Formal analysis of railway signalling data

Alexei Iliasov
- SafeCap/SafeCap+/SafeCap-Impact/… projects
  - formal verification of signalling and interlocking
  - capacity optimisation
  - automated train operation and driver advisory systems
• Train control and formal methods

• Cost efficiency of safety measures

• Challenging rule of thumb safety principles

• Interplay of safety and capacity

• ERTMS Level 3
  • very tight safety envelope
  • plenty of options for capacity optimisation
railway operation is both mission and safety critical
(re-) design of a railway is a predominantly digital process
a range of digital assets must be produced and cross-checked: track topology, track side equipment, interlocking logic, timetables, etc.
railway industry (almost) exclusively uses review and simulation
• an extensive amount of data is collected and created describing existing or planned railway operation

• we propose to do formal checking of data consistency

• and attempt to verify high-level goals on the basis of concrete data
• Model construction
  • for each data storage format there is a procedure to extract relation graphs (sets of mappings)
  • a type inference process constructs typed relations types unified within and across inputs
  • the end result is a set-theoretic representation of input data
  • untyped parts are reported and discarded
  • input models are often under-specified: there would references to undefined elements
• Verification

  • a conjecture may be posited asserting a property of the input data
    the conjecture plus set-theoretic model of input data are either

  • in a contradiction

  • non-constraining if previously abstract relations remain
    unconstrained

  • constraining if the conjecture makes the input data model more
    specific

• a number of constraining conjectures must be given to tighten data
  semantics and the meaning of missing data

• verification property is a conjecture that is a contradiction (error in input
  data) or is non-constraining
Verification

- conjectures are formulated as SMT problems and passed to a number of state-of-the-art provers: Z3, Vampire, ProB, SPASS, E, ...

- once proven, a conjecture may be relied upon in following proofs (and thus complex statements may be effectively and safely decomposed)

- ultimately: show that signalling configuration data meets the SIL 4 industry standards of CENELEC (EN 50126, 8 & 9) and IEC 61508
• Questions?