



ARTIST2 – Year 1 Review

Grenoble, October 3rd-4th, 2005

Platform

Platform for Testing and Verification

Activity leader : Kim G Larsen (Aalborg U, DK)

Outline of the Presentation

Industrial Needs and Experience

Year 1 Activities

- 18 month objectives
- Achievements and ongoing work
- Interaction and Building Excellence Between Partners

18 Month Perspective

• Work planned for the next 18 months

Industrial Needs and Experience

*** INDUSTRIAL NEEDS:**

30-40% of production time is currently spend on elaborate, ad-hoc testing

- The potential of existing/improved testing methods and tools is enormous
- Especially important and challenging for embedded systems

* AIM

- Continued effort: on development of tools owned by cluster participants.
- Easy overview: of academic state-of-the-art tools, there domain of applicability, features, successful applications, etc.
- Increase scalability: Price of PC-cluster technology is going down and should be utilized in scaling up verification and analysis of models.
- Coordination: Realization of a European Verification Grid.

Activities – T&V Platform 18 month objective

* A. Testing and Verification Server:

≻ T0+06:

Evaluation of main testing and verification tools wrt maturity for integration.

➤ T0+18:

Installed and configured (virtual) server containing main testing and verification tools, e.g.:

- SPIN, SMV, UPPAAL, Kronos, Blast, TorX, TGV, FAST, CADP, IF

Original

- HyTech, visualSTATE, TAU, LASH, EMTCC, Rapture, ...

B. Parallel and Distribution Model Checking (PDMC):

≻ T0+6:

Evaluation of tools currently supporting PDMC on local PC-clusters.

➤ T0+18:

Design of coordination layer for integrating PDMC methods.

* C. European Test and Verification GRID

≻ T0+6:

Preevaluation of UPPAAL running on NORDUGRID

➤ T0+18:

Design of GRID infrastructure with links to national as well as European GRID activities.

***** Work on individual tools:

- New version of TGV (based on on-the-fly enumerative algorithms) linked to the IF toolbox (Verimag) has been developed using STL libraries (in place of CADP libraries) (IRISA)
- Extensions of real-time model checker UPPAAL with C-code (Aalborg)
- Development of IF tool-suit (Verimag)
- Support of the verification tool LASH and hosts powerful servers dedicated to verification (CFV)
- Linking between MoDEST/MOTOR and UPPAAL (Twente/Aalborg)
- DiVinE (Brno) has been extended with a Promela front-end for SPIN compatible distributed model checking.
- Development of UPPAAL Cora for optimal planning and scheduling (Aalborg)
- Development of UPPAAL Tron for real-time testing (Aalborg)
- Development of TIMES for schedulability analysis (Uppsala)



Work on Web-based Repository of Tools:

YAHODA, Verification Tools Database

🙀 YA	HODA - Verification To	ols Databas	se - Mozilla																
Eile	Eile Edit View Go Bookmarks Tools Window Help																		
1															500				
- (Search Search																		
_ <u>1</u>	The Bookmarks																		
e	VERIFICATION TOOLS Introduction Tools Table Login Registration																		
	DATABASE																		
	F :10																		A
	Filtering query not set	i 																	
1	Found 53 matching records.																		
	Purpose Specific Features Graphical Interface Availability Platforms Contact																		
		Model										Free							
	Name		<u>Equiv.</u> <u>Checking</u>	<u>Proving</u>	<u>Real</u> <u>Time</u>	Probabi listic	Hybrid	GUI	Graph. Specif.	<u>Graph.</u> Sim.	Free	Under Cond	<u>Commer</u> <u>cial</u>	<u>Win.</u>	related	<u>Others</u>	<u>vveb</u> <u>Site</u>	<u>Email</u>	-
	ACL2										0	Ø					×	*	8
	APMC																×	×	
	Atelier B			*			C			S	8						×	×	
	Bandera																	×	
	<u>Blast</u>			Į.						2				۲			X	×	
1	Cadence SMV	*		#											#		×	×	
	<u>CADiZ</u>							۲	3								X	×	
1	CADP							۲									N	×	
	CVVB - NC			ų.	#			۲		2	2				#		X	×	
	DBRover													۲				×	
	DiVinE Tool Set	#									1				1		× .	×	



***** Work on Web-based Repository of Tools:

YAHODA, Verification Tools Database

YAHODA -	- Verification T	ools Dat	abase - I	Mozilla																- 0
<u>F</u> ile <u>E</u> dit	<u>V</u> iew <u>G</u> o <u>B</u> oo	kmarks	<u>T</u> ools <u>W</u>	indow <u>H</u>	<u>t</u> elp															
6	6	\odot	No ht	:tp://anna	a.fi.muni.cz/	/yahoda/											🔍 Sear	ch	3	5 M
🚮 Home	Home Bookmarks																			
ب ^ع ال	VERIFICATION TOOLS DATABASE	F	Introd	uction)	Tools Ta	ble_)	4	Log	in)	Regis	stration)						
		-																		
Filtering query: (Model Checking) AND (Real Time) AND (GUI) AND (Win.)																				
E	C																			
Found	6 matching re	cords.			202			- E - E		0	Et al la com	-	-	0	190		DL			
Found	6 matching re	cords.		Purpo: <and:< td=""><td>se ></td><td></td><td>Spe</td><td>cific Fea <and></and></td><td>tures</td><td>Grap</td><td>hical Int <and></and></td><td>erface</td><td></td><td>Availabi <or></or></td><td>lity</td><td></td><td>Platform <or></or></td><td>IS</td><td>Con <at< td=""><td>tact ND></td></at<></td></and:<>	se >		Spe	cific Fea <and></and>	tures	Grap	hical Int <and></and>	erface		Availabi <or></or>	lity		Platform <or></or>	IS	Con <at< td=""><td>tact ND></td></at<>	tact ND>
Found	6 matching re	cords. <u>Mo</u> Linear Time	del Check <u>AntiD></u> Branch. Time	Purpos <u><and< u=""> ing Others</and<></u>	se ≥ <u>Equiv.</u> <u>Checking</u>	Theorem Proving	Spe <u>Real</u> <u>Time</u>	cific Fea <u><and></and></u> Probabi listic	tures <u>Hybrid</u>	Grap <u>GUI</u>	hical Inti <u>≺AND></u> <u>Graph.</u> <u>Specif.</u>	erface <u>Graph.</u> <u>Sim.</u>	/ <u>Free</u>	Availabi <u><or></or></u> <u>Free</u> <u>Under</u> <u>Cond.</u>	lity <u>Commer</u> <u>cial</u>	<u>Vvin.</u>	Platform <u>≤OR></u> <u>Unix &</u> related	Others	Con <u>≺Al</u> <u>Web</u> <u>Site</u>	itact ND≥ Email
Found	6 matching re Name	Linear Time	del Check ▲ <u><attid></attid></u> Branch. <u>Time</u> ●	Purpos <u><and< u=""> ing Others</and<></u>	se ≥ <u>Equiv.</u> <u>Checking</u>	Theorem Proving	Spe Real Time	cific Fea <u><and></and></u> Probabi listic	tures <u>Hybrid</u>	Grap <u>GUI</u>	hical Intr <u><and></and></u> <u>Graph.</u> <u>Specif.</u>	erface <u>Graph.</u> <u>Sim.</u>	Free	Availabi <u><or></or></u> <u>Eree</u> <u>Under</u> <u>Cond.</u>	lity <u>Commer</u> <u>cial</u>	VVin.	Platform <u>≤OR≥</u> <u>Unix &</u> related	Others	Con <u>≺Al</u> <u>Web</u> <u>Site</u>	Itact
Found	6 matching re Name <u>CWB - NC</u> DBRover	Linear Time	del Check <u>AntiD></u> Branch. <u>Time</u>	Purpos <u><and< u=""> ing Others</and<></u>	se <u>Equiv.</u> <u>Checking</u>	Theorem Proving	Spe Real Time	cific Fea <u><and></and></u> <u>Probabi</u> <u>listic</u>	tures <u>Hybrid</u>	Grap GUI Č	hical Intr <u><and></and></u> Graph. Specif.	erface <u>Graph.</u> <u>Sim.</u>	, <u>Free</u>	Availabi <u><or></or></u> <u>Free</u> <u>Under</u> <u>Cond.</u>	lity <u>Commer</u> <u>cial</u>	Vin.	Platform <u><or≥< u=""> <u>Unix &</u> related €</or≥<></u>	Others	Con <u><al< u=""> <u>Web</u> <u>Site</u></al<></u>	itact ND> Email
Found	6 matching re Name CWB - NC DBRover E	Linear Time	del Check <u>Attiba</u> Branch. <u>Time</u> <i>i</i>	Purpo: <and: ing Others</and: 	se <u>Equiv.</u> <u>Checking</u>	Theorem Proving	Spe Real Time	cific Fea <u><and></and></u> Probabi listic	Hybrid	Grap GUI Č	hical Intr <u><and></and></u> <u>Graph.</u> <u>Specif.</u>	erface <u>Graph.</u> Sim.	Free •	Availabi <u><or></or></u> Eree Under Cond.	lity <u>Commer</u> <u>cial</u>	Vvin.	Platform <u><or≥< u=""> <u>Unix &</u> related €</or≥<></u>	S Others	Con <u><a< u="">t <u>Web</u> <u>Site</u> ▼</a<></u>	tact ND≥ Email
Found	6 matching re Name CWB - NC DBRover IE PEP	Linear Time	del Check < <u>AttiD></u> Branch. <u>Time</u> € €	Purpo: <and: ing Others</and: 	se ≥ <u>Equiv.</u> <u>Checking</u>	Theorem Proving	Spe Real Time	cific Fea <u><and></and></u> Probabi listic	Hybrid	Grap GUI é	hical Int <u><and></and></u> Graph, Specif,	erface Graph. Sim.	Free •	Availabi <u><or></or></u> Free Under Cond.	lity Commer cial	Vin.	Platform <u><or></or></u> Unix & related	S Others	Con <u><al< u=""> <u>Web</u> <u>Site</u> X X X</al<></u>	Email
Found	6 matching re Name CVVB - NC DBRover IE PEP SGM	Linear Time 6	del Check <u>AntD></u> Branch. <u>Time</u> <i>i</i> <i>i</i> <i>i</i>	Purpo: <u><and< u="">: ing Others</and<></u>	se <u>Equiv.</u> <u>Checking</u>	Theorem Proving	Spe Real Time	cific Fea <u><and></and></u> Probabi listic	tures	Grap GUI Č	hical Int. <u><and></and></u> <u>Graph.</u> <u>Specif.</u> <i>•</i>	erface Graph. Sim.	Free ·	Availabi <u><or></or></u> <u>Eree</u> <u>Under</u> <u>Cond</u> .	lity Commer cial	VVin. * * *	Platform <u><or></or></u> Unix & related	S Others	Con <u><al< u=""> <u>VVeb</u> <u>Site</u> X X</al<></u>	Email X

ARTIST2

r.	Year 1 activ	/ities	
	File Edit View Go Bookmarks Tools Window Help		
	S S S https://benedict.aau.dk/duppaal/		🖸 🔍 Search 🛛 💐 🚺
* W	Home Bookmarks		
D	File information:		
C	Model: AN ASTRONOMICALLY BIG MODEL	Browse	
	Query: A VERY INTERESTING QUESTION	Browse	×
)	Model checking options		
	Search order: C bredth first C width first State space reduction: C none C conservative C aggressive State space representation: C DBM C compact data structure C under New syntax: C no Ves	approximation 🤉 over approximati	on
	Distribution options		
)	Number of CPUs: C 1 C 5 C 10 C 15 C 20 C 25 C 30 C 35 O 4	9	
	Run options		
	Max walltime (minutes): O 1 O 5 O 15 O 30 O 60 O 120 @ 240		
	Contact information		
]	Email: kgl@cs.auc.dk]	
	Submit Query Reset		
	T Q Q F G GZ Find stonned.		
	∰Start Y @Ju @Jp @Jc @Jc @Jr @Jr @Jr [∭M 21 @	🔅 🕲 🖂 🥥 🏈 🤷 👰	
		Oslo Grid Cluster 43	8+14 0+1
	Handreich Norway	Oslo Temp Cluster 7	8+8 0+0

Work on Parallel and Distributed Model Checking

Application of Distributed UPPAAL to Leader Election Algorithm for Mobile Ad-hoc Networks by Leslie Lamport (1 year effort).



(id,dest,id.lead,id.hops)



Leslie Lamport

All,

Thanks for the spec. It seems to run fine. As expected, it's 2 or 3 orders of magnitude faster than TLC. I'm wondering if your algorithms could be used for checking specs written in a higher level language like TLA+.

Year 1 activities Interaction & Building Excellence

- Tutorials and tool presentations given at several conferences, workshops and schools: eg
 - Embedded World Nürnberg
 - > ARTIST2 summerschool
 - ≻ RTSS05
 - ≻ TECS06
- Several exchange visits between Brno and Aalborg University.
- Steering committee membership and invited presentations at PDMC workshop (ICALP2005).

18 Month Perspective Work Planned for the next 18 months

- Extend Yahoda Database with testing tools and links to repository for case studies.
- Continue effort on individual tools.
- Extend parallel and distributed model checking capabilities from safety to liveness properties.
- Initiative effort on Parallel and Distributed Methods for Verification and Performance Evaluation with European Teams outside the cluster November 16-17, 2005, INRIA Rhone-Alpes (Grenoble).

Jiri Barnat (Masaryk Univ. Brno) Gerd Behrmann (Aalborg Univ.) Stefan Blom (Univ. of Innsbruck) Jeremy Bradley (Imperial College) Lubos Brim (Masaryk Univ. Brno) Ivana Cerna (Masaryk Univ. Brno) Hubert Garavel (INRIA Rhone-Alpes) Boudewijn Haverkort (Univ. Twente) Christophe Joubert (INRIA Rhone-Alpes) Josva Kleist (Aalborg Univ.) William Knottenbelt (Imperial College) Martin Leucker (TU Munich) Radu Mateescu (INRIA Rhone-Alpes) Jaco van de Pol (CWI) Michael Weber (Aachen and CWI) X (Twente U)

Activities – T&V Platform 18 month objective

* A. Testing and Verification Server:

≻ T0+06:

Evaluation of main testing and verification tools wrt maturity for integration.

➤ T0+18:

Installed and configured (virtual) server containing main testing and verification tools Link from Yahoda to easy downloadable versions of **mature** and **stable** versions of tools with links to common repository of successful case studies.

Modified

B. Parallel and Distribution Model Checking (PDMC):

≻ T0+6:

Evaluation of tools currently supporting PDMC on local PC-clusters.

➤ T0+18:

(Initiate) Design of coordination layer for integrating PDMC methods.

* C. European Test and Verification GRID

≻ T0+6:

Preevaluation of UPPAAL running on NORDUGRID

➤ T0+18:

Design of GRID infrastructure with links to national as well as European GRID activities.

ARTIST2

Network of Excellence on Embedded Systems Design Year1 Review -- Grenoble, October 3rd-4th, 2005

END

Schedule & Milestones

Joint Cluster Meeting (w. parallel sessions) medio December

Quantitative Testing & Verification

- A. Foundation for black-box testing of real-time systems established T0+6:
 - a. Soundness and limit-completenessb. Metric for coverage.

T0+18:

- a. Computability and Complexity of learnability.
- b. Robustness and Implementability

B. Improved tools for quantitative analysis with experimental evaluation T0+6: a. Improved symbolic datastructures b. Houristics for officient guiding

b. Heuristics for efficient guiding **T0+18:**a. Abstraction methods

- a. Abstraction methods
- b. Comparison with (MI)LP and OR
- c. Stochastic Model Checking
- d. Controller Synthesis

C. Industrial case studies.

T0+6: Collection of case studies on web. T0+18: Classification of case studies

Verification of Security Properties

- A: Cryptographic protocols T0+6:
 - a. A common language for security protocolsb. A publicly available data base of
 - security protocols and their
 - analysis (attacks, proofs,
 - assumptions/properties....)
 - T0+18:
 - a. A validation tool set that is accessible via the web.b. Two industrial case studies that
 - are already available.

B: Certification technology and virtual machine validation

- T0+6:
- A methodology for certification of the levels EAL6 and EAL7 of the common criteria.
- T0+18:
- A (prototype) tool set for certification of the levels EAL6 and EAL7 of the common criteria.

Testing & Verification Platform

A. Testing and Verification Server: T0+06: Evaluation of main testing and verification tools wrt maturity for integration.

T0+18:

Installed and configured (virtual) server – Links to mature/stable versions

B. Parallel and Distribution Model Checking (PDMC):

T0+6: Evaluation of tools currently supporting PDMC on local PCclusters.

T0+18:

(Initiate) design of coordination layer for integrating PDMC methods.

C. European Test and Verification GRID T0+6: Preevaluation of UPPAAL running on NORDUGRID T0+18:

Design of GRID infrastructure