AVACS
Automatic Verification and Analysis of Complex Systems

Werner Damm
AVACS coordinator

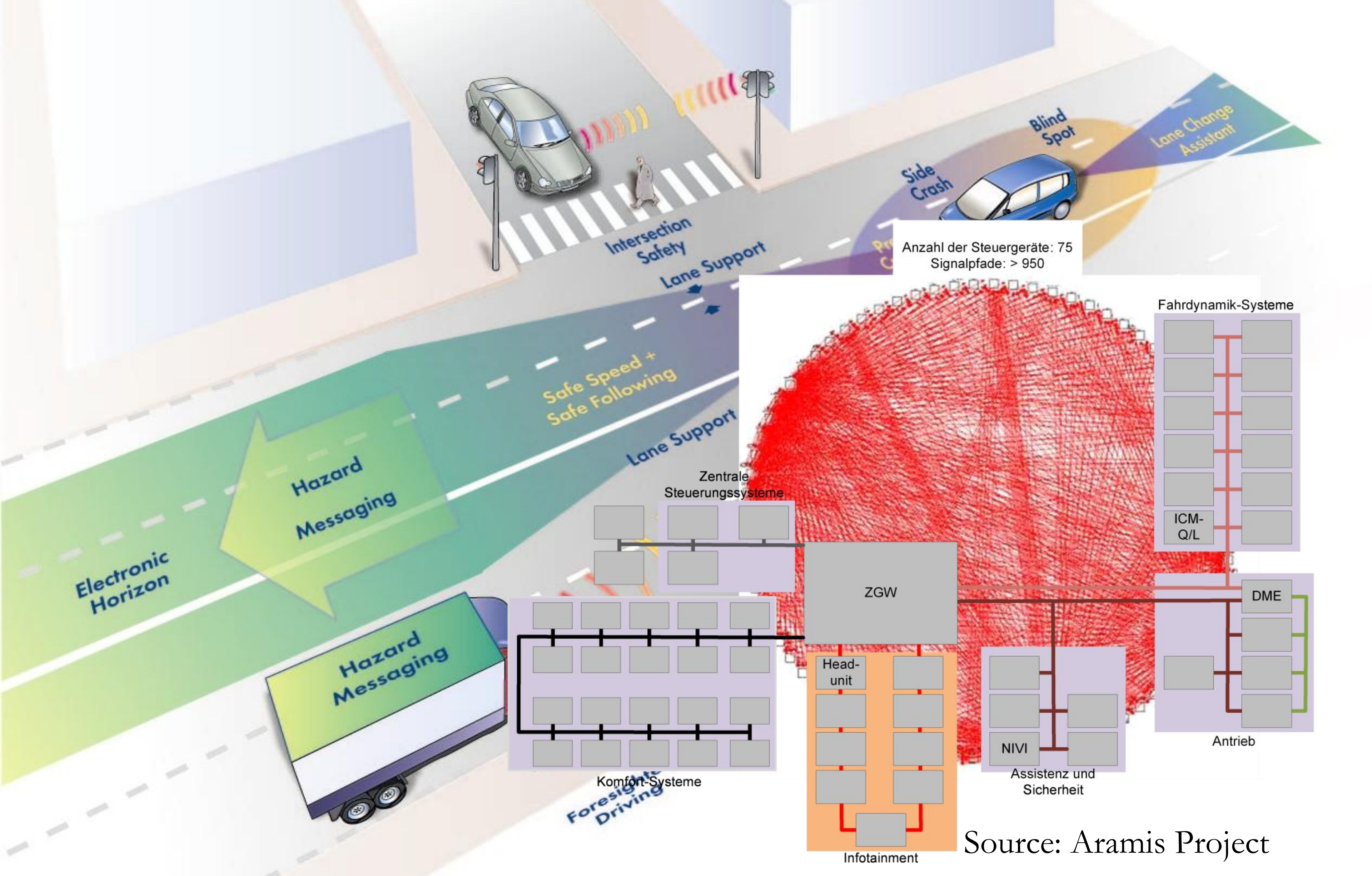
Carl von Ossietzky Universität Oldenburg
Albert-Ludwigs Universität Freiburg
Universität des Saarlandes

Structure of Presentation

The AVACS Vision

Highlights of Phase II

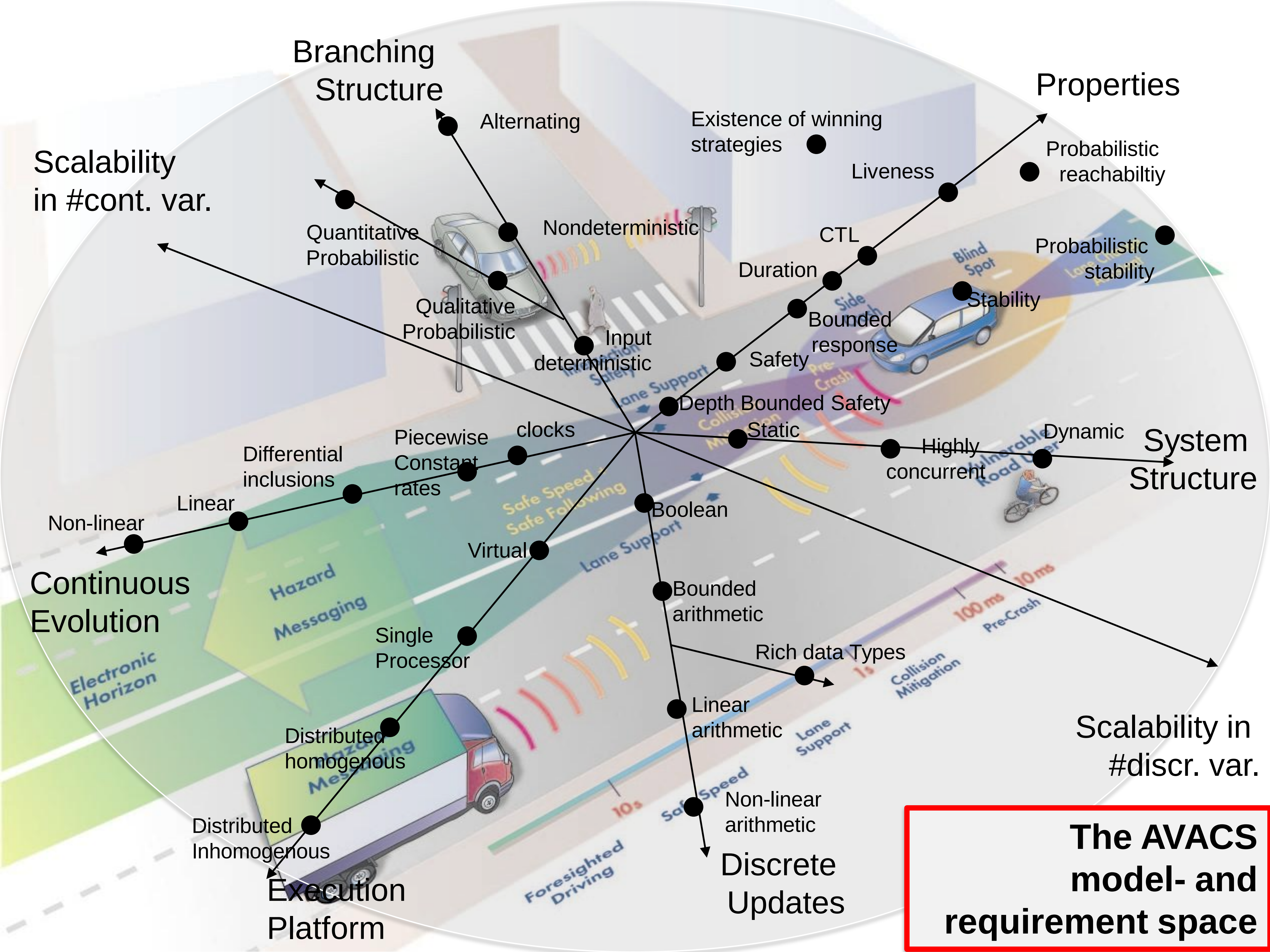
Complex Systems



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, …)


Branching Structure
Alternating
Nondeterministic
Input deterministic
Scalability in #cont. var.
Quantitative Probabilistic
Qualitative Probabilistic
Properties
Existence of winning strategies
Liveness
Probabilistic reachabiltiy
CTL
Probabilistic stability
Duration
Stability
Bounded response
Safety
Depth Bounded Safety
System Structure
Static
Highly concurrent
Dynamic
Continuous Evolution
clocks
Piecewise Constant rates
Differential inclusions
Linear
Non-linear
Boolean
Bounded arithmetic
Rich data Types
Linear arithmetic
Non-linear arithmetic
Discrete Updates
Scalability in #discr. var.
Execution Platform
Virtual
Single Processor
Distributed homogenous
Distributed Inhomogenous
The AVACS model- and requirement space

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

AVACS Competence Layers

Complex Systems

Embedded Transportation Applications

Models of Complex Systems

real-time – hybrid – distributed systems – system of systems

Combining V&A Technology

$(x_1 \wedge x_2 \wedge ...x_n \text{ for } s)$

$x_j \in$ V&A core technologies, $s \in$ systems

V&A Core Technologies

Abstraction – Decision Diagrams – Constraint Solving – Heuristic Search

Linear Programming – Model Checking – Lyapunov Method

Abstract Interpretation – SMT – Decision Procedures

Research

Areas

R

Real-Time

H

Hybrid

S

Coarse

Grain

System

Structure

Sites and PIs

Analysis of Extremely Large State Spaces

- Heuristic Planning
- SAT, BDD, AIG
- Directed Model Checking
- Abstraction

Bernd Becker
Bernhard Nebel
Andreas Podelski
Christoph Scholl

Systems & Models

- Domain Expertise
- Specification and verification of embedded systems
- Control, Real-Time, Hybrid
- SAT(T)

Werner Damm
Martin Fränzle
Ernst-Rüdiger Olderog
Oliver Theel

CARL VON OSSIETZKY universität OLDENBURG

ALBERT-LUDWIGS UNIVERSITÄT FREIBURG

UNIVERSITÄT DES SAARLANDES

+ MPI

Ernst Althaus
Bernd Finkbeiner
Sebastian Hack
Holger Herrmanns
Jan Reinecke

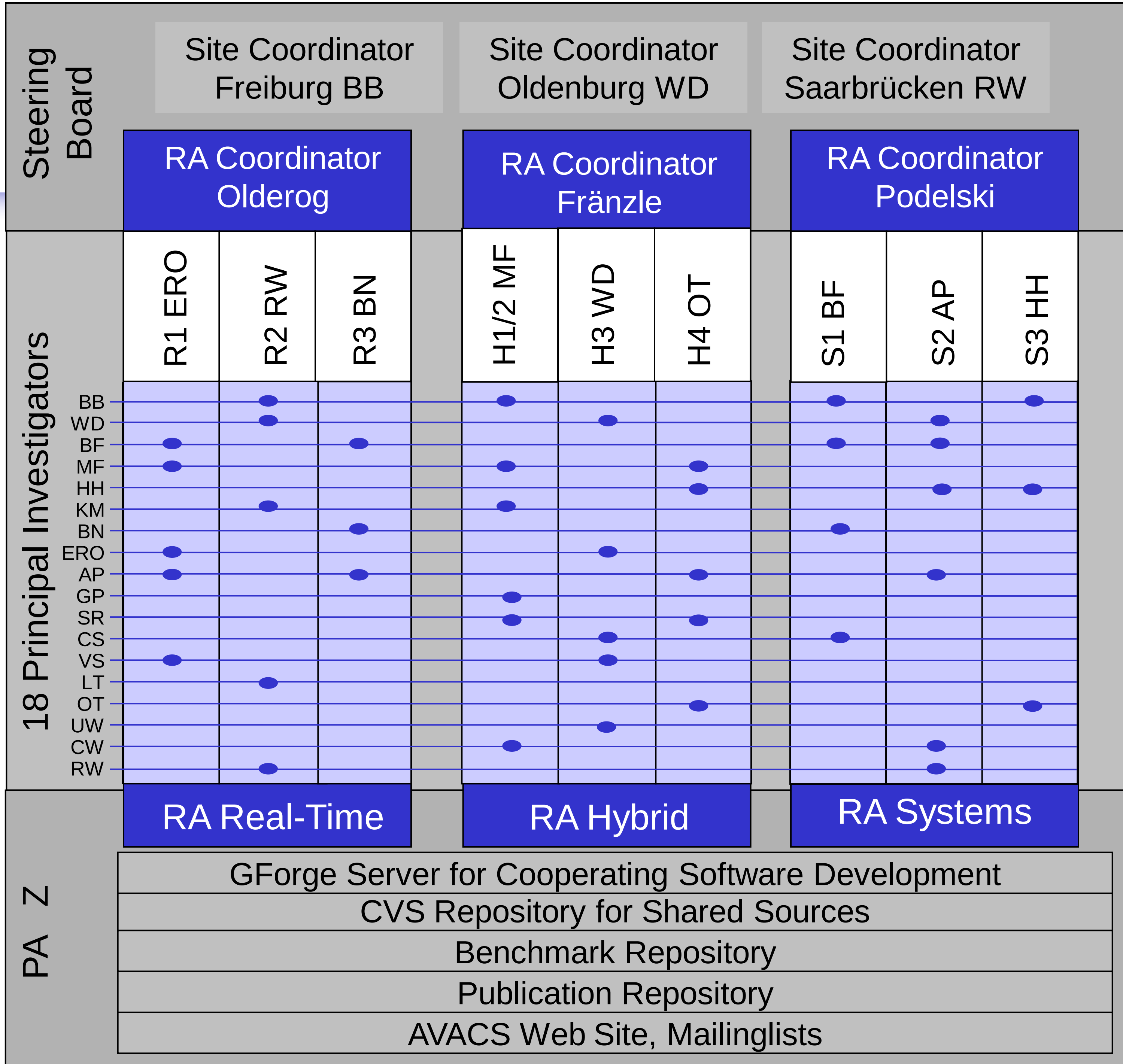
Viorica Sofrie-Stokkermanns
Uwe Waldmann
Christoph Weidenbach
Reinhard Wilhelm
Verena Wolf

Algorithmic Aspects

- Decision Procedures
- Constraint solving
- ILP
- Probabilistic model checking
- Abstract Interpretation
- Shape Analysis

Three funding periods à 4 years
funding third period 2012-2015 9,6 Mill Euro

Project Structure

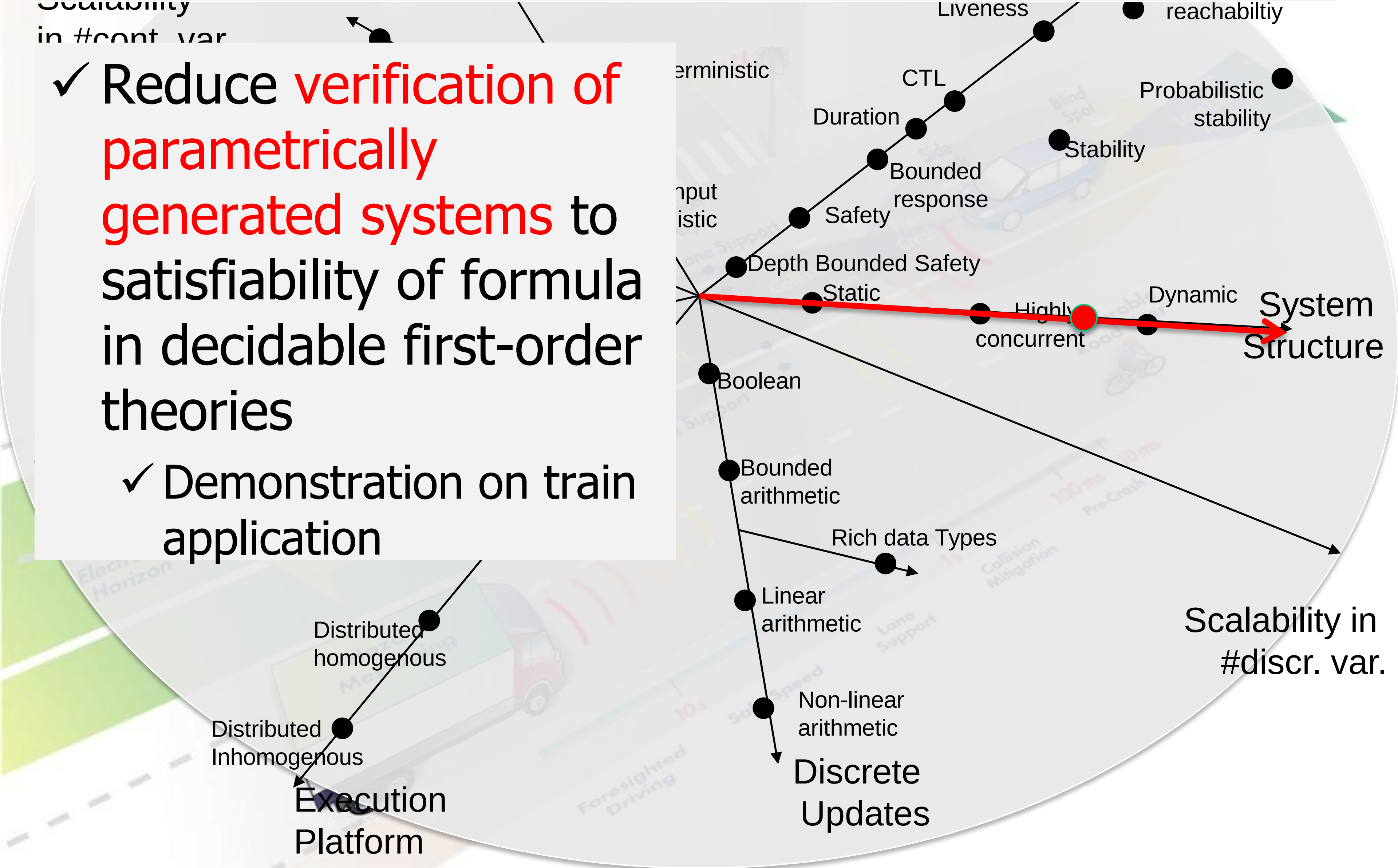


UNIVERSITÄT DES SAARLANDES

Selected Highlights of Phase II

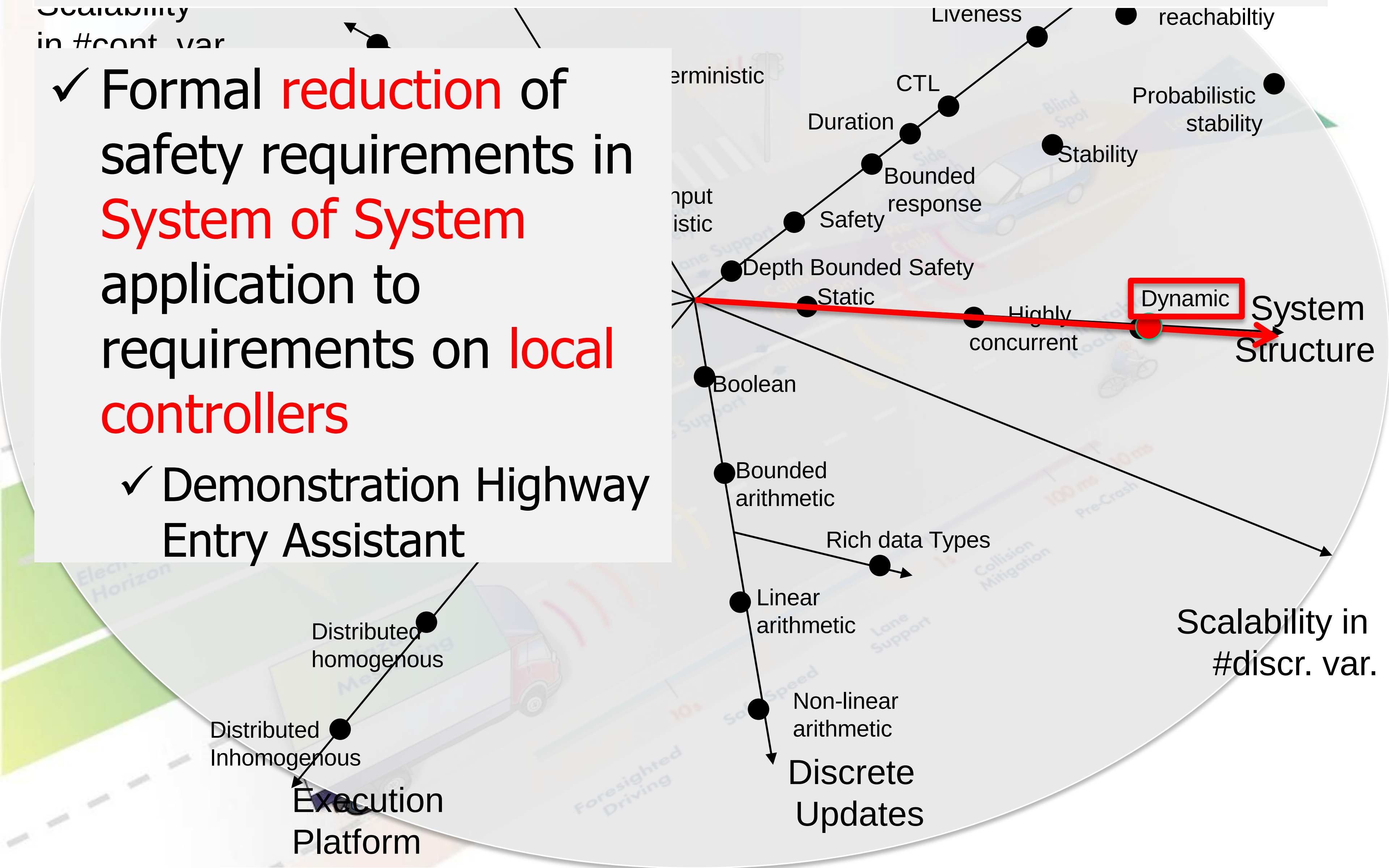
Selected Highlights Phase II: System Structure

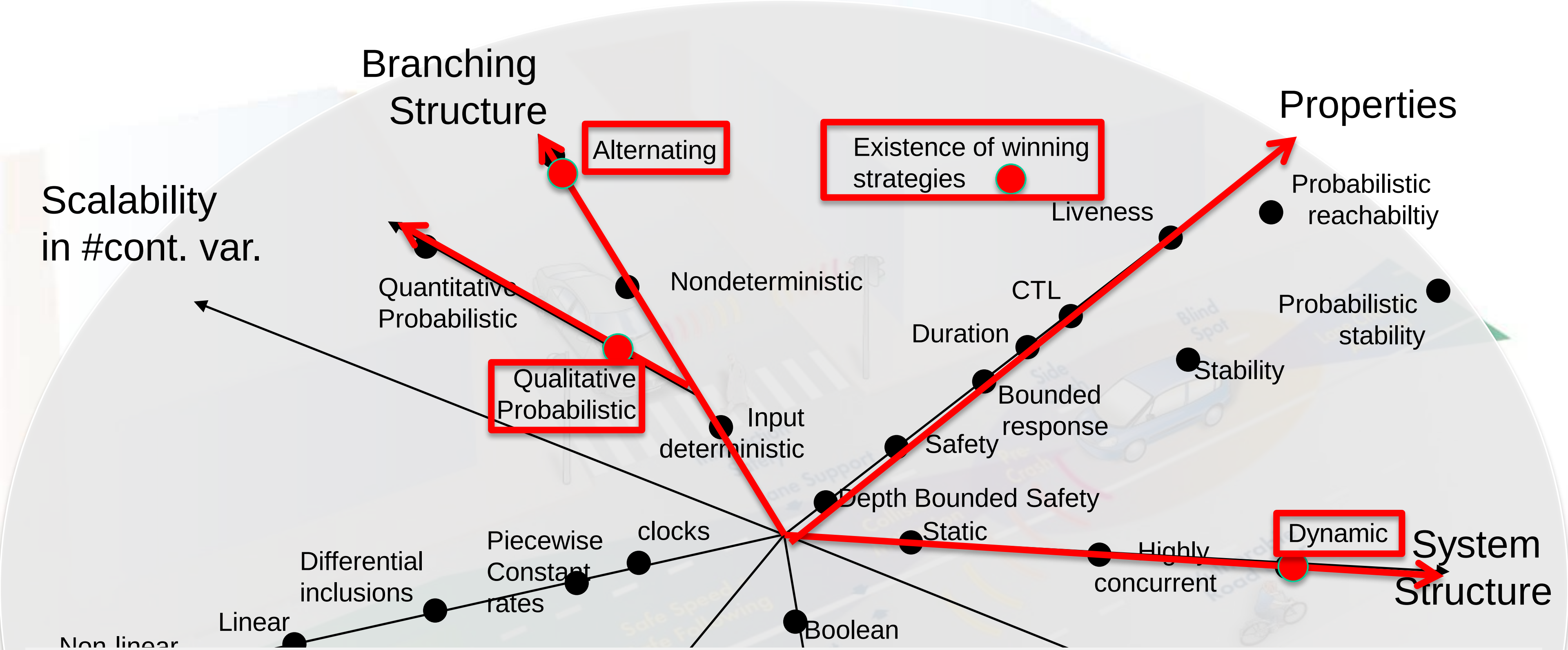
- ✓ Reduce verification of parametrically generated systems to satisfiability of formula in decidable first-order theories
  - ✓ Demonstration on train application



Selected Highlights Phase II: System Structure

- ✓ Formal reduction of safety requirements in System of System application to requirements on local controllers
  - ✓ Demonstration Highway Entry Assistant

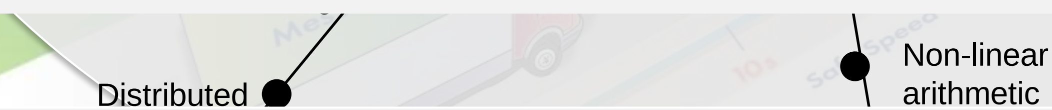




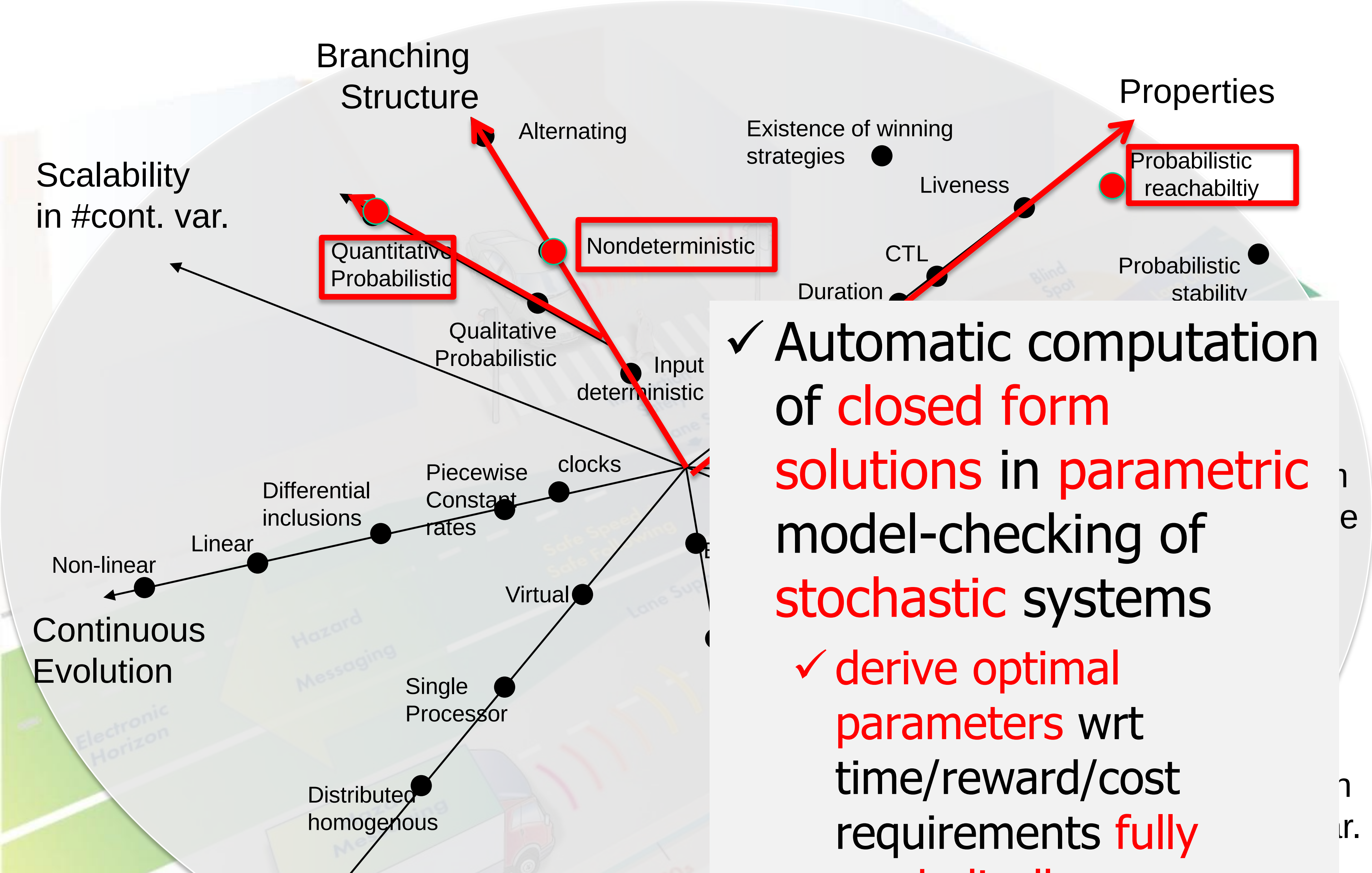
✓ Formal model of cooperating transportation systems catering for failures, abstracted car dynamics, evolving shapes

✓ Formal automatic synthesis of winning cooperation strategies

✓ Demonstrated on Highway-Entry Assistance System



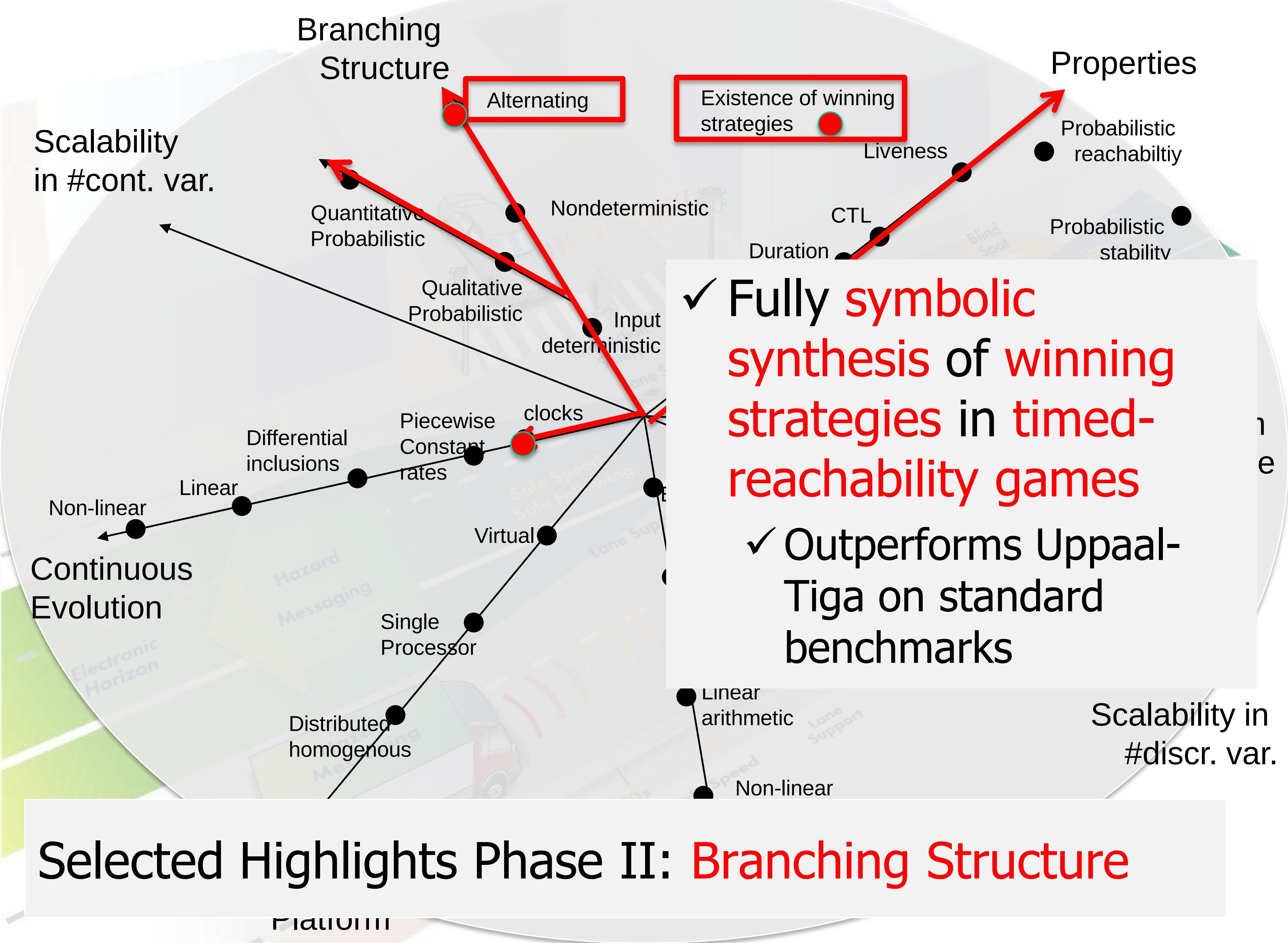
Selected Highlights Phase II: Branching/System structure



- ✓ Automatic computation of closed form solutions in parametric model-checking of stochastic systems
  - ✓ derive optimal parameters wrt time/reward/cost requirements fully symbolically

Selected Highlights Phase II: Branching Structure

Selected Highlights Phase II: Branching Structure

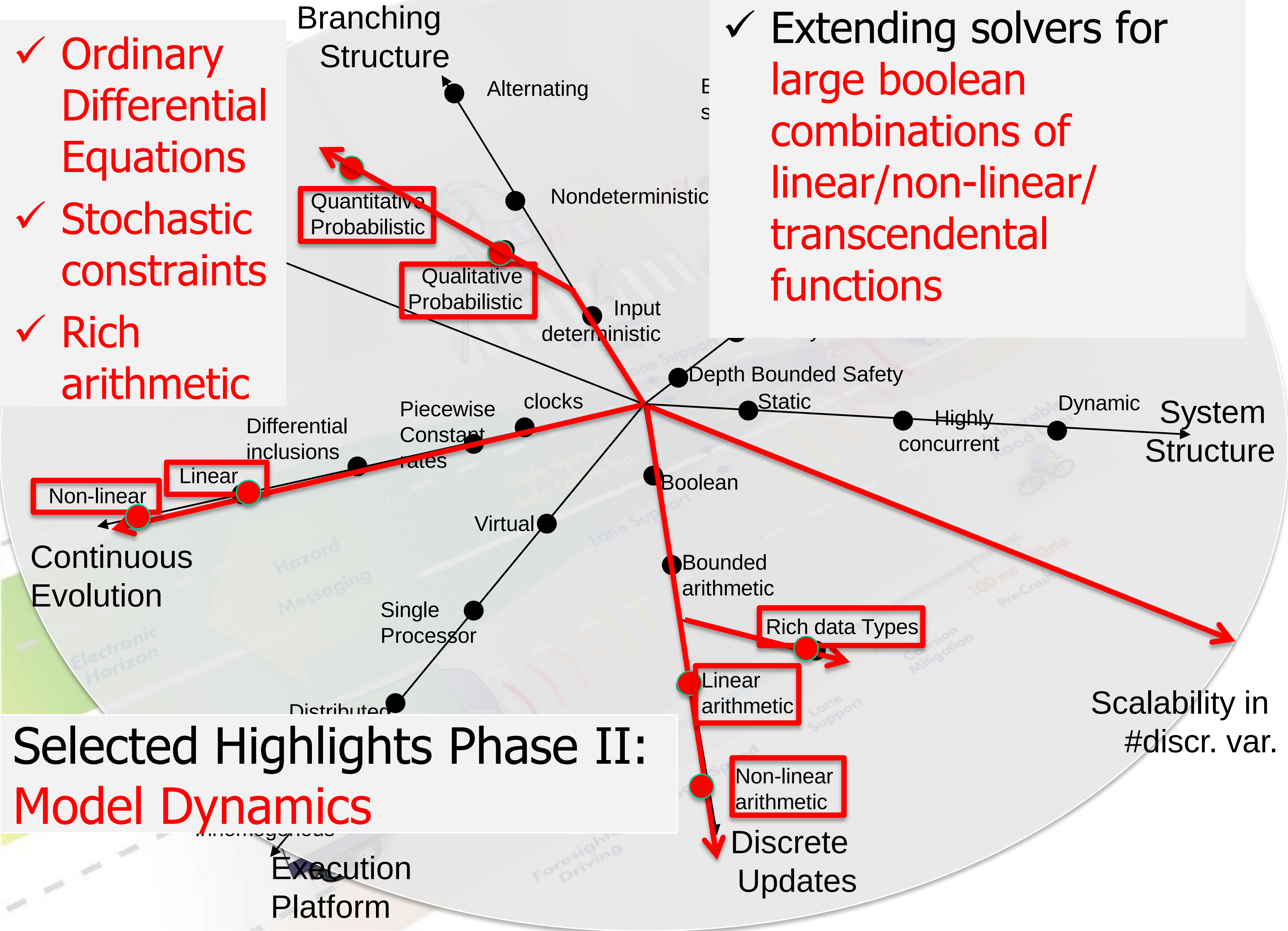


- ✓ Fully symbolic synthesis of winning strategies in timed-reachability games
  - ✓ Outperforms Uppaal-Tiga on standard benchmarks

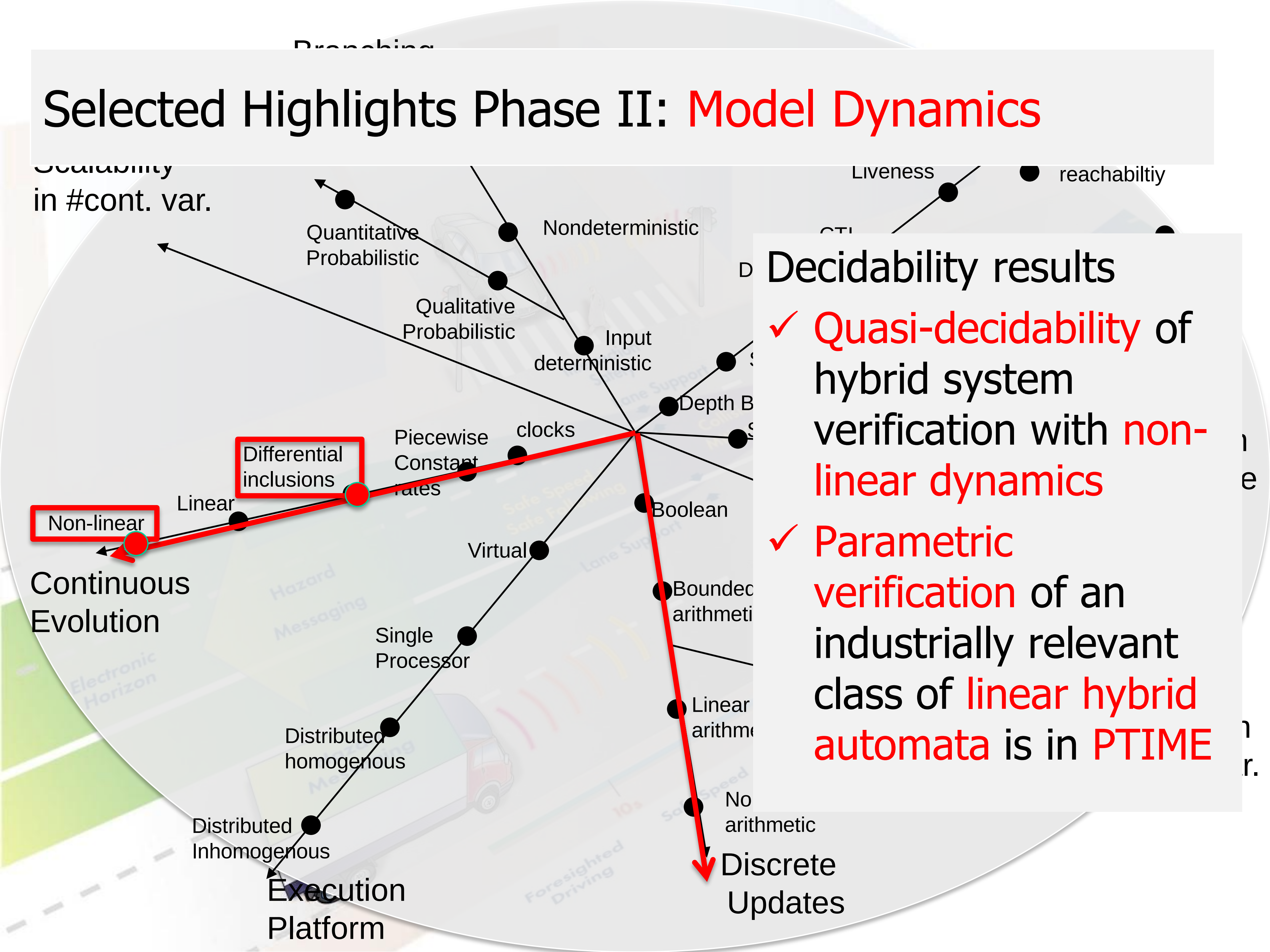
Selected Highlights Phase II: Model Dynamics

- ✓ Ordinary Differential Equations
- ✓ Stochastic constraints
- ✓ Rich arithmetic

- ✓ Extending solvers for large boolean combinations of linear/non-linear/ transcendental functions



Selected Highlights Phase II: Model Dynamics

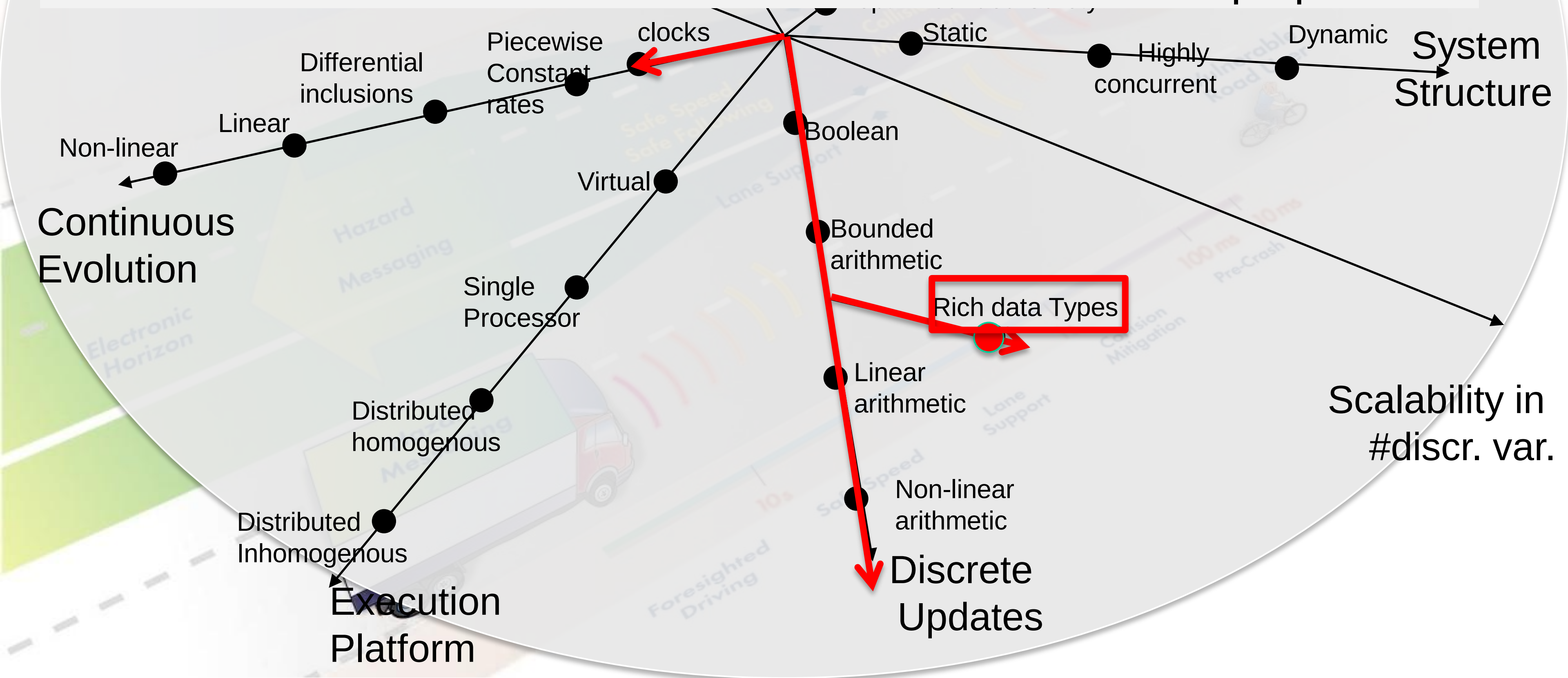


Decidability results

- ✓ Quasi-decidability of hybrid system verification with non-linear dynamics
- ✓ Parametric verification of an industrially relevant class of linear hybrid automata is in PTIME

Selected Highlights Phase II: Model Dynamics

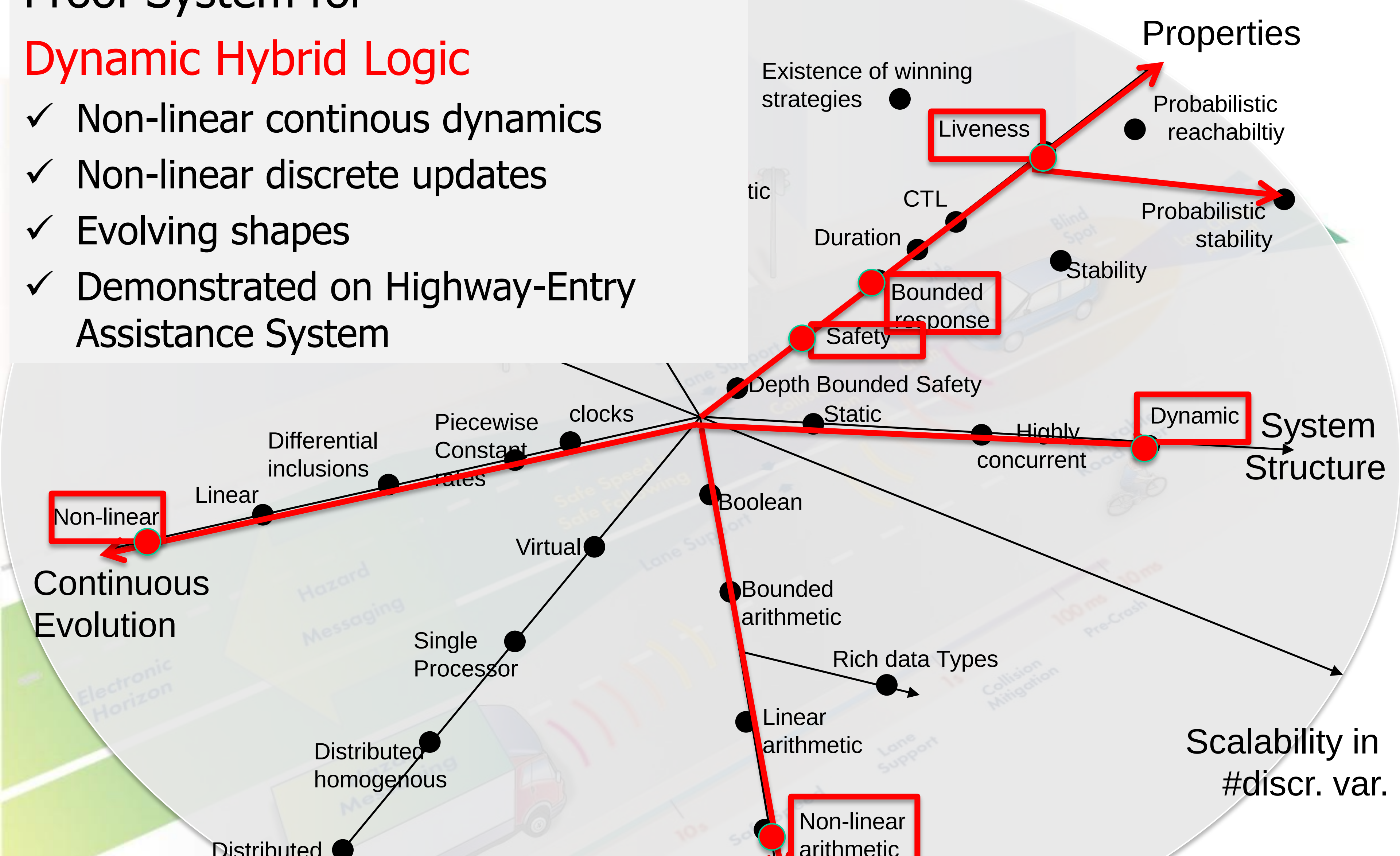
- ✓ Verification of timed systems with complex types
  - ✓ lists, arrays, pointers, sets
  - ✓ primitive recursive functions
  - √ uninterpreted functions over reals satisfying monotonicity and boundedness properties



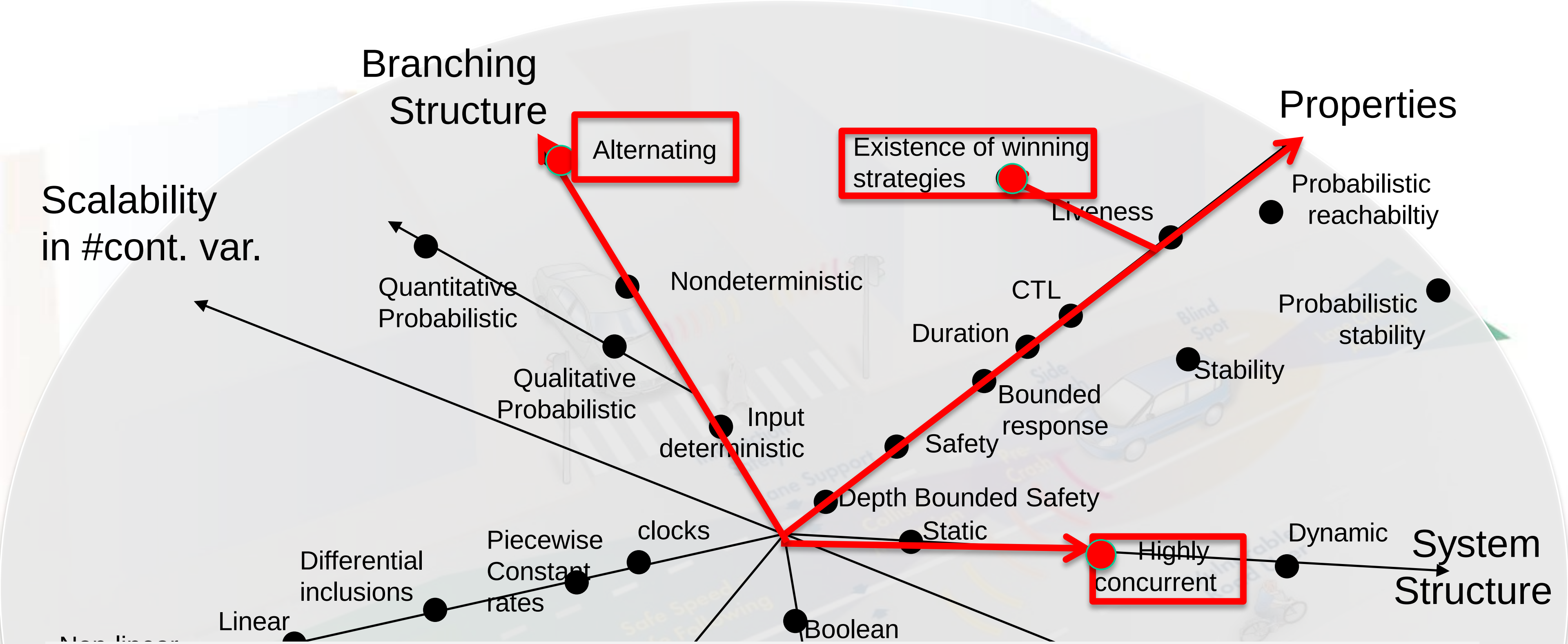
Proof System for

Dynamic Hybrid Logic

- ✓ Non-linear continous dynamics
- ✓ Non-linear discrete updates
- ✓ Evolving shapes
- ✓ Demonstrated on Highway-Entry Assistance System



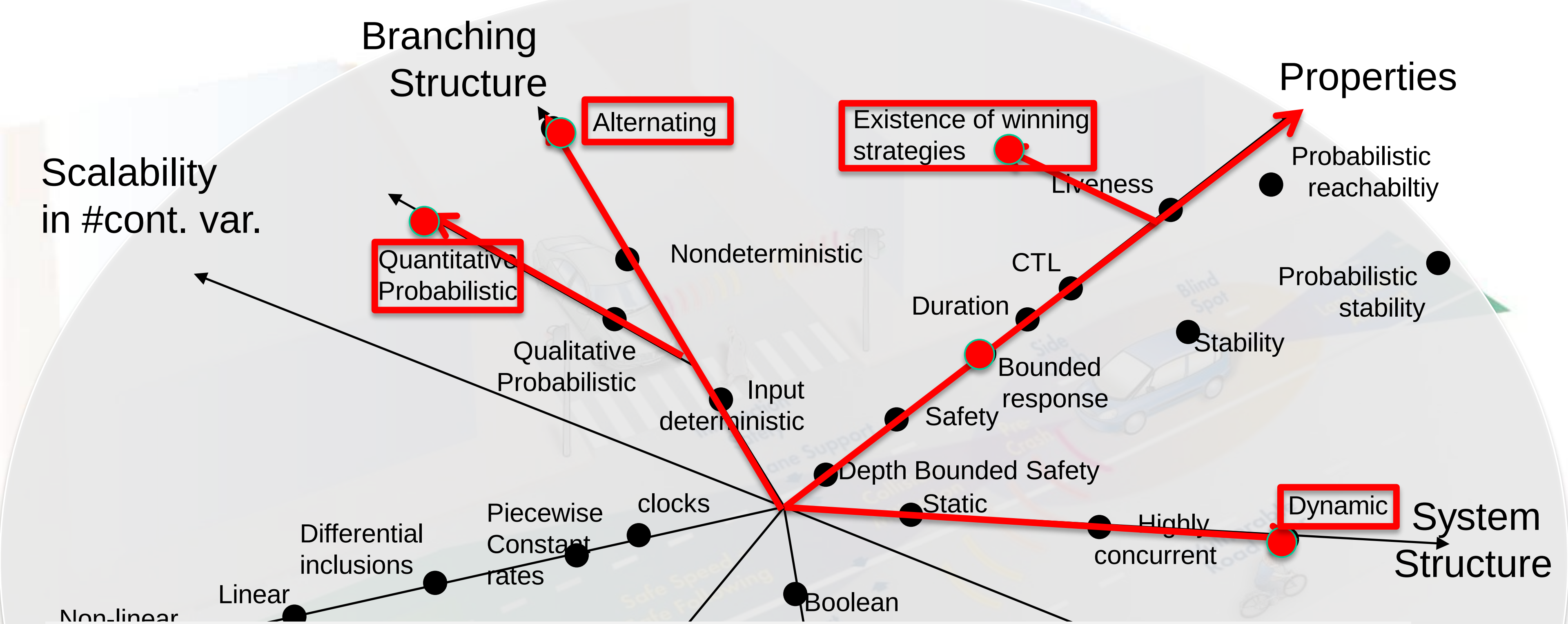
Selected Highlights Phase II: Specification Logics



Coordination logic

- ✓ Logical representation for all decidable distributed realizability problems
- ✓ Quantification over strategies with incomplete information
- ✓ Explicates level of informedness given to strategies

Selected Highlights Phase II: Specification Logics



Specification Logic for SoS applications

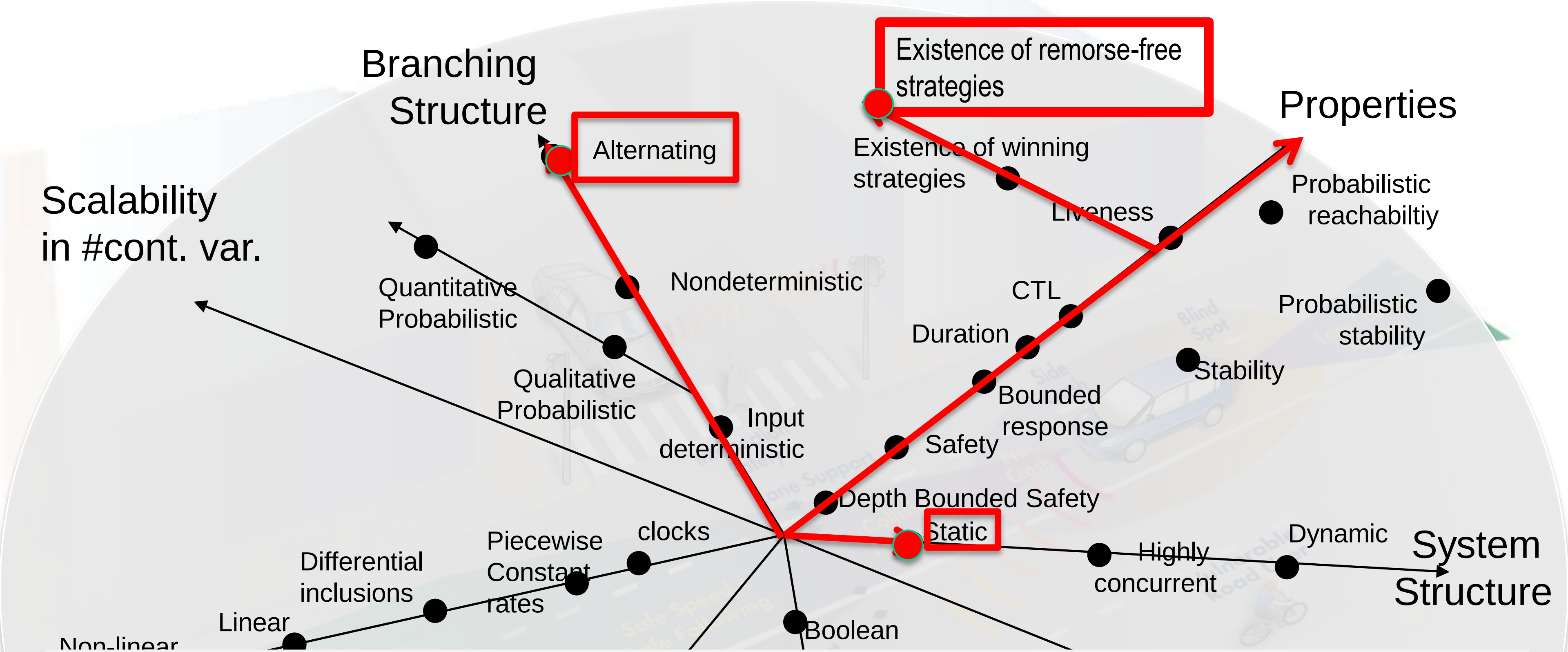
- ✓ First-order quantification over agents
- ✓ Quantification over strategies with sets of agents
- ✓ For time-bounded probabilistic reachability of SoS configurations
- ✓ Demonstrated on Highway Entry Assistance Systems

ability in iscr. var.

Distributed

arithmetic

Selected Highlights Phase II: Specification Logics



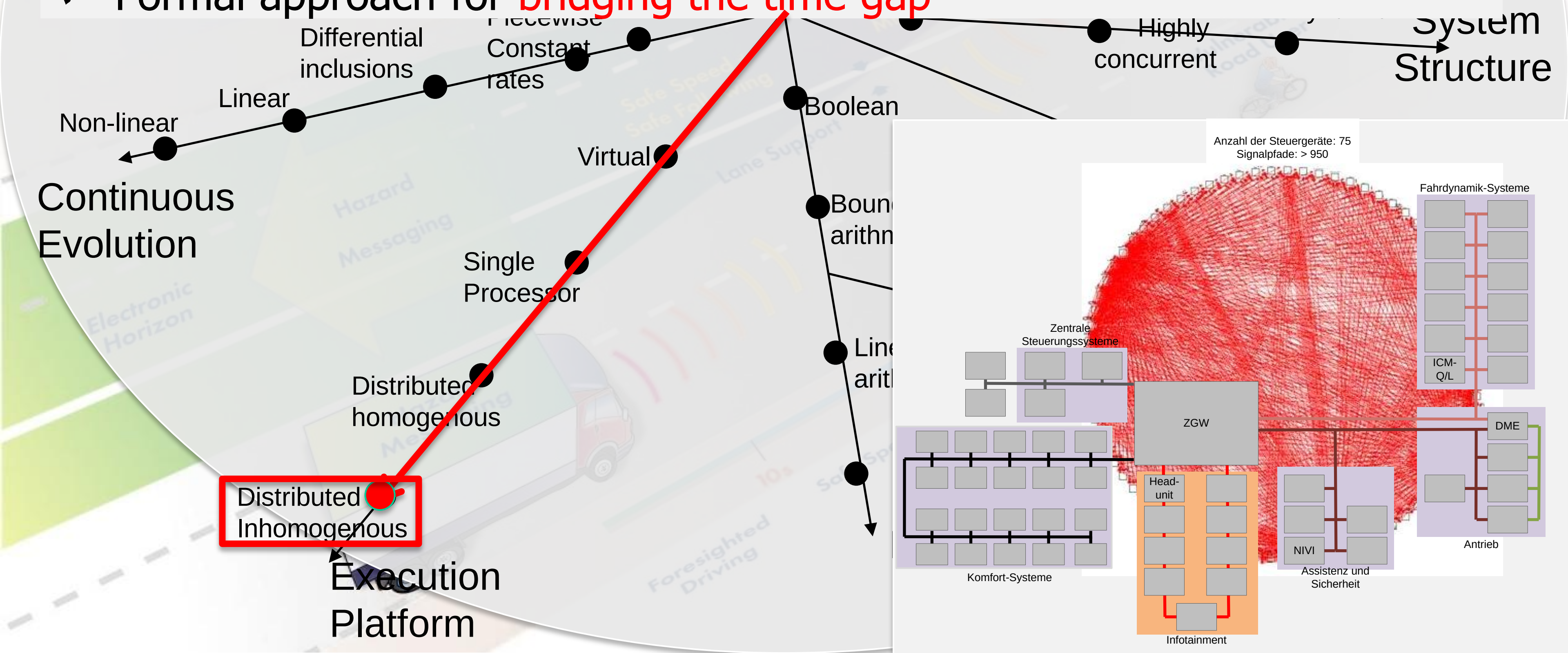
Reasoning about Remorse

- ✓ Replacing the un-achievable concept of „winning strategy“ by new concept of remorse-free strategies: wrt a given world model and given set of observables, no other strategy can do better in comparable situations (i.e. environment moves)
- ✓ Allows to define and test for optimal world models

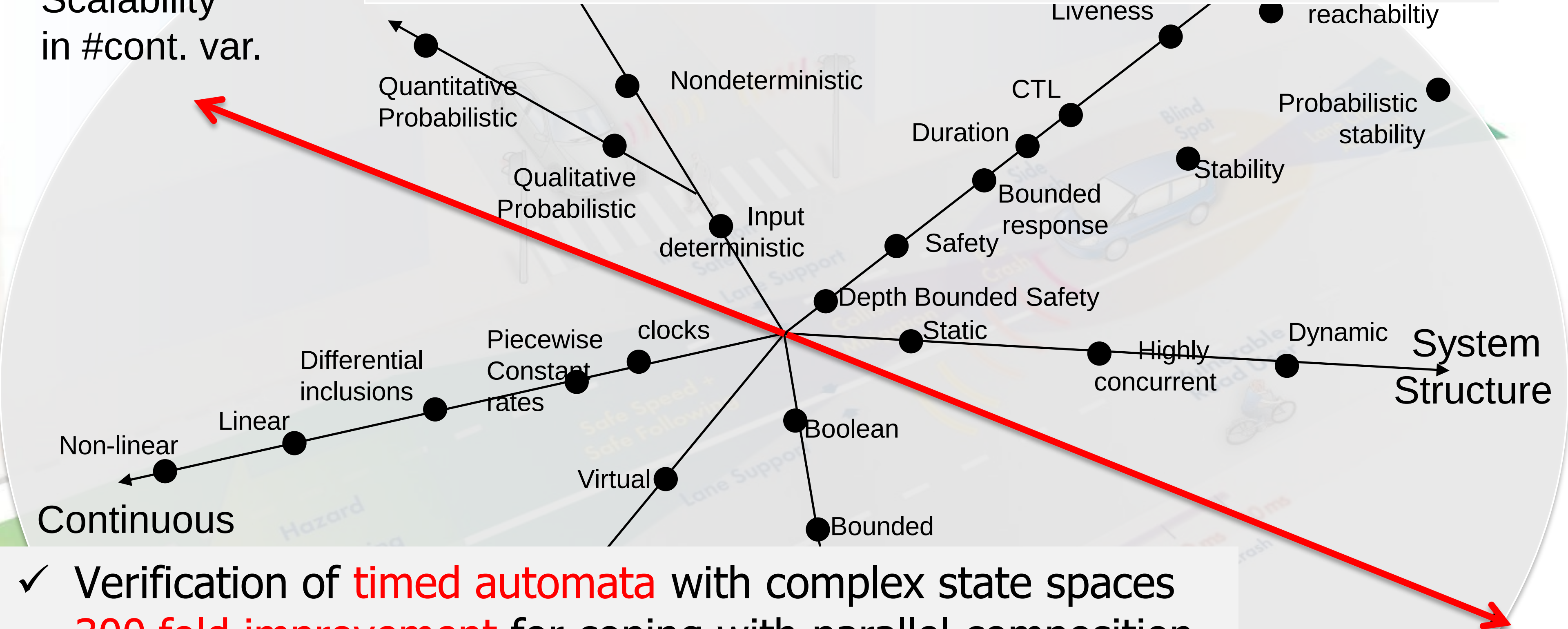
Selected Highlights Phase II: Specification Logics

Selected Highlights Phase II: Execution Platform

- ✓ Increased scope and precision of safe timing certificates
  - ✓ Distributed hierarchical inhomogenous bus architectures
  - ✓ Complex processors with out-of-order execution and speculation
- ✓ Developed first formal notion of predictability and identified classes of predictable architectures
- ✓ Formal approach for bridging the time gap

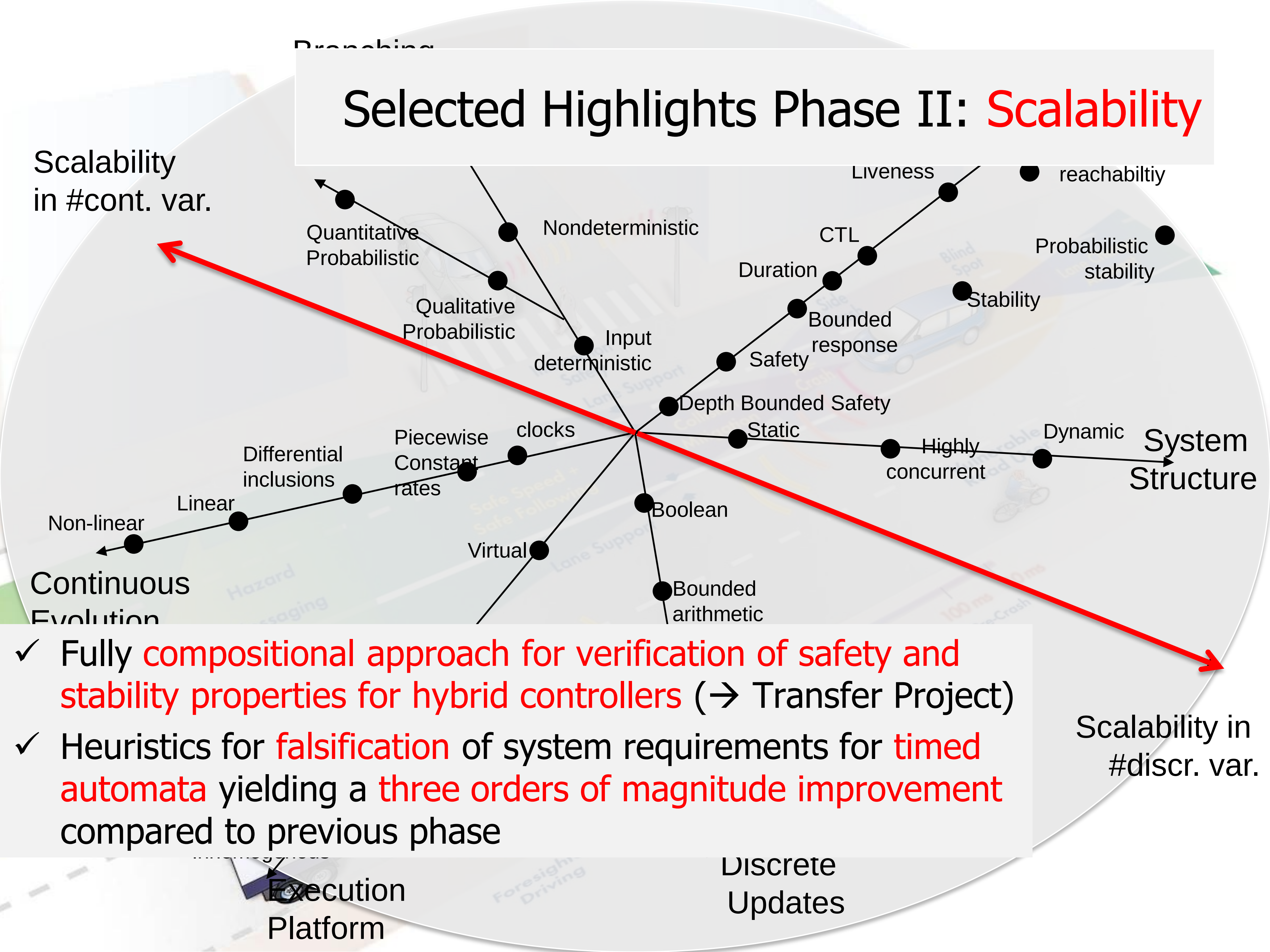


Selected Highlights Phase II: Scalability



- ✓ Verification of timed automata with complex state spaces 300 fold improvement for coping with parallel composition
- ✓ Fully symbolic and precise verification of hybrid systems with large discrete state spaces outperforming Phaver
  - ✓ Dam controller with 11 real variables and 2^{100} discrete states verified in 80 seconds
- ✓ Tuning stochastic SMT solving for applications with up to 24 million discrete states and 23 real variables

Selected Highlights Phase II: Scalability



- ✓ Fully compositional approach for verification of safety and stability properties for hybrid controllers (→ Transfer Project)
- ✓ Heuristics for falsification of system requirements for timed automata yielding a three orders of magnitude improvement compared to previous phase

Increasing Automation

- 67 tools supporting the AVACS approach to the analysis of complex systems
- see www.avacs.org/ tools