Functional Safety Assessment of Train Management Control System

Kevin Anderson
Systra Scott Lister
7/600 Bourke Street, Melbourne VIC 3000
kanderson@systra.com

Abstract

The NSW Country Regional Network (CRN) was established in 2011. The legacy Train Management Control System (TMCS) was supported by a safety-related GPS Watchdog and the combination (TMACS) initially certified in 2000 covering train orders principally for the Parkes –Broken Hill Indian Pacific route and from 2011 rolled out across all relevant CRN territory.

Obviously, in the more than twenty years since TMACS was conceived and executed, technologies, techniques and assurance methods have changed markedly. At each step, tests of 'due diligence' have been applied to maintain system safety assurance.

Keywords: Train Management and Control System, Functional Safety Assessment.

1. Introduction

1.1 Background

Introduction of Train Order Working (TOW) to New South Wales was proposed by Freight Rail Train Operations Group in 1994. A Phase 1 report (VRJ Risk Engineers, 1994) used cause-consequence modelling to assess individual risks to crew by comparison of 'not less safe' with then Staff and Ticket /Electric staff safeworking. In parallel, research conducted for National Rail (Anderson, 1994) investigated the role of human error in railway operations pursuant to emerging standard AS 4048.1(Int.), (1992) – later superseded by draft IEC 1508 (1995) and then by AS 61508 from 1999.

The author raised concerns as to validation of proposed computer assistance – Train Management Control System (TMCS) as to its application to TOW (Anderson, 1995). Anderson (1977) went on to describe Functional Safety Assessor processes in the light of IEC 1508 (now AS 61508), from which emerged the concept of developing a safety-related GPS Watchdog to complement TMCS.

Anderson and Alam (1999) further explained the use of human error probability analysis in expressing individual fatality risks in relation to the above 'not less safe' criterion.

A formal Functional Safety Assessment of Train Orders Computer Systems was reported to Railways Safety Panel, Rail Services Australia (RSA), (R2A, 2000). This provided Certification that GPS Watchdog met Safety Integrity Level 2 (SIL 2) of AS /IEC 61508 and so the TMACS system went 'live' in September 2000. Anderson (2000) further described the enhanced integrity testing of the Train Order Computer System (now known as TMACS). RSA later established a group of Subject Matter Experts to decide on the safeworking encoding in preference to attempts to create algorithms to predict the rules.

1.2 TMACS Early Operations

A TMACS Functional Safety Audit was conducted in 2005 and reported to Rail Corporation New South Wales, based on Stakeholder meetings and interviews, system snap shots and review of safeworking encodings. (R2A, 2005). Subject to proceeding with recommendations relating to Portable Radios and Safeworking Rules, the FSA judged that, in four years of implementation, the system had demonstrated adequate integrity in meeting its safety requirements.

In the longer term it was stated that continuous improvement towards an electronic in-cab system of transmission and acknowledgement should be progressed.

This is not to say the system has been perfect. Anecdotally, on the plus side, its treatment of track workers as if they were 'trains' has been lauded, albeit with 'continuous improvement' updates. As investigated by ATSB (2011), a safeworking irregularity involving a freight train and an empty passenger train occurred at Manildra on 10 February 2010. The investigation report provides a detailed time sequence analysis of events that led to both trains having authority over the same piece of track – a clear 'loss of control'. The system of safeworking was described in some detail along with the interface between technology and individuals. It was noted that the GPS Watchdog performs location checks but is only accurate to +/- 100m (so unable to distinguish between occupancy of the main line track or the loop track). The situation was also exacerbated by a different radio on one of the freight train hauling locomotives that had been left on transmitting GPS data, raising numerous GPS Watchdog alarms.

Despite the technologies employed, safeworking was said to rely heavily on human actions. No specific deficiencies were found with either TMCS or GPS Watchdog. Rather, it was found that the controller made a number of mistakes: the controller failed to enter the road occupancy information, then

expected the crew to make contact (whereas they thought the opposite), and then the controller forgot about the track occupancies.

'Safety Alerts' have since been issued and other actions take to reduce the risk of recurrence to 'as low as reasonably practicable' (ALARP).

2 Country Regional Network

The Country Regional Network (CRN) covers 2,386 route kilometres of track in NSW and was established in 2011. John Holland Rail (JHR) manage Train Management and Control System (TMACS) for CRN at the Newcastle Network Management Centre (NMC). Technology provider 4Tel maintain the system. Systra is the Functional Safety Assessor (FSA) represented by the author.

The GPS train radio in 1995 provided the impetus for computerised Train Order Working in the form of TMACS (TMCS + GPS Watchdog). Train orders in 2000 were initially focussed on the Parkes –Broken Hill Indian Pacific route and from 2011 rolled out across all relevant CRN territory.

Every location, crossing loop, siding, junction and interface to signalled territory has its own set of safeworking encodings, expressed as tables comparing proposed authority to current authority with Rules for: Pass, Conflict Pass, Conflict Fail and Fail Safeworking subject to Exceptions such as 'Same train' replacing initial computer algorithms with Subject Matter Expert determined encodings.

2.1 TMACS Components

A good description of the current form of TMACS is given in Hjort, G (2015) - Implementation of electronic train order working on the NSW Country Regional Network. *AusRail 2015*. It reports that the above audit recommendation for in-cab data transmission has now been implemented by electronic authorities (EA).

Further initiatives for improved Work Train Orders, Special Orders and more are in train (sic).

The various components that comprise TMACS systems at the Network Management Centre (NMC) are:

- Network Control Officer (NCO) responsible for issuance and fulfilment of the various types of authority
- Communications touchscreen to Rail Traffic Crew (RTC)
- Train Management Control System (TMCS) – 3 screens
- Safety-related GPS Watchdog (certified to Safety Integrity Level (SIL 2) – 2 screens
- 4Trafic, 4Trak and 4ABS support systems – 3 screens – high reliability but not formal SIL

While only the GPS Watchdog has been formally classified to a SIL, other necessary risk reductions include reliability evidence to AS 61508 1#7.5.2.6 and consideration of human factors.

Organisational Safety Management Systems (SMS) ensure compliance with Rail Safety Act and Regulations and its underlying principle of reducing risks .. So Far As Is Reasonably Practicable (SFAIRP). This principle is also espoused in AS 61508 .. As Low As Reasonably Practicable (ALARP). Due diligence support to these principles is described in Anderson (2003) through the four common law tests of negligence – causation, foreseeability, presentability and reasonableness.

Further principles collated here are:

- Not less safe
- Compliance with standards
- Good Practice
- SFAIRP
- Continuous improvement

Further information on the Rail Safety National Law and SFAIRP is given in Anderson and Hughes (2012) The role of the FSA as Independent Safety Assessor (ISA) is further defined in Anderson and Mahmood (2014) using TMACS as a Case Study.

In relation to TMACS, the original certification in September 2000 by the author as Functional Safety Assessor (FSA) related to the safety-related 'GPS Watchdog' judged at SIL 2 to the then standard AS 61508 Edition 1. No claim was made for the Train Order Management System (TMCS) as itself safety-related, albeit reliability and evidentiary requirements were still applied per AS 61508 #1- 7.5.2.6. The safety-related GPS Watchdog not only enforces safeworking encodings but also monitors and alarms locomotive positions in relation to each other and limits of authorities. Refer methodology update papers: Anderson, K, Hughes, P. (2012): A due diligence approach to safety validation by means of SFAIRP. *Conference on railway engineering* (CORE 2012) and 'Anderson, K, Mahmood, T. (2014): Independent safety assessment – White paper.' Australian System Safety Conference (ASSC2014) *Journal of Research and Practice in Information Technology*.

The cause-consequence claims for necessary risk reduction though SIL rating, other technology and human factors have been maintained by the FSA to this day, now reporting to CRN /JHR. In the more than twenty years since TMACS was conceived and executed, technologies, techniques and assurance methods have changed markedly.

These changes include:

- digital voice /data train radio
- GPS accuracy and timeliness
- increasingly - networking of mobile devices

The five core elements of the Train Order System are:

- Train Management Control System (TMCS) – train planning and graph
- GPS Watchdog (GPS WD) – safety-related watchdog encoding and position checks (SIL 2)
- Authority Server – Electronic Authorities (EA)

- XML server to locomotives – In-cab equipment (ICE)
- TCMGR – graphs, alarms

Relatively recent support systems have been added. These have been mostly developed by technology specialist 4Tel and comprise:

- 4Site – Infrastructure monitoring using Internet-of-Things
- 4Trak – mobile tracking system including trains, track vehicles, road vehicles and staff
- 4Trip, 4ABS – rail access and billing system
- Occupation Server

In 2015, CRN /JHR implemented a number of packages for server platform migration and hardware replacement, override enhancements (in relation to use by a second person of Superintendent Codes), electronic authorities (EA) and work on track enhancements. Refer Advisian Pty Ltd. (2015): Functional Safety Assessment of TMACS package 2b, OE, 3 and 4 - First issue report to John Holland - including findings that GPS Watchdog is retaining its SIL 2 classification and that each of the packages investigated meets its functional requirements'

The Office of National Rail Safety Regulator (ONRSR) was involved under Notification of Change. The test for TMACS with ONRSR was to demonstrate that changes made since September 2000 (and there have been many) have not invalidated the original safety approval and certification of the GPS Watchdog to SIL 2 as SFAIRP.

Detailed tables were prepared in relation to risk management, system, hardware and software techniques and measures in compliance with the AS 61508 standard, with particular reference to highly recommended (HR) SIL 2 items. With ONRSR concurrence, ongoing developments in 2018 /2019 for Work Train Orders, Special Orders etc. are moderated by the Safeworking Encoding Panel (SEP) and witnessed by the author as FSA. The role of the SEP is to set the Rules and Exceptions for each location type (of which there are many: crossing, shunting, junction, yard to name a few). While the 2015 FSA addressed only comparisons with the original AS 61508-2000, consideration is now being given at least informally to Update to Edition 2 -2011.

There are myriad examples as to how TMACS has evolved to exploit developing technologies over the last 25-year period. With reference to safety assurance technology themes, the following points are relevant:

Safety and systems assurance: The original GPS Watchdog proof of concept was based on decoding CountryNet Train Radio GPS to determine location and marrying that location to the electronic Train Order Graphs, with the cross checking of safeworking encodings certified to Safety Integrity Level 2 (SIL 2).

Maintenance, risk and asset management: A risk management approach continues to be used to quantify the risk profile of:

- Train and Track Occupancy location
- Control system
- Communications
- Driver performance

The four sources of hazard were considered with different control measures impacting differently:

- Train and Track Occupancy Location error: Reduced by greater frequency of ICE messages
- Controller error: Addressed after ATSB report, unchanged in recent times
- Communications risk: Considered to have halved with In-Cab Equipment (ICE) electronic authorities
- Crew error: Marginally improved with ICE

Keeping our people, customers and workplaces safe: As above, the GPS Watchdog was developed to Safety Integrity Level 2 as per AS 61508 using agreed techniques and measures, separate Ada coding to TMCS C code, comprehensive testing and WIKI (now JIRA – Issue and Project Tracking Software - https://www.atlassian.com/software/jira for a variety of documentation tasks.

Safety in design, engineering and construction: A process of functional specification, coding and testing was employed in the system realisation to maintain assurance in compliance to SIL 2.

Power, signalling and communication upgrades: TMACS is a communications-based system and has benefited greatly from ICE in locomotives, enabling electronic authorities.

Automation and innovations in technology: ICE data has significantly enhanced the frequency and reliability of GPS train location plots.

Managing skills, assets and resources: The new technologies have enhanced Controller efficiency and operations at NMC.

Safety Assurance: Technical documentation was matched to system safety assurance evidence including use of Goal Structured Notation (GSN).

Hardware: Modern hardware and Disaster Recovery Facilities (DRF) are now in place.

Software: Detailed and Internal requirements and data flow diagrams were developed for implementation in the Ada language. Key routines included 'Train', 'Snapshot Manager', 'Authority', 'Safe Working Rules'.

Configuration management: A number of change packages were implemented for TMACS in 2015, including:

- Server Platform Migration and Hardware Enhancements
- Override Enhancements, including use of Superintendent Codes
- Electronic Authorities, including considerations of Rail Traffic Crew (RTC) risks, safeworking procedural breaches modified by more frequent ICE /GPS position data and Network Management Centre (NMC) controls

- Work on Track Enhancements – Terminal Locations and Track Vehicle Enhancements

Tables of compliance with Techniques and Measures specified for SIL 2 covered:

- Requirements – structured diagrams, semi-formal methods, modular approach, recovery, Ada programming language, tools proven in use
- Detailed Design – defensive programming, coding standards, structured programming
- Software Module Testing – dynamic analysis and testing, data analysis
- Software Integration Testing – functional and black box testing, interface testing
- Hardware /Software Integration and Software Safety Validation - impact analysis, software configuration, software verification, walkthrough /design reviews, analysis and testing
- Modification – management of change processes

Post-commissioning review found:

- There were no electronic authority (EA) system failures
- Ten field events were investigated and workflows between NCO and RTC were updated
- Some minor bugs were revealed and prioritised for future releases
- Operational benefits of EA were found to satisfy Goal Structured Notation (GSN) goals
- ONRSR further considered a number of items, focussing on Highly Recommended (HR) recommendations for SIL 2 including:
  - Use of certified tools and translators
  - Impact analysis – Requirements Specification and traceability matrix
  - No dynamic objects – legacy code
  - Performance modelling resources
  - Response timings and memory constraints – software memory and response
  - Design review – checked /verified
  - A series of updated Safety Assurance Reports and meetings took place post-commissioning, focused on change management and revised operational configurations.

These led to full approvals and support to the FSA judgement that the GPS Watchdog has retained its SIL 2 rating in accordance with the original AS 61508 Edition 1 2000 i.e. GPSWD is not 'less safe'. In addition, many of the new techniques and measures introduced in AS 61508 Edition 2, 2011 have been noted. These do not replace any techniques or measures initially followed but may offer advantages to current good practice and continuous improvement. However, at this point in time, the requirement for the FSA was only to assess changes against the original year 2000 certification.

Conclusions

The paper outlines five safety principles expounded by the author. From these, the following conclusions have been drawn:

- Not less safe: The original risk assessment made in 1994 was predicated on demonstration that train order working would be 'not less safe' compared to Staff & Ticket /Electric staff working. By the time that the CRN was established in 2011, TMACS had been in operation for some ten years and, notwithstanding the above related ATSB investigation, the decision was made by the CRN to roll out TMACS on all relevant NSW country line.
- Compliance with standards: The TMCS was originally developed without reference to the emerging safety critical standards. As above, difficulties with validation of such a legacy system led to the addition of the GPS Watchdog rated at SIL 2 in compliance with IEC 1508 /AS 61508
- Good Practice: The original concept for the GPS Watchdog took advantage of GPS signals embedded in CountryNet Train Radio. The introduction of National Train Communication System In-Cab Equipment (ICE) from 2007 to 2013 has significantly improved the frequency of GPS messages. Over that time, the TMACS hardware has been brought up-to-date and the GPS software changes re-certified to SIL 2.
- SFAIRP: Arguably, the difference between ALARP and SFAIRP is that the former looks to achieve tolerable risk through 'necessary risk reduction' while the latter focusses on the more stringent test of tolerability: 'Tolerable only if further risk reduction is impracticable or if its cost is grossly disproportionate to the improvement gained'. As was said in the abstract - At each step tests of 'due diligence' have been applied to maintain system safety assurance – the summation of all of these steps is expressed in compliance with the Rail Safety National Law in the service provider SMS
- Continuous improvement: Twenty-five years of digital train orders has led to enhanced capacity planning and scheduling and enhanced safeworking rules validated by Subject Matter Experts and Safety Integrity Level (SIL) certified by GPS Watchdog. The author as FSA has been involved in realisation and assurance over that entire period. This demonstrates that TMACS as a whole is modern with the original cores of train control TMCS and safety-related GPS Watchdog SIL 2 still representing good practice. There is always room for improvement. As changes have been made to TMCS, consequential changes have been required for GPS Watchdog. For example, safety assurance of changes made to date has focussed on comparison with the year 2000 certification. The update of the standard AS 61508 to Edition 2 (2011) has yet to be countenanced.

The Author wishes to acknowledge the support of John Holland Rail, 4Tel and Systra Scott Lister in preparation of this paper. However, opinions expressed in this paper are those of this author only.

References

Advisian Pty Ltd. (2015): Functional Safety Assessment of TMACS package 2b, OE, 3 and 4. First issue report to John Holland, including findings that GPS Watchdog as retaining its SIL 2 classification and that each of the packages investigated meets its functional requirements.

Anderson, K. (1994) Estimation of Human Error probability in Railway Operations. *Discussion Paper*. National Rail.

Anderson, K. (1995) Functional Safety of Computer Systems in Railway Operations, *Conference on railway engineering* (CORE 1995). –

Anderson, K. (1997) Train Order Computer Systems *Experience Report*. Collected proceedings of *Australian Workshops on Industrial Experience with safety critical systems and software.*

Anderson, K, Alam, T. (1999): Functional Safety Assessment of Train Order Working. Collected proceedings of *Australian Workshops on Industrial Experience with safety critical systems and software*.

Anderson, K. (2000): Train Order Computer Systems. *Conference on railway engineering* (CORE 2000).

Anderson, K. (2002): Establish Risks As Low As Reasonably Practicable (ALARP), Rail Industry Briefing, July 2002.

Anderson, K (2003): State-of-the-art Systems Assurance Techniques *Railway Technology in the New Millennium* – the Malaysian Tradition - RailTech 2003, Kuala Lumpur.

Anderson, K, Hughes, P. (2012): A due diligence approach to safety validation by means of SFAIRP. *Conference on railway engineering* (CORE 2012).

Anderson, K, Mahmood, T. (2014): Independent safety assessment – White paper.' Australian System Safety Conference (ASSC2014). *Journal of Research and Practice in Information Technology*.

AS 4048.1(INT) – 1992. Functional safety of electrical /electronic /programmable electronic systems – Generic aspects General requirements

AS 61508 -2000 Functional safety of electrical /electronic /programmable electronic safety-related systems.

AS 61508 -2011 Functional safety of electrical /electronic /programmable electronic safety-related systems. Parts 0-7. Second edition

Hjort, G. (2015): Implementation of electronic train order working on the NSW Country Regional Network. *AusRail 2015*.

JIRA – Issue and Project Tracking Software - https://www.atlassian.com/software/jira - accessed 15/3/2019

IEC 1508 draft international standard – Functional safety: Safety-related systems (1995)

Risk & Reliability Associates Pty Ltd (R2A) (2000): Functional Safety Assessment of Train Orders Computer Systems. Report to *Railways Safety Panel*, Rail Services Australia providing Certification that GPS Watchdog meets Safety Integrity Level 2 of AS /IEC 61508

Risk & Reliability Associates (R2A) (2005): TMACS Functional Safety Audit. *Audit report* to Rail Corporation New South Wales.

VRJ Risk Engineers (1994): Risk Analysis of train order system implementation. *Phase 1 report to Freight Rail Train Operations Group.*