Functional Safety Assessment of Train Order Working

Kevin Anderson
Kevin J Anderson & Associates Pty Ltd
Melbourne Australia
Railways of Australia: Multitude of safeworking and communications systems - single line territory - long distance, low density, locomotives
Traditional staff and ticket safeworking with copper wire signal telephones necessitated constant stopping. Communications replaced by Train Radio System (TRS) including trackKm to nearest 0.5 km from Global Positioning System (GPS). Tender of Train Order Working (TOW) 1994. Risk assessment: 'not less safe' requires computer support to Train Controller (TC)
Trial implementation: Orange - Parkes and Orange - Dubbo 1998

Train Controller (TC) formulates authority (Train Order for train, Track Warrant for trackforce), details are read out and written down including security code. Handed back verbally on fulfillment and train clear of territory or protected by another authority.
Legacy System
Alternative Safeworking System

ASW was implemented in Victoria in 1993 and provided for transmission of train orders one section at a time to in-cab screens displaying 'Current' and 'Next' Orders. The following screen shows a functional safety audit time-distance graph. In the centre, train 9823 is going down and train 9712 is travelling up and waits in the loop for 9823 to cross.
Crossing loops are provided at regular locations along the main line. Train Drivers (TD) are required to report at penultimate location and are given reminders where other trains are to be crossed.
An audit tool was developed to read radio and system logs and reconstruct the 'life cycle' of an authority from the 27 types of messages.

Typically, an authority goes through five steps to establish (proposed, validated, sent to train screen, acknowledged by train driver, acknowledged by system) and three steps to clear (relinquished by TD, returned and released).
Evidence

The audit tool creates a graphical representation of each authority bounded in space and time. The history of each authority state is stored in the script or tag of each graphic.

As a matter of 'proof by result' the relevant original log files are also stored in the tag.

The audit tool allowed measurement of controller workload and human error rates as well as providing a basis for enhanced integrity testing of the safeworking interlocking rules.
Train Management Control System (TMCS)

Due to legacy system problems revealed by the FSA audit, TMCS was declared to be NOT safety-related. The promised use of dual programming had not been installed and inspection of the source code revealed more problems than answers. Rather, it was decided to restore confidence in integrity of the interlocking through a safety-related GPS Watchdog.
GPS Watchdog

• Stage 1 as installed June 1999:
  – Proof of TMCS and GPSW intercommunications
  – TRS polling ability
  – Plotting of both systems on Map and Graph

• Stage 2
  – Proximity detection and alarm capabilities

• Stage 3
  – Diverse implementation of safeworking rules
Risk Assessment

1. Train Location sub-system (Train Driver and Train Controller and GPS Watchdog)
   - 4.4 chances per million per year.

2. Train Control sub-system (TC and TMCS and GPS Watchdog computer support)
   - 5.5 chances per million per year.

3. Communications sub-system (TD and TC and TRS).
   - 11.0 chances per million per year.

4. Train Driver sub-system (TD only)
   - 5.5 chances per million per year.
<table>
<thead>
<tr>
<th></th>
<th>Train Location Error</th>
<th>Train Control Error</th>
<th>Communications Error</th>
<th>Train Driver Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>Credible Threat:</td>
<td>Misreport 1.00E-03</td>
<td>Rules Error 5.00E-04</td>
<td>Comms Failure 1.00E-04</td>
<td>Exceed Authority 1.00E-05</td>
</tr>
<tr>
<td>Moderated by</td>
<td>Track Km 4.00E-04</td>
<td>Computer Interlock 1.00E-03</td>
<td>Fallback 1.00E-02</td>
<td>Overlap Recovery 5.00E-02</td>
</tr>
<tr>
<td>Loss of Control</td>
<td>4.00E-07</td>
<td>5.00E-07</td>
<td>1.00E-06</td>
<td>5.00E-07</td>
</tr>
<tr>
<td>per exposure</td>
<td>110</td>
<td>110</td>
<td>110</td>
<td>110</td>
</tr>
<tr>
<td>times crossing trials per annum</td>
<td>110</td>
<td>110</td>
<td>110</td>
<td>110</td>
</tr>
<tr>
<td>of collision not avoided locally</td>
<td>20%</td>
<td>20%</td>
<td>20%</td>
<td>20%</td>
</tr>
<tr>
<td>and fatality per collision</td>
<td>50%</td>
<td>50%</td>
<td>50%</td>
<td>50%</td>
</tr>
<tr>
<td>Individual risk contributor chances per million years</td>
<td>4.4</td>
<td>5.5</td>
<td>11.0</td>
<td>5.5</td>
</tr>
<tr>
<td>Total risk assessment:</td>
<td>26.4 chances of fatality per million years</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Human Error Probability

1 in 1000 (1E-3) is established in various studies dating back to Three Mile Island Inquiry, 1975 as a demand rate that complex systems should be designed to defend against. (e.g. security code errors 6 in 20,000 is 3 E-4).

TC claim 5E-4 implies a second chance - propose then validate.

TD claim 1E-5 assumes strong second chance equiv SPAD caution AND stop
Failure Rate Assumptions

Track km check 1E-3 without GPS, 4E-4 with GPS.

Computer interlock 1E-3 limit claim SIL2.
Enhanced test matrix 89x74=n=7921 test cases.
At 99% confidence 4.5/n = 5.84E-4.

Overlap recovery (300m) less certain, say 5E-2.
Safety Argument

• Exposure and balance of probability figures were used to translate relative risks to purported absolute figures, but the primary safety argument rests on the relative risks and the safety principles of 'not less safe', 'as low as reasonably practicable '(ALARP) and 'continuous improvement'.

• GPSW provides monitoring, alarms and enhanced safeworking rules. However, in-cab communications and enforcement remain for the future.
FSA Audit

An audit was conducted by the FSA after three years of operations. The audit comprised a document review and generative interviews at Orange Train Control Centre and with system maintainers. A system snapshot was taken and safeworking encodings were reviewed. Train Controller workload issues were raised, in particular the time consuming nature of voice transmissions.
Example of Rule Enforcement

As train 8888 is standing on main, 8885 cannot be issued order to loop until existing order to Yard Limit Board is fulfilled.
PKS-BKH plot
Location Types

In the GPS Watchdog, safeworking encoding tables have been prepared for nine types of location:

• STD  Standard Crossing Loop
• SSB  Standard Crossing Loop with Shunt Limit Boards
• BSB  Block Location with Shunt Limit Boards (aka Siding)
• BLK  Block
• PKW  Parkes Sub siding no Up YLB
• ADJ  Crossing Loop with Junction
• SIG  Signalled Location
• SS   Single Line Section
• MLS  Mishap Line Section
Authority Cases

The encoding and exception tables cover numerous cases (refer overleaf for one example from matrix):

• Down Train Order (20 cases)
• Up Train Order (20 cases)
• Shunt Order (4 cases)
• Track Occupancy Down and Up (8 cases each)
• Mishap Down and Up (9 cases each)
• UNIMO (2), BIMO (2), BIMOL (2) B (1) L (2)
Train Order from Stuart Town to Wellington Yard Limit Board

STUART TOWN

COMBO

sw001
Example of excessive polling
due to portable logon issue
Next Steps

In-cab communication and location advice (the TC knows location of other trains, TD does not)

• Data transmission for efficiency as well as safety
• Future of Enforcement
• Tolerate risk vs timeline (continue to improve)
• Generic commercial-off-the-shelf (COTS) solution (applicable to track circuits (TX) not just Train Order Working (TOW))