AVACS*
Automatic Verification and Analysis of Complex Systems
Selected Results first funding phase

Werner Damm
AVACS coordinator

***see www.avacs.org**

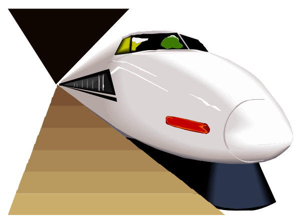
Carl von Ossietzky universität Oldenburg
Albert-Ludwigs Universität Freiburg
Universität des Saarlandes

AVACS Structure

65 Research Assistants,
29 of which are funded by the DFG

- Werner Damm
- Martin Fränzle
- Ernst Rüdiger Olderog
- Oliver Theel

- Bernd Becker
- Bernhard Nebel
- Andreas Podelski
- Christoph Scholl



DFG Funding:
~ 2.5 M € /Year
4+4+4 years, 1.1.2004

- Bernd Finkbeiner
- Holger Hermanns
- Reinhard Wilhelm

- Kurt Mehlhorn
- Viorica Sofronie-Stokkermann
- Uwe Waldmann
- Christoph Weidenbach

Associated PIs

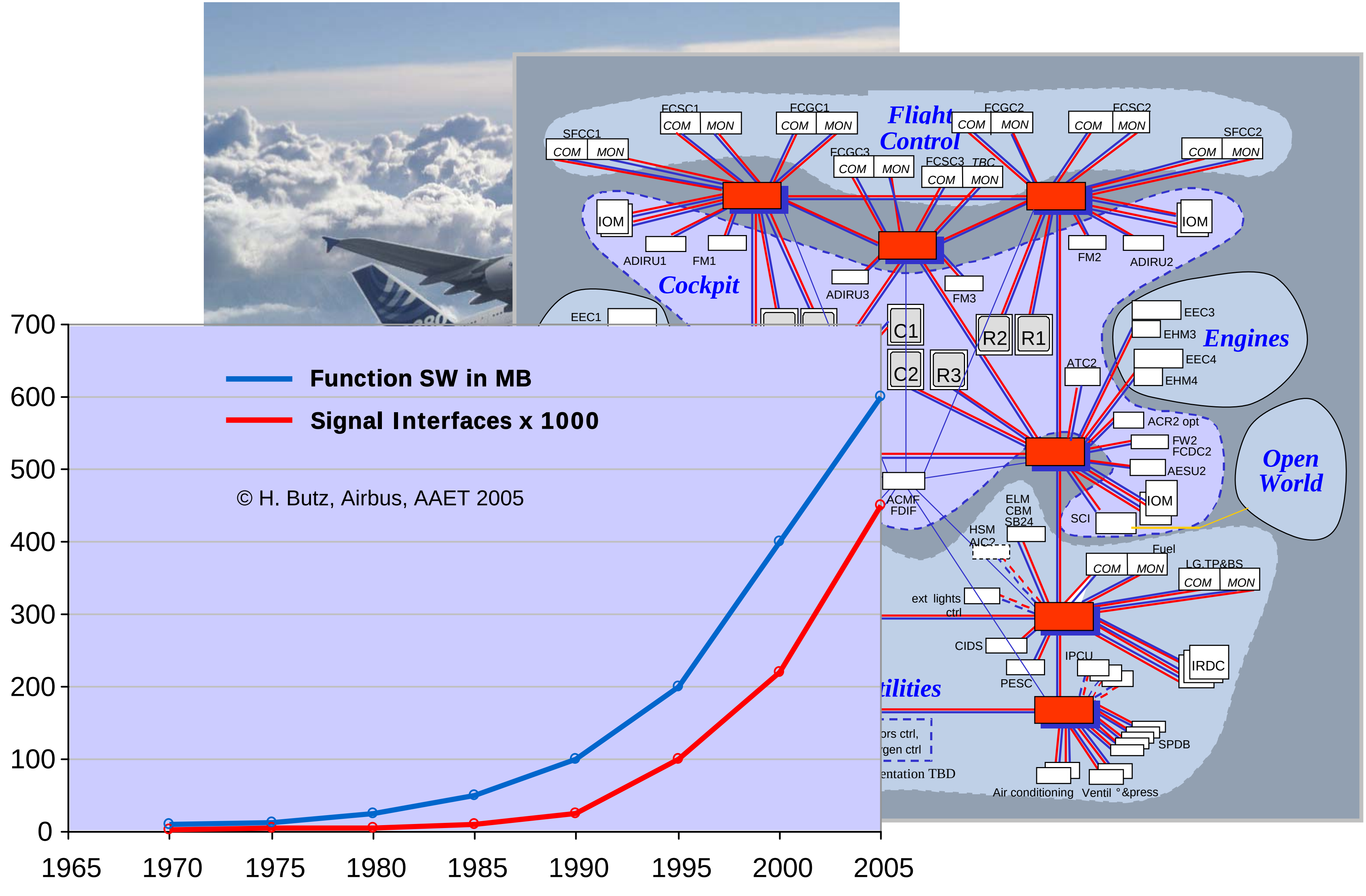
- George Pappas, U of Pennsylvania
- Stephan Ratschan Academy of Sciences of the Czech Republic
- Lothar Thiele ETHZ

Structure of Presentation

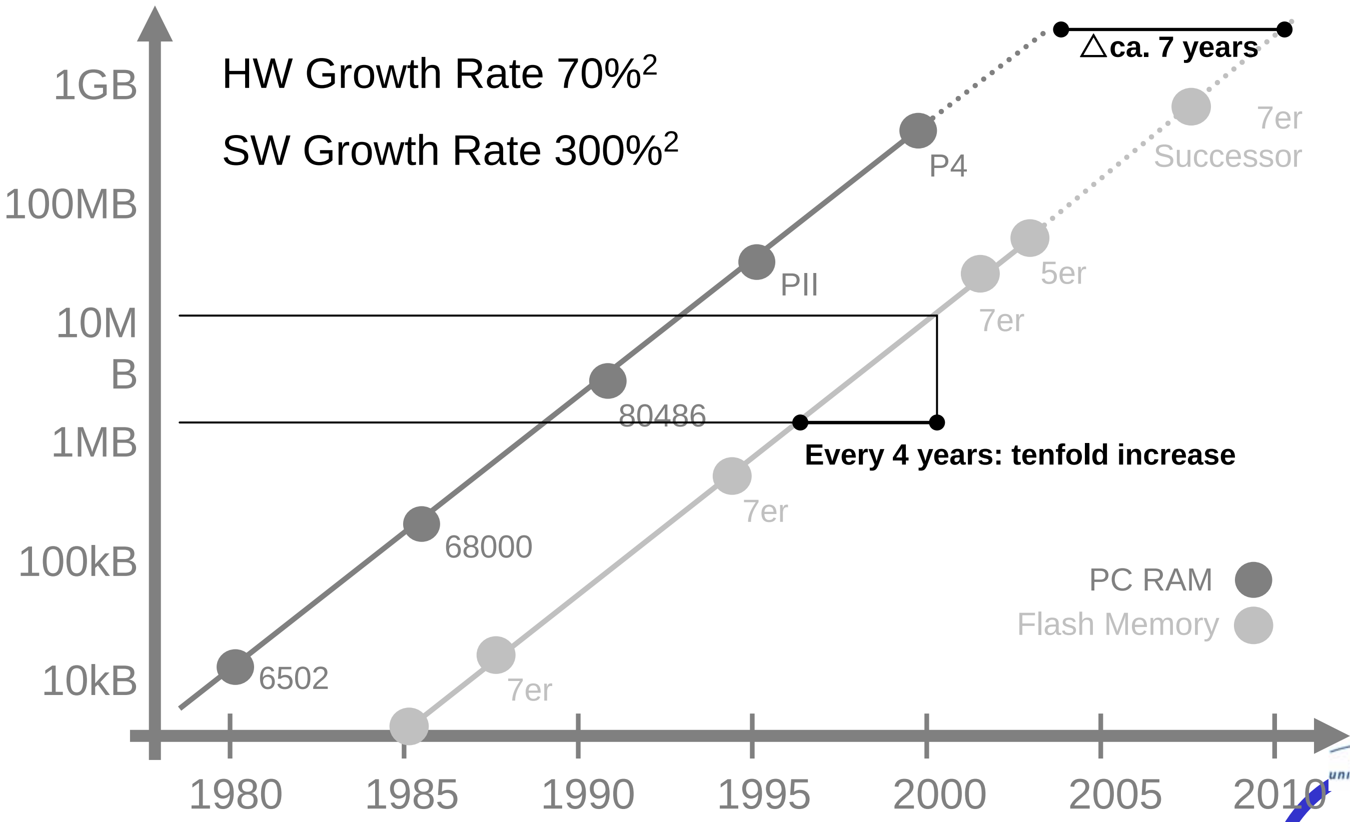
- Application Challenges
- Where we are: Highlights of Phase I
- Conclusion

carl von ossietzky universität OLDENBURG
ALBERT-LUDWIGS UNIVERSITÄT FREIBURG
UNIVERSITÄT DES SAARLANDES

Exponential Growth in Complexity: Avionics



Exponential Growth in Complexity – Memory Usage in Vehicles[1]



[1] H.-G. Frischkorn, BMW [2]W. Schleuter, Audi

Sample Automotive Applications: Active and Passive Safety Systems

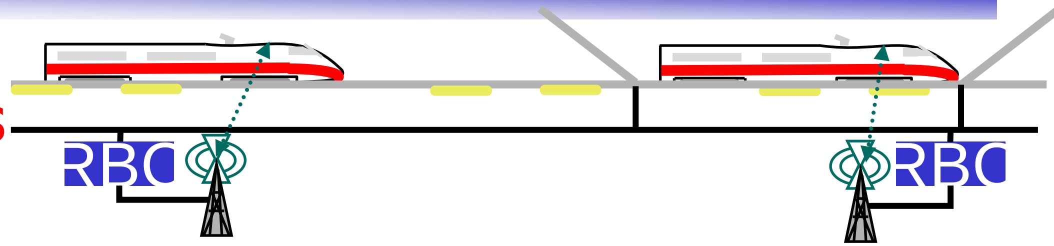
				Crash		
Scope	Reduction of accident probability		Get ready for the accident		Mitigation of accident impact for passengers	
System	**pro.pilot** ▪ Blind Spot Detection ▪ Lane Departure Warning ▪ Night Vision ▪ Adaptive Cruise Control ▪ Driver Monitoring	**Vehicle Dynamics** ▪ ABS ▪ Anti Slip Control (e.g. ESP)	**Pre-Crash system**		**Restraint System** ▪ Front Airbag ▪ Side Airbag	**Post-Crash system** ▪ GSM ▪ Telemetrics Rescue
Situation	Normal Driving	Critical Condition	Pre-Crash		In-Crash	Post-Crash
	Accident avoidance				Accident happens	

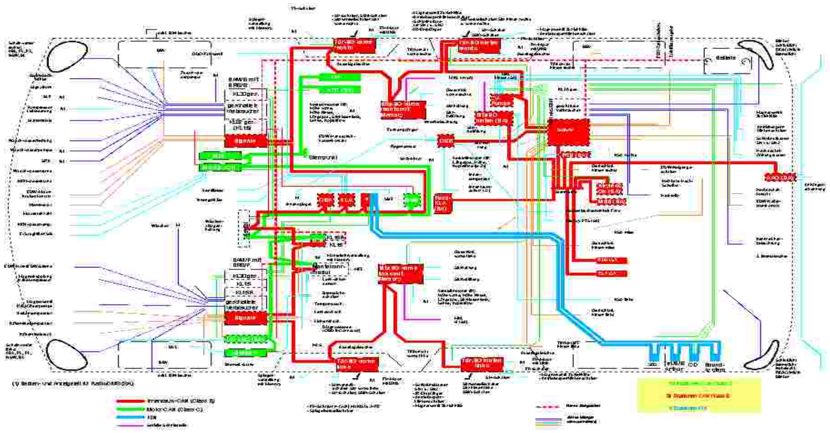
The Application Context

- Complex Embedded Systems are key enablers for safe flight and safe ground transportation
- Exponential growth in system complexity is a challenge for quality assurance
- In choosing benchmarks from embedded transport applications, AVACS contributes to meeting forthcoming requirements of pertinent safety standards
  - "If a model-based approach meets the criteria to be considered a formal method, formal verification techniques such as reasoning or proof can be used to meet certification objectives. . . " (from moderated forum on DO 178 C definition)

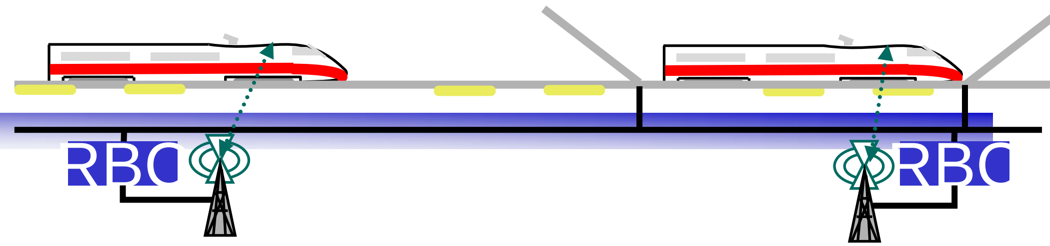
Automatic Verification of Complex Systems: Models

- Extremely Heterogeneous Model Space
  - Systems of Systems
  - ....
  - Cycle Accurate models of HW
- Comprehensive and Scalable Verification requires
  - Relating Models at different Design Levels
  - Identification of typical model characteristic





Requirements



Heterogeneous Requirement Space

- Reliability

  „probability of total a/c failure is less than 10^{-9} per flight hour"

- Coordination

  "Crossing will grant access if secured"

- Local Control

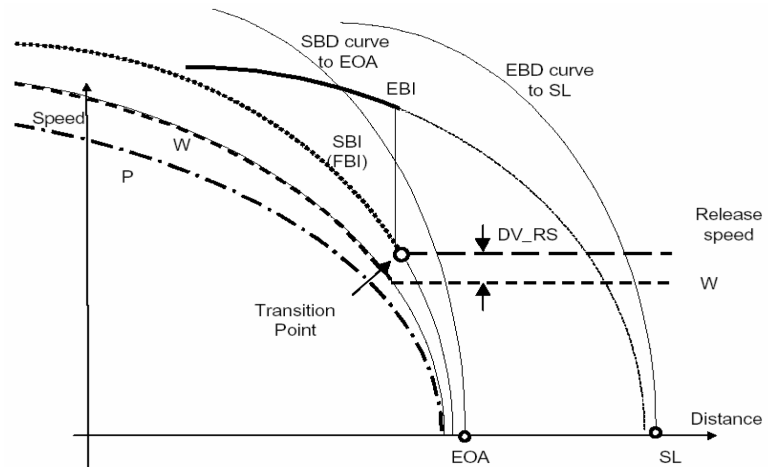
  "The train will never run faster than permitted speed"

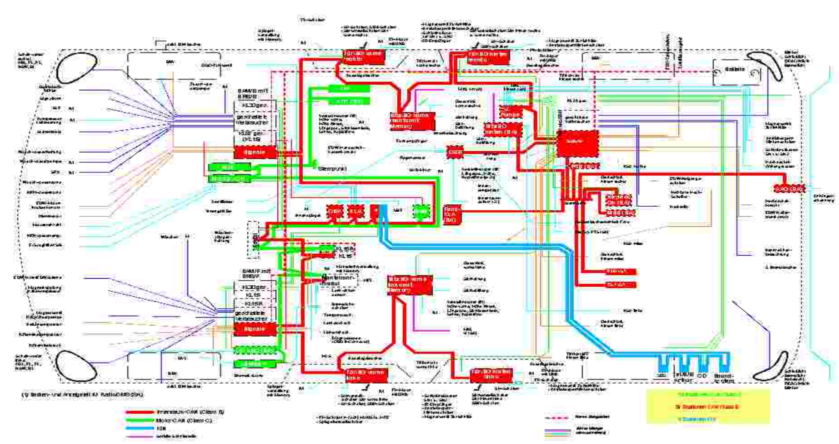
  "enforce brake profile"

- Real-Time

  "When receiving unconditional emergency stop message the train shall be tripped within 5 msec"

  "Brake curve control task activated every 30 msecs"





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

Carl von Ossietzky universität Oldenburg

Albert-Ludwigs Universität Freiburg

Universität des Saarlandes

AVACS

Holistic System Verification

AVACS Competence Layers

Complex Systems
Embedded Transportation Applications

Models of Complex Systems
real-time – hybrid –distributed system – systems of systems

Combining V&A Technology
(x1&x2& …xn for s)*
xj ∈ v&a kernel technologies, s ∈ systems

V&A Core Technologies

Abstraction – Decision Diagrams – Constraint Solving – Heuristic Search – Linear Programming – Model Checking – Lyapunov Method – SMT – Decision Procedures

Verification of Hybrid Systems

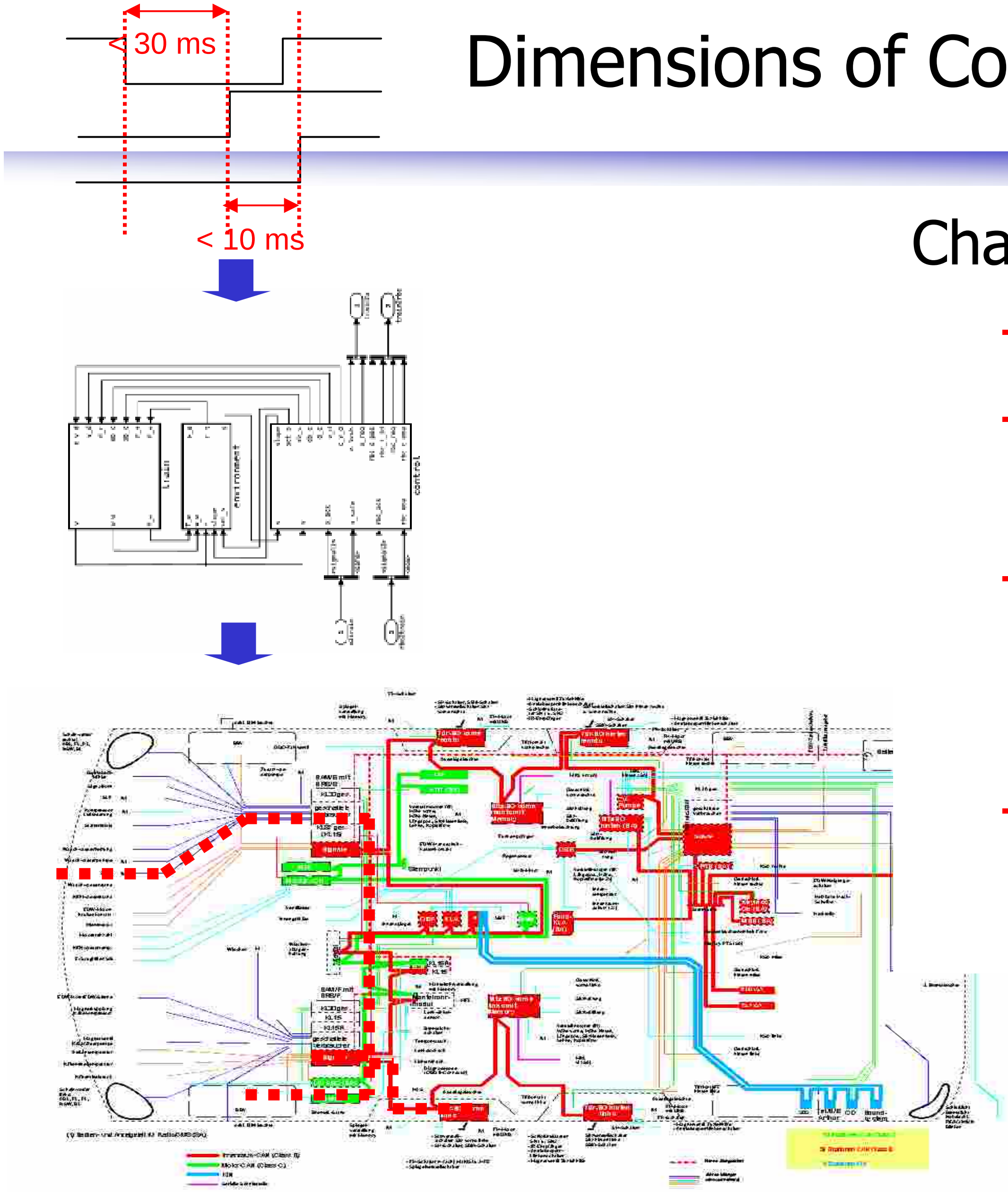
Verification of Real-Time Systems

Apply divide-and-conquer approach:

Tackle in first phase each dimension of complexity in isolation

Where we are: Highlights of Phase I

Dimensions of Complexity I: Real-Time



Challenge

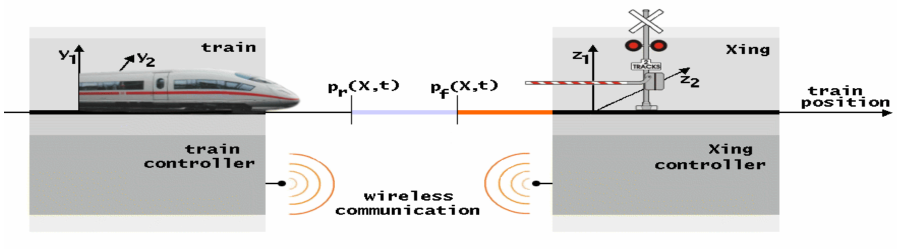
- Concurrency
- Rich specification languages
- Time Gap from virtual Timing to physical Execution Time
- WCET on distributed target architectures

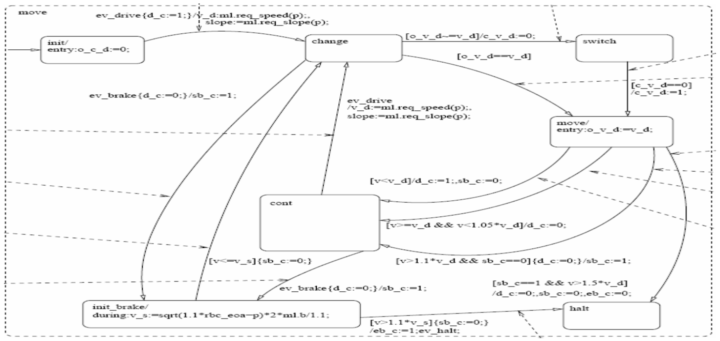
universität OLDENBURG
ALBERT-LUDWIGS UNIVERSITÄT FREIBURG
UNIVERSITÄT DES SAARLANDES

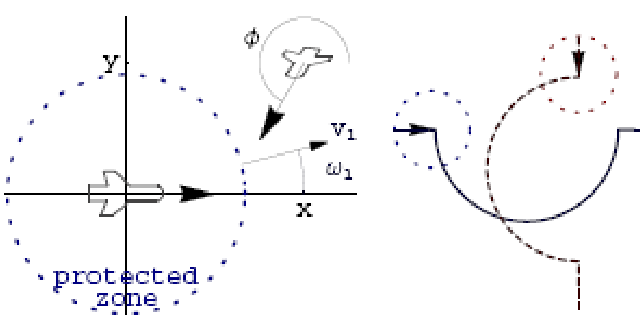
AVACS Today

- ✓ Automatically verify real time systems with complex data (reals, parameters, unbounded arrays of reals, …., ETCS emergency message system)
- ✓ Fast bug finding in systems with 65 processes and a product state space of 1.88×10^{104} states
- ✓ Guarantees for Worst Case Execution Time for airborne processor boards used for primary flight control in A380
- ✓ Automatic optimal task deployment (100 tasks) on industry standard target architectures (30 Electronic Control Units)
- ✓ Bridge from virtual time models to physical execution time on industry standard target architectures

Dimensions of Complexity II: Hybrid Systems







Challenge

- Dimensionality Barrier
  „Does it work? Up to 10 dimensions. Sometimes...“ [E. Asarin, 2004]
- Complex dynamics
  Closed deterministic linear vs open non linear
- Large discrete state space
- Beyond Safety

AVACS Today

- ✓ Bounded model checking of open linear hybrid systems with up to 25 dimensions (Train Collision Avoidance system)
- ✓ Proving safety of non-linear hybrid systems with transcendental functions (TCAS Round-About maneuver)
- ✓ Verification of linear hybrid automata with up to 2^{20} discrete states (Flap Controller)
- ✓ BMC on design-level controller models with linear dynamics and up to 2^{240} discrete states and 18 dimensions
- ✓ Verify asymptotic stability of linear HS (speed supervision) and non-linear systems
- ✓ Verify full LTL requirements on non-linear discrete time HS (TCAS Round-About man.)

Coping with Complex Dynamics in Hybrid Systems

- Developed suite of constraint-solving (HySAT, HSolver, iSAT) and automata based approaches (LIRA) for BMC of hybrid systems with linear and non-linear dynamics
- Key Results
  - HySAT: performance improvements for linear dynamics by multiple orders of magnitude, demonstrated using scalable model of "elastic train-platoon" benchmark over existing BMC approaches, based on learning and structure exploitation
  - iSAT: integrating learning into interval-based constraint solving for non-linear robust systems leads to consistent speed-up of multiple orders of magnitude, outperforms AB-Solver by orders of magnitude on non-trivial benchmarks
  - LIRA outperforms LASH as decision procedure for FO(R,Z,+,<) by orders of magnitude, based on BDD based automata representations

Coping with large discrete state spaces in HS

- Challenge addressed
  - Industrial controller models show large discrete state spaces (induced e.g. from counters, healthiness checks, parallel state machines, …)
  - Explicit discrete state representation not feasible
- Key results
  - Model-Checking of linear hybrid automata with precise on-the-fly predicate abstraction combining AIG(Lin), HySAT, and decision procedures demonstrated on variants of Flap Controller and Train Application with more than 2^{20} discrete states
  - CEGAR Approach addressing design-level controller models as captured in Statemate, Scade, … by learning ω-Automata from counterexamples drastically reduces number of refinement steps, demonstrated on
    - Autopilot model with 2^{35} discrete states and 23 reals
    - Flap Controller with 2^{240} discrete states and 18 reals

universität OLDENBURG

UNIVERSITÄT DES SAARLANDES

ALBERT-LUDWIGS UNIVERSITÄT FREIBURG

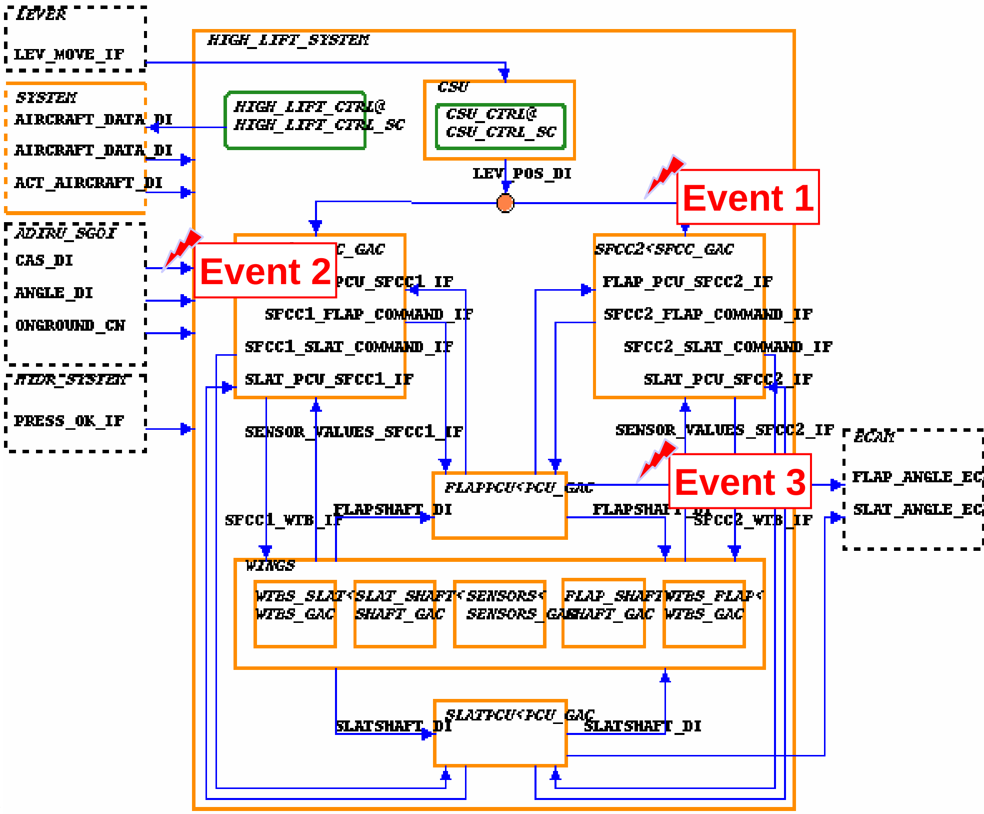
Beyond Safety: coping with Richer Requirements

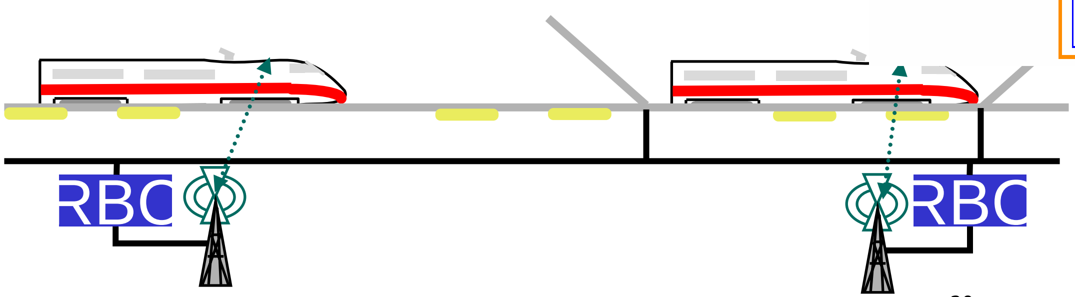
- Challenge addressed
  - Extending the scope of hybrid system verification methods beyond verification of safety properties
- Key results
  - Automatic synthesis of Lyapunov function demonstrating asymptotic stability based on LMI (linear systems) resp. non-linear robust constraint solving, demonstrated e.g. on train-speed supervision controller
  - Abstraction refinement based approach for proving region stability for linear hybrid systems, demonstrated on suite of benchmarks including emergency braking
  - Abstraction refinement based algorithm for verifying full LTL requirements for non-linear discrete time hybrid systems guaranteed to terminate for robust designs
  - Proof System for Hybrid Dynamic Logic for parameterized verification of non-linear hybrid systems
    - demonstrated on ETCS collision avoidance protocol

Dimensions of Complexity III: Systems

Challenge

- Complexity
- Dynamically Cooperating Systems
- Dependability Properties





ALBERT-LUDWIGS UNIVERSITÄT FREIBURG

CARL VON OSSIETZKY universität OLDENBURG

UNIVERSITÄT DES SAARLANDES

AVACS Today

- ✓ Disproving Realizability through Black-Boxing reduces state space of 2^{310} to 2^{184} states in Wireless Interlocking Protocol of Deutsche Bahn (FFB) (13.8 s falsification time)
- ✓ Automatic Verification of safety and liveness properties of dynamically communicating systems (Platooning)
- ✓ Integrated tool-chain for probabilistic timed reachability analysis of hazardous states (Brake-Risk Assessment for ETCS Level 3, 10^{23} states, reduced by optimizations to 10^{5} states)

Automating Compositional Verification

- Challenge addressed: Partial design verification
  - Proving realizability of partial designs
  - Inferring all we need to know about unknown components
  - Generating certificates/documentation sufficient to re-verify designs for changed component implementations
- Key results
  - Precise characterization of borderline of decidability of realizability based on key concept of information forks
  - On-the-fly synthesis of assumptions for compositional model-checking yielding 6 fold improvement over monolithic verification
  - Combination of AI-learning, SAT/BDD based multi-valued logic verification, and automata-minimization based methods
    - FFB Benchmark 4 trains, 28 train segments, demonstrated collision in presence of faulty component within 15 s
    - Multi-party signature signing protocol, outperforming Mocha by two orders of magnitude

Coping with systems-of-systems

- Challenge addressed
  - Cooperation between traffic agents is based on dynamically changing communications structures, with agents dynamically entering and leaving cooperation-partnerships
  - Automatic verification of coherence to cooperation protocols coping with dynamically changing communication structure
- Key results:
  - Concise mathematical models, logics and algorithms for the verification of dynamically communicating systems combining shape analysis, abstraction refinement, predicate- and data-abstraction, abstraction refinement, and symbolic model-checking for verification of both safety (e.g. about adhering to legal shapes) and liveness (e.g. merge maneuvers will complete) properties
  - Demonstrated on car-platooning benchmark

Formal dependability analysis of system models

- Challenge addressed:
  - Provision of guaranteed probabilistic bounds on occurrence of top-level events for system models enriched with fault-hypothesis within given time-period
- Key results:
  - Formal Reduction to model-checking of continuous time markov decision processes, underlying complete tool-chain computing probability of cut-sets for system models and failures captured in extension of Statemate
  - Drastric improvements in efficiency due to series of optimizations including fully symbolic algorithm for computing branching simulation quotients allowing to handle models out of reach for previously existing stochastic model-checking algorithms
  - Demonstrated on ETCS case study
    - Allowing to handle models with 10^{23} states
    - Optimizations size passed to stochastic mc to 10^{5} states

Conclusion

Conclusion

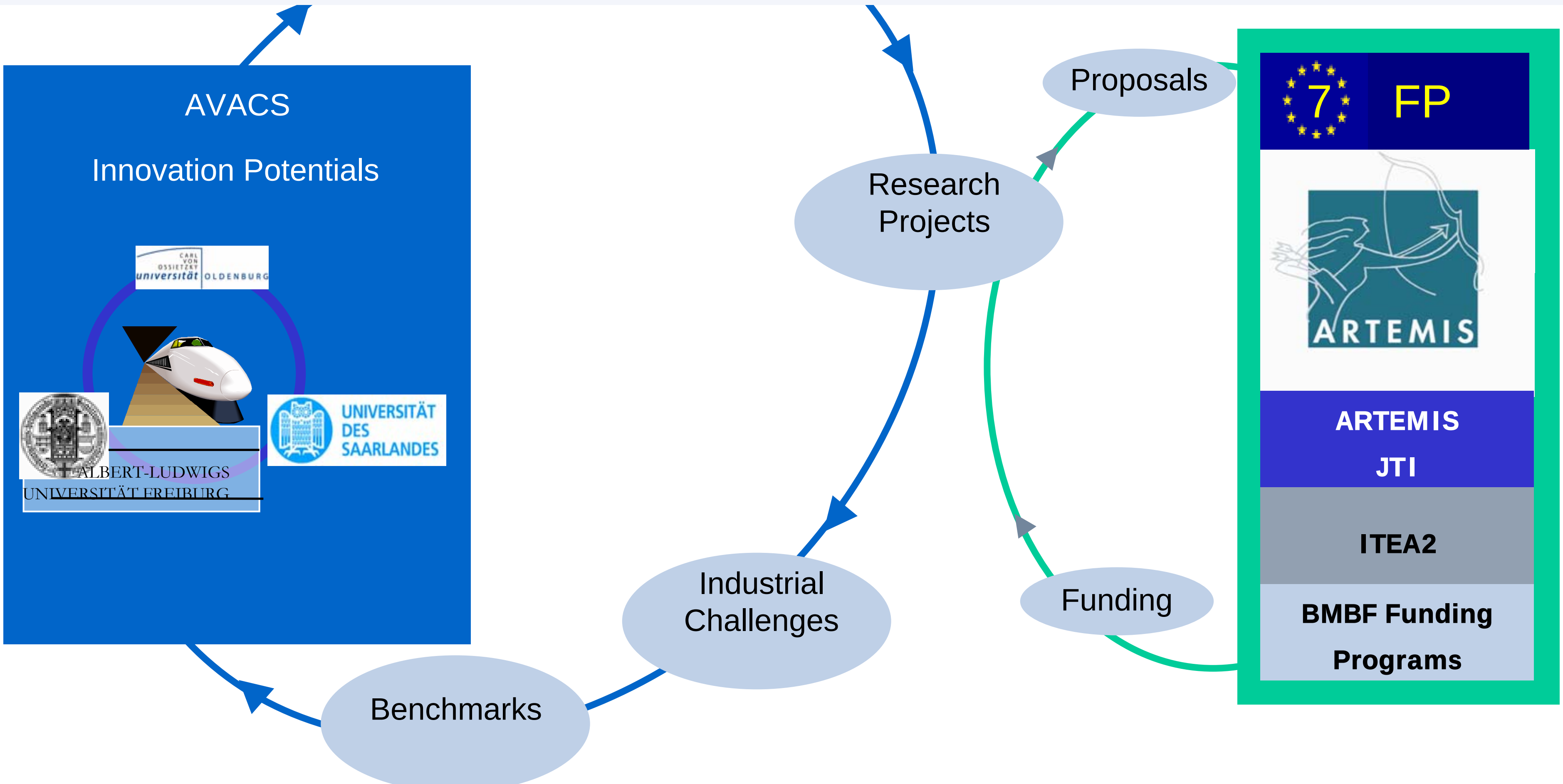
- Symbolic analysis methods are instrumental for coping with the complexity of industrial applications in demonstrating their safety
- Industry standards are increasingly pushing towards application of formal methods in establishing safety
  - ISO CD 26262
  - DO 178 C
  - Cenelec EN 50128
- Significant investments in foundational research are required to lift scalability and scope of symbolic analysis methods to the level required for such future usages
- See www.avacs.results for publications and benchmarks

UNIVERSITÄT OLDENBURG

UNIVERSITÄT DES SAARLANDES

ALBERT-LUDWIGS UNIVERSITÄT FREIBURG

Airbus, Alstom, Bosch, BMW, Carmeq, Continental, DaimlerChrysler, EADS,
IAI, Infineon, Knorr-Bremse, SiemensTransportation, SiemensVDO, ST Microelectronics, Thales
AbsInt, Extesy, ETAS, EsterelTechnologies, OSC Embedded Systems, Telelogic



Impact on Transportation Domain