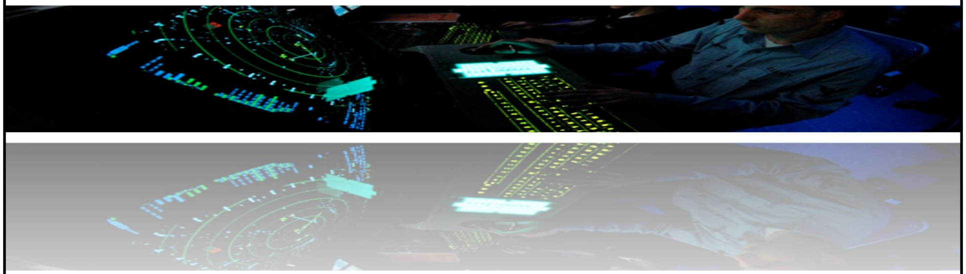
4th June, 2019

SafeCap

Automated formal verification of railway signalling interlockings

Presented by Dr Alexei Iliasov (*alexei.iliasov@newcastle.ac.uk*) &
Eur Ing Dominic Taylor MIRSE MBA (*dtaylor@systra.com*)



Newcastle University UK | Malaysia | Singapore

SYSTRA SCOTTLISTER

SafeCap

Plan for tutorial

1. Introductory presentation
   - Current approach to interlocking data
   - Benefits of automated verification
   - The SafeCap approach to automated verification
   - Expected benefits of SafeCap
   - Current SafeCap application
   - Illustrative example
   - Adaptability and certification

Newcastle University UK | Malaysia | Singapore

SYSTRA SCOTTLISTER

Slide 2

SafeCap

Plan for tutorial

2. SafeCap technology

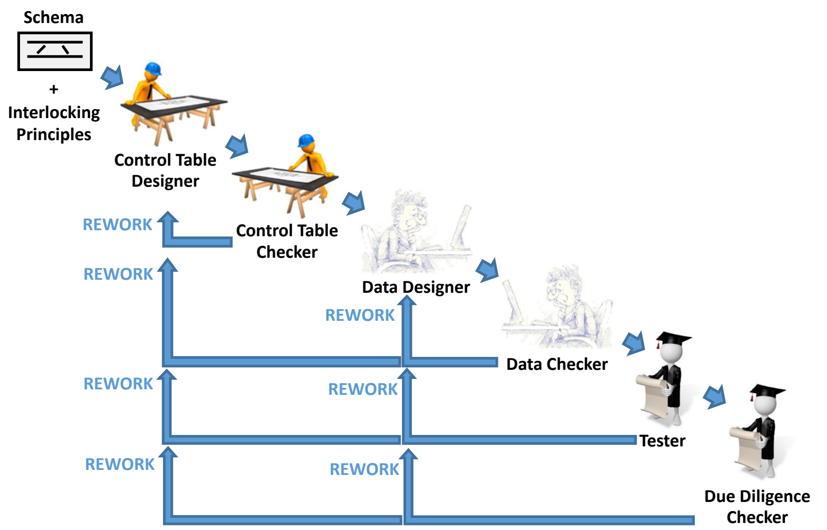
3. Demonstration
   - Entry of a real world layout and interlocking data
   - Transformation into a state transition system, defined in formal notation
   - Verification against safety properties that express signalling principles
   - Production of automated report

Newcastle University UK | Malaysia | Singapore

SYSTRA SCOTTLISTER

Slide 3

Introductory presentation
Current approach to interlocking data



Newcastle University UK | Malaysia | Singapore

SYSTRA SCOTTLISTER

Slide 4

Introductory presentation
Benefits of automated verification

By contrast to the current manual approach, automatic data verification can be

- much quicker (minutes versus weeks),
- cheaper (as it is far less labour intensive) and
- more comprehensive in its scope.

Introductory presentation
The SafeCap approach to automated verification

- Approaches to automatic verification can be categorised as follows.
  - **Automated test scripts -** easy to implement, but limited in what they test.
  - **Formal verification -** comprehensive, but historically have required large up-front investment and process change.
- SafeCap overcomes previous limitations by applying formal methods **incrementally within existing data processes**.

Introductory presentation
The SafeCap approach to automated verification

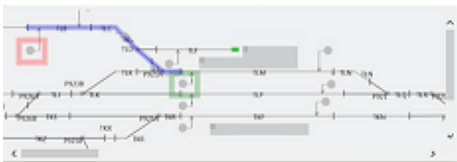
- Interlocking data is automatically read in the format used by signalling engineers and converted into a state transition system
- Signalling layouts are entered in graphical form, familiar to signalling engineers, and automatically converted into machine readable datasets
- Signalling principles are represented as safety invariants, configured within SafeCap, for which the tool seeks to automatically proof compliance

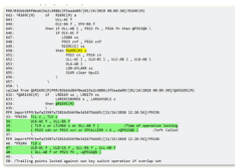
Newcastle University UK | Malaysia | Singapore

SYSTRA SCOTTLISTER

Introductory presentation
The SafeCap approach to automated verification

Results are presented in an automated report with graphical illustrations of where safety invariant violations were found





Newcastle University UK | Malaysia | Singapore

SYSTRA SCOTTLISTER

Introductory presentation
Expected benefits of SafeCap

- Estimated cost savings of **5 – 10%** for initial advisory service *
  10 – 20% as scope of verification increases *
  30 – 50% if safety case developed †
- **1-3 months reduction** in project duration for initial advisory service
- **Improved confidence in safety of data**

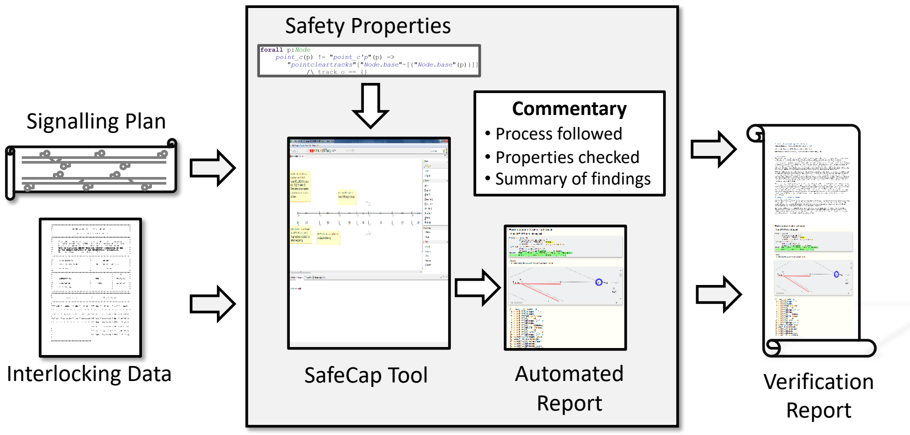
** through reduction in re-work.*
† through elimination of checking / testing activities.

Newcastle University UK | Malaysia | Singapore

SYSTRA SCOTTLISTER

Slide 9

Introductory presentation
Current SafeCap application



Newcastle University UK | Malaysia | Singapore

SYSTRA SCOTTLISTER

Slide 10

Introductory presentation
Current SafeCap application

Currently, SafeCap verifies the following signalling principles:

- Points deadlocking
- Points locked by sub-route
- Points locked by route
- Points locked in front of train in route
- Technician's route disable
- Other classes of route normal.

Newcastle University UK | Malaysia | Singapore

SYSTRA SCOTTLISTER

Slide 11

Introductory presentation
Current SafeCap application

- SafeCap has been trialled on real world data sets for multiple station areas in the UK.
- Data has been analysed for Solid State Interlocking (SSI) Geographic Data Language (GDL) for two different interlocking technologies
- Two previously known errors, which would have allowed points to move underneath a train, were successfully found in (non in-service) versions of the data.
- Over ten deliberately seeded errors were successfully found in data.
- SafeCap has also identified a number of risk areas, where there was no immediate safety issue, but where the logical complexity meant that one could easily be introduced by modification of an interlocking or its neighbour.

Newcastle University UK | Malaysia | Singapore

SYSTRA SCOTTLISTER

Slide 12

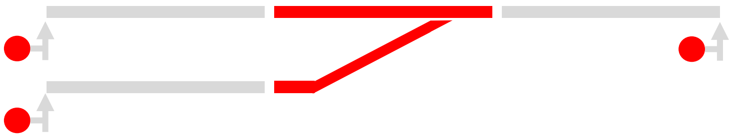
Introductory presentation
Illustrative example: points deadlocking

NR/L2/SIG/11201/Mod B11, Issue 5, Clause 4.5.1 Pg 4 b)

The tools shall be capable of establishing…that points cannot be called to move when track deadlocking is applied;

NR/L2/SIG/30009/GKRT0060, Issue 2, Clause C6.3 b)

Points shall only be permitted to move if they are free of all of the following conditions:… track locking (including dead … locking)



Newcastle University UK | Malaysia | Singapore

SYSTRA SCOTTLISTER

Introductory presentation
Illustrative example: points deadlocking

G 1
Commanded position of points never changes when a track section over those points is detected to be occupied.

↓

Property 13 : Point movement track circuit check

Whenever a point is commanded to a new position it is checked that all the track circuits over which the point lies (accounting for merged points) are checked free.

Semi formal

for
every point setting command `Pxx c`
it holds that
every track section over which the point lies is positively checked free `Txx c`

Newcastle University UK | Malaysia | Singapore

SYSTRA SCOTTLISTER

Introductory presentation
Illustrative example: points deadlocking

…but

testing this property by itself can lead to false positives as it makes no assumptions about other safety properties

to remove these false positives, we have to constrain it with a lemma (such as points always align with locked sub-overlaps) and prove this lemma as a separate safety property.

Newcastle University UK | Malaysia | Singapore

SYSTRA SCOTTLISTER

Slide 15

Introductory presentation
Illustrative example: points deadlocking

G 1
Commanded position of points can only change when all track sections over

Property 13b : Point movement track circuit check

Whenever a point is commanded to a new position it is checked that all the track circuits over which the point lies (accountin sub-overlap locked in a directi different) set of points.

Semi formal

for
every point se
it holds that
every track se
or
there is a sub
when those po
or
there is a sub-overlap locked `Uyy l` over a (potentially different) set of points in the reverse lie
when those poinst are commanded normal `Pyy cn`

Property 14a : a

Whenever a poin which the point ir

Semi formal

for
every point settin
it holds that
every sub-overla

Property 14b : alignment of sub overlap locking with points

Whenever a sub-overlap is locked over a set of points it is checked that those points are commanded to a position consistent with the sub-overlap

Semi formal

for
every sub-overlap locking command `Oxx l`
it holds that
every set of points that the sub-overlap passes over in the normal direction is commanded normal `Pxx cn`
and
every set of points that the sub-overlap passes over in the reverse direction is commanded reverse `Pxx cr`

Newcastle University UK | Malaysia | Singapore

SYSTRA SCOTTLISTER

Slide 16

Introductory presentation
Adaptability and certification

- SafeCap has shown itself a viable approach with SSI geographic data language, widely used by UK signalling engineers
- By modifying the front-end conversion tool, SafeCap is readily adaptable to other interlocking languages: HLL, ladder logic, etc.
- Safety invariants can similarly be specified as required to align with the signalling principles employed by different railways

Newcastle University UK | Malaysia | Singapore

SYSTRA SCOTTLISTER

Slide 17

Introductory presentation
Adaptability and certification

- Currently SafeCap can operates in an advisory capacity, helping signalling engineers find errors earlier in the design process
- The technology has the potential to deliver much greater benefits if used as an alternative to current manual checking and testing processes such as
  - 'due diligence' verification of data carried out by a railway client or
  - a signalling supplier's internal processes.
- This would require some level of safety certification, the level of which varies according to the dependency placed on the tool

Newcastle University UK | Malaysia | Singapore

SYSTRA SCOTTLISTER

Slide 18

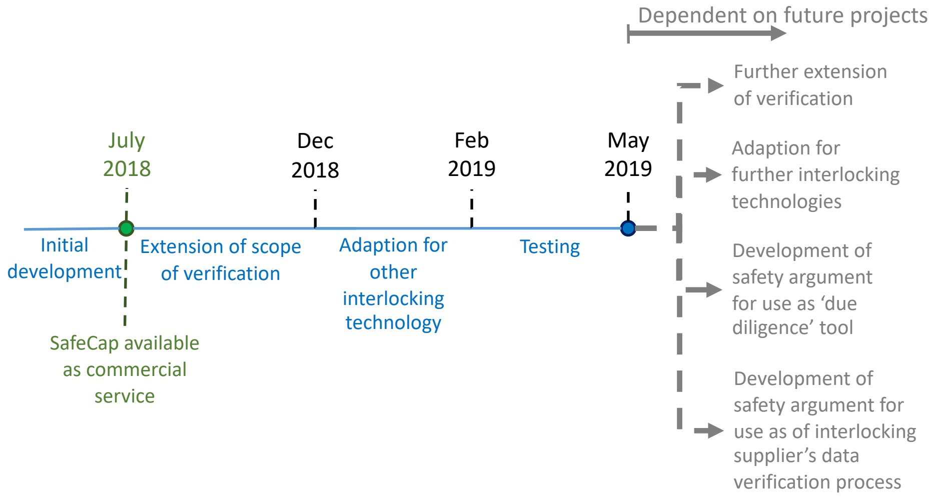
Introductory presentation
Adaptability and certification

- Expertise on how to approach such safety certification is being provided by Frazer-Nash consultancy
- Two possible approaches have emerged
  - Where a low level of dependency is placed on the tool, safety could be demonstrated through testing with in-service data sets
  - Where there is a higher depending, such as replacing supplier checking / testing procedures, a dedicated tool would need to be developed and assessed in accordance with EN 50128 for a specific Safety Integrity Level (SIL)

Newcastle University UK | Malaysia | Singapore

SYSTRA SCOTTLISTER

Introductory presentation
Adaptability and certification



Newcastle University UK | Malaysia | Singapore

SYSTRA SCOTTLISTER

2.

SafeCap Technology

Newcastle University UK | Malaysia | Singapore

SYSTRA SCOTTLISTER

Slide 21

SafeCap Technology

SafeCap Philosophy

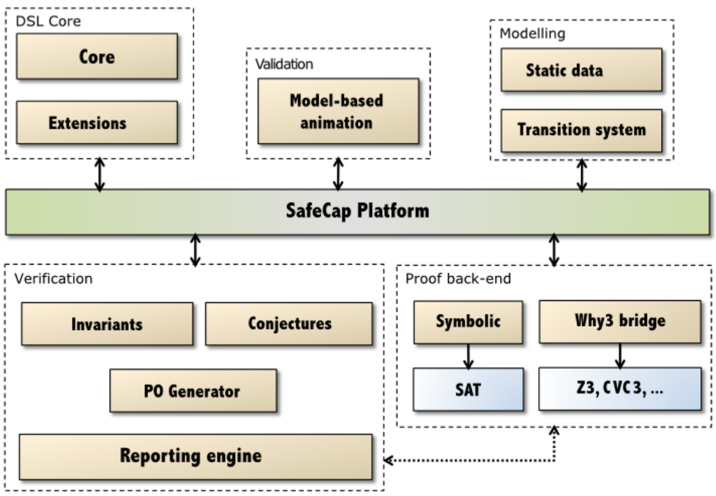
- ***Notation-less*** *formal method, an assembly language of FMs*
  - *FOL + ZF set theory*
  - *state transition system*
  - *stored in a database*
- *Maximum* ***proof efficiency*** *and scalability*
  - *Symbolic prover with third party provers*
  - *SAT*
  - *SMT-LIB2*
  - *Why3: Alt-Ergo, Z3*

Newcastle University UK | Malaysia | Singapore

SYSTRA SCOTTLISTER

Slide 22

SafeCap Technology

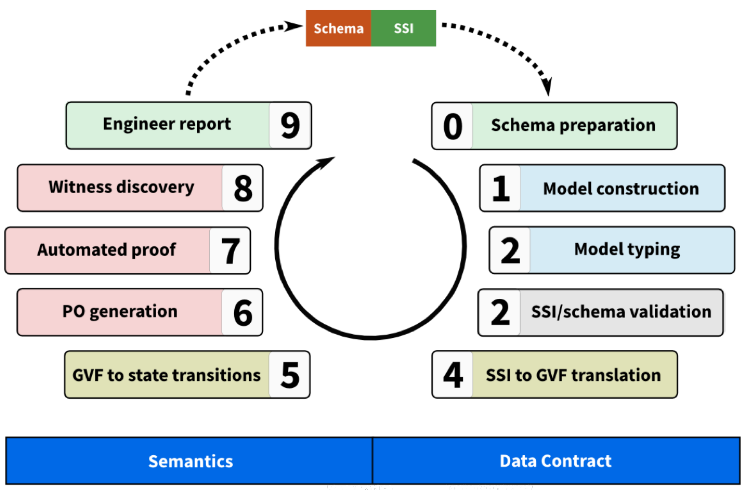


Newcastle University UK | Malaysia | Singapore

SYSTRA SCOTTLISTER

Slide 23

SafeCap Technology



Newcastle University UK | Malaysia | Singapore

SYSTRA SCOTTLISTER

Slide 24

3.

Demonstration

Slide 25