

COMPETITIONS

SV-COMP	Since 2022 Concurrency focus 3 configurations
Since 2023 Gold medal (array)	CHC-COMP
HWMCC	Planned AIGER (bit-level) BTOR2 (word-level)

PROPERTIES

- LTL properties (Timed) state reachability
- Signed integer overflow Array under- and overindexing
- Data races Dynamic memory safety
- Liveness (incl. termination) Concurrent reachability
- Petri Net props (deadlock, safety) Memory cleanup ...

PORTFOLIO

Dynamic Portfolio with
Algorithm Selection

Push-button verification
without FM expertise

Based on **theoretical**
knowledge and
empirical experience

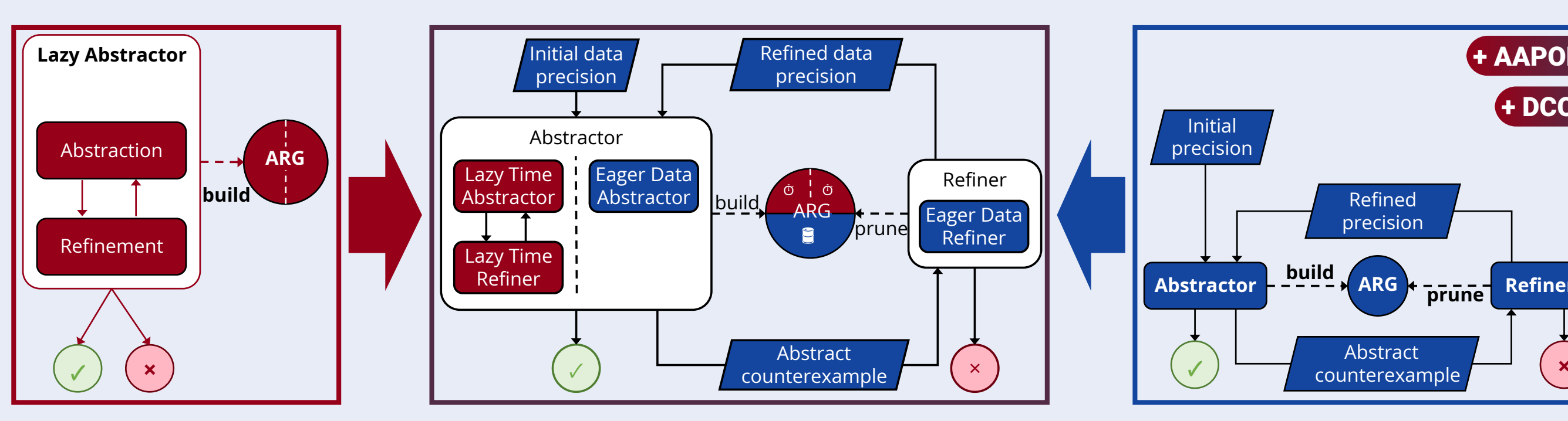
TRANSITION SYSTEM ANALYSES

Reverse → **Symbolic Transition System** → Abstract
Liveness-to-Safety

↓

K-IND BMC IMC IC3 GSAT

CEGAR: COMBINED LAZY AND EAGER ABSTRACTION



VERIFICATION WITH HORN CLAUSES

Reachability:
Invariants by construction (location, loop, function)

Termination:
Recurrence sets and ranking functions

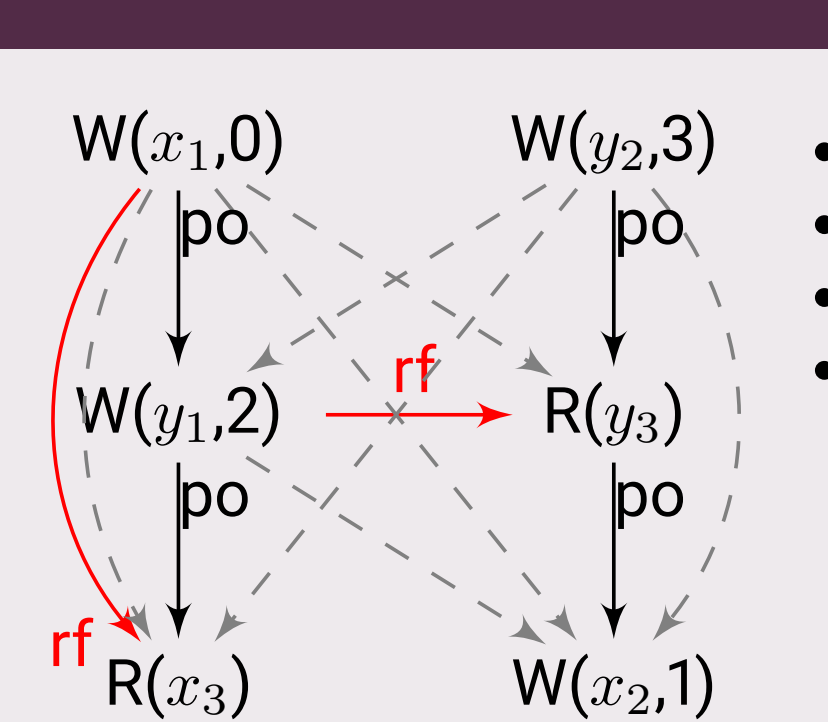
Multithreading:
Invariants for weakly consistent software (WiP)

Supported solvers: Z3, ELDARICA, GOLEM, ...

Language Frontends

Timed Automata
LLVM IR CAIGER
CHC PLC
Statecharts
Petri Nets BTOR2

ORDERING CONSISTENCY



- Happens-before partial orders
- Memory-Model-Aware Verification
- BMC via SMT encoding
- Supported decision procedures:
 - Integer Difference Logic
 - Step-by-step refinement
 - Propagator-based consistency

WSC (natively) SC (by extension) MCA (by modification)

Witness Generation

Traceable witnesses: Proofs and counterexamples

Software: Correctness and violation witnesses

Hardware: Certificates (WiP)

CHC: Models and counterexamples

Statecharts: Traces

Test generation:
CONCURRENTWITNESS2TEST

Direct SMT encoding:
termination

Witness Validation

WITNESS GENERATION & VALIDATION

SMT SOLVERS

Native solvers Thoroughly tested, mature integration
Minimal overhead, diverse OS-support

Broad solver support New API features (ex: User Propagator)

JavaSMT

SMT-LIB Flexible: any solver, any version
Slower interaction

INDUSTRIAL PROJECTS

thyssenkrupp Verifying a steer-by-wire system design	CERN PLCVERIF: verifying safety interlocks for superconducting test benches
NASA JPL, IncQuery Dynamic Verification Toolkit (Model Checking as a Service)	Prolan Railway interlocking system verification

COLLABORATIONS

SoSy-Lab	Summer sojourns Active collaboration
Seminar series Integrated research	FBK
CERN	PLCVERIF Summer students
V&V in Future CPS	ADVANCE

ONGOING/PLANNED EXTENSIONS

CAR/DAR Reimplement successful algorithms in THETA	Saturation Extensions and generalization of the saturation algorithm	Liveness Advanced liveness-checking algorithms (rlive, k-fair)
PROBTHETA Probabilistic Model Checking in THETA	Metasolver Online SMT-solver-portfolio to handle bugs and improve interpolants	ITP, PROOF Better interpolants with CHC-solvers, and proofs instead of unsat cores

CODE  github.com/ftsrg/theta	PAPERS  theta.mit.bme.hu/publications	WIKI  theta.mit.bme.hu/wiki	JAVADOC  theta.mit.bme.hu/javadoc	MAVEN  mavenrepository.com/artifact/hu.bme.mit.theta	DOCKER  github.com/ftsrg/packages	RELEASE  github.com/ftsrg/theta/releases/latest	FMTOOLS  fm-tools.bony-lab.org/#tool-theta
---	---	---	---	--	---	---	--