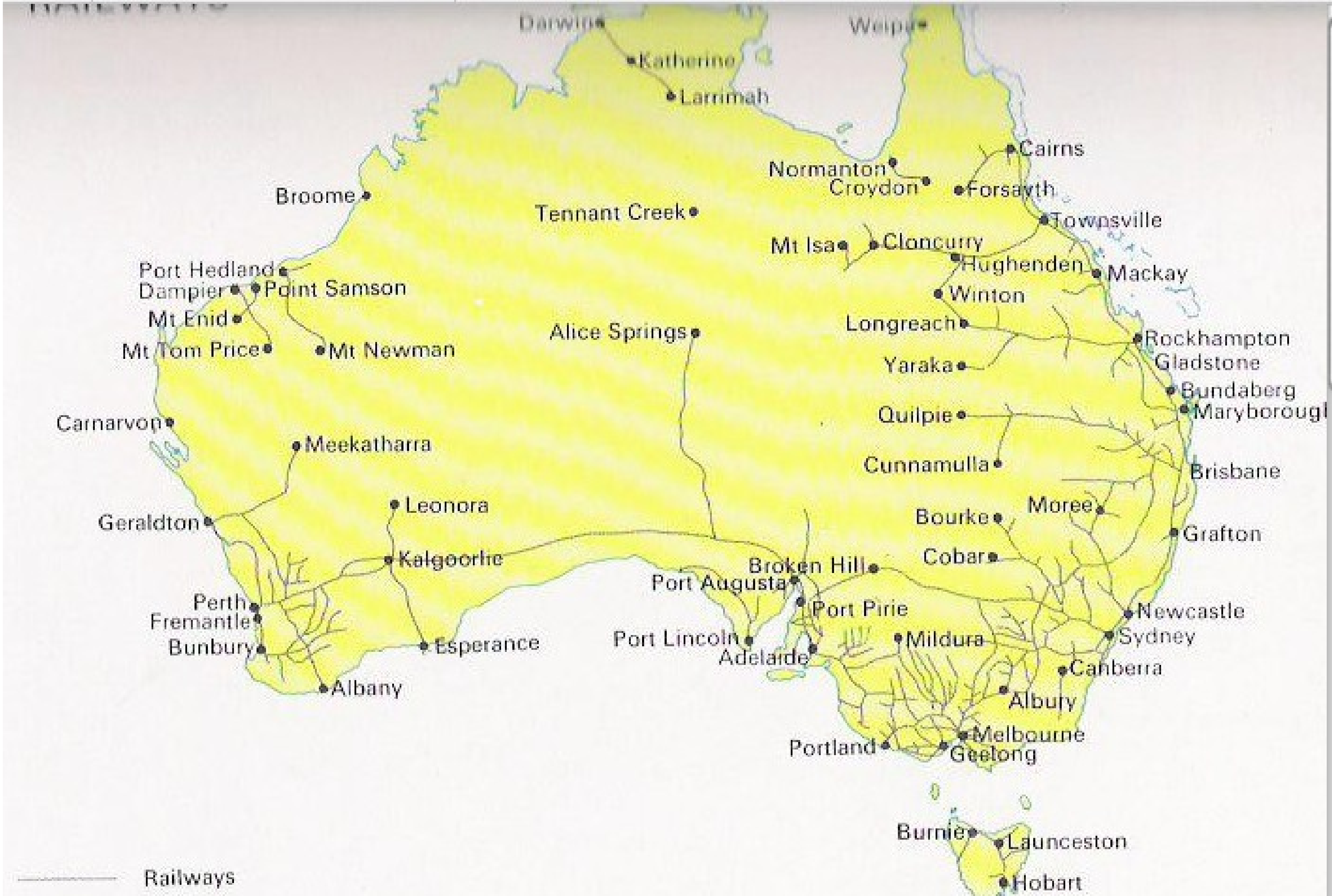
# Functional Safety Assessment of Train Order Working

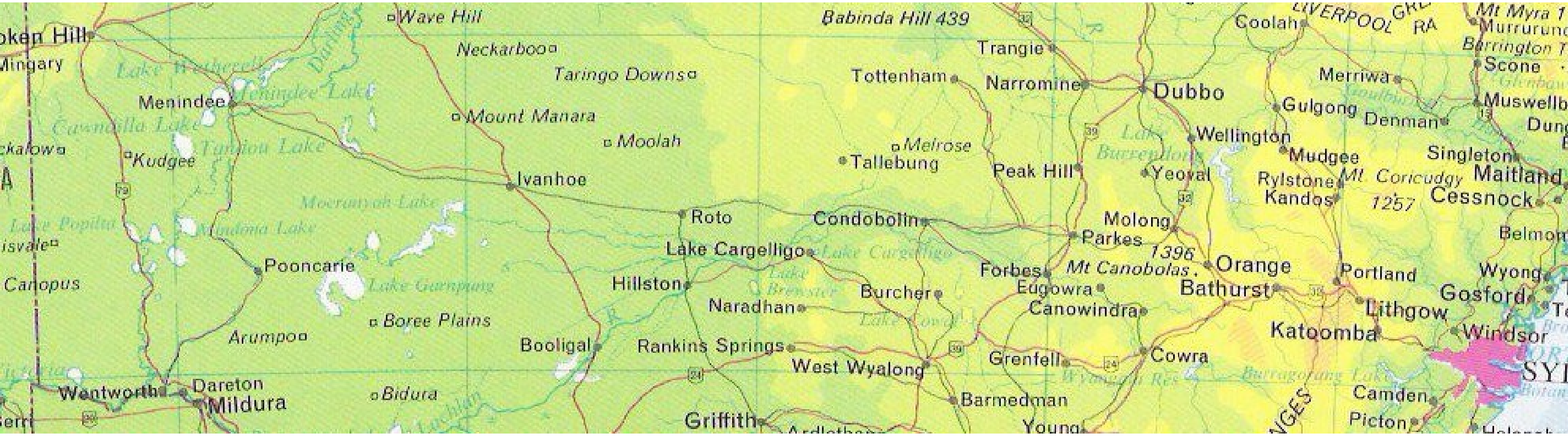
Kevin Anderson

Kevin J Anderson & Associates Pty Ltd

Melbourne Australia

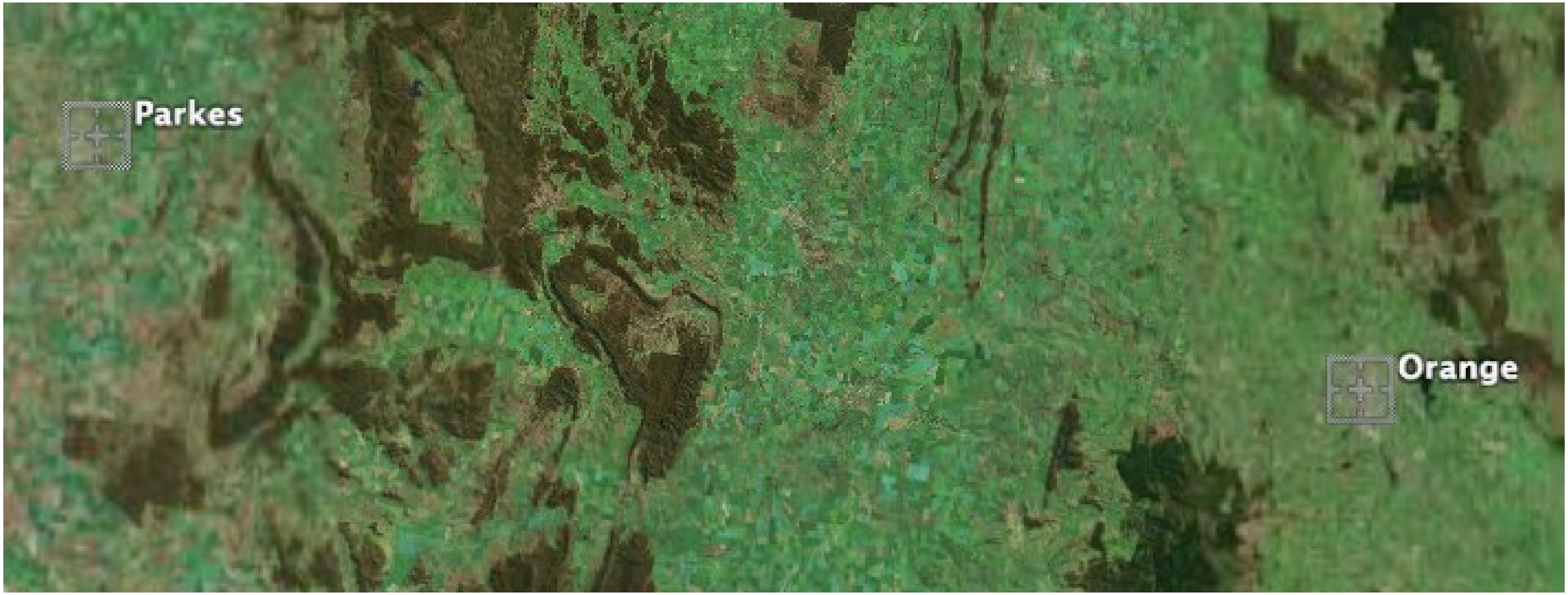


Railways of Australia: Multitude of safeworking and communications systems - single line territory - long distance, low density, locomotives



Broken Hill Ivanhoe Parkes Orange

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)



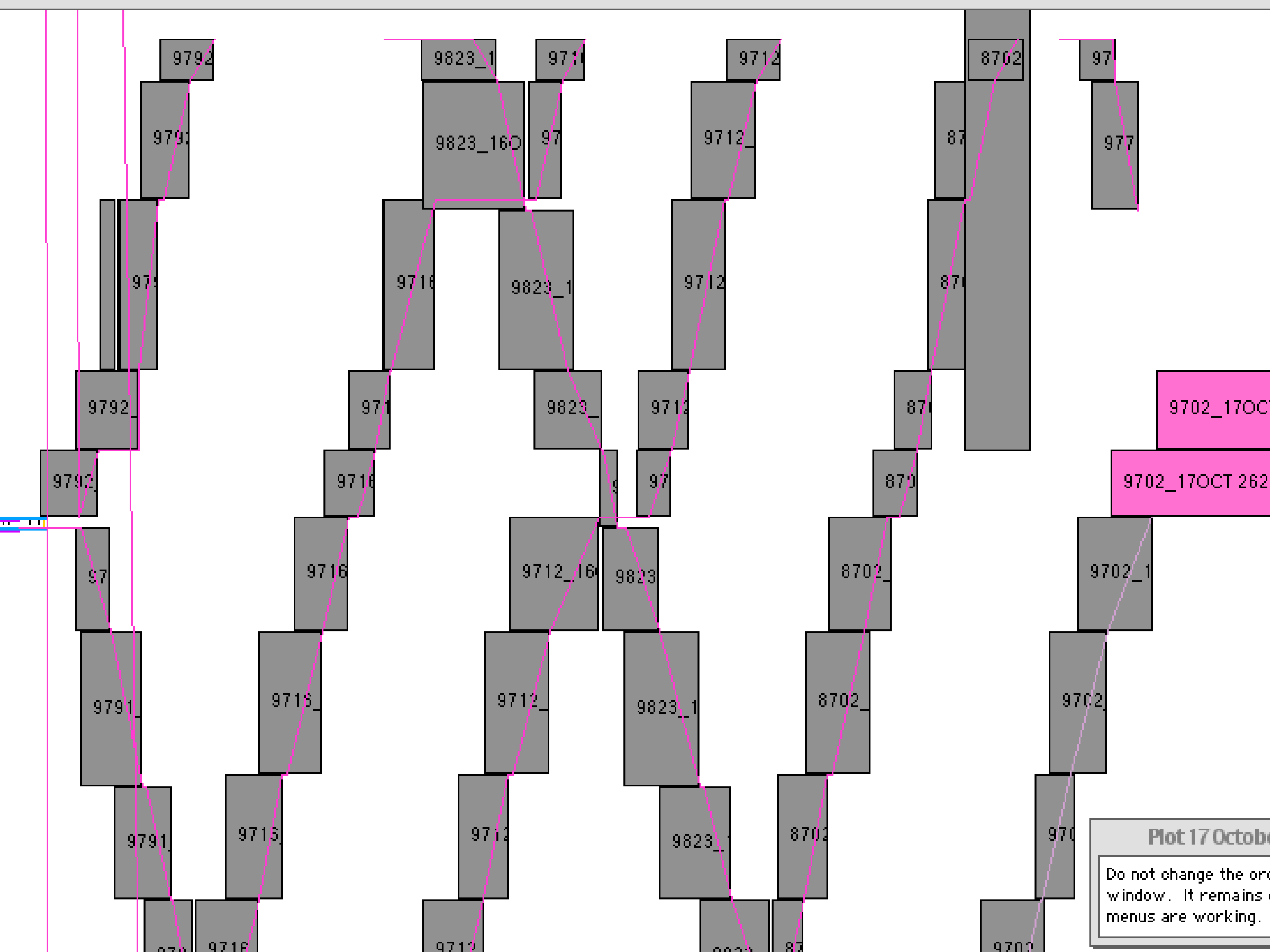
Trial implementation: Orange - Parkes and Orange - Dubbo 1998

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.



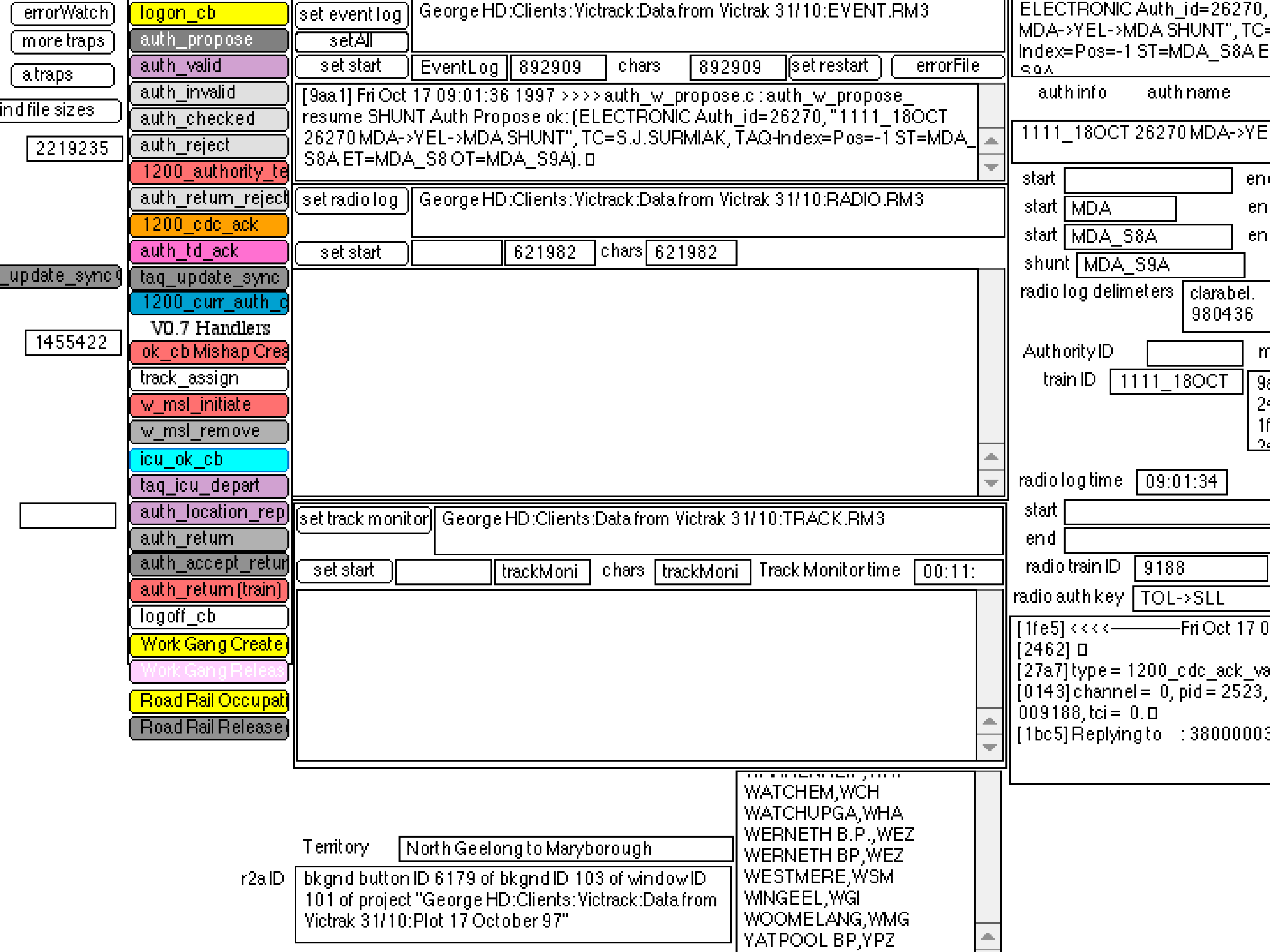
Plot 17 Octobe

Do not change the or
window. It remains
menus are working.

# Functional Safety Assessment Audit Tool

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).



2219235

1455422

George HD:Clients:Victrack:Data from Victrak 31/10:EVENT.RM3

EventLog 892909 chars 892909

```
[9aa1] Fri Oct 17 09:01:36 1997 >>>> auth_w_propose.c : auth_w_propose_
resume SHUNT Auth Propose ok: (ELECTRONIC Auth_id=26270, "1111_18OCT
26270 MDA->YEL->MDA SHUNT", TC=S.J.SURMIAK, TAQ-Index=Pos=-1 ST=MDA_
S8A ET=MDA_S8 OT=MDA_S9A). □
```

George HD:Clients:Victrack:Data from Victrak 31/10:RADIO.RM3

621982 chars 621982

George HD:Clients:Data from Victrak 31/10:TRACK.RM3

trackMoni chars trackMoni Track Monitor time 00:11:

```
ELECTRONIC Auth_id=26270,
MDA->YEL->MDA SHUNT", TC=
Index=Pos=-1 ST=MDA_S8A E
S9A
```

1111_18OCT 26270 MDA->YE

start MDA

start MDA_S8A

shunt MDA_S9A

radio log delimeters clarabel.
980436

train ID 1111_18OCT

9a
2
1f
2

radio log time 09:01:34

radio train ID 9188

radio auth key TOL->SLL

```
[1fe5] <<<<———————Fri Oct 17 0
[2462] □
[27a7] type = 1200_cdc_ack_va
[0143] channel = 0, pid = 2523,
009188, tci = 0. □
[1bc5] Replying to    : 38000003
```

Territory North Geelong to Maryborough

r2a ID bkgnd button ID 6179 of bkgnd ID 103 of window ID 101 of project "George HD:Clients:Victrack:Data from Victrak 31/10:Plot 17 October 97"

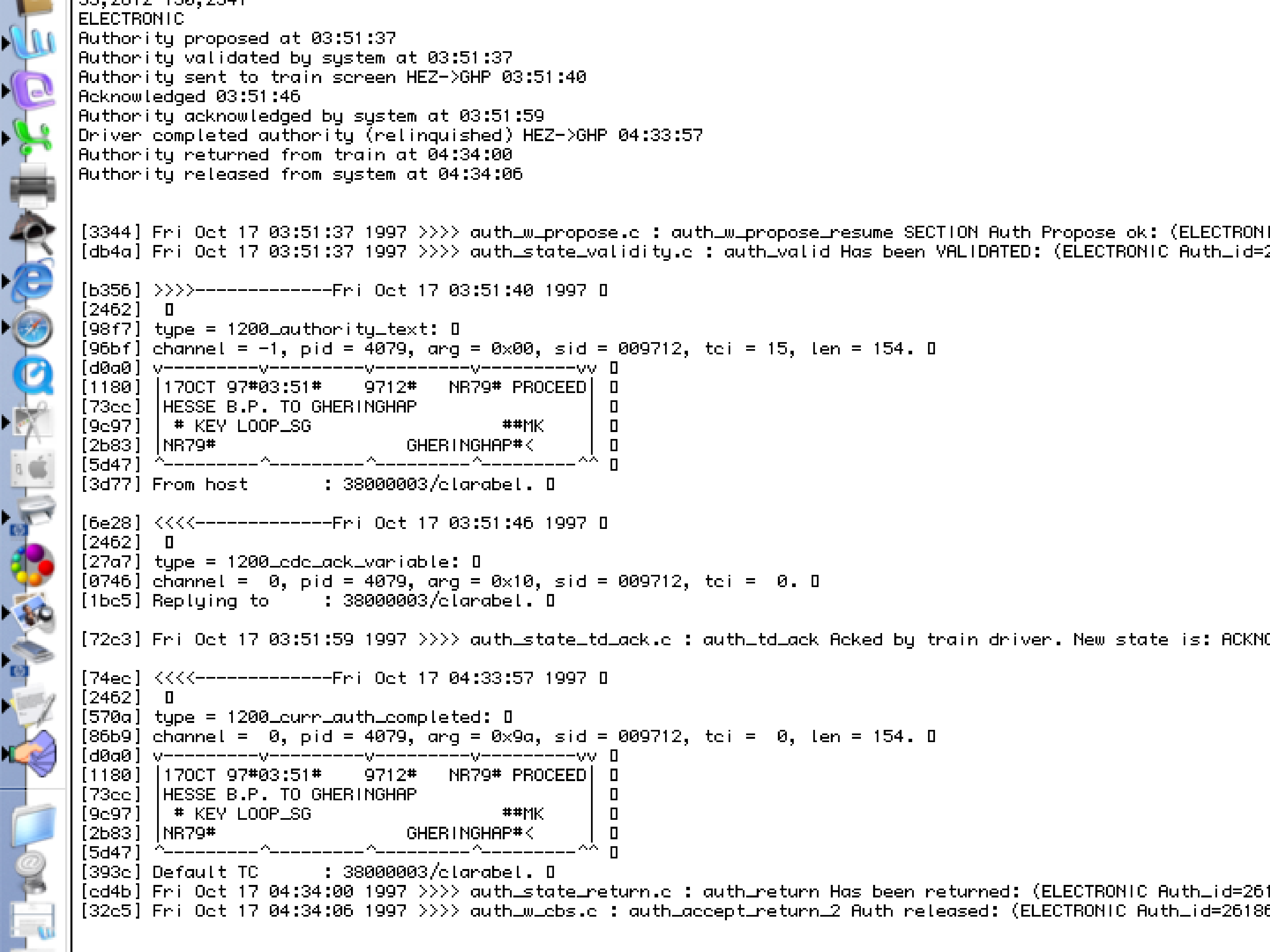
WATCHEM,WCH
WATCHUPGA,WHA
WERNETH B.P.,WEZ
WERNETH BP,WEZ
WESTMERE,WSM
WINGEEL,WGI
WOOMELANG,WMG
YATPOOL BP,YPZ

# 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.



```
55,2012 156,2541
ELECTRONIC
Authority proposed at 03:51:37
Authority validated by system at 03:51:37
Authority sent to train screen HEZ->GHP 03:51:40
Acknowledged 03:51:46
Authority acknowledged by system at 03:51:59
Driver completed authority (relinquished) HEZ->GHP 04:33:57
Authority returned from train at 04:34:00
Authority released from system at 04:34:06


[3344] Fri Oct 17 03:51:37 1997 >>>> auth_w_propose.c : auth_w_propose_resume SECTION Auth Propose ok: (ELECTRONI
[db4a] Fri Oct 17 03:51:37 1997 >>>> auth_state_validity.c : auth_valid Has been VALIDATED: (ELECTRONIC Auth_id=2

[b356] >>>>------------Fri Oct 17 03:51:40 1997 □
[2462]  □
[98f7] type = 1200_authority_text: □
[96bf] channel = -1, pid = 4079, arg = 0x00, sid = 009712, tci = 15, len = 154. □
[d0a0] v---------v---------v---------v---------vv □
[1180] |17OCT 97#03:51#    9712#   NR79# PROCEED|  □
[73cc] |HESSE B.P. TO GHERINGHAP               |  □
[9c97] | # KEY LOOP_SG                  ##MK   |  □
[2b83] |NR79#                  GHERINGHAP#<    |  □
[5d47] ^---------^---------^---------^---------^^ □
[3d77] From host        : 38000003/clarabel. □

[6e28] <<<<------------Fri Oct 17 03:51:46 1997 □
[2462]  □
[27a7] type = 1200_cdc_ack_variable: □
[0746] channel =  0, pid = 4079, arg = 0x10, sid = 009712, tci =  0. □
[1bc5] Replying to      : 38000003/clarabel. □

[72c3] Fri Oct 17 03:51:59 1997 >>>> auth_state_td_ack.c : auth_td_ack Acked by train driver. New state is: ACKNO

[74ec] <<<<------------Fri Oct 17 04:33:57 1997 □
[2462]  □
[570a] type = 1200_curr_auth_completed: □
[86b9] channel =  0, pid = 4079, arg = 0x9a, sid = 009712, tci =  0, len = 154. □
[d0a0] v---------v---------v---------v---------vv □
[1180] |17OCT 97#03:51#    9712#   NR79# PROCEED|  □
[73cc] |HESSE B.P. TO GHERINGHAP               |  □
[9c97] | # KEY LOOP_SG                  ##MK   |  □
[2b83] |NR79#                  GHERINGHAP#<    |  □
[5d47] ^---------^---------^---------^---------^^ □
[393c] Default TC       : 38000003/clarabel. □
[cd4b] Fri Oct 17 04:34:00 1997 >>>> auth_state_return.c : auth_return Has been returned: (ELECTRONIC Auth_id=261
[32c5] Fri Oct 17 04:34:06 1997 >>>> auth_w_cbs.c : auth_accept_return_2 Auth released: (ELECTRONIC Auth_id=2618
```

# 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).

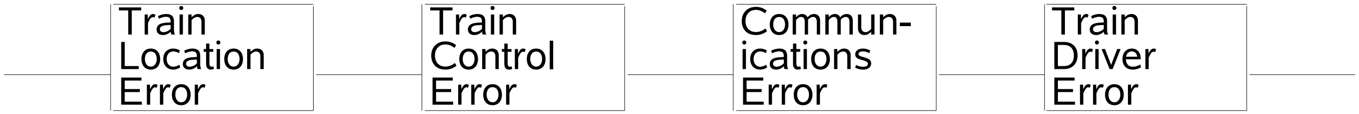
   - 11.0 chances per million per year.

4. Train Driver sub-system (TD only)

   - 5.5 chances per million per year.

# Reliability Block Diagram

Train Operations sub-system lifecycle


Train Location Error

Train Control Error

Communications Error

Train Driver Error

| | | | | |
|---|---|---|---|---|
| Credible Threat: | Misreport | Rules Error | Comms Failure | Exceed Authority |
| | 1.00E-03 | 5.00E-04 | 1.00E-04 | 1.00E-05 |
| Moderated by Sensible Precaution: | Track Km | Computer Interlock | Local Fallback | Overlap Recovery |
| | 4.00E-04 | 1.00E-03 | 1.00E-02 | 5.00E-02 |
| Loss of Control per exposure | 4.00E-07 | 5.00E-07 | 1.00E-06 | 5.00E-07 |
| times crossing trials per annum | 110 | 110 | 110 | 110 |
| times balance of probability of collision not avoided locally | 20% | 20% | 20% | 20% |
| and fatality per collision | 50% | 50% | 50% | 50% |
| Individual risk contributor chances per million years | **4.4** | **5.5** | **11.0** | **5.5** |

Total risk assessment: **26.4 chances of fatality per million years**

# Human Error Probability

1in 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.

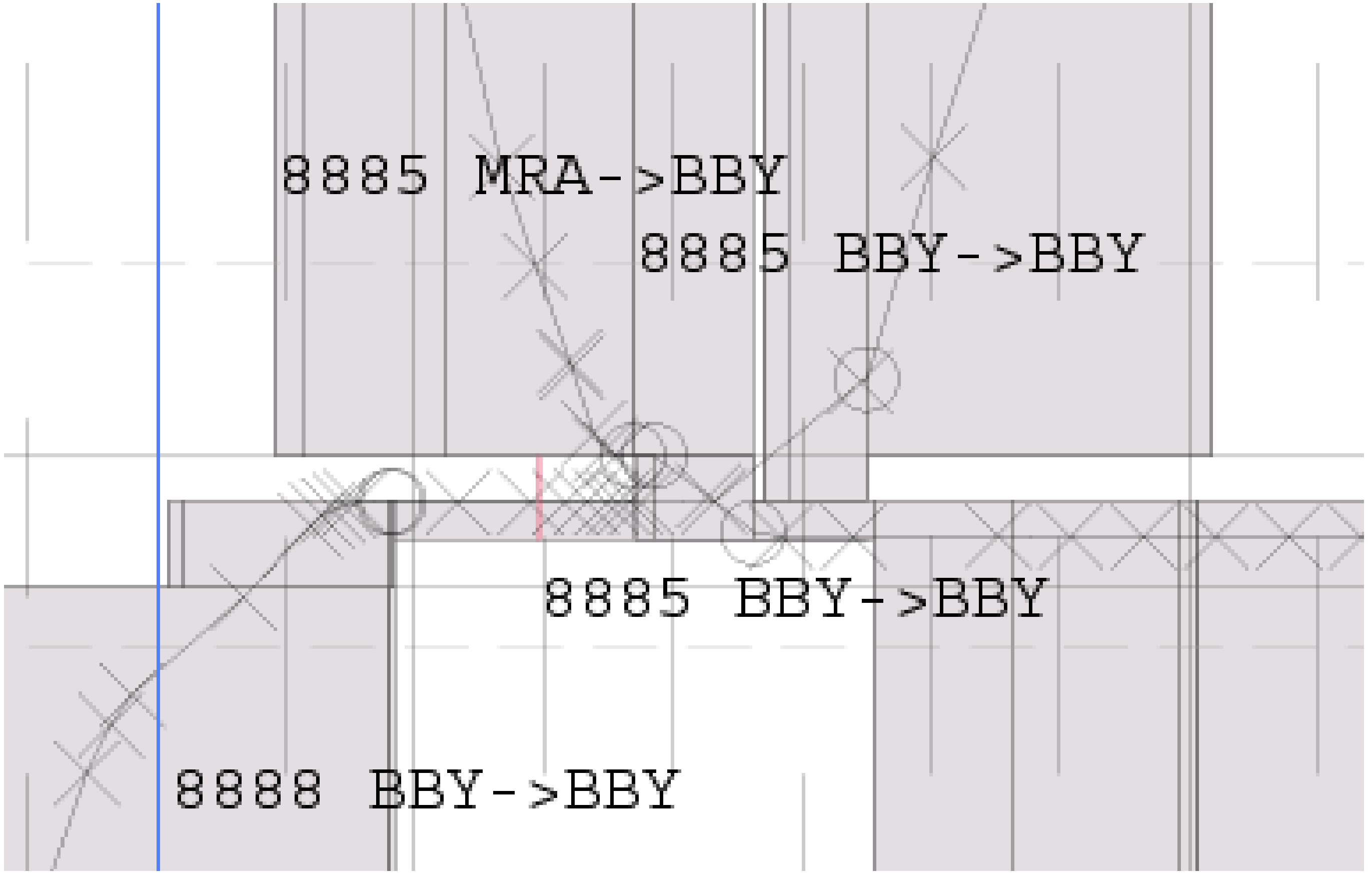
# FSA Audit

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 snap shot was taken and safeworking encodings were reviewed.

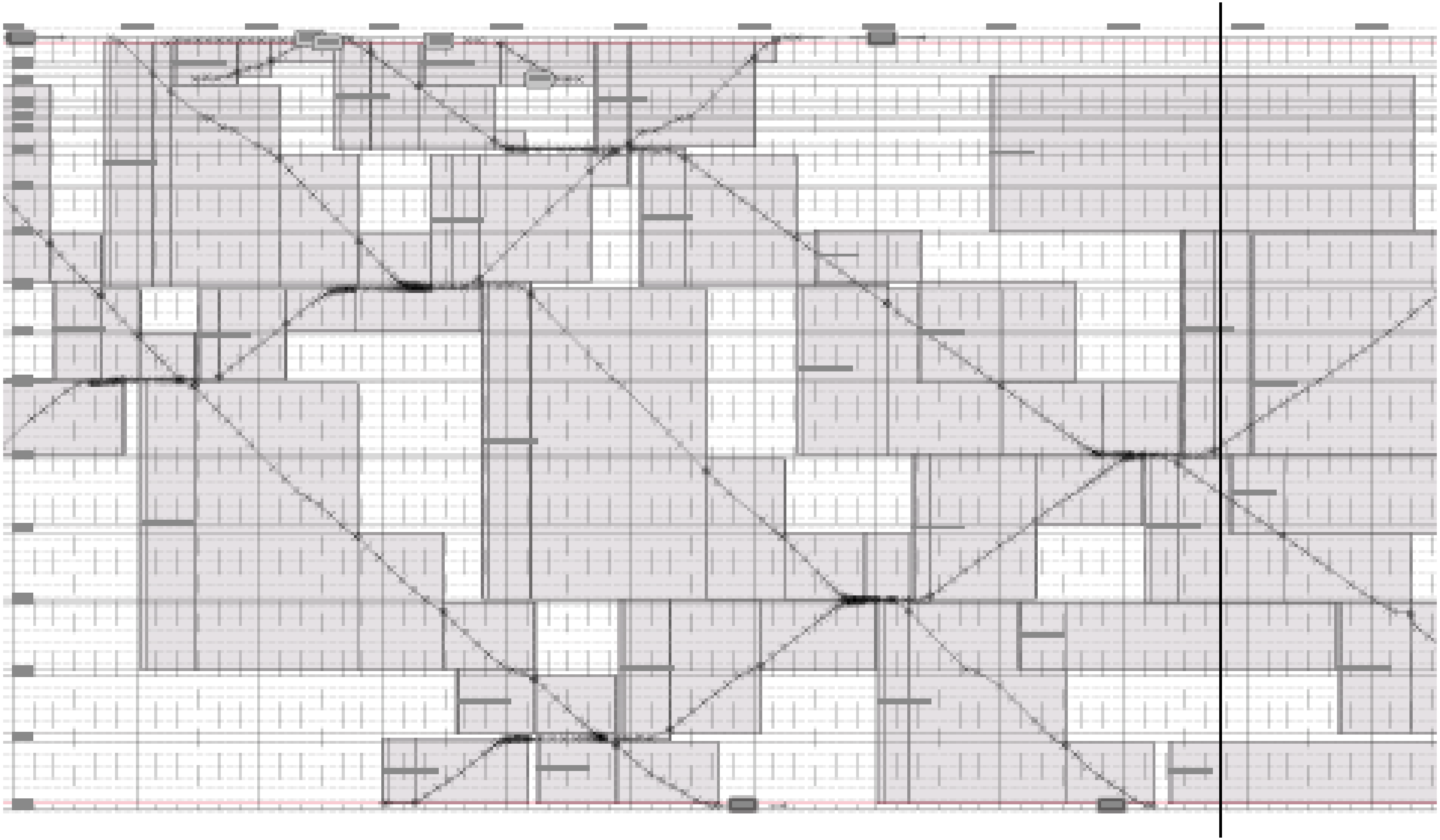
Train Controller workload issues were raised, in particular the time consuming nature of voice transmissions.

# 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:

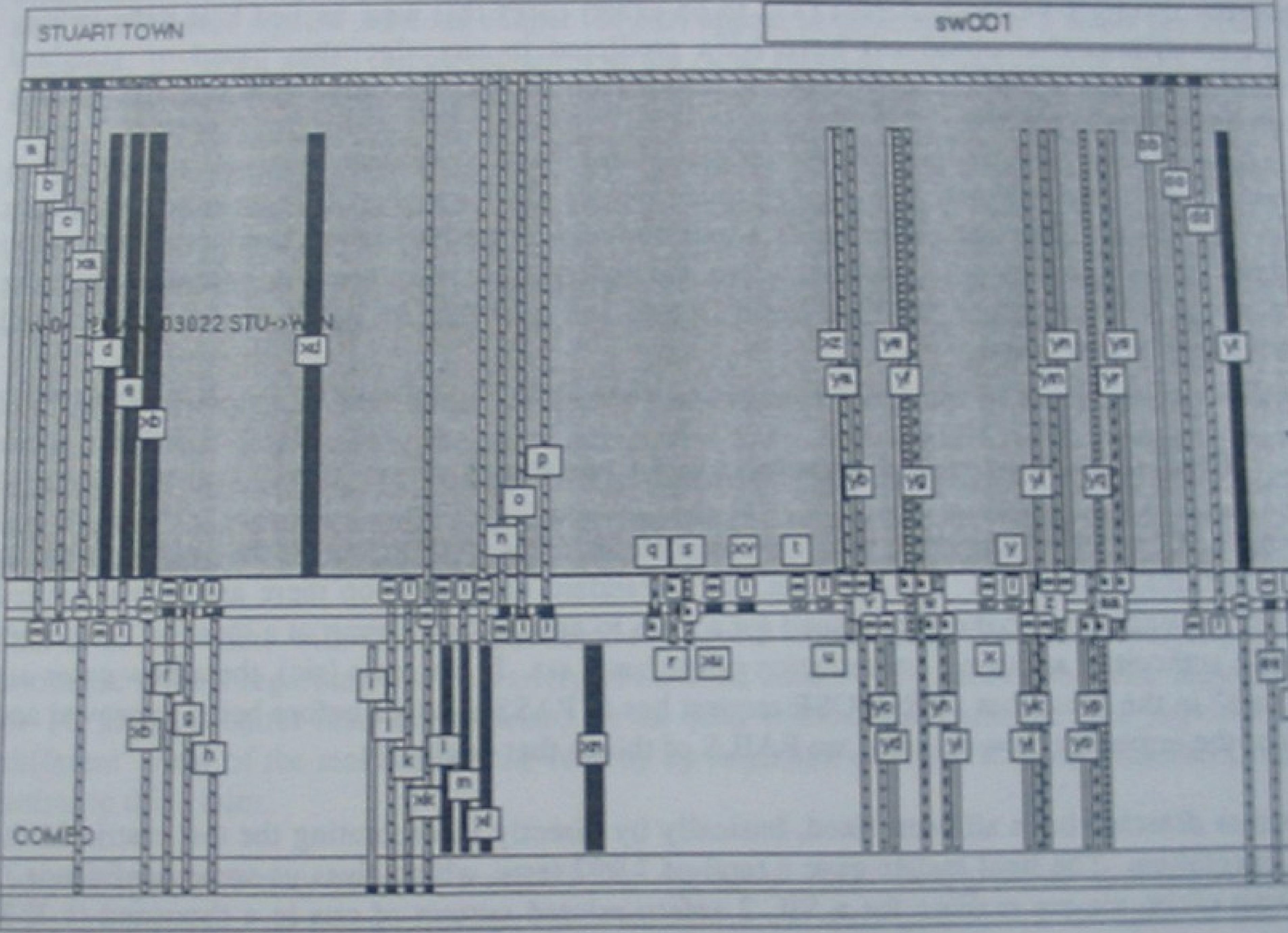
- STD Standard Crossing Loop
- SSB Standard Crossing Loop with Shunt Limit Boards
- BSB Block Location with Shunt Limit Boards (aka Siding)
- BLK Block
- PKW Parkes Sub siding no Up YLB
- ADJ Crossing Loop with Junction
- SIG Signalled Location
- SS Single Line Section
- MLS Mishap Line Section

# Authority Cases

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

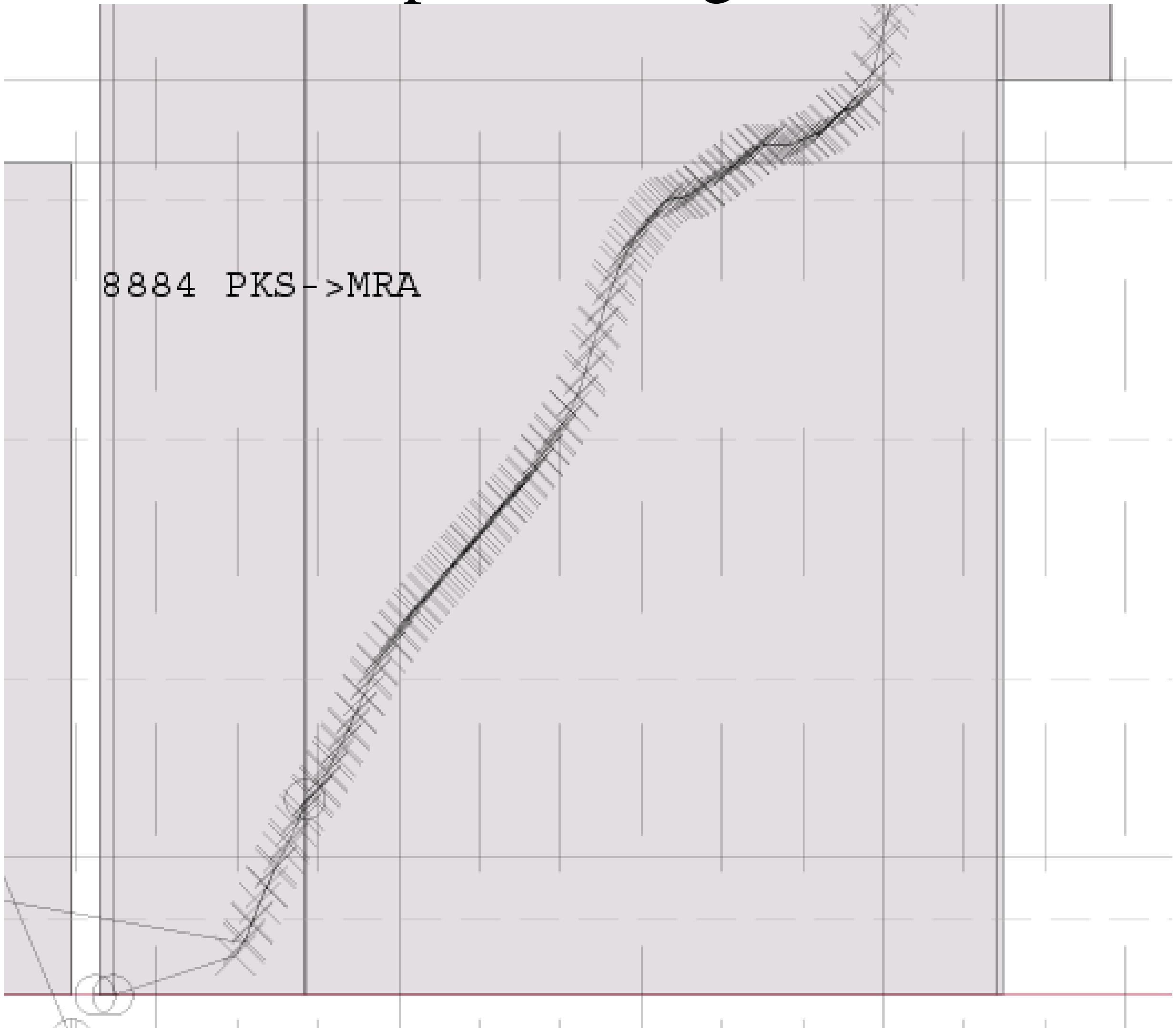
- Down Train Order (20 cases)
- Up Train Order (20 cases)
- Shunt Order (4 cases)
- Track Occupancy Down and Up (8 cases each)
- Mishap Down and Up (9 cases each)
- UNIMO (2), BIMO (2), BIMOL (2) B (1) L (2)

Train Order from Stuart Town to Wellington Yard Limit Board



# 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))