FORMAL METHODS – *AN INTRODUCTION*

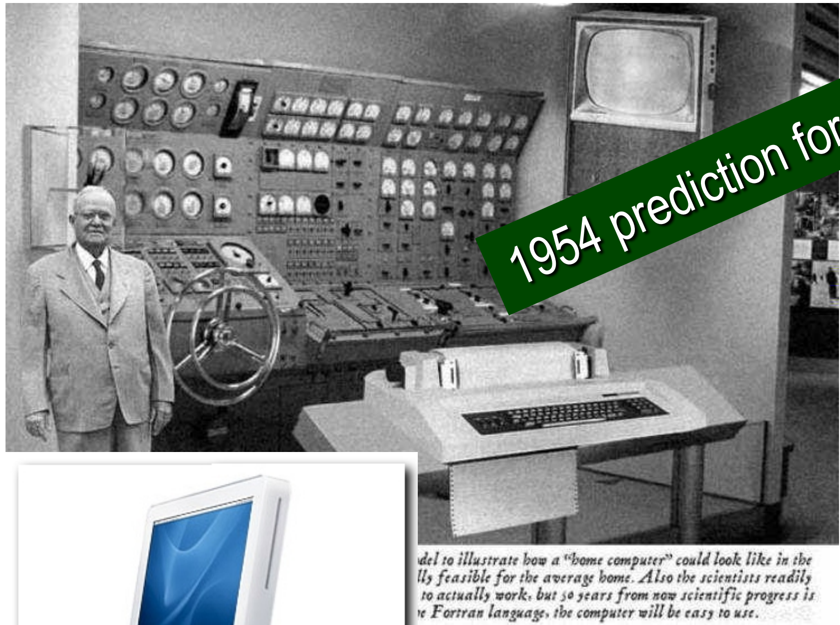
FMSAFE

FORMAL METHODS FOR SAFETY CRITICAL SYSTEMS

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY KHARAGPUR

Dr Pallab Dasgupta, Professor

The Evolution of Electronic Computing



1954 prediction for 2004

5 MB

32 GB

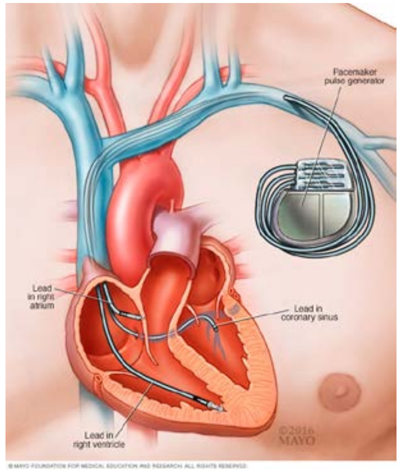
Computation
became free !!

Storage
became free !!

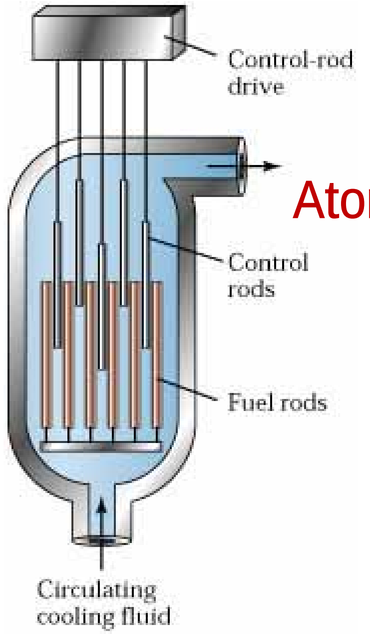
Communication
became free !!

1980 1990 2000 2010

Computing is not confined to labs anymore !!

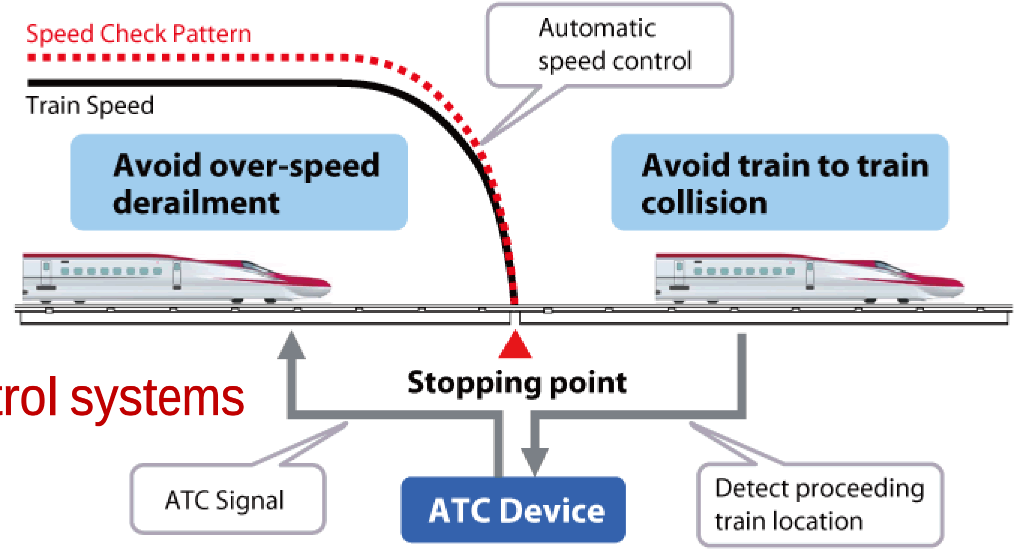


Healthcare devices

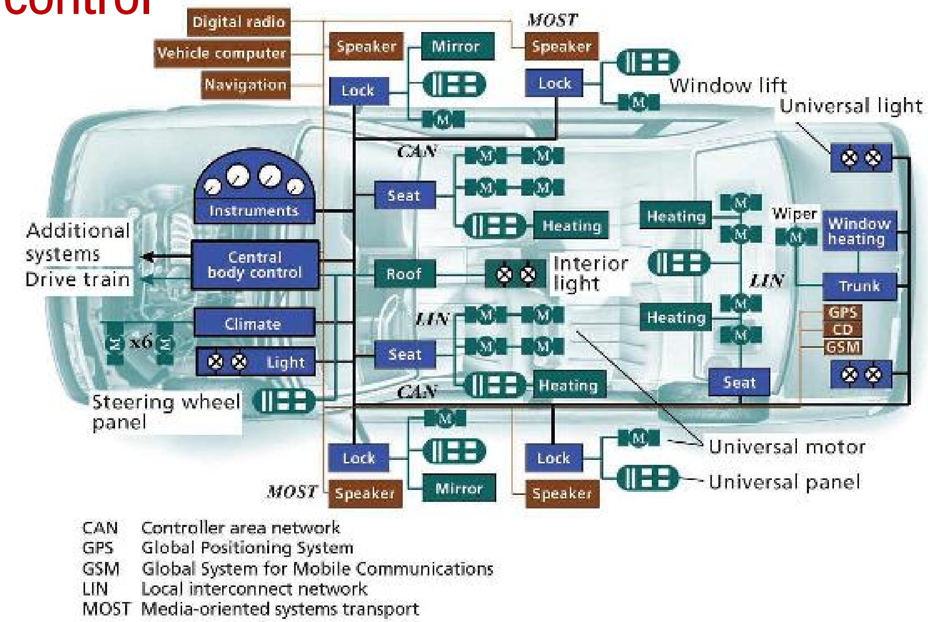


Atomic reactors

Train control systems



Automotive control systems



- Safety and security are the primary concerns today
- Why is this a relatively new challenge?

Modern systems are software based !!

Modern systems are designed using software !!

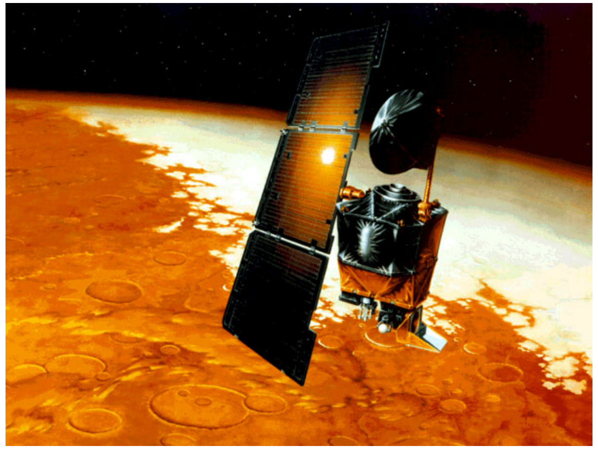
Safety and Computer Science

- In view of the proliferation of electronics and software in everything that we use:
  - Safety has a new meaning – the electronics and software must not do things that cause my gadgets to harm me
  - Only Computer Science can solve the problems related to cyber safety
  - Today there are at least two people in verification for every person in design. And this is true in:
    - Design of integrated circuits
    - Design of software
    - Design of control systems

⇒ Verification experts are in high demand in modern engineering. Yet bugs continue to haunt the industry.

Famous incidents from software bugs

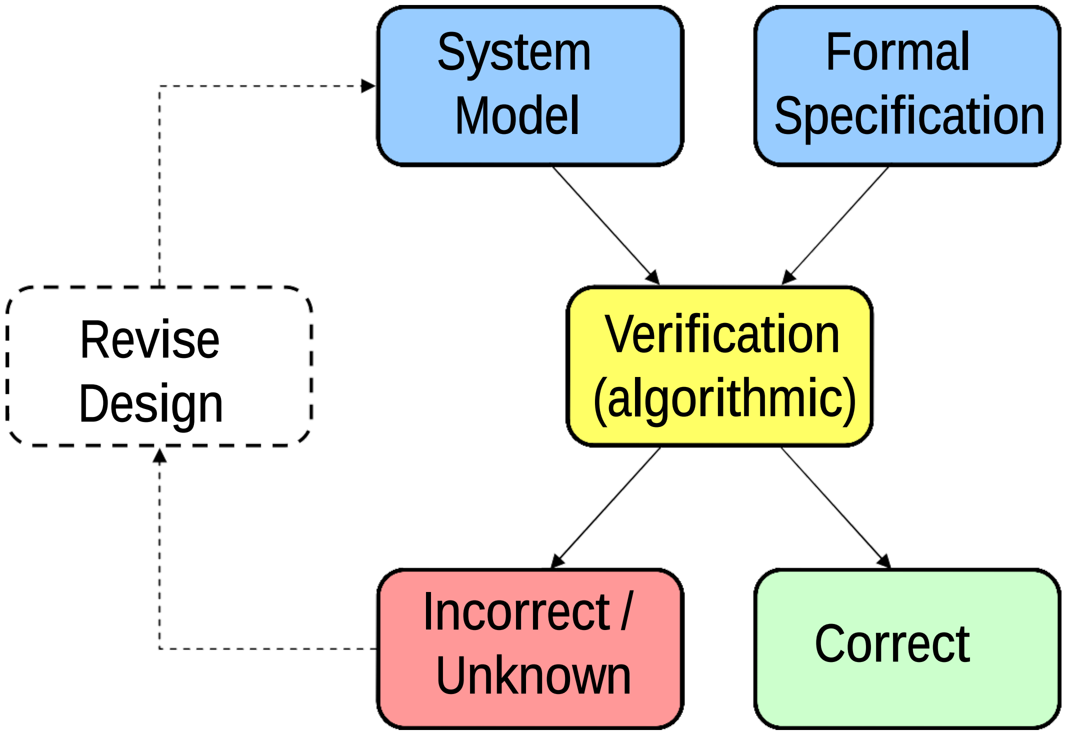
Explosion of Ariane 5, 1996 due to *".. conversion of a 64 bit integer into a 16 bit signed integer lead to an overflow ..."*

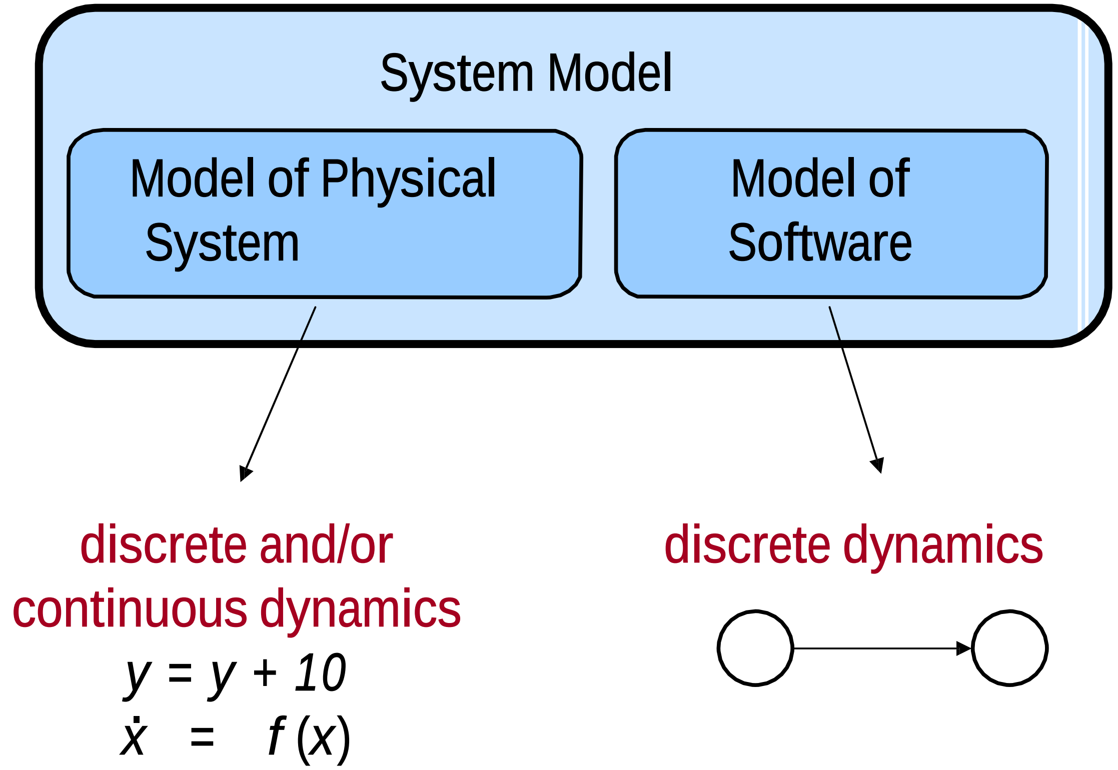


Loss of Mars Climate Orbiter, 1999 due to *"...mix-up between pounds and kilogram...."*

USS Yorktown died in the water, 1998 due to *"....input and Division by '0'. „ X / 0 = undefined..."*

Formal Methods are used to prove designs to be correct !!



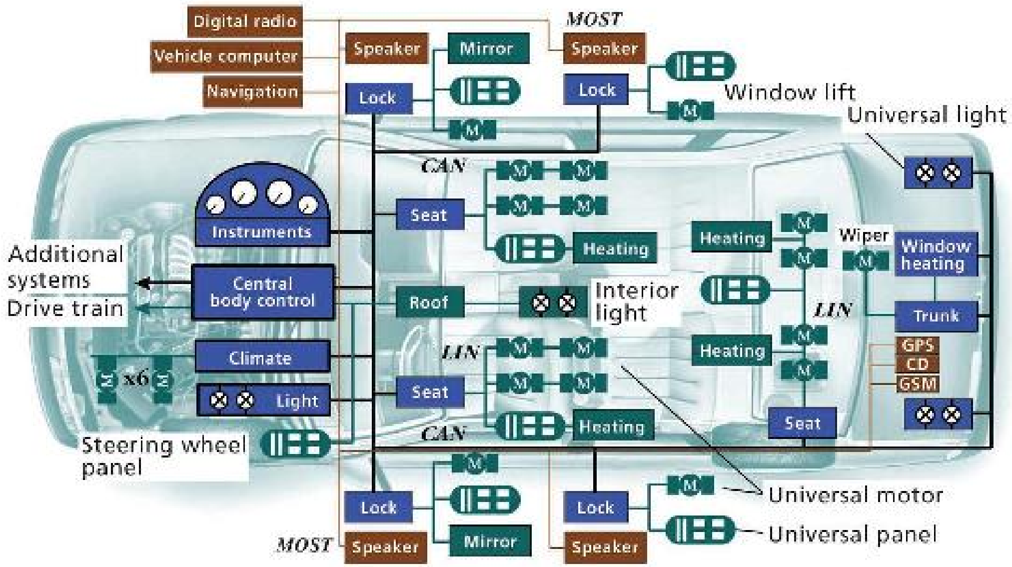


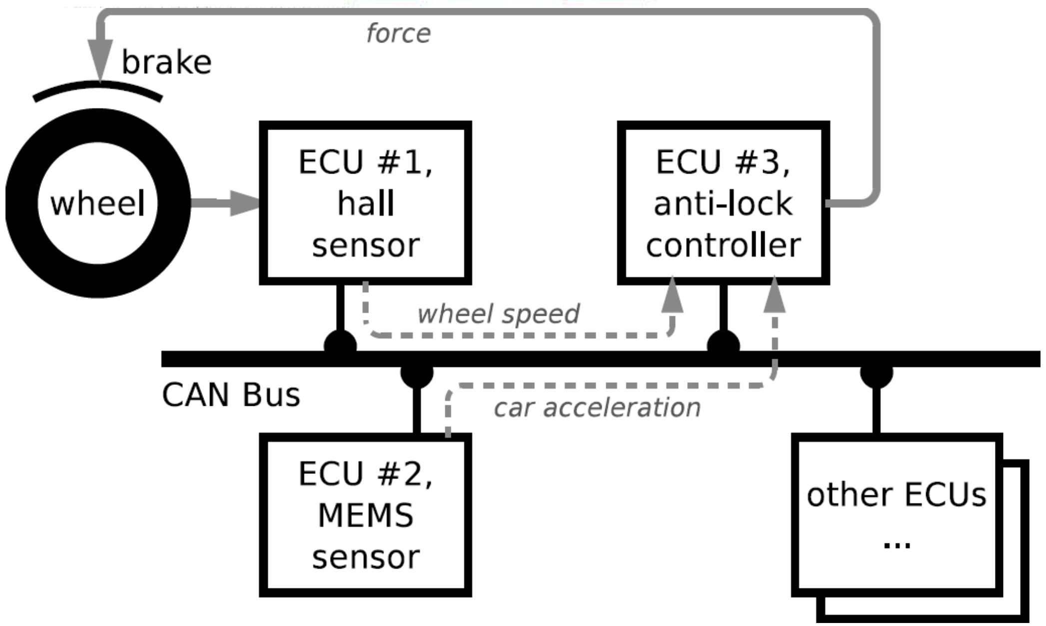
- More than 70 top scientists work in the NASA Langley formal methods group
- Top companies (Intel, IBM, Google, Microsoft, General Motors) have dedicated formal methods groups
- So does ministries of defense, atomic energy, space, etc.

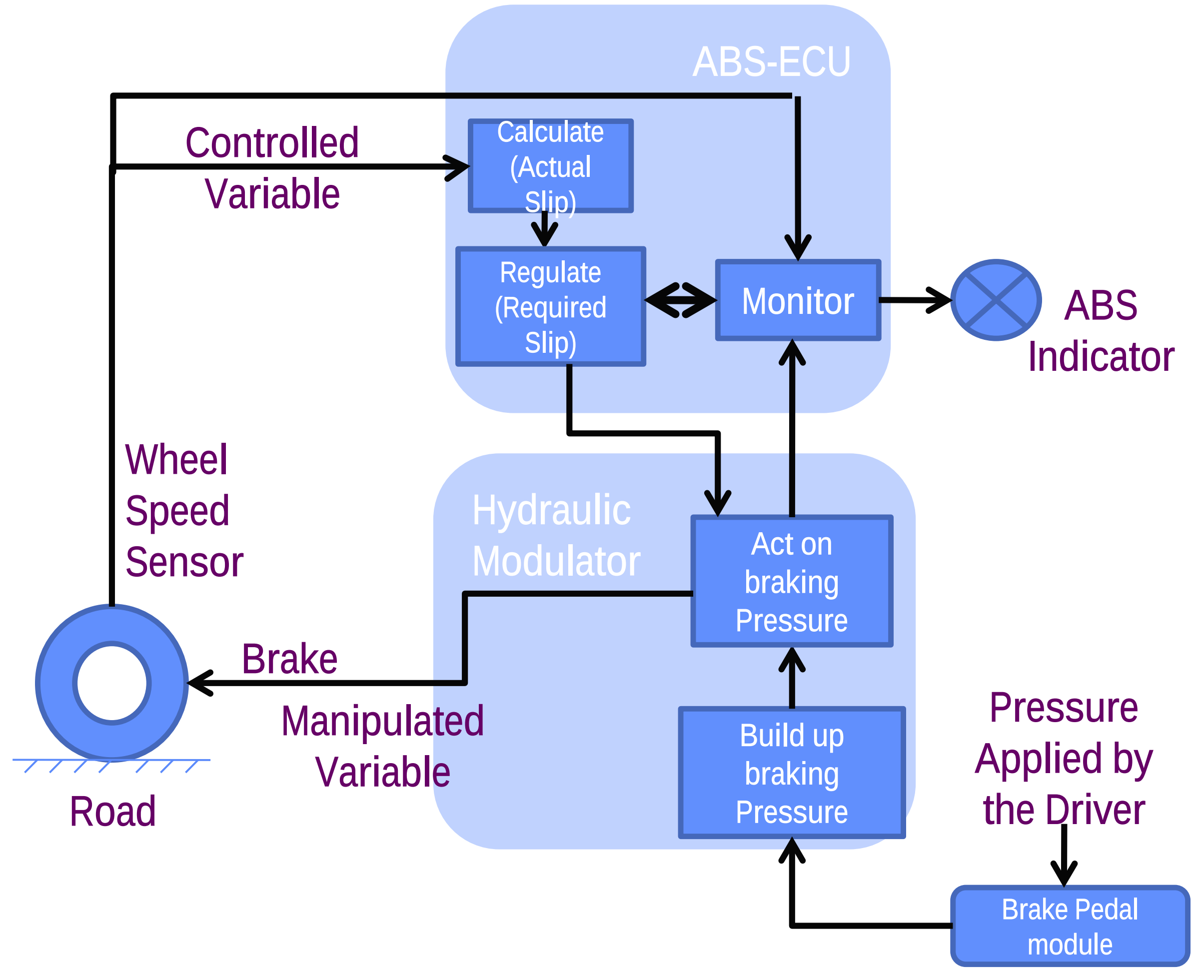
International Safety Standards recommending Formal Methods in Verification

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

Examples of Safety Critical Systems



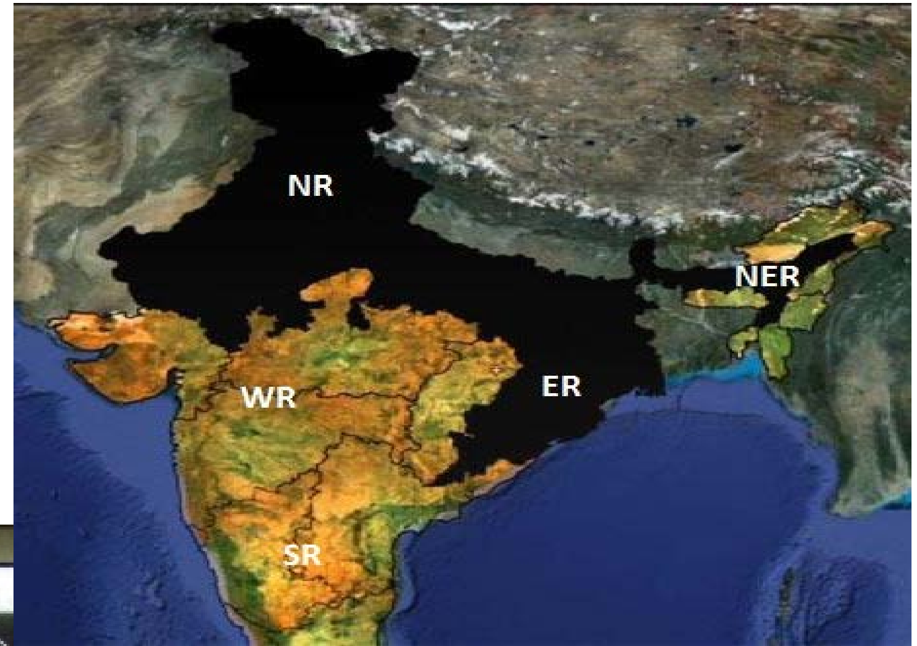




Antilock braking system (ABS)

Examples of Safety Critical Systems

- Power Grids



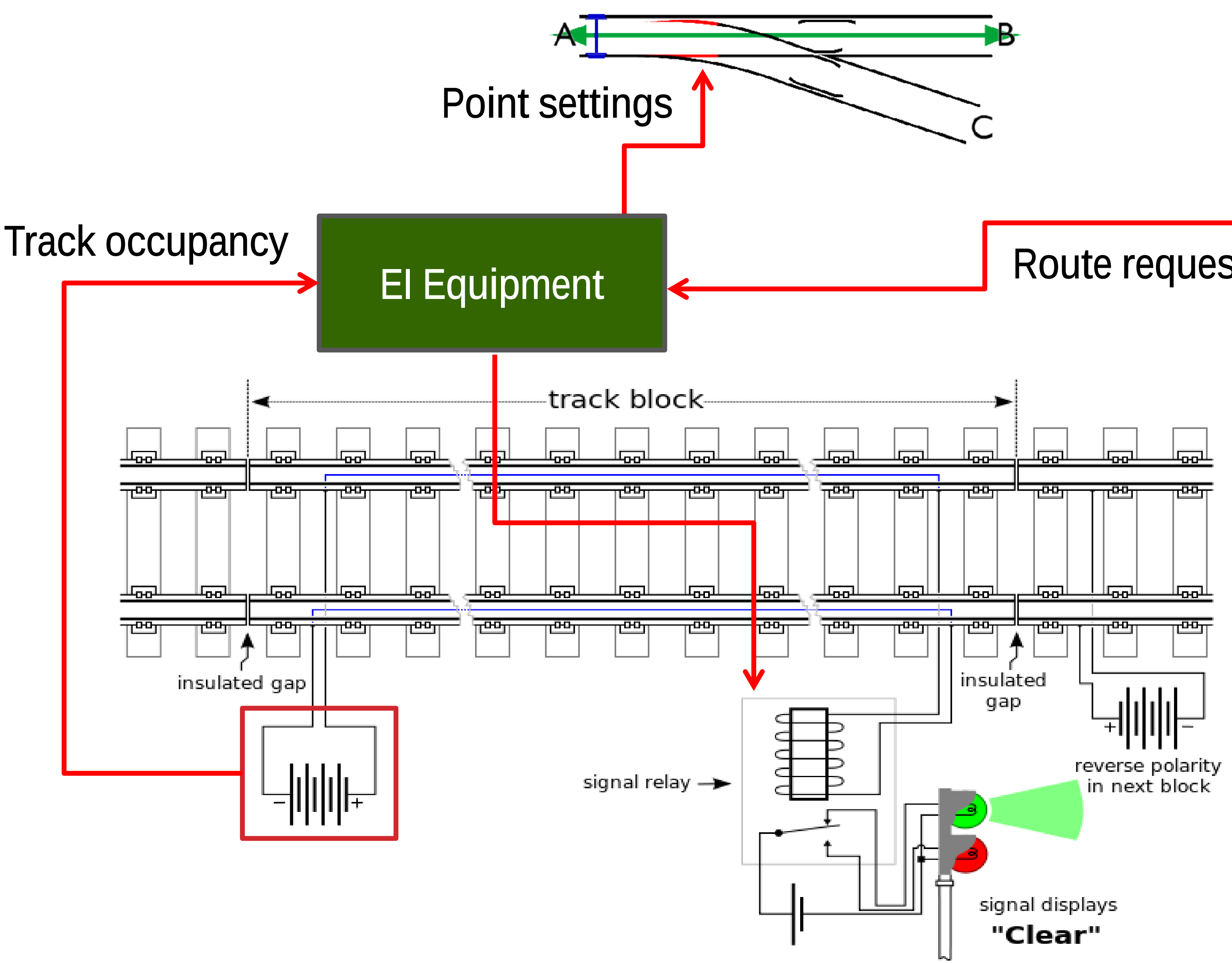
NATIONAL LOAD DESPATCH CENTER - Control room
At the Top of Control Heirarchy

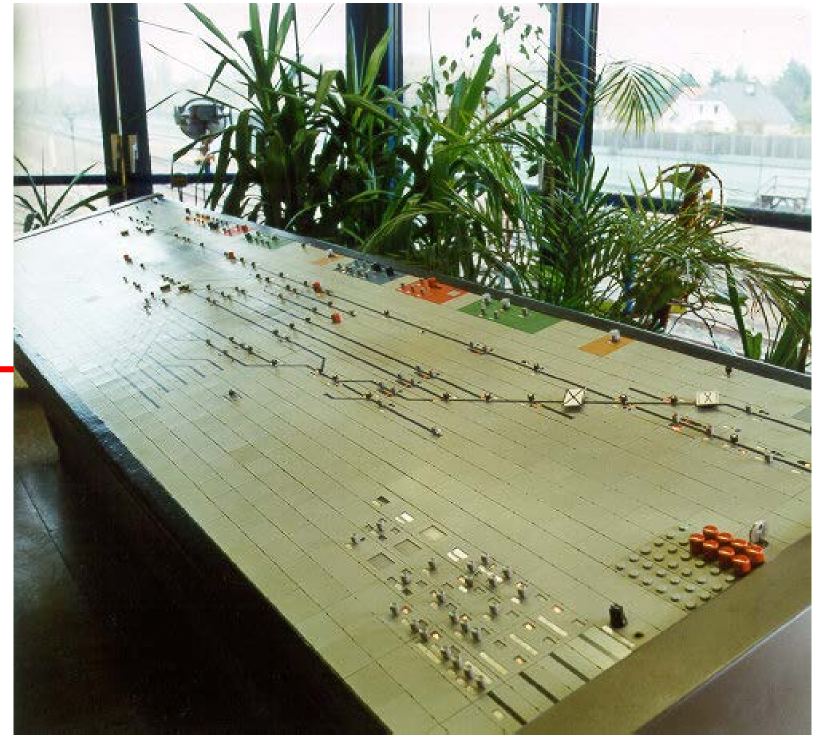
Course Topics

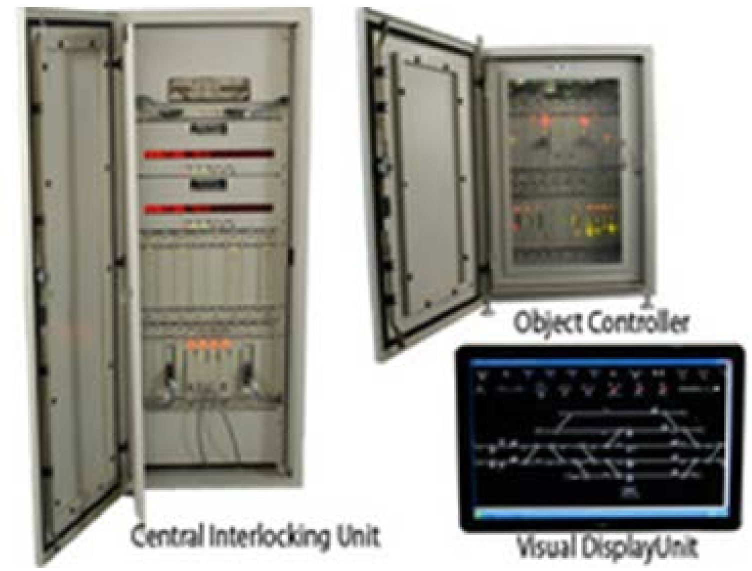
- Formal Specifications.
  - Automata over finite and infinite words, Communicating concurrent state machines, Temporal and Modal Logics, Relationship between Logic and Automata, Satisfiability, Validity and Model checking problems.
- Handling Large State Spaces.
  - Succinct representations of state spaces and their traversal, SAT and BDD-based symbolic reachability approaches, abstraction refinement approaches.
- Model Checking.
  - Temporal logic model checking, Symbolic and automata theoretic approaches.
- Formal representation of time.
  - Timed automata, Timed temporal logic, Model checking timed systems.
- Formal representation of hybrid systems.
  - Hybrid automata, Reachability problems in hybrid automata, Polyhedral approximation techniques.
- Formal analysis of programs.
  - Abstract interpretation, Predicate abstraction, Model checking software systems.
- Industrial applications of formal methods.

A Real World Case Study

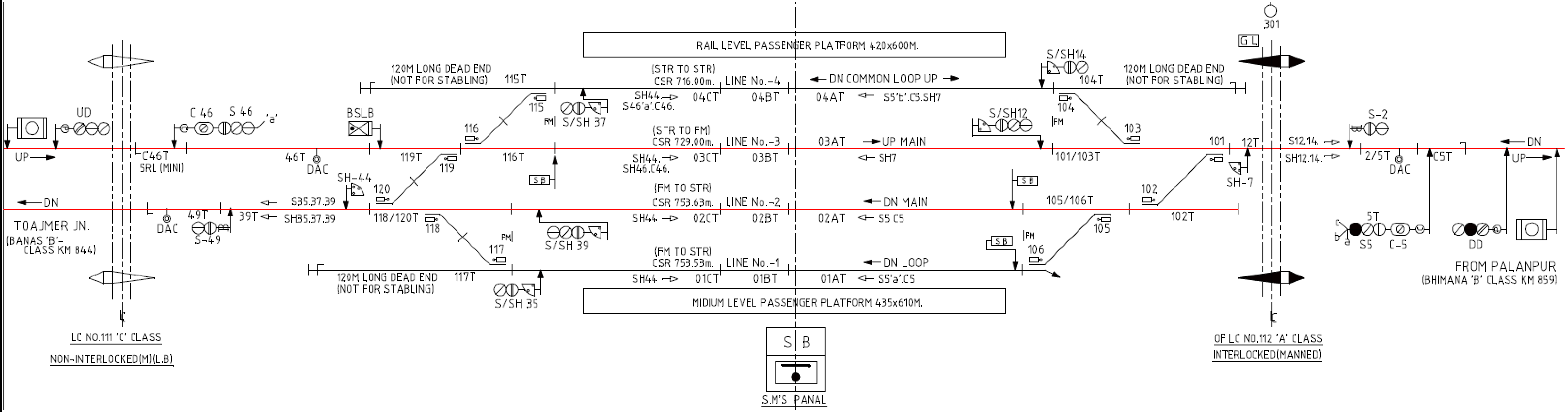
Electronic Interlocking in Railways







Life-cycle of signaling logic: Step-1 (Yard Layout)



Traditionally the layout (signal plan) is created manually

- Upgradations are reflected manually on paper
- No automatic consistency checking
- No automatic way to guarantee that upgradations in signaling plan and control table are consistent

Life-cycle of signaling logic: Step-2 (Control Table)

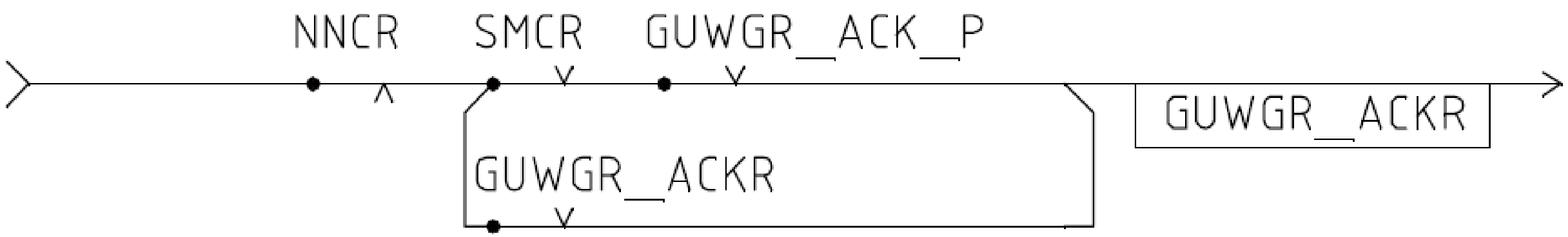
S.NO	MOVEMENT FROM	MOVEMENT TO	BUTTON OPERATION GN	BUTTON OPERATION UN	IN ROUTE POINTS NORMAL	IN ROUTE POINTS REVERSE	IN ROUTE TRACK CIRCUITS	IN ROUTE ISOLATION POINTS NORMAL	IN ROUTE GATE CONTROL & OTHERS SLOTS REQUIRED NORMAL	IN ROUTE CRANK HANDLE	IN OVERLAP POINTS NORMAL	IN OVERLAP POINTS REVERSE	IN OVERLAP TRACK CIRCUITS	IN OVERLAP ISOLATION POINTS	IN OVERLAP GATE CONTROL & OTHERS SLOTS REQUIRED NORMAL	IN OVERLAP CRANK HANDLE	SIGNAL TO DANGER WITH	ROUTE RELEASED TRACK CIRCUITS OCCUPIED/CLEARED	APPROCACH LOCKING	ROUTES LOCKED	SIGNAL ASPECT CONTROLLED BY YELLOW	SIGNAL ASPECT CONTROLLED BY GREEN	REMARKS
1.	S2	BHIMANA	S2	UM	-	-	2/5T	-	-	-	-	-	-	-	-	-	2/5T	-	-	(S5.C5-LN1.2.4) SH7-LN 3.4. SH12.SH14.	-	-	CONTROLLED BY BHIMANA SIDE SINGLE LINE TOKENLESS B/INSTT. IN TGT POSITION WITH SSDAC.
2.	S5'b'	S39	S5	02	105/106	101/102	2/5T 12T 101/103T 102T 105/106T, 02AT/BT/CT	-	301	CH-3 CH-1	117/118 119/120	-	118/120T 39T.	-	-	CH-9 CH-10	2/5T	2/5T 12T 101/103T 102T 105/106T	DEAD	(C46-LN4 W 103/104 R) S2.C5-LN2 SH39 SH44-LN2 C46-LN3 X	S39 R OR Y OR G	-	-
3.	C5	S39	S5+ COGGN	02	105/106	101/102	-	-	301	CH-3 CH-1	-	-	-	-	-	-	-	2/5T 12T 101/103T 102T 105/106T OR THRO'EM. CO.CANC.	-	S2.S5-LN2 S35 SH35.S37 SH37 SH39 SH44-LN1 2 3 4 C46-LN3 X (C46-LN4 W 103/104 R)	-	-	CLEARS 60 SEC. AFTER OCC. OF C5T & REPLACED TO 'ON' WHEN C5T IS CLEARED
4.	S5'a'	S35	S5	01	-	101/102 105/106	2/5T 12T 101/103T 102T 105/106T, 01AT/BT/CT	-	301	CH-1 CH-3	117/118 119/120	- 117/118	117T 117T, 118/120T. 39T.	- -	- -	CH-9 CH-10 CH-6	2/5T	2/5T 12T 101/103T 102T 105/106T.	DEAD	S2.C5-LN1. SH44-LN.2.3 X C46-LN3 X SH44-LN4 W 103/104 R C46-LN4 W 103/104 R S2.C5-LN1. SH35.SH44-LN1. C46-LN3 X C46-LN4 W 103/104 R	S35 R S35 R OR Y	- -	-
5.	C5	S35	S5+ COGGN	01	-	101/102 105/106	-	-	301	CH-1 CH-3	-	-	-	-	-	-	-	2/5T.12T 101/103T 102T 105/106T OR THRO'EM. CO.CANC.	—	S2.S5-LN1.SH35.SH37.S37. SH44-LN 1.2.3 X C46-LN3 X (SH37.S37 W 117/118 R) (SH44-LN4 W 103/104 R & 117/118 R) (C46-LN4 W 103/104 R)	-	-	CLEARS 60 SEC AFTER OCC. OF C5T & REPLACED TO 'ON' WHEN C5T IS CLEARED
							2/5T																

Traditionally the control table is created manually from the layout

- Upgradations are reflected manually on paper
- No automatic consistency checking
- No automatic way to guarantee that upgradations in control table are consistent with application logic

Life-cycle of signaling logic: Step-3 (Application Logic)

GUWGR__ACKR = !NNCR & ((SMCR & GUWGR__ACK__P) # GUWGR__ACKR);



Traditionally the application logic is created manually from the control table

- Uses traditional relay logic (ladder network) for legacy reasons
- Lack of standardization in terms of the set of relays used to define the logic
- RDSO has been working towards a standard for Indian Railways. This will significantly help if vendors are made to comply.

How would we verify 1000 pages of logic which looks like this?

S2GNR = S2GN_P & !S5GNR & !SH7GNR & !S12GNR & !SH12GNR & !S14GNR & !SH14GNR & !S35GNR & !SH35GNR & !S37GNR & !SH37GNR & !S39GNR & !SH39GNR & !SH44GNR & !S46GNR & !S49GNR & !GSBR & !GSRBR & !EWNR;

S5GNR = S5GN_P & !S2GNR & !SH7GNR & !S12GNR & !SH12GNR & !S14GNR & !SH14GNR & !S35GNR & !SH35GNR & !S37GNR & !SH37GNR & !S39GNR & !SH39GNR & !SH44GNR & !S46GNR & !S49GNR & !GSBR & !GSRBR & !EWNR;

SH7GNR = SH7GN_P & !S2GNR & !S5GNR & !S12GNR & !SH12GNR & !S14GNR & !SH14GNR & !S35GNR & !SH35GNR & !S37GNR & !SH37GNR & !S39GNR & !SH39GNR & !SH44GNR & !S46GNR & !S49GNR & !GSBR & !GSRBR & !EWNR;

S12GNR = S12GN_P & !S2GNR & !S5GNR & !SH7GNR & !SH12GNR & !S14GNR & !SH14GNR & !S35GNR & !SH35GNR & !S37GNR & !SH37GNR & !S39GNR & !SH39GNR & !SH44GNR & !S46GNR & !S49GNR & !GSBR & !GSRBR & !EWNR;

SH12GNR = SH12GN_P & !S2GNR & !S5GNR & !SH7GNR & !S12GNR & !S14GNR & !SH14GNR & !S35GNR & !SH35GNR & !S37GNR & !SH37GNR & !S39GNR & !SH39GNR & !SH44GNR & !S46GNR & !S49GNR & !GSBR & !GSRBR & !EWNR;

S14GNR = S14GN_P & !S2GNR & !S5GNR & !SH7GNR & !S12GNR & !SH12GNR & !SH14GNR & !S35GNR & !SH35GNR & !S37GNR & !SH37GNR & !S39GNR & !SH39GNR & !SH44GNR & !S46GNR & !S49GNR & !GSBR & !GSRBR & !EWNR;

SH14GNR = SH14GN_P & !S2GNR & !S5GNR & !SH7GNR & !S12GNR & !SH12GNR & !S14GNR & !S35GNR & !SH35GNR & !S37GNR & !SH37GNR & !S39GNR & !SH39GNR & !SH44GNR & !S46GNR & !S49GNR & !GSBR & !GSRBR & !EWNR;

S35GNR = S35GN_P & !S2GNR & !S5GNR & !SH7GNR & !S12GNR & !SH12GNR & !S14GNR & !SH14GNR & !SH35GNR & !S37GNR & !SH37GNR & !S39GNR & !SH39GNR & !SH44GNR & !S46GNR & !S49GNR & !GSBR & !GSRBR & !EWNR;

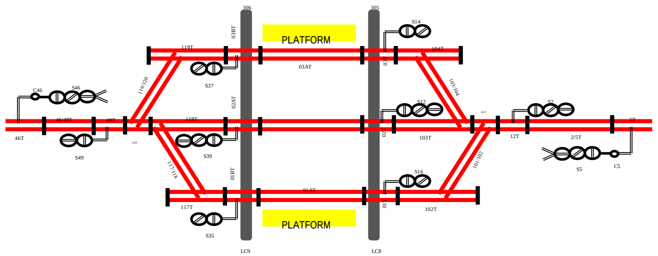
SH35GNR = SH35GN_P & !S2GNR & !S5GNR & !SH7GNR & !S12GNR & !SH12GNR & !S14GNR & !SH14GNR & !S35GNR & !S37GNR & !SH37GNR & !S39GNR & !SH39GNR & !SH44GNR & !S46GNR & !S49GNR & !GSBR & !GSRBR & !EWNR;

S37GNR = S37GN_P & !S2GNR & !S5GNR & !SH7GNR & !S12GNR & !SH12GNR & !S14GNR & !SH14GNR & !S35GNR & !SH35GNR & !SH37GNR & !S39GNR & !SH39GNR & !SH44GNR & !S46GNR & !S49GNR & !GSBR & !GSRBR & !EWNR;

SH37GNR = SH37GN_P & !S2GNR & !S5GNR & !SH7GNR & !S12GNR & !SH12GNR & !S14GNR & !SH14GNR & !S35GNR & !SH35GNR & !S37GNR & !S39GNR & !SH39GNR & !SH44GNR & !S46GNR & !S49GNR & !GSBR & !GSRBR & !EWNR;

S39GNR = S39GN_P & !S2GNR & !S5GNR & !SH7GNR & !S12GNR & !SH12GNR & !S14GNR & !SH14GNR & !S35GNR & !SH35GNR & !S37GNR & !SH37GNR & !SH39GNR & !SH44GNR & !S46GNR & !S49GNR & !GSBR & !GSRBR & !EWNR;

Life-cycle for Signaling Logic



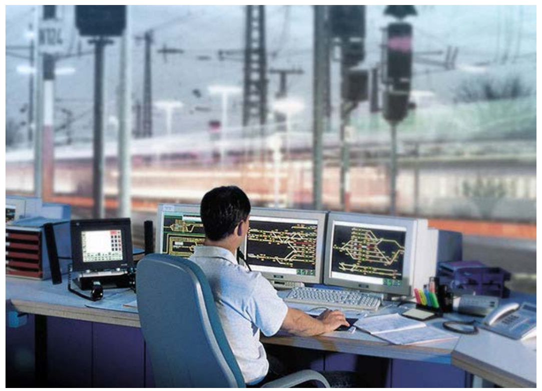
Control Table

Application Logic

Factory Acceptance Testing (FAT)
Thousands of tests, where engineers visually examine the signaling principles !!

Railways has to pay for each loop

Error in logic?

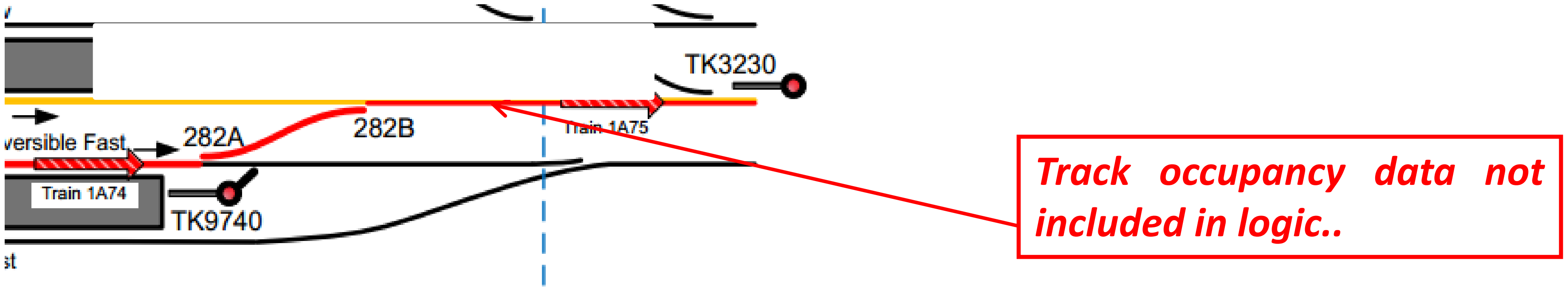


Deployment and Site Acceptance Testing (SAT)

Upgradation needed?

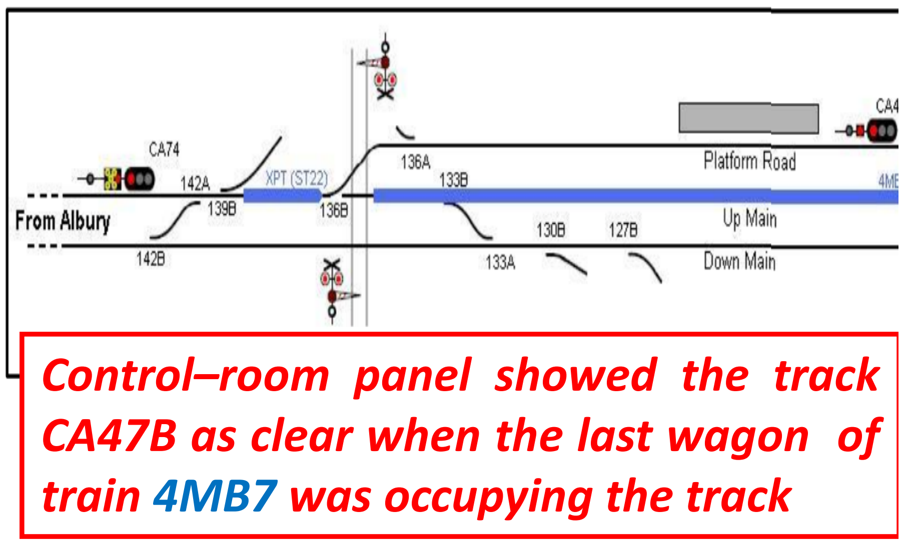
Milton Keynes, UK, 2008 – Cause

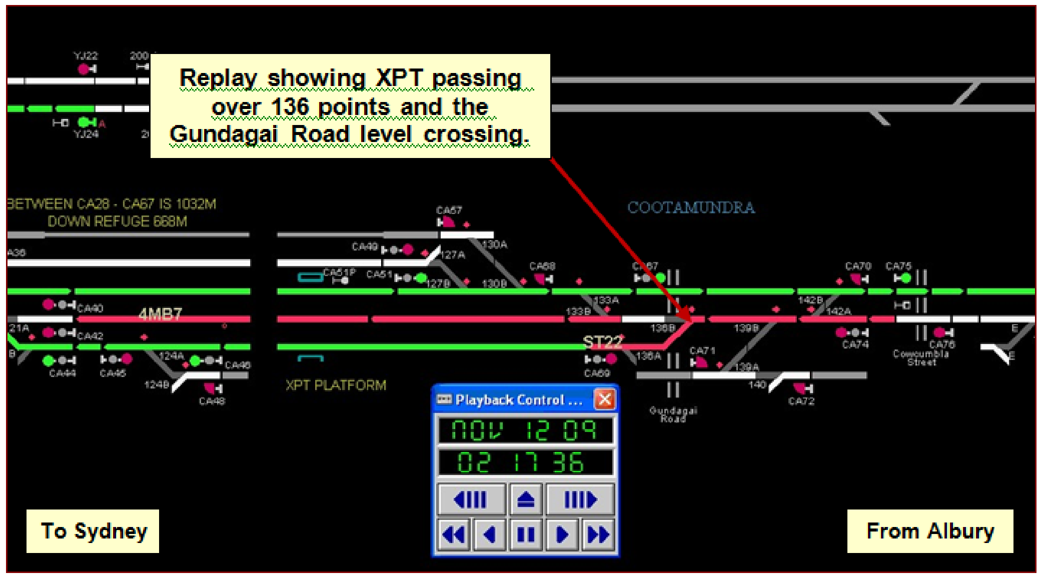
Formal investigations revealed, the axle-counter data was not included in the SSI logic associated with the aspect controls for signals *TK9740* and *TK3230*



Cootamundra, NSW Australia, 2009 – The incident

Figure 3: Signal schematic (part) - Cootamundra Yard.





Railway Safety Standards recommend *Formal Methods*

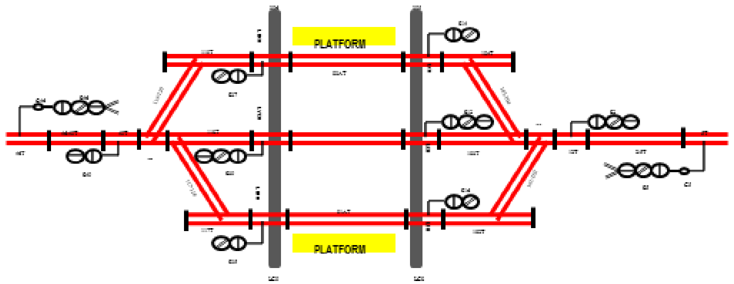
Table A.4 — Software design and implementation (clause 10)

TECHNIQUE/MEASURE	Ref.	SWSIL 0	SWSIL 1	SWSIL 2	SWSIL 3	SWSIL 4
1. Formal methods including for example CCS, CSP, HOL, LOTOS, OBJ, Temporal Logic, VDM, Z and B	B.30	—	R	R	HR	HR
2. Semi-formal methods	D.7	R	HR	HR	HR	HR

Source: Page 50, EN50128: 2001

There are no guidelines in EN50128 on how such methods may be used in the context of Application Logic

IIT Kharagpur Contributions



Layout Editor Tool

- Yard layout is created using this tool
- The tool can perform several sanity checks
- Updates can be made as and when required

SL NO	ENTRY SIGNAL	EXIT SIGNAL	ROUTE	ROUTE		OVERLAP				CONTROLLED BY TRACK CIRCUIT	SIGNAL REPLACED BY TRACK CIRCUIT	BACK LOCKED UNTILL TRACK CIRCUIT CLEAR	LEVEL CROSSING	CRANK HANDLES	CONFLICTING ROUTES
				POINT NORMAL	POINT REVERSE	TRACKS	POINT NORMAL	POINT REVERSE	OVERLAP SET						
1	S1	S5	1A	51	---	5T, 07T	52	---	OV-5	1T, 2T, 02T, 4T, 04T, 05T1, 05T2, 05T3, 05T	1T	1T, 2T, 02T, 4T	LC 1	CH1, CH2	C-1A, 4, 8A, 78A
2	S1	S3	1BD	---	51	3T	52	---	OV1-3	1T, 2T, 02T, 4T, 6T, 06T, 06T1, 06T2, 06T3, 03T	1T	1T, 2T , 02T, 4T, 6T	LC 1	CH1, CH2	C-1B, 6, 78A
			1BM			3T, 5T, 07T	---	52	OV2-3				LC 1		C-1B, 6, 8B, 78A, 78B, 8A, 5
3	S3	S7	3	---	52	---	---	---	---	3T, 5T, 07T	3T	3T, 5T		CH2	8B, 78B, 6, C-1B
4	S5	S7	5	52	---	---	---	---	---	5T, 07T	5T	5T		CH2	8A, 78A, 4, C-1A

Control Table Generator Tool

- Control table is automatically generated from the layout created by layout editor
- The tool checks for inherent inconsistencies
- Push-button solution whenever the layout is upgraded

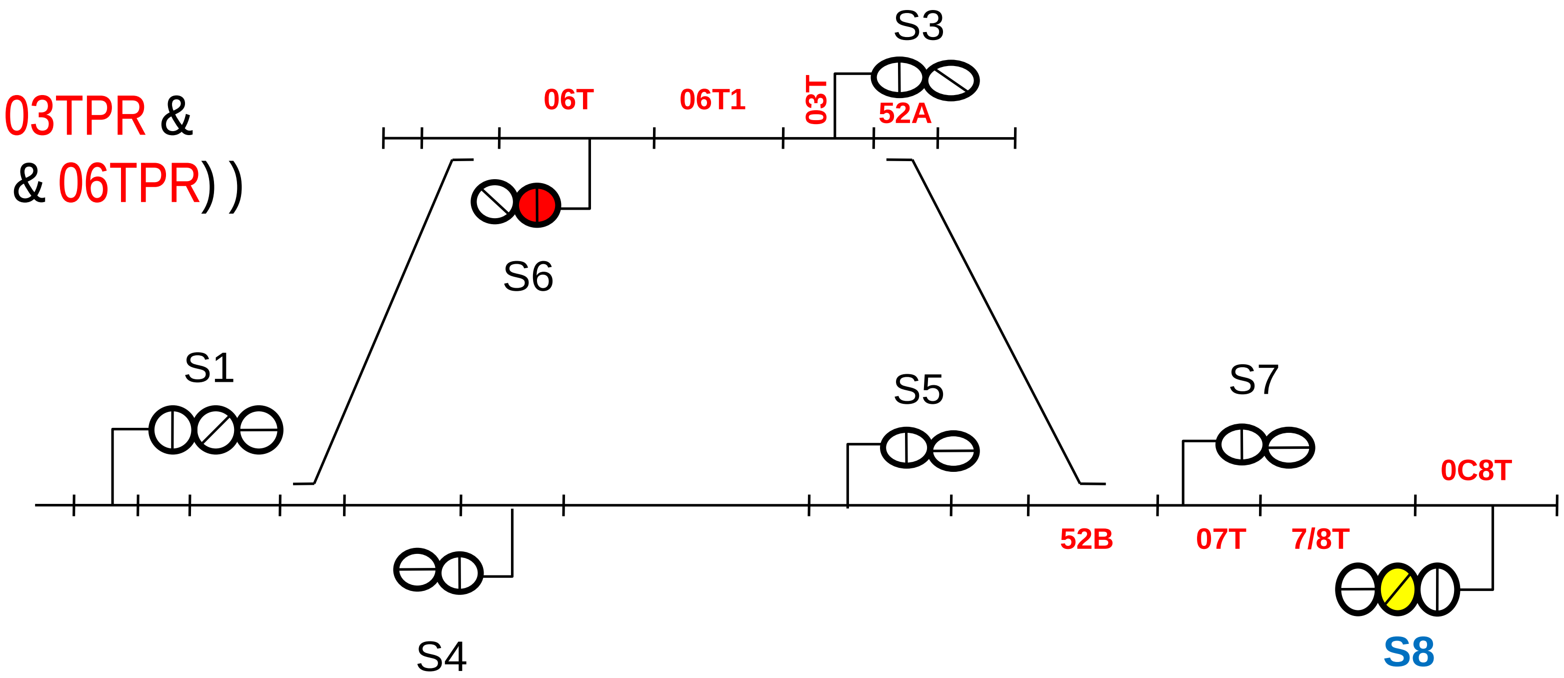
IIT Kharagpur Contributions

The SafeR Tool

- Reads the control table
- Creates a comprehensive set of *formal properties*
- Built in knowledge about international railway signaling principles
- Thousands of properties are automatically verified using back-end formal tools

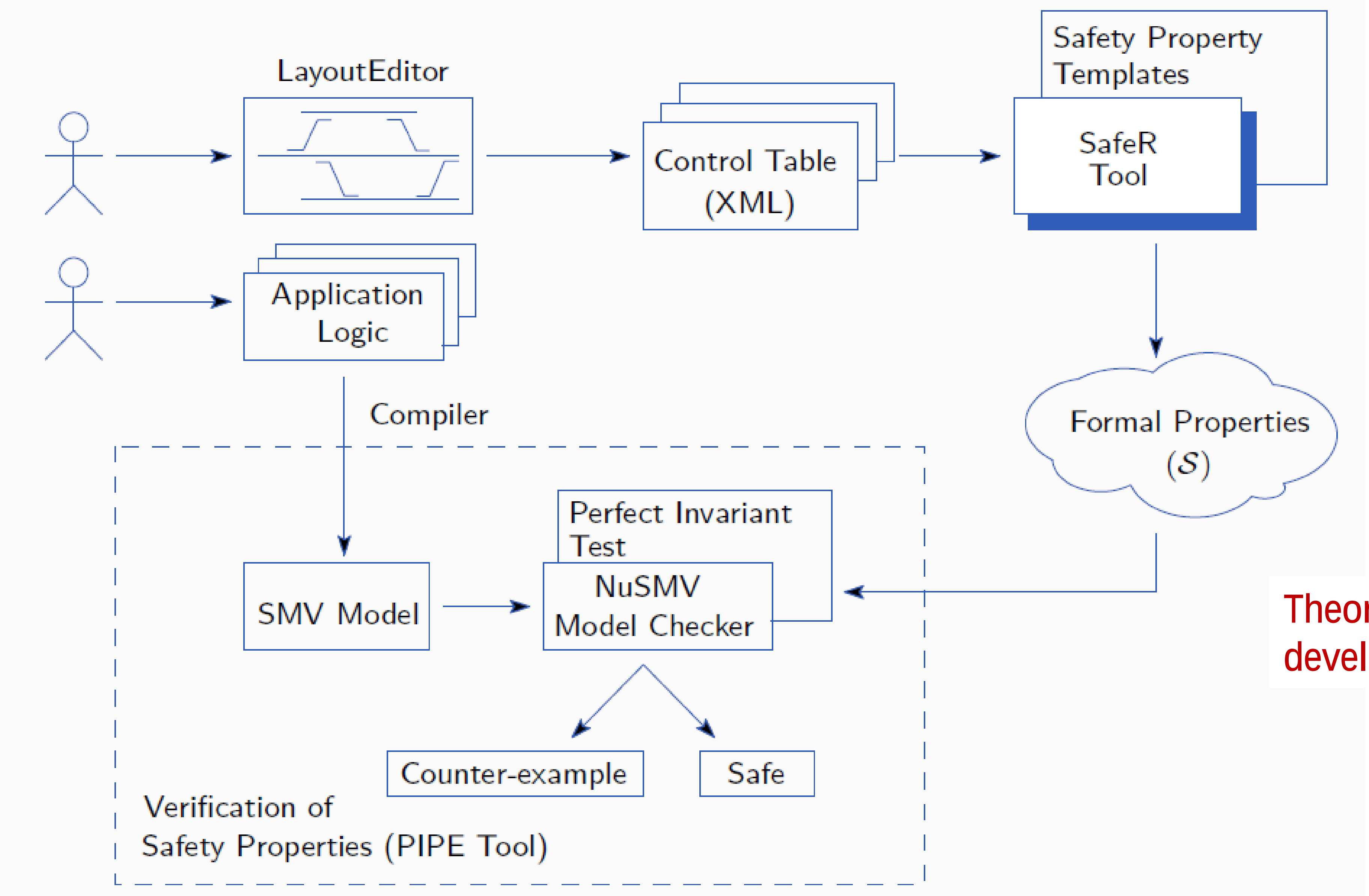
Example: Proving that the track circuits in the route up to the next signal and its overlap are clear. SafeR generates the following formal property.

LTLSPEC G(X 8HR → (0C8TPR & 7/8TPR & 07TPR & 52BTPR & 52ATPR & 03TPR & 06_1TPR & 06TPR))



8HR is the "YELLOW" signal relay
TPR are track status relays

IIT-KGP EI Verification Tool Flow



Theory of perfect invariants developed for scaling verification