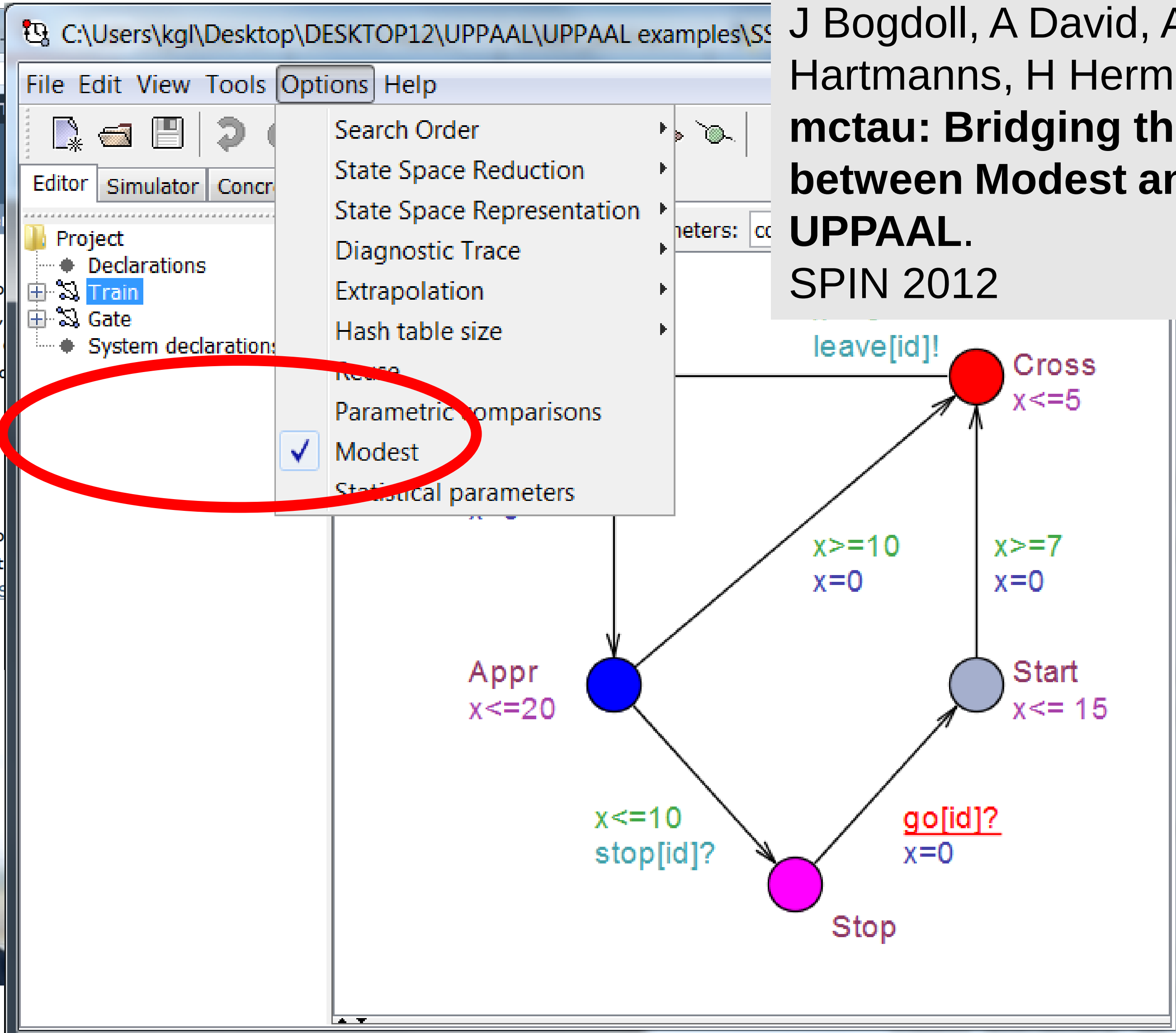
German Science Foundation, 1.1.04 – 31.12. 15.

Project Group R	Project Group H	Project Group S
Project Group R Real-Time Systems Coordinator: E. Olderog, CvOU Summary	**Project Group H** Hybrid Systems Coordinator: M. Fränzle Summary	**Project Group S** Coarse Grain System Structure Coordinator: Podelski Summary
R1: Beyond Timed Automata Coordinator: E. Olderog, CvO… Additional PIs: B. Finkbeiner, UdS M. Fränzle, CvOU A. Podelski, ALU V. Sofronie- Stokkermans, M…I	H1/2: Constraint-based	S1: Compositional Aproaches to …dS
R2: Timing Analysis and Distribution of Real-Time Tas… Coordinator: Wilhelm, UdS Additional PIs: E. Althaus, MPII W. Damm, CvOU S. Hack, UdS J. Reineke, UdS	U. Waldmann, MPII	C. Weidenbach, MPII
R3: Heuristic Search and Abstract Model Checking Coordinator: B. Nebel, ALU Additional PIs: B. Finkbeiner, UdS A. Podelski, ALU	H4: Automatic Verification of Hybrid System Stability Coordinator: O. Theel, CvOU Additional PIs: M. Fränzle, CvOU H. Hermanns, UdS A. Podelski, ALU V. Wolf, UdS	S3: Formal Verification of Dependability Properties Coordinator: H. Hermanns, UdS Additional PIs: B. Becker, ALU O. Theel, CvOU V. Wolf, UdS

S3: Formal Verification of Dependability Properties
Coordinator: H. Hermanns, UdS
Additional PIs:
B. Becker, ALU
O. Theel, CvOU
V. Wolf, UdS

S3: Dependability Properties



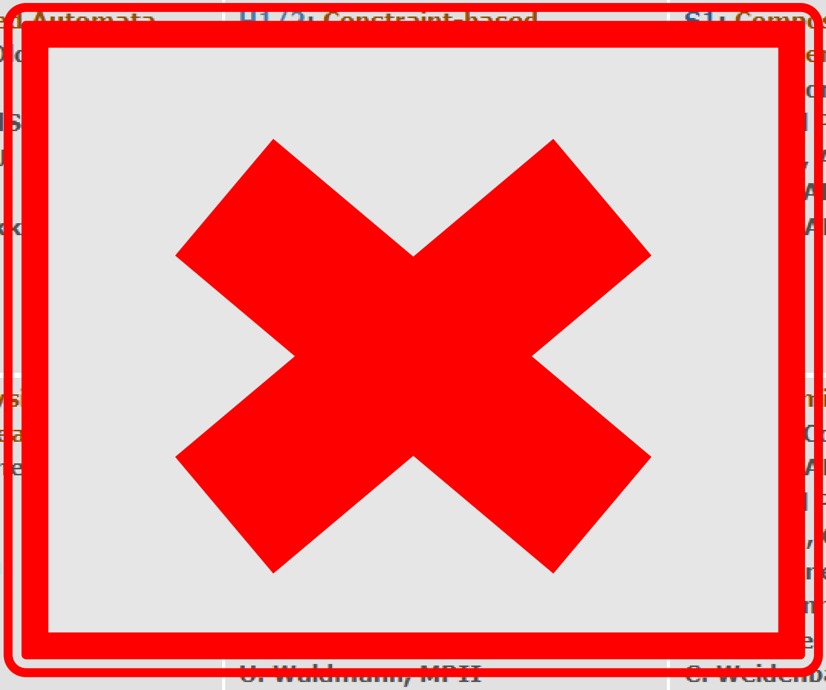


J Bogdoll, A David, A Hartmanns, H Hermanns: **mctau: Bridging the Gap between Modest and UPPAAL**.
SPIN 2012

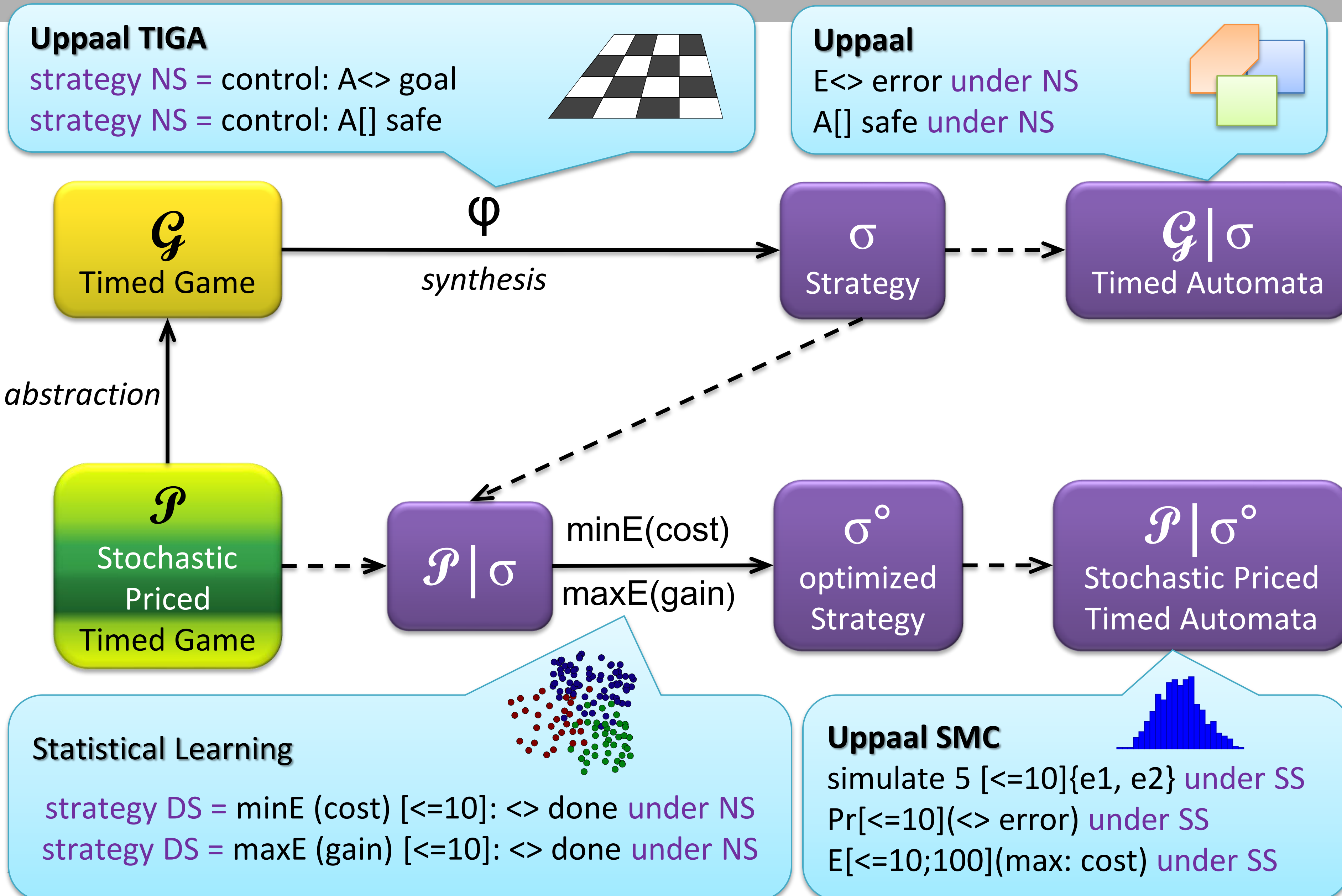
AVACS

German Science Foundation, 1.1.04 – 31.12. 15.

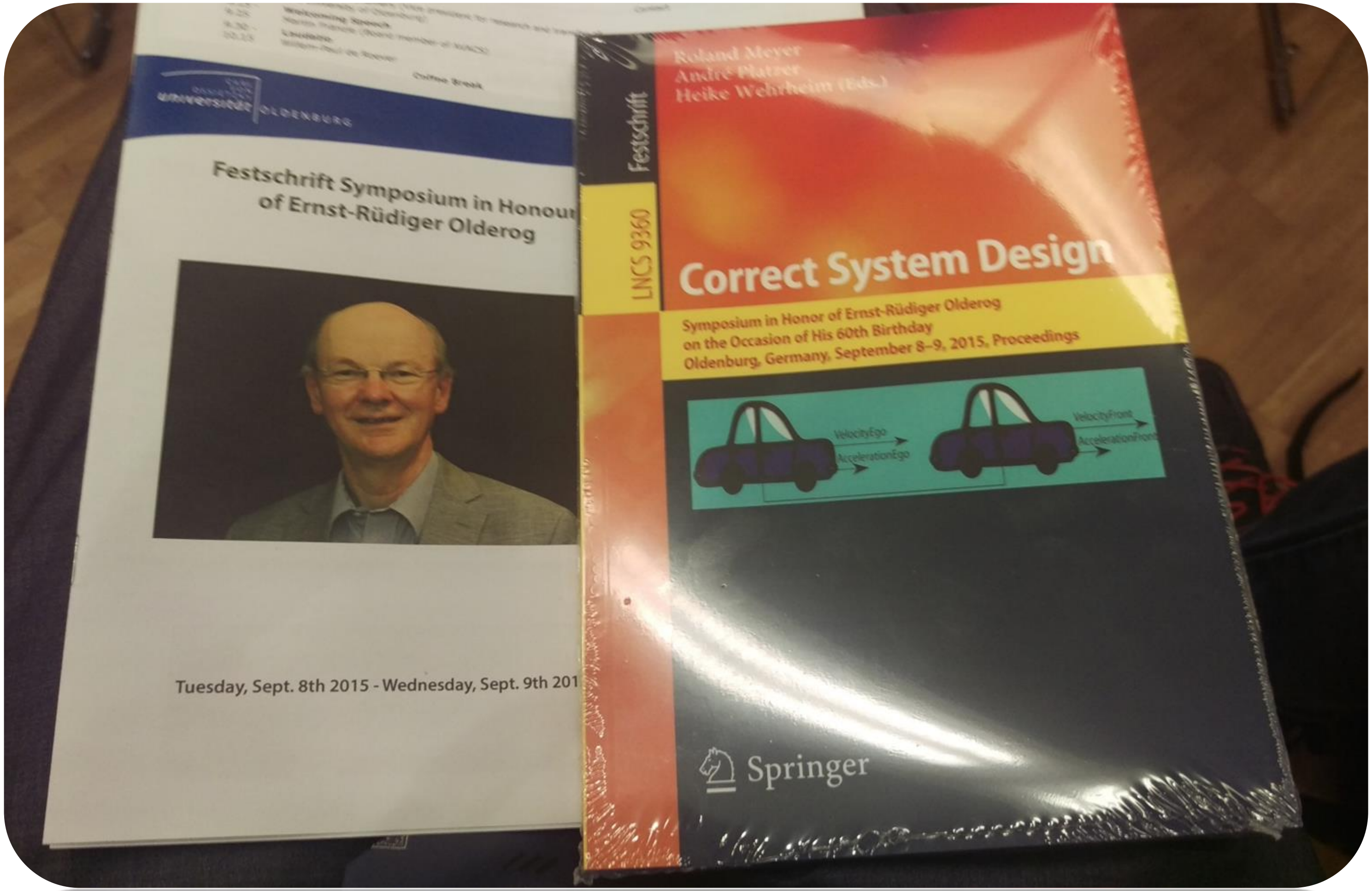
Project Group R Real-Time Systems Coordinator: E. Olderog, CvOU Summary	**Project Group H** Hybrid Systems Coordinator: M. Fränzle Summary	**Project Group S** Coarse Grain System Structure Coordinator: Podelski Summary
R1: Beyond Time… Automata Coordinator: E. Ol… Additional PIs: B. Finkbeiner, Ud… M. Fränzle, CvOU A. Podelski, ALU V. Sofronie- Stok…	H1/2: Constraint-based …	S1: Comp…sitional Aproaches to …erification …r: B. Finkbeiner, UdS …PIs: …, ALU …LU …LU
R2: Timing Analysi… Distribution of Re… Coordinator: Wilhe… Additional PIs: E. Althaus, MPII W. Damm, CvOU S. Hack, UdS J. Reineke, UdS	… U. Waldmann, MPII	…ic Communication …oordinator: A. …LU …PIs: …, CvOU …er, UdS …ns, UdS … UdS C. Weidenbach, MPII
R3: Heuristic Search and Abstract Model Checking Coordinator: B. Nebel, ALU Additional PIs: B. Finkbeiner, UdS A. Podelski, ALU	H4: Automatic Verification of Hybrid System Stability Coordinator: O. Theel, CvOU Additional PIs: M. Fränzle, CvOU H. Hermanns, UdS A. Podelski, ALU V. Wolf, UdS	S3: Formal Verification of Dependability Properties Coordinator: H. Hermanns, UdS Additional PIs: B. Becker, ALU O. Theel, CvOU V. Wolf, UdS



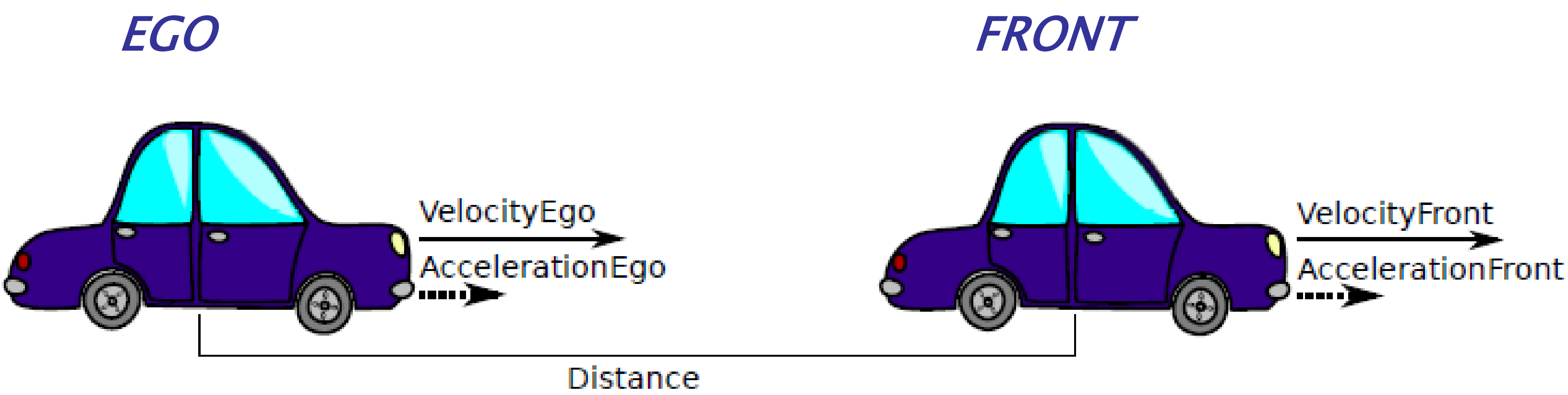
X: UPPAAL Stratego



X: UPPAAL Stratego



X: UPPAAL Stratego



Q1: Find a safety **strategy** for *Ego* such no crash will ever occur no matter what *Front* is doing.

Q2: Find the **most permissive strategy** ensuring safety

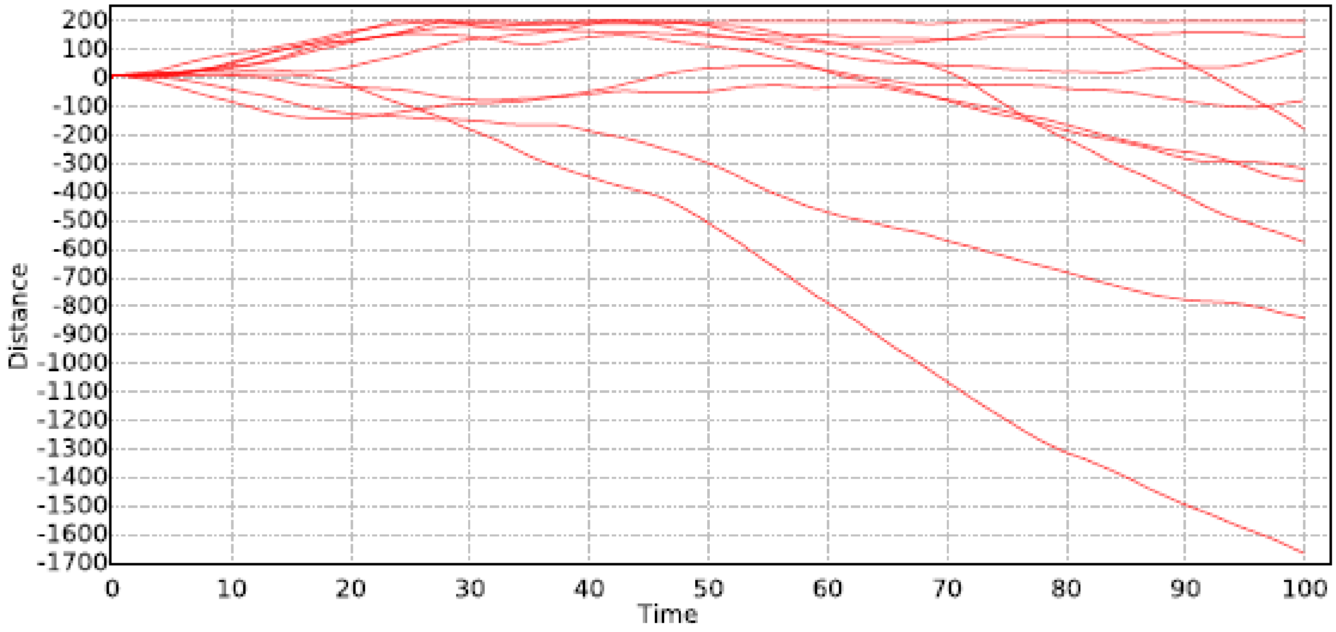
Q3: Find the **optimal sub-strategy** that will allow *Ego* to go as far as possible (without overtaking).

Safe and adaptive cruice control
L, Mikucionis, Taankvist 2015

X: UPPAAL Stratego

Pr[<=100] (<> distance <= 5)

A[] distance > 5



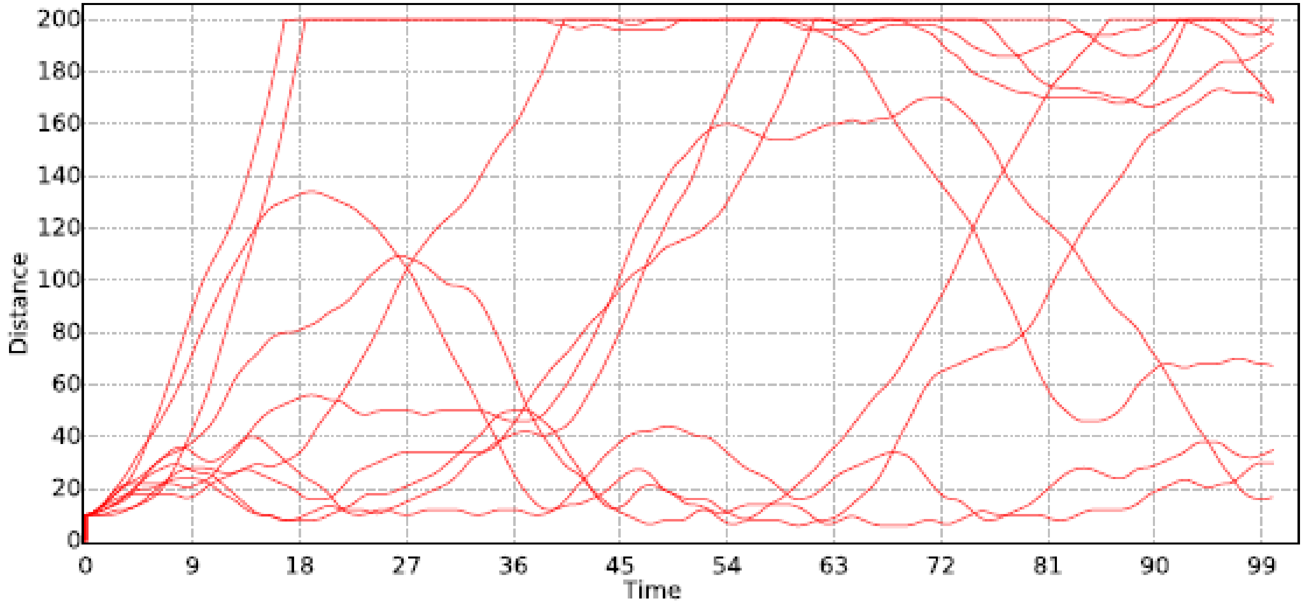
y
ative
je

No Strategy

X: UPPAAL Strategoego

```
strategy safe = control: A[] distance > 5
```

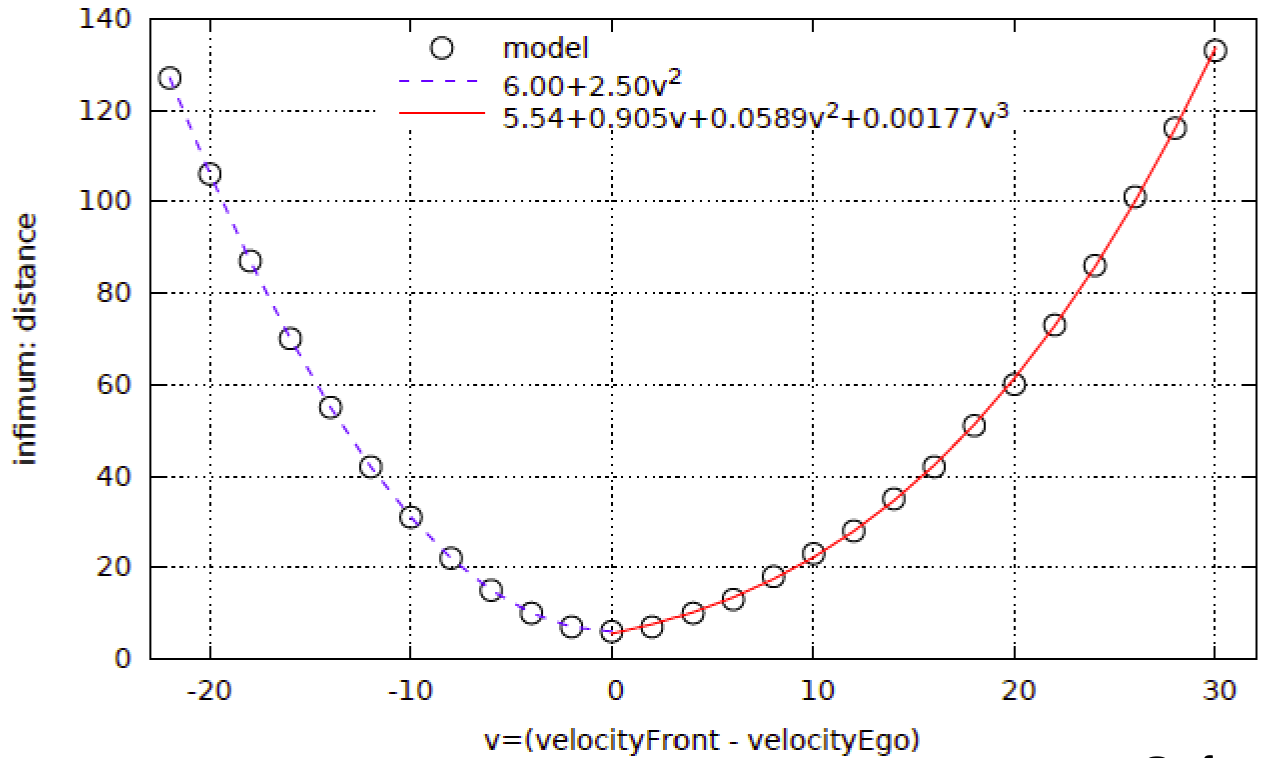
```
A[] distance > 5 under safe
```



Safety Strategy

X: UPPAAL Stratego

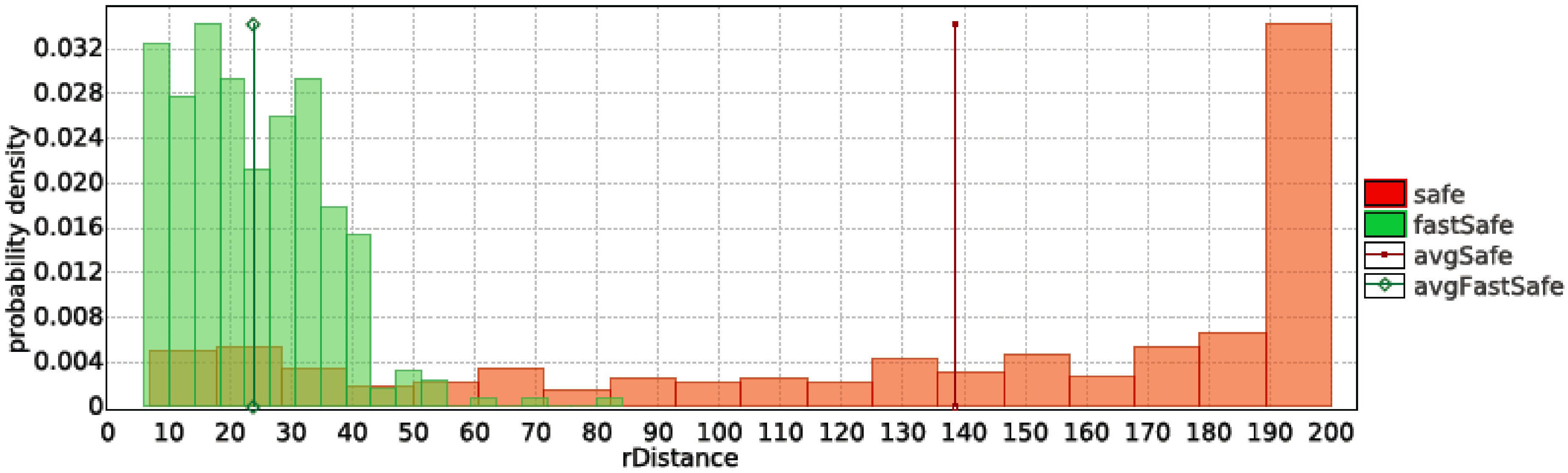
```
inf{velosityFront-velosityEgo==v}: distance under safe
```



Safety Strategy

X: UPPAAL Stratego

```
strategy safeFast = minE (D) [<=100]: <> time >= 100 under safe
```



Optimal and Safety Strategy

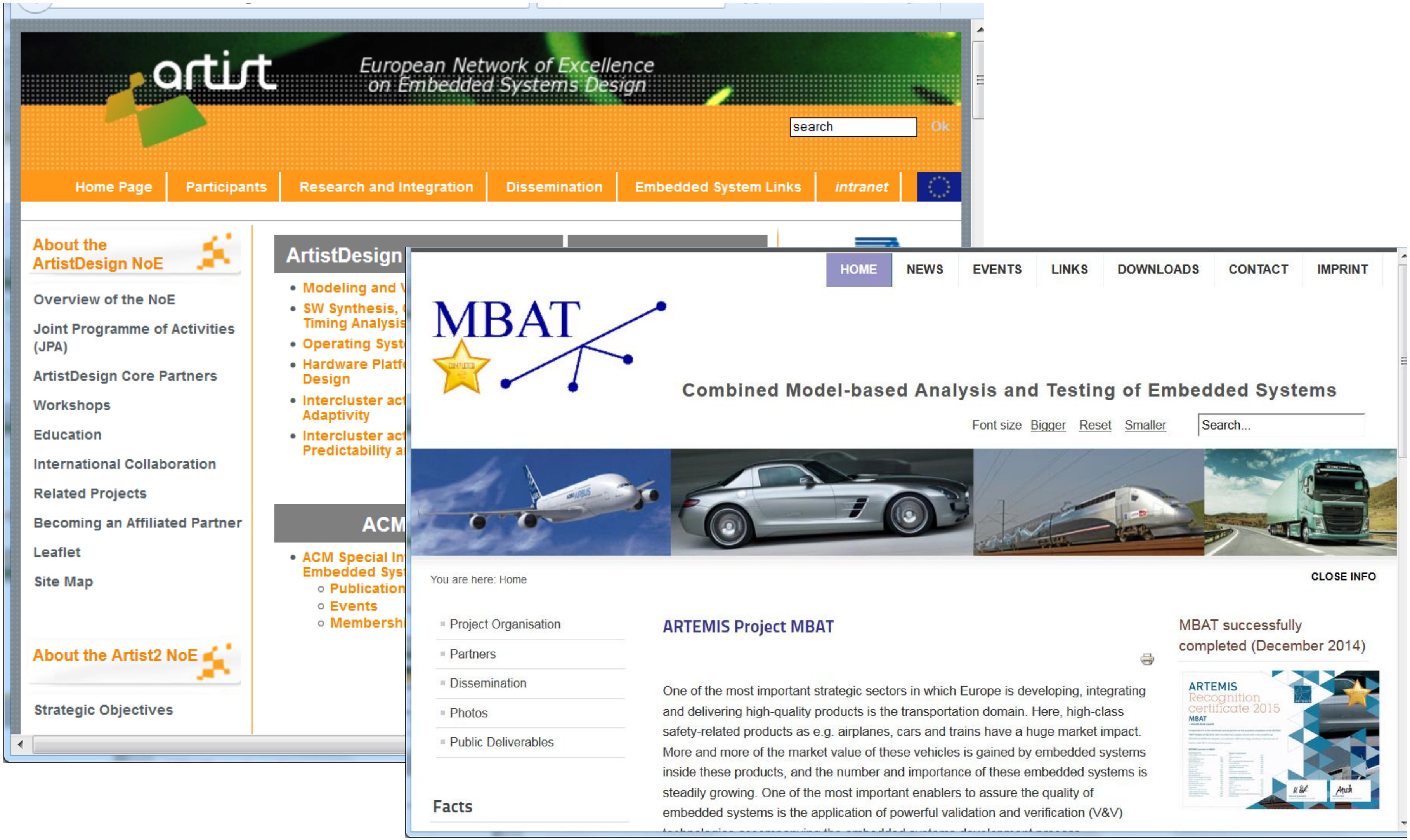
AVACS

German Science Foundation, 1.1.04 – 31.12. 15.

Project Group R Real-Time Systems Coordinator: E. Olderog, CvOU Summary	**Project Group H** Hybrid Systems Coordinator: M. Fränzle Summary	**Project Group S** Coarse Grain System Structure Coordinator: Podelski Summary
R1: Beyond Time Coordinator: E. Ol Additional PIs: B. Finkbeiner, UdS M. Fränzle, CvOU A. Podelski, ALU V. Sofronie- Stok		S1: Comp sitional Aproaches to erification r: B. Finkbeiner, UdS PIs: , ALU ALU ALU
R2: Timing Analysi Distribution of Re Coordinator: Wilhe Additional PIs: E. Althaus, MPII W. Damm, CvOU S. Hack, UdS J. Reineke, UdS		ic Communication Coordinator: A. ALU PIs: , CvOU er, UdS ns, UdS UdS C. Weidenbach, MPII
R3: Heuristic Search and Abstract Model Checking Coordinator: B. Nebel, ALU Additional PIs: B. Finkbeiner, UdS A. Podelski, ALU	H4: Automatic Verification of Hybrid System Stability Coordinator: O. Theel, CvOU Additional PIs: M. Fränzle, CvOU H. Hermanns, UdS A. Podelski, ALU V. Wolf, UdS	S3: Formal Verification of Dependability Properties Coordinator: H. Hermanns, UdS Additional PIs: B. Becker, ALU O. Theel, CvOU V. Wolf, UdS

INDUSTRIAL IMPACT

Industrial Impact



DiCyPS

CENTER FOR DATA-INTENSIVE CYBER-PHYSICAL SYSTEM

(2015–2021)

32.5, 74 MDKK

Innovationsfonden

FlexDanmark

Danfoss

Nyfors

Energistyrelsen

Rambøll

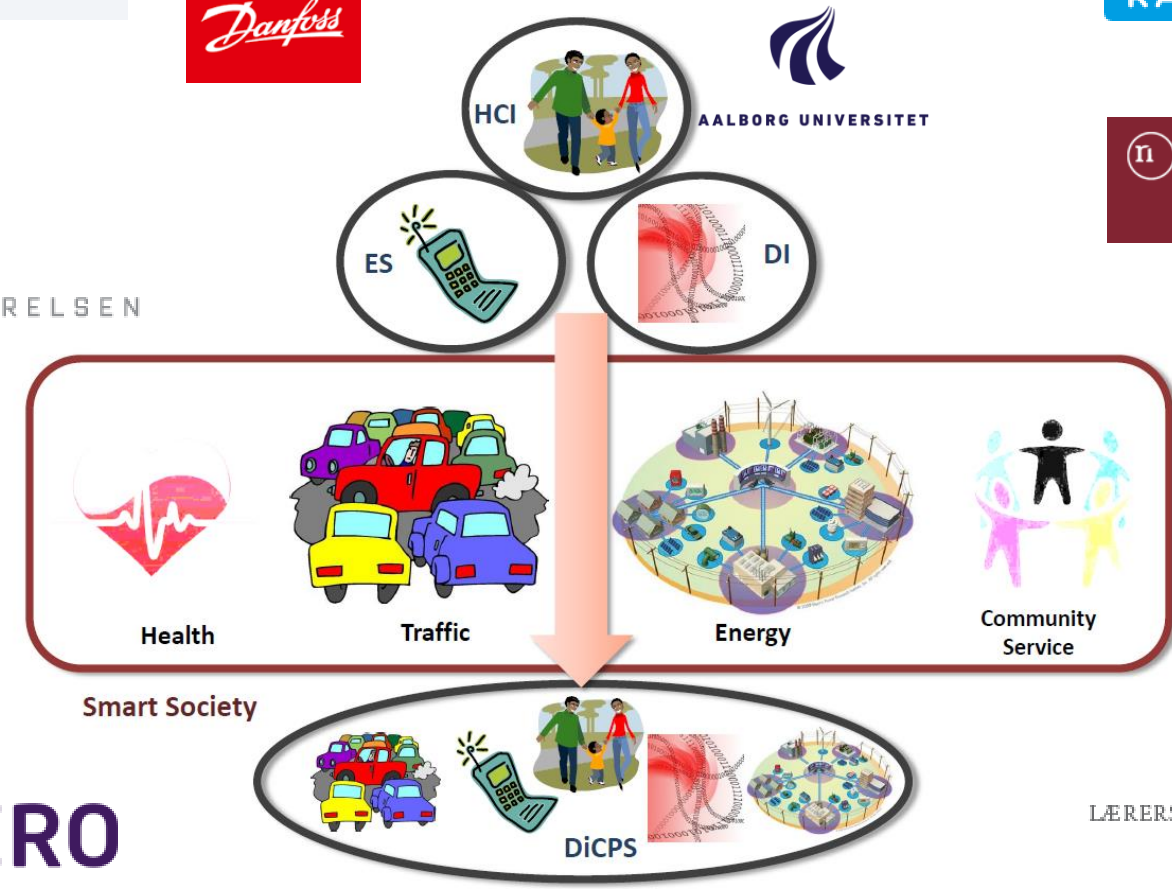
BLIP systems

Aalborg Universitet

Region Nordjylland – i gode hænder

Aalborg Kommune

Rejsekort



INSERO

Lærerstandens Brandforsikring

SCADA international

TU Dresden   INRIA   U College London

seluxit

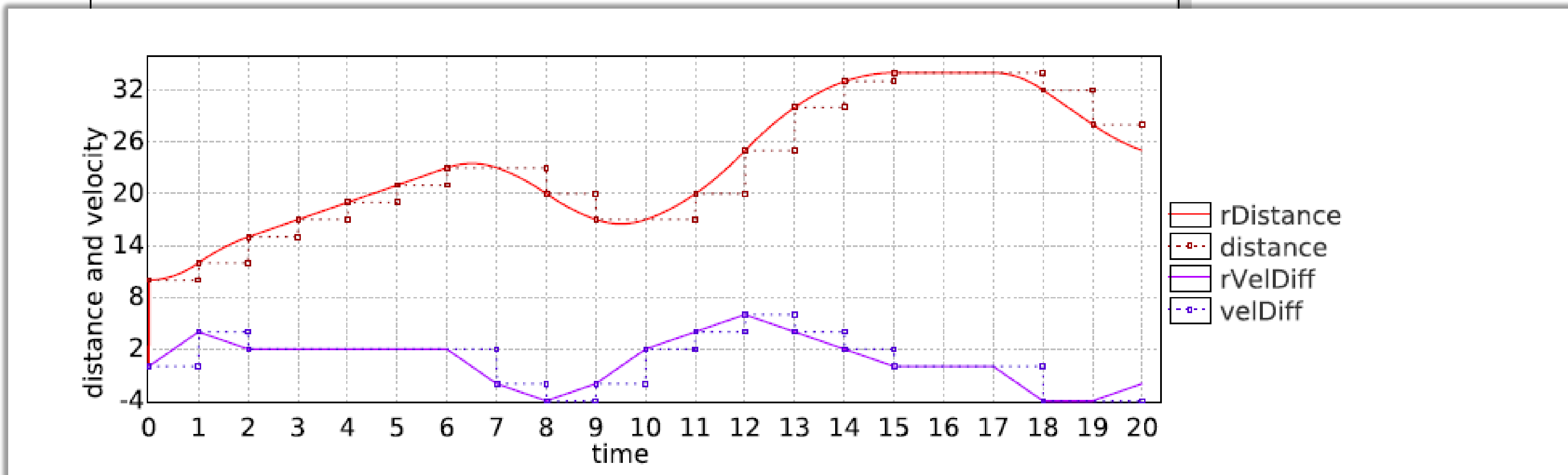
AVACS

German Science Foundation, 1.1.04 – 31.12. 15.

X: UPPAAL Stratego

Discrete

```
void updateDiscrete(){
    int oldVel, newVel;
    oldVel = velocityFront - velocityEgo;
    velocityEgo = velocityEgo + accelerationEgo;
```

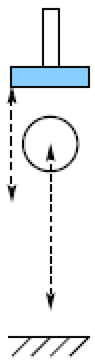


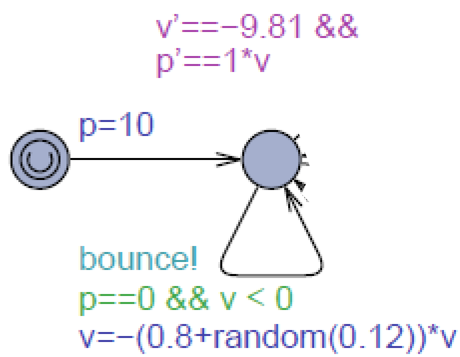

```
    rDistance) &&
D' == rDistance
```

Continuous

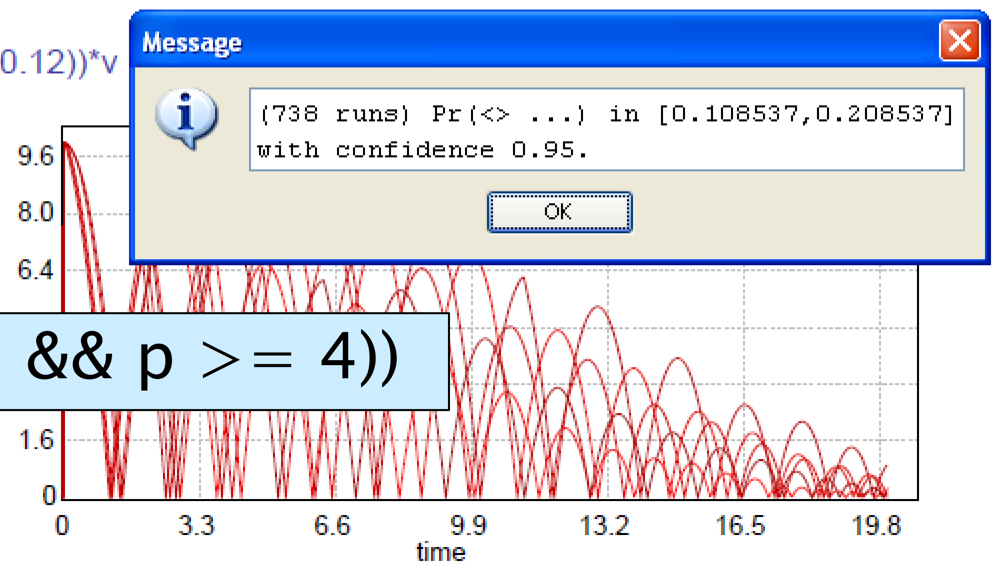
H: Hybrid Systems
Statistical MC,Stochastic HS

- A Bouncing Ball



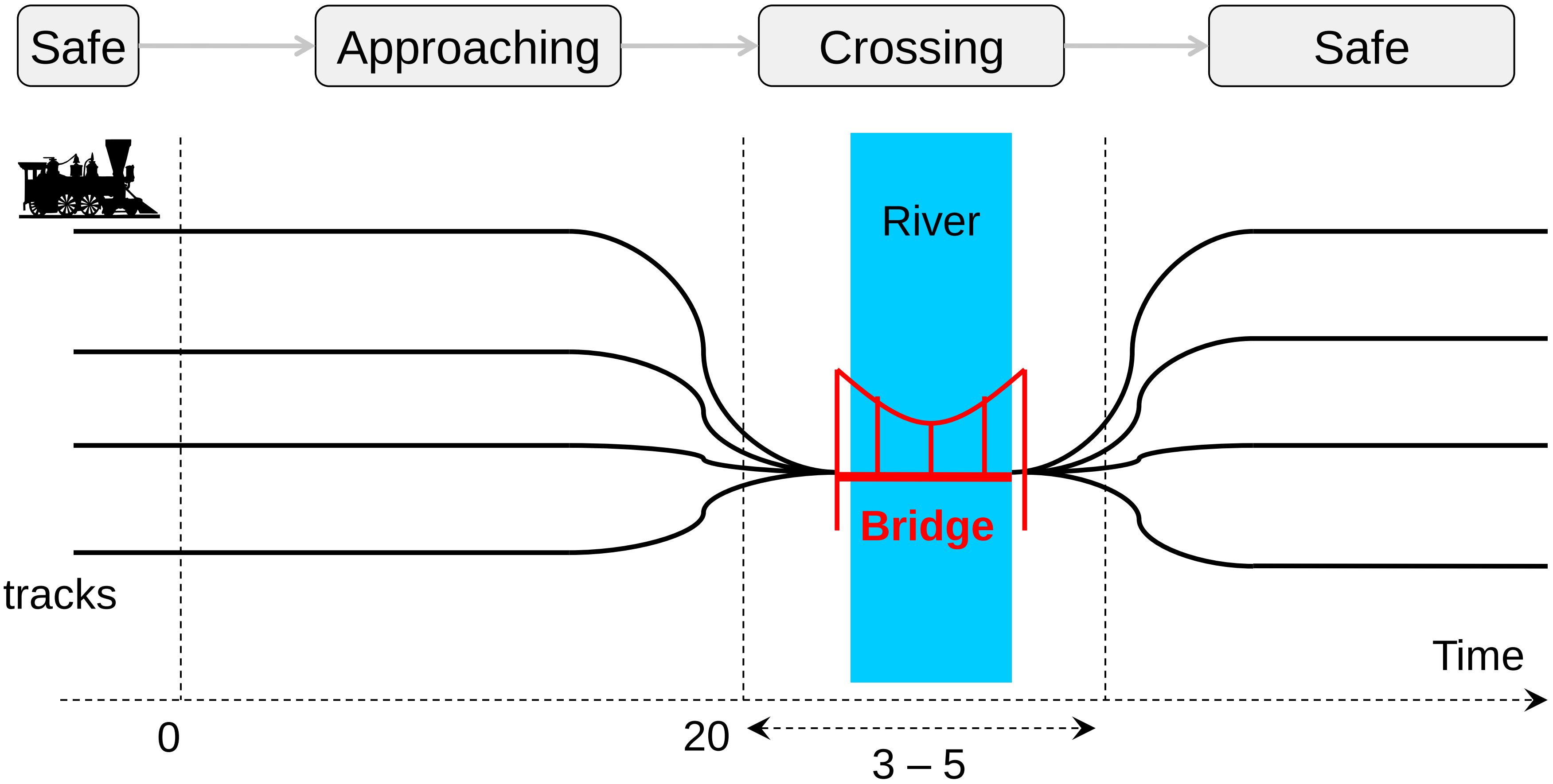


Simulate 5 [<=20] {p}

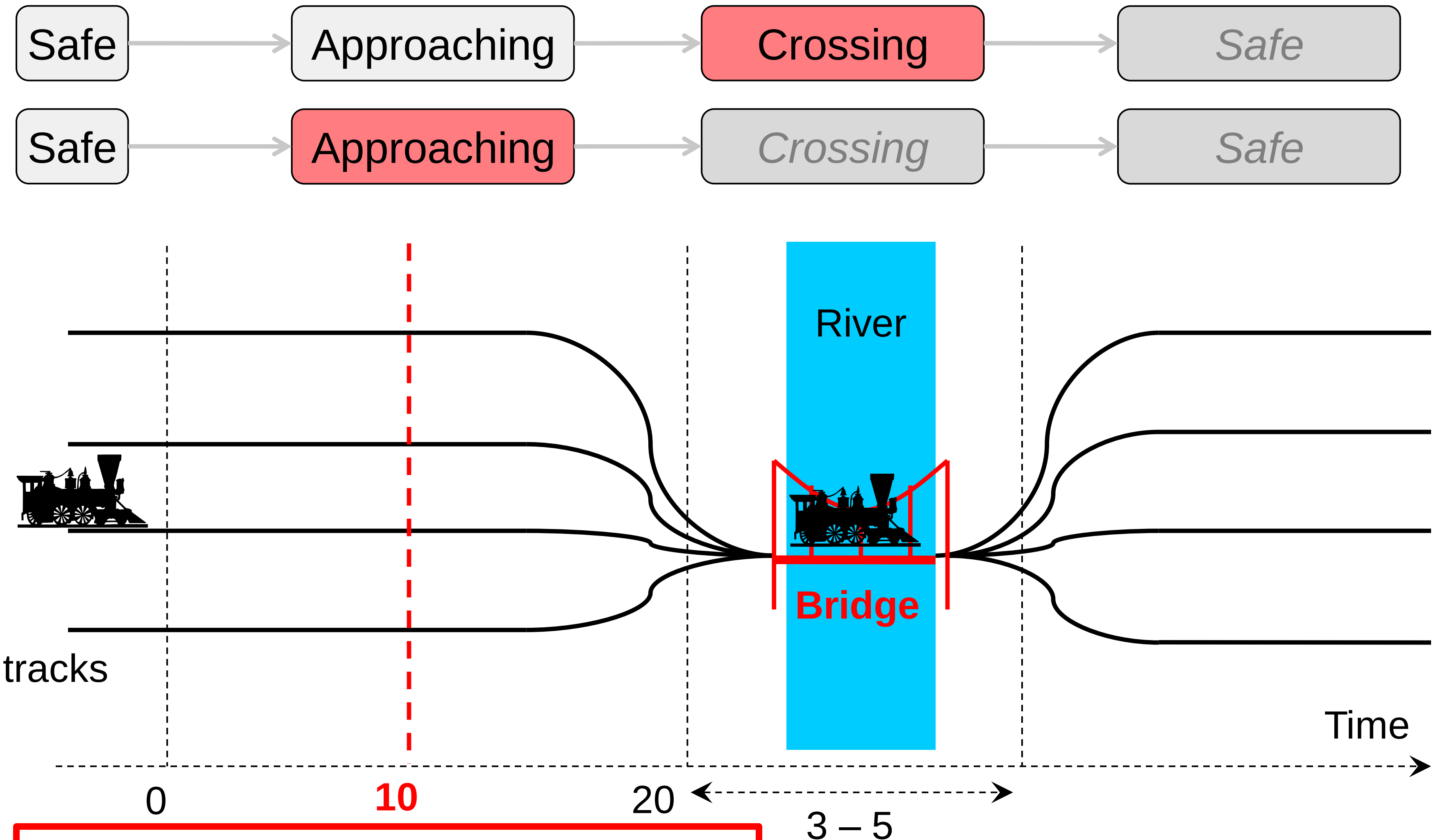


Pr[<=20](<>(time >=12 && p >= 4))

Train Crossing

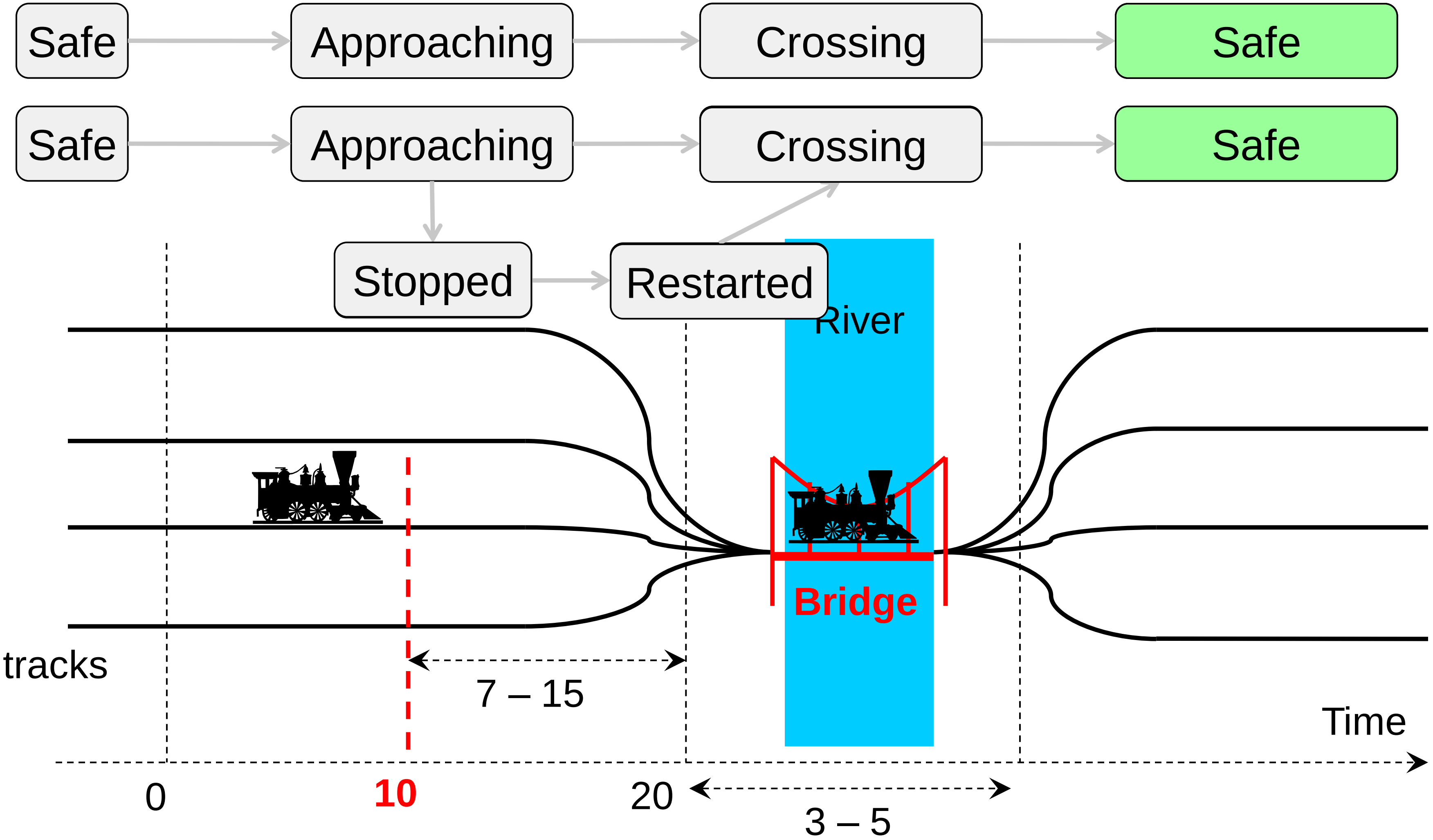


Train Crossing



Stop the train while it still stoppable!

Train Crossing



Train Crossing