26th September, 2019

Safecap

Automating Signalling Verification Using Formal Methods

Presented by Eur Ing Dominic Taylor MBA

Newcastle University
UK | Malaysia | Singapore

SYSTRA SCOTTLISTER

Safecap

Automating Signalling Verification Using Formal Methods

1. Railway signalling

2. Signalling interlockings

3. Automating interlocking verification

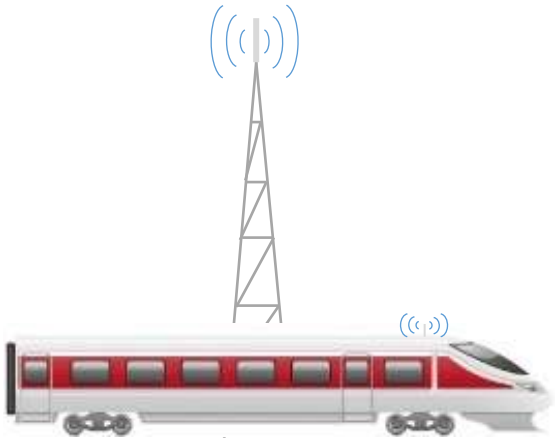
Railway Signalling

Signalling enables railways to operate train services that

- travel at high speed,
- run close together and
- serve multiple destinations.

Railway Signalling

It only allows trains to move when it is safe to do so.

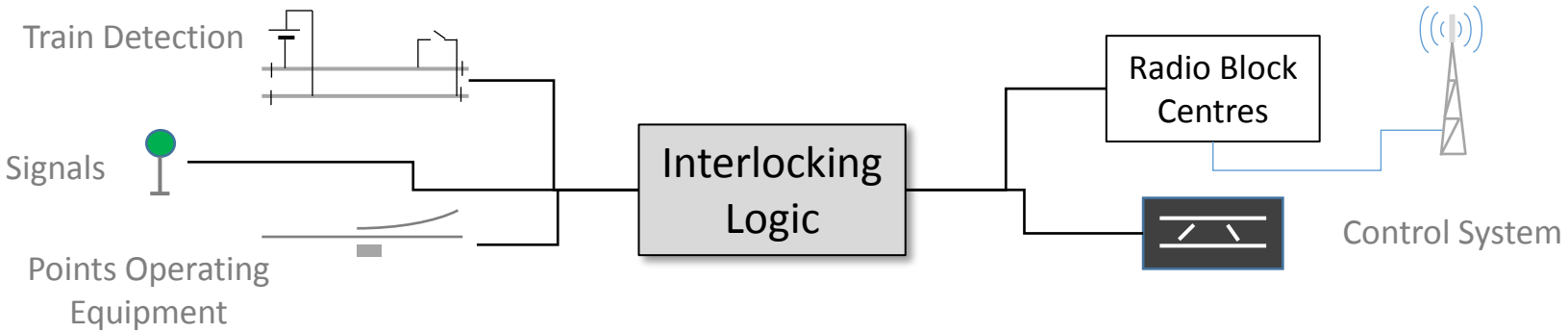


Railway Signalling

It locks moveable infrastructure before a train can travel over it.

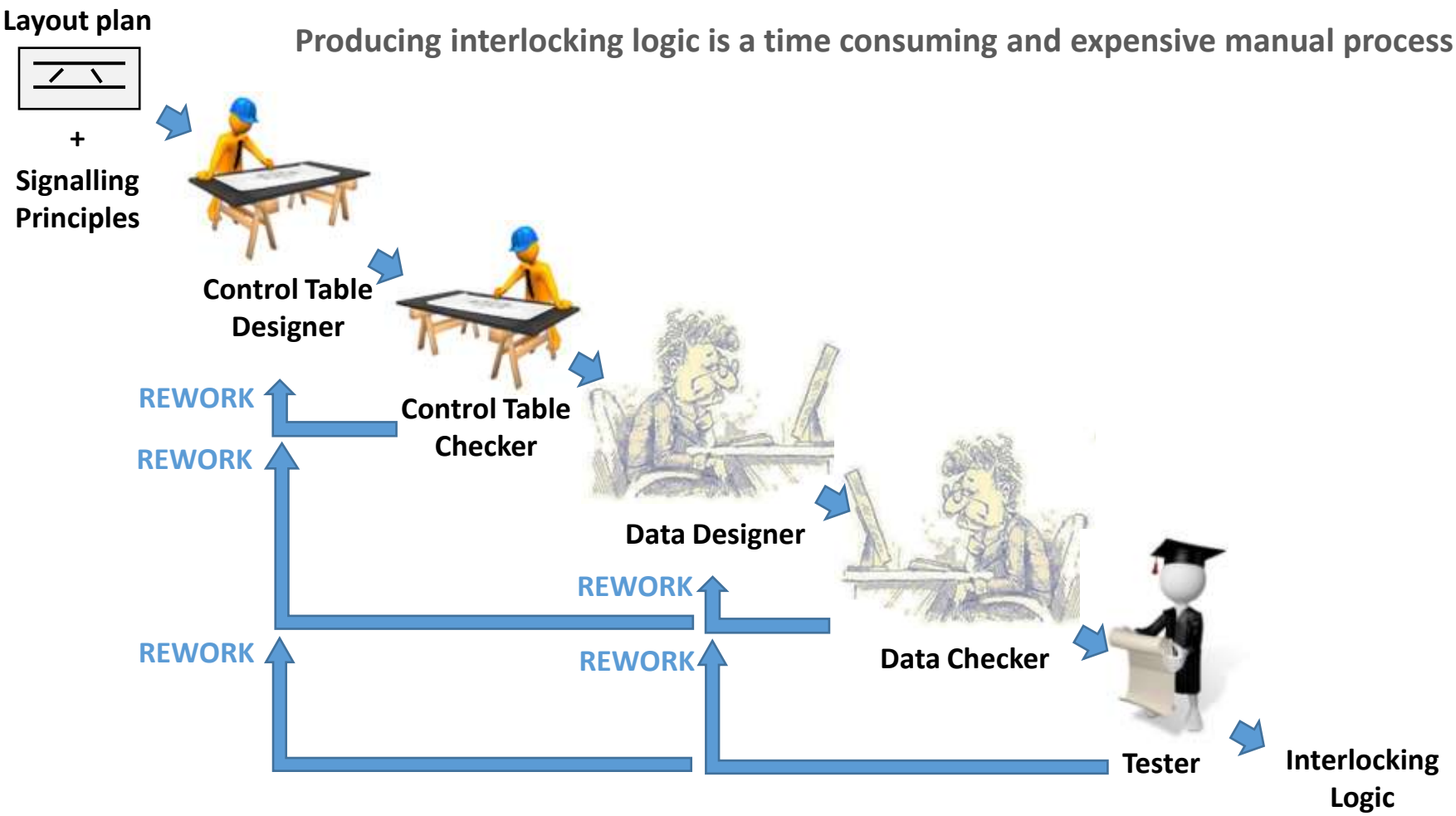
Signalling Interlocking Logic

- At the heart of a signalling system is the interlocking logic.



- This constrains authorisation of train movements and movement of infrastructure to prevent unsafe events:
  - train passing over moveable infrastructure when it is not safe to do so;
  - train colliding with another train;
  - train traveling too fast around a curve.

Signalling Interlocking Logic



Signalling Interlocking Logic

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

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

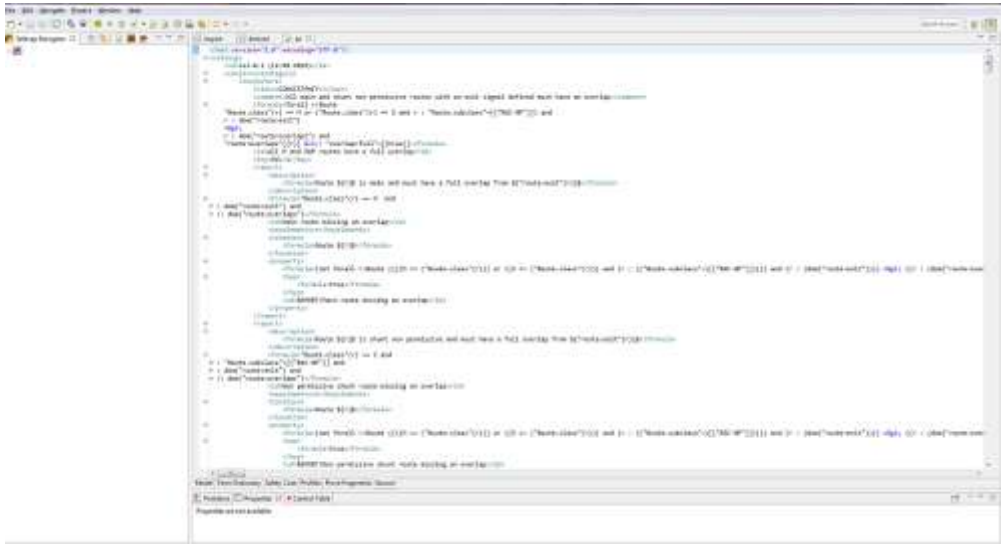
Automating interlocking verification

- Approaches to automatic verification can generally be categorised as follows.
  - **Automated test scripts:** easiest to implement, but limited in scope.
  - **Formal methods tools:** comprehensive, but have previously required large upfront investment and been limited to simple layouts.

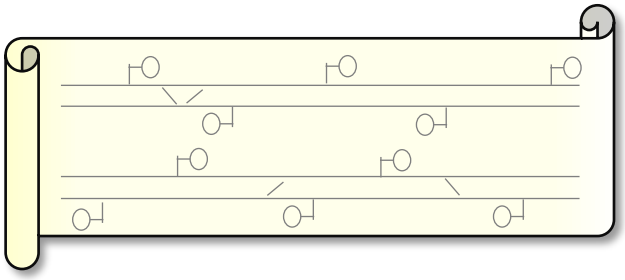
- The SafeCap Approach overcomes existing limitations by applying formal methods **incrementally within existing processes.**

Automating interlocking verification

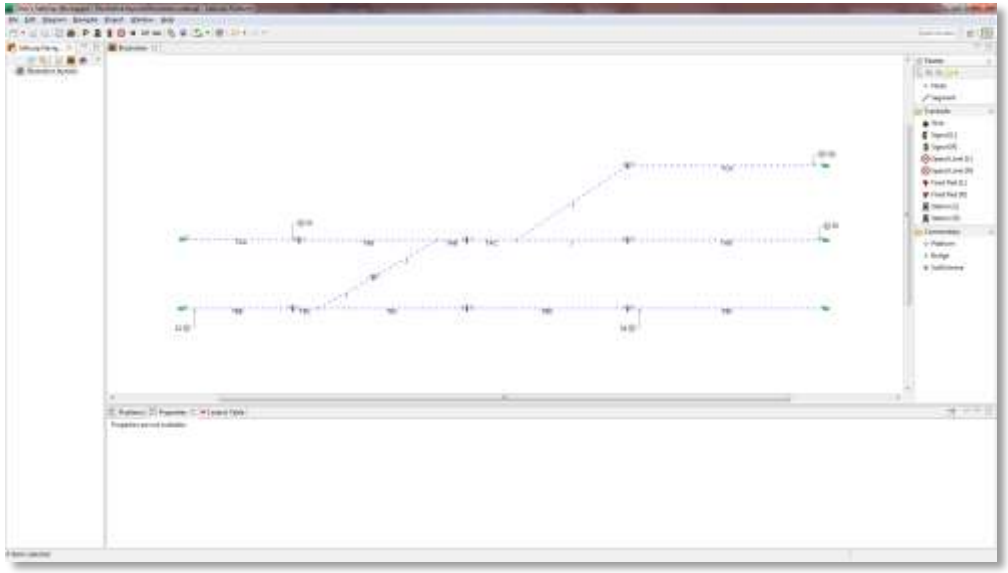
Interlocking logic is automatically read in the data formats used by signalling engineers



Automating interlocking verification

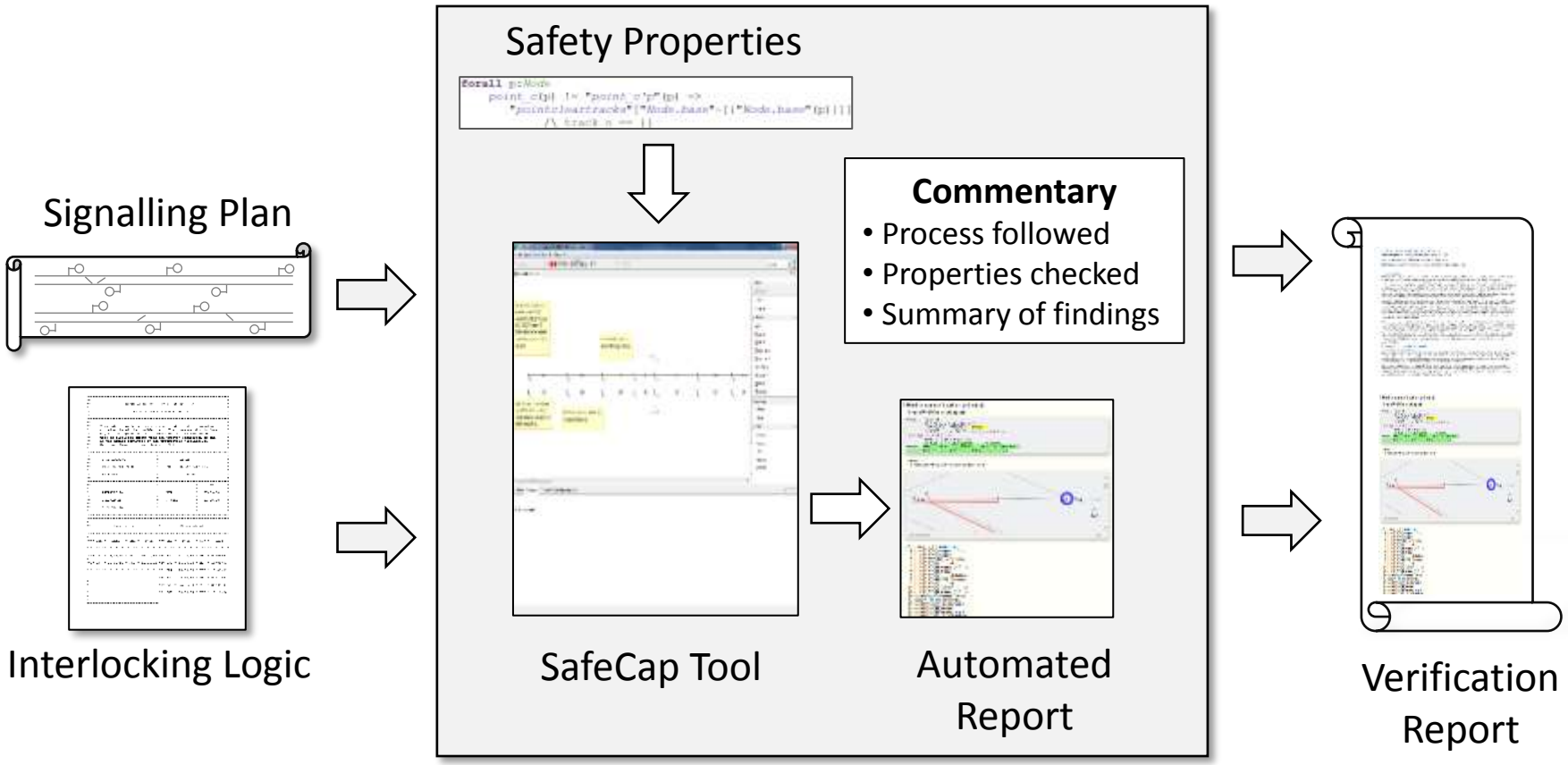


Signalling layouts are entered in graphical form, familiar to signalling engineers



Automating interlocking verification

Results are presented in a graphical report, illustrating where issues were found with extracts from the interlocking logic and layout drawing



Automating interlocking verification

- 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 logic**

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

Automating interlocking verification

Six interlockings analysed

- All known errors found (including seeded errors)
- Intended violations of normal principles identified
- Significant risk areas identified in logic

Typical verification times

Case study	Number of routes	Number of state transitions	Verification time, seconds
N	220	22115	192
T	93	5293	142
O	118	2322	141
PW	56	956	102

Summary

- Railway signalling is essential for delivering high-quality, cost effective services to railway customers
- Producing signalling interlocking logic is currently an expensive, time-consuming manual process
- By automating verification of interlocking logic, SafeCap enables time and cost savings in the delivery of signalling projects