Retrascope: Open-Source Model Checker for HDL Descriptions

Alexander Kamkin, Mikhail Lebedev, Sergey Smolov

Ivannikov Institute for System Programming of RAS

accellera SYSTEMS INITIATIVE

ISP RAS Ivannikov Institute for System Programming Russian Academy of Sciences

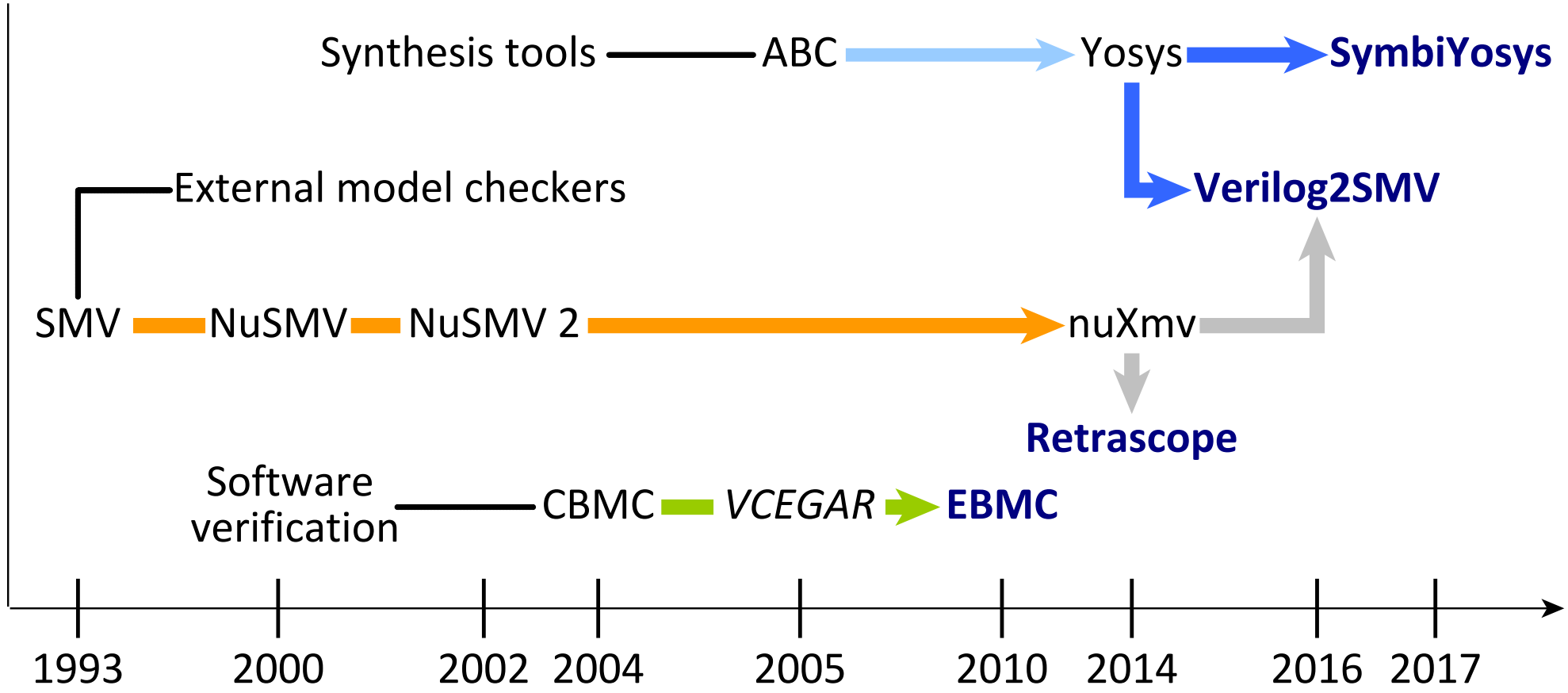
2019 DESIGN AND VERIFICATION DVCON CONFERENCE AND EXHIBITION EUROPE

Formal Verification in HDL

Goal: check user-defined properties on HDL modules quickly, correctly and without user's additional efforts

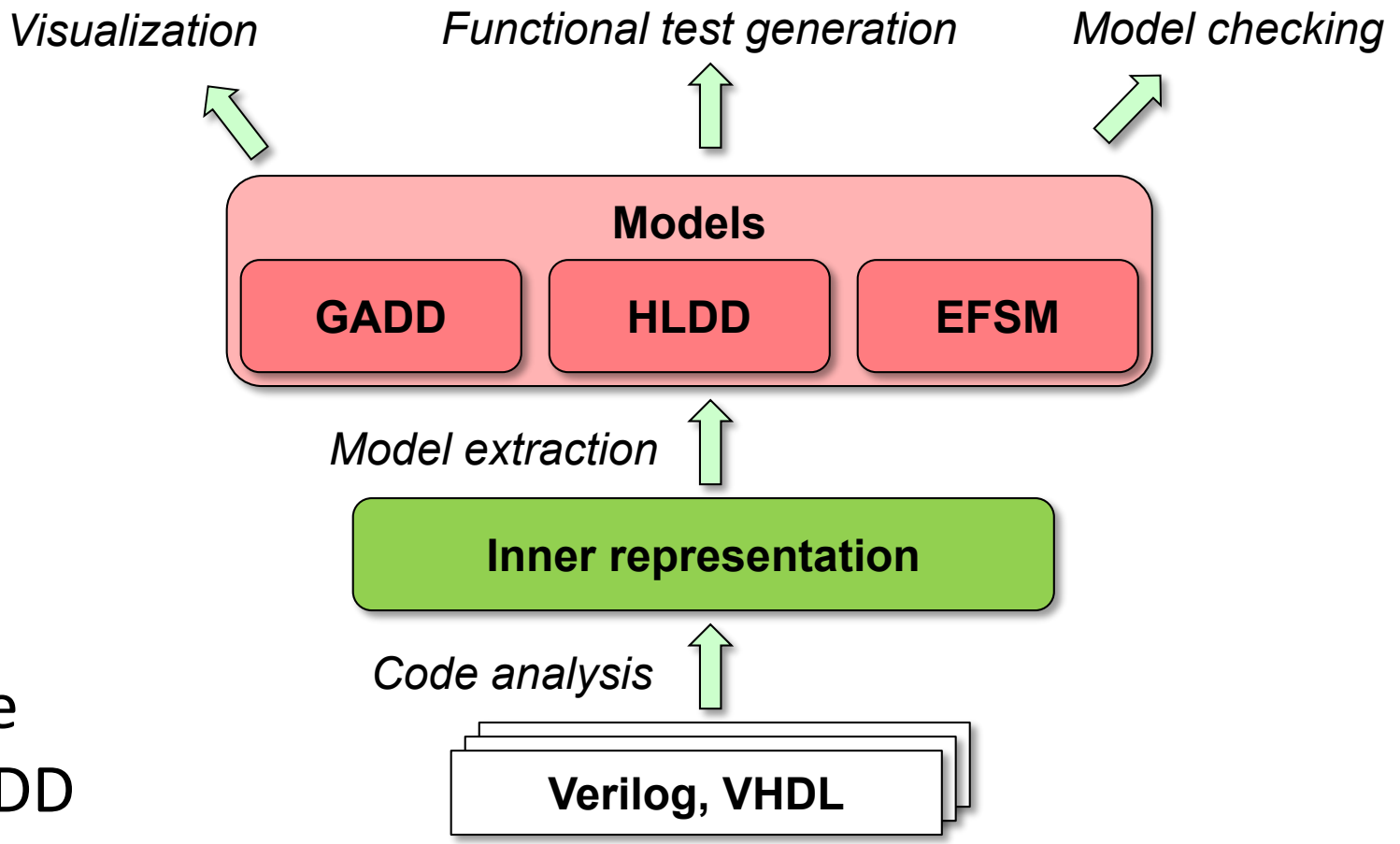
- **Interest & strength growth**
  - More automation, more tools (SMT solvers, abstraction)
  - Attempts to apply FV tools to industrial cases
- **Open Source invades HW world**
  - RISC-V, MIPS Open
- **Model checking**
  - Formal techniques for determining whether a given **model** satisfies given **specifications**
  - Counterexample generation (+)
  - "State explosion" problem (-)

HDL Model Checkers: History



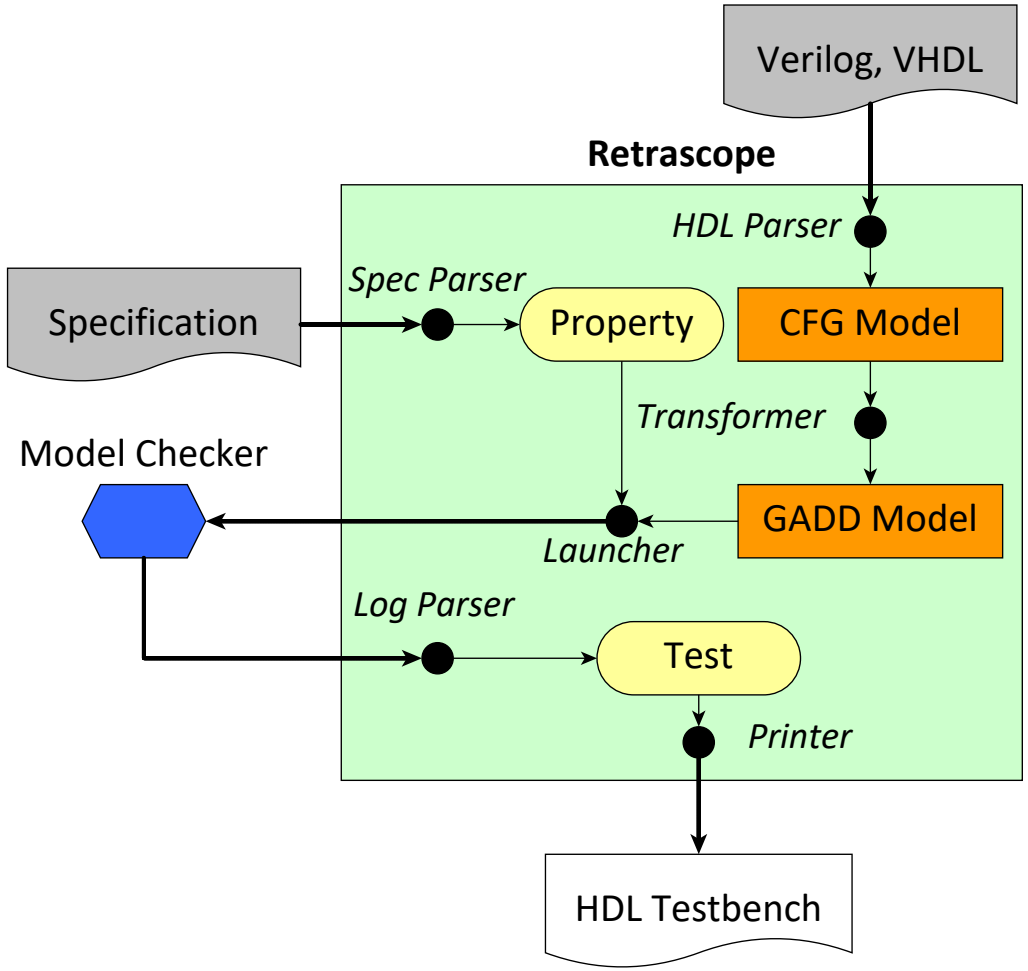
Retrascope toolkit

- **Extendible framework** for functional verification and analysis of HDL modules
- Provides **engines** for code parsing, model extraction and visualization
- Several kinds of **models** are supported: CFG, EFSM, GADD



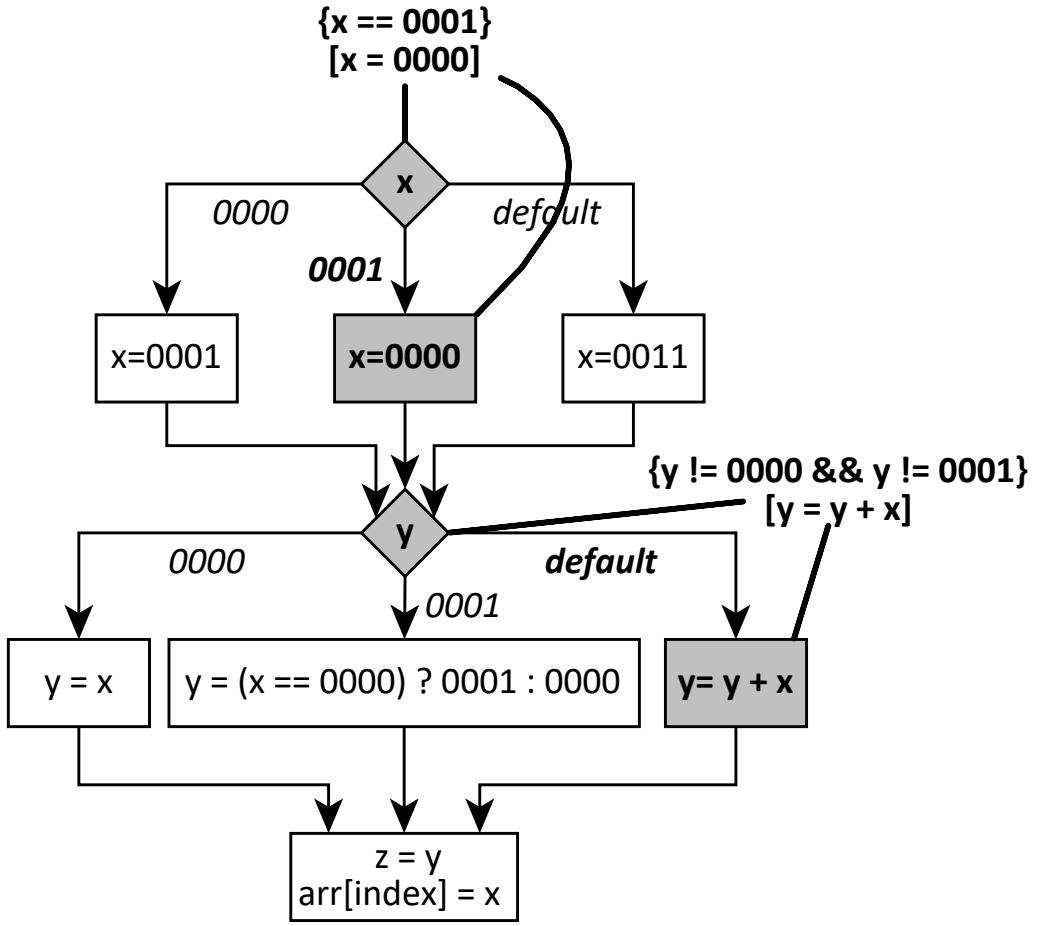
Model checking flow in Retrascope

1) HDL code & specification parsing
2) Control Flow Graph (CFG) building
3) CFG → GADD transformation
4) SMV model generation
5) SMV model checking
   a) Standalone checker (NuSMV, nuXmv)
6) Model checker trace parsing
   a) HDL testbench generation



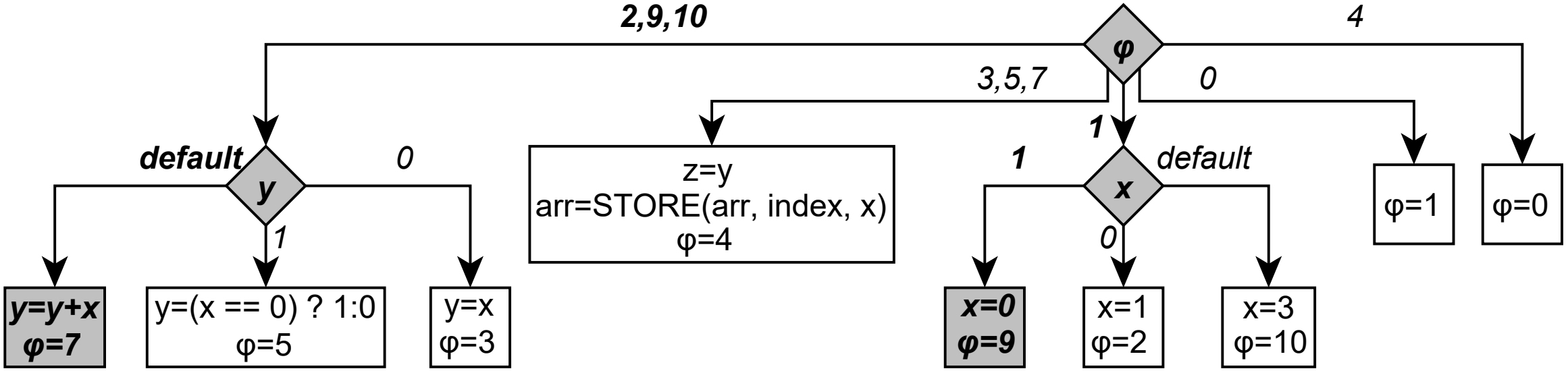
Guarded actions in CFG model

- **guard** – branch condition
- **action** – assignments
- **guarded action** (GA) is a pair $\gamma \rightarrow \delta$, where γ is a guard and δ is an action
- GADD – Guarded Actions Decision Diagram
  - transformed CFG
  - GA are **atomic**



Guarded Actions Decision Diagram

- Phase (φ) – integer variable that keeps it's value within a GA
- New value of φ is assigned at the action of every GA
- GADD is translated into the SMV format



Properties in Retrascope

- Automatically generated for typical errors
  - Potential **conflicts**
    - **Write-write**: at least 2 processes write the same variable on the same tick
    - **Write-read-write**: no reads between two writes
    - **Undefined**: variable is read before initialization
  - **Dead code** detection
    - EFSM model extraction, enabling conditions for transitions are checked by nuXmv
- User-defined specifications
  - **PSL** (supported by the SMV-based checkers)
  - **SVA** subset → automatically translated to PSL

Evaluation: HDL Model Checkers

- **EBMC**
  - The Enhanced Bounded Model Checker
  - University of Oxford, England (Daniel Kroening)
- **SymbiYosys**
  - Front-end driver program for Yosys Open SYnthesis Suite
  - Clifford Wolf, Austria
- **Verilog2SMV**
  - Yosys-based Verilog-to-SMV translation tool
  - Foundazione Bruno Kessler (FBK), Italy

Model checker overview

Tool	EBMC	SymbiYosys	Verilog2SMV	Retrascope
Input	Verilog, netlist, SystemVerilog, SMV	Verilog, SystemVerilog	Verilog, SystemVerilog	Verilog, SystemVerilog, VHDL
Properties	LTL, SVA subset	SVA subset	SVA subset	PSL, SVA subset
Distribution	binary	source code	source code	source code
Multi-file module processing	+	+	-	+
Separate property checking	+	-	-	+
VCD counterexample generation	+	+	-	-
HDL counterexample generation	+	-	-	+
GUI	-	+	-	+
License	ISC	ISC	GNU GPL v3	Apache License 2.0

HDL benchmarks

Quite a long story…

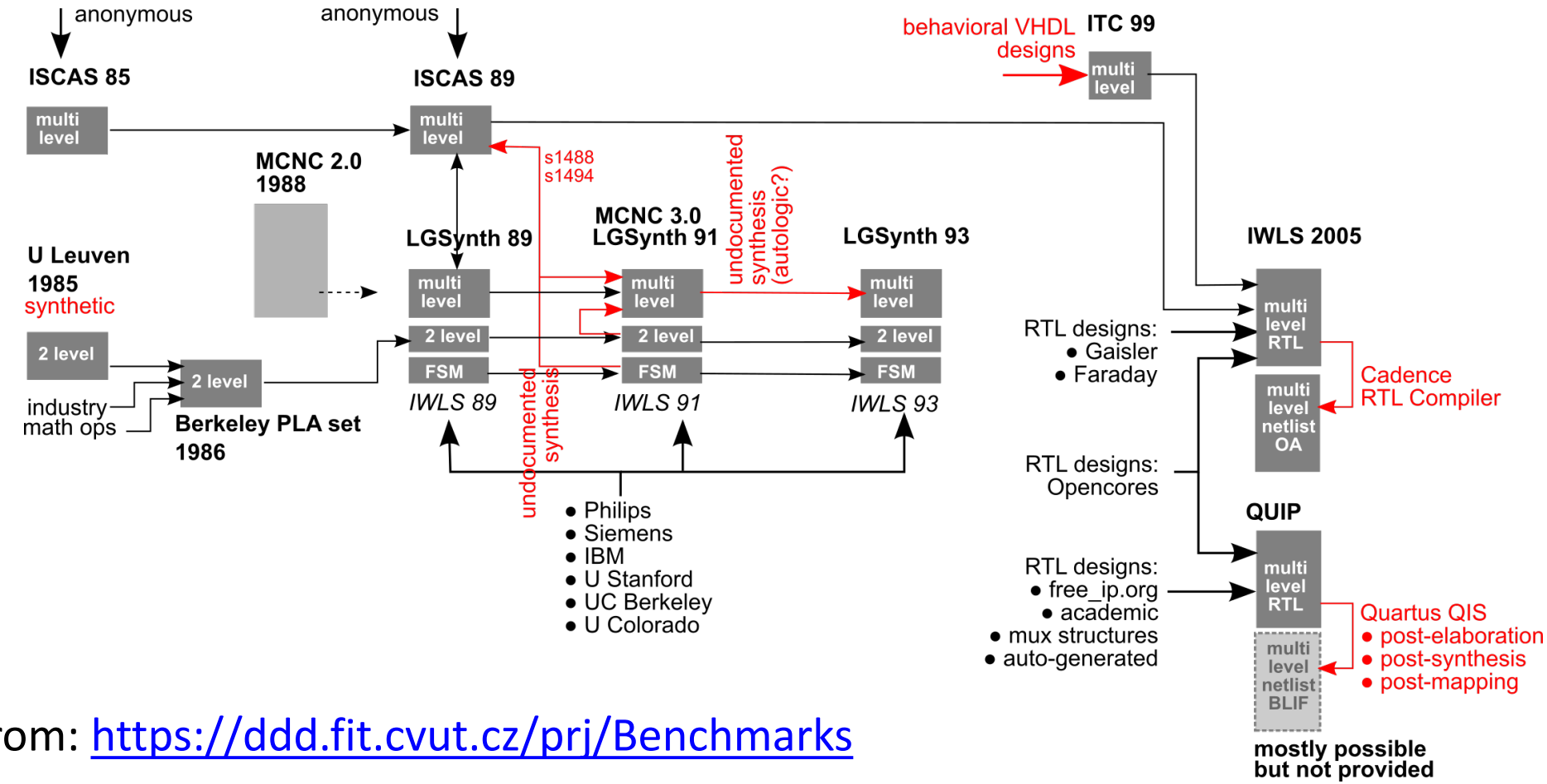


figure from: https://ddd.fit.cvut.cz/prj/Benchmarks

Selected Verilog benchmarks

- **Texas-97**
  - University of Texas, part of Prof. A. Aziz course on formal verification
  - 74 files, 45655 LOC, 0 properties
- **VCEGAR**
  - Benchmarks for VCEGAR tool (former EBMC)
  - 37 files, 11037 LOC, 2 SVA assertions
- **Verilog2SMV**
  - Benchmarks for Verilog2SMV tool
  - 58 files, 17634 LOC, 92 SVA assertions

Experiment #1: Verilog support

Reference compiler – ModelSim Starter Edition

1) Run tools on **original** benchmarks
2) Fix errors that were detected by ModelSim
3) Run tools again on **fixed** benchmarks

Tool behaviors (*legend*):

OK – no errors

ERR – error is found in erroneous Verilog module

FAIL – error is found in *correct* Verilog module

CRASH – unexpected crash

Experiment #1: Results

Tool	Texas-97				VCEGAR				Verilog2SMV			
	Ok	Err	Fail	Crash	Ok	Err	Fail	Crash	Ok	Err	Fail	Crash
EBMC	12	0	54	12	37	0	0	0	92	0	4	1
	9	48	20	1	35	1	0	1	3	3	90	0
SymbiYosys	8	0	63	7	22	0	15	0	96	0	0	0
	10	47	17	4	20	4	13	0	96	0	0	0
Verilog2SMV	9	0	65	4	21	0	15	1	96	0	0	0
	8	47	19	4	19	4	13	1	96	0	0	0
Retrascope	21	0	57	0	36	0	1	0	93	0	3	0
	20	46	12	0	35	1	1	0	93	0	3	0

Unsupported (but correct!) Verilog

- EBMC
  - Assigning inputs to regs or outputs
  - **task** without parameters
- SymbiYosys, Verilog2SMV
  - 2 or more complement declarations of the same signal
  - Different types of left / right sides of assignments
  - Uninitialized variables

Experiment #2: Property checking

- In benchmarks – **assert property** *expr*
  - EBMC doesn't support them, rewrite with ***always*** and ***assert***(...)
- Time limit – 1 hour per module
- Bounded model checking, bound 100
- Tool behaviours (*legend*)

  FALSE – property is ***false***, counterexample is generated

  TRUE – property is ***true*** or bound is reached, no counterexamples

  ERR – error is found in erroneous Verilog module

  FAIL – error is found in ***correct*** Verilog module

  CRASH – unexpected crash

  TIMEOUT – time limit expiration

Experiment #2: Results

Tool	FALSE	TRUE	ERR	FAIL	CRASH	TIME
EBMC	40	105	0	6	**0**	**2**
SymbiYosys	29	98	0	11	3	6
VerilogSMV	27	90	0	13	3	14
Retrascope	**44**	81	**4**	**1**	3	15

- Yosys-based tools are unable to check properties separately
- Retrascope has found **max num of counterexamples** (“FALSE”)
- Retrascope is the best **bug detector** (“ERR”)
- Retrascope provides the largest **Verilog support** (“FAIL”)
- Most **stable** tool is EBMC (“CRASH”)
- **Performance** leader is EBMC; SymbiYosys is close (“TIME”)

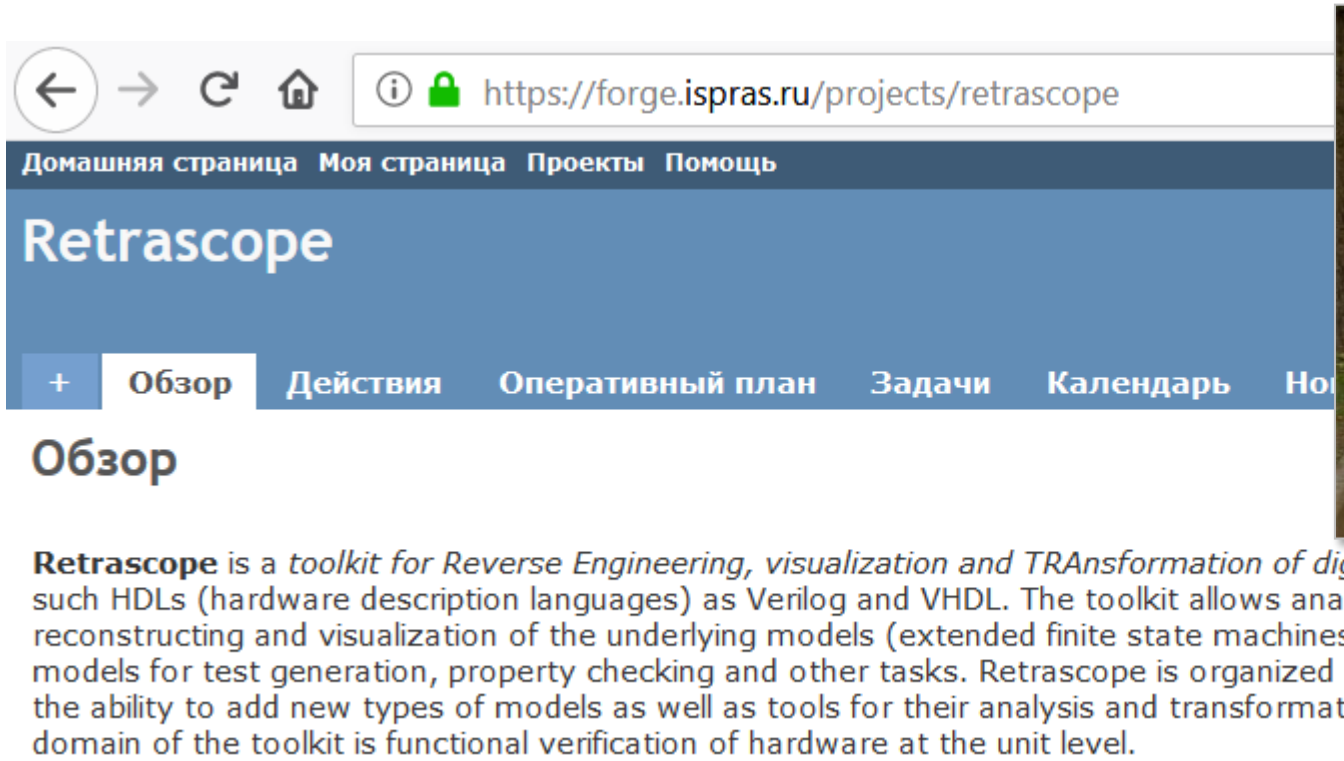
Case study

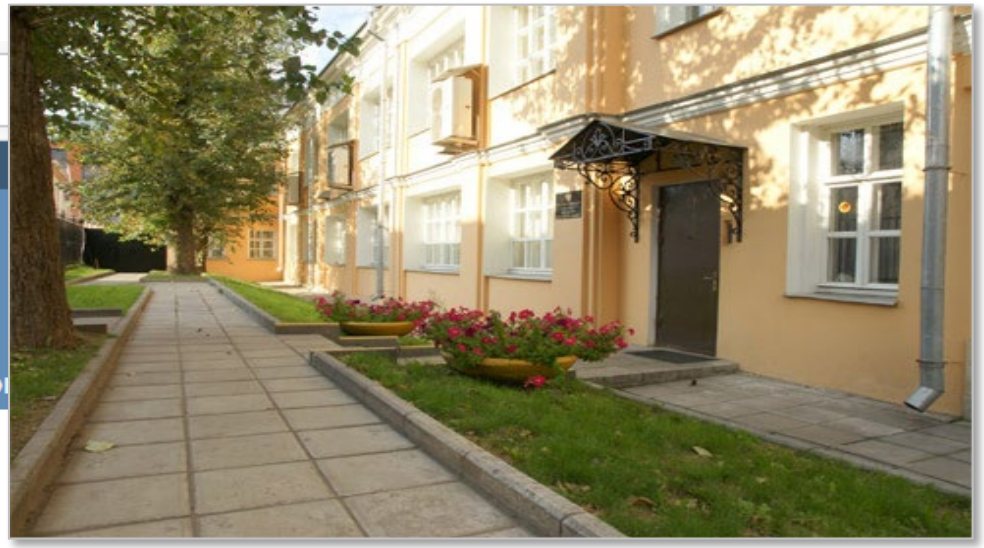
- Dispatcher module from Intel Quartus Prime
  - 2200 LOC, 8 sub-modules
  - SystemVerilog properties in a separate top level checker
- Retrascope only is able to check it formally! (small bound)
  - EBMC: doesn't support ***defparam***, local values for params
  - SymbiYosys: incorrect param redefinition
  - Verilog2SMV: incorrect sub-module instantiation, param redefinition

Contacts

Retrascope toolkit page: https://forge.ispras.ru/projects/retrascope

E-mail: retrascope-support@ispras.ru





Thank you!

Questions?