Verification and Validation of a new type of Railway Signal using MBSE and Simulation

Don Stevenson – Network Rail
Ken Vine – Network Rail
James Towers – Scarecrow Consultants

INCOSE UK Annual Systems Engineering Conference 2018
Introduction

• Background
  – Problem Description
  – Proof of Concept (Prototype)

• Model-Based Systems Engineering
  – Approach
  – Requirements Views
  – System Structure & Behaviour Views
  – Simulation Views
  – Traceability Views
  – Specification View (Document)

• Conclusions
The Future
In Cab Signalling
Semaphore signalling
Semaphore signalling
Signalling Island with cabling

**Typical Signalling Island**

- **Distant Signal**
- **Home Signal**
- **Equipment Room**

**Cabling**

- To Signal
- To Axle Counter

- To Signal
- To Axle Counter
- To Axle Counter
- To Signal

INCOSE UK ASEC 2018 “The Year Of Engineering”
Signalling Island with cabling

Typical Signalling Island

Distant Signal
Home Signal
Equipment Room
Home Signal
Distant Signal

Cabling

To Signal
To Axle Counter
To Signal
To Axle Counter
To Signal
To Axle Counter
To Signal
….and with wireless Distant signals

Typical Signalling Island

Cabling

To Signal
To Signal
To Axle Counter
To Axle Counter
To Axle Counter
To Axle Counter
Signalling Island – with data ring and radial power cabling

**Typical Signalling Island**

- **Distant Signal**
- **Home Signal**
- **Equipment Room**

- **Data cable ring** up to 2000 m
- **Power cable radial** up to 500 m

- **Home Signal** up to 500 m
- **Distant Signal** up to 2000 m
Signalling Island – with data ring and radial power cabling

**Typical Signalling Island**

- **Distant Signal**
- **Home Signal**
- **Equipment Room**
- **Data cable ring**
- **Power cable radial**

**Cabling**

- Up to 2000 m
- Up to 500 m
- Up to 500 m
- Up to 2000 m
....and with wireless Distant signals
Operation

Typical Signalling Island
Operation

Typical Signalling Island

Distant Signal
Home Signal

Distant Signal
Home Signal

Equipment Room
Operation

Typical Signalling Island
Operation

Typical Signalling Island
Operation

Typical Signalling Island

Distant Signal  Home Signal  Distant Signal  Home Signal

Equipment Room
Operation

Typical Signalling Island

Distant Signal
Home Signal
Distant Signal
Home Signal
Operation

Typical Signalling Island
Operation

Typical Signalling Island

Distant Signal  Home Signal  Distant Signal  Home Signal

Equipment Room
Operation

Typical Signalling Island

Distant Signal  Home Signal  Distant Signal  Home Signal

Equipment Room
Operation

Typical Signalling Island
Proof of Concept
Proof of Concept
The System

- Methanol fuel cell
- Air Intake
- Water drain
- 60 MHz Radio
- SIL 3 rated PLC
- 24v Battery
- 2 x 28 litre canisters of Methanol
Model-Based Systems Engineering
Approach

- People
  - Small team of 4 People
    - 2 domain experts, 1 MBSE expert with some experience within the domain, plus a placement student
- Process
  - Series of workshops followed by construction / refinement of the model
- Tools
  - Architecture Framework previously defined for Network Rail Control, Command and Signalling projects (CCSAF)
    - Incorporates use of several standard Scarecrow Frameworks (FAF, ACRE, Enabling Patterns)
  - No Magic Cameo System Modeler
    - Full SysML 1.4 support
    - Activity Engine (fUML Engine)
      - The OMG fUML (a foundational subset of the Executable UML) standard
    - State-Machine Engine (SCXML Engine)
      - The W3C SCXML (State Charts XML) standard, which is an open-source Apache implementation
    - Parametric Engine
      - Enabling Cameo Simulation Toolkit to simulate SysML Parametric diagrams
Requirements Views – Operational Context

Operational Context

- System Context
  - Train Environment
  - Interlocking
  - Electromagnetic Interference
  - AWS Notification
  - Train Movement

System Control
- SWORD
  - Coloured Light Aspect

System Status
- Interlocking

Train
Requirements Views – Maintenance Context

The Maintainer will be required to visually inspect signal aspect during test.

The organisation responsible for refueling should have some mechanism for remotely monitoring the fuel level.

The Maintainer will need to provide (or simulate) train movement to test the Local Train Detection.

The Maintainer will need to measure magnetic flux of the AWS Ramp.

INCOSE UK ASEC 2018 “The Year Of Engineering”
Requirements Views – Operational Use Cases

- Display Yellow Aspect
- Display Green Aspect
- Extinguish Aspect once Stop Signal has been passed
- Suppress AWS Permanent Magnet (for reverse train movements)
- Initiate Self Test
## Requirements Views – Tables

<table>
<thead>
<tr>
<th>#</th>
<th>△ Name</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5.1.1 Display Aspect</td>
<td>While not in ‘AWS Suppression Mode’, when requested by the Interlocking by setting the ‘Light Aspect’ request the System shall display the required Aspect.</td>
</tr>
<tr>
<td>2</td>
<td>5.1.1.1 Delay Aspect Command Until Required</td>
<td>The Interlocking will request the System to display an appropriate Aspect once a Train, traveling in the in the normal direction has entered the section (MD / ABE) containing the Signal Head. It may be delayed, if necessary, until the time the Train (traveling at the maximum line speed) is 1000m away from the Signal Head.</td>
</tr>
<tr>
<td>3</td>
<td>5.1.1.2 Indicate Successful Aspect to Interlocking</td>
<td>On the detection and maintenance of a successfully displayed Aspect the System shall report this to the Interlocking by setting the appropriate output (Yellow Aspect Indication) or (Green Aspect Indication).</td>
</tr>
<tr>
<td>4</td>
<td>5.1.1.3 Display Yellow Aspect</td>
<td>The System shall display a Yellow Aspect when requested by the Interlocking unless it has previously extinguished an aspect due to the Train passing the Signal Head and it has not yet received a request to extinguish the Aspect from the Interlocking (Maintain Indication) Period.</td>
</tr>
<tr>
<td>5</td>
<td>5.1.1.3.1 Failure to display Yellow Aspect</td>
<td>If the System is unable to detect that it has successfully displayed a Yellow Aspect it will set the ‘Signal Faults To Light’ and ‘System Fault’ outputs to the Interlocking.</td>
</tr>
<tr>
<td>6</td>
<td>5.1.1.3.2 Display Yellow Aspect when Green Aspect Already Displayed</td>
<td>While currently displaying a Green Aspect, if commanded by the Interlocking to display a Yellow Aspect the System shall display a Yellow Aspect, unset the Yellow Aspect Indication and set the Green Aspect Indication.</td>
</tr>
<tr>
<td>7</td>
<td>5.1.1.3.3 Failure to maintain Yellow Aspect</td>
<td>If the System is unable to detect that it has successfully maintained display of a Yellow Aspect it will unset the ‘Yellow Aspect Indication’ and set the ‘System Fault’ outputs to the Interlocking.</td>
</tr>
<tr>
<td>8</td>
<td>5.1.1.4 Display Green Aspect</td>
<td>The System shall display a Green Aspect when requested by the Interlocking unless it has previously extinguished an aspect due to the Train passing the Signal Head and it has not yet received a request to extinguish the Aspect from the Interlocking (Maintain Indication) Period.</td>
</tr>
<tr>
<td>9</td>
<td>5.1.1.5 Extinguished Aspect once Train has passed</td>
<td>Once the System has detected that the Train has passed the Signal Head in the normal direction (via the Local Train Detection) then the System shall extinguish the Signal Head.</td>
</tr>
<tr>
<td>10</td>
<td>5.1.1.6 Extinguished Aspect when requested by Interlocking</td>
<td>When requested by the Interlocking the System shall extinguish the Signal Head (if not previously extinguished) and unset all ‘Aspect Indication’ outputs to the Interlocking.</td>
</tr>
<tr>
<td>11</td>
<td>5.1.1.7 Complete Wireless Communication Test before Displaying Aspect</td>
<td>If the System is performing either a Wireless Communication Test when the Interlocking requests the System to display an Aspect, the System shall complete the test before displaying the Aspect.</td>
</tr>
<tr>
<td>12</td>
<td>5.1.1.8 Interrupt Field Equipment Test to Display Aspect</td>
<td>If the System is performing a Field Equipment Test when the Interlocking requests the System to display an Aspect, the System shall immediately terminate the test and display the Aspect.</td>
</tr>
<tr>
<td>13</td>
<td>5.1.1.9 Attempt to Display Aspect even if Self-Test has failed</td>
<td>When requested by the Interlocking to display an Aspect the System shall attempt to display that Aspect even if the previous Self-Test had failed (as shown by the ‘Self Test Failed’ indication being set).</td>
</tr>
</tbody>
</table>
System Structure & Behaviour Views

package System Architecture { System Structure View with Properties }

```
<package>
  <system>
    VHFChannel
    FieldEnd
    OfficeEnd
  </system>
  ToOffice
  ToField
</package>
```

Conceptual Channel allows us to simulate 'lost' messages

INCOSE UK ASEC 2018 “The Year Of Engineering”
• Field End
  – Signal Head
  – Signal Post
  – Local Train Detection
  – Field Controller
  – Off-Grid Power Supply
  – Wireless Communication Module
  – AWS Coil Driver x 2
  – Radio Antenna
  – Equipment Housing
Structure View - Signal Head

```xml
<Component>
  SignalHead
  
  values:
  yellowFault : Boolean = false
  greenFault : Boolean = false
  standbyPower : power[ Watt ] = 0.0 [ unit = Watt ]
  yellowOnPower : power[ Watt ] = 1.0 [ unit = Watt ]
  greenOnPower : power[ Watt ] = 1.0 [ unit = Watt ]
  output : SignalHeadOutput
  supplyPower : ElectricPower [ Watt ] = 0.0 [ unit = Watt ]
  supplyVoltage : voltage[ Volt ] = 50.0 [ unit = Volt ]
  supplyCurrent : electricCurrent[ Ampere ] = 0.0 [ unit = Amp ]
  
  out ports:
  output fieldController: SignalHeadControl-IF
  output powerSupply: ElectricPower-IF

  <interface Blocks>
    SignalHeadControl-IF
    
    in command : SH-Command
    out status : SH-Status

  <valueType>
    SignalHeadOutput
    
    value:
    yellow
    green
    black

  <valueType>
    AspectValueType
    
    value:
    black
    yellow
    fault
    green
```
### Behaviour View – Signal Head

#### State Machine

- **Start**
  - When **greenFault**
  - When **!greenFault**
  - When **yellowFault**
  - When **!yellowFault**

#### Transition Diagram

**Signal Head**

- **Black**
  - Entry / DisplayBlack
- **Green**
  - Entry / DisplayGreenAndReportSuccess
- **Yellow**
  - Entry / DisplayYellowAndReportSuccess
- **Green Commanded**
  - [greenFault]
  - [!greenFault]
- **Yellow Commanded**
  - [yellowFault]
  - [!yellowFault]
- **Yellow Displayed**
  - Entry / DisplayYellowAndReportSuccess
  - When **yellowFault**
  - When **!yellowFault**
  - SH-YellowCommand
- **Green Displayed**
  - Entry / DisplayGreenAndReportSuccess
  - When **!greenFault**
  - When **greenFault**
  - SH-GreenCommand
  - SH-BlackCommand
  - SH-YellowCommand
  - SH-GreenCommand
  - SH-BlackCommand

**Error Handling**

- **Report Green Fault**
  - Entry / GreenFault
- **Report Yellow Fault**
  - Entry / YellowFault
- **Report Success**
  - Entry / ReportSuccess
Behaviour View – Power-up Field Controller
Parametric View – AWS Coil
Simulation Views – AWS ‘Ramp’ Equipment

State machine defining component behaviour

Diagram is animated with changing colours during execution

Test harness UI

AWS Equipment UI
Full System Simulation
Traceability – Requirements Diagram

"The Year Of Engineering"

**Field End**
- **Id**: "4.6.2.2"
- **Text**: "The Field End shall be comprised of a number of Components."

**Field Controller**
- **Id**: "4.6.2.1"
- **Text**: "The Field End shall include a Field Controller. This will control the Field End Components."

**FieldController**
- **values**
  - `supplyPower`: electric power [Watt] (unit = Watt)
  - `rst`: Boolean = false
  - `standbyPower`: electric power [Watt] = 0.1 W (unit = Watt)
  - `bootingPower`: electric power [Watt] = 10.0 W (unit = Watt)
  - `operatingPower`: electric power [Watt] = 8.0 W (unit = Watt)
  - `status`: PowerStatus Type = Off
  - `supplyVoltage`: voltage [Volt] = 0.0 V (unit = Volt)
  - `minSupplyVoltage`: voltage [Volt] = 11.0 V (unit = Volt)
  - `bootTime`: time [second] = 10.0 s (unit = second)
  - `greenTimeout`: time [second] = 3.0 s (unit = second)
  - `trainDetected/Normal`: Boolean = false
  - `maxSignalDarkTime`: time [second] = 120.0 s (unit = second)
  - `maxAWSSuppressionTime`: time [second] = 15.0 s (unit = second)
  - `maxReadyToPowerDownTime`: time [second] = 9.0 s (unit = second)
  - `feedback`: Boolean = false
  - `stmMessagesReceived`: Integer = 0
  - `stmTarget`: Integer = 9
  - `returnToldie`: Boolean = false
  - `stmMessagesSent`: Integer = 0

**proxy ports**
- `out AWSElectric`: -AWSControl-IF
- `out AWSSupression`: -AWSControl-IF
- `inout oc`: RemoteController-IF
- `inout powerIn`: ElectricalPower-IF
- `inout signalHead`: -SignalHeadControl-IF
- `inout localTrainDetection`: -LTD-IF
### Traceability - Matrix

<table>
<thead>
<tr>
<th>Legend</th>
<th>4.6.2 Field End</th>
</tr>
</thead>
<tbody>
<tr>
<td>Satisfy</td>
<td>4.6.2.1 Field Controller</td>
</tr>
<tr>
<td></td>
<td>4.6.2.2.1 Signal Head Standard</td>
</tr>
<tr>
<td></td>
<td>4.6.2.3.1 AWS Ramp Standards</td>
</tr>
<tr>
<td></td>
<td>4.6.2.4 AWS Coil Drivers</td>
</tr>
<tr>
<td></td>
<td>4.6.2.6 Wireless Communication Module</td>
</tr>
<tr>
<td></td>
<td>4.6.2.7 Off Grid Power Supply Voltage</td>
</tr>
<tr>
<td></td>
<td>4.6.2.8 Radio Antenna</td>
</tr>
<tr>
<td></td>
<td>4.6.2.9 Equipment Housing</td>
</tr>
<tr>
<td></td>
<td>4.6.2.12.1 Radio Antenna Mounting</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AWS Equipment</th>
<th>1</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS Coil Driver</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>AWS Coil Driver</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>AWS Equipment</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Field Controller</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Local Train Detection</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Local Train Detection</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Mechanical Component</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Equipment Housing</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Radio Antenna</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Signal Post</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Off Grid Power Supply</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Off Grid Power Supply</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Signal Head</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Signal Head</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
Conclusions
Conclusions

- The use of SysML allowed us to describe the system in both natural language requirements and as an executable model with precise semantics.
  - Able to output a ‘readable’ document to supplement the model.
- End to end traceability allows us to perform verification in the model.
- Simulation allows us to perform validation with the model.
- People: Access to the appropriate skills is vital.
- Process: Successful realisation is only possible with an appropriate process.
- Tools: Access to the appropriate tools is vital.
  - Network Rail already had access to a suitable MBSE tool and Architecture Framework.