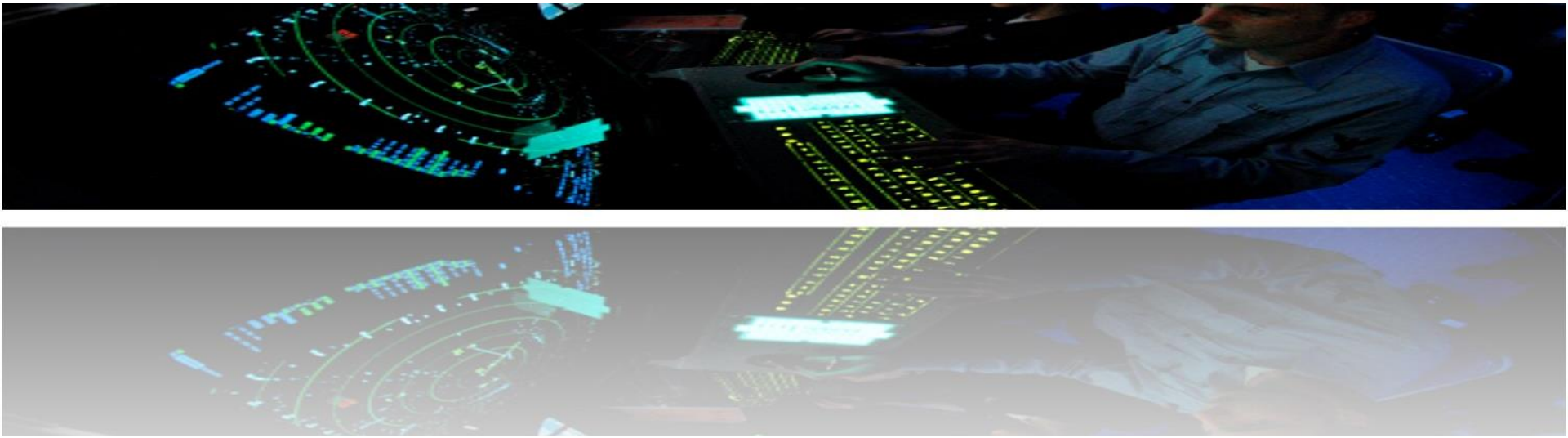
24th October, 2019

Driving Efficiency & Resilience to Human Error:
SafeCap Automated Verification of Signalling Data

Presented by Eur Ing Dominic Taylor MIRSE MBA (dtaylor@systra.com)



Driving Efficiency & Resilience to Human Error:
SafeCap Automated Verification of Signalling Data

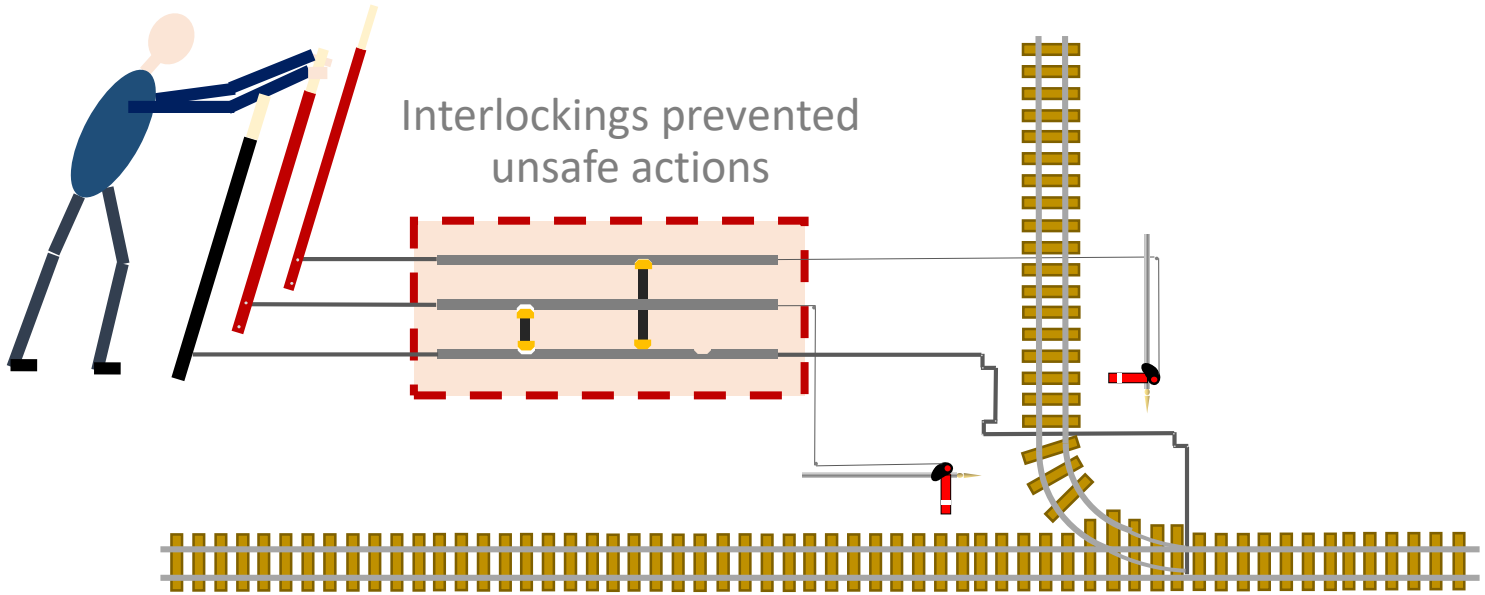
1. Resilience to error provided and eroded by signalling
2. Efficiency and resilience in complex software systems
3. SafeCap practical results and findings
4. Future developments

1.

Resilience to error provided and eroded by signalling

In the beginning:

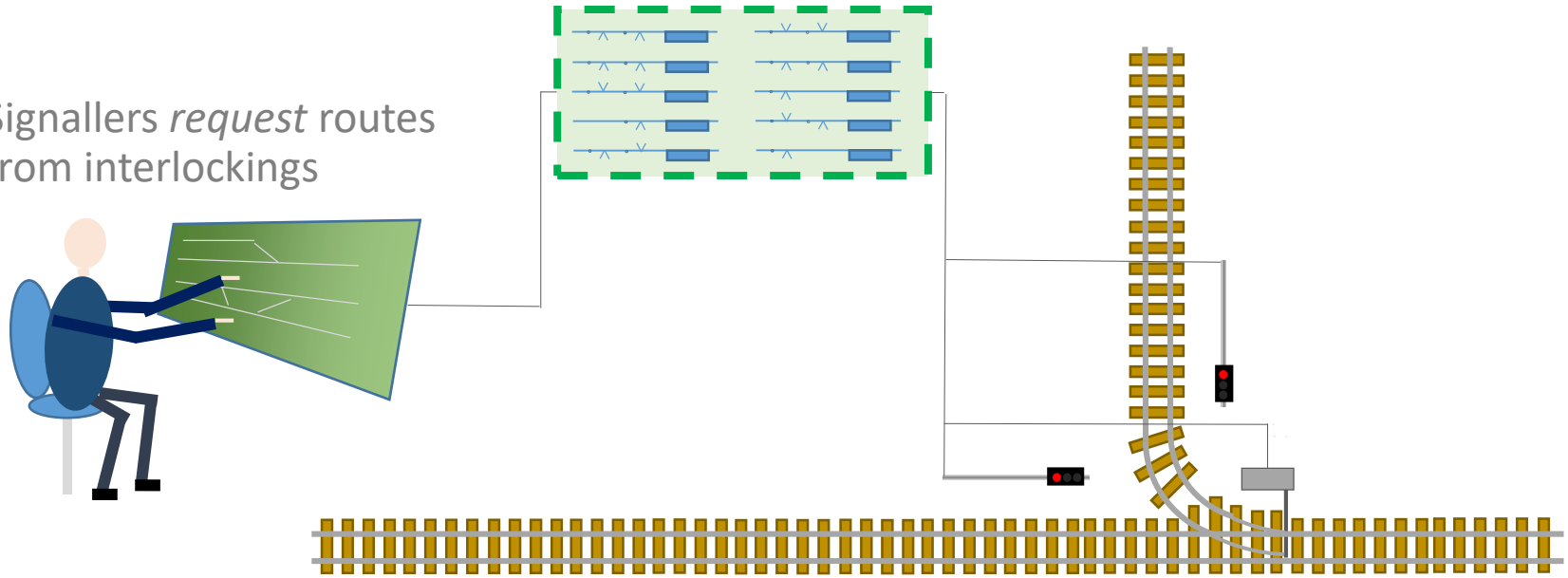
Signallers physically controlled signals and points and visually detected trains



With the advent of power signalling:

Interlockings electrically control signals and points and detect trains

Signallers *request* routes from interlockings



Resilience to error provided and eroded by signalling
Vulnerability to Designer Error Brought About by Automation

A fault in the interlocking can now lead to an accident,
even when the signaller does nothing unsafe

Source: Investigation into the Clapham Junction Railway Accident, Department of Transport (UK)

Source: Rail Accident Report, Collision at London Waterloo 15 August 2017, Rail Accident Investigation Branch (UK)

Resilience to error provided and eroded by signalling
The Impact of Increasing Software Complexity and Control

Increasing data complexity increases likelihood of an error

X

Increasing automation increases risk of unsafe state resulting from error

X

Increasing traffic increases accident risk associated with unsafe state

2.

Efficiency and resilience in complex software systems

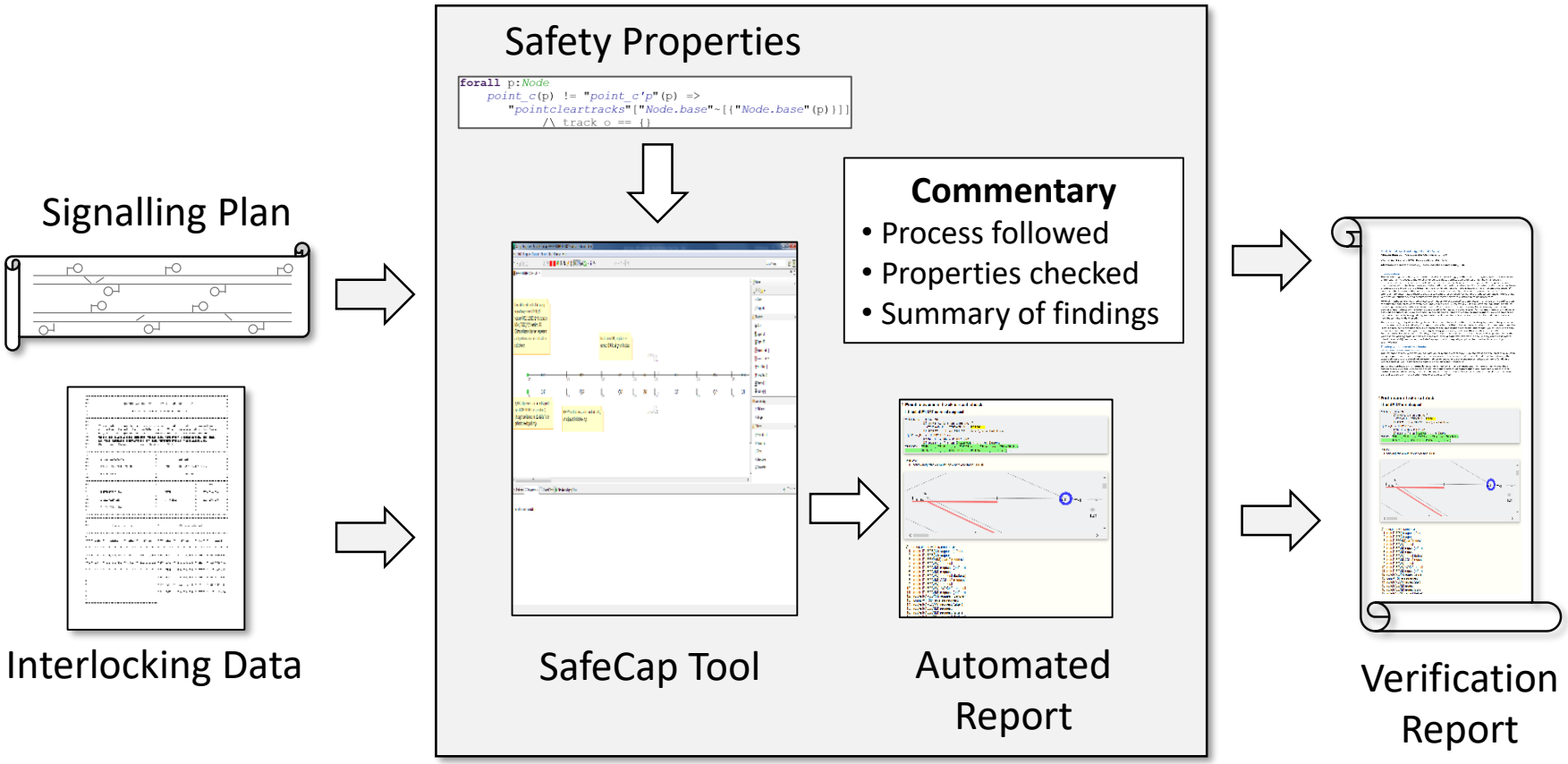
Efficiency and resilience in complex software systems
Formal verification

- Formal verification uses logic to reason about complex systems
- Unlike testing, formal verification is comprehensive within the constraints of the properties being verified
- Modern computational power enables automated reasoning tools that can process thousands of formal proofs within a few seconds

Efficiency and resilience in complex software systems
Formal verification

- Formal verification methods have been successfully used in multiple industries including transport, defence, telecommunications and power
- The uptake of formal verification in railway signalling has previously been hampered by limited scalability and upfront costs
- SafeCap overcomes previous limitations by applying static verification **incrementally within existing data processes**.

Efficiency and resilience in complex software systems
The SafeCap approach



3.

SafeCap practical results and findings

SafeCap practical results and findings
Scope of verification undertaken

Signalling Principles

Points deadlocking

Locking of points within a route

Opposing Route locking

Sequential route release

Overlap locking

…

Semi Formal *(plain text)*
'For each point commanded into a new state, no track sections over that point are occupied.'

Formal (first order logic)

```
forall p:Node
    point_c(p) != "point_c'p"(p)
    =>
    PointTracks[{p}] /\ track_o == {}
```

SafeCap practical results and findings
Summary of findings

Six interlocking data sets analysed

- All known errors found (including seeded errors)
- Intended violations of properties identified
- Significant risk areas identified in data

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

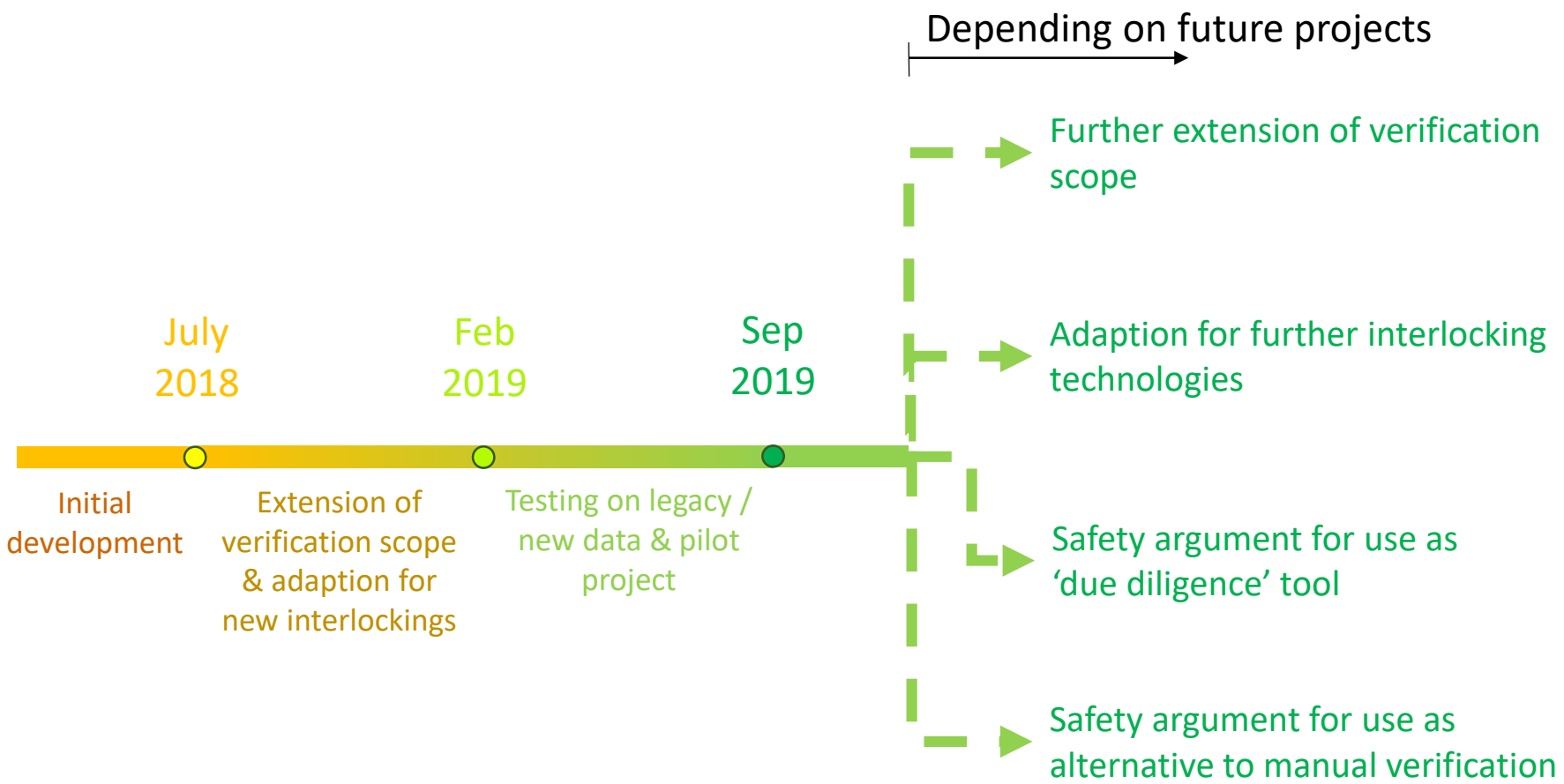
SafeCap practical results and findings
Lessons learnt for interlocking data

- **Simplicity**
- **Defensive programming**
- **Modularisation**

4.

Future developments

Future developments



5.

Summary

Summary

- Long term signalling trends drive rapidly increasing risk due to data errors
- Formal verification offers resilience to error by designers of signalling data
- SafeCap has shown a practical way of applying formal methods within existing processes
- It has also identified opportunities to further increase resilience to human error by changing how we write signalling data

Thank you for your attention.

Dominic Taylor CEng MBA	(dtaylor@systra.com)
Alexei Iliasov PhD	(alexei.iliasov@newcastle.ac.uk)
Alexander Romanovsky PhD	(alexander.romanovsky@newcastle.ac.uk)
Karl King MEng(Hons), MSc(Res) CEng	(k.king@fnc.co.uk)