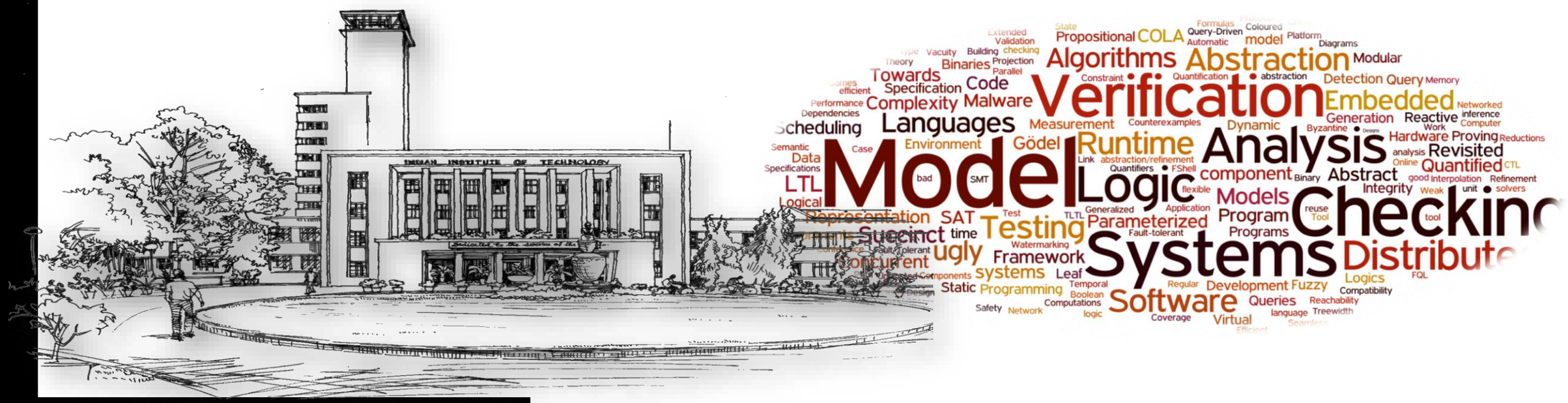
The Science of Formal Safety Assurance of Embedded Electronic Systems



FMSAFE

FORMAL METHODS FOR SAFETY CRITICAL SYSTEMS

Dr Pallab Dasgupta,

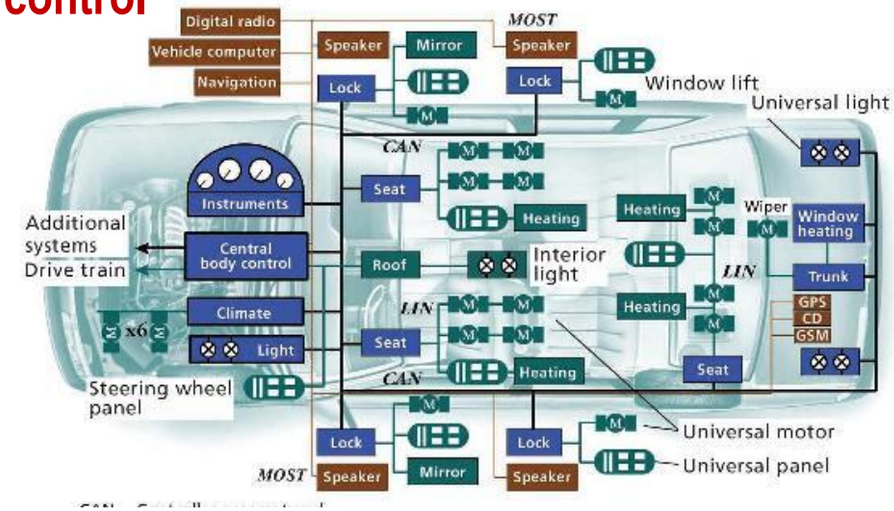
Professor, Computer Science & Engineering,

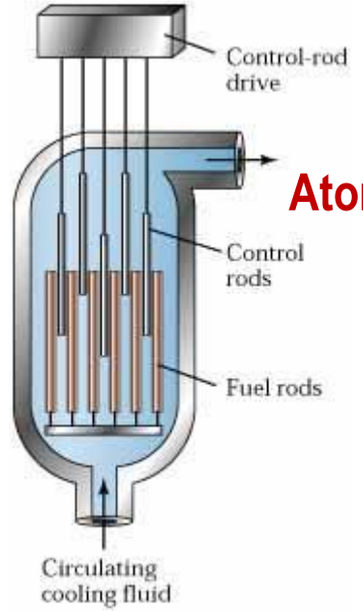
Dean (Sponsored Research and Industrial Consultancy)

INDIAN INSTITUTE OF TECHNOLOGY KHARAGPUR

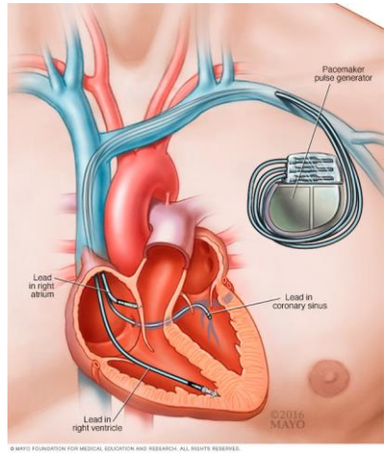
Software and embedded electronics control most things

Automotive control systems

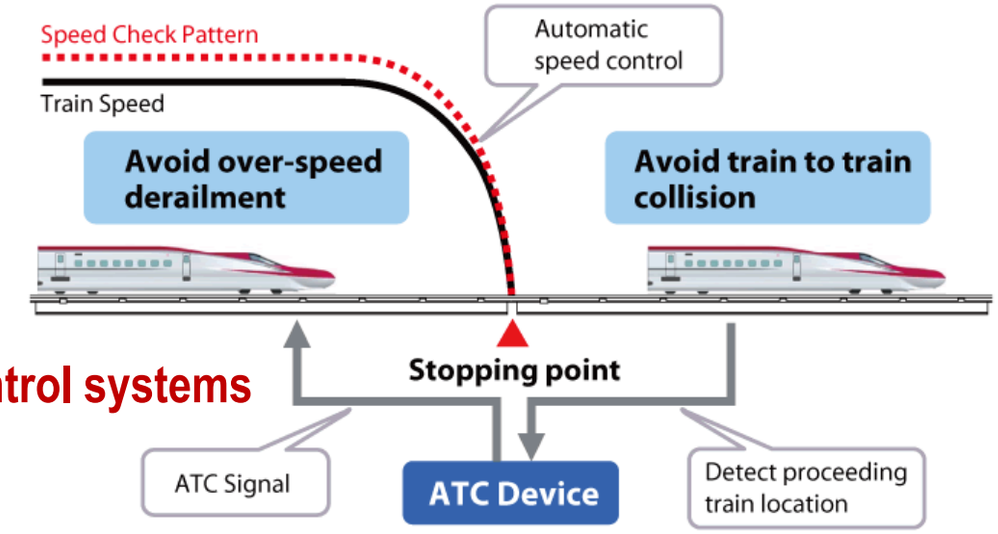




Atomic reactors

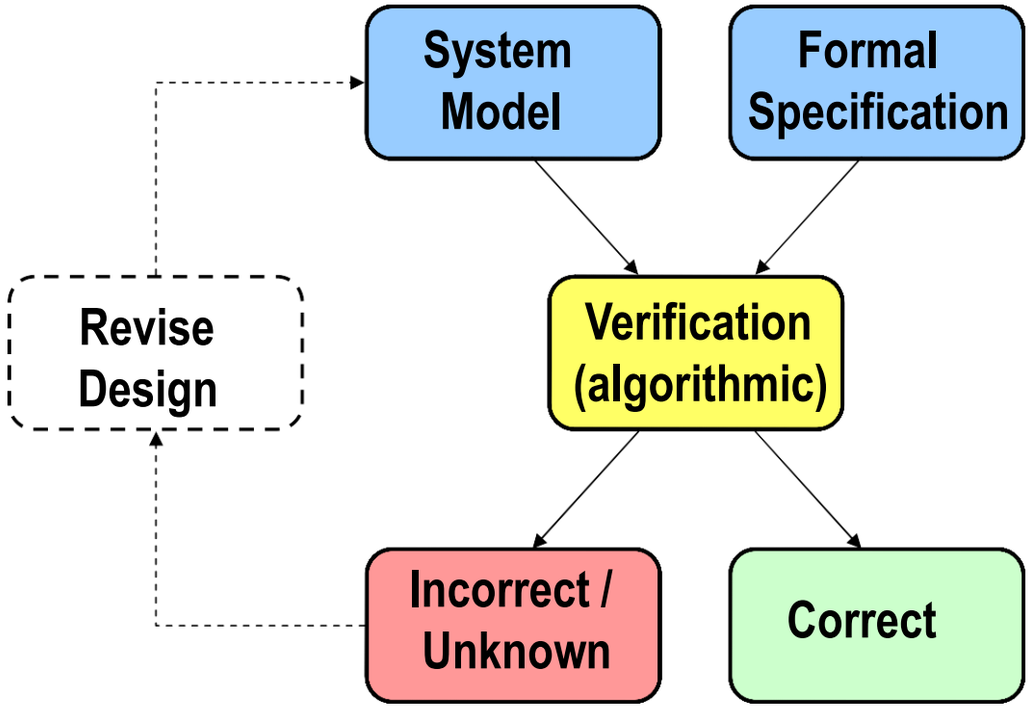


Healthcare devices

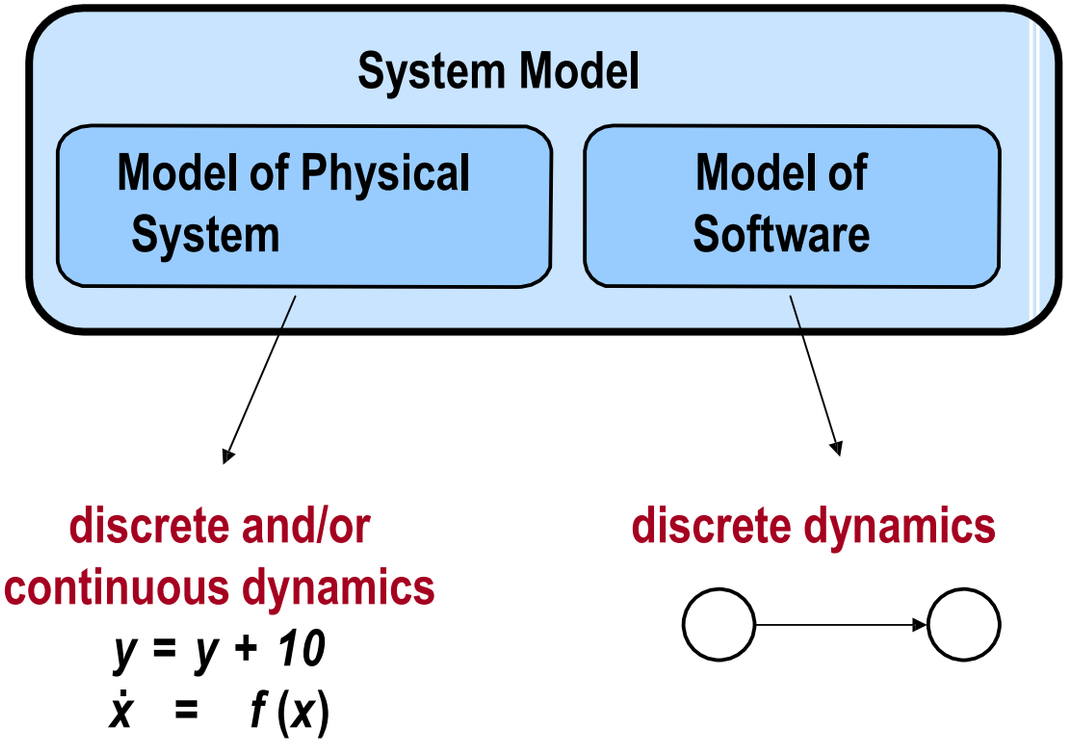


Train control systems

Formal Methods are used to prove designs to be correct



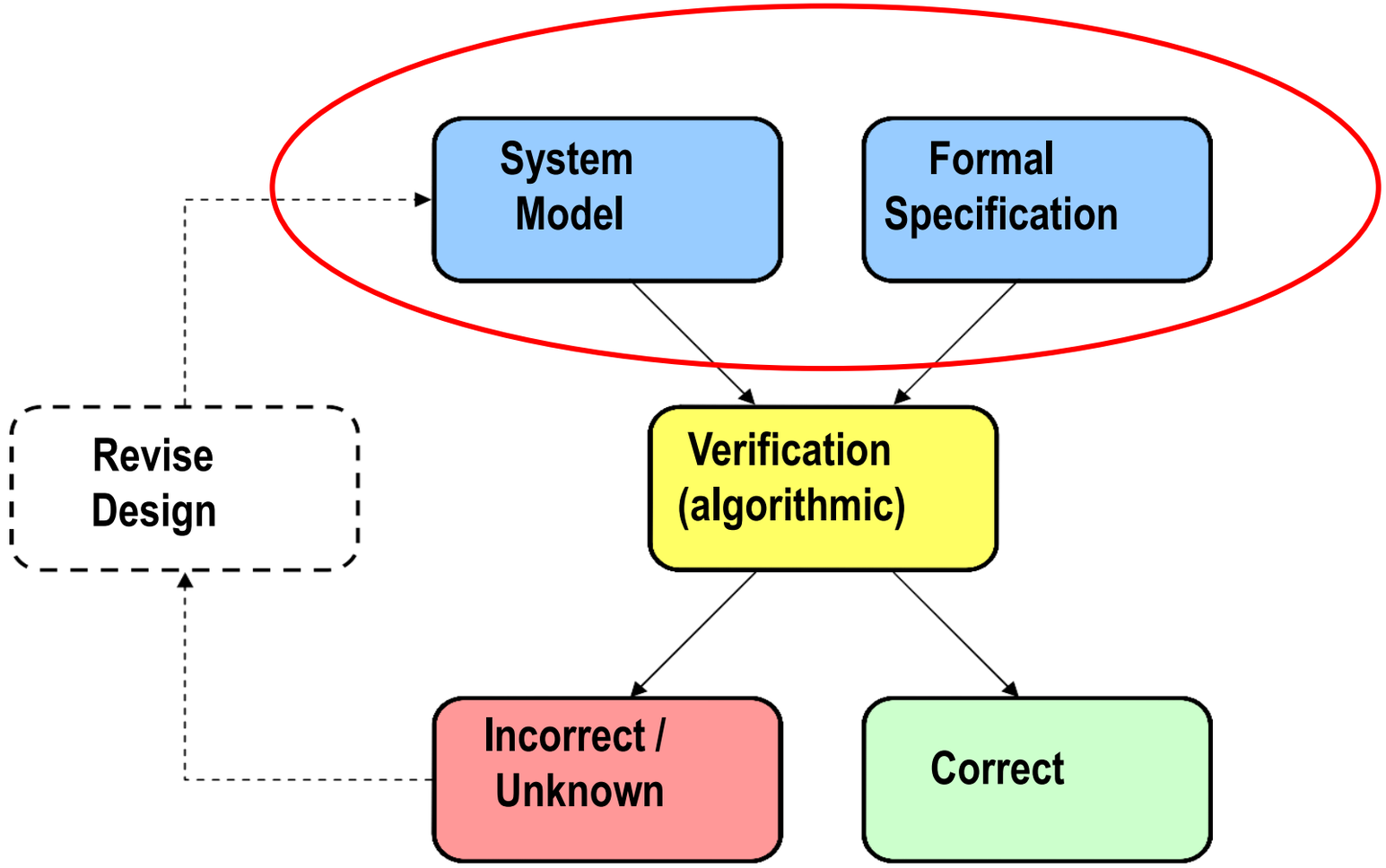
- More than 70 top scientists work in the NASA Langley formal methods group
- Top companies (Intel, IBM, Google, Microsoft, General Motors) have dedicated formal methods groups
- So does ministries of defense, atomic energy, space, etc.



International Safety Standards recommending Formal Methods in Verification

- Aeronautics (DO-178C)
- Automotive (ISO 26262)
- Industrial process automation (IEC 61508)
- Nuclear (IEC 60880)
- Railway (EN 50128)
- Space (ECSS-Q-ST-80C)

The two important components



Formal Specification of Safety

- Boolean Logic, Predicates (as we do in AI Planning for example)
  - $g1 \wedge g2$ — both signals in a traffic crossing are green at once
  - (dosage > 3.2) — where dosage is a variable in an insulin pump program
- Temporal Logic (when we want to express sequential / timing issues)
  - bus_req ##1 ! bus_gnt ##1 ! bus_gnt — No grant of access to bus in two cycles from request
- Language standards exist in many domains
  - SystemVerilog Assertions in the circuit domain
  - Predicates over real variables in program verification
  - Linear Temporal Logic in several tools

Succinct representation of state spaces

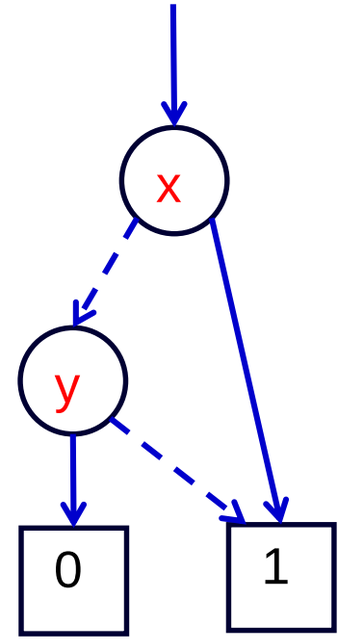
BOOLEAN EXPRESSIONS

- Let our state be denoted by $\langle x, y \rangle$ where *x* and *y* are state variables
  - The formula: $x \vee \neg y$ is a succinct representation of a set of three states:

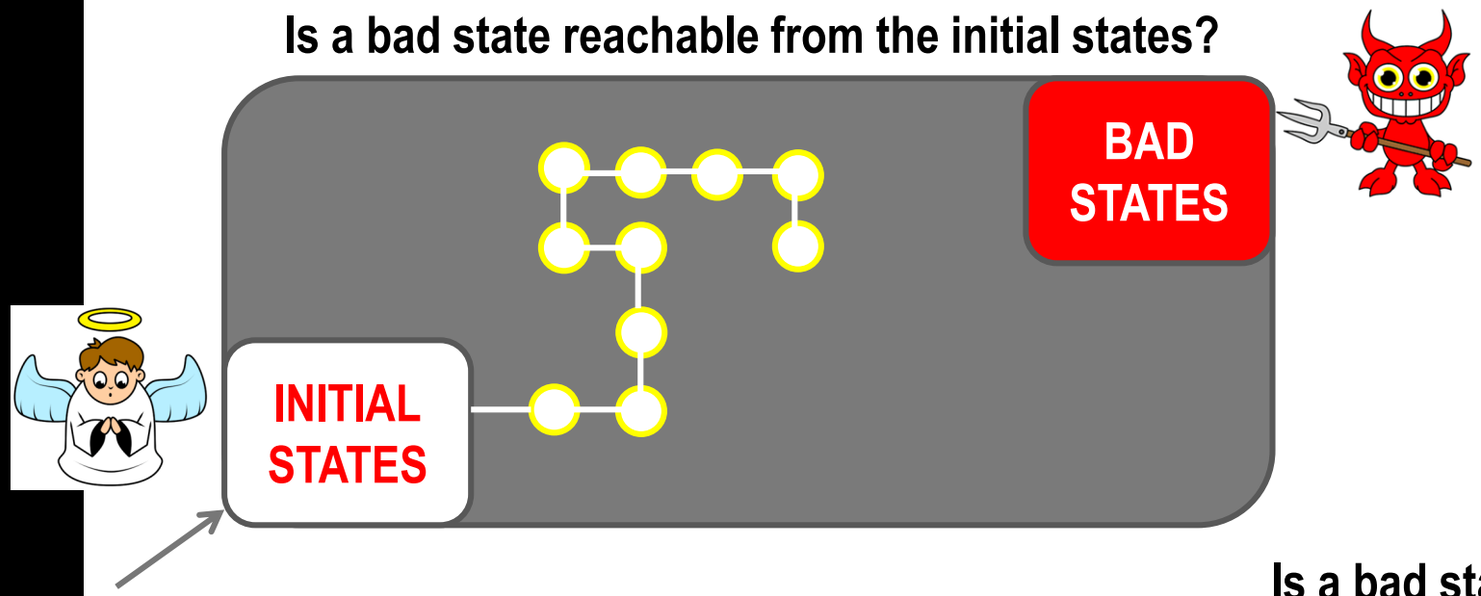
    $\{\langle 1, 1 \rangle, \langle 0, 0 \rangle, \langle 1, 0 \rangle\}$

DECISION DIAGRAMS

- The decision diagram represents a set of states
- Take bold edge for valuation-1 an dashed edge for valuation-0
- Each valuation leading to the vertex with label 1 represents a member of the set



How is a formal analysis different from simulation?

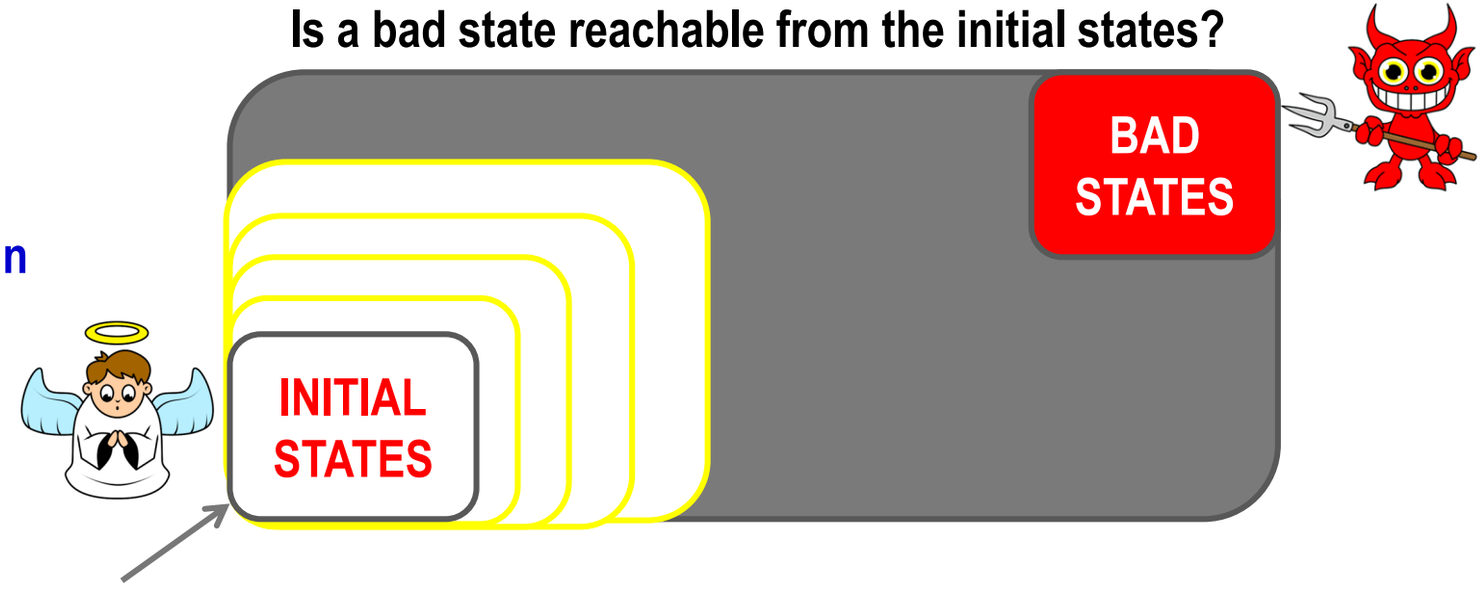


SIMULATION

- States are visited one at a time
- We need many simulation runs to cover all behaviors

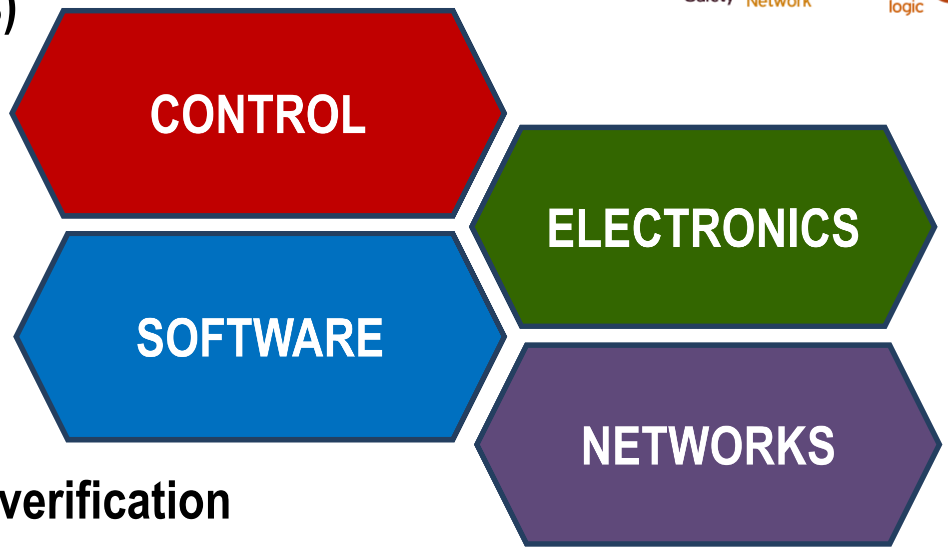
FORMAL VERIFICATION

- Sets of states are visited at a time
- We find all reachable states in one run
- Sets of states are maintained symbolically, not explicitly



Toolscape

Formal tools for verifying hybrid systems
(control law, stability, features)
PHAVER, SpaceX, Statemate

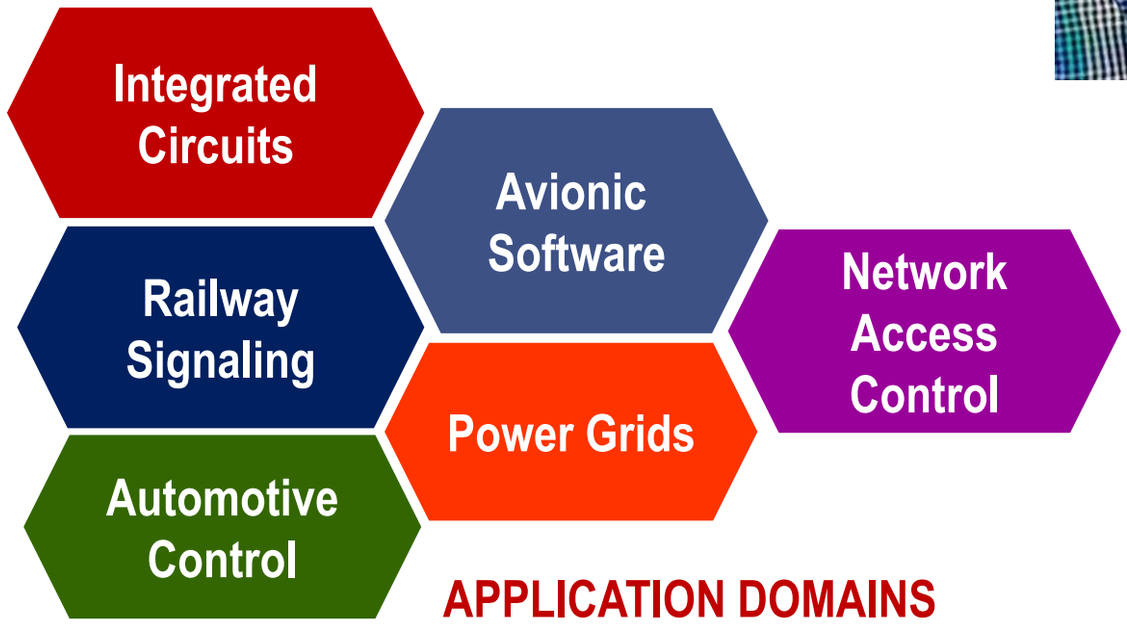


Formal tools for verifying circuit designs
(functional properties, power)
Many commercial and non-commercial tools
(VCFormal, JasperGold, abc)

Formal tools for software verification
(correctness, timing)
Model checkers, WCET analyzers
(CBMC, CPAChecker, SATABS, Spin)

No Commercial Tool
(Coq Theorem Prover, SPIN)

Formal Methods Group @ IIT Kharagpur



APPLICATION DOMAINS

AREAS OF STRENGTH

- Modeling Formalisms
- Decision Procedures
- Software Verification
- Hardware Verification
- Verification of Control Systems
- Performance verification
  - Power, Reliability, Timing

INDUSTRY PARTNERS

intel. IBM SYNOPSYS® SRC® National Semiconductor The Sight & Sound of Information Google INDIAN RAILWAY HAL GM

Summary of Contributions

LANGUAGE FORMALISMS AND DECISION PROCEDURES

- *Logics for reasoning about quantitative artifacts*
- *Auxiliary specifications – beyond temporal logic*
- *Methods for reasoning with formal properties*
- *Features – non Boolean functional properties*

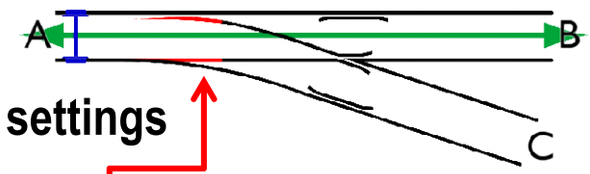
VERIFICATION METHODOLOGIES FOR THE CIRCUIT DOMAIN

- *Analog and Mixed-signal Assertion-based verification*
- *Formal verification methods for on-chip power management*
- *Methods for getting around the state-explosion problem*

VERIFICATION OF AUTOMATED SYSTEMS

- *Formal Methods for Verification of Railway Signaling and Interlocking*
- *Formal Methods for Verification of Automotive Control*
- *Formal Methods for Verification of Real Time Operating Systems*
- *Formal Methods for Verification of Access Control in Corporate Networks*

Electronic Interlocking in Railways

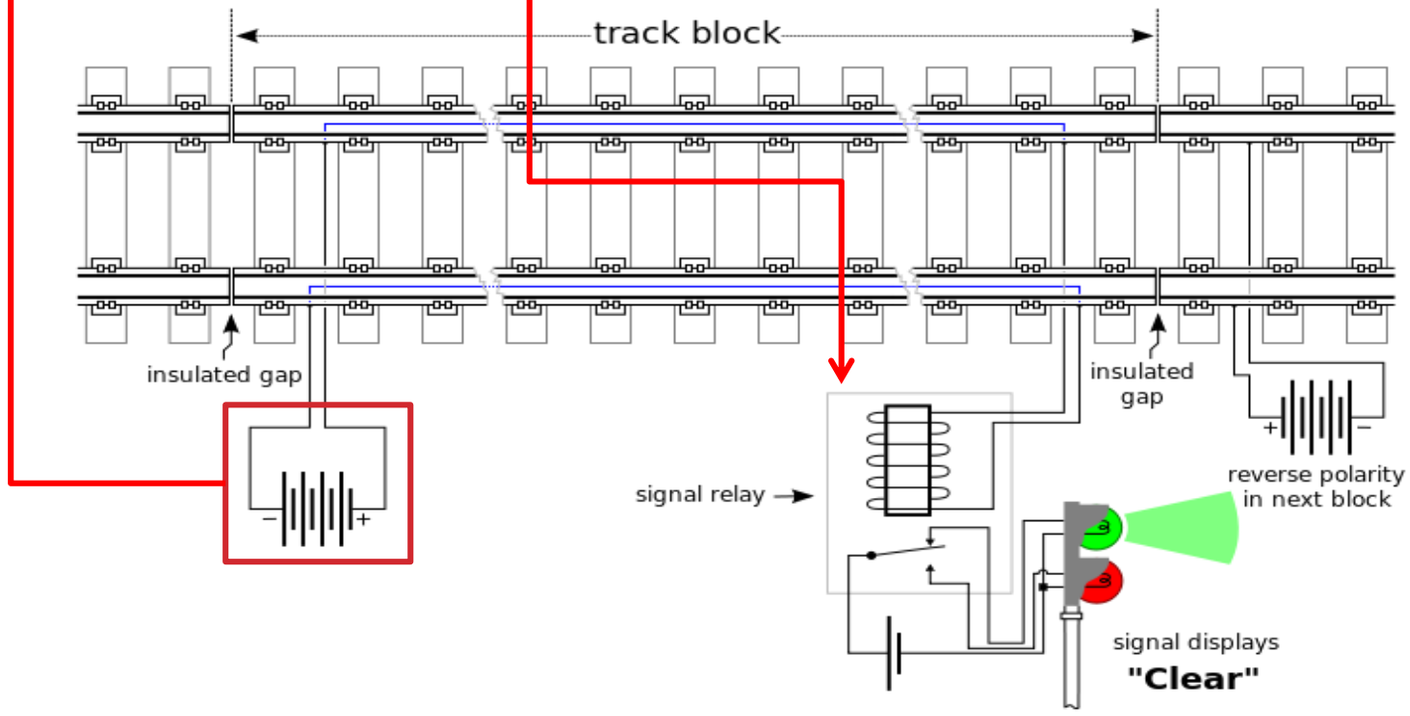


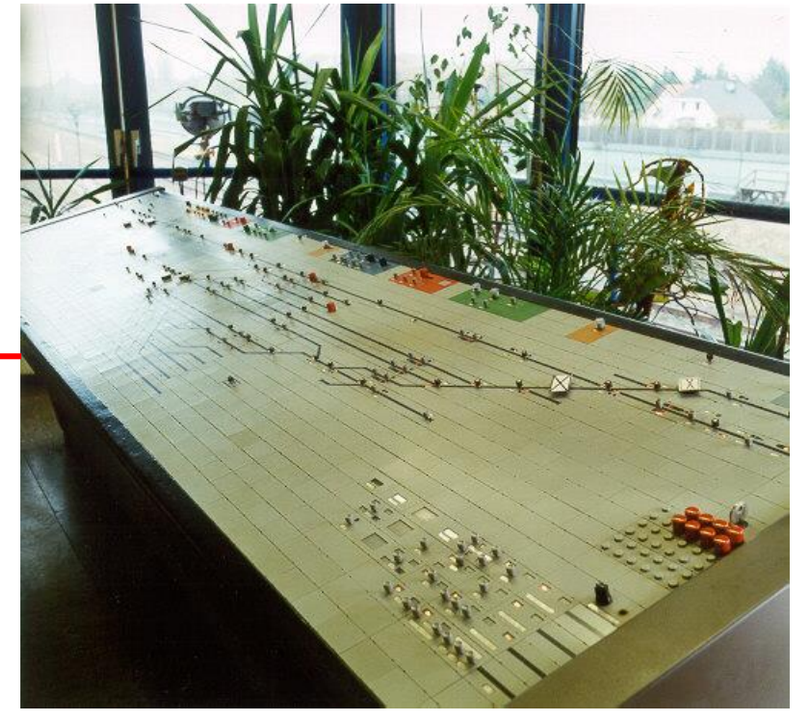
Point settings

Track occupancy

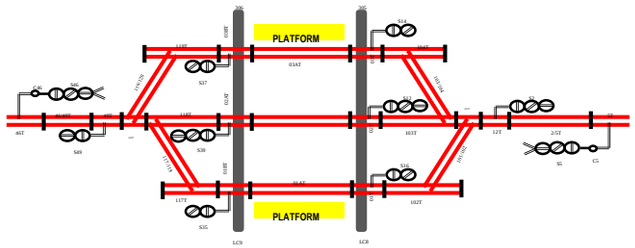
EI Equipment

Route requests





Life-cycle for Signaling Logic



Control Table

Application Logic

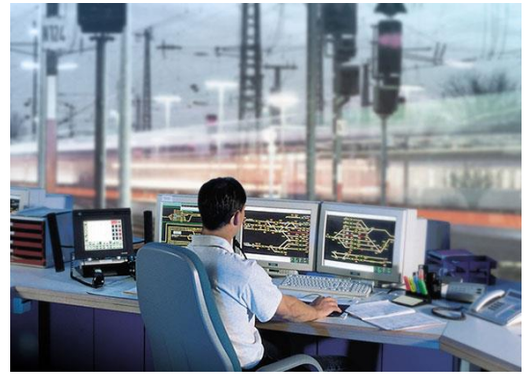
Railways has to pay for each loop

Factory Acceptance Testing (FAT)

Thousands of tests, where engineers visually examine the signaling principles !!

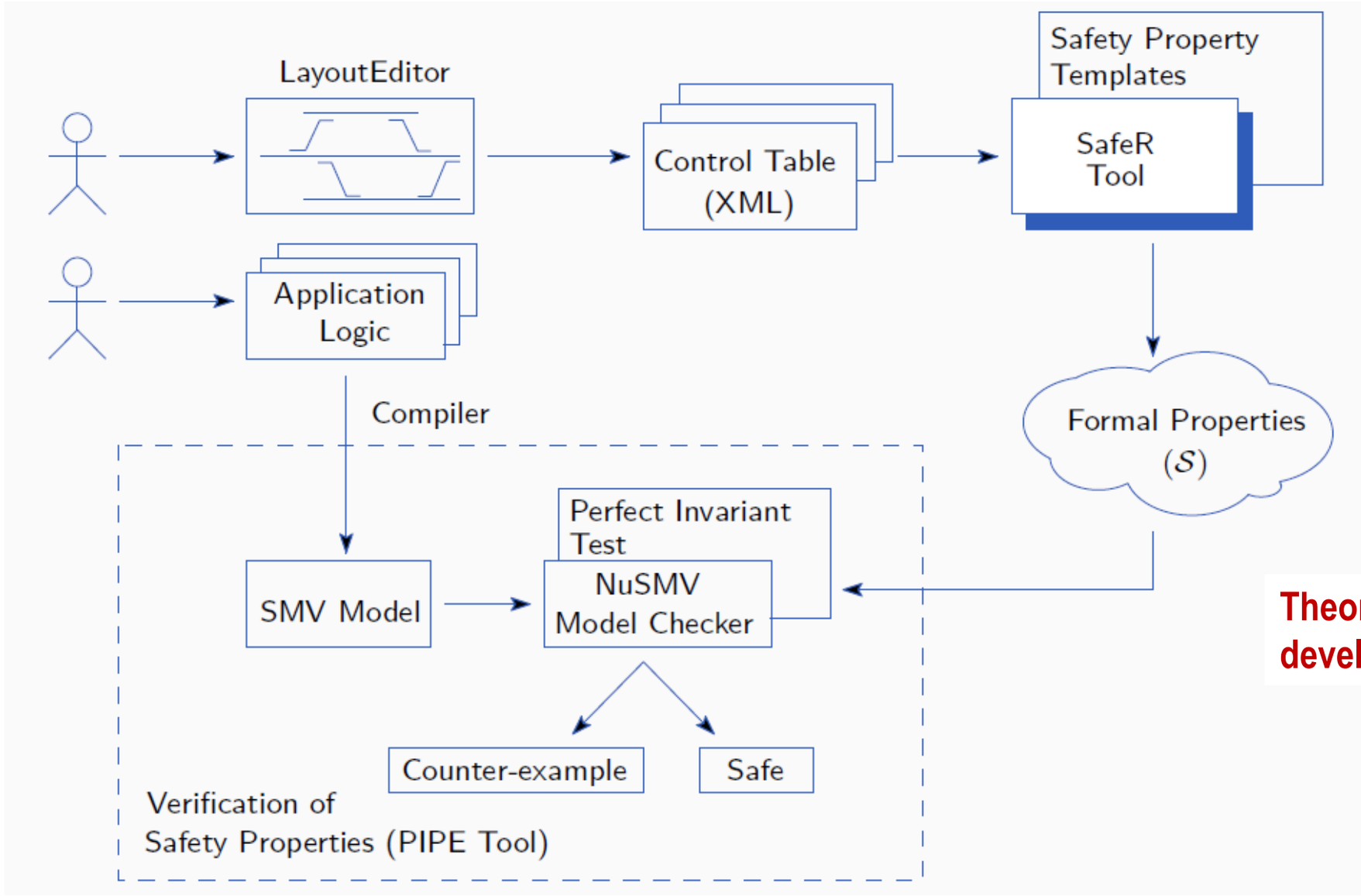
Error in logic?

Deployment and Site Acceptance Testing (SAT)



Upgradation needed?

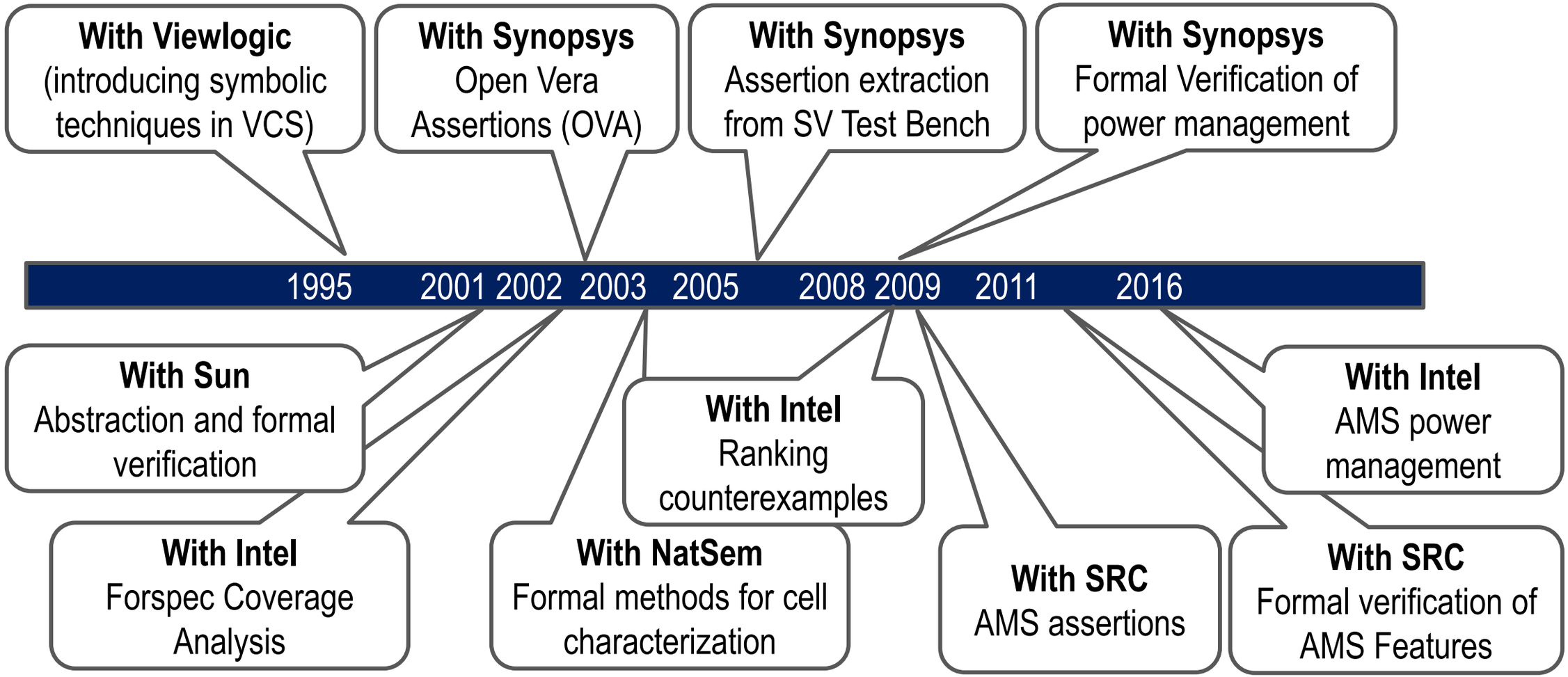
IIT-KGP EI Verification Tool Flow



Theory of perfect invariants developed for scaling verification

Formal Methods in Electronic Design Automation

… one of our main areas of strength



Formal Methods in Cyber Physical Systems

AUTOMOTIVE ECS

Formal analysis of Automotive Feature Specs

Formal methods for early time budgeting in control

Automata based scheduling and multi-rate control

AUTOSAFE

Platform aware formal timing analysis of control loops

COLLABORATORS:

- General Motors
- Technical Univ. of Munich
- TCS (TRDDC)
- Inchron GmbH

Towards the validation of software for PHEV controls

RTOS VALIDATION (DO-178-C)

We are using formal methods for validating India's first Real Time Operating System developed by HAL

We are building a tool for health monitoring of power grids

ELECTRICAL POWER GRIDS

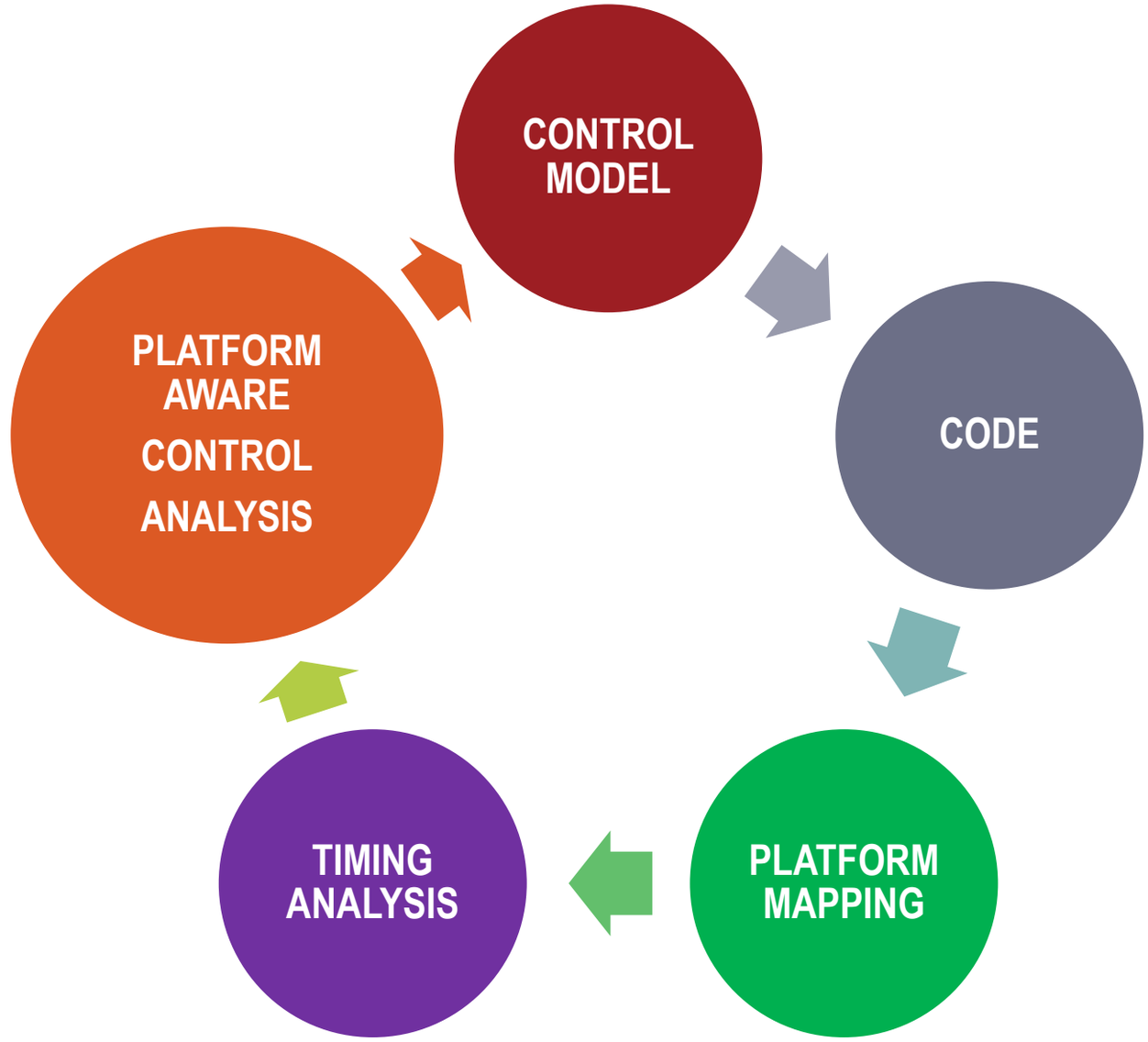
We are collaborating with POSOCO, the national power grid operators

Integration of Solar PV in Indian Grid

The AUTOSAFE Project

AUTOSAFE develops the notion of *platform aware control analysis*

Built-in formal methods guarantee early resolution of *timing issues*



Our partners in AUTOSAFE

Technische Universität München

Technische Universität München, Real-Time Computer Systems (RCS)

INCHRON THINK REAL-TIME

INCHRON GmbH

TATA

Tata Research Development and Design Centre (TRDDC)

INDIAN INSTITUTE OF TECHNOLOGY KHARAGPUR

FMSAFE

FORMAL METHODS FOR SAFETY CRITICAL SYSTEMS

A networked center for formal methods in validation and certification procedures for safety-critical ICT systems

- **This center, led by IIT Kharagpur and partnered by IIT Kanpur and IIT Bombay aims to serve as the national knowledge hub on formal methods.**
- **We shall work closely with Indian Railways (the world's largest railways) on next generation railway technologies**
- **We intend to help other safety critical domains like atomic energy and automotive.**

IMPRINT CENTER PARTNERING WITH MINISTRY OF RAILWAYS

Contact: pallab@cse.iitkgp.ernet.in Web: http://cse.iitkgp.ac.in/~pallab

INDIAN INSTITUTE OF TECHNOLOGY KHARAGPUR